Carlos Ivorra Castillo

HISTORIA DE LA FUNDAMENTACIÓN DE LA MATEMÁTICA

Pero, ¿las matemáticas necesitan certeza absoluta para su justificación? En particular, ¿por qué necesitamos estar seguros de que una teoría sea consistente o de que pueda derivarse de una intuición absolutamente cierta del tiempo puro, antes de usarla? En ninguna otra ciencia hacemos tales exigencias. En física, todos los teoremas son hipotéticos; adoptamos una teoría mientras haga predicciones útiles y la modificamos o la descartamos en cuanto deja de hacerlo. Esto es lo que les pasó a las teorías matemáticas en el pasado, donde el descubrimiento de contradicciones ha llevado a la modificación en las doctrinas matemáticas aceptadas hasta el momento de ese descubrimiento. ¿Por qué no deberíamos hacer lo mismo en el futuro?

Haskell B. Curry.

Índice

Preámbulo **ix**

Capítulo I: Un siglo de historia: 1870–1970 **1**

1 Preludio: La matemática antigua . . . 1
2 Antecedentes: Series trigonométricas . . . 2
3 El inicio de la historia . . . 4
4 Los números reales según Dedekind . . . 5
5 Conjuntos numerables y no numerables . . . 6
6 Los números ordinales . . . 9
7 La teoría de conjuntos . . . 13
8 Los números naturales según Dedekind . . . 14
9 Peano y Frege . . . 16
10 El teorema de Cantor . . . 18
11 La medida de Jordan . . . 19
12 La antinomia de Burali-Forti . . . 20
13 La medida de Borel . . . 26
14 Inducción y recursión transfinita . . . 27
15 La paradoja de Cantor . . . 29
16 El formalismo . . . 29
17 Los álefs . . . 31
18 La paradoja de Russell . . . 32
19 La medida de Lebesgue . . . 33
20 El axioma de elección . . . 35
21 La teoría descriptiva de conjuntos . . . 37
22 Poincaré . . . 38
23 El predicativismo . . . 41
24 Espacios métricos . . . 43
25 Los axiomas de Zermelo . . . 45
26 Los *Principia Mathematica* . . . 48
27 La teoría de conjuntos de Hausdorff . . . 51
28 Conjuntos analíticos . . . 52
29 El intuicionismo . . . 53
30 *Fundamenta Mathematicae* . . . 54
31 La paradoja de Berry . . . 56
32 Lenguajes formales . . . 57
33 La paradoja de Skolem . . . 61
34 Finitismo, platonismo e intuicionismo . . . 66
35 La teoría de von Neumann . . . 67
36 El programa de Hilbert . . . 70
La intuición . . . 74
37 El teorema de Kőnig . . . 77
38 La teoría de la demostración . . . 78
39 El teorema de completitud semántica . . . 81
40 El axioma de regularidad . . . 83

41 Cardinales fuertemente inaccesibles . . . 87
Cardinales $\mathbb{R}$-medibles . . . 90
42 El álgebra de van der Waerden . . . 91
43 Conjuntos proyectivos . . . 91
44 La lógica intuicionista . . . 93
45 Los teoremas de incompletitud . . . 93
46 Funciones recursivas . . . 94
47 Matemática y metamatemática . . . 97
48 Modelos no estándar . . . 100
49 La formalización de la lógica . . . 103
La consistencia de los cardinales inaccesibles . . . 105
50 Representación de funciones recursivas . . . 106
51 ω-consistencia . . . 108
52 La teoría de von Neumann-Bernays I . . . 108
53 Gödel y el intuicionismo . . . 109
54 El teorema de Tarski . . . 110
55 Descripciones . . . 112
56 Deducción natural . . . 114
57 El cálculo secuencial . . . 117
58 El lema de Zorn . . . 121
59 El platonismo . . . 123
60 La consistencia de la aritmética . . . 125
61 El problema de la decisión . . . 133
62 La teoría de von Neumann-Bernays II . . . 139
63 Los Nuevos Fundamentos de Quine . . . 140
64 Funciones recursivas parciales . . . 141
65 La Segunda Guerra Mundial . . . 144
66 Nicolas Bourbaki . . . 144
67 Las condiciones de Hilbert-Bernays . . . 147
68 La consistencia del axioma de elección y de la hipótesis del continuo . . . 151
69 El problema de Suslin . . . 162
70 El fin de la guerra . . . 164
71 Categorías . . . 165
72 La hipótesis del continuo generalizada implica el axioma de elección . . . 167
73 Henkin y el teorema de completitud . . . 167
74 Álgebras de Boole . . . 171
75 ZFC y NBG . . . 175
Clases en ZF . . . 176
76 La *Introducción a la metamatemática* de Kleene . . . 181
77 La *Lógica para matemáticos* de Rosser . . . 186
78 Determinación . . . 190
79 La aritmética de Robinson . . . 195
80 La aritmética recursiva primitiva . . . 197
81 El teorema de Löb . . . 205
82 La teoría de conjuntos de Morse-Kelley . . . 206
83 La teoría de conjuntos de Bourbaki . . . 207
84 La teoría de modelos . . . 218
Submodelos . . . 225
Inmersiones . . . 225
Inmersiones elementales . . . 226
Cardinales sin el axioma de elección . . . 227
85 El teorema de reflexión . . . 228
Conceptos absolutos . . . 230
86 La consistencia de la hipótesis del continuo generalizada . . . 233
87 El décimo problema de Hilbert . . . 234
88 Ultraproductos . . . 236

89 Cardinales medibles . . . 240
90 El castor laborioso . . . 245
91 La independencia de la hipótesis del continuo . . . 247
Constructibilidad relativa . . . 247
92 La *Introducción a la lógica matemática* de Mendelson . . . 254
93 El axioma de determinación . . . 256
94 La teoría de conjuntos de Morse . . . 260
95 El desarrollo del forcing . . . 261
Feferman . . . 261
Lévy . . . 263
Solovay . . . 264
Cohen . . . 266
96 La *Lógica matemática* de Kleene y la de Shoenfield . . . 272
Modelos booleanos . . . 275
Conjuntos genéricos . . . 277
97 Los Ángeles 1967 . . . 280
1. Forcing no ramificado (Shoenfield) . . . 280
La independencia del axioma de elección . . . 282
2. Problemas no resueltos en la teoría de conjuntos (Erdős, Hajnal) . . . 284
3. La consistencia de la HCG con la existencia de un cardinal medible (Silver) . . . 285
4. Cardinales $\mathbb{R}$-medibles (Solovay) . . . 285
5. Sobre modelos de la teoría de conjuntos sin AE (Jech) . . . 286
6. Observaciones sobre las discusiones populares sobre fundamentos (Kreisel) . . . 287
7. Comentarios sobre la fundamentación de la teoría de conjuntos (Cohen) . . . 289
La crisis de los fundamentos . . . 293
98 Las *Pruebas de independencia simplificadas,* de Rosser . . . 294
Modelos booleanos y *forcing* . . . 296
99 Aplicaciones de la teoría de extensiones genéricas . . . 301
El axioma de Martin . . . 303
100 El formalismo moderno . . . 306

Capítulo II: Epílogo al capítulo I **315**
2.1 Cardinales grandes . . . 315
El axioma de determinación . . . 318
El problema de los cardinales singulares . . . 318
Axiomas de forcing . . . 320
Cardinales de Mahlo . . . 320
2.2 Constructibilidad . . . 321
2.3 Afirmaciones indecidibles en matemáticas . . . 322
Afirmaciones indecidibles en topología . . . 322
Afirmaciones indecidibles en análisis . . . 323
Afirmaciones indecidibles en álgebra . . . 325
Ecuaciones diofánticas indecidibles . . . 326
2.4 La teoría descriptiva de conjuntos . . . 326

Capítulo III: Nuevas alternativas a la matemática clásica **329**
3.1 El constructivismo de Bishop . . . 329
3.2 El análisis no estándar . . . 341
La teoría de Nelson . . . 343
La teoría de Hrbáček . . . 349
Balance . . . 351
3.3 Otras teorías alternativas . . . 352
La teoría de Kripke-Platek . . . 352
Los Nuevos Fundamentos . . . 352
La teoría de Mac Lane . . . 353
El Cálculo de Construcciones . . . 356

Capítulo IV: La formalización de la metamatemática **357**
4.1 La aritmética recursiva primitiva . . . 358
4.2 La aritmética de Peano con inducción restringida . . . 360
4.3 La lógica de segundo orden . . . 363
La aritmética de Peano de segundo orden I . . . 365
La semántica estándar y la semántica de Henkin . . . 365
La Aritmética de Peano de segundo orden II . . . 366
4.4 Comprensión aritmética y comprensión recursiva . . . 368
Comprensión aritmética . . . 368
Inducción de primer y segundo orden . . . 369
Comprensión recursiva . . . 370
Matemáticas en ACR_0 . . . 371
La formalización de la lógica en ACR_0 . . . 372
Modelos en ACR_0 . . . 373
4.5 El lema de Kőnig débil . . . 375
4.6 Recursión aritmética . . . 379
La consistencia de RA_0 . . . 382
Recursión transfinita . . . 383

Apéndice A: Glosario de términos mencionados en el capítulo I **385**

Preámbulo

El capítulo I de este libro expone en orden cronológico el proceso que ha llevado hasta la concepción moderna de las matemáticas, explicando las ideas relevantes, detallando las definiciones y demostraciones que hemos considerado ilustrativas, pero omitiendo los aspectos técnicos y rutinarios. Esto hace que muchas demostraciones no estén completas, en el sentido de que a menudo contengan pasos de tipo "se puede demostrar que..." Esto puede resultar desagradable a un matemático, pero debería pensar en este texto como un término medio entre un libro con demostraciones detalladas y un *survey* en el que se presentan y discuten resultados sin sus demostraciones. El objetivo de las demostraciones (a veces parciales) que presentamos es el de transmitir las ideas principales en las que se basan. Detallar todas las demostraciones presentadas aquí multiplicaría por diez el tamaño de este libro.

Nuestro propósito es que el lector de forme una idea lo suficientemente clara de estas ideas que le pueda servir de orientación a la hora de enfrentarse a los textos técnicos que presentan los detalles de la historia. Ni siquiera es evidente en absoluto qué hay que entender por "fundamentación de las matemáticas", pero precisamente la filosofía de este trabajo es no tratar de explicarlo *a priori,* sino intentar que el lector se forme una idea lo más fiel posible al respecto a través del desarrollo histórico.

Por otro lado, el lector siempre tiene la posibilidad de leer el libro saltándose las demostraciones, e incluso las definiciones técnicas y concentrarse en la parte puramente histórica. Y también está, por supuesto, la opción intermedia de interesarse por unas demostraciones y descartar otras (con el único riesgo intrascendente de volver un poco más incompletas aquellas demostraciones que se apoyen en otras previas).

Los años en negrita marcan el orden cronológico (forman una sucesión creciente), mientras que los demás corresponden a fechas anteriores o posteriores al año "en curso" con antecedentes o consecuencias futuras.

Dado que el orden cronológico dificulta buscar en el texto las definiciones de conceptos tratados previamente, hemos incluido un apéndice con las definiciones de los conceptos más destacados mencionados en el capítulo I.

Este capítulo I cubre esencialmente un siglo de historia: desde la publicación en 1870 del primer artículo de Cantor sobre series trigonométricas, que lo llevaría al descubrimiento de la teoría de ordinales y cardinales, hasta el año 1970, en el que la teoría de conjuntos ya estaba plenamente consolidada y en un vertiginoso proceso de expansión.

No obstante, como el relato deja numerosos episodios inacabados y sería caótico tratar de narrar los desenlaces manteniendo el orden cronológico (que nos obligaría a saltar desordenadamente de un tema a otro una y otra vez), en el capítulo II resumimos brevemente en secciones temáticas la evolución de varios aspectos de la teoría de conjuntos tratados en el capítulo I a partir de la década de los 70, sin tratar de ser exaustivos ni, mucho menos, de presentar los avances más destacados en la teoría de conjuntos, que, por otro lado, ya no se pueden considerar propiamente avances en la fundamentación de la matemática, sino más bien avances en una de sus disciplinas.

En el capítulo III discutimos algunos hechos sobre la concepción moderna de las matemáticas que han sido objeto de debate a partir de la década de los 70. Finalmente, en el capítulo IV nos ocupamos, también en forma temática y no cronológica, de algunos avances más recientes de la lógica y la teoría de conjuntos que sí que tienen gran relevancia a la hora de entender la fundamentación de la matemática. Concretamente, como veremos en los primeros capítulos, la definición y el análisis de las teorías axiomáticas formales que requiere la fundamentación de la matemática tiene que llevarse a cabo necesariamente en un marco conceptual informal intuitivo, por lo que cabe preguntarse qué presupuestos intuitivos son necesarios. Lo que haremos en el capítulo IV será presentar varias teorías axiomáticas mucho más débiles que las teorías de conjuntos usuales, hasta el punto de que podemos afirmar que sus axiomas son intuitivamente verdaderos en un sentido preciso, pero lo suficientemente fuertes como para formalizar todos los resultados metamatemáticos necesarios.

Capítulo I

Un siglo de historia: 1870–1970

1 Preludio: La matemática antigua Los vestigios más antiguos que tenemos de las matemáticas de las civilizaciones antiguas consisten en fórmulas y técnicas para resolver ciertos problemas aritméticos y geométricos, a menudo presentados indirectamente a través de ejemplos concretos. Esto cambió sustancialmente con la matemática griega. Fueron los griegos quienes introdujeron la idea de que cada afirmación matemática debía ser demostrada en toda su generalidad a partir de resultados previos, tomando como punto de partida unos principios o postulados explícitos. Hay constancia de que se escribieron muchos "libros de texto", que presentaban razonadamente los resultados básicos de la aritmética y la geometría. Muchos de ellos se han perdido, pero el más famoso y completo que se conserva es el conocido como los *Elementos,* de Euclides, redactados hacia el **300 a.C.**, y que se han usado como libro de texto hasta hace relativamente poco tiempo —Albert Einstein los recordaba como uno de los libros que más influyeron en él de niño— y que ejercieron también una gran influencia sobre otros manuales de geometría.

Los *Elementos* fueron considerados durante siglos como el canon de rigor matemático: a partir de unas definiciones y unos axiomas (clasificados como "nociones comunes" y "postulados"), cada enunciado iba seguido indefectiblemente de su correspondiente demostración. Esto confería a las matemáticas un *status* de "ciencia exacta", en la que todos los resultados pueden justificarse plenamente sin el menor resquicio para la duda.

Así, en **1677**, se publicó póstumamente el tratado que el filósofo Baruch Spinoza había titulado *"Ética demostrada según el orden geométrico",* donde lo del "orden geométrico" no quería decir que hablara de círculos y de triángulos, sino que cada afirmación era demostrada "rigurosamente" a partir de afirmaciones y definiciones previas y de unos postulados básicos, tal y como hacían los geómetras.

Paradójicamente, mientras Spinoza trataba de imitar el "orden geométrico" en su filosofía, los matemáticos hacía mucho que se habían alejado de él. El "orden geométrico" no era, en general, el "orden matemático". Los algebristas hablaban de "números imaginarios", que eran unos números que claramente no podían existir, pero con los que se podía trabajar y se podían usar en cálculos que, de un modo u otro, acababan proporcionando resultados "reales" coherentes y ciertos. Los analistas hablaban de "infinitésimos", que eran unas cantidades menores que cualquier cantidad positiva, pero a la vez no nulas, si bien en los momentos oportunos se las podía considerar nulas. Matemáticos de primera línea discrepaban en si una suma como

$$1 - 1 + 1 - 1 + 1 - 1 + \cdots$$

era o no igual a 0, y obviamente no era por falta de luces, sino por falta de un concepto preciso sobre cómo había que entender una suma de infinitos sumandos.

Los matemáticos eran conscientes de que esta falta de precisión dificultaba el avance de su ciencia, no sólo porque cada vez era más difícil juzgar si una teoría matemática era correcta o tenía alguna laguna, sino porque incluso hacía difícil discernir si se trataba de una teoría profunda o de un completo despropósito. Matemáticos como Fourier o Galois tuvieron problemas para que se reconociera su trabajo, en parte por la imprecisión de sus exposiciones, pero en parte también porque no estaba claro cómo había que entender muchos conceptos supuestamente bien conocidos, como, por ejemplo, si una función definida a trozos era "realmente" una función, o si la gráfica de una función podía tener tramos verticales, etc.

Por ello, a lo largo de los siglos XVIII y XIX, a la vez que se ensanchaban cada vez más los límites superiores del conocimiento matemático, se fueron desarrollando paulatinamente sus cimientos, dando definiciones cada vez más precisas y reduciendo los conceptos más complejos a los más simples.

2 Antecedentes: Series trigonométricas En **1807** Joseph Fourier presentó su *Memoria sobre la propagación del calor en los cuerpos sólidos,* en la que planteaba un modelo matemático sobre cómo evoluciona con el tiempo la temperatura de un sólido. En el caso más simple, de una barra sólida, su modelo se reduce a la ecuación diferencial

$$\frac{\partial^2 T}{\partial x^2} = k\frac{\partial T}{\partial t},$$

donde $T(x,t)$ representa la temperatura en el punto x de la barra en el tiempo t, para $a \leq x \leq b$, donde a y b son los extremos de la barra. Naturalmente, para que el problema esté determinado hay que especificar la función $f(x)$ que da la temperatura inicial de la barra: $T(x,0) = f(x)$, para $a \leq x \leq b$.

Fourier resolvió esta ecuación, pero, para que la solución obtenida satisficiera la condición inicial, era necesario que $f(x)$ pudiera expresarse en términos de una serie trigonométrica:

$$f(x) = a_0 + \sum_{n=1}^{\infty} (a_n \cos nx + b_n \operatorname{sen} nx), \qquad -\pi \leq x \leq \pi,$$

donde, por simplicidad, aquí convenimos en que la barra se extiende concretamente en el rango $-\pi \leq x \leq \pi$.

Fourier afirmó que cualquier función dada $f(x)$ admite una expresión de esta forma y, más aún, calculó exactamente cuánto tenían que valer sus coeficientes:

$$a_0 = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)\,dx, \quad a_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos nx\,dx, \quad b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\operatorname{sen} nx\,dx.$$

Sin embargo, Lagrange y Laplace plantearon serias dudas sobre la validez de sus argumentos y su memoria no fue publicada. El Instituto de Francia convocó un premio sobre el tema en **1811**, y Fourier lo ganó en **1812** con una versión expandida de su trabajo anterior, pero tampoco fue publicado. Finalmente, en **1822** Fourier logró publicar su *Teoría analítica del calor,* donde insistía en que las funciones $f(x)$ que consideraba eran "arbitrarias", es decir, que no suponía que venían dadas por una determinada expresión algebraica:

> *En general, la función $f(x)$ representa una sucesión de valores u ordenadas, cada una de las cuales es arbitraria. Dados infinitos valores para la abscisa x, existe un número igual de ordenadas $f(x)$. Todas tienen valores numéricos reales, ya sean positivos, negativos o nulos. No suponemos que estas ordenadas estén sujetas a una ley común; se suceden de cualquier manera, y cada una de ellas se da como si fuera una sola cantidad.*

Este concepto era totalmente novedoso y, de hecho, no está claro en qué medida entendía Fourier esa generalidad, porque todos los ejemplos que ponía correspondían, a lo sumo, a funciones definidas a trozos con un número finito de discontinuidades. Pero, incluso para este tipo de funciones, se planteaba entonces cómo había que entender las integrales que Fourier consideraba. Justo un año después, en **1823**, Augustin Louis Cauchy publicó su *Resumen de las lecciones impartidas en la Real Escuela Politécnica sobre cálculo infinitesimal,* donde, además de introducir por primera vez las definiciones $\epsilon - \delta$ de límite y derivada, definió el concepto de integral para una función continua arbitraria. Ahora, si el integrando no era una función continua, ya no estaba claro de qué hablaba Fourier.

Si se interpreta literalmente la cita anterior, Fourier pretendía que cualquier función definida en un intervalo cerrado podía integrarse. Pero, aun suponiendo que así fuera, tampoco estaba claro que la serie que Fourier había asociado a la función $f(x)$ tuviera que converger o, incluso, si lo hacía, que convergiera precisamente a $f(x)$. Lo único que había "justificado" Fourier (supuesto que las integrales que usaba tuvieran sentido y que fueran válidos sus cambios entre sumas infinitas e integrales) es que si una función admitía un desarrollo en serie trigonométrica, sus coeficientes tenían que ser los que él había calculado.

Sobre esto, un joven de 24 años llamado Peter Gustav Lejeune Dirichlet demostró en **1829** que si una función $f(x)$ está definida para $-\pi \leq x \leq \pi$, es continua salvo a lo sumo en un número finito de puntos, está acotada y es monótona a trozos (es decir, que el intervalo completo puede dividirse en un número finito de intervalos en cada uno de los cuales f es creciente o decreciente), entonces la *serie de Fourier* de f converge a f en todos los puntos en los que es continua (y en los puntos donde no lo es converge al punto medio de sus límites laterales).

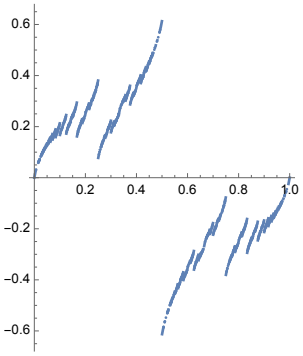
En realidad, el argumento de Dirichlet no requería que la función fuera continua salvo a lo sumo en un número finito de puntos. Esta hipótesis la ponía sólo porque así podía definir las integrales necesarias como la suma de las integrales en los intervalos de continuidad. Por lo tanto, en la medida en que tuviera sentido integrar funciones que fueran discontinuas en infinitos puntos, el resultado de Dirichlet valdría igualmente.

En **1851**, a sus 25 años, se doctoró en Gotinga Bernhard Riemann, bajo la dirección de Karl Friedrich Gauss (y en su tesis introdujo las llamadas *ecuaciones de Cauchy-Riemann* y el concepto de *superficie de Riemann*). En **1854** Riemann presentó su memoria de habilitación en Gotinga. Tenía que presentar tres propuestas de tema en orden de preferencia para que el tribunal eligiera uno. Lo usual era que se eligiera el primero o el segundo. Riemann propuso:

- Sobre la representación de una función sobre una serie trigonométrica.
- Sobre la teoría de la electricidad, el galvanismo y la conexión entre ellos y la luz.
- Sobre las hipótesis que subyacen en los fundamentos de la geometría.

Para su espanto, Gauss eligió el tercero, y tuvo que prepararlo desde cero en poco más de un mes. En su memoria, sentó las bases de lo que hoy se conoce como la geometría riemanniana.

Lo que tenía preparado sobre los desarrollos de funciones en series trigonométricas quedó inédito. En ese trabajo, generalizando ligeramente la definición de integral de Cauchy, pudo poner un ejemplo de función integrable en cualquier intervalo acotado que era discontinua en todos los números racionales de la forma p/q, con p impar y q par (con lo que tiene infinitos puntos de discontinuidad en cualquier intervalo). Concretamente, el ejemplo de Riemann era la función siguiente, representada en la gráfica:



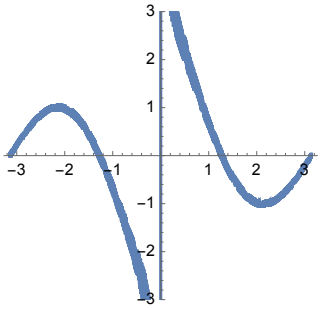
$$f(x) = \sum_{n=1}^{\infty} \frac{\phi(nx)}{n^2},$$

donde ϕ es la función periódica de periodo 1, que para $0 \leq x \leq 1$ viene dada por $\phi(x) = x$.

En **1855** se doctoró en Gotinga Richard Dedekind, que fue el último alumno de doctorado de Gauss, pues éste murió ese mismo año a los 77 años. Su cátedra fue ocupada por Dirichlet, pero murió en **1859** de un ataque al corazón. En **1866** estalló una guerra entre los reinos de Hannover y Prusia, Riemann huyó de Gotinga y murió en Italia, a los 39 años. Su trabajo sobre la *integral de Riemann* y sobre las series trigonométricas se publicó póstumamente en **1868** y su ejemplo causó sensación. Los matemáticos nunca habían visto una función tan extraña.

Un año antes, en 1867, se había doctorado en Berlín un joven de 22 años llamado Georg Cantor, bajo la dirección de tres de los matemáticos más importantes del momento: Karl Weierstrass, Ernst Kummer y Leopold Kronecker. En **1869** Cantor dejó Berlín para ocupar una plaza en la universidad de Halle. Allí entabló amistad con Heinrich Eduard Heine, que estaba trabajando en el problema de los desarrollos en series trigonométricas y le planteó el problema de la unicidad: si una función $f(x)$ definida en un intervalo admite un desarrollo en serie trigonométrica, ¿los coeficientes de la serie están unívocamente determinados por f?

No estaba claro en principio que los coeficientes de la serie trigonométrica tuvieran que ser necesariamente los determinados por las fórmulas de Fourier. De hecho, años más tarde, en 1925, Andréi Nikoláyevich Kolmogórov publicaría su trabajo *Sobre las funciones armónicas conjugadas y las series de Fourier,* en el que mostraba un ejemplo de serie trigonométrica convergente en todos los puntos, pero que no es una serie de Fourier, porque no es integrable.[1] Se trata simplemente de la función



$$f(x) = \sum_{n=2}^{\infty} \frac{\operatorname{sen} nx}{\log n}$$

cuya gráfica es la que muestra la figura (el grosor del trazo se debe a las rápidas oscilaciones de la función). La función es continua en todo punto $-\pi \leq x \leq \pi$ excepto en $x = 0$.

Riemann no había logrado resolver el problema, y en **1870** Heine probó la unicidad bajo el supuesto de que la función $f(x)$ sea continua y de que la serie converja uniformemente, lo cual era una restricción muy fuerte.

[1] No es integrable Lebesgue.

3 El inicio de la historia Ese mismo año de **1870**, Cantor publicó su artículo *Sobre un teorema concerniente a las series trigonométricas,* en el que eliminaba la hipótesis de la convergencia uniforme, es decir, demostraba que si una serie trigonométrica converge a una función f en un intervalo, entonces sus coeficientes están unívocamente determinados por f. En **1871** publicó una breve nota titulada *Sobre series trigonométricas* en la que señalaba que la unicidad seguía dándose aunque la serie no converja en un número finito de puntos. No obstante, Cantor constató que esta condición, aunque suficiente, no era necesaria, y que los coeficientes eran únicos igualmente si la convergencia fallaba en un conjunto infinito de puntos, siempre y cuando tuviera una cierta "estructura". Sin embargo, a la hora de expresar esa estructura lo más claramente posible, se encontró con el problema de que no existía un concepto bien definido de "número real" que le permitiera justificar sus argumentos. Por ejemplo, a pesar de que los "infinitésimos" habían sido descartados hacía tiempo de la teoría matemática, aún había quienes seguían usándolos y Cantor no tenía argumentos para probar que no existen.

Esto lo llevó a reflexionar sobre el concepto de número real, y en **1872** publicó su artículo *Sobre la extensión de un teorema de la teoría de series trigonométricas,* en el que incluía una construcción explícita de los números reales. Concretamente, Cantor consideraba una familia de sucesiones de números racionales a las que llamaba "sucesiones fundamentales", que eran lo que actualmente se conoce como "sucesiones de Cauchy", y estipulaba que cada una de ellas "tenía asociado" un número real que se convertía en su límite,[2] con la precaución de que, dos sucesiones fundamentales determinan el mismo número real si su diferencia converge a 0.

Con este marco, Cantor pudo enunciar una condición suficiente para la unicidad de los desarrollos en serie trigonométrica mucho más general que la finitud del conjunto de puntos donde no hay convergencia. Para expresarlo más cómodamente, introducimos el concepto siguiente:

> **Definición** Un conjunto C contenido en el intervalo $[\pi, \pi]$ es un *conjunto de unicidad* si toda serie trigonométrica que converge a la función nula salvo a lo sumo en los puntos de C tiene todos sus coeficientes nulos.

Esto implica que si dos series trigonométricas convergen a una misma función f salvo a lo sumo en los puntos de C, entonces tienen los mismos coeficientes (pues la diferencia de ambas converge a la función nula, luego tiene sus coeficientes nulos).

En estos términos, en su artículo anterior, Cantor había demostrado que todos los conjuntos finitos son conjuntos de unicidad, y ahora había encontrado una familia mayor de conjuntos con esta misma propiedad.

Para cada conjunto C, Cantor definió su *conjunto derivado* como el conjunto C' formado por todos los *puntos de acumulación* de C, es decir, todos los puntos que pueden obtenerse como límite de una sucesión de puntos de C. Cantor definió un conjunto *cerrado* como un conjunto que contiene a todos sus puntos de acumulación. Para cualquier conjunto C, su conjunto derivado C' siempre es cerrado.

En principio, no hay relación entre C y C', en el sentido de que un punto de C puede estar o no en C' y viceversa. Los puntos de C que no son puntos de acumulación se llaman *puntos aislados* de C. Es fácil ver que un punto de C es aislado si, en un radio suficientemente pequeño, no tiene a su alrededor ningún otro punto de C (de ahí el nombre de "aislado").

En general, C' puede ser un conjunto mucho mayor que C. Por ejemplo, si C es el conjunto de los números racionales, entonces C' es todo el conjunto de los números reales. Pero si C es un conjunto cerrado, su derivado C' resulta de quitarle a C sus puntos aislados, luego en particular está contenido en C. Ahora bien, esto no significa que C' ya no pueda tener puntos aislados. Puede ocurrir que un punto de C sea de acumulación porque es límite de una sucesión de puntos aislados de C, pero que, al eliminar esos puntos aislados, él mismo quede aislado.

Por ejemplo, podemos considerar el conjunto C formado por los números racionales siguientes:

1. 0,
2. $1/n$, para todo número natural $n \geq 1$,
3. $1/m + 1/n$, para todo par de números naturales $m, n \geq 1$.

[2]En el marco teórico actual la construcción de Cantor consiste en dividir el conjunto de todas las sucesiones de Cauchy de números racionales en clases de equivalencia, de modo que dos sucesiones están en la misma clase si y sólo si su diferencia tiende a 0 y establecer que cada clase *es,* por definición, un número real. Cantor, por el contrario, consideraba que "el pensamiento" asocia a cada clase un número real. En la práctica es lo mismo.

Es fácil ver que 0 es el límite de una sucesión de puntos de tipo 1, mientras que cada punto de tipo 1 es el límite de una sucesión de puntos de tipo 2, por lo que todos estos puntos son de acumulación. En cambio, los puntos de tipo 3 son aislados. Por lo tanto, el derivado C' está formado por los puntos de tipo 1 y 2, y sucede que en C' los puntos de tipo 2 son aislados, por lo que C'' consta únicamente del punto 0.

Cantor llamó $C^{(n)}$ al derivado n-simo del conjunto C, de modo que

$$C^{(0)} = C, \qquad C^{(1)} = C', \qquad C^{(2)} = C'', \qquad C^{(3)} = C''', \qquad \dots$$

Si C es cerrado, así tenemos una sucesión decreciente de conjuntos. En estos términos, lo que Cantor demostró en su artículo es que todo subconjunto cerrado C del intervalo $[-\pi, \pi]$ tal que existe un número natural n para el que el derivado n-simo C^n es vacío es un conjunto de unicidad.

El ejemplo que hemos puesto más arriba muestra que hay conjuntos infinitos de esta forma, por lo que la unicidad de un desarrollo en serie trigonométrica puede darse aunque ésta no converja en un conjunto infinito de puntos.

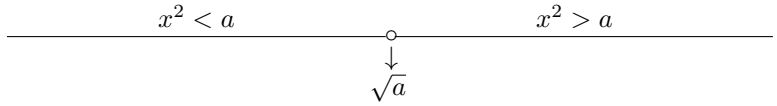
4 Los números reales según Dedekind Hacía diez años que Dedekind ocupaba una plaza en la Universidad Técnica de Brunswick, su localidad natal. Ese año de **1872** conoció a Cantor en unas vacaciones en Suiza y entabló amistad con él (Dedekind tenía entonces 41 años y Cantor 27). Cantor le envió su último artículo y Dedekind lo citó en otro suyo titulado *Continuidad y los números irracionales,* publicado ese mismo año, en el que presentaba una construcción de los números reales a partir de los números racionales distinta de la de Cantor, pero equivalente. Concretamente, Dedekind señala esta característica de los puntos de una recta:

> *Si todos los puntos de la línea recta caen en dos clases tales que cada punto de la primera clase se encuentra a la izquierda de cada punto de la segunda clase, existe un único punto que produce esta división de todos los puntos en dos clases, esta separación de la recta en dos porciones.*

Dedekind llama *secciones* a los pares (A_1, A_2) de clases de puntos de la recta en las condiciones indicadas y razona que los números racionales no cumplen esta propiedad, es decir, que existen secciones en el conjunto de los números racionales que no están "producidas" por ningún número racional. Por ejemplo, muestra que si a es un número natural que no es un cuadrado, no hay ningún número racional que "produzca la separación" entre la clase de los números racionales cumplen $x^2 < a$ y los que cumplen $a < x^2$. Entonces concluye:

> *Entonces, siempre que tengamos que tratar con una sección* (A_1, A_2) [de números racionales] *no producida por ningún número racional, creamos un nuevo número irracional* a*, que consideramos completamente definido por esta sección* (A_1, A_2)*.*

Así, para cada sección del tipo descrito anteriormente, "creamos"[3] el número irracional $\sqrt{a}$



Cuando a los números racionales les añadimos los números irracionales creados de este modo, obtenemos los números reales, que sí que cumplen el principio establecido para los puntos de una recta y eso permite identificar los números reales con los puntos de una recta. Entre los teoremas más importantes sobre los números reales figura el siguiente:

> *Si una magnitud* x *crece continuamente, pero no más allá de cualquier límite, se aproxima a un valor límite.*

En términos modernos, esto expresa el principio de existencia de supremo. Cambiando la "magnitud x" por el conjunto X de los valores que toma (y sin que importe si varía o no de forma continua), lo que dice Dedekind es que si X es un conjunto no vacío de números reales "que no crece más allá de cualquier límite", es decir, que tiene una cota superior c (un valor tal que todos los elementos de X cumplen $x \leq c$), entonces existe una cota superior s que es el "límite" de X, en el sentido de que todos los elementos de X cumplen $x \leq s$, pero además podemos tomar valores de x en X tan cercanos a s como queramos. Es fácil ver que esto equivale a que s es la menor cota superior de X. Así pues:

[3] Como en el caso de la construcción de Cantor, la concepción moderna es considerar que las secciones (A_1, A_2) del conjunto de los números racionales son, por definición, los números reales, e incluso se puede simplificar la construcción definiendo los números reales como las secciones iniciales (los conjuntos A_1), pues cada A_1 determina el correspondiente A_2. Así le ahorramos a "el pensamiento" tener que crear nada, pero a efectos prácticos es lo mismo.

Principio de existencia de supremo e ínfimo Si un subconjunto no vacío de la recta real tiene una cota superior, entonces tiene supremo (una mínima cota superior), y si tiene una cota inferior, tiene ínfimo (una máxima cota inferior).

5 Conjuntos numerables y no numerables Cantor siguió meditando sobre qué diferencia esencial había entre un conjunto infinito del tipo al que se aplicaba el teorema y un conjunto arbitrario de números reales. Eso lo llevó a plantearse un problema extraño para su época:

Dado un conjunto infinito, ¿es siempre posible emparejar sus elementos con los números naturales, sin repeticiones, y sin que sobre ninguno?

Ningún matemático se había planteado antes algo así. Si queremos buscar un antecedente, tenemos que remontarnos a 1638, el año en que Galileo publicó su ensayo *Dos nuevas ciencias.* En él observaba que, entre conjuntos infinitos, no tiene sentido decir si uno es mayor o menor que otro, y ponía un ejemplo que hoy se conoce como *paradoja de Galileo:*

Consideremos el conjunto de los números naturales:

$$0,\quad 1,\quad 2,\quad 3,\quad 4,\quad 5,\quad 6,\quad 7,\quad 8,\quad 9,\quad 10,\quad \ldots$$

y, por otro lado, consideremos el conjunto de los cuadrados perfectos:

$$0,\quad 1,\quad 4,\quad 9,\quad 16,\quad 25,\quad 36,\quad 49,\quad 64,\quad 81,\quad 100,\quad \ldots$$

Si nos preguntamos cuál es mayor, cuál tiene más elementos, podemos dar dos respuestas contradictorias. Uno podría decir que claramente hay más números naturales que cuadrados perfectos, porque los números naturales incluyen a los infinitos números que son cuadrados perfectos, y también a los infinitos números que no lo son. Hasta se podría decir que hay el doble de números naturales que de cuadrados perfectos. En general, *el todo es mayor que una parte* (y ésta es precisamente una de las "nociones comunes" que Euclides tomó como presupuestos en sus *Elementos*). Pero, por otro lado, también estaría justificado afirmar que ambos conjuntos tienen el mismo tamaño, el mismo número de elementos, porque podemos emparejar cada número natural con su cuadrado (o cada cuadrado con su raíz cuadrada), así:

$$\begin{array}{cccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 0 & 1 & 4 & 9 & 16 & 25 & 36 & 49 & 64 & 81 & 100 & \cdots \end{array}$$

Por cada número natural hay un cuadrado y viceversa, luego hay la misma cantidad de números que de cuadrados. Galileo concluyó de aquí que no tenía sentido comparar conjuntos infinitos por su tamaño.

En realidad, había alguien más que se había planteado estas cosas más recientemente. Se trataba de un cura checo llamado Bernard Bolzano, fallecido en 1848. No había publicado prácticamente nada en vida, pero dejó una serie de manuscritos que fueron publicados póstumamente. En 1854 se había publicado su trabajo *Paradojas del infinito,* en el que precisamente afirmaba que los conjuntos infinitos podían caracterizarse por el hecho de que se pueden poner en correspondencia biunívoca con subconjuntos propios. Bolzano fue el primero en emplear la palabra "conjunto" (*Menge*) con el sentido que tiene usualmente en matemáticas.

Pero, volviendo a Cantor, estas "paradojas" no desproveían de sentido a la pregunta que se había planteado. Por ejemplo, una ligera variante del razonamiento de Galileo permitía emparejar los números naturales con los números enteros:

$$\ldots\quad -3,\quad -2,\quad -1,\quad 0,\quad 1,\quad 2,\quad 3,\quad \ldots$$

Basta emparejar los naturales impares con los enteros positivos y los pares con los negativos y el cero, así:

$$\begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 0 & 1 & -1 & 2 & -2 & 3 & -3 & \cdots \end{array}$$

Consideremos ahora el conjunto de los números racionales. Si los pensamos como puntos de una recta, "están por todas partes", entre dos cualesquiera de ellos siempre hay un tercero, por lo que cuesta imaginar como se podrían enumerar todos uno detrás de otro sin olvidarnos de ninguno. Sin embargo, Cantor demostró que era

posible. Para ello conviene observar antes que es posible emparejar los números naturales con todos los pares ordenados de números naturales, es decir, pares como $(3,5)$, $(5,3)$, $(1,1)$, $(0,7)$, etc., donde se entiende que $(3,5)$ y $(5,3)$ son dos pares distintos. El esquema siguiente nos da una forma de emparejarlos:

$\vdots$						
4	10					
3	6	11				
2	3	7	12			
1	1	4	8	13		
0	0	2	5	9	14	
	0	1	2	3	4	$\cdots$

Sólo tenemos que emparejar cada número con el par formado por el número que tiene debajo y el que tiene a la izquierda, así:

$$\begin{array}{cccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ (0,0) & (0,1) & (1,0) & (0,2) & (1,1) & (2,0) & (0,3) & (1,2) & (2,1) & \cdots \end{array}$$

El resultado es una enumeración de todos los pares ordenados que empieza con el par cuyas componentes suman 0, seguido de los dos pares cuyas componentes suman 1, seguido de los tres pares cuyas componentes suman 2, etc. Si prolongamos un poco más la enumeración, obtenemos:

$$(0,0),\ (\mathbf{0},\mathbf{1}),\ (1,0),\ (0,2),\ (\mathbf{1},\mathbf{1}),\ (2,0),\ (0,3),\ (\mathbf{1},\mathbf{2}),\ (\mathbf{2},\mathbf{1}),\ (3,0),\ (0,4),\ (\mathbf{1},\mathbf{3}),\ (2,2),\quad \ldots$$

Ahora, para enumerar los números racionales sólo tenemos que cambiar cada par (m,n) por el número racional m/n, descartando los pares con $n=0$ o los que den lugar a una fracción equivalente a otra ya incluida en la enumeración, y repetir cada fracción añadiéndole un signo negativo. En la lista precedente, nos quedamos sólo con los pares en negrita. Los pares $(0,2),(0,3),(0,4)$ se descartan porque dan lugar al mismo número $0/1$ y $(2,2)$ se descarta porque $2/2=1/2$. Con esto nos queda la enumeración que empieza así:

$$\begin{array}{cccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 0 & 1 & -1 & 1/2 & -1/2 & 2 & -2 & 3 & -3 & 1/3 & -1/3 & \cdots \end{array}$$

Es evidente que cualquier número racional terminará apareciendo en la lista formada con este criterio.

Más difícil parecía emparejar los números naturales con todos los números reales. En **1873** Cantor escribió a Dedekind:

> *Permítame plantearle una pregunta que me interesa teóricamente, pero que no puedo responder; quizás usted pueda, y sería tan amable de escribirme al respecto. Es la siguiente:*
>
> *Se toma el agregado de números enteros positivos n y se denota por (n); además se considera el agregado de todos los números reales positivos x y se denota por (x); entonces la pregunta es simplemente si (n) y (x) pueden ponerse en correspondencia de tal manera que cada individuo de un agregado pertenezca a sólo uno del otro y viceversa.*
>
> *A primera vista, uno se dice a sí mismo, no, no es posible, porque (n) consta de partes discretas, pero (x) forma un continuo; pero nada se gana con esta objeción, y por mucho que me incline a pensar que (n) y (x) no permiten una correlación clara, todavía no puedo encontrar la razón, y eso es lo que me preocupa; quizás sea muy simple.*
>
> *¿No estaría uno inclinado, a primera vista, a afirmar que (n) no puede asignarse unívocamente al agregado (p/q) de todos los números racionales positivos p/q? Y, sin embargo, no es difícil demostrar que (n) puede asignarse unívocamente no sólo a este agregado, sino también al más general* [formado por las sucesiones finitas de números naturales].

Dedekind le respondió que no sabría responder a su pregunta, pero Cantor encontró una respuesta negativa ese mismo año. No vamos a detallar aquí el argumento porque era más complicado que otro que encontraría posteriormente y, además, luego veremos otro mucho más general.

Más adelante, Cantor llamaría *conjuntos numerables* a los conjuntos que, o bien eran finitos, o bien se podían emparejar (sin repeticiones) con los números naturales (es decir, los conjuntos que se podían contar usando los primeros números naturales, si eran finitos, o bien todos ellos, si eran infinitos). En estos términos, había demostrado que el conjunto de los números naturales, el conjunto de los números enteros y el conjunto de los números racionales son numerables, mientras que el conjunto de los números reales no era numerable. Todo esto podrían parecer meras curiosidades matemáticas, pero Cantor les encontró una primera aplicación:

Como es bien sabido, los números reales se dividen en algebraicos y trascendentes. Un número real es *algebraico* si es la raíz de un polinomio con coeficientes enteros (o racionales, que es equivalente), mientras que en caso contrario es *trascendente.* Probar que un número es trascendente no es fácil. No fue hasta 1844 cuando Joseph Liouville demostró por primera vez que un cierto número real es trascendente, y se trataba de un número que había definido él mismo a propósito para que satisficiera un criterio de trascendencia que había demostrado. Y no fue hasta ese mismo año, en **1873**, cuando Hermite había logrado probar que un número no diseñado a propósito para la ocasión, concretamente el número e, es trascendente.

El mismo argumento que prueba que al unir los enteros positivos (que son un conjunto numerable) con los enteros negativos (que son otro conjunto numerable) obtenemos un conjunto numerable, muestra que lo mismo pasa siempre que unimos dos conjuntos numerables. Cantor observó que el conjunto de los números reales es la unión del conjunto de los números algebraicos y el conjunto de los números trascendentes, y pudo probar que el primero es numerable. Si el segundo también lo fuera, se podría concluir que todo el conjunto de los números reales es numerable, cuando ya había demostrado que esto es falso. Por lo tanto, el conjunto de los números trascendentes es infinito no numerable.

De este modo, mediante un argumento mucho más simple que los de Liouville o Hermite, Cantor había demostrado la existencia, no de uno o dos, sino de una cantidad infinita no numerable de números trascendentes. Eso sí, su demostración no proporcionaba ningún ejemplo concreto. Era un ejemplo típico de prueba no constructiva. Estos resultados los publicó en un artículo de **1874** titulado *Sobre una propiedad del conjunto de todos los números reales algebraicos.*

Cantor siguió desarrollando sus ideas. Había demostrado que cualquier intento de emparejar cada número natural con un número real nunca "agotará" a los números reales, sino que siempre quedarán números reales sin emparejar. Esto lo interpretó como que el conjunto de los números reales era *más potente* que el conjunto de los números naturales. Cada conjunto tenía una *potencia,* y, en contra de lo que podría parecer, no todos los conjuntos infinitos eran igual de potentes. Y entonces, con las definiciones siguientes, Cantor dio un paso adelante en el punto en que Galileo se había detenido:

> Dos conjuntos X e Y *tienen la misma potencia (son equipotentes)* cuando es posible establecer una correspondencia biunívoca entre los elementos de X y los de Y, es decir, si es posible emparejar cada elemento de X con un elemento de Y sin repeticiones y sin que sobren elementos de Y.

Así, el conjunto de los números naturales tiene la misma potencia que el conjunto de los cuadrados perfectos y, en contra de lo que Galileo había concluido, esto no lleva a ninguna contradicción, pues Cantor no aceptó la otra mitad de su paradoja: no hay razón para afirmar que el conjunto de los cuadrados perfectos tiene que tener menos potencia que el conjunto de los números naturales por el mero hecho de que el segundo incluya al primero junto con infinitos números más. Simplemente, al tratar con conjuntos infinitos, ya no es válido el principio de que el todo es mayor que la parte. En su lugar, Cantor adoptó esta definición:

> Un conjunto X *tiene potencia menor o igual que otro* Y (X es *minuspotente* a Y) cuando es posible emparejar cada elemento de X con un elemento de Y sin repeticiones (pero si sobran elementos en Y no podemos deducir de ello que X tenga una potencia estrictamente menor que la de Y).

Para que podamos decir que un conjunto infinito tiene estrictamente menos elementos que otro, lo que tiene que suceder es lo siguiente:

> Un conjunto X *tiene una potencia estrictamente menor que otro* Y (y diremos que X es *estrictamente minuspotente* a Y) cuando X es minuspotente, pero no equipotente, a Y.

Así, para probar que un conjunto infinito X es estrictamente menos potente que otro Y, no basta emparejar los elementos de X con los de Y sin repeticiones de modo que en Y queden elementos sin emparejar, sino que hay que demostrar que es imposible encontrar otra forma de emparejarlos de modo que no sobren elementos en Y, tal como Cantor había probado para el caso de los números naturales y los reales.

Entendiendo las cosas así, la paradoja de Galileo no es ninguna contradicción. Simplemente es la constatación de que un conjunto infinito puede tener el mismo número de elementos que una de sus partes, cosa que no les sucede a los conjuntos finitos.

Ese año Cantor se casó con una amiga de su hermana y se fue de luna de miel a Suiza, pero dedicó bastante tiempo a discutir sobre matemáticas con Dedekind. En una carta le habló de un nuevo problema sobre el que estaba meditando:

> *¿Puede una superficie (por ejemplo, un cuadrado que incluye su borde) ponerse en correspondencia con una línea (por ejemplo, un segmento de recta que incluya sus extremos) de modo que para cada punto de la superficie exista un punto correspondiente de la línea y, a la inversa, que para cada punto de la línea exista un punto correspondiente de la superficie? Creo que responder a esta pregunta no sería tarea fácil, a pesar de que la respuesta parece tan claramente negativa que la demostración parece casi innecesaria.*

Pasarían más de tres años antes de que encontrara la respuesta. En **1877** escribió a Dedekind para comunicarle una demostración que había encontrado de que existe una correspondencia biunívoca entre el intervalo $[0,1]$ y el conjunto de todos los puntos de un espacio de dimensión n. En la carta exclamaba: *¡Lo veo y no lo creo!* Dedekind le mostró un error que no tardó en corregir. El resultado fue publicado en *Una contribución a la teoría de las multiplicidades,* donde presentó también el concepto de "potencia" de un conjunto y planteó otro problema más complejo:

Desde que demostró que la potencia del conjunto de los números reales era estrictamente mayor que la del conjunto de los números naturales, Cantor había estado tratando de encontrar un subconjunto de la recta real que tuviera una potencia estrictamente menor, pero a la vez estrictamente mayor que la del conjunto de los números naturales. No encontró ninguno, lo que lo llevó a conjeturar que no existía ninguna potencia intermedia, es decir, que todo conjunto infinito que tenga estrictamente menos potencia que el conjunto de los números reales tiene que ser numerable. Como Cantor llamaba "el continuo" a la recta real, llamó a esta conjetura la *hipótesis del continuo.*

El resultado de Cantor tenía implicaciones sobre el concepto de "dimensión". Cuando se dice que un plano tiene dos dimensiones y que el espacio ordinario tiene tres, esto se entiende como que hacen falta dos números reales para identificar un punto del plano, mientras que hacen falta tres para identificar un punto del espacio. Sin embargo, Cantor había demostrado que bastaba un único número real para identificar un punto del plano, o del espacio.

Otro que vio este resultado y no lo creyó fue Kronecker, que era uno de los matemáticos más influyentes de la época, a la vez que uno de los que tenían una visión más estrecha de las matemáticas, una visión hiperconstructivista que le hacía rechazar como sin sentido resultados como el teorema de Bolzano-Weierstrass, o la trascendencia del número e que había probado Hermite. Los resultados de Cantor estaban en las antípodas de lo que él consideraba "matemáticas de verdad", y Kronecker había tratado de evitar la publicación de su artículo en la *Revista de matemáticas puras y aplicadas.* Aunque logró retrasarla, finalmente se publicó gracias a la intervención de Dedekind y Weierstrass. Cantor se sintió indignado y ofendido por la actitud de Kronecker y no volvió a publicar en esa revista.

6 Los números ordinales En **1879** empezó a publicar una serie de artículos en la revista *Mathematische Annalen* (editada por Felix Klein y Adolph Mayer), con el título común de *Sobre las variedades de puntos lineales infinitas.* En **1880** Kronecker fue nombrado editor de la *Revista de matemáticas puras y aplicadas,* lo que acabó de confirmar la ruptura de Cantor con dicha revista.

El segundo artículo en *Mathematische Annalen,* publicado en **1880**, fue una nota breve en la que retomó los conjuntos derivados que había definido para su estudio de la unicidad de los desarrollos en serie trigonométrica. Ahora le interesaban de nuevo porque había observado que si C es cualquier subconjunto de la recta real, el conjunto de sus puntos aislados es necesariamente numerable. Por lo tanto, si, a partir de un cerrado C, vamos construyendo la sucesión de derivados:

$$C = C^{(0)}, \quad C^{(1)}, \quad C^{(2)}, \quad C^{(3)}, \quad \dots$$

cada conjunto resulta de quitarle al anterior un conjunto numerable de puntos. La sucesión puede estabilizarse, es decir, puede llegar un momento en que $C^{(n)} = C^{(n+1)}$. En general, Cantor definió un conjunto perfecto como

un conjunto C que es igual a su propio derivado: $C = C'$. Esto implica en particular que es cerrado. Cantor conjeturaba que un conjunto perfecto (salvo que sea vacío) tiene que tener la potencia del continuo, luego si se lleg a un n tal que $C^{(n)}$ es perfecto, tendremos descompuesto C como unión de un conjunto numerable (la unión del número finito de conjuntos numerables de puntos aislados que hemos ido quitando hasta llegar a $C^{(n)}$) y un conjunto perfecto. Por lo tanto C será numerable o tendrá la potencia del continuo según si el conjunto perfecto $C^{(n)}$ es o no vacío.

Cantor vio que puede suceder que la sucesión de derivados no se estabilice, pero se dio cuenta de que, en tal caso, podía definir $C^{(\infty)}$ como la intersección de todos los conjuntos $C^{(n)}$, que es un conjunto cerrado contenido en todos ellos:

$$C = C^{(0)}, \quad C^{(1)}, \quad C^{(2)}, \quad C^{(3)}, \quad \dots \quad C^{(\infty)}.$$

Si este "derivado infinito" $C^{(\infty)}$ no es perfecto, podemos continuar la sucesión de derivados:

$$C = C^{(0)}, \quad C^{(1)}, \quad C^{(2)}, \quad C^{(3)}, \quad \dots \quad C^{(\infty)}, \quad C^{(\infty+1)}, \quad C^{(\infty+2)}, \quad C^{(\infty+3)}, \quad \dots$$

pero si no se llega aún a un conjunto perfecto, nada impide tomar la intersección $C^{(\infty+\infty)} = C^{(2\infty)}$ de todos los conjuntos obtenidos hasta el momento y así tenemos un nuevo cerrado en la sucesión:

$$C = C^{(0)}, \quad C^{(1)}, \quad C^{(2)}, \quad C^{(3)}, \quad \dots \quad C^{(\infty)}, \quad C^{(\infty+1)}, \quad C^{(\infty+2)}, \quad C^{(\infty+3)}, \quad \dots \quad C^{(2\infty)},$$

con el que a su vez se podía iniciar otra serie de derivados, que, de no estabilizarse, permitía calcular el conjunto $C^{(3\infty)}$, e incluso, si la serie de derivados no se estabiliza al pasar por $C^{(\infty)}, C^{(2\infty)}, C^{(3\infty)}, C^{(4\infty)}, \dots$, por debajo de todos ellos podemos formar la intersección $C^{(\infty\infty)} = C^{\infty^2}$, y este proceso podía no terminar nunca, en un sentido muy radical de "nunca".

Cantor dedicó varios años a asimilar y desarrollar estas ideas, hasta que en **1883** publicó su quinto artículo en *Matematische Annalen,* que además fue publicado de forma independiente con el título de *Fundamentos de una teoría general de agregados,* que fue especialmente relevante por varias razones que expondremos a continuación.

Por una parte, Cantor consideró nuevamente la sucesión de conjuntos derivados, pero ahora escribía ω donde antes había escrito ∞:

$$C = C^{(0)}, \quad C^{(1)}, \quad C^{(2)}, \quad \dots \quad C^{(\omega)}, \quad C^{(\omega+1)}, \quad \cdots \quad C^{(2\omega)}, \quad \dots \quad C^{(3\omega)}, \quad \dots \quad C^{(\omega^2)}, \quad C^{(\omega^2+1)}, \quad \dots$$

Anteriormente, Cantor se había referido a las expresiones como $3\infty^4 + 2\infty^2 + 7$ como "índices transfinitos", pero ahora a las expresiones como $3\omega^4+2\omega^2+7$ las llamaba *números transfinitos,* o también *ordinales transfinitos,* y esto no era un mero cambio de notación y de lenguaje, sino que había varias ideas de fondo que trataremos de explicar:

Para empezar, Cantor pasó a considerar a sus "indices" como números porque vio que podía estudiarlos independiente de la sucesión de conjuntos derivados, no como meras etiquetas para distinguir un conjunto derivado de otro. En efecto, Cantor presentaba ahora los números ordinales como los números que podemos obtener a partir del 0 por la aplicación sucesiva de dos *principios generadores:*

Primer principio generador *Todo ordinal α tiene un sucesor inmediato $\alpha + 1$.*

Segundo principio generador *Por encima de toda sucesión creciente de ordinales hay un mínimo ordinal posterior a todos ellos.*

En palabras de Cantor:

> *A esto lo llamo el segundo principio de generación de números enteros reales y los defino con mayor precisión: si existe una sucesión definida de números enteros reales definidos, para la cual no hay un mayor, entonces se crea un nuevo número mediante este segundo principio de generación, que se considera el límite de esos números, es decir, se define como el siguiente número mayor que todos ellos.*

Así, partiendo del 0 y aplicándole sucesivamente el primer principio generador, obtenemos la *primera clase numérica* (I), formada por los números naturales:

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad \dots$$

Si ahora aplicamos el segundo principio, hay un mínimo ordinal mayor que todos los números naturales, al que Cantor llamó ω. A partir de aquí, el primer principio generador nos prolonga la sucesión de los ordinales hasta

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad \ldots \quad \omega, \quad \omega+1, \quad \omega+2, \quad \omega+3, \quad \ldots$$

Pero de nuevo podemos aplicar el segundo principio generador para añadir a esta sucesión doblemente infinita el ordinal $\omega+\omega=2\omega$. Luego, el primer principio generador nos da:

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad \ldots \quad \omega, \quad \omega+1, \quad \omega+2, \quad \omega+3, \quad \ldots \quad 2\omega, \quad 2\omega+1, \quad 2\omega+2 \quad \ldots$$

Análogamente podemos ir generando los ordinales $2\omega, \quad 3\omega, \quad 4\omega, \quad \ldots$, pero el segundo principio generador también se aplica a esta sucesión, para obtener, por encima de todos estos ordinales, el ordinal $\omega\cdot\omega=\omega^2$, que está por encima de todos los ordinales de la forma $m\omega+n$.

Por encima de todos los ordinales $\omega^2, \quad \omega^2+1, \quad \omega^2+2, \quad \ldots$ se encuentra $\omega^2+\omega$ y, tras una nueva sucesión infinita de sucesores $\omega^2+\omega+1, \omega^2+\omega+2$, etc., llegamos a $\omega^2+\omega+\omega=\omega^2+2\omega$, e igualmente podemos obtener $\omega^2+3\omega, \quad \omega^2+4\omega, \omega^2+5\omega, \quad \ldots$, tras los cuales viene $\omega^2+\omega\cdot\omega=\omega^2+\omega^2=2\omega^2$. Similarmente, al aplicar el segundo principio generador a la sucesión $\omega^2, \quad 2\omega^2, \quad 3\omega^2, \quad \ldots$ obtenemos $\omega^2\cdot\omega=\omega^3$. E igualmente, la sucesión $\omega, \quad \omega^2, \quad \omega^3, \quad \ldots$ se prolonga con ω^ω, y así podríamos continuar sin fin.

Cantor expresó esta idea de "continuar sin fin" llamando *números transfinitos* a los ordinales, porque, en virtud del segundo principio generador, los ordinales van más allá de cualquier prolongación infinita.

Pero la razón más importante por la que Cantor pasó a considerar números a los ordinales era que, como los números, pueden usarse para medir algo, concretamente, las formas de enumerar un conjunto.

La sucesión de conjuntos derivados era un ejemplo de cómo los ordinales podían hacer falta para enumerar unos objetos que nos podemos encontrar en un orden dado que no podemos elegir (no podemos calcular $C^{(\omega+3)}$ antes de haber calculado antes todos los derivados precedentes), y por ello no eran meros "signos sin sentido".

Más precisamente, Cantor distinguía entre *Zahl* (número) y *Anzahl* (enumeración). Para conjuntos finitos no hay diferencia. Por ejemplo, si queremos contar un conjunto como $\{a,b,c\}$, sólo tenemos una forma posible de enumerar sus elementos: tomamos uno, luego otro y luego el otro. Y esa enumeración se "mide" con el ordinal 3. Se podría objetar que podemos enumerarlos como a,b,c o como b,a,c, etc., pero para Cantor eso era una misma enumeración. Al enumerar hacemos abstracción de qué elemento ponemos en cada lugar. Si visualizamos esto sustituyendo el nombre individual de cada objeto con una figura común, como $\circ$, vemos que las dos enumeraciones anteriores se reducen a $\circ, \ \circ, \ \circ$, y éste es el tipo de orden que "mide" el ordinal 3.

La situación es diferente para conjuntos infinitos. Si queremos enumerar los números enteros, podemos hacerlo así:

$$0, \quad 1, \quad -1, \quad 2, \quad -2, \quad 3, \quad -3, \quad \ldots$$

y en tal caso Cantor diría que esto es una enumeración de ordinal ω.

El ordinal ω corresponde a las enumeraciones idénticas a la enumeración natural del conjunto de los números naturales: un objeto, luego otro, luego otro, etc. Pero otra enumeración posible de los números enteros es

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots \quad -1, \quad -2, \quad -3, \quad \ldots$$

la cual tiene ordinal $\omega+\omega=2\omega$, el ordinal de las enumeraciones doblemente infinitas. Pero también podemos considerar ésta otra:

$$1, \quad 2, \quad 3, \quad \ldots \quad -1, \quad -2, \quad -3, \quad \ldots \quad 0.$$

primero enumeramos los números positivos "cuando acabamos" enumeramos los negativos y "cuando acabamos" añadimos el 0, que nos faltaba. Esta enumeración tiene ordinal $2\omega+1$ (el ordinal de una enumeración doblemente infinita seguida de un último elemento). Notemos que si en las tres enumeraciones anteriores sustiuimos cada número por $\circ$, seguiremos distinguiendo una de otra y reconociendo a qué ordinal corresponde cada una. Por ejemplo, si vemos una enumeración de este tipo:

$$\circ \quad \circ \quad \circ \quad \cdots \quad \circ \quad \circ \quad \circ \quad \cdots \quad \circ \quad \circ \quad \circ \quad \cdots \quad \circ \quad \circ.$$

podemos asegurar que corresponde al ordinal $3\omega+2$, sin que importe qué objeto va en el lugar de cada $\circ$. De este modo, el conjunto de los números enteros tiene potencia numerable, pero admite infinitas enumeraciones distintas.

En realidad, en este punto hay que precisar qué entendemos por una "enumeración", porque, por ejemplo, el orden usual de los números enteros:

$$\cdots \quad \circ \quad \circ \quad \circ \quad \circ \quad \circ \quad \circ \quad \circ \quad \cdots$$

no es una enumeración. Enumerar un conjunto significa disponer sus elementos en lo que Cantor llamó un *buen orden:*

Definición Un conjunto está bien ordenado si sus elementos están dispuestos uno tras otro con la propiedad de que cualquier subconjunto no vacío tiene un mínimo elemento.

Por ejemplo, en la enumeración de los números enteros que hemos dado antes de ordinal $2\omega + 1$, el mínimo del conjunto de los números negativos es -1. En cambio, la ordenación usual de los números enteros no es un buen orden, pues con ella no hay un mínimo número negativo.

En estos términos, Cantor explicaba que los ordinales "miden" las distintas formas de *ordenar bien* un conjunto.

Cantor llamó *segunda clase numérica* (II) a la clase de todos los ordinales correspondientes a formas de ordenar bien un conjunto infinito numerable (fue precisamente en este trabajo en el que Cantor acuñó el término "numerable"), y llamó ω_1 al menor ordinal mayor que todos los de dicha clase, es decir, el menor ordinal que tiene por debajo una cantidad no numerable de ordinales. El el resultado principal de su artículo era que, así como la primera clase de números determina un conjunto numerable, la segunda clase de números determina un conjunto no numerable y, más aún, su potencia es la menor posible de entre las potencias no numerables.

A su vez, ω_1 era el primer ordinal de la *tercera clase numérica* (III), la clase de todos los ordinales correspondientes a formas de ordenar un conjunto de la potencia de (II), y se cumple que la potencia de esta clase es la menor potencia mayor que la potencia de (II), y así sucesivamente, con lo que Cantor había demostrado que existen infinitas potencias infinitas (mientras que hasta entonces sólo conocía dos, la de los conjuntos numerables y la del continuo). Así pues, las primeras potencias eran

$$0, \quad 1, \quad 2, \quad \ldots \quad \text{(I)}, \quad \text{(II)}, \quad \text{(III)}, \quad \ldots$$

En este trabajo en el que Cantor enunció por primera vez —y usó libremente— lo que llamó *principio de buena ordenación,* según el cual *todo conjunto puede ser bien ordenado,* pero no trató de demostrarlo, sino que lo tomó como un "principio fundamental del pensamiento", es decir, que Cantor consideraba que nada nos impide pensar en los elementos de un conjunto dispuestos en un buen orden.

Volviendo a la sucesión de conjuntos derivados, Cantor enunció en su artículo —sin demostración— que, dado un conjunto C, existe un ordinal α, de primera o segunda clase, tal que el derivado $C^{(\alpha)}$ es perfecto, y eso permite concluir lo que hoy se conoce como:

Teorema de Cantor-Bendixson[4] Todo subconjunto cerrado C de la recta real se descompone de forma única como unión de un conjunto perfecto y un conjunto numerable.

Demostración: Si C es cerrado y α es un ordinal de primera o segunda clase tal que $C^{(\alpha)}$ es perfecto, entonces C es la unión del conjunto perfecto $P = C^{(\alpha)}$ y de la unión N de todos los conjuntos numerables de puntos aislados que hemos ido quitándole a C hasta llegar a $C^{(\alpha)}$. Cantor había demostrado que una unión numerable de conjuntos numerables es numerable, luego N es numerable. ∎

Cantor afirmó —sin demostrarlo— que todo conjunto perfecto no vacío tiene la potencia del continuo. (La demostración la publicaría en 1884). Como consecuencia, todo conjunto cerrado es numerable o tiene la potencia del continuo, según si el conjunto perfecto que proporciona el teorema de Cantor-Bendixson es o no vacío.

Esto suponía un avance considerable hacia la demostración de la hipótesis del continuo, pues ahora Cantor podía asegurar que si existe un subconjunto no numerable de la recta real cuya potencia sea estrictamente inferior a la del continuo, éste no puede ser cerrado. Una de las vías por las que Cantor abordó el problema fue tratar de probar que todo subconjunto no numerable de la recta real contiene un subconjunto perfecto.

[4]Ivar Otto Bendixson era un estudiante sueco de 23 años que escribió una carta a Cantor para informarle de un error en su artículo de **1883**, relativo a que había enunciado el teorema de Cantor-Bendixson en un contexto más general, sin suponer que C fuera cerrado, y no había expresado correctamente la conclusión. La parte puramente matemática de dicha carta fue publicada ese mismo año con el título de *Algunos teoremas de la teoría de conjuntos de puntos,* en el cual apareció la primera demostración del teorema.

Esto lo llevó a estudiar con detalle los conjuntos perfectos. Precisamente en este artículo construyó lo que hoy se conoce como el *conjunto de Cantor,*[5] que era muy peculiar. La idea de su construcción es muy simple y la ilustra la figura siguiente:

Partimos del intervalo I_0 formado por todos los números reales $0 \leq x \leq 1$, lo dividimos en tres partes iguales y eliminamos la central (sin sus extremos). Equivalentemente, nos quedamos con el conjunto cerrado I_1 formado por todos los números que (en base 3) empiezan por 0.0 o por 0.2, pero no por 0.1.

Los dos intervalos que nos quedan los dividimos en tres partes iguales y eliminamos la central (sin sus extremos), con lo que obtenemos el conjunto cerrado I_2 formado por los números cuya expresión en base 3 empieza por $0.00, 0.02, 0.20, 0.22$, pero sin que aparezcan unos.

Así repetimos el proceso para construir la sucesión decreciente de cerrados $I_0, I_1, I_2, I_3, I_4, \ldots$ La figura muestra precisamente estos cinco primeros términos de la sucesión. El conjunto de Cantor $\mathcal{C}$ es la intersección de todos ellos o, equivalentemente, el conjunto de todos los números $0 \leq x \leq 1$ en cuya expresión decimal en base 3 no aparece la cifra 1.

Cantor demostró que $\mathcal{C}$ es un conjunto cerrado perfecto, luego tiene la potencia del continuo, luego es "todo lo grande que podría ser", pero, en cierto sentido, es un conjunto muy pequeño. En efecto, a I_0, le hemos quitado un intervalo de longitud $1/3$; a I_1 le hemos quitado otros 2 intervalos de longitud $1/9$ cada uno, luego una longitud total de $2/9$; a I_2 le quitamos 4 intervalos de longitud $1/27$, luego una longitud total de $4/27$, y así sucesivamente, a cada I_n lequitamos una longitud total de $2^n/3^{n+1}$. Por lo tanto, la suma de las longitudes que hemos quitado en total al intervalo inicial I_0 es

$$L = \sum_{n=0}^{\infty} \frac{2^n}{3^{n+1}} = \frac{1}{3} \sum_{n=0}^{\infty} \left(\frac{2}{3}\right)^n = \frac{1}{3} \cdot \frac{1}{1 - 2/3} = 1.$$

Como I_0 tiene longitud 1, hay que concluir que ¡$\mathcal{C}$ tiene longitud 0!

7 La teoría de conjuntos Kronecker seguía usando su influencia para evitar, o al menos, retrasar, las publicaciones de Cantor, que a menudo veían la luz gracias a oportunas intervenciones de Dedekind o de Weierstrass. Cantor estaba molesto, pero en su artículo de **1883** había rebatido educada y respetuosamente las posturas de Kronecker, sin mencionarlo explícitamente:

> [...] *hay un punto de vista ampliamente defendido sobre la esencia y el significado de las cantidades numéricas de acuerdo con el cual los únicos números que son concebidos como efectivamente existentes son los números enteros finitos de nuestra clase numérica* (I).
>
> *A lo sumo una cierta realidad es concedida a los números racionales que se obtienen directamente a partir de ellos. Pero en lo que respecta a los números irracionales, en la matemática pura deben recibir un significado meramente formal, en que, por así decirlo, sólo sirven como marcas de cálculo para fijar propiedades de grupos de enteros y para describir estas propiedades de una manera simple y unificada. De acuerdo con esta opinión, el verdadero objeto del análisis está formado exclusivamente por los enteros finitos, y todas las verdades descubiertas o todavía por descubrir de la aritmética y el análisis deben ser concebidas como relaciones de los números finitos entre sí; el análisis infinitesimal y, con él, la teoría de funciones son considerados legítimos sólo en la medida en que sus teoremas puedan ser interpretados como demostrables mediante las leyes que gobiernan a los números enteros finitos. Esta concepción de la matemática pura, aunque yo no pueda suscribirla, tiene ciertas ventajas incontestables que me gustaría subrayar aquí. Además, algunos de los más ilustres matemáticos de la actualidad están entre sus defensores, y este hecho habla en favor de su relevancia.*

[5] Aunque ya había sido descubierto independientemente por Henry Smith en 1875 y por Vito Volterra en 1881.

Sin embargo —y esto era lo que más irritaba a Cantor— Kronecker nunca habló públicamente en contra de las teorías de Cantor, con lo que no le daba la oportunidad de defenderse. Hablaba despectivamente de Cantor y de su trabajo a sus alumnos y a otros matemáticos, pero nunca de forma directa. Kronecker llegó a decir que Cantor era un charlatán, un renegado y un corruptor de la juventud. A principios de **1883** Cantor se enteró de que Kronecker había escrito a Hermite calificando a los trabajos de Cantor como "estupidez". Ese año Cantor se presentó como aspirante a una plaza en la Universidad de Berlín (donde estaba Kronecker), tal vez sólo por incordiarle, pero Kronecker movió los hilos necesarios para que no se la concedieran. Cantor permanecería en Halle toda su vida.

La hostilidad de Kronecker provocó en Cantor una susceptibilidad que rayaba en la paranoia, y esto, unido a la frustración que le provocaba el fracaso de sus intentos por demostrar o refutar la hipótesis del continuo, le provocó una crisis nerviosa en **1884**, por la que durante un tiempo tuvo que reducir su trabajo a lo que eran estrictamente sus obligaciones docentes. En cuanto se recuperó, se fue de vacaciones y no tardó en escribir eufórico una carta a Gösta Mittag-Leffler (su amigo y editor de *Acta Mathematica,* la revista en la que había publicado sus últimos trabajos) anunciándole que por fin había demostrado la hipótesis del continuo, prometiéndole los detalles en cuanto "hubiera puesto todo en orden", pero el 20 de octubre le escribió para anunciarle que su demostración era incorrecta. El 14 de noviembre una nueva carta anunciaba que había demostrado que la hipótesis del continuo es falsa, pero no tardó más de 24 horas en darse cuenta de que su nueva demostración también estaba mal.

Es posible que estos vaivenes hicieran dudar a Mittag-Leffler de la solvencia de Cantor como matemático, porque en **1885** Cantor le envió un artículo titulado *Principios de una teoría de los tipos de orden,* en el que extendía el concepto de ordinal a conjuntos no necesariamente bien ordenados y daba caracterizaciones del tipo de orden de varios conjuntos, como el de los números racionales o el de los números reales, pero, para su amarga decepción, Mittag-Leffler le recomendó con mucho tacto y adulación no publicarlo (y nunca se publicó). Cantor le diría más adelante a Poincaré que, en su opinión, Mittag-Leffler había temido que su artículo dañara el prestigio de su revista.

Uno de los puntos más interesantes de este artículo no publicado era que en él Cantor afirmaba explícitamente por primera vez que la matemática pura no era sino teoría de conjuntos pura, y que los principios de la teoría de conjuntos eran tan generales y profundos que toda la matemática podía ser entendida en términos esencialmente conjuntistas.

Durante los años siguientes Cantor se ocupó más de defender sus teorías que de desarrollarlas, y se carteaba más con filósofos y teólogos que con matemáticos. No obstante, podemos señalar algunos avances conceptuales. Una vez establecido que había infinitas potencias infinitas, era natural considerarlas como números. En sus *Notas sobre la doctrina del transfinito,* publicadas en **1887** en la *Revista de Filosofía y Teología Especulativa,* empezó a hablar de *cardinales infinitos* en lugar de "potencias". Para representar el cardinal de un conjunto M introdujo la notación $\overline{\overline{M}}$, donde las dos barras indicaban una doble abstracción: si hacemos abstracción únicamente de la naturaleza de los elementos de M, conservando su ordenación, obtenemos el ordinal de M, que Cantor representaba por $\overline{M}$, y si además hacemos abstracción de la forma en que están ordenados los elementos de M, entonces tenemos su cardinal.

En ese mismo artículo Cantor afirmó sin demostración alguna un teorema básico para que tenga sentido considerar a las "potencias" o "cardinales" como determinaciones del "número de elementos" de un conjunto infinito:

> $(*)$ Si un conjunto M es minuspotente a otro N y a su vez N es minuspotente a M, entonces M y N son equipotentes.

En otras palabras, si podemos emparejar (sin repeticiones) cada elemento de M con uno de N (aunque sobren elementos en N) y también podemos emparejar elementos de N con elementos de M (aunque sobren elementos en M), también es posible emparejar los elementos de ambos conjuntos (sin repeticiones) sin que sobren elementos en ninguno de los dos.

8 Los números naturales según Dedekind En **1888** Dedekind publicó *¿Qué son y para qué sirven los números?,* donde construía los números naturales a partir de las propiedades básicas de los conjuntos.

Con una notación bastante diferente a la que hoy es habitual, Dedekind empieza hablando de "cosas", conjuntos de "cosas" (entendiendo que los conjuntos también son cosas que pueden formar parte de otros

conjuntos) y define los conceptos de unión, intersección, funciones que hacen corresponder los elementos de un conjunto en los de otro, etc. Una vez presentados estos conceptos básicos, Dedekind presenta una definición conjuntista de "conjunto infinito". En lenguaje moderno:

> Un conjunto A es *infinito* si existe una aplicación $S : A \longrightarrow A$ inyectiva y no suprayectiva. En caso contrario se dice finito.

En otras palabras, un conjunto es infinito si podemos emparejar (sin repeticiones) los elementos de A con los de un subconjunto propio de A. En efecto, un conjunto finito A no tiene esta propiedad, pues si tiene n elementos, cualquier subconjunto propio (es decir, que no sea el propio A) tendrá a lo sumo $n-1$ elementos, y éstos no podrán emparejarse con los n elementos de A. En cambio, todo conjunto infinito A tiene esta propiedad, pues si a un conjunto infinito le quitamos uno de sus elementos, el conjunto A' resultante tiene el mismo cardinal que A, por lo que es posible emparejar los elementos de A con los de A'.

Dedekind señala que Cantor y otros habían observado que los conjuntos infinitos tienen esta propiedad, pero que él era el primero que la usaba como definición de infinitud para demostrar a partir de ella las propiedades básicas de los conjuntos finitos e infinitos.

A continuación, Dedekind parte de un conjunto infinito cualquiera A y fija en él una aplicación $S : A \longrightarrow A$ inyectiva y no suprayectiva. Esto significa que cada elemento a de A se empareja con un elemento $S(a)$, de modo que no haya repeticiones y exista en A un elemento, al que llamamos[6] 0, que no esté emparejado con nadie. El propósito de Dedekind es definir

$$1 = S(0), \quad 2 = S(1) = S(S(0)), \quad 3 = S(2) = S(S(S(0))), \quad \ldots$$

Pero la parte delicada es definir un subconjunto N de A que no contenga más que estos objetos, es decir, que podamos decir que

$$N = \{0, 1, 2, 3, \ldots\},$$

pero explicitando qué significan esos puntos suspensivos. Para ello Dedekind introduce la definición siguiente:

> Una *cadena* es un subconjunto de A que contiene a 0 y de modo que, si contiene un elemento n, también contiene a $S(n)$.

Y esto le permite definir el conjunto N de los *números naturales* como la intersección de todas las cadenas de A, es decir, como el conjunto cuyos elementos están en todas las cadenas. Así, N contiene necesariamente al conjunto $\{0, 1, 2, \ldots\}$ y, como éste es una cadena, N tiene que estar contenido en él. Más precisamente, Dedekind demuestra los hechos siguientes:

1. 0 es un número natural.
2. Si n es un número natural, también lo es $S(n)$ (y se llama *sucesor* de n).
3. 0 no es el sucesor de ningún número natural.
4. Números naturales distintos tienen sucesores distintos.
5. **(Principio de inducción)** Para probar que todos los números naturales tienen una propiedad, basta probar que la tiene 0 y que, si la tiene n, también la tiene $S(n)$.

Demostración: 1) se cumple por definición de conjunto inductivo (0 está en todos ellos, luego es un número natural por definición de número natural).

2) se cumple porque si n es un número natural, por definición de número natural está en todo conjunto inductivo, luego, por definición de conjunto inductivo, lo mismo le sucede a $S(n)$, luego $S(n)$ es un número natural (por definición de número natural).

3) se cumple por la elección de 0 y 4) es una propiedad general de la aplicación S (que empareja sin repeticiones).

Por último, si llamamos N al conjunto de todos los números naturales que tienen la propiedad considerada en 5), lo que afirma 5) es que se trata de un conjunto inductivo, pero los números naturales están en todos los conjuntos inductivos, luego todos tienen la propiedad en cuestión. ∎

[6] En realidad Dedekind toma al 1 como primer número natural, pero aquí adaptamos la construcción empezando con el 0 para enlazar mejor con lo que discutiremos más adelante.

Aunque pospone un poco el enunciado y la demostración, Dedekind acaba demostrando que no importa qué conjunto infinito A tomemos como punto de partida de la construcción precedente, ni que aplicación S ni qué elemento 0, pues si partimos de dos elecciones distintas, $S : A \longrightarrow A$ y $S' : A' \longrightarrow A'$, con dos elementos 0 y $0'$, los conjuntos $\mathbb{N}$ y $\mathbb{N}'$ obtenidos son "esencialmente" el mismo conjunto, pues existe una correspondencia biunívoca $f : \mathbb{N} \longrightarrow \mathbb{N}'$ tal que $f(0) = 0'$ y $f(S(n)) = S'(f(n))$ para todo número natural n de $\mathbb{N}$.

Esto significa que $S(0) = 0'$, $S(1) = 1'$, $S(2) = 2'$, etc., de modo que si alguien toma como números naturales a los elementos de $\mathbb{N}$ y otro toma como números naturales a los elementos de $\mathbb{N}'$, la diferencia es como si uno llama a los números naturales cero, uno, dos, tres, etc. mientras que otro los llama *zero, one, two, three,* etc. simplemente estamos usando representaciones diferentes de los números naturales, pero con ambas podemos hacer exactamente las mismas cosas.

Seguidamente Dedekind define la relación de orden sobre los números naturales, la suma, el producto y la exponenciación de números naturales y demuestra sus propiedades básicas, es decir, expone con todo detalle la aritmética elemental de los números naturales. Finalmente muestra cómo los números naturales se pueden usar para contar conjuntos finitos.

En realidad Dedekind desarrolló una teoría más general que la que necesitaba para construir los números naturales, a la que llamó *teoría de cadenas,* y que más adelante se aprovecharía en otros contextos. Por ejemplo, el propio Dedekind la usó en 1887 para demostrar el teorema $(*)$ de la página 14, si bien no publicó la demostración ni se la comunicó siquiera a Cantor (hacía unos cinco años que se habían distanciado).

9 Peano y Frege Aunque cada vez más matemáticos se interesaban por la teoría de conjuntos, no todos consideraban razonable deducir la aritmética elemental de los principios conjuntistas como había hecho Dedekind, pues eso suponía a menudo demostrar hechos evidentes a partir de principios abstractos mucho menos evidentes. En esta línea se encontraba Giuseppe Peano, que en **1889** publicó un artículo titulado *Arithmetices Principia Noua Methodo Exposita* (Los principios de la aritmética presentados siguiendo un método nuevo). A pesar de que tenía sólo 31 años, consideró que era una buena idea publicar su trabajo en latín, algo ya anticuado en su época. En el preámbulo explica así la motivación de su trabajo:

> *Las cuestiones relativas a los fundamentos de las matemáticas, aunque tratadas por muchos en la actualidad, aún carecen de una solución satisfactoria. La dificultad surge principalmente de la ambigüedad del lenguaje ordinario. Por esta razón, es de suma importancia considerar atentamente las palabras que utilizamos. Me propuse hacerlo y presento en este trabajo los resultados de mi estudio con aplicaciones a la aritmética.*
>
> *He indicado mediante signos todas las ideas que aparecen en los fundamentos de la aritmética, de modo que cada proposición se enuncia sólo con estos signos. Los signos pertenecen a la lógica o a la aritmética. Los signos lógicos que aparecen aquí son unos diez, aunque no todos son necesarios. El uso de estos signos y varias de sus propiedades se explican en lenguaje ordinario en la primera parte. No quise presentar su teoría más extensamente aquí. Los signos aritméticos se explican a medida que aparecen.*
>
> *Con esta notación, cada proposición adquiere la forma y precisión que disfrutan las ecuaciones en el álgebra, y de las proposiciones así escritas pueden deducirse otras, mediante un proceso que se asemeja a la solución de ecuaciones algebraicas. Ésa es la razón principal para escribir este trabajo.* [...] *Las proposiciones que se deducen de otras por las operaciones de la lógica son teoremas; aquellas para las que esto no es cierto las he llamado axiomas. Aquí hay nueve axiomas, y expresan propiedades fundamentales de los signos no definidos.*

Los nueve axiomas a los que hace referencia Peano, desprovistos de su notación, que es muy distinta a la notación matemática actual, son los siguientes:

1. El 0 es un número natural.[7]
2. Si a es un número natural, entonces $a = a$.
3. Si a, b son números naturales, $a = b$ equivale a $b = a$.

[7] Como Dedekind, en realidad Peano toma al 1 como primer número natural, pero aquí adaptamos los axiomas para relacionarlos más fácilmente con lo que veremos más adelante.

4. Si a, b, c son números naturales y $a = b$ y $b = c$, entonces $a = c$.

5. Si $a = b$ y b es un número natural, entonces a es un número natural.

6. Si a es un número natural, también lo es su siguiente.

7. Dos números naturales a y b son iguales si y sólo si sus siguientes son iguales.

8. El 0 no es el siguiente de ningún número natural.

9. Si A es un conjunto que contiene a 0 y, siempre que contiene a un número natural, también contiene a su siguiente, entonces A contiene a todos los números naturales.

Como vemos, Peano mezcla axiomas sobre la igualdad con axiomas que hablan propiamente sobre los números naturales. Si eliminamos los cuatro axiomas lógicos, los cinco que nos quedan, es decir, los axiomas 1, 6, 7, 8, 9 son los que hoy se conocen como *axiomas de Peano* y se corresponden con los teoremas de Dedekind había demostrado sobre los números naturales el año anterior.[8] Así, mientras Peano toma estos axiomas como punto de partida de su exposición de la aritmética elemental, Dedekind los demuestra a partir de los principios generales de la teoría de conjuntos y, aunque no lo expresa así exactamente, del trabajo de Dedekind se sigue inmediatamente que los axiomas de Peano caracterizan a los números naturales, en el sentido de que dos conjuntos cualesquiera (dotados de sendas funciones "siguiente" y en los que hemos escogido sendos elementos como 0) que cumplan los axiomas de Peano son esencialmente lo mismo, en cuanto que los elementos de uno pueden ponerse en correspondencia biunívoca de modo que el 0 de uno se corresponde con el 0 del otro, el siguiente de 0 de uno se corresponde con el siguiente de 0 del otro, etc.

Peano usa signos lógicos con el sentido de "y", "o", "si, ..., entonces", etc., aunque son bastante diferentes de los que se usan hoy en día. Por ejemplo, su octavo axioma lo expresaba así (literalmente, esta vez con el 1 en lugar del 0 moderno):

$$a \,\epsilon\, N.\Im.a + 1- = 1$$

Con notación moderna sería[9] $a \in \mathbb{N} \to a + 1 \neq 1$. No obstante, de su notación cabe destacar el uso de la letra griega épsilon en expresiones como $x \,\epsilon\, y$, que indican que x es un elemento del conjunto y , o que x pertenece a y, o que x está en y. Peano eligió precisamente la letra griega épsilon como abreviatura de $\grave{\epsilon}\sigma\tau\acute{\iota}$, que significa "está" en griego.

Tal y como el propio Peano explicaba en el preámbulo de su artículo, su propósito era diseñar un lenguaje, una notación matemática, que permitiera expresar y manipular las afirmaciones matemáticas con total precisión, pero, por lo demás, el contenido lógico de su trabajo era escaso.

En otro orden de cosas, en **1890** Peano publicó un artículo titulado *Sobre una curva que llena completamente un área plana,* en el que construye lo que en términos modernos es una aplicación continua y suprayectiva $f : [0, 1] \longrightarrow [0, 1] \times [0, 1]$. Como él mismo señala, Cantor había demostrado que es posible establecer una biyección entre ambos conjuntos, pero tal biyección no puede ser continua. Su curva era continua y suprayectiva, pero, necesariamente, no era inyectiva.

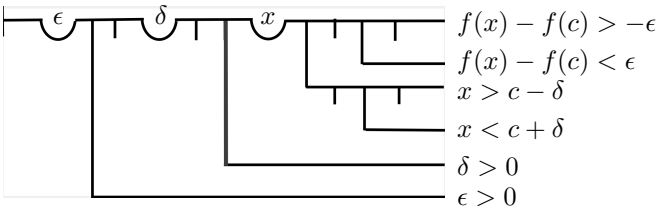
Aunque la idea de formalizar el razonamiento lógico se remonta a Aristóteles y tiene varios precedentes históricos, como en Leibniz, en Augustus De Morgan, o en George Boole (que era la principal referencia de Peano en materia de lógica), el primer ensayo moderno sobre lógica matemática había sido publicado en 1879 por Gottlob Frege con el título de *Conceptografía, un lenguaje basado en fórmulas, modelado sobre el de la aritmética, para el pensamiento puro,* pero su notación era tan técnica y enrevesada que la obra había pasado sin pena ni gloria entre la comunidad matemática. Por ejemplo, he aquí el enunciado de la definición de continuidad escrito con la notación de Frege:

[8] Peano cita el trabajo de Dedekind como una de sus fuentes.

[9] La notación $a + 1$ no supone que Peano hubiera definido la suma de números naturales previamente a la formulación de sus axiomas, sino que era meramente la forma en que expresaba el concepto de "siguiente de". La suma la define posteriormente con la "definición"

$$a, b \,\epsilon\, N.\Im.a + (b + 1) = (a + b) + 1$$

que explica que ha de entenderse así: *Si a, b son números y $a + b$ está definido, pero $a + (b + 1)$ aún no ha sido definido, entonces $a + (b + 1)$ denota al siguiente de $a + b$.* El signo $\Im$ es una C al revés que Peano usaba por el latín *continet* (contiene).



Hay que leer: para todo $\epsilon > 0$ existe un $\delta > 0$ tal que para todo x, si $c - \delta < x < c + \delta$, entonces $-\epsilon < f(x) - f(c) < \epsilon$ (por ejemplo, las rayitas verticales que hay antes y después del δ indican que es "existe un δ" y no "para todo δ").

Desde que publicó su *conceptografía,* Frege seguía tratando de establecer una fundamentación lógica de toda la matemática. En 1894 escribiría:

> *No puede pedirse que se demuestre todo, pero sí que podemos exigir que todas las proposiciones que se utilizan sin demostración sean expresamente proclamadas como tales, de manera que podamos ver con exactitud en qué se apoya toda la estructura. Después de esto, debemos tratar de reducir todo lo posible el número de estas leyes primitivas demostrando todo lo que sea demostrable. Además pido —y en eso voy más lejos que Euclides— que todos los métodos de inferencia utilizados se especifiquen de antemano.*

Tampoco tendría mucho éxito entre los matemáticos la obra de Charles Sanders Peirce, que en 1881 había axiomatizado la aritmética de los números naturales de forma similar a Peano, aunque menos detallada, y que en 1885 había estudiado la lógica de los cuantificadores "para todo" y "existe", cosa que también había hecho Frege, pero la obra de Peirce se popularizó un poco más gracias a Ernst Schröder, que en **1890** publicó (a su costa) el primero de los tres volúmenes de su obra maestra, titulada *Lecciones sobre el álgebra de la lógica,* donde, siguiendo a Peirce, usaba $\sum_x$ para indicar "existe un x" y $\prod_x$ para indicar "para todo x".

Schröder usaba también los signos $\subset$ y $\supset$ para indicar tanto la inclusión entre conjuntos (en el sentido moderno) como la implicación lógica. Así, $p \supset q$ significaba para él que la proposición p incluye (implica) la proposición q. No parece que tenga conexión con la C invertida $\Im$ de Peano, porque Schröder explica su notación como derivada de los signos aritméticos $<$ y $>$.

10 El teorema de Cantor En **1891** murió Kronecker a sus 68 años. Cantor tenía entonces 46. Ese año publicó un artículo titulado *Sobre una cuestión elemental de la teoría de la multiplicidad,* en el que presentó una prueba mucho más sencilla de la no numerabilidad del conjunto de los números reales (lo que hoy se conoce como el argumento diagonal de Cantor) junto con un teorema mucho más general que hoy se conoce como

> **Teorema de Cantor** Todo conjunto X tiene cardinal estrictamente menor que el del conjunto $\mathcal{P}X$ formado por todos los subconjuntos de X.

Demostración: Por una parte, podemos considerar la asignación $x \mapsto \{x\}$ que a cada elemento x de X le asocia el elemento de $\mathcal{P}X$ cuyo único elemento es x. Este emparejamiento prueba que el cardinal de X es menor o igual que el de $\mathcal{P}X$, pero recordemos que el hecho de que haya muchos subconjuntos de X con más de un elemento y que, por lo tanto, no tienen pareja, no prueba que el cardinal de $\mathcal{P}X$ sea estrictamente mayor. Para probar que es así hay que demostrar que ambos conjuntos no son equipotentes, es decir:

> No es posible emparejar cada elemento x de X con un elemento A_x de $\mathcal{P}X$ (con o sin repeticiones) de modo que todos los elementos de $\mathcal{P}X$ tengan una pareja.

En realidad habría que probar que es imposible hacer un emparejamiento así sin repeticiones, pero el argumento de Cantor no requiere esa hipótesis. Merece la pena analizarlo con detalle:

Demostración: Supongamos que tal emparejamiento fuera posible, es decir, a cada elemento x de X le podemos asignar un subconjunto A_x de X, de modo que todo subconjunto de X es de la forma A_x para algún elemento x.

Puesto que x es un elemento de X y A_x es un subconjunto de X, caben dos posibilidades, según si x es concretamente un elemento de A_x o si no lo es. Esto nos permite definir como sigue un subconjunto de X:

> Llamamos C al conjunto formado por cada elemento x de X que no está en el conjunto A_x.

No excluimos la posibilidad de que C sea el conjunto vacío, es decir, de que no contenga elemento alguno, lo cual significaría que cada elemento x de X es siempre un elemento de su pareja A_x. Sea como sea, lo cierto es que C es un subconjunto de X (un elemento de $\mathcal{P}X$), y estamos suponiendo que hemos construido una correspondencia por la que todo elemento de $\mathcal{P}X$ tiene una pareja, es decir, que tiene que existir un elemento c en X tal que $C = A_c$. Pero entonces, ¿c está o no está en A_c?

Si suponemos que c está en $A_c = C$, por definición de C, esto requeriría que c no estuviera en A_c, en contra de lo supuesto, pero si suponemos que c no está en $A_c = C$, de nuevo por la definición de C tendría que cumplirse que c sí que está en A_c. Sea como sea, tenemos una contradicción, y esto nos permite concluir, por reducción al absurdo, que el conjunto $\mathcal{P}X$ tiene estrictamente más elementos que X. ∎

Por ejemplo, si aplicamos el argumento cuando X es el conjunto de los números naturales, lo que se prueba es que si consideramos cualquier sucesión

$$A_0, \quad A_1, \quad A_2, \quad A_3, \quad \dots$$

de subconjuntos del conjunto de los números naturales, siempre es posible construir un subconjunto C (el formado por los números n que no están en el correspondiente A_n) que no es ninguno de los de la sucesión. Ninguna sucesión puede recorrer todos los conjuntos formados por números naturales. Siempre hay al menos uno que se queda fuera.

11 La medida de Jordan En 1882 Camille Jordan había publicado el primer volumen de su *Curso de análisis,* y en **1892** apareció el tercero y último con algunos conceptos nuevos que conviene que analicemos.

Riemann había definido lo que hoy se conoce como integral de Riemann para funciones f acotadas en un intervalo $a \le x \le b$. Su definición consistía en considerar particiones

$$a = x_0 \le x_1 \le \cdots \le x_n = b,$$

tomar puntos $x_{i-1} \le t_i \le x_i$, y calcular las sumas

$$S = \sum_{i=1}^{n} f(t_i)(x_i - x_{i-1}).$$

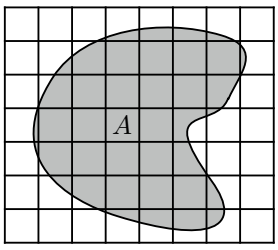
Una función es integrable Riemann si y sólo si estas sumas tienden a un límite L, en el sentido de que, tomando particiones en las que todas las longitudes $x_i - x_{i-1}$ sean suficientemente pequeñas, se puede asegurar que $|S - L|$ se hace arbitrariamente pequeño. En tal caso, dicho límite L es lo que se conoce como la integral $\int_a^b f(x)\,dx$.

Esta definición había sido mejorada por Gaston Darboux en su *Memoria sobre las funciones discontinuas,* de 1875, donde introdujo los conceptos de *integral inferior* e *integral superior* de Darboux.[10]

Muchos libros generalizaban de la forma obvia el concepto de integral Riemann a funciones de varias variables. Por ejemplo, si tenemos una función f acotada sobre un recinto acotado del plano A, como el que muestra la figura siguiente, cubrimos el dominio con una red de cuadrados (o rectángulos) C_{ij}, elegimos un punto t_{ij} de cada uno de ellos, y calculamos la suma

$$S = \sum_{i,j} f(t_{ij})\, a(C_{ij}),$$

donde $a(C_{ij})$ es el área del cuadrado que ocupa la posición i, j. Como en el caso de una variable, si estas sumas tienden a un límite L, se dice que la función es integrable Riemann y el límite es el valor de la integral $\int_A f(x,y)\,dxdy$.



Ahora bien, falta especificar si estas sumas se calculan sobre todos los cuadrados que cortan al dominio de la función, o únicamente sobre los que están totalmente contenidos en él. Se decía que esto era irrelevante, porque la suma de las áreas de los cuadrados que tocan la frontera del conjunto se vuelve arbitrariamente pequeña

[10] Para cada partición del intervalo, Darboux definía el ínfimo m_i y el supremo M_i de los valores que toma f para $x_{i-1} \le x \le x_i$, y consideraba las sumas

$$\underline{S} = \sum_{i=1}^{n} m_i(x_i - x_{i-1}), \qquad \overline{S} = \sum_{i=1}^{n} M_i(x_i - x_{i-1}).$$

La integral inferior se define como el supremo de las sumas $\underline{S}$, para todas las particiones posibles, y la integral superior como el ínfimo de las sumas $\overline{S}$. La función es *integrable Darboux* cuando ambas sumas coinciden, y el valor común es el valor de la integral. La integrabilidad Darboux era equivalente a la integrabilidad Riemann.

cuando más pequeños son los cuadrados considerados, pero la curva que había construido Peano en 1890 y que llenaba un cuadrado mostraba que esto no era necesariamente cierto. Si la frontera del conjunto A "llenaba un área", como la curva de Peano, no estaba unívocamente determinada cuál es el área del conjunto A, ni, por consiguiente, cuál es el valor de la integral de una función sobre A. (Podría pensarse en adoptar el convenio de definir la integral con todos los cuadrados que cortan a A, pero esta clase de convenios arbitrarios es la que hace que luego en las demostraciones las cosas no encajen.)

Por esto Jordán introdujo la integral de Riemann para funciones de varias variables de una forma novedosa, calculando primero lo que debe entenderse por área de un conjunto A antes de entrar a definir la integral. Y a su vez, para ello imitó la construcción de la integral de Darboux, es decir (considerando el caso bidimensional por simplicidad), para cada conjunto acotado A, consideró todas las sumas

$$\underline{S} = \sum_{ij} a(C_{ij}), \qquad \overline{S} = \sum_{ij} a(C_{ij}),$$

donde en el primer caso se suma sobre todos los cuadrados contenidos en A, y en el segundo caso sobre todos los cuadrados que tienen puntos de A. De este modo, $\underline{S}$ es la suma de las áreas de un conjunto finito de cuadrados que no se solapan y que están todos contenidos en A. Cualquier número $a(A)$ que queramos tomar como medida del área de A debe cumplir $\underline{S} \leq a(A)$. Similarmente, la suma $\overline{S}$ es la suma de las áreas de un conjunto finito de cuadrados que no se solapan y cubren A por completo, por lo que cualquier medida del área de A debe cumplir, de hecho:

$$\underline{S} \leq a(A) \leq \overline{S}.$$

Esto significa que el área de A (que queremos definir) tiene que ser una cota superior del conjunto de todas las sumas $\underline{S}$ que pueden formarse considerando cuadrados (o rectángulos) arbitrariamente pequeños, y también una cota superior del conjunto de todas las sumas $\overline{S}$.

Jordan definía el *contenido interior* de un conjunto acotado A como el supremo $c_i(A)$ de las sumas $\underline{S}$ y el *contenido exterior* como el ínfimo $c_e(A)$ de las sumas $\overline{S}$. Recordando que el supremo es la menor cota superior y que el ínfimo es la mayor cota inferior, tiene que cumplirse que

$$c_i(A) \leq a(A) \leq c_e(A).$$

Si se da la desigualdad $c_i(A) < c_e(A)$, no tenemos criterio para tomar como área de A ningún número en particular que esté comprendido entre estos dos valores, pero si los dos contenidos coinciden, el valor común es el único número que resulta razonable tomar como área de A.

Jordan llamó conjuntos medibles (y no tardaron en llamarse conjuntos *medibles Jordan*) a los conjuntos acotados del plano (o de cualquier espacio de n dimensiones) que cumplen $c_i(A) = c_e(A)$, y a dicho valor común se le llamó *medida de Jordan* del conjunto A.

Jordan demostró que un conjunto A es medible Jordan si y sólo si su frontera tiene medida de Jordan 0 (es decir, si puede cubrirse con un número finito cuadrados que no se solapen cuyas medidas sumen una cantidad arbitrariamente pequeña). Y a continuación definió la integral de una función acotada sobre un conjunto medible Jordan, para lo cual ya no necesitaba limitarse a considerar cuadrados, sino que podía cubrir el conjunto con familias finitas de conjuntos medibles Jordan cualesquiera, y todo funcionaba bien. La integral resultante era la integral de Riemann usual.

Naturalmente, para conjuntos "clásicos" (polígonos, círculos, pirámides, conos, esferas, etc.) su medida de Jordan era su área o su volumen con el valor usual que ya habían determinado los matemáticos griegos.

Este enfoque de Jordan del cálculo integral podía calificarse de "cantoriano", pues nunca hasta entonces se había trabajado con conjuntos tan generales como los conjuntos medibles Jordan.[11]

12 La antinomia de Burali-Forti En **1895** Cantor publicó la primera parte de un trabajo titulado *Contribuciones a la fundación de la teoría de los números transfinitos,* en el que expone desde cero su teoría sobre cardinales y ordinales infinitos, empezando por la definición de conjunto:

> *Por un "conjunto" entenderemos una colección cualquiera M de objetos definidos y bien diferenciados de nuestra percepción o de nuestro pensamiento (los cuales se llaman elementos de M) como un todo.*

[11] En realidad Peano había llegado a resultados similares en un trabajo de 1887 titulado *aplicaciones geométricas del cálculo diferencial.*

Tras discutir el concepto de "parte" (es decir, "subconjunto"), da esta definición:

> *Cada agregado M tiene una "potencia" definida, a la que también llamaremos su "número cardinal".*
>
> *Llamaremos "potencia" o "número cardinal" de M al concepto general que, mediante nuestra facultad activa de pensamiento, surge del agregado M al abstraer la naturaleza de sus diversos elementos m y el orden en que se dan.*
>
> *Denotamos el resultado de esta doble abstracción, el número cardinal o potencia de M, por $\overline{\overline{M}}$.*

Luego convierte esto en algo operativo introduciendo el concepto de equipotencia y afirmando que dos conjuntos tienen el mismo cardinal si y sólo si son equipotentes, y seguidamente introduce el concepto de minuspotencia y lo traduce a una relación de orden entre cardinales. Una diferencia respecto a trabajos anteriores consiste en que Cantor demuestra que, dados dos cardinales $\mathfrak{a}$ y $\mathfrak{b}$, sólo puede darse una de las tres relaciones

$$\mathfrak{a} = \mathfrak{b}, \qquad \mathfrak{a} < \mathfrak{b}, \qquad \mathfrak{b} < \mathfrak{a},$$

pero no es capaz de demostrar que tiene que darse al menos una de ellas. Cantor sabía demostrar este *principio de tricotomía* a partir del principio de buena ordenación, que anteriormente había dado por evidente, pero ahora consideraba que éste requeriría una prueba. Cantor señala que el principio de tricotomía permitiría demostrar el teorema $(*)$ que había enunciado unos años atrás (página 14), que ahora enunciaba advirtiendo de que no lo iba a usar.

A continuación, Cantor define la suma, el producto y la exponenciación de cardinales. Las definiciones generalizan las usuales para cardinales finitos. En términos resumidos:

- La suma de dos cardinales $\mathfrak{a}$ y $\mathfrak{b}$ es el cardinal $\mathfrak{a}+\mathfrak{b}$ de cualquier conjunto obtenido como unión de dos conjuntos disjuntos de los cardinales dados.
- El producto de dos cardinales $\mathfrak{a}$ y $\mathfrak{b}$ es el cardinal $\mathfrak{ab}$ del conjunto formado por todos los pares ordenados que pueden formarse con los elementos de un conjunto A de cardinal $\mathfrak{a}$ y otro conjunto B de cardinal $\mathfrak{b}$.
- La exponenciación de dos cardinales $\mathfrak{a}$ y $\mathfrak{b}$ es el cardinal $\mathfrak{a}^{\mathfrak{b}}$ del conjunto de todas las aplicaciones[12] de un conjunto de cardinal B en un conjunto de cardinal A.

Esta última operación la había descubierto ese mismo año. Cantor demuestra que estas operaciones satisfacen todas las relaciones aritméticas usuales, del estilo de $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{ab}+\mathfrak{ac}$.

Luego estudia los cardinales finitos e introduce un nombre para el cardinal de los conjuntos numerables: $\aleph_0$, donde $\aleph$ (álef) es la primera letra hebrea. (Cantor era un luterano devoto, pero tenía ascendencia judía.)

Cantor muestra que la aritmética de los cardinales infinitos presenta diferencias sustanciales con la de los cardinales finitos. Por ejemplo, si μ es un cardinal finito (no nulo en el caso de la segunda igualdad), entonces

$$\aleph_0 + \mu = \aleph_0, \qquad \aleph_0 \cdot \mu = \aleph_0, \qquad \aleph_0 + \aleph_0 = \aleph_0, \qquad \aleph_0 \cdot \aleph_0 = \aleph_0.$$

Por ejemplo, las dos últimas igualdades las hemos demostrado en la sección 5. El hecho de que al unir los números enteros positivos con los números enteros negativos (es decir, dos conjuntos numerables disjuntos) se obtenga un conjunto numerable, prueba que $\aleph_0+\aleph_0 = \aleph_0$, y el hecho de que los pares de números naturales sean un conjunto numerable prueba que $\aleph_0 \cdot \aleph_0 = \aleph_0$. Las dos primeras igualdades se demuestran más fácilmente.

En cuanto a la exponenciación de cardinales, Cantor demuestra que la potencia del continuo es $2^{\aleph_0}$. Esto lo consideró un gran avance, pues, por ejemplo, con esta expresión podía pasar inmediatamente de la igualdad elemental $\aleph_0 + \aleph_0 = \aleph_0$ a que

$$2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0+\aleph_0} = 2^{\aleph_0},$$

que a su vez se traducía en que hay el mismo número de puntos en el continuo de dimensión 1 y el continuo de dimensión 2 (y, más en general, en el continuo de cualquier dimensión finita n). En otras palabras, que hay el mismo número de puntos en una recta, que en un plano o que en un espacio de n dimensiones. Cantor se mostró muy satisfecho de que con este cálculo demostraba "de un plumazo" lo que años antes había obtenido con un argumento mucho más complicado.

[12] Así tenemos $\mathfrak{a}$ asignaciones posibles para cada elemento b de B, con lo que el número total de asignaciones posibles resulta de multiplicar $\mathfrak{a}$ por sí mismo $\mathfrak{b}$ veces. Cantor llama "cubrimientos de B por A" a las aplicaciones de A en B.

A continuación Cantor define un concepto general de ordinal, como determinación del tipo de orden de cualquier conjunto, no necesariamente bien ordenado:

> *Todo agregado ordenado M tiene un "tipo ordinal" definido, o más brevemente, un "tipo" definido, que denotaremos por $\overline{M}$. Con esto entendemos el concepto general que resulta de M si simplemente abstraemos la naturaleza de los elementos m y conservamos el orden de precedencia entre ellos. Así, el tipo ordinal $\overline{M}$ es en sí mismo un agregado ordenado cuyos elementos son unidades que tienen el mismo orden de precedencia entre sí que los elementos correspondientes de M, de los cuales se derivan por abstracción.*

Como en el caso de los cardinales, esto se concreta definiendo que dos conjuntos ordenados son *similares* si es posible poner en correspondencia biunívoca sus elementos de modo que se respete la ordenación, es decir, que si un elemento es menor que otro, los elementos correspondientes en el otro conjunto cumplen la misma relación. Entonces, dos conjuntos son similares si y sólo si tienen el mismo ordinal.

Luego Cantor explica que los ordinales (de conjuntos) finitos se corresponden con los cardinales finitos, mientras que cada cardinal infinito se corresponde con una "clase de tipos", es decir, con las distintas formas en que puede ordenarse un conjunto de un cardinal dado. (Hemos visto ejemplos de esto en la sección 6.)

Después define la suma y el producto de ordinales:

- La suma de dos ordinales α, β es el ordinal $\alpha+\beta$ del conjunto ordenado que resulta de disponer primero los elementos de un conjunto de ordinal α seguidos de los elementos de un conjunto de ordinal β.

- El producto de dos ordinales α, β es el ordinal $\alpha\beta$ del conjunto ordenado formado por todos los pares (a,b) formados con los elementos de un conjunto de ordinal α y otro de ordinal β, ordenados de modo que $(a,b)<(a',b')$ si se cumple $b<b'$ o, en caso en que $b=b'$, entonces $a<a'$.

Con esto Cantor se corrige a sí mismo y muestra que el ordinal $\omega+\omega$ es igual a $\omega\cdot 2$, pero no a $2\cdot\omega=\omega$, en contra de la notación que había venido empleando hasta entonces. En efecto, $\omega\cdot 2$ es el tipo de orden que se obtiene al considerar pares (a,b), donde a recorre los números naturales y $b=0,1$, comparando primero la segunda componente, es decir, poniendo primero todos los pares que terminan en 0 y luego todos los que terminan en 1:

$$(0,0),\quad (1,0),\quad (2,0),\quad \ldots\quad (0,1),\quad (1,1),\quad (2,1),\quad \ldots$$

Vemos que el tipo de orden es $\omega+\omega$, es decir, el orden que resulta de poner primero ω elementos y luego otros ω. En cambio, $2\cdot\omega$ es el tipo de orden de

$$(0,0),\quad (1,0),\quad (0,1),\quad (1,1),\quad (0,2),\quad (1,2),\quad \ldots$$

que claramente es ω.

Similarmente, si n es un ordinal finito, se cumple que $n+\omega=\omega$, mientras que $\omega+n$ es un ordinal mayor. Por ejemplo, $\omega+2$ se obtiene disponiendo primero ω elementos, y luego otros dos:

$$\circ\quad \circ\quad \circ\quad \circ\quad \circ\quad \cdots\quad \bullet\quad \bullet,$$

mientras que $2+\omega$ se obtiene disponiendo primero dos elementos y luego otros ω:

$$\bullet\quad \bullet\quad \circ\quad \circ\quad \circ\quad \circ\quad \circ\quad \cdots$$

con lo que el resultado es obviamente ω.

En particular la suma y el producto de ordinales no son conmutativos. Por lo demás, Cantor demuestra que cumplen la propiedad asociativa y la distributiva por la izquierda (pero no por la derecha):

$$\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma.$$

Para terminar Cantor presenta los resultados que deberían haber aparecido en el artículo que Mittag-Leffler le había pedido que retirara de *Acta Mathematica.* Sus conclusiones principales son las siguientes:

1) Todo conjunto ordenado X que a) sea numerable, b) no tenga máximo ni mínimo y c) sea denso en sí mismo (entre dos cualesquiera de sus puntos haya un tercero) tiene el mismo tipo de orden que el conjunto de los números racionales $0 < q < 1$.

2) Todo conjunto ordenado X que a) toda sucesión creciente (o decreciente) en X tiene supremo (ínfimo) y b) X contiene un subconjunto denso numerable D (donde "denso" significa que entre dos puntos de X hay siempre un punto de D) tiene el mismo tipo de orden que el "continuo lineal" (el intervalo de los números reales $0 \leq x \leq 1$).

Observemos que el conjunto de todos los números racionales cumple los requisitos del teorema 1, luego también podemos decir que todo conjunto ordenado numerable sin máximo ni mínimo y denso en sí mismo tiene el mismo tipo de orden que el conjunto de los números racionales.

En cuanto al segundo teorema, una ligera variante caracteriza el tipo de orden de la recta real como el tipo de orden de cualquier conjunto que cumpla a) no tiene máximo ni mínimo, b) es completo en el sentido de Dedekind (todo subconjunto no vacío y acotado superiormente tiene supremo) y c) contiene un subconjunto denso numerable.

Con esto termina la primera parte del trabajo, pero antes de que fuera publicada Cantor ya estaba ya preparando la segunda, cuyos contenidos vamos a seguir comentando aquí.

La primera sección de la segunda parte (que es la duodécima del trabajo completo) introduce el concepto de buen orden. La definición que da Cantor es un poco complicada, pero acaba demostrando que un conjunto está bien ordenado si cada uno de sus subconjuntos no vacíos tiene un mínimo elemento.

Luego estudia las propiedades básicas de los conjuntos bien ordenados. Para enunciarlas es fundamental el concepto de "sección inicial" de un conjunto bien ordenado (Cantor usa la palabra "segmento"):

Definición Si A es un conjunto ordenado y $a \in A$, *la sección inicial* determinada por a en A es el conjunto ordenado formado por los elementos de A menores que a.

Los resultados principales que demuestra Cantor son los siguientes:

1. Un conjunto bien ordenado nunca es similar a una de sus secciones iniciales.

   Demostración: Sea A un conjunto bien ordenado y sea A' la sección inicial formada por los elementos de A menores que un cierto a. Supongamos que A es similar a A'. Esto significa que podemos hacer corresponder cada x en A con un x' en A' (y así $x' < a$) de modo que se conserve el orden. Sea $a' < a$ el elemento correspondiente a a.

   Sea a'' el elemento correspondiente a a'. Como $a' < a$ y la correspondencia conserva el orden, tiene que ser $a'' < a' < a$. Igualmente, si consideramos el elemento a''' correspondiente a a'', tiene que ser $a''' < a''$, y así vamos obteniendo una sucesión

   $$a > a' > a'' > a''' > \cdots$$

   de elementos de A, que forman un subconjunto de A sin mínimo elemento, en contradicción con que A está bien ordenado. ∎

2. Dados dos conjuntos bien ordenados, o bien son similares, o bien uno es similar a una única sección inicial del otro.

   En lugar de discutir los tecnicismos de la demostración, vamos a dar la idea subyacente a la prueba. Para ello pongamos que tenemos un conjunto A de ordinal $\omega + 2$ y otro B de ordinal $\omega + \omega$. La situación es la que muestra el esquema siguiente:

   $$\begin{array}{c|ccccccccccc} A & a_0 & a_1 & a_2 & \cdots & a_\omega & a_{\omega+1} & a_{\omega+2} & & & \\ & \downarrow & \downarrow & \downarrow & & \downarrow & \downarrow & \downarrow & & & \\ B & b_0 & b_1 & b_2 & \cdots & b_\omega & b_{\omega+1} & b_{\omega+2} & b_{\omega+3} & b_{\omega+4} & \cdots \end{array}$$

   En una correspondencia entre A y una sección inicial de B, si un elemento de B se corresponde con uno de A, todos los menores que él tienen que corresponderse también con algún elemento de A o, de lo contrario, la imagen de la correspondencia no sería una sección inicial. Por eso, al mínimo elemento a_0 de A tenemos que hacerle corresponder necesariamente el mínimo b_0 de B. Pero entonces, al siguiente elemento de A (el elemento a_1), tenemos que asignarle necesariamente el siguiente elemento de B (el elemento b_1) y así, no tenemos opción a la hora de elegir las imágenes de $a_0, a_1, a_2, \ldots$

Una vez hemos asignado a estos elementos sus imágenes $b_0, b_1, b_2, \ldots$, tampoco tenemos opción a la hora de elegir la imagen de a_ω. Tiene que ser el menor elemento de B que no tiene aún imagen (o de lo contrario, nos saltaríamos un elemento y la imagen no sería una sección inicial). Así pues, a_ω tiene que corresponderse con b_ω, e igualmente estamos forzados a asignar $b_{\omega+1}$ y $b_{\omega+2}$ a los dos últimos elementos de A.

En general, pueden darse dos casos:

(a) Llega un momento en que a un elemento de A, digamos a_α, no se le puede hacer corresponder ningún elemento de B. Eso sólo puede deberse a que ya los hemos usado todos, y entonces B es similar a la sección inicial de A determinada por a_α.

(b) Podemos asignar un elemento de B a cada elemento de A. En este caso, si todos los elementos de B están asignados a alguno de A, tenemos que A y B son semejantes. En caso contrario, podemos tomar el mínimo b_β en B que no está asignado a ningún elemento de A, y resulta que A es similar a la sección inicial de B determinada por b_β.

En la sección siguiente Cantor define los "números ordinales" como los ordinales (en el sentido genérico de tipo de orden que hemos indicado más arriba) de los conjuntos bien ordenados. Luego define una relación de orden sobre los propios ordinales, según la cual dos números ordinales cumplen $\alpha < \beta$ si un conjunto de ordinal α es similar a una sección inicial de un conjunto de ordinal β. Y dice:

Así, los números ordinales forman, al ordenarse en orden de magnitud, un agregado ordenado; más adelante se verá que es un agregado bien ordenado.

Sin embargo, Cantor se pone a discutir la aritmética de los números ordinales y "más delante" no se vuelve a hablar del asunto. ¿Por qué? Antes de responder a esa pregunta, observemos que, con lo visto hasta aquí, la situación es sencilla:

Teorema El conjunto de todos los ordinales menores que uno dado α es un conjunto bien ordenado de ordinal α.

La idea de fondo es muy simple. Por ejemplo, si $\alpha = \omega + \omega$, un conjunto bien ordenado de ordinal $\omega + \omega$ es de la forma

$$a_0, \quad a_1, \quad a_2, \quad \ldots \quad a_\omega, \quad a_{\omega+1}, \quad a_{\omega+2}, \quad \cdots$$

y la correspondencia $a_\alpha \mapsto \alpha$ muestra que A es similar al conjunto de todos los ordinales menores que $\omega + \omega$, luego éste está bien ordenado con ordinal $\omega + \omega$. Ahora veámoslo en general.

Demostración: Sea A un conjunto bien ordenado de ordinal α. Para cada elemento a de A, la sección inicial A_a que determina en A es un conjunto bien ordenado. Llamemos α_a a su ordinal.

Vamos a probar que la correspondencia $a \mapsto \alpha_a$ hace corresponder los elementos de A con todos los ordinales menores que α, lo que demuestra que el conjunto de todos ellos es similar a A, luego es un conjunto bien ordenado de ordinal α, como queremos demostrar.

Hemos demostrado que un conjunto bien ordenado A nunca es similar a una de sus secciones iniciales A_a, lo que se traduce en que $\alpha \neq \alpha_a$. Pero, hilando un poco más fino, tampoco puede ser $\alpha < \alpha_a$, pues esto significaría que A sería similar a un segmento inicial de A_a, digamos el determinado por b, pero el segmento inicial determinado por b en A_a es lo mismo que el segmento inicial determinado por b en A (es simplemente el conjunto de los elementos menores que b), y sabemos que A no puede ser similar a uno de sus segmentos.

Así pues, para cada a en A, se cumple que $\alpha_a < \alpha$. Por otra parte, todo $\beta < \alpha$ se corresponde con un elemento a de A, por la propia definición de la relación de orden: si $\beta < \alpha$ y B es un conjunto bien ordenado de ordinal β, como A tiene ordinal α, tenemos que B es similar a una sección inicial de A, digamos a la determinada por a, y entonces, por definición $\alpha_a = \beta$.

Esto prueba que la asignación $a \mapsto \alpha_a$ es una correspondencia biunívoca entre los elementos de A y los ordinales menores que α. Sólo falta probar que conserva el orden, pero si $a < b$ son elementos de A, tenemos que A_a es el segmento inicial de A_b determinado por a, luego, por la definición del orden entre ordinales, se cumple que $\alpha_a < \alpha_b$. ∎

De aquí se sigue lo que había anunciado Cantor:

Teorema El conjunto W de todos los ordinales está bien ordenado.

DEMOSTRACIÓN: Sea A es un subconjunto no vacío de W. Tenemos que probar que tiene un mínimo elemento. Sea α cualquier elemento de A. Si es el mínimo, ya hemos terminado. En caso contrario, sea A' el conjunto de los elementos de A menores que α, que es no vacío. Por el teorema anterior, el conjunto de todos los ordinales menores que α está bien ordenado, luego el conjunto A' tiene un mínimo elemento μ. Obviamente, si μ es el menor ordinal de A menor que α, también es el mínimo ordinal de A. ∎

Cantor sabía esto, pero no lo incluyó en la segunda parte de sus *Contribuciones.* ¿Por qué? Porque en **1895**, antes incluso de que la primera parte estuviera publicada, se encontró con algo desconcertante:

Llamemos Ω al ordinal de W. Si α es cualquier ordinal, hemos demostrado que el conjunto de los ordinales menores que α, es decir, la sección inicial de W determinada por α, tiene ordinal α, luego por la definición de la relación de orden entre ordinales, se cumple que $\alpha < \Omega$ (porque α es el ordinal de una sección inicial de W, que tiene ordinal Ω).

En suma, el ordinal Ω tiene que ser mayor que todos los ordinales. ¡Pero eso incluye al propio Ω!, es decir, se tiene que cumplir que $\Omega < \Omega$, que es tanto como decir que W es semejante a una sección inicial propia, cuando hemos probado que eso es imposible.

O una variante: Podemos considerar el ordinal $\Omega + 1$, que es el ordinal del conjunto bien ordenado W' que se obtiene añadiendo a W un elemento máximo M. Entonces W es la sección inicial de W' determinada por M, luego, por definición de la relación de orden, $\Omega < \Omega + 1$, pero también hemos demostrado que $\Omega + 1 < \Omega$ (¡porque todo ordinal es menor que Ω!)

¿Cómo puede ser que podamos demostrar que $\Omega < \Omega + 1$ y a la vez que $\Omega + 1 < \Omega$? En matemáticas es habitual el razonamiento por reducción al absurdo: se supone una hipótesis, a partir de ella se razona hasta llegar a una contradicción, y de ello se concluye que la hipótesis de partida era falsa, es decir, se considera demostrada su negación, pero Cantor había llegado a un absurdo sin suponer nada cuestionable. La teoría de Cantor permitía demostrar un hecho, y también lo contrario, sin que ningún paso del argumento pudiera considerarse erróneo por ningún motivo.

En los últimos años, uno de los más eminentes matemáticos de la época, David Hilbert, se había interesado por la teoría de conjuntos y había empezado a mantener correspondencia con Cantor. En **1895** Hilbert obtuvo una cátedra en la universidad de Gotinga, y en **1896** Cantor le escribió para contarle la paradoja que había descubierto. Hilbert quedó igualmente perplejo.

En **1897** se publicó finalmente la segunda parte de las *Contribuciones a la fundación de la teoría de los números transfinitos.* Cantor no había logrado descubrir ningún error que explicara la paradoja que había encontrado, así que, como hemos visto, guardó silencio sobre el hecho de que el conjunto de todos los ordinales está bien ordenado y, a partir de ese punto, pasó a estudiar la segunda clase numérica, es decir, los ordinales numerables, sin presentar prácticamente ninguna novedad, más allá de que da el nombre de $\aleph_1$ al cardinal de la segunda clase numérica y demuestra que es el menor cardinal infinito posterior a $\aleph_0$.

El trabajo termina con lo que hoy se conoce como

Teorema de la forma normal de Cantor Todo ordinal α se puede expresar de forma única como

$$\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_n},$$

con $\eta_0 \geq \eta_1 \geq \cdots \geq \eta_n$.

Esto viene a ser un análogo para ordinales de la expresión decimal de un número natural, pero tomando como base el ordinal ω.

Por las mismas fechas en que Cantor envió este trabajo para su publicación, un matemático italiano llamado Cesare Burali-Forti envió a su vez un artículo titulado *Una cuestión sobre los números transfinitos,* que esencialmente expone la paradoja que Cantor había encontrado (aunque se había abstenido de difundir), y que por ello se conoce hoy en día como la *antinomia de Burali-Forti.*

Técnicamente, Burali-Forti no la presentaba como una paradoja, sino como una demostración de que existen ordinales α y β que no cumplen ni $\alpha = \beta$, ni $\alpha < \beta$, ni $\beta < \alpha$. En efecto, suponiendo lo contrario, es decir, que cualquier par de ordinales son comparables, Burali-Forti llegaba a la contradicción $\Omega < \Omega + 1$ y $\Omega + 1 < \Omega$ a la que Cantor había llegado por su cuenta. O bien Burali-Forti desconocía que Cantor había demostrado lo contrario, o bien era una forma discreta de indicar que algo tenía que estar mal en dicho teorema (pero la prueba de Cantor no daba indicios de tener ninguna laguna).

Cantor había sido, junto con Felix Klein, uno de los impulsores del *Primer Congreso Internacional de Matemáticos,* que se celebró en Zúrich ese año con la presencia de 208 matemáticos de 16 países. Cantor tuvo ocasión de exponer su teoría y fueron muchos los asistentes que quedaron impresionados por sus resultados. Sus *Contribuciones* no tardaron en ser traducidas al italiano y al francés.

Cantor anunció en el congreso un resultado que había obtenido ese mismo año de **1897** un alumno suyo de 19 años llamado Felix Bernstein, que había demostrado el teorema $(*)$ de la página 14 sin recurrir al principio de buena ordenación, y por eso hoy se conoce como *teorema de Cantor-Bernstein.* El año anterior Schröder había anunciado una demostración que finalmente publicó en **1898**, pero cuatro años más tarde (poco antes de la muerte de Schröder) Alwin Reinhold Korselt señalaría que tenía un error.[13] La prueba de Bernstein se publicó ese mismo año en las *Lecciones sobre la teoría de funciones* de Émile Borel, a sugerencia de Cantor.

En 1899 Dedekind le comunicó a Cantor su prueba del teorema de Cantor-Bernstein, basada en las técnicas que había desarrollado en su artículo *¿Qué son y para qué sirven los números?* Cantor le respondió que sería muy útil si pudiera demostrar por los mismos métodos el principio de tricotomía.

13 La medida de Borel Émile Borel se había doctorado en 1893 bajo la dirección de Darboux, un año después de que Jordan publicara su concepto de medida. Desde entonces se había suscitado un debate entre los matemáticos. La medida de Jordan es *finitamente aditiva,* lo que significa que si una figura A se puede descomponer en unión disjunta de un número finito de figuras medibles Jordan $A_1, \ldots, A_k$, entonces A es medible Jordan, y su medida es

$$m(A) = \sum_{n=0}^{k} m(A_n).$$

La cuestión es si no sería razonable extenderla de modo que fuera σ-aditiva, es decir, que cumpliera esta misma propiedad, pero para una cantidad numerable de partes. En este sentido, la medida de Jordan es "casi" σ-aditiva, en cuanto a que si $\{A_n\}_{n=0}^{\infty}$ es una familia de conjuntos medibles Jordan disjuntos dos a dos cuya unión A es también medible Jordan, entonces

$$m(A) = \sum_{n=0}^{\infty} m(A_n),$$

pero hace falta suponer que A es medible Jordan, cosa que en general no tiene por qué ser cierta.

La cuestión, pues, era que, si tenemos un conjunto A en estas condiciones, entre considerar que no es medible o considerarlo medible y asignarle la medida dada por la suma de las medidas de los conjuntos A_n, ¿no era preferible la segunda opción?

La objeción principal es que los puntos tienen medida 0, por lo que en una extensión σ-aditiva de la medida de Jordan todos los conjuntos numerables tendrían medida 0. Pensemos, por ejemplo, en el conjunto A de los números racionales $0 \leq q \leq 1$. Forman un conjunto numerable que, en cierto sentido, "llena" el intervalo unitario. Es fácil ver que no es medible Jordan, porque su contenido interior es 0 (porque no cabe ningún segmento dentro de A) y su contenido exterior es 1. ¿No sería más razonable, puestos a asignarle a A una medida, hacer que ésta fuera 1 y no 0?

Estaba claro que la aditividad de una medida tiene que tener un límite. Por ejemplo, cualquier segmento (o cualquier círculo) está formado por $2^{\aleph_0}$ puntos de medida 0, y no por eso esperamos que tenga medida 0. ¿Es razonable pretender que un conjunto numerable tenga medida 0 sólo porque está compuesto por puntos de longitud 0?

El caso era que en análisis surgían contextos en los que era natural considerar como despreciables los conjuntos numerables, incluso si eran densos, como los números racionales, que "están por todas partes". El propio Borel se había encontrado con un caso así en su tesis doctoral. Por ello, en sus *Lecciones sobre la teoría de funciones,* de **1898**, "definió" una extensión σ-aditiva de la medida de Jordan. Ponemos "definió" entre comillas porque su definición era bastante críptica:

> *Todos los conjuntos que consideraremos estarán formados por puntos entre* 0 *y* 1. *Cuando un conjunto está formado por todos los puntos de una infinidad numerable de intervalos que no se superponen y tienen una longitud total s, diremos que el conjunto tiene medida s. Cuando dos conjuntos no tienen puntos comunes y sus medidas son s y s', el conjunto resultante de unirlos, es decir, su suma, tiene medida $s + s'$.*

[13] Por eso el teorema se conoce tanto como Teorema de Schröder-Bernstein o como teorema de Cantor-Bernstein, o incluso como Teorema de Cantor-Schröder-Bernstein.

> *De forma más general, si se tiene una infinidad numerable de conjuntos que, por pares, no tienen ningún punto común y cuyas medidas son $s_1, s_2, \ldots, s_n, \ldots$, su suma tiene medida $s_1 + s_2 + \cdots + s_n + \cdots$*
>
> *Todo esto es consecuencia de la definición de medida. Ahora bien, aquí hay algunas definiciones nuevas: si un conjunto E tiene medida s y contiene todos los puntos de un conjunto E' cuya medida es s', se dirá que el conjunto $E - E'$ tiene medida $s - s'$. Los conjuntos cuya medida se puede definir en virtud de las definiciones anteriores los denominaremos conjuntos medibles.*

Borel no aclaró más esta definición, pero, por los ejemplos que pone a continuación, se entiende que consideraba como tales a todas las uniones numerables de intervalos disjuntos dos a dos y a todos los conjuntos que pueden obtenerse de tales uniones mediante el cálculo de complementos y de uniones numerables:

> *Los conjuntos cuya medida puede definirse en virtud de las definiciones precedentes serán llamados por nosotros conjuntos medibles, sin que con esto queramos dar a entender que no es posible dar una definición de la medida de otros conjuntos; pero una definición así nos sería inútil; incluso podría estorbarnos, si no conservara en la medida las propiedades fundamentales que le hemos atribuido en las definiciones que hemos dado.*
>
> *Estas propiedades esenciales, que resumimos aquí por su utilidad, son las siguientes: la medida de la suma de una infinidad numerable de conjuntos es igual a la suma de sus medidas; la medida de la diferencia de dos conjuntos es igual a la diferencia de sus medidas;* la medida nunca es negativa; cualquier conjunto cuya medida no sea cero no es numerable. Es especialmente esta última propiedad la que utilizaremos. Se entiende expresamente que sólo hablaremos de medida en relación con los conjuntos que hemos llamado medibles.*
>
> (*) *Por supuesto, cuando hablamos de la suma de varios conjuntos, suponemos que no tienen, dos a dos, ningún elemento común y, cuando hablamos de su diferencia, suponemos que uno de ellos contiene todos los elementos del otro.*

Esto suponía un avance respecto a la medida de Jordan. Por ejemplo, Cantor había introducido el concepto de subconjunto cerrado de la recta real, y por esas fechas ya existía cierta costumbre de llamar "abiertos" a los complementarios de los conjuntos cerrados. Todo subconjunto abierto de la recta real se puede expresar como unión disjunta de intervalos abiertos, por lo que todos los conjuntos abiertos (en el intervalo unitario) eran medibles en el sentido de Borel, luego también lo eran sus complementarios, los cerrados. Esto no es cierto para la medida de Jordan. Por ejemplo, el conjunto de Cantor es medible Jordan, de medida 0, mientras que su complementario (siempre en el intervalo unitario) es un abierto no medible Jordan. En cambio, es medible Borel con medida 1.

14 Inducción y recursión transfinita En **1899** leyó su tesis doctoral René-Louis Baire, bajo la dirección de Charles Hermite. Se titulaba *Sobre las funciones de variables reales* y, entre otras cosas, se proponía iniciar un estudio sistemático de las funciones discontinuas, de las cuales se conocían ejemplos muy patológicos. Para ello definió una clase de funciones que más adelante se conocerían como *funciones de Baire.* Baire consideraba, concretamente, funciones definidas sobre un intervalo cerrado en la recta real, si bien la idea se extendía fácilmente a dominios más generales. Concretamente:

- Baire definía las funciones *de clase* 0 como las funciones continuas.
- Las funciones *de clase* 1 eran[14] los límites (puntuales) de una sucesión de funciones de clase 0 (lo que incluía trivialmente a las de clase 0).
- Las funciones *de clase* 2 eran[15] los límites de sucesiones de funciones de clase 1, etc.

  Pero, siguiendo a Cantor, ese "etc." no se detenía en los números naturales, sino que, para cada ordinal $\alpha < \omega_1$, Baire definía las *funciones de clase* α como los límites (puntuales) de sucesiones de funciones de clase menor que α.
- Las que hoy se conocen como *funciones de Baire* son las funciones de clase α, para algún $\alpha < \omega_1$.

[14] Por ejemplo, la derivada de una función continua no tiene por qué ser continua, pero siempre es una función de clase de Baire 1. Un ejemplo concreto de función (muy) discontinua de clase 1 es la función que vale 0 en los números irracionales y vale $1/q$ en los números racionales p/q (donde la fracción es irreducible).

[15] Un ejemplo de función de clase 2 que no es de clase 1 es la función que vale 1 en los números irracionales y vale 0 en los irracionales.

Esta definición se apoya en un principio fundamental sobre los ordinales de Cantor: el principio de recursión transfinita. En general, si queremos demostrar que todos los ordinales cumplen una determinada propiedad, podemos usar el *principio de inducción transfinita,* por el que basta demostrar que un ordinal α cumple la propiedad deseada tomando como hipótesis de inducción que los ordinales menores que α la cumplen.

Igualmente, para definir una sucesión transfinita (en este caso la sucesión de clases de funciones $\mathcal{B}_\alpha$), podemos aplicar el *principio de recursión transfinita*, por el que es legítimo definir el término α-ésimo de la sucesión suponiendo que ya están definidos los términos correspondientes a ordinales menores que α.

Por ejemplo, en el caso de la inducción transfinita, si hemos demostrado que α cumple la propiedad supuesto que la cumplen todos los ordinales menores que α, podemos razonar así:

- Todos los ordinales menores que 0 tienen la propiedad (porque no hay ninguno), luego podemos concluir que también la cumple el 0.
- Entonces, todos los ordinales menores que 1 cumplen la propiedad, luego podemos concluir que también la cumple el 1.
- Luego todos los ordinales menores que 2 cumplen la propiedad, luego también la cumple el 2, etc.

  $\vdots$
- Luego todos los ordinales menores que ω cumplen la propiedad, luego también la cumple ω.
- Luego todos los ordinales menores que $\omega+1$ cumplen la propiedad, luego también la cumple $\omega+1$, etc.

  $\vdots$
- Luego todos los ordinales menores que $\omega+\omega=\omega\cdot 2$ cumplen la propiedad, luego también la cumple $\omega\cdot 2$,

y así podemos ascender indefinidamente por todos los ordinales.[16] La idea subyacente bajo la recursión transfinita es la misma: Borel define el conjunto de las funciones de clase α supuesto que ya están definidos los conjuntos de funciones de clase β, para todo $\beta<\alpha$. El principio de recursión transfinita nos permitiría definir las funciones de clase α para cualquier ordinal α, no necesariamente menor que ω_1, pero sucede que todo límite puntual de una sucesión de funciones de Baire es de nuevo una función de Baire, por lo que las clases $\mathcal{B}_{\omega_1}, \mathcal{B}_{\omega_1+1}, \mathcal{B}_{\omega_1+2}$, etc. coinciden todas con la clase de Baire.

Hay otra forma de enunciar los principios de inducción y recursión transfinita que a menudo son más convenientes. Para ello observamos que hay tres clases de ordinales:

- El 0, que no tiene anteriores.
- Los *ordinales sucesores,* como $5,\ \omega+7,\ \omega^\omega+\omega+1$, etc., que tienen un inmediato anterior.
- Los *ordinales límite,* como $\omega,\ \omega\cdot 2,\ \omega^3\cdot 5+\omega,\ \omega^\omega$, etc., que tienen anteriores, pero no un inmediato anterior.

Entonces, para demostrar que todos los ordinales cumplen una propiedad, basta probar:

- que el 0 tiene la propiedad,
- que si un ordinal α tiene la propiedad, también la tiene el siguiente, $\alpha+1$.
- que si todos los ordinales anteriores a un ordinal límite λ tienen la propiedad, también la tiene λ.

Y, análogamente, para definir una sucesión transfinita $\{x_\alpha\}$, basta definir:

- x_0.
- $x_{\alpha+1}$ supuesto que ya está definido x_α.
- x_λ, donde λ es un ordinal límite, supuesto que ya está definido x_δ para todo ordinal $\delta<\lambda$.

[16] Esto no es una demostración del principio de inducción transfinita, sino sólo una explicación de por qué es razonable. La demostración es mucho más simple: si existiera un ordinal que no cumpliera la propiedad, como los ordinales están bien ordenados, podríamos considerar el mínimo ordinal α que no la cumple, pero entonces tendríamos que todos los ordinales menores que α tienen la propiedad, y estamos suponiendo que eso implica que α también la cumple, con lo que tenemos una contradicción.

15 La paradoja de Cantor En **1899** Cantor encontró una nueva paradoja en su teoría. Ésta surge cuando tratamos de aplicar el teorema de Cantor al conjunto V formado por todos los conjuntos. Si consideramos el conjunto $\mathcal{P}V$ de todos los subconjuntos de V, se da la peculiaridad de que $\mathcal{P}V$ es un subconjunto de V, ya que si X es un elemento de $\mathcal{P}V$, por definición es un subconjunto de V, luego en particular es un conjunto, luego es un elemento de V. Y un resultado elemental de la teoría de cardinales cantoriana es que si A es un subconjunto de B, entonces el cardinal de A es menor o igual que cardinal de elementos de B. En nuestro caso, tenemos que el número de elementos de $\mathcal{P}V$ tiene que ser menor o igual que el número de elementos de V, que es justo lo contrario de lo que afirma el teorema de Cantor.

En resumen: podemos demostrar (trivialmente) que el conjunto $\mathcal{P}V$ debe de tener un número de elementos menor o igual que el de V y (por el teorema de Cantor) también que ha de darse justo el caso contrario. Y tenemos así una contradicción que no procede de suponer nada cuestionable.

Hay un paralelismo completo con la antinomia de Burali-Forti: el ordinal del conjunto de todos los ordinales debería ser el mayor de todos, y el cardinal del conjunto de todos los conjuntos debería ser el mayor de todos, pero Cantor podía demostrar que por encima de un ordinal siempre hay otro, y que por encima de un cardinal siempre hay otro.

Cantor se dio cuenta de que las numerosas paradojas que surgían en su teoría tenían todas el mismo aspecto: surgían de considerar ciertos conjuntos "muy grandes". La antinomia de Burali-Forti surgía de considerar "el conjunto de todos los ordinales", la paradoja de Cantor de considerar "el conjunto de todos los conjuntos" y, descubierta la técnica, era posible generar contradicciones similares a partir de "el conjunto de todos los conjuntos finitos" o "el conjunto de todos los conjuntos infinitos" o "el conjunto de todos los conjuntos con siete elementos", etc.

Ello lo llevó a distinguir entre "conjuntos" y "multiplicidades inconsistentes", donde lo segundo eran colecciones de objetos que daban lugar a contradicciones si se las pretendía tratar como conjuntos. De este modo, se podía trabajar con relativa seguridad en su teoría de conjuntos sin más precaución que abstenerse de tratar como conjuntos las "multiplicidades inconsistentes", pero no había una definición precisa de "multiplicidad inconsistente", sino que éstas eran simplemente los conjuntos que se observaba que daban lugar a paradojas.

En estas condiciones, la situación de la fundamentación de la matemática en estas fechas era comparable a la de "los viejos tiempos". No había mucha diferencia conceptual entre aquellos números imaginarios que no existían, pero de los que podíamos hablar con moderación, (o entre aquellas cantidades infinitesimales que no eran cero, pero en los momentos oportunos se podían despreciar como si lo fueran) y las multiplicidades inconsistentes, que no eran conjuntos, pero que hasta cierto punto era como si lo fueran, y de las que podíamos hablar con moderación, siempre y cuando no abusáramos de ellas y cayéramos en contradicciones. Decididamente, las matemáticas estaban en ese momento muy lejos de poder ser expuestas en el "orden geométrico", partiendo de unas definiciones y unos principios básicos explícitos de los que puede deducirse todo lo demás mediante razonamientos lógicos sin riesgo de caer en contradicciones.

16 El formalismo Es posible que las paradojas de la teoría de conjuntos hubieran llevado a Hilbert a la convicción de que las matemáticas necesitaban una fundamentación al estilo de Euclides, y que, a su vez, esto lo hubiera llevado a interesarse por los *Elementos* como sistema lógico.

Hacía ya un tiempo que los geómetras se habían dado cuenta de que los *Elementos* de Euclides, aun siendo un excelente tratado de geometría, no eran exactamente lo que se decía que eran. No era cierto que todos los teoremas que Euclides demostraba en ellos se pudieran deducir lógicamente de sus postulados y definiciones. Quizá el primero en señalarlo había sido Moritz Pasch en 1882, quien identificó lo que hoy se conoce como *Axioma de Pasch,* que Euclides usaba implícitamente en algunas de sus demostraciones sin que pudiera deducirse de sus postulados. Dice así:

> Si una recta no pasa por los vértices de un triángulo, pero corta a uno de sus lados, necesariamente tiene que cortar también a uno de los otros dos lados.

Cualquiera que trate de dibujar un triángulo y una recta que pase por uno de sus lados (pero no por sus vértices) se convencerá inmediatamente de que no puede evitar que la recta pase también por otro de los lados. No se trata de poner en duda que esto es cierto, sino del hecho de que Euclides lo usaba sin que sea posible demostrarlo a partir de sus postulados. Y hay casos mucho más evidentes: el primer teorema que demuestra Euclides es la construcción de un triángulo equilátero a partir de un lado. El proceso es muy simple:

> Dado un segmento AB, se traza la circunferencia de centro A que pasa por B y la circunferencia de centro B que pasa por A y cualquiera de los dos puntos C donde ambas circunferencias se cortan sirve como tercer vértice de un triángulo equilátero ABC.

El único problema de esta "demostración" es que ninguno de los postulados de Euclides permite probar que las dos circunferencias tengan que cortarse en un punto C. Nuevamente, cualquiera que haga una figura se convencerá de que es imposible que no se corten, pero una cosa es que el hecho sea cierto y otra que sea consecuencia de unos principios dados.

Así, en general, los *Elementos* no se basan exclusivamente en los postulados que presentan como punto de partida, sino que ocasionalmente se usan otros hechos que pueden ser justificados fácilmente sin más que mirar la figura adecuada, pero que tendrían que ser incorporados a la lista de principios si queremos que ésta contenga realmente todos los principios que se presentan como evidentes, sin una demostración que los justifique a partir de otros más elementales.

En **1899**, Hilbert publicó sus *Grundlagen der Geometrie* (Fundamentos de la geometría), en los que daba una auténtica lista completa de axiomas para la geometría euclídea, de forma que todos sus teoremas pudieran demostrarse a partir de ellos sin necesidad de introducir "de contrabando" afirmaciones adicionales no demostradas. En total, Hilbert necesitó 21 axiomas (aunque posteriormente se dio cuenta de que uno de ellos era redundante y la lista se redujo a 20). Para que el lector se haga una idea del aspecto de estos axiomas, uno afirma, por ejemplo, que, dados dos puntos A y B, existe al menos un punto C situado entre ambos, y otro es el axioma de Pasch, que acabamos de comentar.

Para enfatizar la diferencia entre los *Elementos* y los *Grundlagen,* Hilbert señaló que para seguir los *Elementos* es imprescindible tener claro que la palabra "punto" significa punto, que "recta" significa recta, que "circunferencia" significa circunferencia, etc., de modo que, si estamos comprobando que la construcción de los triángulos equiláteros es correcta, tenemos que dibujar dos puntos, trazar dos circunferencias y convencernos de que necesariamente se tienen que cortar. En cambio, los *Grundlagen* podrían seguirse igualmente y comprobar que todos sus razonamientos son correctos aunque cambiáramos las palabras "punto", "recta", "plano" etc. por "mesa", "silla" y "jarra de cerveza". Esto es un hecho crucial, y quizá se entienda mejor con un ejemplo sencillo. Consideremos este razonamiento:

Toda palabra properispómena es barítona,
δῶρον es una palabra properispómena,
luego δῶρον es una palabra barítona.

Si consultamos una gramática griega y un diccionario veremos que todas estas palabras raras existen realmente y tienen un significado preciso, pero lo maravilloso del caso es que no necesitamos saber lo que significan para concluir que el razonamiento es correcto: Si sabemos que toda palabra properispómena (sea esto lo que sea) es barítona (sea esto lo que sea), así como que "*δῶρον*" (sea lo que sea) es una palabra properispómena (sea lo que sea), podemos afirmar sin miedo a equivocarnos que "*δῶρον*" (sea lo que sea) es una palabra barítona (sea lo que sea). Lo que Hilbert decía es que sus *Grundlagen* eran una lista de razonamientos cuya corrección se puede verificar sin necesidad de saber qué significan las palabras "punto", "recta", "pasar por", "estar entre", etc. exactamente igual que el razonamiento precedente se puede verificar sin necesidad de saber qué significan las palabras "properispómena", "barítona", etc.

Esto se expresa diciendo que los *Grundlagen* son una teoría axiomática *formal,* donde "formal" significa que el paso de unas afirmaciones a otras no depende de su *significado* (de su contenido material), sino de su *forma* (de su estructura formal). Por ejemplo,

Todo A es B,
C es A,
luego C es B

es una *forma* de razonamiento válida, en el sentido de que, si en lugar de A, B, C, ponemos expresiones cualesquiera que tengan sentido, si las dos primeras afirmaciones resultan ser verdaderas, signifiquen lo que signifiquen, la tercera también lo será necesariamente.

Naturalmente, no es obvio *a priori* qué formas de razonamiento son válidas. Por ejemplo, la forma

Todo A es B,
C no es A,
luego C no es B

no es una forma de razonamiento válida, como puede comprobarse mediante una elección oportuna de A, B, C:

Toda gallina es un ave,
un gorrión no es una gallina,
luego un gorrión no es un ave.

Aquí vemos que las dos primeras afirmaciones son verdaderas, pero la tercera es falsa. Precisamente, determinar las formas de razonamiento válidas es uno de los propósitos básicos de la lógica matemática, y la importancia de esto se entenderá en breve.

17 Los álefs En **1900** se celebró en París el *Segundo Congreso Internacional de Matemáticos,* en el que David Hilbert dio una conferencia en la que presentó una lista con los 23 problemas que, a su juicio, eran los más importantes que tenía planteada la matemática del próximo siglo. El primero de ellos era demostrar o refutar la hipótesis del continuo.

Tres o cuatro años antes, Cantor le había enviado una demostración del principio de buena ordenación, pero Hilbert no debió de considerar la prueba concluyente, porque al comentar la hipótesis del continuo señaló que, probablemente, el primer paso necesario para demostrarla sería probar que la recta real puede ser bien ordenada.

Felix Bernstein tenía ya 22 años y había marchado a Gotinga para doctorarse bajo la dirección de Hilbert. En **1901** leyó su tesis con el título de *Investigaciones en teoría de conjuntos,* en la que da por conocido un hecho que sólo había sido esbozado por Cantor en sus *Contribuciones,* donde sólo había mencionado explícitamente los cardinales $\aleph_0$ y $\aleph_1$. Bernstein usa que, para cada ordinal α, es posible definir un cardinal $\aleph_\alpha$, cosa que ciertamente era fácil de probar generalizando ligeramente los resultados demostrados por Cantor. Esto daba una sucesión transfinita bien ordenada de cardinales:

$$0,\quad 1,\quad 2,\quad \ldots\quad \aleph_0,\quad \aleph_1,\quad \aleph_2,\quad \ldots\quad \aleph_\omega,\quad \aleph_{\omega+1},\quad \aleph_{\omega+2},\quad \ldots\quad \aleph_{\omega\cdot 2},\quad \aleph_{\omega\cdot 2+1},\quad \ldots$$

donde conviene recordar que "transfinita" indica que supera cualquier intento de darla por terminada. Por ejemplo, por encima de los cardinales

$$\aleph_\omega,\qquad \aleph_{\omega\cdot 2},\qquad \aleph_{\omega\cdot 3},\qquad \ldots$$

venía el cardinal $\aleph_{\omega^2}$, y por encima de los cardinales

$$\aleph_\omega,\qquad \aleph_{\omega^2},\qquad \aleph_{\omega^3},\qquad \ldots$$

venía $\aleph_{\omega^\omega}$, etc.

Por ejemplo, $\aleph_{\alpha+1}$ podía definirse como el cardinal del conjunto de ordinales posibles para conjuntos de cardinal $\aleph_\alpha$, mientras que, para ordinales límite λ (que recordemos que son los que no tienen un anterior inmediato) $\aleph_\lambda$ podía definirse como el cardinal de la unión de un conjunto de cardinal $\aleph_\delta$ para cada $\delta < \lambda$.

No obstante, no podía afirmarse que los álefs fueran todos los cardinales infinitos a menos que se aceptara el principio de buena ordenación, del que seguía sin conocerse una demostración. En principio, no se podía asegurar siquiera que el cardinal del continuo, que Bernstein designaba con la letra $\mathfrak{c}$, fuera uno de los álefs. Para ser más precisos, los álefs eran los cardinales de los conjuntos infinitos que admiten un buen orden. Y nadie había demostrado que la recta real, o el conjunto de los subconjuntos del conjunto de los números naturales, cuyo cardinal también es $\mathfrak{c}$, pudiera ser bien ordenado.

Bernstein también afirma lo siguiente:

Lema 1. *Si n es un número natural, entonces $\aleph^n = \aleph$, para cada álef.*

La demostración del teorema, que conozco por una comunicación oral de G. Cantor, se realiza de la misma manera que en el caso más simple $\aleph = \aleph_0$, convirtiendo una serie doble en una serie simple.

Así pues, Cantor conocía una demostración de que $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$. De aquí, usando propiedades elementales de la aritmética cardinal, se sigue que

$$\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \max\{\aleph_\alpha, \aleph_\beta\}.$$

En efecto, si, por ejemplo, $\alpha \leq \beta$, tenemos que

$$\aleph_\beta \leq \aleph_\alpha + \aleph_\beta \leq \aleph_\beta + \aleph_\beta = 2 \cdot \aleph_\beta \leq \aleph_\alpha \cdot \aleph_\beta \leq \aleph_\beta \cdot \aleph_\beta = \aleph_\beta.$$

Igualmente se prueba que $n + \aleph_\alpha = n \cdot \aleph_\alpha = \aleph_\alpha$, para todo cardinal finito $n > 0$.

El hecho de que $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$ no es trivial. Es posible que Cantor no publicara estos hechos porque dudara de su corrección a causa de las paradojas que había encontrado. Probablemente, Bernstein vio a Cantor demostrarlo, pero luego no logró reconstruir la demostración y por ello no la incluyó en su tesis.

18 La paradoja de Russell Las paradojas de la teoría de conjuntos seguían sin encontrar una explicación o una resolución. En **1901** el filósofo Bertrand Russell trató de explicar la paradoja de Cantor. Puesto que era imposible que el conjunto V de todos los conjuntos tuviera mayor cardinal que el conjunto $\mathcal{P}V$, dado que se trata de un subconjunto de V, Russell concluyó que la prueba del teorema de Cantor, que presuntamente lo demostraba, debía de tener un error, y para encontrarlo, la particularizó al caso concreto del conjunto V que daba lugar a la paradoja.

Según el teorema de Cantor, es imposible emparejar (con o sin repeticiones) cada elemento x de V (es decir, cada conjunto) con un elemento A_x de $\mathcal{P}V$ (es decir, con un subconjunto de V, con un conjunto de conjuntos) de modo que no quede ningún elemento de $\mathcal{P}V$ sin pareja. Ahora bien, es fácil construir un emparejamiento así: Si el conjunto x está formado únicamente por conjuntos, definimos $A_x = x$, y en caso contrario definimos $A_x = V$, por poner algo. Es claro entonces que todo elemento x de $\mathcal{P}V$ tiene una pareja, a saber, él mismo, pues se cumplirá $A_x = x$. Veamos ahora en qué falla el argumento que pretende probar que esto —que ciertamente es posible— es imposible.

La prueba del teorema de Cantor nos lleva a considerar el conjunto que llamábamos C, pero que aquí vamos a llamar R, formado por todos los conjuntos x tales que x no es un elemento de A_x. Esto no puede pasar cuando $A_x = V$, pues entonces, ciertamente x es un elemento de V. Sucede cuando x es un conjunto formado exclusivamente por conjuntos, pero x no es un elemento de $A_x = x$. En resumen:

> Llamamos R al conjunto de todos los conjuntos (cuyos elementos son conjuntos) y que no son elementos de sí mismos.

Ahora bien, así R es entonces un conjunto formado por conjuntos, y cabe preguntarse si es o no un elemento de sí mismo. Pero si suponemos que lo es, por definición de R no tendría que serlo, y si no lo es, por definición de R tendría que serlo, luego tenemos una contradicción en cualquier caso.

En lugar de encontrar un fallo en la demostración del teorema de Cantor, lo que obtuvo Russell fue una paradoja mucho más elemental, en cuanto que no depende para nada de la teoría de conjuntos cantoriana, sino meramente de la pura y simple noción de "conjunto". En efecto, una vez encontrada la idea, podemos exponer la que ahora se conoce como *paradoja de Russell* de forma más directa, sin referencias al teorema de Cantor:

1. Partimos del concepto de "conjunto", entendiendo que un conjunto es cualquier colección de objetos, sin perjuicio de que tales objetos sean también conjuntos. Así, por ejemplo, podemos considerar el conjunto $\mathcal{F}$ formado por todos los conjuntos finitos, y también el conjunto $\mathcal{I}$ formado por todos los conjuntos infinitos.

2. Es fácil ver que hay infinitos conjuntos finitos, y también infinitos conjuntos infinitos (basta pensar, por ejemplo, en subconjuntos del conjunto de los números naturales). Esto se traduce en que el conjunto $\mathcal{F}$ de todos los conjuntos finitos es un conjunto infinito, luego no es un elemento de sí mismo, mientras que el conjunto $\mathcal{I}$ de todos los conjuntos infinitos es un conjunto infinito, luego es uno de sus propios elementos.

3. Vemos, pues, que es igualmente posible que un conjunto sea un elemento de sí mismo (como $\mathcal{I}$ o V) o que no lo sea (como $\mathcal{F}$). Y, dado que existen tanto conjuntos que son elementos de sí mismos como conjuntos que no son elementos de sí mismos, tiene sentido considerar el conjunto de Russell R formado exclusivamente por los segundos, es decir, que podemos considerar el conjunto R de todos los conjuntos que no son elementos de sí mismos.

4. Pero entonces cabe preguntarse si R es o no un elemento de sí mismo, y sucede que ninguna de las dos opciones es posible: si R es un elemento de sí mismo, por definición de R eso significa que R no debería ser un elemento de sí mismo, pero si R no es un elemento de sí mismo, por definición de R eso significa que R debería ser un elemento de sí mismo.

5. Así pues, tenemos una contradicción que no procede de suponer nada en absoluto. Simplemente hemos considerado cierto conjunto que tiene pleno sentido considerar... salvo por el hecho de que —inexplicablemente— lleva a una contradicción.

En **1902** Russell recordó que Frege le había enviado hacía un tiempo un manuscrito titulado *Leyes básicas de la aritmética,* en el que pretendía deducir la aritmética a partir de la lógica pura, según su programa de detallar minuciosamente de antemano todos los axiomas y reglas de razonamiento empleados. Pero era tan técnica o más que su *Conceptografía,* por lo que el manuscrito llevaba año y medio abandonado en un cajón.

El trabajo de Frege no era una teoría de conjuntos propiamente dicha, no permitía demostrar en ella los resultados generales de la teoría de conjuntos cantoriana, pero indirectamente hablaba de conjuntos, y Russell, al acordarse del manuscrito, se planteó estudiar cómo evitaba el puntilloso Frege la paradoja que él —Russell— había descubierto, pero se encontró con que no la evitaba. Las leyes lógicas propuestas por Frege daban por válida una variante de la paradoja adaptada al contexto. El resultado era que toda la teoría de Frege era inútil: en ella se podía demostrar igual que $2 + 2 = 4$ o que $2 + 2 = 7$. Y no se veía arreglo posible. La conclusión era que la paradoja de Russell, que podía verse como la forma más pura de las contradicciones de la teoría de conjuntos cantoriana, aquejaba incluso a las teorías lógicas más meditadas y elaboradas, por lo que el problema de diseñar una lógica matemática, unas leyes de razonamiento matemático, que no acabara siendo contradictoria por permitir una variante de la paradoja de Russell no era un problema trivial en absoluto.

Russell informó a Frege del problema de su tratado cuando éste estaba ya en la imprenta. Frege había sido muy crítico con la forma vaga en que Cantor exponía sus teorías, aunque no era de los que despreciaban la teoría de conjuntos, al contrario, consideraba que podrían presentarse con el rigor debido y entonces serían una teoría matemática valiosa. Cuando tuvo noticia de las contradicciones de la teoría de conjuntos no se sorprendió, y lo atribuyó a que, con la falta de rigor de Cantor, no era extraño que se hubiera colado alguna demostración incorrecta en su teoría, pero cuando se encontró con la paradoja de Russell y comprobó que todos sus esfuerzos por corregir su teoría resultaban inútiles, terminó aceptando que sus ideas para fundamentar la matemática no servían y que los matemáticos tendrían que encontrar otro camino.

Las paradojas hicieron que algunos matemáticos empezaran a mirar con más interés las investigaciones sobre lógica. Ese año de **1902** murió Schröder, dejando incompleta la publicación de los tres volúmenes de sus *Lecciones sobre el álgebra de la lógica,* que sólo se completaría tres años después y que durante un tiempo sería la referencia por excelencia para la lógica matemática.

Mientras tanto, Peano llevaba ya ocho años elaborando un *Formulario de matemáticas* que presentaba resultados matemáticos propios de la enseñanza secundaria y universitaria en un lenguaje simbólico que pretendía ser una *pasigrafía*[17] *matemática,* es decir, un lenguaje matemático a través de conceptos, que pudiera ser entendido por cualquiera, sin necesidad de dominar ninguna lengua natural en particular. Cada nueva edición no era una continuación de la anterior, sino una reelaboración con nuevos contenidos.

Peano consideraba que lo que necesitaban sus alumnos para asimilar correctamente las matemáticas eran enunciados completamente precisos, y con ello logró que sus alumnos lo tuvieran por el peor profesor universitario de la época, porque en lugar de explicar la materia, la encriptaba. Por ejemplo, he aquí uno de sus enunciados:[18]

$$u \in \mathrm{Cls}.f, g \in qFu.x \in u \cap \delta u.Dfx, Dgx \in q.\supset.D[(fx + gx)[x, u]x = Dfx + Dgx$$

Sin embargo, Russell había conocido a Peano en el Congreso de Matemáticos de París, en 1900, donde éste le había obsequiado con un ejemplar de su *Formulario,* y el filósofo quedó muy positivamente impresionado.

19 La medida de Lebesgue En **1902** leyó su tesis doctoral Henri Léon Lebesgue. Se titulaba *Integral, longitud, área,* y había sido realizada bajo la dirección de Borel. En ella se plantea en estos términos lo que llama "el problema de la medida":

[17] El término "pasigrafía" (escritura para todos) fue acuñado en 1797 por Joseph de Maimieux, y desde entonces se llamaba así a cualquier intento de establecer un lenguaje internacional, comprensible por todos. Los matemáticos han usado desde hace mucho tiempo un lenguaje pasigráfico parcial, en el sentido de que cualquiera entiende el significado de $2 + 2 = 4$ o $|x - 2| < 10$ aunque estas fórmulas aparezcan en un texto escrito en una lengua desconocida, pero rara vez es posible entender un texto matemático sin dominar la lengua en la que está escrito. Peano aspiraba a presentar las matemáticas de modo que el significado de todo el texto pudiera ser reconocido universalmente, como se reconoce el significado de la notación matemática usual.

[18] Como el lector habrá adivinado, se trata del teorema que afirma que la derivada de la suma de dos funciones es la suma de sus derivadas.

Proponemos asignar a cada conjunto acotado un número positivo o cero, al que llamaremos su medida, que cumpla las siguientes condiciones:

1. *Existen conjuntos cuyo número no es cero.*
2. *Dos conjuntos iguales* [congruentes en el sentido geométrico] *tienen la misma medida.*
3. *La medida de la suma de un número finito o de una cantidad infinita numerable de conjuntos sin puntos comunes dos a dos es la suma de las medidas de estos conjuntos.*

Sólo resolveremos este problema de medida para conjuntos que llamaremos medibles. Este problema, además, admite diferentes soluciones según nos limitemos a conjuntos cuyos puntos están todos en una línea recta, o a aquellos cuyos puntos están todos en un plano, etc. Para distinguir, diremos, cuando sea necesario: medida lineal, medida de superficie, etc.

Lebesgue razona en primer lugar con subconjuntos acotados de la recta y luego considera subconjuntos del plano, indicando que el caso n-dimensional es análogo. Por simplicidad consideramos aquí únicamente el caso unidimensional.

Lebesgue toma un conjunto acotado E en la recta real, y considera familias numerables $\{I_n\}_{n=0}^{\infty}$ de intervalos cuya unión contenga a E. A su vez, considera las sumas $S = \sum_{i=0}^{\infty} l(I_n)$, donde $l(I_n)$ es la longitud del intervalo (la diferencia entre sus extremos). Cualquier definición razonable de medida de E debe cumplir $m(E) \leq S$, para cualquiera de estas sumas, por lo que Lebesgue llama *medida exterior* $m_e(E)$ del conjunto E al ínfimo de las sumas S.

La diferencia con el contenido exterior de Jordan es que éste sólo admite uniones finitas de intervalos, y Lebesgue admite uniones numerables. Como las sumas que considera Jordan son parte de las que considera Lebesgue, es fácil ver que $m_e(E) \leq c_e(E)$.

Para definir la medida interior Lebesgue toma un intervalo I que contenga a E y razona que cualquier medida razonable de E debe cumplir que $m(E) = l(I) - m(I - E) \geq l(I) - m_e(I - E)$, por lo que define $m_i(E) = l(I) - m_e(I - E)$. Así resulta que

$$c_i(E) \leq m_i(E) \leq m_e(E) \leq c_e(E).$$

Entonces, Lebesgue llama conjuntos medibles a los que cumplen $m_i(E) = m_e(E)$, y en tal caso define su medida $m(E)$ como este valor común.

Las desigualdades precedentes muestran que todo conjunto medible Jordan es medible Lebesgue, y que en tal caso las medidas coinciden. Pero Lebesgue demuestra que sus conjuntos medibles tienen estas propiedades:

1. Los conjuntos abiertos y cerrados son medibles.
2. La diferencia de conjuntos medibles es medible.
3. La unión numerable de conjuntos medibles es medible. Si además son disjuntos dos a dos, la medida de la unión es la suma de las medidas.
4. La intersección numerable de conjuntos medibles es medible.
5. Todo subconjunto de un conjunto medible de medida nula es medible y de medida nula.

En particular esto implica que todos los conjuntos medibles Borel son medibles Lebesgue. Con el tiempo se extendió la costumbre de llamar *medidas* a las asignaciones de números reales no negativos a conjuntos de modo que se cumplieran las propiedades 2 y 3 anteriores (que a su vez implican la 4). Esto hacía que la medida de Jordan ya no fuera una medida, por lo que pasó a ser habitual referirse a ella como "contenido de Jordan".

Las medidas que cumplen la quinta propiedad se llaman *completas.* Sucede que la medida de Borel no es completa, y lo único que hace la medida de Lesbesgue es completarla. Más concretamente, se puede probar que todo conjunto medible Lebesgue es la unión de un conjunto medible Borel y un conjunto nulo para la medida de Lebesgue.

Otra propiedad importante de la medida de Lebesgue es que la medida (n-dimensional) de un conjunto no se altera al aplicarle un movimiento, e incluso una simetría.

La extensión de la medida de Jordan a la medida de Lebesgue permitía a su vez extender la integral de Riemann a la llamada integral de Lebesgue, mucho más versátil, pues presenta varias propiedades de paso al límite que no son válidas en general para la integral de Riemann.[19] Lebesgue define esta integral en su tesis y luego la aplica al cálculo de longitudes de curvas y áreas de superficies.

Como aplicación de su integral, Lebesgue publicó en **1903** su artículo *Sobre las series trigonométricas,* en el que demuestra que los cerrados numerables son conjuntos de unicidad en el sentido definido en la página 4, lo que mejoraba sustancialmente el resultado que había obtenido Cantor, pues eliminaba la condición que que el conjunto tuviera un derivado n-simo vacío. Lebesgue conjeturó que todos los conjuntos nulos debían de ser conjuntos de unicidad.

20 El axioma de elección En **1903** Russell publicó su paradoja en su libro *Los principios de las matemáticas,* y Hilbert le respondió en una carta que ese ejemplo ya era conocido en Gotinga desde hacía tres o cuatro años, que lo había encontrado el Dr. Zermelo después de que él —Hilbert— le hubiera comunicado unas paradojas similares. Estaba hablando de Ernst Zermelo, que había empezado trabajando en hidrodinámica, pero al que Hilbert había atraído hacia la teoría de conjuntos, y era entonces su principal colaborador en esta área. El año anterior había publicado su primer artículo sobre teoría de conjuntos, titulado *Sobre la adición de números cardinales transfinitos* y en **1904** se hizo famoso al dar lo que Hilbert había considerado como el primer paso para demostrar la hipótesis del continuo: demostrar el principio de buena ordenación:

Teorema de buena ordenación (Zermelo) Todo conjunto puede ser bien ordenado.

Esbozo de la demostración:[20] Dado un conjunto M:

> *Imaginemos que a cada subconjunto* [no vacío] M *se le asocia un elemento arbitrario* m_1 *que se halla en el propio* M*; llamemos a* m_1 *el elemento "distinguido" de* M*.*

Llamamos γ-*conjunto* a cualquier subconjunto A de M tal que exista un buen orden $\leq$ en A con la propiedad de que, para todo elemento a de A, si A_a es la sección inicial que determina (el conjunto de todos los elementos de A menores que a), entonces a es precisamente el elemento distinguido de $M \setminus A_a$.

La idea subyacente es que si A es un γ-conjunto, la relación de orden que cumple la definición es única. En efecto, si a_0 es su mínimo elemento, entonces A_{a_0} es el conjunto vacío, luego a_0 tiene que ser necesariamente el elemento distinguido del conjunto M. Si A tiene un segundo elemento a_1, entonces $A_{a_1} = \{a_0\}$, luego a_1 tiene que ser necesariamente el elemento distinguido de $M \setminus \{a_0\}$, etc.

En particular, es inmediato que existen γ-conjuntos (si a_0 es el elemento distinguido de M, sucede que $\{a_0\}$ es un γ-conjunto).

Si A y B son γ-conjuntos y existe un elemento b que está en B, pero no en A, tomando el mínimo b que cumple esto, no es difícil probar[21] que $A = B_b$ y que la relación de orden en A coincide con la de B. En particular, dos γ-conjuntos están uno contenido en el otro.

Esto hace que, si llamamos γ-elementos a los elementos de los γ-conjuntos, el conjunto M_0 de todos los γ-elementos es un γ-conjunto (dados dos elementos a, b en M_0, ambos tienen que estar contenidos en el mismo γ-conjunto A, y definimos $a \leq b$ si cumplen esto en A, y así obtenemos un buen orden en M_0 que cumple lo requerido).

Pero M_0 tiene que ser necesariamente igual a M, porque en caso contrario, podríamos considerar el elemento distinguido a de $M \setminus M_0$, y al añadir a a M_0 como máximo elemento, obtendríamos un γ-conjunto, pero entonces a sería un γ-elemento y debería estar en M_0, cuando no lo está.

Por lo tanto, M es un γ-conjunto y, por consiguiente, admite un buen orden. ∎

Zermelo concluye su trabajo con esta observación:

[19] Por ejemplo, en 1881 Vito Volterra, en un trabajo titulado *Sobre los principios del cálculo integral* construyó una función derivable en un intervalo cuya derivada está acotada, pero no es integrable Riemann. En cambio, si la derivada de una función está acotada, es integrable Lebesgue, y $\int_a^b f'(x)\,dx = f(b) - f(a)$.

[20] Esbozamos la demostración de Zermelo porque las demostraciones que suelen venir en los libros usan el axioma del reemplazo, que era desconocido para Zermelo.

[21] Por ejemplo, se puede probar que, para cada $a \in A$, se cumple que $A_a \subset B_b$ y que la relación de orden en A_a es la misma que la de B. Si no fuera cierto, el mínimo a que lo incumple lleva a una contradicción.

La presente demostración se basa en la suposición de que [...]*, incluso para una totalidad infinita de conjuntos, siempre existen aplicaciones que asocian con cada conjunto uno de sus elementos, o, expresado formalmente, que el producto de una totalidad infinita de conjuntos, cada uno con al menos un elemento, es distinto de cero. Este principio lógico no puede, sin duda, simplificarse, pero se aplica sin vacilación en todas partes de la deducción matemática. Por ejemplo, la validez de la proposición de que el número de partes en que se descompone un conjunto es menor o igual que el número de todos sus elementos no puede demostrarse excepto asociando con cada una de las partes en cuestión uno de sus elementos.*

Tal "principio lógico", que recibió el nombre de *Principio de elección,* fue cuestionado por algunos matemáticos. Aparte de las objeciones filosóficas, ese mismo año de **1904**, en el *Tercer Congreso Internacional de Matemáticos,* celebrado en Heidelberg, el húngaro Gyula Kőnig presentó una demostración de que el conjunto de los números reales no podía ser bien ordenado. Su demostración era como sigue:

Si la recta real puede ser bien ordenada, entonces su cardinal es un álef, digamos que $2^{\aleph_0} = \aleph_\alpha$. Kőnig demostraba entonces que, para cualquier ordinal α, se cumple la desigualdad $\aleph_{\alpha+\omega} < \aleph_{\alpha+\omega}^{\aleph_0}$, y luego combinaba este hecho con un resultado de la tesis de Bernstein:

$$\aleph_\alpha^{\aleph_0} = \aleph_\alpha\, 2^{\aleph_0}.$$

Aplicando esto a $\aleph_{\alpha+\omega}$, se obtiene

$$\aleph_{\alpha+\omega}^{\aleph_0} = \aleph_{\alpha+\omega} 2^{\aleph_0} = \aleph_{\alpha+\omega}\aleph_\alpha = \aleph_{\alpha+\omega},$$

con lo que tenemos una contradicción. Esto dio mucho que hablar, y ese mismo año Felix Hausdorff publicó un artículo titulado *El concepto de potencia en la teoría de conjuntos* en el que demostraba una fórmula parecida a la de Bernstein:

$$\aleph_{\alpha+1}^{\aleph_\beta} = \aleph_{\alpha+1}\aleph_\alpha^{\aleph_\beta}$$

a la vez que cuestionaba la validez de la de Bernstein. Pronto se concluyó que "Bernstein era el culpable". Su fórmula estaba mal, mientras que la desigualdad que había demostrado Kőnig era correcta y muy valiosa, pero sin la "ayuda" de Bernstein no probaba que la recta real no pudiera ordenarse bien. Bernstein se defendió señalando que sólo había usado su fórmula para α finito, en cuyo caso era cierta (y se deducía, de hecho, de la fórmula de Hausdorff).

En realidad Kőnig había demostrado un resultado más general, que a su vez, con esencialmente la misma demostración, se generaliza a lo que hoy se conoce como:

Teorema de Kőnig (1) Si $\{\kappa_i\}_{i\in I}$ y $\{\mu_i\}_{i\in I}$ son dos familias de cardinales no nulos tales que $\kappa_i < \mu_i$ para todo i, entonces

$$\sum_{i\in I} \kappa_i < \prod_{i\in I} \mu_i.$$

El interés de esta fórmula es que es esencialmente la única desigualdad estricta que puede demostrarse para la aritmética de los cardinales infinitos, en el sentido de que cualquier otra es un caso particular de ésta. Por ejemplo, el teorema de cantor $\kappa < 2^\kappa$ se obtiene tomando com I un conjunto de cardinal κ y los cardinales $\kappa_i = 1$, $\mu_i = 2$.

Mientras tanto, Russell y el que había sido su director de tesis, Alfred North Whitehead, estaban redactando una fundamentación de las matemáticas a partir de la lógica, similar, en cuanto a su propósito, al intento de Frege, que más adelante publicarían con el título de *Principia Mathematica.* Ese mismo año descubrieron independientemente el principio de Zermelo, al que llamaron *axioma multiplicativo,* porque puede expresarse diciendo que si $\{X_i\}_{i\in I}$ es una familia de conjuntos no vacíos, entonces el producto cartesiano $\prod_{i\in I} X_i$ no es vacío. En palabras de Russell:

En cuanto al axioma multiplicativo, lo descubrí, como si dijéramos, por casualidad. Whitehead y yo solíamos hacer alternativamente recensiones de las distintas partes del libro, corrigiendo cada uno la última recensión hecha por el otro. Al repasar su recensión, que contenía una demostración del axioma, descubrí que la proposición anterior, usada en la demostración, suponía subrepticiamente el axioma. Esto ocurrió en el verano de **1904**. *Al principio pensé que se podría encontrar fácilmente una demostración correcta, pero poco a poco me fui convenciendo de que, si existía una demostración, debía de estar bien escondida.*

En general, el axioma multiplicativo postulaba la existencia de un conjunto sin dar ningún criterio que determine cuáles son sus elementos. Si incluso definiendo conjuntos que parecen perfectamente definidos, como el "conjunto de todos los conjuntos", llegamos a contradicciones, ¿no será peligroso admitir la existencia de conjuntos de los que ni siquiera podemos especificar cuáles son sus elementos? Años más tarde, Russell explicaría la situación con esta analogía:

> *Si tenemos infinitas cajas de zapatos, siempre podemos definir el conjunto formado, por ejemplo, por el zapato derecho de cada una de ellas, pero si en cada caja hay un par de calcetines, ¿cómo seleccionamos un conjunto que tenga un calcetín de cada caja?*

Si hubiera un número finito de cajas, siempre podría decir: "elijo éste, y éste, y éste, y éste", pero si hay infinitas, no podemos estar diciendo "éste mismo" infinitas veces.

A finales de año, a petición de Hilbert, Borel publicaba una nota con su opinión sobre la demostración de Zermelo, en la que explicaba que el principio de elección no le parecía aceptable. Su conclusión era:

> *Un argumento en el que uno supone una elección arbitraria que ha de hacerse una cantidad infinita no numerable de veces se sale del dominio de las matemáticas.*

En cambio, Hadamard respondió a Borel argumentando que Zermelo había reducido una serie de elecciones sucesivas —las que en principio harían falta para ir disponiendo los elementos de un conjunto uno tras otro en un buen orden— a infinitas elecciones simultáneas (mediante una única aplicación del principio de elección), y que, para el caso de elecciones simultáneas, era irrelevante si eran una cantidad numerable o no numerable. Además, una cosa era afirmar la existencia de un conjunto y otra distinta afirmar que ese conjunto puede definirse en la práctica. No hay nada sospechoso en que exista un conjunto con una característica y no tengamos forma de especificar unívocamente uno en concreto.

En **1904** un seguidor de Russell, Philip Jourdain (de 24 años),[22] publicó la primera demostración de que $\aleph_1 \cdot \aleph_1 = \aleph_1$ y decía que el argumento valía en general para cualquier áleph. Pero en realidad su planteamiento era muy vago y nada concluyente.

En **1905** un misterioso A.E. Harward (al parecer un funcionario británico destinado en Calcuta), también seguidor de Russell, publicó un artículo titulado *Sobre los números transfinitos* en el que criticaba la demostración de Jourdain y daba otra que sí que era concluyente (que fue, pues, la primera demostración correcta publicada). Zermelo también cuestionó la prueba de Jourdain.

En **1905** Zermelo ganó una cátedra en Gotinga, mientras los debates sobre si su demostración del principio de buena ordenación era aceptable se extendían entre los matemáticos de todo el mundo. Por ejemplo, ese año Bernstein dio un ejemplo de conjunto que no podía ser bien ordenado, pero su "conjunto" era el conjunto de todos los subconjuntos del conjunto de todos los ordinales, por lo que su argumento no era sino una variante de la antinomia de Burali-Forti, que ponía de manifiesto que las "multiplicidades inconsistentes" podían enturbiar en cualquier momento una discusión matemática.

21 La teoría descriptiva de conjuntos En **1905** Lebesgue publicó su trabajo *Sobre las funciones representables analíticamente,* donde un estudio sobre las funciones de Baire lo llevó a una descripción detallada de los conjuntos de Borel. En principio con notación moderna,[23] Lebesgue definía los subconjuntos de la recta real de clase $\mathbf{\Sigma}^0_\alpha$ como los conjuntos de la forma $f^{-1}\big[\,\big]u, v\big[\,\big]$, donde $f : [a, b] \longrightarrow \mathbb{R}$ es una función de clase de Baire $\alpha < \omega_1$, y los conjuntos de clase $\mathbf{\Pi}^0_\alpha$ como los conjuntos de la forma $f^{-1}\big[\,[u, v]\,\big]$, donde f es igualmente una función de clase α, pero acababa demostrando que estos conjuntos pueden construirse sin hacer referencia para nada a las funciones de Baire:

- La clase $\mathbf{\Sigma}^0_1$ constaba de los subconjuntos abiertos.
- La clase $\mathbf{\Pi}^0_1$ de sus complementarios, los conjuntos cerrados.
- La clase $\mathbf{\Sigma}^0_2$ estaba formada por las uniones numerables de cerrados.
- La clase $\mathbf{\Pi}^2_2$ estaba formada por sus complementarios, que son las intersecciones numerables de abiertos.

[22] Jourdain es famoso por su *paradoja de la tarjeta,* que consiste en escribir en las dos caras de una tarjeta las frases *La frase del otro lado es verdadera.* y *La frase del otro lado es falsa.*

[23] Lebesgue los llamaba conjuntos O o F de clase α, donde la "o" era de *ouvert* (abierto) y la "f" era de "fermée" (cerrado).

En general, si α es un ordinal numerable, las clases $\mathbf{\Sigma}^0_\alpha$ y $\mathbf{\Pi}^0_\alpha$ se definían como las formadas por las uniones e intersecciones numerables (respectivamente) de conjuntos de las clases precedentes $\mathbf{\Pi}^0_\beta$ y $\mathbf{\Sigma}^0_\beta$ (respectivamente), con $\beta < \alpha$, y el resultado es que la clase $\mathcal{B}$ de los conjuntos de Borel podía obtenerse como

$$\mathcal{B} = \bigcup_{\alpha<\omega_1} \mathbf{\Sigma}^0_\alpha = \bigcup_{\alpha<\omega_1} \mathbf{\Pi}^0_\alpha.$$

Esto puede tomarse por una definición alternativa por recursión transfinita de la clase de los conjuntos de Borel: se definen las clases $\mathbf{\Sigma}^0_0$ y $\mathbf{\Pi}^0_0$ y supuestas definidas las clases $\mathbf{\Sigma}^0_\beta$ y $\mathbf{\Pi}^0_\beta$ para todo $\beta < \alpha$, se definen a partir de ellas $\mathbf{\Sigma}^0_\alpha$ y $\mathbf{\Pi}^0_\alpha$.

Así Lebesgue había mostrado una forma precisa de construir los conjuntos que Borel había introducido de una forma "un tanto vaga". Además, si llamamos $\mathbf{\Delta}^0_\alpha = \mathbf{\Sigma}^0_\alpha \cap \mathbf{\Pi}^0_\alpha$, estas clases están ordenadas como sigue:

$$\begin{array}{ccccccccccc}
 & & \mathbf{\Sigma}^0_1 & & & & \mathbf{\Sigma}^0_2 & & & & \mathbf{\Sigma}^0_3 & & \cdots \\
 & \nearrow & & \nwarrow & & \nearrow & & \nwarrow & & \nearrow & & \nwarrow & \\
\mathbf{\Delta}^0_1 & & & & \mathbf{\Delta}^0_2 & & & & \mathbf{\Delta}^0_3 & & & & \mathbf{\Delta}^0_4 \\
 & \nwarrow & & \nearrow & & \nwarrow & & \nearrow & & \nwarrow & & \nearrow & \\
 & & \mathbf{\Pi}^0_1 & & & & \mathbf{\Pi}^0_2 & & & & \mathbf{\Pi}^0_3 & & \cdots
\end{array}$$

Lebesgue demostró que las funciones de Baire no eran sino las funciones medibles Borel, es decir, con notación moderna, las funciones $f : [a, b] \longrightarrow \mathbb{R}$ tales que si $u < v$, entonces $f^{-1}\big]u, v\big[$ es un conjunto de Borel. Su artículo terminaba mostrando que existen conjuntos medibles Lebesgue que no son de Borel, y planteando la pregunta de si existen conjuntos que no sean medibles Lebesgue:

> *Así pues, sabemos nombrar un conjunto medible que no es un conjunto de Borel. Pero la pregunta mucho más interesante: ¿podemos nombrar un conjunto no medible? permanece sin respuesta.*

Aquí "nombrar" tiene un sentido más preciso que "demostrar que existe". Por ejemplo, el año anterior Giuseppe Vitali había publicado *Sobre los conjuntos de puntos,* donde construía la medida de Lebesgue sin conocer el trabajo de éste,[24] y en **1905**, en *Sobre el problema de la medida de los conjuntos de puntos de una recta,* demostró la existencia de un conjunto no medible Lebesgue, pero su prueba usaba de forma esencial el principio de elección de Zermelo. Y eso no encajaba para nada en lo que Lebesgue entendía por "nombrar" un conjunto (es decir, definirlo, construirlo, explicitar cuáles son sus elementos). Para Lebesgue, la cuestión seguía abierta.

La descripción de los conjuntos de Borel como los obtenidos en la jerarquía de las funciones $\mathbf{\Sigma}^0_\alpha$ y $\mathbf{\Pi}^0_\alpha$ se puede considerar como el inicio de la llamada *teoría descriptiva de conjuntos,* es decir, el estudio, no de conjuntos arbitrarios de puntos, sino de conjuntos de puntos que pueden construirse con unos criterios más o menos explícitos que permitan clasificarlos según su complejidad y extraer consecuencias del hecho de que puedan obtenerse de tales construcciones.

22 Poincaré Desde la muerte de Kronecker, la principal oposición a la teoría de conjuntos cantoriana y a los intentos de fundamentar la matemática en la lógica y la teoría de conjuntos se encarnaba en Henri Poincaré (pero en este caso dentro del debate intelectual, sin nada parecido al juego sucio que Kronecker había librado contra Cantor). En **1905** publicó un artículo titulado *Las matemáticas y la lógica,* en el que expresaba sus puntos de vista sobre las posturas de Frege, Russell, Peano o Hilbert.

En primer lugar, en referencia a los *Grundlagen* de Hilbert, Poincaré señala que, aunque Hilbert haya reducido todos los teoremas geométricos a consecuencias que pueden obtenerse formalmente de sus axiomas sin necesidad de saber qué quiere decir "punto", "recta", etc., lo que no es creíble es que se diga que los axiomas se eligen arbitrariamente, sino que hay una razón de fondo que distingue a los axiomas de Hilbert de cualesquiera otros que uno podría haber elegido caprichosamente en su lugar, y es que los axiomas de Hilbert resultan verdaderos cuando se les da la interpretación intuitiva pretendida.

> *Admitamos incluso que se ha demostrado que todos los teoremas pueden deducirse por procedimientos puramente analíticos* [formales] *mediante simples combinaciones lógicas de un número finito de axiomas, y que estos axiomas no son más que convenios. El filósofo conservará el derecho a investigar los orígenes de esos convenios, de ver por qué ésos se han considerado preferibles a los convenios contrarios.*

[24] En **1905** William Henry Young también redescubrió la medida de Lebesgue en su artículo *Sobre la teoría general de la integración.*

Esta objeción no es esencial, porque Hilbert podría responder que con su formalismo simplemente está marcando la línea divisoria entre la matemática y la filosofía de la matemática, sin cuestionar que la segunda tenga sentido y razón de ser. Más relevante es la observación de que, como el propio Hilbert señala, para que unos axiomas sean aceptables es necesario justificar que son consistentes, es decir, que a partir de ellos no es posible demostrar contradicciones. Una forma de probarlo sería encontrar objetos que cumplen los axiomas, pero cuando los matemáticos recurren a axiomas suele ser porque no son capaces de definir los objetos de los que quieren hablar, y entonces la única forma de justificar la consistencia sería analizando las proposiciones que se pueden deducir de los axiomas:

> *Para establecer que los postulados no implican ninguna contradicción, hace falta entonces considerar todas las proposiciones que se pueden deducir de los postulados considerados como premisas y demostrar que, entre esas proposiciones, no hay dos tales que una sea la contraria a la otra. Si se trata de un número finito de proposiciones, una comprobación directa es posible. Este caso es poco frecuente y, por tanto, poco interesante.*
>
> *Si estas proposiciones son infinitas, no es posible esta verificación directa; es necesario recurrir a procedimientos de demostración donde, en general, será necesario recurrir al principio de inducción completa que se trata de verificar.*

Poincaré se refiere a que "los nuevos lógicos" pretenden deducir todas las matemáticas de unos axiomas, pero dichas matemáticas que pretenden justificar incluyen resultados como el principio de inducción, que, no obstante, harían falta para justificar que sus axiomas son aceptables, cayendo así en un círculo vicioso.

A continuación Poincaré considera la pasigrafía de Peano:

> *El elemento esencial de este lenguaje son ciertos signos algebraicos que representan las diferentes conjunciones: si, y, o, entonces. Que estos signos sean cómodos, es posible, pero que estén destinados a renovar toda la filosofía, es otro asunto. Es difícil aceptar que la palabra "si" adquiera una virtud cuando se escribe* ↄ *que no tenía cuando se escribía "si".*
>
> *Esta invención del Sr. Peano se llamó inicialmente pasigrafía, es decir, el arte de escribir un tratado de matemáticas sin usar una sola palabra del lenguaje habitual. Este nombre definía exactamente su alcance, pero desde entonces se ha elevado a una dignidad más eminente, otorgándole el título de logística. Esta palabra se utiliza, al parecer, en la Escuela de Guerra para designar el arte del mariscal de alojamientos,*[25] *el arte de hacer marchar y acantonar a las tropas; pero aquí no hay que temer ninguna confusión y vemos de inmediato que este nuevo nombre implica el propósito de revolucionar la lógica.*

El *logicismo,* también llamado a veces *logística,* lo que da pie al juego de palabras de Poincaré, era la postura que había sostenido Frege y que ahora retomaba Russell que pretendía que los principios de la matemática (incluyendo la aritmética elemental) pueden deducirse y justificarse a partir de los principios de la lógica. Esto se aplicaba en menor medida a Peano, que no aspiraba a deducir nada, sino meramente a plasmar los razonamientos matemáticos de la forma más precisa posible. No obstante, esto lo llevaba a adoptar definiciones con un criterio de Poincaré cuestiona. Para ello toma como ejemplo el uso del lenguaje de Peano el artículo de Burali-Forti en el que encuentra la paradoja que lleva su nombre y que, en efecto, estaba escrito en *peaniano,* como llamaba Poncaré al lenguaje de Peano, no sin cierta sorna:

> *Vemos en primer lugar cómo el Sr. Burali-Forti define el número* 1 *de la forma siguiente:*
>
> $$1 = \overline{\imath}T\text{`}\{\mathrm{Ko} \cap \overline{(u,h)}\,\epsilon\,(u\,\epsilon\,\mathrm{Un})\}$$
>
> *una definición eminentemente apta para ofrecer una idea del número* 1 *a quienes nunca hubieran oído hablar de él.*

Luego se plantea que esta definición es circular, porque en ella aparece el conjunto Un, formado por todos los conjuntos con un elemento. Esto no es exacto, porque Un se puede definir como el conjunto de los conjuntos de la forma $\{x\}$, sin recurrir al número 1, pero más adelante pone ejemplos de mayor calado cuando, citando un artículo de Louis Couturat de 1904, en el que discute *Los principios de las matemáticas,* de Russell, dice:

[25] El *maréchal des logis* era el sargento de caballería encargado de la logística.

> *El Sr. Couturat repite a menudo que esta nueva lógica es completamente independiente de la idea de número. No me divertiré contando cuántas veces su exposición contiene adjetivos numerales, tanto cardinales como ordinales, o adjetivos indefinidos, como "varios". Citemos, no obstante, algunos ejemplos:*
>
> *El producto lógico de* dos *o* más *proposiciones es...*
>
> *Todas las proposiciones son susceptibles de tomar únicamente* dos *valores: verdadero y falso.*
>
> *El producto relativo de* dos *relaciones es una relación.*
>
> *Una relación se da entre* dos *términos ..., etc., etc.*
>
> *A veces este inconveniente no será imposible de evitar, pero otras veces es esencial. Una relación no se entiende sin dos términos. Es imposible tener una intuición de la relación sin tener al mismo tiempo la de estos dos términos y sin recalcar que son dos, pues para que la relación sea concebible hace falta que sean dos y sólo dos.*

Finalmente Poincaré cita los cinco axiomas de Peano y cuestiona que se pueda demostrar que son consistentes sin conocer de antemano lo que son los números naturales, por lo que no pueden considerarse como una definición implícita de los números naturales.

En **1906** publicó una segunda parte de este artículo dedicada a rebatir específicamente la ponencia *Sobre los fundamentos de la lógica y la aritmética,* que Hilbert había presentado en el *Tercer Congreso Internacional de Matemáticos,* de 1904, donde se distanciaba del logicismo dándole la razón a Poincaré:

> *Sin embargo, si miramos con atención, constatamos que en los principios lógicos, como se suelen presentar, se encuentran ya implícitas ciertas nociones aritméticas, por ejemplo la noción de conjunto y, en cierta medida, la noción de número. Así, nos encontramos atrapados en un círculo y, por ello, para evitar toda paradoja, me parece necesario desarrollar simultáneamente los principios de la lógica y los de la aritmética.*

Poincaré señala su extrañeza ante el hecho de que Hilbert considere el concepto de "conjunto" como aritmético, pero, en cualquier caso, esto aumenta la lista de conceptos que Hilbert considera que no son reducibles a la lógica, sino que están entretejidos con ella. Poincaré analiza con detalle la exposición de Hilbert y señala que igualmente contiene la clase de peticiones de principio que pretendía evitar.

Luego pasa a rebatir la tesis logicista según la cual la aritmética tradicional no es más que un caso particular de la aritmética de los cardinales infinitos, de modo que ésta puede desarrollarse en general, sin distinguir entre conjuntos finitos e infinitos, para luego probar los resultados que sólo valen específicamente para conjuntos finitos. En contra de esta posición, Poincaré señala que uno de los resultados básicos de la teoría de cardinales infinitos es el teorema de Cantor-Bernstein, reproduce du demostración y destaca que en ella se definen por recurrencia sucesiones de conjuntos, con lo que se están usando propiedades de los números naturales, por lo que la teoría de los cardinales infinitos presupone las propiedades de la aritmética elemental, y no al revés. La conclusión final del artículo es:

> *En resumen: los Sres. Russell y Hilbert han realizado un vigoroso esfuerzo, y han escrito uno y otro un libro lleno de puntos de vista originales, profundos, y a menudo muy ciertos. Estos dos libros nos darán mucho material para pensar, y para aprender de ellos. Algunos de sus resultados, muchos, de hecho, son sustanciales y están destinados a perdurar.*
>
> *Pero decir que han resuelto la controversia entre Kant y Leibniz de manera definitiva y que han destruido la teoría kantiana de las matemáticas es evidentemente falso. No sé si en realidad creen haberlo logrado, pero si es así, se han equivocado.*

La alusión a Kant y a Leibniz se refiere a la controversia entre el racionalismo de Leibtniz, según el cual todo el conocimiento (en particular, el conocimiento matemático) procede de la razón (de la lógica), frente a la postura de Kant, según el cual la razón no puede llegar a nada sin la intuición (en el caso de las matemáticas) y sin la experiencia (en el caso de la física). Poincaré suscribe a Kant y considera que la matemática tiene un contenido intuitivo que es, de hecho, su objeto de estudio, de modo que la lógica sirve para organizar el conocimiento matemático, pero que *los principios fundamentales de la matemática están justificados por la intuición*[26] y es inviable tratar de justificarlos por la lógica.

[26]Entender esta frase requiere una explicación extensa, pero la posponemos hasta más adelante (página 74 y siguientes).

23 El predicativismo En **1906** Couturat y Mario Pieri (un discípulo de Peano) publicaron artículos en respuesta a los de Poincaré, y a su vez Poincaré publicó una tercera (y última) parte de su artículo como réplica.[27] No vamos a entrar en detalles por las mismas razones que Poincaré señala:

> *Sigo pensando que el Sr. Couturat define lo claro mediante lo oscuro y que no se puede decir x e y sin pensar "dos", pero probablemente hay lectores que quieren seguir esta discusión con interés y no quiero someterlos al fastidioso espectáculo de una interminable guerra de guerrillas.*

Nos centramos aquí en la explicación que da Poincaré a las paradojas de la teoría de conjuntos, que consiste en señalar que se basan en definiciones no predicativas, en el sentido que explicamos a continuación:

Hay, en principio, dos formas de concebir los objetos sobre los que tratan los matemáticos: una es la *constructivista,* que considera que unos conceptos se van construyendo a partir de otros construidos previamente a través de definiciones sucesivas. A partir de unos conceptos ya definidos, podemos definir otros "nuevos". Frente a esta postura, está el *platonismo* que considera que los objetos matemáticos son los que son, de modo que cuando definimos uno cualquiera, no lo estamos construyendo, sino que simplemente lo estamos destacando, empezamos a hablar de él, pero ya estaba ahí antes de que nos fijáramos en él.

La diferencia pude parecer muy filosófica y sin consecuencias prácticas, pero no es así. La diferencia práctica aparece fundamentalmente en el uso de la palabra "todos". Para un constructivista, a la hora de definir un nuevo objeto, cabe distinguir entre "todos" los objetos ya construidos y "todos" incluyendo los que se definirán posteriormente, mientras que para un platonista "todos" significa todos, sin distinción posible. En particular, un constructivista puede exigir que cada definición haga referencia únicamente a los objetos ya definidos y no a los pendientes de definir, mientras que esta distinción carece de sentido para un platonista.

Así, por ejemplo, desde un punto de vista constructivista, si tenemos construidos unos conjuntos, podemos definir el conjunto R de todos los conjuntos (previamente construidos) que no son elementos de sí mismos, y con ello obtenemos un "nuevo" conjunto que no da lugar a ninguna contradicción. Se cumple que R no es un elemento de sí mismo, y eso no contradice a la definición de R, porque de ahí no podemos deducir que R sea un elemento de sí mismo. Para ello haría falta que R fuera uno de los conjuntos que ya teníamos construidos antes de definirlo, y no lo es.

En cambio, desde un punto de vista platonista, si tenemos dados "todos" los conjuntos, en principio podemos definir el conjunto R de todos los conjuntos que no son elementos de sí mismos, pero entonces tenemos que admitir que este "nuevo" conjunto no es nuevo, sino que tenía que estar ya entre los conjuntos que hemos usado para definirlo, y eso nos lleva a la paradoja de Russell.

Por lo tanto, lo que nos enseña la paradoja de Russell es que, a partir de unos conjuntos dados, siempre es posible definir conjuntos "nuevos", de modo que, a veces, forzar a que un conjunto que acabamos de definir tenga que estar ya entre los conjuntos previamente conocidos puede llevar a contradicciones.

El mismo análisis vale para la paradoja de Cantor: para un constructivista, dados unos conjuntos ya construidos, podemos considerar el conjunto V formado por todos ellos, pero será un conjunto "nuevo" y no cabe suponer que sea uno de los conjuntos de partida, es decir, V no debería ser un elemento de sí mismo. Sí que será un elemento del conjunto $\mathcal{P}V$, y por eso mismo no cabe afirmar que $\mathcal{P}V$ sea un subconjunto de V (por ejemplo, porque V está en $\mathcal{P}V$ y no en V).

En cambio, si un platonista admite que, a partir de "todos" los conjuntos podemos definir el conjunto V de "todos" los conjuntos de modo que V es uno de sus propios elementos, y que $\mathcal{P}V$ es un subconjunto de V porque todos sus elementos son conjuntos y, por consiguiente, son elementos de V, a partir de ahí ya tenemos todo lo necesario para acabar en la paradoja de Cantor.

Y lo mismo vale para la antinomia de Burali-Forti: para un constructivista, si tenemos unos ordinales dados, podemos considerar el conjunto W formado por todos ellos, que será un conjunto bien ordenado al cual le podemos asociar un ordinal Ω que será un ordinal "nuevo", distinto de todos los ordinales de partida y, de hecho, mayor que todos ellos.

El problema aparece cuando un platonista pretende que los ordinales de partida son "todos" los ordinales y que el nuevo ordinal Ω tiene que ser uno de ellos, y también su siguiente $\Omega+1$. Al suponer que $\Omega+1$ es uno de los ordinales de partida, la maquinaria de la teoría de Cantor nos lleva a que $\Omega+1<\Omega$ y tenemos una contradicción.

[27] Y ese mismo año, Russell publicó como respuesta en la misma revista que Poincaré su artículo *Les paradoxes de la logique.*

En general, Poincaré considera que una definición es *impredicativa*[28] cuando pretende definir un objeto C a partir de una totalidad de objetos de la cual el objeto definido C tendría que ser uno de ellos. En tal caso, la definición contiene un círculo vicioso y no es válida.

Pero esto no debe verse como una refutación del platonismo en favor del constructivismo. Al contrario, uno puede seguir siendo platonista a condición de ser también *predicativista,* es decir, de considerar que las definiciones impredicativas no definen nada, no tienen significado.[29]

Pero Poincaré va más allá y considera que las definiciones impredicativas son circulares y no admisibles *a priori,* tanto si conducen a paradojas como si no. Por ejemplo, dice:

> *Por ejemplo, la definición de álef-uno es impredicativa; el razonamiento por el que Cantor pretende establecer la existencia de dicho número me parece completamente análogo al de Burali-Forti. Por ello no estoy seguro de que exista álef-uno.*

Antes de analizar esta afirmación, es más sencillo considerar el caso de la no numerabilidad de $\mathcal{P}\mathbb{N}$. El razonamiento con el que Cantor demuestra que $\mathcal{P}\mathbb{N}$ no es numerable consiste (con notación moderna) en suponer que tenemos una enumeración $A_0, A_1, A_2, \ldots$ de "todos" los subconjuntos de $\mathbb{N}$ y, a partir de ella, definir un "nuevo" subconjunto C de $\mathbb{N}$ formado por los números n que no son elementos de A_n. Definir un subconjunto C de $\mathbb{N}$ a partir de "todos" los subconjuntos de $\mathbb{N}$ es un ejemplo de definición no predicativa. Podemos concluir que $\mathcal{P}\mathbb{N}$ no es numerable, como hace Cantor, o bien que la definición de C no tiene sentido y no concluir nada o, a lo sumo, que no es posible "terminar de construir" $\mathcal{P}\mathbb{N}$. Cualquier construcción de subconjuntos de $\mathbb{N}$ estará siempre incompleta, en cuanto que siempre se podrá ampliar. La conclusión predicativista no es que $\mathcal{P}N$ no es numerable, sino que no tiene sentido hablar de la totalidad de los subconjuntos de $\mathbb{N}$, a pesar de que, en principio, no tenemos ningún indico de que hablar de ella conduzca a ninguna contradicción.

En cuanto a $\aleph_1$, Cantor considera "todos" los ordinales numerables, que forman un conjunto bien ordenado, por lo que determinan un ordinal "nuevo", al que se le suele llamar ω_1, y que (por las propiedades de los conjuntos bien ordenados) tiene que ser mayor que todos los ordinales de partida.

Si suponemos que ω_1 es numerable, para llegar a una contradicción todavía tenemos que aceptar que ω_1 no sería un "nuevo" ordinal numerable, sino que, al haber partido de la totalidad (absoluta) de ellos, ω_1 sería uno de los dados de antemano, por lo que también sería uno de ellos su siguiente, $\omega_1 + 1$, y entonces llegamos a una contradicción, porque debería ser $\omega_1 + 1 < \omega_1$, en perfecto paralelismo con la desigualdad $\Omega + 1 < \Omega$ a la que llegaba Burali-Forti. La alternativa es considerar que ω_1 es numerable, pero que no es ninguno de los ordinales numerables de partida, lo que presupone a su vez que no existe la totalidad de los ordinales numerables, igual que no existe la totalidad de los subconjuntos de $\mathbb{N}$. En tal caso no existiría $\aleph_1$ (el cardinal del conjunto de los ordinales numerables), como se planteaba Poincaré.[30]

A continuación Poincaré señala que la construcción de Dedekind de los números naturales no es predicativa, pues define $\mathbb{N}$ como la intersección de todos los subconjuntos inductivos de un conjunto dado A, pero el propio $\mathbb{N}$ resulta ser un conjunto inductivo, por lo que tenemos el típico círculo vicioso impredicativo. Naturalmente, con esto Poincaré no pone en cuestión la existencia de los números naturales, sino que tenga sentido definirlos en términos conjuntistas. Poincaré vincula la impredicatividad con suponer que existe el infinito actual:

> *Es la creencia en la existencia del infinito actual lo que da origen a las definiciones impredicativas. Me explico: en estas definiciones aparece la palabra "todos", como hemos visto en los ejemplos citados más arriba. La palabra "todos" tiene un sentido bien claro cuando se aplica a un número finito de objetos. Para que siga teniéndolo cuando los objetos son infinitos, haría falta que hubiera un infinito*

[28] La distinción entre definiciones predicativas o impredicativas la había formulado Russell, en el sentido más obvio de que una definición es impredicativa si resulta contradictoria, por lo que no está hablando de nada en realidad. Fue Poincaré quien asoció la impredicatividad con la clase de circularidad que acabamos de explicar.

[29] En realidad hay un matiz que es relevante si uno pretende desarrollar unas matemáticas predicativas: en principio, basta con que un predicativista admita que las definiciones predicativas tienen sentido y que no acepte *a priori* la validez de las definiciones impredicativas, pero sin excluir la posibilidad de que determinados razonamientos particulares justifiquen que aceptar las definiciones predicativas obliga a aceptar también algunas definiciones impredicativas concretas.

[30] En realidad este caso es más sutil que el anterior, porque, en principio, no hay nada de impredicativo en la definición del ordinal del conjunto de los ordinales numerables, pero si alguien parte del supuesto de que no existen conjuntos no numerables, puede rechazar la definición de ω_1 por impredicativa, porque define un ordinal (numerable) a partir del conjunto de todos los ordinales numerables. Por ello, la demostración de Cantor no tiene por qué convencer a un predicativista, ya que *podría ser* impredicativa, y lo sería precisamente si es falso lo que pretende demostrar. De hecho, si suponemos que no hay conjuntos no numerables, el conjunto de todos los ordinales numerables es el conjunto de todos los ordinales, y estamos exactamente ante la antinomia de Burali-Forti.

> *actual. En caso contrario "todos" los objetos no podrían concebirse como dados anteriormente a la definición, y entonces, si la definición de una noción N depende de "todos" los objetos A, esta puede caer en un círculo vicioso si entre los objetos A los hay que no pueden definirse sin hacer que intervenga la propia noción N.*
>
> *No existe el infinito actual, los cantorianos lo han olvidado y han caído en la contradicción. Es cierto que el cantorismo ha prestado servicios, pero esto ha sucedido cuando ha sido aplicado a un problema verdadero, cuyos términos estaban claramente definidos y por ello podían avanzar sin preocupaciones.*

24 Espacios métricos Los matemáticos franceses estaban abriéndose cada vez más explícitamente a la teoría de conjuntos cantoriana. En **1906** leyó su tesis doctoral un joven de 28 años llamado René Maurice Fréchet. Su director de tesis era Jacques Hadamard, y su tesis se titulaba *Sobre algunos puntos del cálculo funcional.* Su primer capítulo empieza así:

> 4. Propósito del Cálculo Funcional: *Consideremos un conjunto E formado por elementos cualesquiera (números, puntos, funciones, líneas, superficies, etc.), pero tal que podamos discernir los elementos distintos. A cualquier elemento A de este conjunto le hacemos corresponder un número determinado $U(A)$; definimos así lo que llamaremos una operación funcional uniforme en E.*
>
> *El estudio de estas operaciones es el objeto del Cálculo Funcional. Se supone que las propiedades de cada operación dependerán, por un lado, de las propiedades del conjunto en el que se define la operación y, por otro, de la naturaleza de la correspondencia que la define, es decir, de la correspondencia (no unívoca) entre los elementos de E y ciertos números, que son los valores de la operación. Por lo tanto, vemos que el cálculo funcional incluye necesariamente una teoría preliminar sobre los conjuntos.*
>
> 5. Teoría de conjuntos: *Los resultados que obtendremos en dicha teoría serán tanto más amplios cuanto más generales sean los conjuntos que consideremos. Para obtener la mayor generalidad posible, sería conveniente buscar primero resultados aplicables a conjuntos abstractos, es decir, conjuntos cuya naturaleza de elementos no está especificada.*
>
> *Los resultados más importantes obtenidos hasta ahora en este orden de ideas son los relativos a las nociones (introducidas por el Sr. G. Cantor) de potencia de un conjunto y de conjunto ordenado.*
>
> *Para la primera parte de este trabajo sólo supondré conocidos estos resultados (aparte de las nociones matemáticas más elementales), e de entre ellos sólo los más simples. En particular, no utilizaré la teoría de conjuntos lineales y de las funciones continuas, que, por el contrario, aparecerá como un corolario muy particular de nuestra teoría general.*

A continuación Fréchet define lo que llama una "clase (L)", que es un conjunto abstracto en el que hay definida una noción de convergencia de sucesiones que cumple ciertas propiedades básicas, y muestra cómo muchos conceptos definidos en contextos distintos pueden ser definidos a partir de su noción abstracta de límite, como el de conjunto derivado, conjunto cerrado, conjunto compacto (definido como un conjunto en el que todo subconjunto tiene una sucesión convergente), la continuidad de una función, etc. Luego, en el capítulo segundo define lo que llama una "clase (V)", (por *voisinage* (vecindad)):

> *Consideremos una clase (V) de elementos de cualquier naturaleza, pero tal que podemos discernir si dos de ellos son idénticos o no, y tal que, además, a cualesquiera dos de ellos, A, B, les podemos hacer corresponder un número $(A, B) = (B, A) \geq 0$ que posee las dos propiedades siguientes: 1. La condición necesaria y suficiente para que (A, B) sea nulo es que A y B sean idénticos. 2. Existe una función positiva bien determinada $f(\epsilon)$ que tiende a cero con ϵ, tal que las desigualdades $(A, B) \leq \epsilon$, $(B, C) \leq \epsilon$ implican $(A, C) \leq f(\epsilon)$, cualesquiera que sean los elementos A, B, C. En otras palabras, es suficiente que (A, B) y (B, C) sean pequeños para que lo mismo sea cierto de (A, C). Llamaremos al vecindad de A y B al número (A, B).*

Fréchet evita usar la palabra "distancia" porque quiere que su "vecindad" (en el sentido de "medida de la proximidad" se vea como algo abstracto, pero en la introducción ha explicado que el número (A, B) tiene propiedades análogas a las de la distancia entre dos puntos. A partir de ahí muestra que toda clase (V) es una

clase (L), es decir, que cada "distancia abstracta" define una noción de límite,[31] y caracteriza la continuidad de una función definida sobre una clase (V) en términos de la distancia.

Tras demostrar resultados generales sobre espacios (V), la segunda parte de la tesis se dedica a mostrar cómo éstos se aplican a contextos muy diversos (funciones de una y varias variables reales, espacios de funciones continuas, funciones holomorfas, etc.).

Ese mismo año de **1906** Baire publicó la primera parte de *Sobre la representación de las funciones discontinuas,* cuya segunda parte se retrasaría hasta 1909, y en ella se aprecia la influencia decisiva del trabajo de Fréchet. En el primer capítulo de esta segunda parte Baire empieza observando que varios conjuntos de puntos están determinados por sucesiones de números naturales. Por ejemplo, cada punto del conjunto de Cantor está determinado por una sucesión de ceros y doses (los que forman su desarrollo decimal en base 3), pero el ejemplo más importante es el del espacio de los números irracionales:

En 1653, en su *Arithmetica infinitorum,* John Wallis presentó la fórmula

$$\frac{4}{\pi} = 1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{2+\cdots}}}},$$

descubierta por su amigo Lord Brunker, y se refirió al miembro derecho como una *fracción continua.* En 1737, en su artículo *De fractionibus continuis,* Euler demostró que cada número irracional positivo α se expresa de forma única como una fracción continua de la forma

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}},$$

donde los números a_i son números naturales no nulos (salvo a lo sumo a_0, que puede ser 0). El miembro derecho hay que entenderlo como el límite de la sucesión de números racionales $\{\alpha_n\}_{n=0}^{\infty}$ que resulta de cortar la expresión en cualquier punto. Por ejemplo,

$$\alpha_3 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}}.$$

Euler demostró que todas las fracciones continuas de esta forma convergen a números irracionales positivos, con lo que, si fijamos $a_0 = 0$, tenemos una correspondencia biunívoca entre el conjunto $\mathbb{I}$ de los números racionales $0 < \alpha < 1$ y el conjunto $\mathcal{N}^*$ de las sucesiones $(a_1, a_2, \ldots)$ de números naturales no nulos.

Notemos que, si llamamos $\mathcal{N}$ al conjunto de todas las sucesiones de números naturales (posiblemente nulos), a cada sucesión $(a_0, a_1, a_2, \ldots)$ de $\mathcal{N}$ le podemos asignar la sucesión $(a_0 + 1, a_1 + 1, a_2 + 1, \ldots)$ de $\mathcal{N}^*$, la cual a su vez determina la fracción continua de un número de $\mathbb{I}$. Por lo tanto, también tenemos una correspondencia biunívoca entre $\mathcal{N}$ e $\mathbb{I}$.

El caso es que Baire trabajaba con $\mathcal{N}^*$, pero, para que su teoría encaje con las definiciones modernas, conviene enunciar sus resultados en términos de $\mathcal{N}$ en lugar de $\mathcal{N}^*$, lo cual es una modificación trivial. Así pues, salvo por que, como decimos, Baire trabajaba en realidad con $\mathcal{N}^*$, lo que observó Baire fue que era posible definir un concepto de límite en $\mathcal{N}$, en el sentido abstracto de Fréchet, con el cual la correspondencia biunívoca entre $\mathcal{N}$ e $\mathbb{I}$ era bicontinua, es decir, continua con inversa continua (lo que hoy en día se llama un homeomorfismo). Y este concepto de límite en $\mathcal{N}$ es el más simple que se puede concebir:

> Una sucesión $\{a^n\}_{n=0}^{\infty}$ en $\mathcal{N}$ converge a una sucesión a si para cada número natural N existe un n_0 tal que si $n \geq n_0$ entonces, para todo $i < N$, se cumple $a_i^n = a_i$.

Aunque dicho así pueda parecer enrevesado, es muy simple: la convergencia equivale a que, para cualquier N prefijado, a partir de un n suficientemente grande, todos los términos a^n de la sucesión tienen sus N primeros términos iguales a los de a. En otras palabras, a que los términos de la sucesión se parecen cada vez más al límite, donde "parecerse cada vez más" se entiende como que coinciden con los del límite hasta un valor N tan alto como se quiera.

[31] Fréchet señala que en una clase (V) se pueden definir conceptos que no tienen sentido en cases (L) arbitrarias, como la "propiedad de Cauchy" de una sucesión y, de hecho, establece que va a estudiar únicamente lo que llama clases (V) normales, que son lo que hoy en día se llaman espacios métricos completos separables sin puntos aislados.

Baire no se molestó en mostrar que esta noción de límite se deriva de una distancia en el sentido de Fréchet, pero es fácil probar que sirve ésta:

$$d(x,y) = \sum_{n=0}^{\infty} \frac{\text{mín}\{1, |x(n) - y(n)|\}}{2^{n+2}}.$$

El lector puede comprobar que $d(x,y) < \frac{1}{2^N}$ equivale a que $x_i = y_i$ para $i < N$.

Actualmente se llama *espacio de Baire* al espacio $\mathcal{N}$ dotado de esta distancia. Baire lo considera un espacio de dimensión 0, en un sentido no preciso de la palabra dimensión (pero que es precursor del concepto topológico de dimensión):

> *Podemos decir, en resumen, que los conjuntos de sucesiones, tal como los hemos construido, poseen los atributos del continuo, en lo que respecta a la noción de límite, y solamente en lo que respecta a esta noción. La noción de orden relativo, que es fundamental en las cuestiones relativas a los continuos (de* $1, 2, \ldots, n$ *dimensiones), y de donde se derivan en particular las nociones de caminos y de conexión, no existe en los conjuntos de sucesiones.*
>
> *Se nos conduce así a considerar los conjuntos de sucesiones como conjuntos de 0 dimensión; llamaremos espacio de dimensión* 0 *al conjunto fundamental* G_0 $[= \mathcal{N}^*]$ *de todas las sucesiones; cada sucesión será un punto de este espacio.*

Se refiere a que $\mathcal{N}$ es un espacio métrico completo, como lo es $\mathbb{R}$, y en eso se parece "al continuo", pero, por otra parte, no es posible establecer en $\mathcal{N}$ una ordenación de los puntos, ni unos ejes de coordenadas, ni nada que permita hablar de "movimiento continuo" en $\mathcal{N}$. En términos modernos, esto tiene que ver con que las únicas aplicaciones continuas $[0,1] \longrightarrow \mathcal{N}$ son las constantes.

25 Los axiomas de Zermelo En **1908** Zermelo publicó un artículo titulado *Una nueva prueba de la posibilidad de un buen orden,* en la que, como su título indica, presentaba una prueba del principio de buena ordenación y detallaba explícitamente todos los presupuestos en que se basaba. En realidad la nueva demostración, basada en la teoría de cadenas de Dedekind, era más técnica y sofisticada que la anterior (que era lógicamente impecable en términos modernos), pero a la vez más elemental en cuanto a los argumentos que usaba. Luego respondía a las críticas que había recibido su demostración anterior. Respecto a las críticas al principio de elección dice (entre otras cosas):

> *En primer lugar, consideramos las objeciones dirigidas contra el "postulado de elección" formulado anteriormente y que, por lo tanto, atacan ambas pruebas por igual. Admito que están justificadas hasta cierto punto, ya que, como enfaticé expresamente al final de mi nota, no puedo probar este postulado y, por lo tanto, no puedo obligar a nadie a aceptarlo apodícticamente.*
>
> *Por lo tanto, si el Sr. E. Borel y el Sr. G. Peano en sus críticas señalan la falta de prueba, simplemente han adoptado mi propio punto de vista. Incluso me habrían puesto en deuda si, por su parte, hubieran establecido la improbabilidad que afirmé —es decir, que este postulado es lógicamente independiente de los demás—, corroborando así mi convicción.*
>
> *Ahora bien, incluso en matemáticas, la indemostrabilidad, como es bien sabido, no equivale en absoluto a la no validez, ya que, después de todo, no todo puede demostrarse, sino que toda prueba presupone, a su vez, principios no demostrados. Por lo tanto, para rechazar un principio tan fundamental, habría que comprobar que en algún caso particular no se cumpliera o derivar consecuencias contradictorias de él; pero ninguno de mis oponentes ha intentado hacerlo.*

El predicativismo de Poincaré lo rechaza de plano, asegurando que satisfacer los requisitos de predicativismo que pedía Poincaré volvería imposible toda definición y, por consiguiente, toda ciencia. Su conclusión final era:

> *El número de críticas relativamente grande dirigidas contra mi nota corta atestigua el hecho de que, evidentemente, muchos prejuicios bloquean el camino del teorema que afirma que un conjunto arbitrario puede ser bien ordenado. Pero el hecho de que, a pesar del escrutinio, por el que estoy en deuda con todos los críticos, no se haya podido encontrar ningún error matemático en mi prueba, así como que como que las objeciones levantadas contra mi principio son mutuamente contradictorias y así, en cierto sentido, se cancelan unas a otras, me permiten esperar que con el tiempo toda resistencia será vencida a través de las clarificaciones adecuadas.*

Pero Zermelo tenía una pieza de artillería guardada en su arsenal. Hacía ya tres años que había diseñado un sistema de axiomas pensado para que a partir de ellos pudieran demostrarse todos los teoremas matemáticos. No los había publicado porque había estado tratando de probar que eran consistentes, es decir, que de ellos no puede deducirse ninguna contradicción, pero finalmente había desistido del intento y los publicó en un artículo titulado *Investigaciones en la fundamentación de la teoría de conjuntos* I.

Aunque Zermelo no hubiera logrado demostrar la consistencia de sus axiomas, el hecho era que ninguna de las contradicciones conocidas podía demostrarse a partir de ellos. Con los axiomas de Zermelo la fundamentación de las matemáticas volvió al "orden geométrico", no ya en el sentido laxo de los *Elementos,* sino en el más estricto de los *Grundlagen* de Hilbert. El punto de partida para entender cabalmente la teoría axiomática de Zermelo es concienciarse de este hecho:

> No podemos introducir el concepto de conjunto en matemáticas tomando como definición que un conjunto es cualquier colección de objetos.

Si pretendemos definir un conjunto como cualquier colección de objetos (tal y como había hecho Cantor hasta el momento), entonces tenemos que admitir que "los conjuntos que no son elementos de sí mismos" forman una colección de objetos perfectamente definida que, por lo tanto, constituye un conjunto, y a partir de ahí la paradoja de Russell resulta imparable y nos da una contradicción.

Lo máximo que podemos pretender es que la matemática estudia conjuntos, que son *ciertas* colecciones de objetos, pero no que cualquier colección de objetos forma un conjunto y, en lugar de tratar de especificar cuáles son las colecciones de objetos que forman conjuntos y cuáles no, la propuesta de Zermelo era partir de unos axiomas que garanticen que todas las colecciones de objetos de interés en matemáticas son conjuntos, pero que, a la vez, no justifiquen la existencia de ninguna de las "multiplicidades inconsistentes" que generan contradicciones.

Concretamente, los axiomas de Zermelo eran los siguientes:

Axioma I (de extensionalidad) *Si todo elemento de un conjunto M lo es también de N y viceversa, entonces M y N son el mismo conjunto. Más brevemente: un conjunto está determinado por sus elementos.*

Axioma II (de los conjuntos elementales) *Existe un (ficticio) conjunto vacío 0 que no tiene elementos; si a es un objeto del dominio, existe el conjunto*[32] *$\{a\}$ cuyo único elemento es a; si a y b son dos objetos del dominio, existe el conjunto $\{a, b\}$ cuyos elementos son a y b.*

Axioma III (de especificación) *Si una propiedad $\mathfrak{E}(x)$ está definida para los elementos de un conjunto M, entonces M posee un subconjunto $M_{\mathfrak{E}}$ que contiene precisamente a los elementos de M para los que $\mathfrak{E}(x)$ es verdadera.*

Axioma IV (del conjunto de partes) *Dado un conjunto T, existe otro conjunto*[33] *$\mathfrak{U}T$ cuyos elementos son todos los subconjuntos de T.*

Axioma V (de la unión) *Si T es un conjunto, existe otro conjunto $\mathfrak{S}T$ cuyos elementos son precisamente los elementos de los elementos de T.*

Axioma VI (de elección) *Si T es un conjunto cuyos elementos son conjuntos no vacíos y sin elementos en común, su unión $\mathfrak{S}T$ contiene al menos un subconjunto S_1 que tiene un único elemento en común con cada elemento de T.*

Axioma VII (de infinitud) *Existe un conjunto Z en el dominio que contiene al conjunto vacío como elemento y que, si contiene a un elemento a, también contiene al conjunto $\{a\}$.*

La clave para mantener a raya las paradojas está en el axioma III. Dicho axioma NO afirma que, dada una propiedad P, existe un conjunto que contiene a todos los objetos que tienen la propiedad P. Si así fuera, considerando la propiedad "ser un conjunto", podríamos demostrar la existencia del conjunto V de todos los conjuntos, y la paradoja de Cantor nos daría una contradicción, y considerando la propiedad "ser un conjunto que no es un elemento de sí mismo", podríamos demostrar la existencia del conjunto R de todos los conjuntos que no son elementos de sí mismos, y la paradoja de Russell nos daría una contradicción.

[32] Fue Zermelo quien introdujo la notación $\{a\}$, o $\{a, b\}$, etc. para nombrar conjuntos finitos a través de sus elementos.
[33] La U es de Untermenge (subconjunto).

El axioma de especificación sólo nos dice que, dado un conjunto X prefijado, existe el conjunto formado por todos los elementos de X que tienen la propiedad P. Así, si aplicamos el axioma a la propiedad "ser un conjunto" obtenemos el conjunto Y de todos los conjuntos que son elementos de X, que a lo sumo será el propio conjunto X, si es que todos sus elementos son conjuntos, pero no el conjunto de todos los conjuntos, y de ahí no obtenemos ninguna contradicción conocida. Al contrario, todo el argumento de la paradoja de Cantor se traduce ahora en una demostración en la teoría de Zermelo de que no existe ningún conjunto V que contenga a todos los conjuntos.

Similarmente, si aplicamos el axioma a la propiedad "ser un conjunto que no es un elemento de sí mismo", obtenemos un conjunto Y formado por todos los conjuntos que son elementos de X, pero no de sí mismos, y esto no es contradictorio. Sólo podemos razonar que si Y fuera un elemento de sí mismo, entonces, por construcción, no tendría que ser un elemento de sí mismo, y con ello concluimos, por reducción al absurdo, que Y no es un elemento de sí mismo, pero ahí termina todo. No podemos probar la otra mitad de la paradoja de Russell: si Y no es un elemento de sí mismo, eso no implica que Y deba ser un elemento de sí mismo, pues para ello haría falta que además Y fuera un elemento de X. Lo que concluimos ahora es que, necesariamente, Y no es un elemento de X. Al igual que antes, el argumento de la paradoja de Russell no nos da ahora una contradicción, sino sólo una demostración de que no existe ningún conjunto R que contenga a todos los conjuntos que no son elementos de sí mismos. Similarmente, la antinomia de Burali-Forti se traduce ahora en una demostración de que no existe el conjunto de todos los ordinales.

La restricción del axioma de especificación por la que cada propiedad no define conjuntos en general, sino sólo subconjuntos de un conjunto dado, se traduce en la necesidad de introducir los axiomas II, IV y V, que postulen la existencia de conjuntos básicos que no pueden obtenerse como subconjuntos de otros dados.

El axioma VII postula la existencia de un conjunto X que satisface la definición de Dedekind de conjunto infinito. En efecto, basta considerar (usando lenguaje moderno) la aplicación $S : X \longrightarrow X$ dada por $S(a) = \{a\}$. Claramente es inyectiva y no suprayectiva (pues $\varnothing$ no es la imagen de ningún elemento de X). Siguiendo a Dedekind, a partir de aquí es posible definir el conjunto $\mathbb{N}$ de los números naturales, de modo que

$$0 = \varnothing, \quad 1 = S(0) = \{\varnothing\}, \quad 2 = S(1) = \{\{\varnothing\}\}, \quad 3 = S(2) = \{\{\{\varnothing\}\}\}, \quad \ldots$$

Finalmente, el axioma VI era el principio de elección, que postulaba la existencia de un conjunto sin proporcionar ningún criterio sobre cuáles eran sus elementos.

Como ilustración de las posibilidades de sus axiomas, Zermelo construyó los números naturales, definió los conceptos básicos de la teoría de cardinales de Cantor y demostró (sin usar el axioma de elección) el teorema de Cantor-Bernstein, así como varios resultados que requieren el axioma de elección, como el teorema de Kőnig en toda su generalidad (véase la nota al pie de la página 36), o el teorema que afirma que una unión numerable de conjuntos numerables es numerable, o que todo conjunto infinito contiene un subconjunto numerable. No demostró de nuevo el principio de buena ordenación, pero era claro que la prueba que había presentado ese mismo año no requería nada que no pudiera demostrarse a partir de sus axiomas. Más aún, era claro que si se sustituía el axioma de elección por el principio de buena ordenación, entonces era posible demostrar el axioma de elección, por lo que ambos eran equivalentes (suponiendo los demás axiomas).

Los axiomas de Zermelo zanjaron prácticamente todas las polémicas puramente matemáticas que habían dividido a los matemáticos durante los últimos años, dejando únicamente abiertas las de naturaleza más filosófica. Ya no había lugar a las dudas sobre si Bernstein podía hacer referencia al conjunto de todos los ordinales para probar la existencia de un conjunto que no puede ser bien ordenado (la respuesta era que, en la teoría de Zermelo, NO), ni había motivos para filosofar sobre si una elección simultánea no numerable estaba o no fuera del dominio de la matemática, como había afirmado Borel (la respuesta era que, en la teoría de Zermelo, SÍ era admisible), etc.

Naturalmente, estaba pendiente la cuestión de si los axiomas de Zermelo eran o no contradictorios, y muchas otras cuestiones de naturaleza lógica que uno se podía plantear sobre ellos, pero lo cierto era que proporcionaban un marco de trabajo a los matemáticos que no dejaba ninguna duda sobre qué razonamientos eran válidos y cuáles no, sin necesidad de pararse a filosofar para juzgar cada paso. Otra cosa era que alguien se negara a aceptar, por ejemplo, el axioma de elección, en cuyo caso también estaba claro qué demostraciones seguían a su disposición y cuáles no.

Con el tiempo, los matemáticos constatarían que a partir de los axiomas de Zermelo[34] era posible demostrar formalmente todos los teoremas del álgebra, la geometría, el análisis matemático, etc. conocidos hasta ese momento exactamente igual que a partir de los axiomas de Hilbert es posible demostrar formalmente todos los teoremas de la geometría euclídea. Pero aquí hay que subrayar lo de "formalmente", porque, mientras en el caso de la geometría euclídea el razonamiento formal no es imprescindible (no necesitamos razonar "olvidando" el significado de las palabras "punto", "recta", etc., porque sabemos perfectamente cuál es este significado, y en cualquier momento podemos hacer uso de un resultado intuitivamente evidente sobre puntos y rectas sin necesidad de tomarnos la molestia de deducirlo formalmente de los axiomas, sin perjuicio de que tenga interés el hecho de que siempre vaya a ser posible deducirlo), en el caso de la teoría axiomática de Zermelo el formalismo es esencial, porque *no estamos en condiciones de afirmar que sabemos de qué hablamos exactamente cuando hablamos de conjuntos.* Más precisamente:

> Podemos decir que los conjuntos son colecciones de elementos, pero no que cualquier colección de elementos sea un conjunto, y no podemos afirmar que cualquier colección de objetos en la que podamos pensar tenga que ser un conjunto, sino que sólo podremos asegurar que lo es si su existencia es demostrable a partir de los axiomas de Zermelo.

Esto es precisamente lo que libra a la teoría de Zermelo de las paradojas. Como hemos señalado, en ella podemos reproducir íntegramente el argumento que conduce a la paradoja de Cantor, o a la de Russell o a cualquier otra, pero la conclusión es una contradicción que parte de suponer que existe el conjunto V de todos los conjuntos, o el conjunto R de todos los conjuntos que no son elementos de sí mismos, etc., y con ello simplemente estamos demostrando que no existen tales conjuntos V o R, y ello no genera ninguna contradicción, al menos en apariencia, porque los axiomas de Zermelo no afirman que estos "conjuntos" tengan que existir. Pero el "al menos en apariencia" es crucial, pues nada nos garantiza *a priori* que en la teoría de Zermelo no se puedan demostrar otras paradojas. De hecho, como señalábamos más arriba, Zermelo había fracasado en su intento de asegurarlo.

En **1908** Jourdain publicó *Sobre la multiplicación de los álefs,* donde daba una nueva prueba de la igualdad $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$, esta vez correcta, y que además no usaba el axioma de elección. En el artículo agradecía a Zermelo sus observaciones al artículo precedente y su ayuda con la nueva demostración. En 1906 Gerhard Hessenberg había publicado otra prueba más sencilla en su trabajo *Conceptos básicos de la teoría de conjuntos,* basada en el teorema de la forma normal de Cantor.

Por su parte, Bernstein demostró que todos los conjuntos numerables son conjuntos de unicidad en el sentido definido en la página 4, lo que mejoraba el resultado que había obtenido Lebesgue cinco años atrás.

En **1910** Ernst Steinitz, en su artículo *Teoría algebraica de cuerpos,* usó el principio de buena ordenación para demostrar que todo cuerpo admite una clausura algebraica, única salvo isomorfismo.

26 Los Principia Mathematica En **1910** Russell y Whitehead publicaron el primer volumen de sus *Principia Mathematica.* Como las fallidas *Leyes básicas de la aritmética* de Frege, la teoría de Russell y Whitehead era una compleja teoría lógica que pretendía evitar las contradicciones de la teoría de conjuntos, no mediante unos convenios arbitrarios, como hacían los axiomas de Zermelo al evitar que pudieran definirse las multiplicidades inconsistentes, sino mediante principios justificados por la lógica. La vamos a describir brevemente:

La lógica de los *Principia* es lo que se conoce como una *teoría de tipos ramificada.* Esto significa que distingue entre objetos de tipo 0, que son objetos indeterminados, sin propiedades específicas, los objetos de tipo 1, que son las propiedades de los objetos de tipo 0, los objetos de tipo 2, que son las propiedades de los objetos de tipo 1, etc., pero a su vez estos tipos se ramifican en órdenes. Una propiedad de un tipo dado es de orden 0 si se define sin ningún cuantificador (es decir, sin usar "para todo" o "existe"), es de primer orden si en su definición sólo se cuantifica respecto de objetos de tipo 0, es de segundo orden si en su definición sólo se cuantifica respecto de objetos de tipo 0 o 1, etc. Gracias a esta clasificación, Russell y Whitehead pueden enunciar con precisión lo que denominan *principio del círculo vicioso,* que prohibe que una propiedad se defina en términos de una totalidad de propiedades entre las que figura ella misma. En la introducción de los *Principia* figura este ejemplo:

[34] En realidad, como veremos más adelante, en 1921 Abraham Fraenkel le señaló a Zermelo que para demostrar algunos resultados de la teoría de conjuntos cantarinas era necesario sustituir el axioma III por otro más fuerte, y con ello definió lo que hoy se conoce como teoría de conjuntos de Zermelo-Fraenkel (ZFC), pero lo cierto es que la mayor parte de las matemáticas, las que no dependen esencialmente de la teoría de ordinales y cardinales infinitos, no requieren más que los axiomas de Zermelo.

En la proposición

Napoleón era corso.

podemos considerar a Napoleón como un objeto de tipo 0 y a "ser corso" como una propiedad de tipo 1. En cambio, en

Napoleón tenía todas las características de un buen general.

tenemos una propiedad de tipo 1 (porque es una propiedad que pueden tener o no los objetos de tipo 0) definida en términos de todas las propiedades de tipo 1, y por ello es una definición impredicativa que no puede ser admitida. En su lugar, la lógica de los *Principia* sólo permite definir una proposición como

Napoleón tenía todas las características de tipo 1 *y orden* 0 *de un buen general.*

donde ahora la propiedad es de tipo 1 y de primer orden, porque sólo cuantifica sobre las propiedades de orden 0, o también valdría:

Napoleón tenía todas las características de tipo 1 y de primer orden de un buen general.

en cuyo caso estamos predicando del objeto Napoleón una propiedad de segundo orden de tipo 1.

En los dos últimos ejemplos las propiedades consideradas son predicativas, porque no hacen referencias a la totalidad de las propiedades de su mismo tipo y orden, sino únicamente a propiedades de orden inferior.

Sin embargo, Zermelo tenía razón cuando le respondió a Poincaré que exigir que todas las definiciones fueran predicativas era inviable. Russell y Whitehead se habían dado cuenta de que en su teoría era imposible definir, por ejemplo, el conjunto de los números reales. Para arreglarlo habían introducido lo que llamaron *axioma de reducibilidad,* que venía a decir que toda propiedad de orden arbitrario es lógicamente equivalente a una propiedad de primer orden. Esto resolvía todos los problemas, pero, por una parte, no tenía ninguna justificación lógica (del estilo de las que Russell y Whitehead habían prometido para su teoría) y, por otra —como se observaría más adelante— con el axioma de reducibilidad la ramificación de tipos resultaba innecesaria. Es posible demostrar los mismos resultados considerando una *teoría de tipos simples* (es decir, eliminando el concepto de orden de un tipo) y admitiendo desde el principio las definiciones impredicativas.

El axioma de reducibilidad hace que no pueda decirse que los *Principia* fueran realmente lo que se pretendía que fueran. Eran una forma de evitar las paradojas en matemáticas, pero no una forma "justificada a partir de la pura lógica", y sí una forma mucho más complicada que la solución proporcionada por los axiomas de Zermelo. Esto último fue lo que en la práctica explica el escaso interés que los *Principia* suscitaron entre los matemáticos, unido a que estaban escritos en lo que Poincaré llamaría "un dialecto del peaniano". Por ejemplo, el extracto siguiente corresponde a la página 379 del primer volumen:

$*54{\cdot}43.\quad \vdash :. \alpha, \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

Dem.

$\vdash . *54{\cdot}26 . \supset \vdash :. \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . x \neq y .$

$[*51{\cdot}231] \qquad \equiv . \iota`x \cap \iota`y = \Lambda .$

$[*13{\cdot}12] \qquad \equiv . \alpha \cap \beta = \Lambda \qquad (1)$

$\vdash . (1) . *11{\cdot}11{\cdot}35 . \supset$

$\vdash :. (\exists x, y) . \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . \alpha \cap \beta = \Lambda \qquad (2)$

$\vdash . (2) . *11{\cdot}54 . *52{\cdot}1 . \supset \vdash . \text{Prop}$

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

El teorema afirma que la unión de dos conjuntos disjuntos con un elemento cada uno tiene dos elementos. Tras la demostración se promete que de ahí se deducirá que $1 + 1 = 2$, pero para llegar a este hecho hubo que esperar dos años, a la publicación en **1912** del segundo volumen de la obra, en cuya página 86 se puede leer:

***110·643.** $\vdash . 1 +_c 1 = 2$

Dem.

$$\vdash . *110{\cdot}632 . *101{\cdot}21{\cdot}28 . \supset$$
$$\vdash . 1 +_c 1 = \hat{\xi}\{(\exists y) . y \in \xi . \xi - \iota`y \in 1\}$$
$$[*54{\cdot}3] \quad = 2 . \supset \vdash . \text{Prop}$$

The above proposition is occasionally useful. It is used at least three times, in *113·66 and *120·123·472.

Ese año murió Poincaré, de una embolia, a los 58 años, pero no hay ningún indicio que vincule tan lamentable pérdida con que hubiera leído esta demostración o el pedante comentario que le sigue.

Del "peaniano" de los *Principia* cabe destacar el uso de $x \in y$ para indicar que x es un elemento de y, y el uso de (x) y $\exists x$ con el significado de "para todo x" y "existe un x", respectivamente. Además, los *Principia* introdujeron el signo $\vee$ para representar "o" (del latín *vel,* pero usaban $\cdot$ con el sentido de "y").

En **1913** apareció el tercer y último volumen de los *Principia.* Whitehead y Russell tenían previsto escribir un cuarto sobre los fundamentos de la geometría, pero, según explicaron, lo dejaron estar por agotamiento.

En **1914** Norbert Wiener observó que definiendo el par ordenado formado por dos conjuntos como

$$(x, y) = \{\{\{x\}, \varnothing\}, \{\{y\}\}\},$$

se podía demostrar que $(x, y) = (u, v)$ si y sólo si $x = u$ y $u = v$, y esto permitía evitar algunos usos del axioma de reducibilidad, pero no todos (y así no se arreglaba nada). La definición parece más complicada de lo necesario, pero era así para que fuera compatible con la lógica de los *Principia.*

Definir —de un modo u otro— un par ordenado de conjuntos como un conjunto simplificaba enormemente el tratamiento conjuntista de las relaciones y funciones y no tardó en convertirse en un convenio universalmente aceptado. Prueba de su conveniencia es que Russell había considerado esta opción en *Los principios de las matemáticas,* pero la había descartado por motivos filosóficos. Citamos el pasaje como muestra de la clase de consideraciones filosóficas del logicismo de Russell que traían sin cuidado a los matemáticos:

> *Existe la tentación de considerar una relación como definible por su extensión, es decir, como una clase de pares. Esto tiene la ventaja formal de que evita la necesidad de postular una proposición primitiva que afirme que cada par tiene una relación que no se da entre ningún otro par de términos.*
>
> *Pero es necesario darle sentido al par, distinguir el referente* [el primer término] *del relato* [el segundo término]*: así, un par se vuelve esencialmente distinto de una clase de dos términos, y debe ser introducido él mismo como una idea primitiva.*
>
> *Filosóficamente, parecería que el sentido sólo puede derivarse de alguna proposición relacional, y que la afirmación de que "a" es el referente y "b" el relato ya involucra una proposición puramente relacional en la que "a" y "b" son términos, aunque la relación afirmada sea sólo la general de referente a relato.*
>
> *Existen, de hecho, conceptos como "mayor que", que aparecen de forma diferente a como términos en proposiciones con dos términos (secciones 48, 54); y ninguna doctrina de parejas puede eludir tales proposiciones. Por lo tanto, parece más correcto adoptar una visión intensional de las relaciones, e identificarlas más con conceptos de clase que con clases.*
>
> *Este procedimiento es formalmente más conveniente y también parece más cercano a los hechos lógicos. En todas las matemáticas existe la misma relación, bastante curiosa, entre los puntos de vista intensional y extensional: los signos distintos de los términos variables (es decir, los conceptos de clase y las relaciones variables) representan intensiones, mientras que los objetos reales con los que se trata son siempre extensiones. Así, en el cálculo de relaciones, lo relevante son las clases de pares, pero el simbolismo las maneja por medio de relaciones. Esto es precisamente similar al estado de cosas explicado en relación con las clases, y parece innecesario repetir las explicaciones en detalle.*

27 La teoría de conjuntos de Hausdorff En **1914** Felix Hausdorff publicó sus *Fundamentos de la teoría de conjuntos,* un libro de unas 500 páginas, dedicado a la memoria de Georg Cantor, que puede considerarse la primera exposición moderna de la teoría de conjuntos para uso de los matemáticos, es decir, sin preocupaciones filosóficas. En él introduce los conceptos modernos de relación y función como conjuntos de pares ordenados, donde los pares ordenados los define como[35]

$$(x, y) = \{\{x, 0\}, \{y, 1\}\}.$$

En la primera parte, titulada *Elementos de la teoría de conjuntos pura,* introduce los conceptos conjuntistas básicos (las operaciones conjuntistas de unión, intersección, diferencia, etc., los conceptos de relación y función, el producto cartesiano, etc.) y expone los resultados básicos de la teoría de cardinales y ordinales.

No expone explícitamente los axiomas de Zermelo, pero dice lo siguiente:

> *Tales sistemas de cosas, que no pueden ser concebidos como un conjunto, son, como veremos, los números cardinales (finitos e infinitos) o también los números ordinales. El intento, necesario a raíz de esto, de restringir el proceso de formación ilimitada de conjuntos mediante requisitos adecuados, fue emprendido por E. Zermelo.*
>
> *Sin embargo, dado que estas investigaciones extremadamente perspicaces aún no pueden considerarse concluidas y dado que una introducción al principiante en la teoría de conjuntos por esta vía probablemente estaría asociada con grandes dificultades, nosotros permitiremos aquí el concepto ingenuo de conjunto, pero de hecho mantendremos las restricciones que cortan el camino a esa paradoja.*

Esto significa que Hausdorff no hace nada que no pueda hacerse en la teoría de Zermelo, pero no se para a deducir de sus axiomas las propiedades básicas de los conjuntos.[36]

En la segunda parte, bajo el título de *Teoría de los conjuntos de puntos,* introduce por primera vez el concepto de *espacio topológico*[37] y acuña el concepto de *espacio métrico* para distinguir los espacios que Fréchet había llamado "clases (V)" en su tesis de 1906 de sus espacios, aún más generales. Si Fréchet había demostrado que a partir de una noción abstracta de "distancia" es posible definir los conceptos de límite de una sucesión y continuidad de una función, Hausdorff mostraba que cada distancia abstracta define una topología, y que, a su vez, cada topología permite definir los conceptos de límite de una sucesión y de continuidad de una función.

Hausdorff introdujo una clasificación importante de los cardinales infinitos. Una propiedad general de los cardinales infinitos es que, si κ es uno de ellos, la unión de a lo sumo κ conjuntos de cardinal a lo sumo κ tiene cardinal a lo sumo κ. Pero un cardinal infinito se dice *regular* si la unión de menos de κ conjuntos de cardinal menor que κ tiene cardinal menor que κ. En caso contrario de dice *singular.*

Por ejemplo, $\aleph_0$ es un cardinal regular, porque la unión de menos de $\aleph_0$ (es decir, de una cantidad finita) de conjuntos de cardinal menor que $\aleph_0$ (es decir, conjuntos finitos) es finita (tiene cardinal menor que $\aleph_0$).

Por otra parte, el hecho de que la unión de una cantidad numerable de conjuntos numerables es numerable (la unión de menos de $\aleph_1$ conjuntos de cardinal menor que $\aleph_1$ tiene cardinal menor que $\aleph_1$) se traduce en que $\aleph_1$ es un cardinal regular. Más en general, exactamente por el mismo argumento, todo cardinal de la forma $\aleph_{\alpha+1}$ es regular.

Los cardinales que tienen un inmediato anterior se llaman *cardinales sucesores.* Esto incluye a todos los cardinales finitos no nulos y a los cardinales de la forma $\aleph_{\alpha+1}$, pues $\aleph_{\alpha+1}$ es el sucesor de $\aleph_\alpha$. En estos términos, acabamos de observar que todo cardinal sucesor (infinito) es regular.

En cambio, los cardinales no nulos que no tienen un inmediato anterior se llaman *cardinales límite.* Por ejemplo, $\aleph_0$ es un cardinal límite, pues tiene por detrás los cardinales finitos, pero ninguno es inmediatamente anterior a él, y también $\aleph_\omega$, que tiene por detrás los cardinales finitos y $\aleph_0, \aleph_1, \aleph_2, \ldots$, pero ninguno es justo anterior a él. (En general, son los cardinales de la forma $\aleph_\lambda$, donde $\lambda = 0$ o bien λ es un ordinal límite.)

[35] El convenio universalmente aceptado en la actualidad es

$$(x, y) = \{\{x\}, \{x, y\}\},$$

y lo propondría Kazimierz Kuratowski en 1921

[36] Es probable que Hausdorff no se decidiera a partir de los axiomas de Zermelo porque había un inconveniente técnico que entonces no se sabía resolver y se pasaba de soslayo, y era cómo definir concretamente los cardinales y los ordinales infinitos. Este problema lo resolvería von Neumann en 1923 (véase la sección 35).

[37] Aunque lo que Hausdorff llama "espacio topológico" es el caso particular que hoy se conoce como "espacio de Hausdorff".

Así, $\aleph_0$ es un ejemplo de cardinal límite regular, mientras que $\aleph_\omega$ es un ejemplo de cardinal límite singular, pues A_n es un conjunto de cardinal $\aleph_n$, la unión de todos los conjuntos A_n es un conjunto de cardinal $\aleph_\omega$, y tenemos así una unión de menos de $\aleph_\omega$ conjuntos de cardinal menor que $\aleph_\omega$ cuyo cardinal no es menor que $\aleph_\omega$.

Hausdorff se había interesado en la teoría de conjuntos a través de la hipótesis del continuo. En una carta a Hilbert de 1904 le decía que le había invadido casi como una monomanía. Eso lo había llevado a estudiar en profundidad los conjuntos ordenados, y a estudiar y clasificar los posibles tipos de órdenes. En tal estudio, hacía ya unos años, se había encontrado con algunos casos que podrían darse si existiera un cardinal límite regular no numerable. Sin embargo, no fue capaz de encontrar ninguno. $\aleph_\omega$ es un cardinal límite, pero es singular, igual que $\aleph_{\omega\cdot 2}$, o como $\aleph_{\omega^7}$, etc.

Un cardinal límite regular no numerable es lo que hoy se conoce como un *cardinal (débilmente) inaccesible.* Como decíamos, Hausdorff no pudo encontrar ninguno, pero constató que, en caso de existir, deberían ser increíblemente grandes.

En otro orden de cosas, en una sección final de notas, Hausdorff incluyó en su libro un resultado que acababa de publicar ese mismo año, conocido como la *paradoja de Hausdorff,* que no es ninguna paradoja en el sentido que hemos estado considerando aquí, sino un teorema (demostrable a partir de los axiomas de Zermelo, en el que el axioma de elección es esencial) según el cual, es posible tomar una esfera S en el espacio tridimensional y descomponerla en cuatro partes disjuntas

$$S = A \cup B \cup C \cup N,$$

donde N es numerable y A, B, C pueden transformarse uno en otro mediante movimientos adecuados, pero además, cualquiera de ellos puede transformarse en $B \cup C$.

El cálculo integral permite definir una familia de subconjuntos medibles de la esfera S, y definir sobre ella una medida σ análoga a la medida de Lebesgue, que asigne un área a cada porción medible de superficie esférica. La paradoja de Hausdorff demostraba que dicha medida no puede extenderse a todos los subconjuntos de S y que sea invariante por movimientos (como cabe esperar de cualquier concepto razonable de área). Si fuera posible, como N tendría que tener medida nula, sería

$$\sigma(S) = \sigma(A) + \sigma(B) + \sigma(C) = 3\sigma(C) = 3\sigma(B \cup C) = 3(\sigma(B) + \sigma(C)) = 6\sigma(C),$$

de donde $\sigma(S) = \sigma(C) = 0$.

En **1916** Hausdorff obtuvo un progreso en su intento de probar la hipótesis del continuo. En su artículo *La cardinalidad de los conjuntos de Borel* demostró que todo subconjunto de Borel no numerable de la recta real contiene un subconjunto perfecto y, por consiguiente, tiene el cardinal del continuo. Se trataba, pues, de una generalización del teorema de Cantor-Bendixson, y demostraba que ningún conjunto de Borel podía contradecir la hipótesis del continuo, es decir, que no podía tener un cardinal estrictamente intermedio entre $\aleph_0$ y $2^{\aleph_0}$.

28 Conjuntos analíticos En 1915, un estudiante de 19 años llamado Pável Alexandroff demostró que todo conjunto de Borel se puede construir a partir de conjuntos cerrados de una forma mucho más simple que la descrita por Lebesgue en su artículo de 1905, sin necesidad de ordinales transfinitos. Concretamente, Alexandroff demostró que todo conjunto de Borel B (con notación moderna) puede expresarse en la forma

$$B = \bigcup_x \bigcap_n C_{x_0,\ldots,x_n},$$

donde $\{C_s\}$ es una familia de conjuntos cerrados y los índices s recorren las sucesiones finitas de números naturales. En la expresión anterior, x recorre las sucesiones infinitas de números naturales y n recorre los números naturales. En otras palabras, para cada sucesión x, formamos la intersección

$$C_x = C_{x_0} \cap C_{x_0,x_1} \cap C_{x_0,x_1,x_2} \cap \cdots$$

y luego formamos la unión de todos estos conjuntos C_x. Alexandroff comunicó su descubrimiento a su profesor, Nikolái Lusin, éste le sugirió que investigara el recíproco, es decir, si todo conjunto de esta forma es de Borel.

Mientras tanto, otro alumno de Lusin, Mijaíl Suslin, estaba investigando la cardinalidad de los conjuntos de Borel. Lusin le había recomendado que se estudiara el tratado de Lebesgue, y estaba en ello cuando descubrió un error en él. Lebesgue afirmaba que toda proyección de un conjunto de Borel es un conjunto de Borel, pero en

1916 Suslin encontró un contraejemplo, que era precisamente un conjunto de la forma descrita por Alexandroff. Suslin propuso llamar a estos conjuntos A-conjuntos (por Alexandroff) igual que los conjuntos de Borel se llamaban B-conjuntos (por Borel). En estos términos, Alexandroff había probado que todo B-conjunto es un A-conjunto, y Suslin que existen A-conjuntos que no son B-conjuntos.

Pero, así como Suslin había resuelto el problema que Lusin había asignado a Alexandroff, éste resolvió el problema asignado a Suslin, y demostró —independientemente de Hausdorff— que todo conjunto de Borel no numerable contiene un subconjunto perfecto. Su hallazgo fue comunicado en el artículo *Sobre la potencia de los conjuntos B-medibles.*

En **1916** se doctoró Dimitri Menshov, bajo la dirección de Lusin y Dimitri Egorov, y en su tesis mostró un ejemplo de conjunto nulo para la medida de Lebesgue que no era un conjunto de unicidad en el sentido de la página 4 (era una variante del conjunto de Cantor en el que, en lugar de eliminar siempre intervalos de longitud igual a la tercera parte de los intervalos precedentes, en el paso n-simo se quitan intervalos de longitud $(n+1)/(2(n+2))$, lo que refutaba la conjetura de Lebesgue de que todo conjunto nulo tuviera que ser un conjunto de unicidad.

En **1917** Suslin publicó su resultado en una nota *Sobre una definición de los conjuntos B-medibles sin números transfinitos,* donde definía los A-conjuntos y enunciaba varios resultados, como que los B-conjuntos son precisamente los A-conjuntos cuyo complementario es también un A-conjunto, pero que hay A-conjuntos que no son B-conjuntos.

También afirmaba todo A-conjunto es la proyección ortogonal de un B-conjunto y que toda proyección ortogonal de un A-conjunto (en particular de un B-conjunto) es un A-conjunto.

Ese mismo año de **1917** Lusin publicó su nota *Sobre la clasificación del Sr. Baire,* donde presentaba los A-conjuntos con el nombre de *conjuntos analíticos* y los caracterizaba de esta manera:

> **Teorema** *Un conjunto E es analítico si y sólo si admite una representación paramétrica $x = f(t)$, por medio de una función continua sobre $\mathbb{I}$.*

Aquí $\mathbb{I}$ representa al conjunto de todos los números irracionales. En términos modernos, estaba diciendo que los conjuntos analíticos son precisamente las imágenes continuas de $\mathbb{I}$. También enunciaba su resultado según el cual los conjuntos analíticos son medibles Lebesgue.

Más aún, en **1918**, Suslin demostró que todo conjunto analítico no numerable contiene un subconjunto perfecto, lo que suponía un paso más hacia una prueba de la hipótesis del continuo y una muestra de las posibilidades de la teoría descriptiva de conjuntos.

Esto habría alegrado mucho a Cantor, pero ya no estaba para estas cosas. Murió ese mismo año de **1918** a los 72 años. Durante los últimos años de su vida había estado internado varias veces en sanatorios mentales. Los ataques que había recibido por parte de Kronecker y otros detractores de sus teorías, junto con la frustración de no haber sido capaz de demostrar o refutar la hipótesis del continuo pese a todo el empeño que había puesto en ello, habían minado su salud mental. Dedekind había muerto dos años antes, en 1916, a los 84 años.

29 El intuicionismo Hermann Weyl se había doctorado en Gotinga en 1908 bajo la dirección de Hilbert. En **1918** publicó un pequeño tratado en la dirección opuesta al libro de Hausdorff. Se titulaba *El continuo* y, rebosando filosofía (llevaba cinco años casado con una filósofa, discípula de Edmund Husserl), aborda el análisis real en el marco de los *Principia Mathematica,* pero sin usar toda su potencia, para garantizar que todos los razonamientos fueran predicativos. Esto lo privaba, por ejemplo, del teorema de completitud, que afirma que todo subconjunto no vacío y acotado superiormente en la recta real tiene supremo, y hacía que muchos resultados básicos requirieran modificaciones en sus pruebas, o que sólo se pudieran demostrar en versiones restringidas o, a veces, incluso que dejaran de ser aceptables por no admitir una demostración predicativa.

En 1907, un joven matemático neerlandés de 26 años llamado Luitzen Egbertus Jan Brouwer había leído su tesis doctoral titulada *Sobre los fundamentos de las matemáticas,* donde analizaba las posiciones contrapuestas de Hilbert y Russell. Su director de tesis lo obligó a suprimir una parte que juzgó demasiado filosófica y lo instó a centrarse en matemáticas más "respetables". En 1808 publicó un artículo titulado *Sobre la falta de fiabilidad de los principios lógicos,* pero se dio cuenta de que sus excéntricas teorías podrían perjudicar gravemente a su carrera profesional, así que las metió en un armario y e inició una brillante trayectoria en el área de la topología que impresionó a Hilbert, cuya recomendación influyó decisivamente para que Brouwer obtuviera una cátedra

en la Universidad de Amsterdam en 1912. Sin embargo, a partir de **1918** sacó del armario sus teorías sobre la fundamentación de la matemática y se propuso reconstruir todas las matemáticas en el marco lógico que él consideraba aceptable, al que denominaba *intuicionismo,* una versión mucho más restrictiva y radical que las que habían defendido Kronecker y Poincaré, porque Brouwer cuestionaba los mismísimos principios de la lógica.

Ese año publicó su primer artículo al respecto, titulado *La fundamentación de la teoría de conjuntos independientemente del principio del tercio excluso. Primera parte. Teoría de conjuntos general.*

El principio del tercio excluso es el que afirma que, para cualquier afirmación p, siempre es cierto "p o no p". Brouwer sostenía que esto es válido para afirmaciones que traten sobre una cantidad finita de objetos, pero que, igual que hay principios matemáticos que valen para conjuntos finitos y no para conjuntos infinitos, como que "el todo es mayor que la parte", sucede lo mismo con algunos principios lógicos, como el principio del tercio excluso, y que es un error aplicarlos irreflexivamente en general.

Más precisamente, Brouwer sostenía que sólo podemos afirmar una disyunción como p o q si podemos razonar que se cumple p o podemos razonar que se cumple q. En particular, para afirmar p o no p tenemos que ser capaces de demostrar que se cumple p o de demostrar que se cumple no p. Esto tenía sus consecuencias, como que no aceptaba las demostraciones por reducción al absurdo.

Así pues, todos los resultados matemáticos debían ser revisados en el mismo sentido en que Weyl había revisado la teoría sobre el continuo: dando pruebas intuicionistamente aceptables cuando fuera posible, aunque ello obligara a veces a restringir el alcance de algunos enunciados, o rechazarlos como falsos si no podían ser justificados en el marco intuicionista.

No obstante, durante los primeros años las publicaciones de Brouwer pasaron más o menos inadvertidas o fueron vistas como excentricidades sin importancia, y el propio Hilbert ofreció una cátedra a Brouwer en Gotinga, en **1819**, pero Brouwer la rechazó, al igual que otra en Berlín.

En **1920** el intuicionismo empezó a hacerse notar a partir de una charla que dio en Bad Nauheim con el título *¿Tiene todo número real un desarrollo decimal?* (que sería publicada al año siguiente) y con el artículo *Teoría de conjuntos intuicionista,* que fue el primero que publicó en una revista matemática de difusión internacional.

Mientras tanto, Hilbert y sus colaboradores habían estudiado minuciosamente los *Principia Mathematica* y habían constatado que el axioma de reducibilidad hacía que la complejidad filosófica de la obra no aportara nada realmente. En una charla declaró:

> *El intento de reducir a la lógica la teoría de conjuntos y, con ella, los métodos usuales del análisis no se ha logrado hasta hoy y tal vez sea imposible de lograr.*

Ese año Weyl se pronunció en favor del intuicionismo en una charla titulada *La nueva crisis fundacional de las matemáticas,* y Hilbert se enzarzó en los años siguientes en una disputa sobre el intuicionismo a la vez que elaboraba y exponía sus propias ideas al respecto.

30 Fundamenta Mathematicae Wakław Sierpinsński se había doctorado en Cracovia en 1906, y en 1907 se encontró con un teorema que decía que los puntos del plano pueden determinarse mediante una única coordenada. Le escribió a un amigo que estaba entonces en Gotinga para preguntarle cómo era eso posible, y la respuesta que recibió contenía una única palabra: Cantor. Sierpiński estudió la teoría de conjuntos y en 1909 impartió por primera vez en la historia un curso sobre este tema. El estallido de la Primera Guerra Mundial lo pilló en Rusia y, para evitar problemas por su nacionalidad polaca, pasó esos años en Moscú, bajo la protección de Lusin, con quien colaboró en el desarrollo de la teoría de los conjuntos analíticos. En 1913 se doctoró bajo su dirección Stefan Mazurkiewicz. En 1919 ocupó una cátedra en Varsovia y en **1920** se convirtió, junto a Mazurkiewicz, en editor jefe de la revista *Fundamenta Mathematicae,* para reemplazar a Zygmunt Janiszewski, que la acababa de fundar, pero que había fallecido a principios de año (a los 31 años) —víctima de una epidemia de gripe— antes de que llegara a publicarse el primer número. La revista estaba especializada en topología, teoría de conjuntos y fundamentos de las matemáticas. Su primer número incluyó una sección de problemas abiertos, en la que se plantearon los siguientes, que copiamos meramente a título ilustrativo:

Problemas

> 1) Si un conjunto de puntos P es una imagen biunívoca y continua (pero no necesariamente bicontinua) de un conjunto Q y Q es una imagen biunívoca y continua de P, ¿los conjuntos P y Q son necesariamente homeomorfos?
>
> Problema del Sr. W. Sierpiński

2) Un continuo (acotado) plano, topológicamente homogéneo, ¿es necesariamente homeomorfo a una circunferencia?

(Un conjunto E se dice *topológicamente homogéneo* si para todo par de puntos a, b de E, existe una transformación biunívoca y bicontinua de E en sí mismo que transforma a en b).

Problema de los Sres. B. Knaster y C. Kuratowski

3) Un conjunto ordenado (linealmente) sin saltos ni lagunas y tal que todo conjunto de intervalos suyos que contengan más de un punto y no tengan puntos en común los unos con los otros es a lo sumo numerable, ¿es necesariamente un continuo lineal (ordinario)? [cf págs. 162, 305]

Problema del Sr. M. Suslin

4) ¿Existe una descomposición de un intervalo en $\aleph_1$ conjuntos (no vacíos) medibles Borel y sin puntos en común dos a dos? [cf pág. 93]

Problema del Sr. W. Sierpiński

5) ¿Existe un conjunto lineal no numerable E tal que todo conjunto lineal homeomorfo a E tenga medida de Lebesgue nula? ¿Se puede demostrar la existencia de un conjunto así admitiendo que $2^{\aleph_0} = \aleph_1$?

Problema del Sr. W. Sierpiński

6) ¿Se puede demostrar sin la hipótesis del continuo ($2^{\aleph_0} = \aleph_1$) que una suma [unión] de $\aleph_1$ conjuntos de medida de Lebesgue nula no es necesariamente de medida de Lebesgue nula? ¿Y que una suma de $\aleph_1$ conjuntos de primera categoría no es necesariamente de primera categoría? ¿Y que un producto [intersección] de $\aleph_1$ conjuntos analíticos no es necesariamente analítico? [cf pág. 304]

Problema del Sr. W. Sierpiński

7) ¿Se puede establecer sin la hipótesis del continuo la existencia de un conjunto plano que tiene medida de Lebesgue nula sobre toda paralela al eje de abscisas y cuyo complementario tiene medida de Lebesgue nula sobre toda paralela al eje de ordenadas? [cf pág. 325]

Problema del Sr. H. Steinhaus

8) ¿Se puede dar un ejemplo efectivo de un conjunto de números reales E tal que toda suma, toda diferencia, todo producto y todo cociente de dos números de E (excluida la división entre 0) pertenezca a E y que E sea no numerable, pero distinto del conjunto de todos los números reales? [cf pág. 304]

Problema del Sr. S. Mazurkiewicz

9) ¿Cuál es la potencia de los conjuntos complementarios de los conjuntos analíticos? [cf pág. 318]

Problema del Sr. M. Lusin

10) ¿Existe una función de segunda clase que no sea límite de funciones continuas casi por todas partes? ¿Se puede dar un ejemplo efectivo de una función que no sea límite de funciones puntualmente discontinuas?

Problema de los Sres. T Felsztyn y W. Sierpiński

El problema 3) era póstumo, pues Suslin había muerto de tifus el año anterior, en 1919, a los 24 años.

En **1921** se doctoró en Varsovia Kazimierz Kuratowski. Había iniciado su doctorado con Janiszewski, pero su muerte hizo que tuviera que continuar con Mazurkiewicz. Fue ese mismo año cuando Kuratowski publicó su artículo *Sobre la noción de orden en la teoría de conjuntos,* en el que introdujo la definición conjuntista moderna de par ordenado $(x, y) = \{\{x\}, \{x, y\}\}$, que ya hemos mencionado.

También en **1921** se doctoró en Varsovia Aleksander Rajchman, bajo la dirección de Steinhaus, y en su tesis demostraba que el conjunto de Cantor es un conjunto de unicidad, en el sentido de la página 4 por lo que estos conjuntos no eran necesariamente numerables. Ese mismo año Arnaud Denjoy (que se había doctorado en 1909 bajo la dirección de Baire) publicó su artículo *Sobre la unicidad del desarrollo trigonométrico,* donde demostró que todo conjunto de unicidad en el sentido de la página 4 tiene medida de Lebesgue 0.

Ese año Nina Karlovna Bari se convirtió en la primera mujer graduada en la Universidad de Moscú. Empezó sus estudios de doctorado bajo la dirección de Lusin y en **1922** presentó sus primeros resultados ante la Sociedad Matemática de Moscú. Bari descubrió independientemente algunos de los resultados de Rajchman.

En resumen, la situación es que todo conjunto numerable es de unicidad, pero hay conjuntos de unicidad no numerables, y todo conjunto de unicidad es nulo para la medida de Lebesgue, pero hay conjuntos nulos que no son de unicidad.

31 La paradoja de Berry En 1905 Jules Richard había publicado una paradoja que hoy se conoce como *paradoja de Richard* y sobre la que matemáticos y filósofos debatían al igual que sobre las paradojas de la teoría de conjuntos. Aquí vamos a tratar otra muy similar, pero técnicamente más sencilla, que se discute en los *Principia Mathematica* y que Russell atribuye a G.G. Berry, un bibliotecario de Oxford:

Tomamos todas las sucesiones de letras y espacios en blanco que pueden formarse de longitud menor o igual que 100. Claramente sólo hay un número finito de ellas. Descartamos las que no tengan un significado preciso en castellano, como

buen xxz sin donde

y descartemos también las que tengan significado, excepto aquellas que definan unívocamente un número natural. Así nos quedamos con un número finito de definiciones del estilo de:

el menor primo de cinco cifras en base diez

que define al número 10 007. Consideramos el conjunto X de todos los números naturales definibles de este modo, es decir, mediante una definición en castellano que tenga a lo sumo 100 caracteres (entre letras y espacios). Se trata de un conjunto finito de números naturales, luego no puede contener a todos los números naturales, que son infinitos. Así pues, existen números naturales que no son definibles mediante definiciones que tengan a lo sumo 100 caracteres. Sea Y el conjunto de todos ellos, que, según acabamos de justificar, no es vacío.

Un resultado básico sobre números naturales es que todo conjunto no vacío de números naturales tiene un mínimo elemento. Si el conjunto Y no es vacío, podemos considerar, pues, su mínimo, digamos N. Tenemos así un número natural N que está unívocamente determinado por esta definición:

El menor número natural no definible en castellano con menos de cien letras y espacios

Pero esta definición, que está en perfecto castellano, consta de 86 letras y espacios, y define a N. Concluimos que, a la vez, N no es definible con menos de 100 caracteres (porque lo hemos definido como el menor número natural con esa propiedad) y, por otra parte, es definible con 86 caracteres, porque tenemos una definición explícita de N de dicha longitud.

En el caso de la paradoja de Richard —y la situación es la misma con la de Berry— tanto el propio Richard como Poincaré la explicaban por el carácter impredicativo de la definición que la provoca. Estamos definiendo un número natural con una definición que hace referencia a todas las definiciones (pues decir que un número n no es definible es equivalente a que, para toda definición D, no se cumple que D define a n), pero luego pretendemos que esta definición sea una de las definiciones que hemos considerado para definir la definición D. Es, pues, el típico círculo vicioso impredicativo.

La moraleja para un predicativista[38] es que no tiene sentido hablar de la totalidad de las definiciones. Dada cualquier lista de definiciones, siempre tiene sentido construir una más que sería contradictorio suponer que es una de la lista dada. Notemos que eso no puede interpretarse como que hay una cantidad no numerable de definiciones (es imposible crear una cantidad no numerable de definiciones finitas construidas con un número finito de letras). Sólo significa que "todas" no tiene sentido cuando decimos "todas las definiciones".

Pero, aunque un predicativista pueda considerar que la impredicatividad de la definición de Berry zanja el problema, sigue quedando planteada una pregunta crucial: ¿se puede llegar a la contradicción de Berry a partir de los axiomas de Zermelo? Porque los axiomas de Zermelo no ponen trabas a las definiciones impredicativas, y si la paradoja de Berry supera las defensas de los axiomas, entonces la teoría de Zermelo sería tan inútil como la de Frege.

[38] En realidad hay un problema previo a la posible no predicatividad de la definición de Berry, y es si realmente existe un concepto bien definido de "definición" o de "definible". Por ejemplo, consideremos esta candidata a definición:

El número natural n que cumple $2^{\aleph_0} = \aleph_n$

Si, por ejemplo, $2^{\aleph_0} = \aleph_{\omega+5}$, entonces la "definición" anterior no define nada, pero $2^{\aleph_0}$ también podría ser $\aleph_n$ para cualquier $n > 0$, por lo que la "definición" anterior podría definir cualquier número natural según las propiedades que cumplan los conjuntos de los que hablamos. Si una definición matemática se apoya en las propiedades de los conjuntos, podría ocurrir que realmente defina un número si los conjuntos cumplen ciertas propiedades o que no defina ninguno si cumplen otras, y un mismo número natural podría no ser definible con menos de 100 palabras si los conjuntos cumplen ciertas propiedades y sí serlo si cumplen otras. Entonces, ¿realmente tiene sentido decir si una presunta definición es o no una definición? ¿podemos definir la definibilidad?

Si tratamos de deducir la paradoja de Berry de los axiomas de Zermelo nos percataremos de que, tal y como éste los enunció, tienen una brecha por la que podrían entrar ambigüedades y contradicciones si no la sellamos debidamente. Nos referimos a que en el axioma III (de especificación) se hace referencia a una propiedad P, pero no hemos especificado qué debemos entender por "propiedad". ¿Ser un número definible en español con menos de cien letras es una propiedad? En realidad Zermelo no dice "propiedad", sino "función proposicional", pero eso no aclara nada. Sólo exige que "esté definida". Nos ocupamos de esto en el apartado siguiente.

32 Lenguajes formales En la formulación de sus axiomas, Zermelo hablaba de "objetos" y "conjuntos", lo que dejaba la puerta abierta a que se consideraran objetos que no eran conjuntos. Sin embargo, los matemáticos no tardaron en constatar que esto complicaba ligeramente la teoría de conjuntos sin aportar nada sustancial. Era mucho más práctico adoptar el convenio de que no hay nada más que conjuntos, que los elementos de los conjuntos son siempre otros conjuntos.

Si al lector le parece paradójico que se pueda hablar de conjuntos sin hablar de unos elementos de partida, el truco está en el conjunto vacío, que Zermelo representaba como 0. Se trata de un conjunto sin elementos, pero que a su vez puede ser el elemento de otros conjuntos, como $\{0\}$, que es un conjunto con un elemento (no es vacío). Con este conjunto, a su vez, podemos formar el conjunto $\{\{0\}\}$, que es distinto de los dos anteriores y, en general, así podemos formar infinitos conjuntos distintos, como

$$0, \quad \{0\}, \quad \{\{0\}\}, \quad \{\{\{0\}\}\}, \quad \cdots$$

(y muchos más, con otros patrones, como $\{0,\{0\}\}$, etc.). De este modo, cuando un matemático dice: "Consideremos un conjunto $A = \{a, b, c\}$", le da igual si los elementos a, b, c son o no conjuntos, pero, precisamente porque le da igual lo que sean, no pasa nada si suponemos que son, por ejemplo, $a = 0$, $b = \{0\}$, $c = \{\{0\}\}$. Dicho de otro modo, cuando necesitamos "elementos cualesquiera" no hay ningún inconveniente en elegirlos de modo que sean conjuntos (hechos de conjuntos hechos de conjuntos, etc.), por lo que podemos descartar de la teoría cualquier "objeto" que no sea un conjunto. Aunque con ello nos estamos anticipando ligeramente en el tiempo, vamos a suponerlo así para simplificar el asunto que vamos a tratar aquí.

Supongamos ahora que el lector abre cualquier libro de matemáticas y se fija en cualquier enunciado que encuentre en él. Por ejemplo, en el teorema de Bolzano:

> *Si $a < b$ son números reales y $f : [a, b] \longrightarrow \mathbb{R}$ es una función continua tal que $f(a)f(b) < 0$, existe un número real $a < c < b$ tal que $f(c) = 0$.*

Si le preguntamos a un matemático qué significa que f sea una función continua nos podrá dar una definición precisa: "quiere decir que para cada $x \in [a, b]$ y cada $\epsilon > 0$ existe un $\delta > 0$ tal que si..." Si a su vez le preguntamos qué significa que f sea una función, también nos lo podrá definir, y si le preguntamos qué es el intervalo $[a, b]$, también nos lo podrá definir, y si le preguntamos qué significa que $a < b$, también nos lo podrá definir, y si le preguntamos qué es un número real, también nos lo podrá definir, etc. En cada paso podríamos sustituir en el enunciado el término definido por su definición y así, al cabo de un número finito de pasos, llegaríamos a un enunciado equivalente (pero terriblemente largo) en el que no habría ningún concepto susceptible de ser sustituido por una definición a partir de conceptos más simples. ¿Qué conceptos quedarían en ese enunciado final, desprovisto de conceptos definidos? La respuesta es muy simple: sólo tres, los conceptos matemáticos de "conjunto" y "pertenencia" y el concepto lógico de "igualdad". Si le preguntamos a un matemático qué significa $x = y$ nos responderá simplemente que eso indica que x e y son el mismo conjunto, pero esto no nos reduce la igualdad $x = y$ a ningún otro concepto más simple.[39] Así pues:

> Toda afirmación matemática puede expresarse exclusivamente a partir de los conceptos de "conjunto", "pertenencia" e "igualdad".

Ahora falta precisar qué queremos decir exactamente con "exclusivamente". Por ejemplo, tomemos el axioma de extensionalidad:

> Si dos conjuntos x, y cumplen que cuando $u \in x$ también $u \in y$ y viceversa, entonces $u = y$.

[39] En realidad, sería posible definir $x = y$ como "todo conjunto que cumple $u \in x$ cumple también $u \in y$, y viceversa", con lo que la igualdad puede reducirse a la pertenencia, pero en muchas ocasiones es preferible considerar la igualdad como un concepto lógico primitivo, sin definición.

Aquí, además de "conjuntos", $u \in x$, $u \in y$, $u = y$, aparecen también las palabras "si", "dos", "cumplen", "entonces", etc. Sería más sospechoso que apareciera la expresión "más o menos" o la palabra "suerte", etc. Entonces, ¿qué palabras podemos emplear exactamente en un enunciado matemático para que podamos decir que es una definición aceptable, rigurosa?

La forma de responder con precisión a esta pregunta es a través del concepto de "lenguaje formal". En lugar de dar una definición general, vamos a ilustrar la idea describiendo lo que hoy se entiende por "el lenguaje formal de la teoría de conjuntos". Para ello fijamos un *alfabeto* formado por los signos siguientes:

- Variables: $x, y, z, u, v, w, \ldots$
- Signos lógicos: $\neg$, $\to$, $\vee$, $\wedge$, $\leftrightarrow$, $\bigwedge$, $\bigvee$, $=$.
- Signos no definidos: $\in$.

Con los signos de este alfabeto vamos a formar cadenas de signos a las que llamaremos *fórmulas.* En primer lugar definimos las *fórmulas atómicas* como las de la forma $x = y$ y $x \in y$. En segundo lugar establecemos unas reglas para construir nuevas fórmulas a partir de otras α y β ya construidas:

1. $\neg\alpha$ es una fórmula (y se lee no α). Pero en lugar de $\neg x \in y$, se suele escribir $x \notin y$.
2. $\alpha \to \beta$ es una fórmula (y se lee α implica β).
3. $\alpha \vee \beta$ es una fórmula (y se lee α o β).
4. $\alpha \wedge \beta$ es una fórmula (y se lee α y β).
5. $\alpha \leftrightarrow \beta$ es una fórmula (y se lee α si y sólo si β).
6. $\bigwedge x\, \alpha$ es una fórmula (y se lee para todo x, α).
7. $\bigvee x\, \alpha$ es una fórmula (y se lee existe un x tal que α).

Y nada más. Una fórmula es una cadena de signos que puede construirse a partir de fórmulas atómicas aplicando sucesivamente las reglas precedentes de construcción de fórmulas. Por ejemplo, ahora podemos expresar el axioma I de Zermelo mediante la fórmula:

$$\bigwedge XY(\bigwedge u(u \in X \leftrightarrow u \in Y) \to X = Y).$$

Aquí hay que leer:[40] para todos los conjuntos X, Y, si, para todo conjunto u, se cumple que u pertenece a X si y sólo si u pertenece a Y, entonces X es el mismo conjunto que Y.

Notemos que no hemos dotado a nuestro lenguaje de ningún signo que se interprete como "ser un conjunto", porque hemos adoptado el convenio de que todo es un conjunto. Así, $\bigwedge X$ y $\bigvee X$ significan "para todo conjunto X" y "existe un conjunto X", respectivamente. Nunca necesitamos aclarar que un objeto considerado es un conjunto. Si no lo fuera, no podríamos hablar de él en nuestro lenguaje.

El axioma II de Zermelo contiene en realidad tres afirmaciones independientes, de las cuales la segunda se deduce de la tercera. Ésta última, que afirma que, para cada par de conjuntos, existe otro que los tiene por elementos, se expresa mediante esta fórmula:[41]

$$\bigwedge xy\bigvee z\bigwedge u(u \in z \leftrightarrow u = x \vee u = y).$$

Aquí hay que leer: para todos los conjuntos x, y, existe un conjunto z tal que, para todo conjunto u, se cumple que u pertenece a z si y sólo si u es el conjunto x o u es el conjunto y.

[40] Deberíamos precisar el uso que hacemos de los paréntesis a la hora de construir fórmulas, pero no vamos a entrar aquí en esos detalles técnicos.

[41] La notación que estamos empleando es anacrónica. Si quisiéramos imitar el estilo de la época, nos encontraríamos con muchos dialectos. Por ejemplo, los que se inspiraban en Peano escribirían el axioma del par como:

$$(x)(y)\exists z(u)(u\,\epsilon\, z \equiv (u = x)(u = y)),$$

mientras que los seguidores de Schröder preferirían

$$\Pi_{xy}\Sigma_z\Pi_u(u\,\epsilon\, z = (u = x)(u = y)),$$

pero todo esto son variantes superficiales de la misma idea de fondo.

Conviene que introduzcamos ahora un concepto técnico que será necesario en varias ocaciones para hablar con la precisión requerida. En una fórmula como

$$P \equiv \bigwedge u(u \in x \to u \in y),$$

se dice que la variable u está *ligada* (por el cuantificador $\bigwedge$), mientras que las variables x, y están *libres,* en el sentido de que no están bajo el alcance de ningún cuantificador y, por lo tanto, carecen de una interpretación determinada. A menudo, para indicar que una fórmula P tiene libres las variables x, y se usa la notación $P(x, y)$ y en tal caso puede verse como una forma de expresar una propiedad general que pueden tener o no unos objetos dados x, y. En el ejemplo que hemos puesto, la fórmula $P(x, y)$ expresa que x es un subconjunto de y, cosa que se cumplirá o no según qué conjuntos tomemos como x e y.

Con esta notación, si luego escribimos, por ejemplo, $P(\mathbb{N}, \mathbb{R})$, con ello nos referimos a la fórmula que resulta de sustituir x por $\mathbb{N}$ e y por $\mathbb{R}$, que en este caso sería $\bigwedge u(u \in \mathbb{N} \to u \in \mathbb{R})$.

Las fórmulas sin variables libres se llaman *sentencias,* y son las únicas que tienen (o pretenden tener) un significado concreto, que no esté sujeto a qué valores damos a las variables libres.[42]

Y ahora es cuando estamos en condiciones de precisar el alcance del axioma III, que técnicamente deja de ser un axioma para convertirse en un *esquema axiomático,* es decir, una colección de infinitos axiomas. Para cada fórmula $P(u)$ del lenguaje de la teoría de conjuntos, la fórmula siguiente es un axioma (un caso particular del esquema de especificación):

$$\bigwedge X \bigvee Z \bigwedge u(u \in Z \leftrightarrow u \in X \wedge P(u)).$$

Aquí hay que leer: para todo conjunto X existe un conjunto Z tal que, para todo conjunto u, se cumple que u pertenece a Z si y sólo si u pertenece a X y cumple $P(u)$.

La diferencia es que ahora $P(u)$ no es "una propiedad" sino una fórmula del lenguaje de la teoría de conjuntos con la variable libre u, un concepto que puede definirse con absoluta precisión.[43] De hecho, una característica esencial de los lenguajes formales es que en ellos el concepto de "fórmula" y, en general, todos los conceptos relacionados con su gramática, con su sintaxis, se definen sin hacer referencia en absoluto al posible significado de sus signos, de modo que es fácil programar a un ordenador para que, si le damos una cadena de signos del lenguaje, nos diga si corresponde o no a una fórmula.

Por ejemplo, la justificación de que la versión formal que hemos dado del Axioma I de Zermelo es ciertamente una fórmula (una sentencia, de hecho) sería algo de este estilo:

1. Las cadenas de signos formadas por $\in$ o $=$ con dos variables son fórmulas atómicas por definición. Por ello $u \in X$, $u \in Y$, $X = Y$ son fórmulas.

2. Si tenemos dos fórmulas $u \in X$ y $u \in Y$, entonces $u \in X \leftrightarrow u \in Y$ es una fórmula por definición.

3. Si $u \in X \leftrightarrow u \in Y$ es una fórmula y u es una variable, entonces $\bigwedge u(u \in X \leftrightarrow u \in Y)$ es una fórmula por definición.

4. Si $\bigwedge u(u \in X \leftrightarrow u \in Y)$ y $X = Y$ son fórmulas, entonces $\bigwedge u(u \in X \leftrightarrow u \in Y) \to X = Y$ es una fórmula por definición.

5. Si $\bigwedge u(u \in X \leftrightarrow u \in Y) \to X = Y$ es una fórmula, también lo es $\bigwedge XY(\bigwedge u(u \in X \leftrightarrow u \in Y) \to X = Y)$, por definición (donde hemos adoptado el convenio de abreviar $\bigwedge X \bigwedge Y$ a $\bigwedge XY$).

[42] No obstante, en algunos contextos es costumbre (y es lícito) convenir que una fórmula con variables libres debe interpretarse igual que su *clausura universal,* es decir, la sentencia que resulta de cuantificar con $\bigwedge$ sus variables libres. Por ejemplo, el axioma I de Zermelo puede expresarse también como $\bigwedge u(u \in X \leftrightarrow u \in Y) \to X = Y$ siempre que entendamos que es equivalente a la forma en que lo hemos expresado antes, es decir, anteponiendo un $\bigwedge XY$.

[43] En realidad, la notación $P(u)$ expresa que la variable u está libre en P, pero no excluye (salvo que se diga lo contrario) que pueda tener otras variables libres a modo de parámetros. Por ejemplo, si tomamos $P(u) \equiv u \in Y$, el axioma III para esta fórmula es

$$\bigwedge X \bigvee Z \bigwedge u(u \in Z \leftrightarrow u \in X \wedge u \in Y),$$

donde hay que entender que la variable libre Y hace referencia a un conjunto general:

$$\bigwedge XY \bigvee Z \bigwedge u(u \in Z \leftrightarrow u \in X \wedge u \in Y),$$

y tenemos así el axioma que expresa la existencia de la intersección de dos conjuntos.

Lo que decíamos antes es que si tomamos cualquier enunciado matemático (como el teorema de Bolzano) y le vamos sustituyendo paulatinamente los conceptos definidos por sus definiciones, al final llegaremos a una enorme fórmula del lenguaje de la teoría de conjuntos, en la que no aparecerán más que variables, fórmulas atómicas del tipo $x = y$ o $x \in y$ y signos lógicos que las relacionen.

Ahora bien, también hay que destacar que lo que resulta decisivo para que una afirmación sea considerada como una afirmación matemática de pleno derecho es que pueda expresarse en el lenguaje de la teoría de conjuntos, lo cual no significa que sea buena idea hacerlo. De hecho, desde un punto de vista estilístico (e incluso didáctico) se considera desaconsejable emplear signos lógicos en el enunciado y la demostración de teoremas matemáticos salvo que haya algún motivo de peso para ello, lo cual sólo suele suceder si se trata de resultados sobre lógica y en algunos contextos —no todos— de la teoría de conjuntos. Entre:

> Se dice que una función $f : [a, b] \longrightarrow \mathbb{R}$ definida en un intervalo es continua en un punto x de su dominio si para todo $\epsilon > 0$ existe un $\delta > 0$ de modo que si $y \in [a, b]$ cumple $|y - x| < \delta$ entonces $|f(y) - f(x)| < \epsilon$.

y

$$\bigwedge fabx(a \in \mathbb{R} \wedge b \in \mathbb{R} \wedge f : [a, b] \to \mathbb{R} \wedge x \in [a, b] \to$$

$$(f \text{ es continua en } x \leftrightarrow \bigwedge \epsilon > 0 \bigvee \delta > 0 \bigwedge y \in [a, b](|y - x| < \delta \to |f(y) - f(x)| < \epsilon))),$$

el primer enunciado es mil veces preferible al segundo, en contra de lo que tienden a pensar algunos estudiantes posesos del espíritu de Peano que confunden el rigor con la pedantería. Fuera del contexto de la lógica, el concepto de lenguaje formal sirve para delimitar el uso legítimo de las lenguas naturales restringiéndolas a aquellas afirmaciones susceptibles de ser expresadas en un lenguaje formal, lo cual —repetimos— no significa que convenga hacerlo, sino que lo usual es que baste con saber que puede hacerse.

En la práctica, si cada vez que definimos un concepto lo hacemos en términos de la igualdad, la pertenencia y de conceptos ya definidos, tenemos la garantía de que todo lo que digamos al usar los conceptos que usemos podrá expresarse mediante una fórmula del lenguaje de la teoría de conjuntos sin más que ir sustituyendo los términos definidos por sus definiciones y, precisamente porque tenemos la garantía de que así será, no necesitamos hacerlo salvo que tengamos una buena razón para ello, cosa que rara vez sucede.

Volviendo a la paradoja de Berry, ahora podemos afirmar que, para que realmente pudiera llevarnos a demostrar una contradicción a partir de los axiomas de Zermelo, haría falta dar una definición de "número definible en castellano con menos de cien letras" expresable en el lenguaje de la teoría de conjuntos (o, si un buscador de contradicciones lo estima más prometedor, el de "número definible en el lenguaje de la teoría de conjuntos con menos de N signos", con el número N que considere oportuno"). Sin tal definición, no hay paradoja, y hay varios motivos que no podemos discutir aquí por los que no es posible dar tal definición: ser definible no es definible.

Concluimos, pues, que los axiomas de Zermelo (con la precisión de que la "propiedad" del axioma de especificación hay que entenderla como una fórmula de la teoría de conjuntos) nos libra de la paradoja de Berry y, en general, de las llamadas "paradojas semánticas", que no tienen que ver con multiplicidades inconsistentes, sino con las libertades que uno puede tomarse al usar lenguas naturales en lugar de lenguajes formales.

El lenguaje formal de la teoría de conjuntos es sólo un ejemplo. Podemos obtener muchos otros considerando otros signos no definidos en lugar de $\in$. Por ejemplo, el lenguaje formal de la aritmética de Peano tiene como signos no definidos los signos $0, S, +, \cdot$, que corresponden a los conceptos no definidos de "cero", "siguiente de", "suma" y "producto", a los que hay que añadir el concepto primitivo de "número natural", que no se plasma de ningún modo en el lenguaje formal porque en la aritmética de Peano todo son números naturales, y así, "para todo" y "existe" significan "para todo número natural" y "existe un número natural", respectivamente.

Este lenguaje nos permite expresar como sigue los llamados axiomas de la aritmética de Peano:

1. $\bigwedge mn(Sm = Sn \to m = n)$,
2. $\bigwedge m \neg Sm = 0$,
3. $\bigwedge m\, m + 0 = m$,
4. $\bigwedge mn\, m + Sn = S(m + n)$,

5. $\bigwedge m\, m \cdot 0 = 0$,
6. $\bigwedge mn\, m \cdot Sn = m \cdot n + n$.
7. $P(0) \wedge \bigwedge n(P(n) \to P(Sn)) \to \bigwedge n\, P(n)$,

donde, el axioma 7 (el principio de inducción) no es un axioma, sino un esquema axiomático: Para cada fórmula $P(n)$ del lenguaje de la aritmética (que puede tener otras variables libres, aparte de n, como parámetros) tenemos un axioma distinto, exactamente igual que sucede con el axioma de especificación de Zermelo.

Como el lector habrá observado, no se trata de los cinco axiomas que había enunciado Peano, porque, bajo el presupuesto de que todo es un número natural, no es necesario postular que 0 es un número natural ni que el siguiente de un número natural es otro número natural. En cambio, se añaden los axiomas que definen la suma y el producto porque, de este modo, a partir de estos axiomas es posible deducir toda la aritmética básica sin necesidad de ningún concepto conjuntista.

Similarmente podríamos definir otro lenguaje formal para expresar las afirmaciones de la geometría euclídea, el cual debería tener signos no definidos que signifiquen "es un punto", "es una recta", "es un plano", "x está entre a y b", etc.

33 La paradoja de Skolem El problema de la fundamentación de la matemática había hecho que unos cuantos matemáticos desempolvaran los libros de lógica. Lo que inicialmente se había visto como una mera recopilación de obviedades terminó demostrando que tenía bastante que aportar a la comprensión de las matemáticas. Así, en 1920 el matemático noruego Thoralf Skolem demostró un resultado que a los matemáticos les costaría un tiempo encajar. En realidad lo había demostrado ya en 1915 un matemático alemán, Leopold Löwenheim, pero su demostración era oscura y confusa, por lo que había pasado un tanto desapercibida. Para enunciarla, observemos en primer lugar que los axiomas de Zermelo, expresados como fórmulas del lenguaje de la teoría de conjuntos, no son más que afirmaciones sin un significado asignado. Nos dicen las propiedades básicas de los conjuntos, pero no sabemos especificar de qué estamos hablando cuando hablamos de conjuntos (ni cuando hablamos de la pertenencia entre conjuntos). Por lo tanto, es natural formularse esta pregunta:

> ¿Existen unos objetos que cumplan los axiomas de la teoría de conjuntos?

O, equivalentemente, ¿existen unos objetos de modo que si decimos: "cuando hablamos de conjuntos nos referimos a estos objetos", los axiomas de la teoría de conjuntos sean verdaderos?

En realidad la pregunta no es suficientemente precisa. Habría que decir:

> ¿Es posible fijar una colección M de objetos y definir en ellos una cierta relación R (de modo que, dados dos objetos de M, o bien se cumple $R(a, b)$, o bien no se cumple), y de modo que si decimos: "cuando hablamos de conjuntos nos referimos a los objetos de M y cuando decimos que un conjunto (un elemento a de M) pertenece a otro conjunto (a otro elemento b de M) nos referimos a que se cumple $R(a, b)$", entonces los axiomas de la teoría de conjuntos sean verdaderos?

O más concisamente:

> ¿Es posible atribuir un significado a los conceptos de "conjunto" (fijando unos objetos a los que llamar conjuntos) y "pertenencia" (estableciendo una relación entre tales objetos) de modo que los axiomas de la teoría de conjuntos sean verdaderos?

En general, fijado un lenguaje formal, con sus variables, sus signos lógicos y sus signos específicos no definidos, un *modelo*[44] de una colección de fórmulas de dicho lenguaje está determinado por una colección de objetos M, llamada *universo* del modelo y de una interpretación en M de cada uno de los signos no definidos, respecto a la cual las fórmulas dadas resultan ser verdaderas. Un *modelo* de una teoría axiomática es un modelo de sus axiomas.

Cuando los matemáticos razonan a partir de los axiomas de Zermelo (o de cualquier otra teoría axiomática), entienden que con ello están hablando de unos objetos que cumplen los axiomas, y que están demostrando que eso implica que también tienen que cumplir los teoremas que demuestran. Por eso, en un modelo de los axiomas de Zermelo, tienen que ser verdaderos, de hecho, todos los teoremas que se deducen de ellos.

[44] La palabra "modelo" en este sentido la introduciría Alfred Tarski más de tres décadas después, pero el concepto estaba ya implícito en el resultado de Löwenheim y Skolem.

El hecho de que no sean capaces de definir unos objetos que los cumplan no sugiere que no existan tales objetos. Así sucede, por ejemplo, con la geometría. Es imposible definir lo que es un punto o una recta, pero eso no impide que los puntos y las rectas a los que se refieren los axiomas de la geometría euclídea sean unos objetos perfectamente determinados, de modo que, cuando los axiomas se interpretan entendiendo que "punto" significa punto y "recta" significa recta, resultan verdaderos. Más aún, los matemáticos querrían que sus axiomas fueran categóricos, es decir, que no sólo admitieran un modelo, sino que no admitieran más que un único modelo. En el caso de los axiomas de la teoría de conjuntos, esto significaría que sólo hay unos posibles objetos a los que llamar "conjuntos" con una relación de pertenencia adecuada con los que los axiomas de la teoría de conjuntos resultan verdaderos.

Ahora ya podemos enunciar el teorema de Löwenheim-Skolem:

Si unos axiomas admiten un modelo, entonces admiten un modelo de universo numerable.

Aquí hay que entender que "numerable" no excluye que el universo pueda ser finito, pero si hablamos de modelos de la teoría de conjuntos, es fácil convencerse de que no pueden tener un universo finito, pues, por ejemplo, tiene que contener conjuntos distintos dos a dos que se correspondan con los números naturales de Zermelo:

$$0, \quad \{0\}, \quad \{\{0\}\}, \quad \{\{\{0\}\}\}, \quad \ldots$$

El teorema permaneció inadvertido durante un par de años, hasta que el propio Skolem lo promocionó en el *Quinto Congreso de Matemáticos Escandinavos* celebrado en Helsinki en **1922**, donde dio una charla titulada *Algunos comentarios sobre la teoría de conjuntos axiomatizada,* cuyo texto fue publicado en las actas del congreso. En este trabajo Skolem presentaba ocho críticas a la teoría axiomática de Zermelo. En la introducción dice:

> *La teoría de conjuntos, en su versión original, conduce, como sabemos, a ciertas contradicciones (antinomias), y nadie ha logrado hasta ahora presentar una resolución que haya ganado la aceptación general. A la vista de esta amenaza a la teoría de conjuntos, se han hecho intentos de desarrollar esta teoría mediante ciertos supuestos fundamentales, o axiomas, de modo que la parte que se supone que es correcta y útil permanece demostrable, mientras que las contradicciones son evitadas.*
>
> *Hasta ahora, hasta donde yo sé, sólo uno de estos sistemas ha encontrado aceptación general, a saber, el construido por Zermelo. Russell y Whitehead también han construido un sistema lógico que proporciona una fundamentación a la teoría de conjuntos. Sin embargo, si no me equivoco, los matemáticos han mostrado poco interés en él.*
>
> *En lo que sigue, por lo tanto, me centraré casi exclusivamente en la axiomatización de Zermelo, y tocaré la de Russell y Whitehead en una única ocasión, aunque una de gran importancia.*

La crítica número 2 era el hecho de que Zermelo no había definido adecuadamente el concepto de "propiedad bien definida". A este respecto dice:

> *Un punto muy deficiente en Zermelo es la noción de "propiedad bien definida". Probablemente nadie encontrará satisfactorias las explicaciones de Zermelo al respecto, pero, hasta donde yo sé, nadie ha intentado dar una formulación estricta de esta noción. Esto es muy extraño, ya que puede hacerse muy fácilmente.*

Lo que hace Skolem a continuación es esencialmente dar la definición de lo que es una fórmula del lenguaje de la teoría de conjuntos que hemos descrito anteriormente, y señalar que basta tomar como "propiedades" las que se pueden expresar mediante fórmulas de dicho lenguaje, tal y como ya hemos visto.

La crítica número 4 era la demostración de que los axiomas de Zermelo no bastaban para construir determinados conjuntos que requería la teoría de conjuntos, pues, por ejemplo, no permitían demostrar el principio de recursión transfinita. No obstante, Skolem proponía un axioma adicional, de hecho un esquema axiomático, que a su vez permitía demostrar el esquema axiomático de especificación de Zermelo, con el que se resolvía este inconveniente.

Lo que no sabía Skolem era que el año anterior Abraham Fraenkel había mantenido una intensa correspondencia con Zermelo que culminó en un artículo que Fraenkel había enviado a una revista para su publicación el año anterior y que aparecería publicado ese año, en el cual precisó el concepto de "propiedad bien definida" esencialmente igual que Skolem y propuso el mismo axioma que proponía Skolem con el nombre de *Axioma del reemplazo.*

Pero la crítica más sonada fue la número 3, en la que daba una nueva demostración del teorema de Löwenheim-Skolem y destacaba sus implicaciones sobre la teoría de conjuntos. Skolem había demostrado que, supuesto que existan unos objetos que cumplen los axiomas de la teoría de conjuntos, es posible encontrar un conjunto numerable de objetos, digamos $c_0, c_1, c_2, \ldots$ en los que se puede definir una relación de pertenencia R, de modo que si llamamos "conjuntos" a esos objetos (ni más ni menos) y consideramos en ellos la relación de pertenencia R, se cumplen todos los axiomas de la teoría de conjuntos. En sus propias palabras:

> *Hasta donde yo sé, nadie ha llamado la atención sobre este peculiar y aparentemente paradójico estado de cosas: En virtud de los axiomas podemos demostrar la existencia de cardinales superiores, etc. ¿Cómo puede ser, entonces, que todo el universo* [de un modelo numerable de los axiomas] *pueda enumerarse con los números naturales finitos? La explicación no es difícil de encontrar.*

Vamos a tratar de encontrarla con más detalle del que daba Skolem. Suponemos, pues, que tenemos unos objetos $c_0, c_1, c_2, \ldots$ junto con una relación de pertenencia R de modo que, llamando "conjuntos" a esos objetos e interpretando la relación de pertenencia como R, se cumplen todos los axiomas de la teoría de conjuntos.

A partir de dichos axiomas se puede demostrar la existencia del conjunto $\mathbb{N}$ de los números naturales, luego uno de los "conjuntos" c_i tiene que ser "el conjunto de los números naturales" (el que satisface la definición de $\mathbb{N}$). Reordenando la sucesión, podemos suponer que es c_1.

Por otra parte, reordenando de nuevo la sucesión, podemos suponer que los (infinitos) conjuntos que cumplen la propiedad de ser un número natural son

$$c_2, \quad c_4, \quad c_8, \quad c_{16}, \quad \ldots$$

Más concretamente, podemos suponer que c_2 es el conjunto que satisface la definición de número 0, mientras que c_4 es el único conjunto que satisface la definición de número 1 y c_8 es el único conjunto que satisface la definición de número 2, etc. (recordemos que, en una teoría de conjuntos, todos los conceptos matemáticos, incluidos los números naturales, se definen como ciertos conjuntos). Más específicamente, como a partir de los axiomas de la teoría de conjuntos se puede demostrar que $0 \in \mathbb{N}$, en este modelo tiene que cumplirse $R(c_2, c_1)$, e igualmente $R(c_4, c_1)$, etc.

Por otro lado, a partir de los axiomas de la teoría de conjuntos se demuestra que existe el conjunto $\mathcal{P}\mathbb{N}$ de todos los subconjuntos de $\mathbb{N}$, luego tiene que haber un "conjunto" c_i que cumpla la definición de $\mathcal{P}\mathbb{N}$. Reordenando los índices podemos suponer que se trata de c_0. Y, con otra reordenación, podemos suponer además que los (infinitos) conjuntos que cumplen la propiedad de ser un subconjunto de $\mathbb{N}$ son

$$c_1, \quad c_3, \quad c_9, \quad c_{27}, \quad c_{81}, \quad \ldots$$

Así, por ejemplo, podría ser que c_3 fuera el conjunto de los números naturales pares, y c_9 el conjunto de los números menores que 100, y c_{27} el conjunto de los números primos, y c_{81} el conjunto $\{0, 7, 17\}$, etc., pero los únicos c_i que cumplen la definición de subconjunto de $\mathbb{N}$ son los de la forma c_{3^j}, para cierto j.

Ahora bien, a partir de los axiomas de la teoría de conjuntos se demuestra que el conjunto $\mathcal{P}\mathbb{N}$ no es numerable, y como los "conjuntos" c_i cumplen dichos axiomas, tiene que ser cierto que el conjunto c_0 cumple la definición de conjunto no numerable. ¿Pero cómo puede c_0 ser no numerable si sus elementos son $c_1, c_3, c_9, \ldots$, que ciertamente pueden ponerse en correspondencia biunívoca con los números naturales haciendo $i \mapsto c_{3^i}$?

Aparentemente, nos encontramos ante una nueva paradoja, pero una que los axiomas de Zermelo no resuelven. Podemos demostrar que existe un conjunto que es a la vez numerable y no numerable. Sin embargo, cuando Skolem preguntaba cómo era esto posible, lo hacía por enfatizar lo curioso de la situación, porque él conocía la respuesta y la explicó en su artículo. En realidad la "paradoja de Skolem" no es ninguna paradoja. No hay ninguna contradicción en ella. Es algo sorprendente, pero no contradictorio.

Para entender la situación debemos recordar el concepto cantoriano de "conjunto no numerable". En principio, que un conjunto (infinito) sea no numerable significa que no es posible emparejar los números naturales con sus elementos sin repeticiones y sin que sobre ningún elemento, pero ahora conviene expresar esto así:

> Un conjunto infinito X es no numerable si no existe ningún emparejamiento que a cada elemento de $\mathbb{N}$ le asigne uno de X sin repeticiones y sin que sobren elementos en X.

La diferencia fundamental es que, en lugar de decir "no es posible emparejar", lo hemos cambiado por "no existe un emparejamiento". ¿Por qué es esto relevante? Porque "un emparejamiento" es un concepto matemático. Se trata de si existe un objeto matemático, y ese objeto matemático, como cualquier otro, tiene que ser un conjunto. Por lo tanto, ahora es fundamental entender cómo se plasma en términos de conjuntos el concepto de "emparejamiento".

Consideremos dos conjuntos a, b. El axioma II de Zermelo nos asegura que existen los conjuntos $\{a\}$ y $\{a, b\}$, que tienen por elementos sólo a a y sólo a a, b, respectivamente. Aplicando nuevamente el axioma II a estos dos conjuntos, obtenemos que existe el par ordenado $(a, b) = \{\{a\}, \{a, b\}\}$ que los tiene por elementos (según la definición de Kuratowski). A partir de este concepto podemos definir el concepto de *biyección* f entre dos conjuntos X e Y como un conjunto de pares ordenados (a, b) con $a \in X$ y $b \in Y$, con la propiedad de que para cada $a \in X$ existe un único $b \in Y$ tal que $(a, b) \in f$, y viceversa.

Por ejemplo, el conjunto f formado por los pares (n, n^2), donde $n \in \mathbb{N}$, constituye una biyección entre el conjunto de los números naturales y el conjunto de los cuadrados perfectos, y demuestra que éste es numerable.

En estos términos, en la teoría de conjuntos se dice que un conjunto infinito X es *no numerable* si no existe ninguna biyección entre $\mathbb{N}$ y X. Ésta es la versión conjuntista del concepto cantoriano de no numerabilidad.

Volviendo a nuestro modelo numerable, para probar que $\mathcal{P}\mathbb{N}$ (es decir, c_0) es numerable en el modelo no nos sirve el emparejamiento $i \mapsto c_{3^i}$, sino que tenemos que emparejar los números naturales del modelo (es decir, los conjuntos c_{2^i}) con los subconjuntos de $\mathbb{N}$ del modelo. Una posibilidad sería $c_{2^i} \mapsto c_{3^{i-1}}$, para $i \geq 1$.

Puesto que c_{2^i} y $c_{3^{i-1}}$ son conjuntos, y en la teoría de conjuntos se demuestra que, para cada par de conjuntos, existe el par ordenado formado por ellos, tiene que existir un c_j que satisfaga la definición de par ordenado con primera componente c_{2^i} y segunda componente $c_{3^{i-1}}$. Reordenando los índices podemos suponer que se trata de c_{5^i}, es decir, que c_5 es el conjunto que satisface la definición de par ordenado $(0, \mathbb{N})$, mientras que c_{25} es el conjunto que satisface la definición de par ordenado $(1, P)$, donde P es el conjunto de los números naturales pares (si es que suponemos, por ejemplo, que c_3 es dicho conjunto), etc.

En tal caso, los conjuntos $c_5, c_{25}, c_{125}, \ldots$ serían una colección de pares ordenados que pondrían en correspondencia biunívoca los números naturales del modelo numerable que estamos considerando con los subconjuntos de $\mathbb{N}$ de dicho modelo. Y aquí viene el punto crucial: con esto ¡no hemos demostrado que en el modelo $\mathcal{P}\mathbb{N}$ sea numerable! Para que así fuera, necesitaríamos que existiera una biyección f entre $\mathbb{N}$ y $\mathcal{P}\mathbb{N}$, es decir, entre c_1 y c_0, pero, ¿dónde está esa biyección? Lo que hemos encontrado es la sucesión de pares ordenados

$$c_5, \quad c_{25}, \quad c_{125}, \quad \ldots$$

pero eso NO es una biyección. Una biyección tiene que ser un conjunto f y ¿cuál sería? Si existiera un conjunto, por ejemplo c_7, con la propiedad de que los conjuntos c_i que cumplen $R(c_i, c_7)$ fueran justamente los c_{5^i}, para $i \geq 1$, entonces sí que podríamos decir que c_7 es una biyección entre $\mathbb{N}$ y $\mathcal{P}\mathbb{N}$ que prueba que $\mathcal{P}\mathbb{N}$ es numerable, ¿pero quién nos asegura que c_7 cumpla eso? Al contrario, Skolem había demostrado que existe el modelo numerable que estamos considerando, y eso implica que ni c_7 ni ningún otro c_j puede tener por elementos a la sucesión de pares c_{5^i}, ni a ninguna otra sucesión de pares que ponga en correspondencia biunívoca a los elementos de c_1 con los elementos de c_0. En resumen:

> En un modelo numerable de los axiomas de Zermelo (o de cualquier teoría de conjuntos), existe una cantidad numerable de subconjuntos de $\mathbb{N}$ (o de números reales, etc.), pero el conjunto $\mathcal{P}\mathbb{N}$ (o $\mathbb{R}$, etc.) es no numerable, porque, aunque existan colecciones de pares ordenados que pongan en correspondencia biunívoca los elementos de $\mathbb{N}$ con los de $\mathcal{P}\mathbb{N}$, no existe ningún conjunto en el modelo que tenga por elementos a ninguna de dichas colecciones, por lo que en el modelo no existen biyecciones entre $\mathbb{N}$ y $\mathcal{P}\mathbb{N}$.

Más explícitamente: si llamamos "conjuntos" a los objetos c_i cuya existencia había demostrado Skolem (supuesto que la teoría de conjuntos admita un modelo), entonces la colección de conjuntos $c_5, c_{25}, c_{125}, \ldots$ es un ejemplo de colección de conjuntos que NO es un conjunto. Y así tenemos una muestra más de la inviabilidad de identificar "conjunto" con "colección de conjuntos".

Quizá ahora el lector pueda entender las palabras originales de Skolem:

> *La explicación no es difícil de encontrar. En la axiomática, "conjunto" no significa una colección arbitrariamente definida; los conjuntos no son sino objetos conectados entre sí a través de ciertas*

> *relaciones expresadas por los axiomas. Por lo tanto no hay contradicción alguna si un conjunto M del dominio B* [del universo del modelo] *no es numerable en el sentido de la axiomática; pues esto significa meramente que dentro de B* [del modelo] *no hay ninguna biyección de M en el conjunto de los enteros positivos de Zermelo* [el conjunto de los conjuntos que Zermelo define como números naturales]. *Sin embargo, nada impide que se pueda numerar B, y por lo tanto M mediante los enteros positivos. Por supuesto, tal enumeración será una colección de ciertos pares, pero dicha colección no será un "conjunto" (es decir, no aparecerá en el dominio B).*

Skolem expresó esto diciendo que, en su modelo, $\mathcal{P}\mathbb{N}$ era *relativamente* no numerable, es decir, no numerable con respecto al modelo, pero absolutamente numerable.

La idea es que la numerabilidad de un conjunto es "relativa a su entorno", es decir, relativa a qué colecciones de objetos estamos considerando como conjuntos. Un conjunto X es numerable si existe una biyección entre $\mathbb{N}$ y X, pero dicha f es algo externo al propio X. Un mismo conjunto X puede formar parte de un modelo en el que exista tal f, y entonces es numerable relativamente a dicho modelo, pero también formar parte de otro modelo en el que no exista tal f (en el que f sea una colección que no es un conjunto), y entonces será no numerable relativamente a dicho otro modelo.

Más aún, Skolem apuntó que incluso la noción de finitud podía ser relativa a un modelo, al menos si definimos, como había propuesto Dedekind, que un conjunto es finito si no se puede biyectar con un subconjunto propio. Skolem plantea que podría ocurrir que un conjunto sea infinito, pero que las biyecciones con subconjuntos propios que probarían que lo es podrían no corresponderse con ninguno de los conjuntos de un modelo, y entonces sería un conjunto absolutamente infinito, pero finito relativamente al modelo.

Skolem también destacaba que estos argumentos no dependían de que los axiomas de Zermelo fueran concretamente los que eran, sino que se aplicaban igualmente sin cambio alguno a cualquier teoría de conjuntos.

En su crítica número 6, Skolem razona que es imposible que los axiomas de la teoría de conjuntos determinen un único modelo, sino que a partir de un modelo es capaz de construir otro con más conjuntos. Y de ahí especula con que, si hay distintos modelos, que pueden tener características distintas, pero de modo que todos cumplen los mismos axiomas básicos, no sería extraño que muchos problemas no pudieran ser decididos a partir de los axiomas y que, por ejemplo, la hipótesis del continuo no pudiera demostrarse ni refutarse, porque podría haber unos modelos de la teoría de conjuntos en los que fuera verdadera y otros en los que fuera falsa.

La crítica número 5 se refería a la impredicatividad de los axiomas de la teoría de conjuntos:

> *Presumiblemente, aún no se ha demostrado que el sistema axiomático de Zermelo sea consistente, y sin duda será muy difícil hacerlo. En particular, las estipulaciones no predicativas que rigen la formación de conjuntos causarán dificultades. No es descabellado pensar en los axiomas como principios generadores de algún tipo; generamos nuevos conjuntos según ciertas reglas a partir de conjuntos ya conocidos. Si, ahora, la formación de conjuntos fuera una mera cuestión de construir cada nuevo conjunto únicamente a partir de un número finito de conjuntos anteriores, podríamos fácilmente verificar, a través de un proceso infinito, si los axiomas son consistentes. Pero la dificultad es que tenemos que formar algunos conjuntos cuya existencia depende de* todos *los conjuntos. Entonces tenemos lo que se llama una definición no predicativa. Poincaré criticó este tipo de definición y la consideró la verdadera debilidad lógica de la teoría de conjuntos.*
>
> *En el sistema de Russell y Whitehead, este punto ha sido formalmente tenido en cuenta, a saber, en la teoría de lo que ellos llaman los tipos lógicos, pero ellos también se contentan simplemente con sortear la dificultad introduciendo una estipulación, el axioma de reducibilidad. En realidad, este axioma decreta que las estipulaciones no predicativas serán satisfechas. No hay prueba de ello.*

La crítica número 8 tenía que ver con el axioma de elección y su naturaleza no constructiva:

> *Mientras nos movamos en el terreno puramente axiomático no hay, por supuesto, nada especial que señalar sobre el principio de elección (aunque, de hecho, la aplicación de este axioma no genera nuevos conjuntos unívocamente); pero si muchos matemáticos —de hecho, yo creo que la mayoría— no quieren aceptar el principio de elección, es porque no tienen en absoluto una concepción axiomática de la teoría de conjuntos. Piensan en los conjuntos como dados por especificación a partir de colecciones arbitrarias; pero luego piden también que cada conjunto sea definible. Después de todo, podemos preguntar: ¿Qué significa que un conjunto exista si tal vez nunca pueda ser definido?*

> *Parece claro que esta existencia sólo puede ser una manera de hablar, que sólo puede conducir a proposiciones puramente formales —tal vez hechas de muy hermosas palabras— sobre los objetos llamados conjuntos. Pero muchos matemáticos quieren matemáticas para tratar, en última instancia, con operaciones computacionales realizables, y no que consistan en proposiciones formales sobre unos objetos llamados así o asá.*

Skolem termina señalando que ya había comunicado oralmente sus argumentos que probaban que muchos conceptos conjuntistas son relativos al modelo considerado hacía siet años, pero que no había publicado nada al respecto hasta entonces por dos razones:

> *Primero, que este tiempo he estado ocupado con otros problemas y, segundo, que yo creía que era tan claro que la axiomatización en términos de conjuntos no era una fundamentación última satisfactoria de las matemáticas que los matemáticos, en su mayor parte, no se interesarían por ella. Pero en los últimos tiempos he visto, para mi sorpresa, que muchos matemáticos piensan que esos axiomas de la teoría de conjuntos proporcionan la fundamentación ideal de las matemáticas. Por ello, me pareció que había llegado el momento de hacer pública una crítica.*

Zermelo y su escuela recibieron mal el resultado de Skolem. La prueba era complicada (las demostraciones actuales son mucho más sencillas) y durante un tiempo Zermelo estuvo convencido de que debía de estar mal. Cuando se vio obligado a admitir que era correcta, cuestionó la lógica empleada por Skolem.[45]

34 Finitismo, platonismo e intuicionismo Zermelo y Skolem tenían visiones opuestas sobre la filosofía de la matemática. Zermelo era platonista, pues creía que existe una realidad objetiva formada por lo que llamamos "conjuntos" y que los axiomas de la teoría de conjuntos son afirmaciones verdaderas sobre tales conjuntos, igual que los axiomas de la geometría euclídea son afirmaciones verdaderas sobre los puntos, rectas y planos intuitivos.

Por ejemplo, decir que por un mismo punto no pueden pasar más de tres rectas perpendiculares dos a dos es una afirmación verdadera sobre la geometría intuitiva, sin perjuicio de que tenga interés estudiar también geometrías de cuatro dimensiones o no euclídeas, cuyos postulados serán intuitivamente falsos (aunque esto sea irrelevante). Por lo tanto, los teoremas de la teoría de conjuntos son afirmaciones verdaderas sobre los conjuntos. Si se demuestra que $\mathbb{R}$ o $\mathcal{P}\mathbb{N}$ no son numerables, es porque no son numerables.

Por el contrario, Skolem era *finitista,* es decir, que consideraba que existen los conjuntos finitos y, hasta cierto punto, podemos hablar de conjuntos infinitos numerables. Por ejemplo, podemos afirmar que existen infinitos números naturales, pero eso sólo significa que, si estamos razonando con un conjunto (finito) de números naturales, siempre podremos considerar uno más, nunca diremos "aquí ya están todos". En cambio, para Skolem los conjuntos no numerables no eran más que una ficción y consideraba que "su paradoja" lo ponía de manifiesto. Para Skolem, la demostración del teorema de Cantor no era válida porque partía del presupuesto de que hemos logrado numerar todos los subconjuntos de $\mathbb{N}$, lo cual ya es de por sí un sinsentido, ya que una cosa es ir construyendo subconjuntos de $\mathbb{N}$, digamos $A_0, A_1, A_2, \ldots$ y otra cosa pretender que ya tenemos completada la sucesión infinita y seguir razonando a partir de ahí. Si no existe ninguna noción objetiva de "conjunto infinito" (y mucho menos de "conjunto no numerable"), en el supuesto de que existan unos objetos que cumplan los axiomas de la teoría de conjuntos, lo que cabe esperar es que la no numerabilidad de $\mathcal{P}\mathbb{N}$ no sea más que lo que sucede en el modelo numerable de Skolem, un mero "truco de ilusionista": nos parece que $\mathcal{P}\mathbb{N}$ es no numerable porque, en el modelo, no vemos las biyecciones que lo numeran, igual que cuando un ilusionista nos hace creer que estamos viendo una bola que flota en el aire, nos lo parece porque no vemos los hilos que la sujetan.

En suma, Skolem consideraba que una fundamentación razonable de las matemáticas debía tratar moderadamente con conjuntos infinitos y debía descartar definitivamente cualquier conjunto no numerable (lo cual no significaba que no se pudiera hablar de números reales, por ejemplo, pero que plantearse si son o no numerables debía ser un sinsentido que no tuviera cabida en la teoría).

En **1923** Skolem publicó un artículo titulado *Los fundamentos de la aritmética elemental establecidos mediante el modo de pensamiento recursivo sin el uso de variables que recorran conjuntos infinitos.* En él establecía una versión de lo que más adelante se conocería como *Aritmética Recursiva Primitiva* (ARP), y que muchos consideran que puede tomarse como una definición precisa del finitismo: un razonamiento es finitista si y sólo

[45] No es éste buen momento para explicar esto, pero Skolem estaba razonando con un lenguaje formal de primer orden, y Zermelo consideró que lo adecuado (es decir, la forma de evitar la paradoja) era considerar un lenguaje formal de segundo orden. Sin embargo, por razones que no es posible detallar aquí, las objeciones de Zermelo no cuajaron, y hoy en día la teoría de conjuntos se sigue considerando como una teoría axiomática de primer orden.

si puede llevarse a cabo en la ARP. Quienes discrepan de esta afirmación lo hacen porque consideran que hay argumentos no expresables en la ARP, pero que igualmente merecen ser considerados finitistas. Nadie cuestiona, en cambio, que todos los argumentos expresables en la ARP sean finitistas.

Frente a estos dos extremos, Brouwer seguía desarrollando su intuicionismo, según el cual si tenía sentido hablar de conjuntos infinitos, pero sólo desde el marco lógico intuicionista. Ese año publicó el artículo *Sobre la importancia del tercio excluso en matemáticas, especialmente en la teoría de funciones,* en cuya introducción resume su planteamiento:

> *Se atribuyó un carácter* a priori *tan consistentemente a las leyes de la lógica teórica que hasta hace poco estas leyes, incluido el principio del tercio excluso, se aplicaron sin reservas incluso en la matemática de los sistemas infinitos, y no dejamos que nos perturbara la consideración de que los resultados obtenidos de esta manera no están en general abiertos, ni práctica ni teóricamente, a ninguna corroboración empírica. Sobre esta base se construyeron extensas teorías incorrectas, especialmente en el último medio siglo. Las contradicciones que repetidamente se encontraron como consecuencia de ello dieron lugar a la crítica formalista, una crítica que en esencia se reduce a esto: el lenguaje que acompaña a la actividad mental matemática está sujeto a un examen matemático. A tal examen, las leyes de la lógica teórica se presentan como operadores que actúan sobre fórmulas primitivas o axiomas, y uno se propone transformar estos axiomas de tal manera que el efecto lingüístico de los operadores mencionados (que se conservan sin cambios) ya no pueda ser perturbado por la aparición de la figura lingüística de una contradicción. No tenemos motivos en absoluto para desesperar de que este objetivo pueda ser alcanzado, pero nada de valor matemático se ganará así: una teoría incorrecta, incluso si no puede ser inhibida por ninguna contradicción que la refute, no es menos incorrecta, al igual que una política criminal no es menos criminal incluso si no puede ser inhibida por ningún tribunal que la frene.*

Por esta época la relación entre Hilbert y Brouwer era casi tan tensa como lo había sido la relación entre Kronecker y Cantor.

35 La teoría de von Neumann Hilbert tenía entonces 61, y había creado una escuela de colaboradores interesados en la fundamentación de las matemáticas, entre los que destacaban Paul Bernays (de 35 años), Wilhelm Ackermann (de 27 años) y un joven húngaro de 20 años nacido como Neumann János Lajos, pero cuando el emperador Francisco José de Austria-Hungría concedió un título nobiliario a su padre, germanizó su nombre a Johann von Neumann.[46]

En **1923** von Neumann publicó un artículo titulado *Sobre la introducción de los números transfinitos* en el que resolvía un problema técnico en la formalización de la teoría de ordinales.

Por ejemplo, ese año, un estudiante de doctorado de Sierpiński de 22 años llamado Alfred Tajtelbaum se convirtió del judaísmo al catolicismo y cambió su nombre por el de Alfred Tarski. Tarski leería su tesis al año siguiente, en 1924, y ese mismo año publicó un artículo titulado *Sobre ciertos teoremas que equivalen al axioma de elección,* en el que demostraba que varias afirmaciones eran equivalentes al axioma de elección, entre ellas la validez, para todos los cardinales infinitos, de cualquiera de estas tres afirmaciones:

1. $\mathfrak{m} \cdot \mathfrak{n} = \mathfrak{m} + \mathfrak{n}$.
2. $\mathfrak{m} = \mathfrak{m}^2$.
3. Si $\mathfrak{m}^2 = \mathfrak{n}^2$, entonces $\mathfrak{m} = \mathfrak{n}$.

Tarski empezaba en estos términos:

> *La demostración se basará en el sistema de axiomas del Sr. Zermelo, naturalmente sin el axioma de elección. Agrego, sin embargo, a estos axiomas los dos axiomas siguientes, que introducen la noción de número cardinal:*
>
> 1. *A todo conjunto le corresponde un objeto que es su número cardinal.*
> 2. *Para que dos conjuntos cualesquiera sean de la misma potencia, es necesario y suficiente que les corresponda el mismo número cardinal.*

[46] Unos años más tarde emigraría a los Estados Unidos, y allí se haría llamar John von Neumann, que es como se le conoce en la actualidad.

¿Por qué necesitaba Tarski añadirle dos axiomas a la teoría de Zermelo? Porque sucede que en la teoría de Zermelo no había una forma satisfactoria de definir los ordinales y los cardinales.

En la teoría de Cantor cada ordinal representa una forma de ordenar bien un conjunto. En los *Principia Mathematica,* esto se expresaba definiendo los ordinales como clases de equivalencia de conjuntos bien ordenados. Por ejemplo, el ordinal ω estaba formado por todos[47] los conjuntos bien ordenados con el mismo tipo de orden que el conjunto de los números naturales, pero esta definición no era viable en la teoría de Zermelo, porque el "conjunto de todos los conjuntos ordenados como el conjunto de los números naturales" era una de las "multiplicidades inconsistentes" que a partir de los axiomas de Zermelo se podía demostrar que no existían.

Lo mismo sucedía con los cardinales. En los *Principia,* el cardinal 1 estaba formado por todos los conjuntos con un elemento, pero en la teoría de Zermelo se podía demostrar que no existe ningún conjunto que contenga a todos los conjuntos con un elemento. No había inconveniente en definir cuándo dos conjuntos tienen el mismo cardinal, o cuando un conjunto tiene cardinal 1, o $\aleph_{17}$, pero no había una forma obvia de precisar a qué conjunto en concreto llamar 1 o $\aleph_{17}$.

Esto fue lo que resolvió von Neumann al definir los ordinales como los conjuntos bien ordenados por la relación de pertenencia. Von Neumann pudo demostrar que sólo existe un conjunto así para cada forma posible de ordenar bien un conjunto, y eso justificaba que se los considerara como ordinales por definición.

En el sentido de von Neumann, el ordinal 0 no era sino el conjunto vacío; el ordinal 1 no era sino el conjunto $1 = \{0\}$, el ordinal 2 no era sino $2 = \{0, 1\}$ y, en general, cada ordinal coincidía con el conjunto de los ordinales menores que él mismo. Por ejemplo, ω, el menor ordinal infinito, no era sino el conjunto de todos los ordinales finitos (que von Neumann identificaba con los números naturales). Similarmente:

$$\omega + 3 = \{0, \quad 1, \quad 2, \quad \ldots \quad \omega, \quad \omega + 1, \quad \omega + 2\}.$$

A su vez, von Neumann definía los cardinales como lo que llamaba *ordinales iniciales,* es decir, los ordinales no biyectables con ningún ordinal anterior.

Con esta definición, todos los ordinales finitos eran también cardinales, mientras que ω, el mejor ordinal infinito, era, por definición, el cardinal $\aleph_0$. Los ordinales $\omega + 1, \omega + 2$, etc. no son cardinales, porque son numerables, es decir, se pueden biyectar con ω, que es anterior a ellos. El cardinal $\aleph_1 = \omega_1$ es el menor ordinal no numerable, al que le siguen muchos ordinales que no son cardinales, porque tienen cardinal $\aleph_1$, como $\omega_1 + 1$, $\omega_1 + 2$ o $\omega_1 + \omega$. El cardinal $\aleph_2 = \omega_2$ está por encima de todos ellos, y es, por definición, el menor ordinal cuyo cardinal es mayor que $\aleph_1$, y así sucesivamente. En general, cada cardinal κ es un conjunto de cardinal κ.

Estas definiciones no tardaron en ser universalmente aceptadas, pues resolvían el único gran problema técnico (la definición de los ordinales y los cardinales) que obligaba a hacer malabarismos para trabajar con los axiomas de Zermelo (una vez se había incorporado a éstos el axioma del reemplazo).

No obstante, esto no ayudaba a Tarski para su artículo de **1924**, porque los cardinales infinitos de von Neumann eran únicamente los álefs. Un conjunto X tiene cardinal κ si y sólo si existe una biyección entre X y κ y, como κ es un ordinal, y está bien ordenado, esto implica que los únicos conjuntos que tienen un cardinal (de von Neumann) son los conjuntos que admiten un buen orden. Si no suponemos el axioma de elección, todavía necesitamos una definición del cardinal de un conjunto en términos de "el (inexistente) conjunto de todos los conjuntos biyectables con él" y por ello Tarski tuvo que introducir sus dos axiomas adicionales.

Hugo Steinhaus se había doctorado en 1911 bajo la dirección de Hilbert. Un día de 1916 paseaba por un parque de Cracovia cuando vio a dos jóvenes sentados en un banco y oyó que uno pronunciaba las palabras "la integral de Lebesgue". Intrigado por que alguien supiera qué era eso, se acercó, se presentó y entabló conversación con ellos. El más joven era Stefan Banach (de 24 años) y el otro Otto Nykodym (de 29), que había completado sus estudios de matemáticas, mientras que Banach estaba estudiando ingeniería, pero siempre había tenido interés por las matemáticas y estaba aprendiendo de forma autodidacta. Así se inició una fructífera colaboración entre Banach y Steinhaus que probablemente cambió la vida del primero. Banach se doctoró en 1921 bajo la dirección de Steinhaus. En su tesis *Sobre las operaciones en conjuntos abstractos y sus aplicaciones a las ecuaciones integrales* introdujo el concepto que unos años más tarde Fréchet denominaría *espacio de Banach,* lo que a su vez llevaría a Banach a acuñar el concepto de *espacio de Fréchet* para una clase de espacios similares.

[47] Esto no es exactamente así, debido a las características de la lógica de tipos de los *Principia,* pero la idea de fondo era ésa.

En **1924** Banach y Tarski publicaron el artículo *Sobre la descomposición de conjuntos de puntos en partes respectivamente congruentes,* en el que desarrollaron la "paradoja de Hausdorff" y le dieron una forma más impactante que hoy se conoce como la *paradoja de Banach-Tarski,* aunque, como en el caso de la paradoja de Hausdorff, no es una contradicción, sino únicamente un teorema insólito que depende esencialmente del axioma de elección:

> Es posible tomar una esfera (maciza, no una mera superficie) de radio unitario, descomponerla en un número finito de partes (más adelante se vio que cinco son suficientes), mover estas partes sin deformarlas, y reorganizarlas adecuadamente en otra posición, de modo que con algunas de las partes se forme una esfera (maciza) idéntica a la primera y con las restantes se forme otra más.

El "truco" está en que esas partes tienen que ser una especie de "nubes de puntos" que no son medibles Lebesgue, ni medibles respecto de cualquier medida invariante por movimientos, por lo que no se les puede asignar un volumen que tenga que ser conservado por los movimientos. Por ello no cabe pensar en la existencia de objetos físicos reales con las formas necesarias para "poner en práctica" la paradoja.

En **1925** von Neumann publicó un artículo titulado *Una axiomatización de la teoría de conjuntos,* en el que presentaba unos axiomas muy diferentes a los de Zermelo. Era muy peculiar, porque en lugar de partir de los conceptos no definidos de "conjunto" y "pertenencia" tenía tres conceptos no definidos, por una parte había dos clases de objetos "argumentos" y "funciones" y por otra una operación no definida que llamaba "aplicación de funciones", en virtud de la cual, si f era una función y a era un argumento, entonces $[f, a]$ era otro argumento.[48] Un mismo objeto podía ser a la vez función y argumento, en cuyo caso se llamaba "argumento-función".

Por ejemplo, su versión del axioma de extensionalidad decía que si dos funciones asignan la misma imagen a cada elemento, entonces son iguales.

A partir de estos conceptos primitivos, von Neumann definía los conceptos de "conjunto" y "pertenencia", pero además introducía un concepto de "clase" que se correspondía con las multiplicidades inconsistentes de Cantor, que de este modo, dejaban de estar proscritas de la teoría de conjuntos.

Los conjuntos eran (algunas) colecciones de conjuntos y las clases también eran colecciones de conjuntos. Una clase nunca podía pertenecer a otra clase. En estos términos, los axiomas de von Neumann permitían definir la clase V de todos los conjuntos, o la clase Ω de todos los ordinales, o la clase R de todos los conjuntos que no se pertenecen a sí mismos, pero ninguna de ellas daba lugar a contradicción alguna (conocida).

Por ejemplo, la clase R cumple que $R \notin R$, pero eso no nos lleva a concluir que $R \in R$ porque a R pertenecen los conjuntos que no se pertenecen a sí mismos, y R NO es un conjunto. Similarmente, a partir de la clase Ω no podemos derivar la antinomia de Burali-Forti porque, aunque Ω satisface la definición de ordinal de von Neumann, no es cierto que tenga un siguiente $\Omega + 1$, pues sólo los conjuntos que son ordinales tienen un siguiente y Ω no es un conjunto. Igualmente, el teorema de Cantor sólo podía demostrarse para conjuntos, por lo que no podía aplicarse a la clase V y no daba lugar a la paradoja de Cantor.

Pero la teoría de von Neumann no sólo devolvía a las matemáticas las multiplicidades inconsistentes de Cantor, sino que proporcionaba un criterio muy simple que determinaba si los elementos de una clase forman o no un conjunto. En efecto, uno de los axiomas de von Neuman era el *Axioma de limitación de tamaño,* cuyo enunciado es técnico y no vamos a explicarlo aquí, pero que implica lo siguiente:

> Los elementos de una clase forman un conjunto si y sólo si la clase no puede biyectarse con la clase de todos los conjuntos.

En particular, como (en virtud de la antinomia de Burali-Forti) no puede haber ningún conjunto que contenga a todos los ordinales, el axioma de limitación de tamaño implica que existe una biyección entre Ω y V, y esto a su vez, puesto que podemos definir un buen orden en Ω, implica que la clase V también admite un buen orden, por lo que en la teoría de von Neumann el axioma de elección (en una versión más fuerte que la de Zermelo) es un teorema, y lo mismo sucede con el axioma de reemplazo.

Otra característica notable de la teoría de von Neumann era que sólo requería un número finito de axiomas, mientras que los axiomas de la teoría de Zermelo son infinitos, debido al axioma de especificación, que es en realidad un esquema axiomático, y sigue habiendo infinitos axiomas si lo sustituíamos por el axioma del reemplazo, que también es un esquema axiomático. En este artículo von Neumann se refiere a la teoría de Zermelo con el axioma de reemplazo de Fraenkel como la *teoría de conjuntos de Zermelo-Fraenkel,* y así es como se la conoce hoy en día.

[48] Von Neumann explica que escribe $[f, a]$ en lugar de $f(a)$ para enfatizar que f y a deben considerarse igualmente como variables.

36 El programa de Hilbert En **1925** murió Gottlob Frege, a los 76 años. Hilbert asistió a un congreso en Münster en memoria de Karl Weierstrass (que había fallecido en 1897), con motivo del centenario de su nacimiento. En él dio una charla titulada *Sobre el infinito,* en la que expuso las ideas sobre la fundamentación de la matemática que había ido perfilando en los últimos años. Entre otras cosas, rebatió estas palabras de Skolem que hemos citado anteriormente:

> *Pero muchos matemáticos quieren matemáticas para tratar, en última instancia, con operaciones computacionales realizables, y no que consistan en proposiciones formales sobre unos objetos llamados así o asá.*

Hilbert concedía que los conjuntos no numerables no existían, que las afirmaciones sobre conjuntos no numerables eran meras palabras sin significado, pero negaba que fueran matemáticamente inútiles y que debieran ser rechazadas por ello. Al contrario, Hilbert señala que las matemáticas conocen muchos casos en los que el uso de "elementos ideales" ha resultado provechoso:

> *El método de los elementos ideales ya se aplica en la geometría elemental del plano. En ella los puntos y las rectas son inicialmente los únicos objetos reales que existen de hecho. Cumplen, entre otros el axioma de conexión: para cada par de puntos existe una única recta que pasa por ellos. De aquí se sigue que dos rectas se cortan a lo sumo en un punto. En cambio, la proposición de que dos rectas cualesquiera se cortan siempre en un punto no se cumple. En su lugar, las rectas pueden ser paralelas. Pero, como es bien sabido, la introducción de elementos ideales, a saber, los puntos en el infinito, vuelve universalmente válida la proposición de que dos rectas cualesquiera siempre se cortan en un único punto.*
>
> *Los elementos ideales "en el infinito" tienen la ventaja de volver el sistema de las leyes de conexión lo más simple y claro posible. Como es bien sabido, la simetría entre puntos y rectas proporciona el principio de dualidad de la geometría, que es tan fecundo.*
>
> *Las magnitudes complejas ordinarias del álgebra son igualmente un ejemplo del uso de elementos ideales. Sirven para simplificar los teoremas sobre la existencia y el número de raíces de una ecuación.*
>
> *Igual que en geometría infinitas rectas paralelas, a saber, las que son paralelas entre sí, se usan para definir un punto ideal, en la aritmética superior ciertos sistemas de infinitos números se combinan en un número ideal, y probablemente ninguna aplicación del principio de elementos ideales es una idea más brillante que ésta. Cuando este procedimiento se lleva a cabo en general en un cuerpo algebraico, nos encontramos con las simples y bien conocidas leyes de divisibilidad*[49] *exactamente igual como se cumplen para los enteros ordinarios* $1, 2, 3, 4, \ldots$

Así pues, Hilbert concede que la teoría de conjuntos consta en gran medida de afirmaciones ideales que no tienen ningún significado, pero hay otras que sí, que afirman o implican hechos que pueden ser comprobados mediante cálculos explícitos, y lo que importa no es si algunas afirmaciones son sólo palabras sin significado sino 1) si podemos razonar con ellas sin contradicciones y 2) si podemos garantizar que las afirmaciones verificables que podamos razonar usando tales afirmaciones vacías de contenido serán indudablemente verdaderas, como sucede en los ejemplos mencionados. Si es así, los conjuntos ficticios son una herramienta válida de trabajo que no hay razón para despreciar, sino todo lo contrario.

Con sus *Grundlagen der Geometrie,* Hilbert había demostrado que es posible demostrar afirmaciones geométricas como si carecieran de significado (a pesar de que lo tienen, pero sin tenerlo en cuenta para nada), y ahora se trataba de emplear las mismas técnicas de razonamiento formal para demostrar afirmaciones sobre conjuntos como si carecieran de significado (como creían que era el caso Hilbert y Skolem, pero no Zermelo, pero de modo que fuera irrelevante quién tuviera razón).

Por esas fechas Hilbert había establecido un programa, es decir, una lista de objetivos, que a su juicio debían ser alcanzados para llegar a una fundamentación de las matemáticas plenamente satisfactoria, y que fue detallando en una serie de artículos y de trabajos que fue publicando a lo largo de la década. La idea principal era que había que encontrar una teoría axiomática T que cumpliera los requisitos siguientes:

[49] Hilbert se refiere al hecho de que en general los anillos de enteros algebraicos no tienen factorización única, pero son todos ellos dominios de Dedekind, es decir, que cada ideal no nulo (y, en particular, cada entero algebraico identificado con un ideal principal) se descompone de forma única en producto de ideales primos.

1. *Tiene que ser una teoría formal,* es decir, que esté construida sobre un lenguaje formal cuyos signos primitivos no se definen, de modo que todos los conceptos gramaticales del lenguaje se definen en función de la forma de las cadenas de signos, sin tener en cuenta en ningún momento su posible significado. Esto es esencial si queremos usar dicho lenguaje para hablar de unos conjuntos que no sabemos lo que son. Además, por el mismo motivo, las reglas de razonamiento admisibles que permiten deducir teoremas de los axiomas tienen que estar especificadas también formalmente, es decir, que el paso de unas premisas a una conclusión tiene que basarse en la forma de las afirmaciones involucradas y no en su posible significado. Por ejemplo, de $p \to q$ y p se puede deducir q, sea lo que sea lo que signifiquen las fórmulas p y q, simplemente por la forma de las premisas y de la conclusión.

   De este modo, la teoría permitiría razonar sobre conjuntos abstractos sin que tengamos la obligación de precisar qué son esos conjuntos. Sólo tenemos que decir: suponemos que existen unos objetos que cumplen estos axiomas y razonamos sobre ellos aplicando mecánicamente estas reglas. La situación es la misma que si leemos una novela de ficción. Podemos tener la sensación de que estamos pensando en unos personajes reales, pero éstos no son más que palabras que no hacen referencia a nada.

2. *Tiene que ser íntegra,* en el sentido de que todo resultado que un matemático considere satisfactoriamente probado tiene que poder ser enunciado en el lenguaje de la teoría y demostrado siguiendo las reglas de demostración de la teoría.

3. *Tiene que ser consistente*, es decir, que en ella no se puedan demostrar contradicciones.

4. *Tiene que ser completa,* es decir, que toda afirmación pueda ser demostrada o refutada en ella.

Si una teoría de conjuntos T reúne estas características y en ella podemos demostrar, por ejemplo, la conjetura de Goldbach: *Todo número par mayor que* 2 *es suma de dos primos,* por muy abstractos y poco constructivos que sean los argumentos de la prueba, por muchos cardinales transfinitos que aparezcan en ella, podemos asegurar que la conjetura de Goldbach es cierta. Porque si fuera falsa, existiría un número par, digamos $N = 542\,345\,444\,323\,999\,298$, que no podría expresarse como suma de dos primos, y esto podría demostrarse en la teoría T, por la propiedad 2, ya que la comprobación sería elemental (sólo habría que considerar todos los primos $p < N$ y comprobar que $N - p$ nunca es primo), pero entonces en T se podría demostrar que todo número par mayor que 2 es suma de dos primos y también que existe un número par mayor que 2 que no es suma de dos primos, con lo que sería una teoría contradictoria, en contra del supuesto 3.

En realidad este argumento admite una posible objeción: la conjetura de Goldbach sería cierta supuesto que la demostración de 3 sea fiable, porque si la demostración de 3, es decir, de la consistencia de T, se basa en argumentos abstractos no constructivos, un matemático que recele de tales argumentos cuestionará igualmente que T sea realmente consistente y, por consiguiente, que realmente podamos dar por demostrada la conjetura de Goldbach. Esta objeción es un caso particular de una cuestión mucho más básica, en la que ya había insistido Poincaré:

Se supone que estamos tratando de encontrar una teoría axiomática T que sirva de fundamento al razonamiento matemático porque hemos constatado que cuando un matemático razona "libremente", aceptando como conjunto cualquier colección de objetos, sin ceñirse a unos axiomas cuidadosamente elegidos para descartar contradicciones, aparecen contradicciones por motivos que no sabemos explicar. Pero construir un lenguaje formal, determinar unas reglas de razonamiento, justificar que se corresponden con lo que los matemáticos entienden normalmente por "razonar", probar que la teoría es consistente, etc. es, en definitiva, "hacer matemáticas", no es una tarea esencialmente distinta de lo que hace un algebrista cuando define un anillo y estudia sus propiedades, por ejemplo. Entonces, ¿por qué deberíamos fiarnos de los razonamientos que justifican que la teoría T tiene las propiedades requeridas si precisamente buscamos la teoría T para estar en condiciones de hacer razonamientos matemáticos fiables?

También sobre esto versaban precisamente las críticas 1 y 7 que Skolem había hecho a la teoría de conjuntos como fundamentación de la matemática. En la primera Skolem hacía referencia a que Zermelo había presentado sus axiomas postulando un "dominio" (formado por conjuntos y elementos que no eran conjuntos, aunque a estas alturas ya estaba claro que se podía prescindir de los últimos) que cumplía los axiomas de la teoría, y a este respecto decía:

> *Si adoptamos la axiomática de Zermelo, debemos, en sentido estricto, tener una noción general sobre los dominios para proporcionar una fundamentación a la teoría de conjuntos. Todo el contenido de la teoría es como sigue: para cada dominio en el que se cumplan los axiomas, se cumplen también*

> *todos los teoremas de la teoría de conjuntos. Pero claramente es un tanto circular reducir la noción de conjunto a una noción general de dominio.* [...] *Más aún, se verá claramente de lo que sigue que uno no puede emprender investigaciones lógicas sobre tales dominios sin aplicarles hasta cierto punto consideraciones conjuntistas si uno quiere seguir el método puramente conjuntista y evitar la inclusión de la noción de número entre las nociones fundamentales.*

Lo que dice Skolem es que si uno quiere probar la consistencia de la teoría de conjuntos necesita justificar que existe un dominio, es decir, un modelo, en el que se cumplen los axiomas de la teoría de conjuntos, pero para construir ese modelo, necesitamos la teoría de conjuntos, con lo que caemos en un círculo vicioso. Skolem precisa que esto es así supuesto que no queramos tomar la noción de número como una noción fundamental. Esto lo aclara en su objeción número 7:

> *Los especialistas en teoría de conjuntos suelen ser de la opinión de que la noción de número natural debe definirse y que el principio de inducción matemática debe ser demostrado. Pero está claro que no podemos definir y demostrar* ad infinitum. *Tarde o temprano tenemos que llegar a algo que ya no puede ser definido o demostrado. Nuestra única preocupación debe ser, pues, que los fundamentos iniciales sean algo intuitivamente claro, natural, y no cuestionable. Esta condición es satisfecha por la noción de número natural y los razonamientos inductivos, pero decididamente no es satisfecha por los axiomas del tipo de los de Zermelo o cualquier otra cosa de ese estilo.*

Hilbert rebate estas críticas dándole la razón a Skolem, es decir, explicando, por una parte, que no pretende probar la consistencia de los axiomas de la teoría de conjuntos construyendo unos objetos que los satisfagan (en cuyo caso, la crítica de Skolem estaría plenamente justificada), sino analizando el concepto de demostración matemática para probar que no puede existir la demostración de una contradicción a partir de unos axiomas para la teoría de conjuntos escogidos adecuadamente y, como las demostraciones matemáticas son objetos completamente finitistas (son sucesiones de fórmulas de un lenguaje formal), cabe la posibilidad de estudiarlas por técnicas estrictamente finitistas. Y, por otra parte, también le da la razón en que es inviable pretender que los números naturales deban ser definidos a partir de la teoría de conjuntos y que el principio de inducción deba ser demostrado. Al contrario, considera que los conceptos finitistas no necesitan del marco de una teoría axiomática de conjuntos para ser aceptados.

Hilbert distingue entre el razonamiento "con contenido", lo que podemos llamar *razonamiento material,* que requiere tratar exclusivamente con afirmaciones que tengan un significado, un contenido claro y bien definido, el cual se tiene en cuenta para asegurar que todo lo que se va afirmando es verdad, y el *razonamiento formal,* en el que se pasa de una afirmación a otra en virtud de su forma, sin considerar su posible significado. El primero es el que usamos habitualmente para hablar de la realidad, mientras que el segundo sólo es necesario en matemáticas, y sólo cuando hablamos de objetos abstractos de los que no tenemos una representación clara. Además, señala que las contradicciones sólo han aparecido al intentar razonar materialmente sobre conceptos abstractos:

> *Vimos antes que lo infinito no se encuentra en ningún lugar de la realidad, sin importar qué experiencias y observaciones o qué tipo de ciencia podamos aducir.* (2) *¿Podría ser, entonces, que pensar sobre los objetos sea tan diferente de pensar en los sucesos que involucran objetos y que requiere proceder de manera tan distinta, tan apartada de toda realidad?* (3) *¿No está claro, más bien, que cuando creímos haber descubierto que lo infinito era en cierto sentido real, sólo nos dejamos llevar a esa creencia por la circunstancia de que tan a menudo encontramos en la realidad dimensiones tan inconmensurables en lo grande y en lo pequeño?* (4) *¿Y acaso la inferencia lógica material nos ha engañado y abandonado en algún lugar cuando la aplicamos a objetos o sucesos reales? No, la inferencia lógica material es indispensable.* (5) *Sólo nos ha engañado cuando hemos aceptado nociones abstractas arbitrarias, en particular aquellas bajo las cuales se subsumen infinitos objetos. Lo que hicimos, entonces, fue simplemente usar la inferencia material de manera ilegítima; es decir, obviamente no respetamos las condiciones necesarias para el uso de la inferencia lógica material.* (6) *Y al reconocer que tales condiciones existen y deben ser respetadas, nos encontramos en acuerdo con los filósofos, especialmente con Kant.*
>
> (7) *Kant ya enseñó —y de hecho es parte integral de su doctrina— que las matemáticas disponen de un contenido asegurado independientemente de toda lógica y, por lo tanto, nunca pueden ser fundamentadas sólo por medio de la lógica; por eso los esfuerzos de Frege y Dedekind estaban destinados al fracaso.* (8) *Más bien, como condición para el uso de inferencias lógicas y la realización*

> *de operaciones lógicas, algo debe estar ya dado a nuestra facultad de representación, ciertos objetos concretos extralógicos que están intuitivamente presentes como experiencia inmediata antes de todo pensamiento.*
>
> (9) *Si la inferencia lógica ha de ser fiable, debe ser posible examinar completamente estos objetos en todas sus partes, y el hecho de que ocurran, que difieran entre sí y que se sucedan o estén concatenados, se da intuitivamente de inmediato, junto con los objetos, como algo que no puede reducirse a nada más ni requiere reducción.* (12) *Ésta es la posición filosófica básica que considero necesaria para las matemáticas y, en general, para todo pensamiento, comprensión y comunicación científica.* (1) *Y en las matemáticas, en particular, lo que consideramos son los propios signos concretos, cuya forma, según la concepción que hemos adoptado, es inmediatamente clara y reconocible.*

Este pasaje es muy denso y requiere un análisis en profundidad, pero antes de entrar en ello citamos también las palabras con las que Hilbert concluyó su charla, pues entroncan con la cita precedente:

> *Finalmente, recordemos nuestro verdadero tema y, en lo que respecta a lo infinito, saquemos el balance de todas nuestras reflexiones.* (3) *El resultado final es: en ningún lugar se realiza lo infinito; no está presente en la naturaleza ni es admisible como fundamento en nuestro pensamiento racional, una notable armonía entre el ser y el pensar. Obtenemos una convicción que contradice los esfuerzos anteriores de Frege y Dedekind: la convicción de que,* (7) *si el conocimiento científico ha de ser posible, ciertas concepciones intuitivas y representaciones son indispensables; la lógica por sí sola no basta.* (1) *El derecho a operar con lo infinito sólo puede asegurarse por medio de lo finito.*
>
> (10) *El papel que le queda a lo infinito es, más bien, meramente el de una idea —si, de acuerdo con las palabras de Kant, entendemos por idea un concepto de razón que trasciende toda experiencia y por medio del cual lo concreto se completa para formar una totalidad—;* (11) *una idea, además, en la que podemos tener una confianza inquebrantable dentro del marco que proporciona la teoría que he esbozado y defendido aquí.*

Hemos intercalado números en las citas para vincular las aclaraciones siguientes con las frases concretas a las que se refieren:

1. Para estudiar si una teoría matemática satisface los requisitos del programa de Hilbert, en particular, por ejemplo, para investigar si es consistente, lo que procede no es tratar de encontrar unos objetos que satisfagan los axiomas, sino estudiar las demostraciones posibles en la teoría, que son sucesiones finitas de fórmulas de su lenguaje formal, las cuales a su vez son sucesiones finitas de signos. Se trata, pues, de estudiar si existe o no una cierta estructura finita (una demostración de una contradicción en la teoría).

2. Y no tenemos indicio alguno de que, sobre conceptos finitistas, que no involucren ningún conjunto infinito, no podamos razonar como lo hacemos habitualmente al razonar sobre el mundo real, aunque estemos hablando de conceptos matemáticos que no dependen de la realidad física.

3. Si los matemáticos han encontrado contradicciones ha sido porque creyeron que podrían razonar sobre el infinito igual que razonamos sobre la realidad física, a pesar de que el infinito no se da nunca en ésta.

4. Esta lógica material, que se basa en que sabemos de qué estamos hablando, y cuida de no admitir nunca afirmaciones falsas en el discurso, nunca ha dado problemas al ser aplicada al mundo real.

5. Sólo nos ha engañado cuando hemos tratado de aplicarla a nociones abstractas, a conjuntos infinitos sin un contenido intuitivo claro que nos permita, no ya juzgar si lo que se dice es cierto, sino siquiera atribuir un significado preciso a las afirmaciones que se hacen.

6. Para razonar con seguridad sobre conceptos no finitistas es imprescindible hacerlo formalmente, es decir, no tratando de asegurarnos de que lo que decimos es verdad, porque no estamos en condiciones siquiera de atribuir un significado preciso a lo que decimos, sino respetando ciertas reglas de razonamiento formales y tomando como punto de partida unos axiomas adecuados, expresados mediante fórmulas de un lenguaje formal, para no tener que atribuirles un significado. Pero esto no significa que sólo el razonamiento formal sea seguro, sino que para razonar materialmente se deben respetar ciertas condiciones que no están garantizadas fuera del finitismo. Esto es algo que ya había puesto de manifiesto Kant en su teoría del conocimiento.

7. Tal y como explica Kant, la lógica pura no genera más que afirmaciones triviales, como que "si se cumple A o B, pero no se cumple A, entonces se cumple B", pero el conocimiento requiere ir más allá de las meras verdades lógicas. En el caso del razonamiento formal, son los axiomas los que proporcionan afirmaciones no triviales desde un punto de vista lógico de las que la lógica extrae más consecuencias no triviales, pero si pretendemos razonar materialmente, para aceptar cualquier afirmación que no sea una mera verdad lógica, necesitamos asegurarnos de que sea verdadera, y para ello necesitamos atribuirle un significado claro, y para ello necesitamos tener una representación clara de los objetos considerados que nos permita juzgar si lo que estamos diciendo es verdad o no.

   Un objeto matemático finitista, como, por ejemplo, un grupo de orden 5, es un concepto abstracto en el sentido de que es una abstracción de la realidad física, no tiene ningún contenido físico; pero no es un concepto abstracto en el mismo sentido en que lo es un grupo de orden $\aleph_{15}$. El primero tiene un contenido intuitivo, en el sentido kantiano de la palabra "intuición" que luego procederemos a explicar. En cambio, un grupo de orden $\aleph_{15}$ es un concepto abstracto en el sentido fuerte de que podemos razonar sobre él, pero no tenemos forma alguna de representarnos intuitivamente lo que es y juzgar si lo que estamos afirmando es cierto o no. En tal caso, nuestra única guía fiable es asegurarnos de que todo lo que decimos se deduce lógicamente de unos axiomas dados cuidadosamente escogidos.

   Cuando decimos que el razonamiento formal (axiomático) es imprescindible para razonar con objetos abstractos, no nos referimos a "abstraídos de la realidad", es decir, desprovistos de contenido físico, sino a conceptos "abstraídos de la intuición", desprovistos de contenido intuitivo.

8. Para aplicar la lógica, o bien razonamos formalmente a partir de unos axiomas formales, o bien tenemos que tener acceso a ciertas representaciones inmediatas, cuyas propiedades podamos constatar inmediatamente, sin necesidad de ningún razonamiento o de reducirlas a otras más simples. Esto es lo que Kant llamaba intuición (y más abajo pondremos ejemplos para precisar el concepto).

9. Para que los razonamientos lógicos materiales sean fiables, es necesario que los objetos a los que se aplican estén completamente determinados por la intuición (y, como veremos, el "completamente" es esencial). Hilbert habla de "ocurrencias", "concatenaciones", etc. porque está pensando en aplicar su argumento a los signos de un lenguaje formal, pero el alcance de sus afirmaciones es mucho mayor.

10. El infinito, y en general, los conceptos abstractos en el sentido fuerte de "carentes de contenido intuitivo pleno" son ideas en el sentido kantiano de la palabra, es decir, conceptos creados por la razón, que no tienen una interpretación, no ya en la realidad física, sino siquiera en la capacidad de representación que —siguiendo a Kant— llamamos intuición.

11. Ahora bien, si se justifica que una elección adecuada de unos axiomas cumple los requisitos que pedía Hilbert (o al menos, que determinen una teoría axiomática formal consistente), entonces podemos razonar con ideas matemáticas abstractas con total confianza.

12. Si no admitimos que tenemos la capacidad de razonar intuitivamente de forma fiable, entonces no sólo es impensable una fundamentación de las matemáticas, sino que en realidad la intuición está en la base de cualquier forma de pensamiento, comprensión y comunicación científica.

La intuición Con estas anotaciones hemos tratado de aclarar el pensamiento de Hilbert sobre en qué sentido podía y debía fundamentarse la matemática, pero falta, sin duda, aclarar el concepto de "intuición' kantiana al que Hilbert alude. Ante todo, quede claro que la palabra "intuición" se usa en el lenguaje coloquial en sentidos muy distintos y completamente opuestos al sentido que aquí hay que darle si queremos entender algo. Coloquialmente, una "intuición" puede ser un presentimiento, una adivinación perspicaz, una decisión no meditada, etc., pero nada de esto tiene que ver con el concepto kantiano de "intuición". Kant acuñó el término a partir del verbo latino *intueri,* que significa "observar", "mirar con atención".

Comparemos, por ejemplo, un cubo tridimensional con un cubo de cuatro dimensiones. Podemos pensar en ambos y razonar sobre ambos, pero podemos formarnos una imagen de un cubo de tres dimensiones y no de un cubo de cuatro dimensiones.[50] Esa imagen que podemos formarnos de un cubo tridimensional, sin análogo alguno en el caso del cubo cuatridimensional, es una *intuición* o una *imagen intuitiva* de un cubo tridimensional.

[50]Podemos representarnos un cubo de cuatro dimensiones imaginando dos cubos concéntricos con los vértices unidos, pero eso no es la imagen de un cubo de cuatro dimensiones, sino una figura tridimensional que se corresponde hasta cierto punto con un cubo de cuatro dimensiones igual que una imagen bidimensional (en perspectiva) de un cubo de tres dimensiones NO es un cubo de tres

Podemos decir que el concepto de cubo (tridimensional) es un concepto intuitivo, es un concepto que podemos usar para describir una determinada intuición, una determinada imagen que podemos formarnos. En cambio, en los mismos términos en los que se expresa Hilbert, el concepto de cubo de cuatro dimensiones es sólo una idea, un concepto sobre el que podemos razonar, pero que no está vinculado a ningún concepto intuitivo.

De aquí no hay que extraer ningún juicio de valor, según el cual los cubos de tres dimensiones son "mejores" o "más reales" o "más importantes" que los de cuatro dimensiones. Desde el punto de vista de la matemática formal, no hay ninguna diferencia entre la geometría de tres, cuatro o veinte dimensiones. Un cubo de tres dimensiones y otro de cuatro dimensiones son objetos totalmente análogos como ideas, pero un cubo de cuatro dimensiones es únicamente una idea (un contenido abstracto sobre el que podemos razonar), mientras que un cubo de tres dimensiones es una idea que se corresponde con un concepto intuitivo.

Si alguien desconoce el significado de la palabra "cubo" y le decimos que un cubo es la forma geométrica de un dado, y le mostramos la imagen de la derecha para despejar cualquier ambigüedad (precisando que todos los ángulos son rectos y que todas las aristas tienen la misma longitud), con esto nuestro interlocutor habrá entendido perfectamente lo que es un cubo.

Así, si le preguntamos cuántos vértices tiene un cubo, aunque jamás se lo hubiera planteado antes, no tendrá dificultad en observar que, pensando en un cubo en la posición que muestra la figura, tiene cuatro vértices en un plano inferior y otros cuatro en un plano superior, lo que hace un total de ocho vértices. Y si le preguntamos cuántas aristas tiene, observará que tiene cuatro horizontales en el plano inferior, otras cuatro en el superior y otras cuatro verticales, lo que hace un total de doce aristas. Notemos que para llegar a estas respuestas no es necesario que el interrogado tenga ante sí ningún objeto físico con forma de cubo. Ni siquiera sería necesaria ninguna imagen si ya ha entendido plenamente qué es un cubo y puede formarse la imagen de uno en su mente.

El lector debería entender ahora a qué se refiere Hilbert cuando habla de *objetos concretos extralógicos que están intuitivamente presentes como experiencia inmediata antes de todo pensamiento.* Alguien que nunca haya visto o pensado en un cubo entenderá lo que es sin más que ver uno, y no necesita pensar nada para entender lo que está viendo. Toda la información de lo que es un cubo le viene dada inmediatamente y después, si quiere, puede pensar sobre el cubo y deducir hechos sobre los cubos. Si uno, a partir de la imagen de un cubo, deduce que los cubos tienen ocho vértices, no llega a ello mediante ningún razonamiento a partir de ningún axioma, sino que llega a esta conclusión "contando" los vértices (uno a uno, o bien apoyándose en la aritmética), pero todo esto es posterior a tener la imagen intuitiva de un cubo. Incluso uno puede convencerse intuitivamente de hechos más sofisticados, como que se puede cubrir el espacio yuxtaponiendo cubos, sin que queden espacios vacíos entre ellos (cosa que no se puede hacer, por ejemplo, con esferas), y a ello se llega, una vez más, sin ningún razonamiento que parta de ningún axioma.

El concepto de "cubo" es un concepto intuitivo. No es un objeto físico. Cuando nos imaginamos un cubo no estamos imaginando —o no necesitamos imaginar— un cubo de madera, o de plástico, ni necesitamos atribuirle un peso, ni lo estamos situando en ningún punto en particular de universo, ni hay riesgo de que alguien nos lo pise sin querer, porque no está en ninguna parte. Es sólo una construcción mental, pero que nos permite razonar informalmente exactamente igual que lo hacemos habitualmente sobre objetos físicos, como cuando, por ejemplo, vemos varios objetos físicos y nos planteamos cómo podemos disponerlos para que quepan en un armario o en un maletero. El hecho de que una imagen de un cubo no sea un objeto físico no dificulta en absoluto nuestras posibilidades de razonamiento sobre los cubos. Al contrario, las facilita, porque un objeto físico puede tener características que nos sean desconocidas, mientras que un cubo no es ni más ni menos que lo que nos imaginamos al imaginar un cubo. Por eso dice Hilbert que no hay razón para cuestionar que podamos razonar informalmente sobre objetos matemáticos sin realidad física, como es un cubo, usando la misma lógica que usamos para razonar con objetos reales, siempre y cuando hablemos de objetos con un contenido intuitivo preciso, y no de meras ideas, sin contenido intuitivo. Que el concepto "piedra" tenga un contenido físico (Kant diría, empírico) y el concepto "cubo" tenga un contenido meramente intuitivo, pero no empírico (Kant diría que es un concepto puro) no marca ninguna diferencia que condicione la lógica que podemos emplear para razonar con uno u otro.

---

dimensiones, sino una figura bidimensional que se corresponde parcialmente con el cubo, al igual que una imagen tridimensional de un cubo de cuatro dimensiones NO es un cubo de cuatro dimensiones, no tiene, por ejemplo, cuatro aristas perpendiculares dos a dos confluyendo a cada vértice.

No sucede lo mismo con las ideas, es decir, con los objetos de razonamiento carentes de un contenido intuitivo preciso. Pensemos en un poliedro convexo formado por 18 caras que sean triángulos equiláteros. Por ejemplo, podemos razonar que tendrá 27 aristas, ya que 18 caras con 3 aristas cada una hacen 54 aristas, pero cada arista es compartida por 2 caras, luego hemos contado cada una dos veces. A su vez, podemos razonar que tendrá 38 vértices, en virtud del teorema de Euler, que afirma que todo poliedro convexo cumple $V - A + C = 2$. Pero si seguimos analizando las características de este poliedro llegaremos a una contradicción, lo cual prueba que no existen poliedros convexos cuyas caras sean 18 triángulos equiláteros.[51] Así, vemos que tal poliedro no era más que una idea, algo sobre lo que hemos podido razonar, pero en este caso sólo para concluir que era una idea contradictoria. Que podamos pensar en algo no nos da ninguna garantía de que lo que estamos pensando no esconda contradicciones. En cambio, el hecho de que podamos imaginarnos un poliedro regular de 6 caras cuadradas nos da la garantía de que es imposible que el concepto de "cubo" (tridimensional) sea contradictorio. Si los cubos fueran contradictorios, podríamos pensar en ellos, pero no intuirlos.

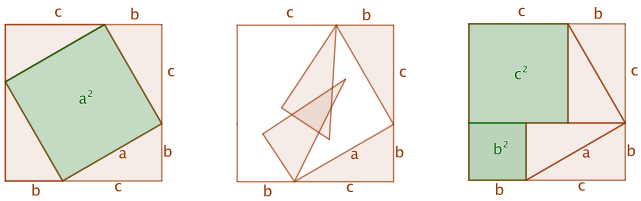
Hilbert sostiene que "el conjunto de todos los conjuntos" es como el poliedro de 18 caras en el que estábamos pensando, una idea sobre la que podemos razonar hasta darnos cuenta de que es contradictoria, pero que esto no puede pasar si hablamos de objetos matemáticos finitistas, todos los cuales tienen un contenido intuitivo preciso.

En cambio, el programa de Hilbert de fundamentación de la matemática tenía como objetivo estar en condiciones de concluir que $\aleph_1$ es como un cubo de cuatro dimensiones, una idea que no podemos asociar a ningún contenido intuitivo, pero que es "segura" en el sentido de que podemos confiar en que no nos llevará a ninguna contradicción.

Hasta aquí hemos puesto algunos ejemplos de lo que podemos llamar *intuición espacial,* es decir, de nuestra capacidad de formarnos representaciones espaciales no empíricas (que no corresponden a objeto físico alguno), pero más importante aún para las matemáticas es el hecho de que también contamos con una intuición temporal.

Si contamos mentalmente: "uno, dos, tres, cuatro", y luego avanzamos dos lugares más, pensando "cinco, seis" (con la conciencia de que hemos dado exactamente dos pasos más), habremos constatado que $4 + 2 = 6$ sin que medie ningún razonamiento formal, sin haber deducido nada de ningún axioma. Del mismo modo que a partir de la imagen de un cubo hemos obtenido inmediatamente información matemática (geométrica) sobre los cubos, a partir de una intuición puramente temporal hemos obtenido una afirmación aritmética que podemos dar por cierta fuera de toda duda razonable.

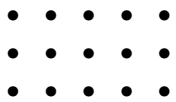
Afirmaciones como "los cubos tienen 12 aristas" o "$4 + 2 = 6$" son ejemplos de afirmaciones intuitivamente evidentes, pero también hay afirmaciones cuya verdad puede razonarse intuitivamente sin que se puedan calificar de evidentes. Por ejemplo, nadie puede imaginarse un triángulo rectángulo arbitrario y afirmar: obviamente, el cuadrado de la hipotenusa es igual a la suma de los cuadrados de los catetos. Eso no es en absoluto intuitivamente evidente. Sin embargo, si le mostramos a alguien las figuras siguientes:



y le explicamos que movemos los triángulos de la primera figura como muestra la segunda hasta situarlos en la posición de la tercera, entonces vemos que el área del cuadrado de la primera figura es la suma de las áreas de los cuadrados de la tercera, lo que demuestra el teorema de Pitágoras (supuesto que ya conozcamos algunos resultados elementales sobre áreas). Lo que sí que podemos dar por evidente es que el razonamiento previo se puede hacer con cualquier triángulo rectángulo dado, sin que importen sus dimensiones. Con ello estamos afirmando que, dado cualquier triángulo rectángulo, siempre seremos capaces de construir mentalmente figuras como las anteriores, y esto nos asegura que el teorema de Pitágoras vale para triángulos rectángulos arbitrarios y no sólo para los que muestre una figura en particular.

Así pues, el teorema de Pitágoras no es intuitivamente evidente, pero es fácil demostrarlo mediante un argumento intuitivo que se basa en que podemos imaginarnos unos triángulos ideales que se mueven de una posición a otra, junto con la conciencia de que esto puede hacerse independientemente de las dimensiones de los triángulos. Similarmente, basta observar una figura como

[51] Puede probarse que los hay únicamente con $4, 6, 8, 10, 12, 14, 16$ y 20 caras, pero no con 18.



para convencernos de que $3 \cdot 5 = 5 \cdot 3$ y, si además nos persuadimos de que podemos formar rectángulos de puntos análogos con cualquier número de puntos en sus lados, nos convencemos de que $mn = nm$ para cualquier par de números naturales m y n (tratando aparte el caso trivial en que alguno de los factores sea 0). Esto es otro ejemplo de razonamiento informal basado en la intuición.

En cambio, no podemos confiar en nuestra intuición para razonar sobre objetos que escapan a su alcance. Por ejemplo, si alguien dice que es "intuitivamente evidente" que no existen funciones continuas no derivables en ningún punto, se está equivocando doblemente. En primer lugar, se equivoca porque es posible demostrar que sí que las hay, y en segundo lugar, se equivoca al creer que está legitimado a concluir que no existen por el mero hecho de que no pueda representarse ninguna intuitivamente. Lo que sucede es que el concepto de función $f : \mathbb{R} \longrightarrow \mathbb{R}$ trasciende con mucho nuestra intuición. Podemos asignar un contenido intuitivo a determinadas funciones relativamente sencillas, pero no podemos afirmar que tenemos la capacidad de concebir intuitivamente cualquier función real de variable real (y las funciones continuas no derivables son una muestra de ello) al contrario de lo que sucede, por ejemplo, con todos los triángulos. La intuición no nos puede engañar cuando nos damos cuenta de que la demostración intuitiva precedente del teorema de Pitágoras es aplicable a cualquier triángulo rectángulo, sin que quepa la posibilidad de que haya un tipo de triángulo rectángulo "que no hubiéramos visto antes" y para el que falle el argumento. Pero en modo alguno podemos afirmar que todas las funciones continuas $f : \mathbb{R} \longrightarrow \mathbb{R}$ que podamos concebir intuitivamente cubren todas las posibilidades del concepto matemático formal de "función continua de variable real".

Y si no podemos razonar intuitivamente sobre funciones de variable real, porque nuestra intuición sólo alcanza a representarse algunas de ellas —sin la generalidad necesaria para que nos legitimara a hacer afirmaciones sobre su totalidad— mucho menos podemos razonar intuitivamente sobre los conjuntos abstractos sobre los que podemos pensar, pero no tenemos ninguna representación intuitiva, como $\mathcal{P}\mathbb{N}$ o $\aleph_{17}$. Es cuando pretendemos pensar en objetos que nuestra intuición no alcanza a representarse (o a hacerlo con toda la generalidad posible) cuando no podemos confiar en nuestro pensamiento ciego y necesitamos una teoría axiomática que nos asegure que no vamos a caer en contradicciones.

37 El teorema de Kőnig Gyula Kőnig había fallecido en 1913, a los 63 años, pero había dejado un hijo llamado Dénes Kőnig, que en 1904 se había doctorado en Gotinga bajo la dirección de Hermann Minkowski (que había muerto de apendicitis en 1909, a los 44 años). En **1926** Kőnig publicó un artículo titulado *Sobre las correspondencias mutívocas de conjuntos.* El resultado que probaba en él no era especialmente interesante, pero, para probarlo, demostró previamente un hecho muy general cuyo interés en sí mismo no se le escapó, y al año siguiente publicó otro artículo titulado *Sobre un método de inferencia de lo finito a lo infinito* en el que lo presentaba y lo reformulaba en términos de grafos. Su enunciado original era el siguiente:

> *Sea $E_1, E_2, E_3, \ldots$ una sucesión numerable de conjuntos finitos no vacíos, y sea R una relación tal que a cada elemento x_{n+1} de E_{n+1} le corresponda al menos un elemento x_n de E_n ligado a x_{n+1} por la relación R, cosa que escribiremos en la forma $x_n\, R\, x_{n+1} (n = 1, 2, 3 \ldots)$. Entonces se puede elegir en cada conjunto E_n un elemento a_n de modo que, para la sucesión infinita $a_1, a_2, a_3, \ldots$ se tenga $a_n\, R\, a_{n+1}$.*

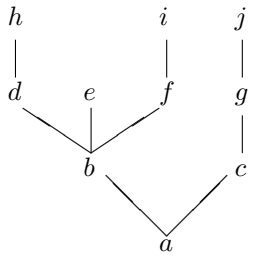
Su reformulación en términos de grafos era la siguiente:

> *Si el conjunto infinito numerable de puntos (nodos) de un grafo G se divide en infinitos conjuntos finitos no vacíos $E_1, E_2, E_3, \ldots$ tales que cada punto de E_{n+1} esté conectado por una arista a un punto de E_n, entonces existe en el grafo un camino infinito $a_1, a_2, a_3, \ldots$ que contiene un punto a_n de cada conjunto E_n. (Aquí los conjuntos E_n no necesitan ser disjuntos.)*

Sin embargo, éste resultado iba a ser en el futuro especialmente interesante en un caso particular, formulado para árboles en el sentido siguiente:

> Un *árbol* es un conjunto A parcialmente ordenado (es decir, dotado de un orden que no exige que dos elementos cualesquiera sean comparables) tal que, para cada elemento a de A, la sección inicial que determina $\{x \in A \mid x < a\}$ sea finita y esté totalmente ordenada.

Esto permite definir la *altura* de un elemento de un árbol como el número de elementos que tiene por debajo, y el *nivel* n-simo de un árbol como el conjunto de todos sus elementos de altura n.



Por ejemplo, la figura muestra un árbol con un elemento de altura 0, dos de altura 1, cuatro de altura 2 y 3 de altura 3. El caso particular que nos interesa del teorema de Kőnig es el siguiente:

Teorema de Kőnig (2) Si un árbol infinito numerable tiene niveles finitos, entonces tiene una rama infinita (un subconjunto infinito totalmente ordenado con nodos de todas las alturas).

DEMOSTRACIÓN: Si A es un árbol infinito con niveles finitos, de entre los elementos del nivel 0, tiene que haber uno, digamos x_0, que tenga infinitos elementos por encima, porque si cada elemento de nivel 0 (que son un número finito) sólo tuviera un número finito de elementos por encima, el árbol sería finito.

Por el mismo motivo, de entre los elementos de altura 1 por encima de x_0, tiene que haber uno, digamos x_1, que tenga infinitos elementos por encima, porque en caso contrario, como x_0 sólo tiene por encima un número finito de elementos de altura 1, en total tendría un número finito de elementos por encima, en contra de la forma en que lo hemos elegido. Similarmente, de entre los elementos de altura 2 que están sobre x_1, tiene que haber uno, digamos x_2, que tenga infinitos elementos por encima, y de este modo vamos construyendo una rama infinita $x_0 < x_1 < x_2 < \cdots$ ∎

El mismo argumento vale para demostrar cualquiera de las versiones previas que hemos enunciado.

38 La teoría de la demostración En la conclusión de su charla en Münster, Hilbert había dicho, hablando del infinito, que es *una idea, además, en la que podemos tener una confianza inquebrantable dentro del marco que proporciona la teoría que he esbozado y defendido aquí.* La teoría que había esbozado y defendido allí era lo que actualmente se conoce como "teoría de la demostración", que convierte a las demostraciones matemáticas en objeto de estudio.

Como parte de esta teoría, hacía unos años Hilbert había desarrollado una técnica para obtener pruebas finitistas de consistencia y la había aplicado con éxito a una versión muy rudimentaria de la aritmética. Luego Ackermann la había perfeccionado hasta un método que llamó *épsilon-sustitución.*

La idea básica consiste en introducir en un lenguaje formal el llamado *operador* ϵ, de modo que si $\alpha(x)$ es una fórmula, entonces $\epsilon_x\,\alpha$ pretende significar "un ejemplo de x que cumple $\alpha(x)$". Esto permite eliminar los cuantificadores en las fórmulas mediante:

$$\bigvee x\,\alpha(x) \leftrightarrow \alpha(\epsilon_x\,\alpha),$$

$$\bigwedge x\,\alpha(x) \leftrightarrow \neg\bigvee x\neg\alpha(x) \leftrightarrow \neg\neg\alpha(\epsilon_x\neg\alpha) \leftrightarrow \alpha(\epsilon_x\neg\alpha),$$

y trabajar con fórmulas con el operador ϵ en lugar de cuantificadores permitía aplicar ciertas técnicas orientadas a demostrar la consistencia de una teoría dada.

En 1925 Ackermann leyó su tesis doctoral, titulada *Justificación del "tertium non datur" utilizando la teoría de consistencia de Hilbert,* en el que aplicaba la técnica a una teoría mucho más potente. Sin embargo, antes de que fuera publicada, el propio Ackermann se dio cuenta de que la prueba tenía un fallo, si bien von Neumann logró arreglarla, pero sólo para una axiomatización de la aritmética de Peano sin el axioma de inducción.

El título de la tesis de Ackermann, con la alusión al *tertium non datur* (el principio del tercio excluso) estaba claramente dirigido contra el intuicionismo de Brouwer. La relación entre Hilbert y Brouwer mejoró temporalmente en **1926**, cuando Brouwer visitó Gótinga para dar una charla y coincidió con Hilbert en una comida en casa de Emmy Noether, pero la tregua no duró. Las diferencias entre ambos eran tan notorias que en **1927** un periódico les propuso un debate público en sus páginas, pero no aceptaron.[52]

Ese año Hilbert dio una charla en Hamburgo con el título de *La fundamentación de las matemáticas,* en la que expuso las ideas básicas de su teoría de la demostración y explicó su método de *épsilon-sustitución.*

[52]Ese año Brouwer publicó *Sobre el dominio de definición de las funciones,* donde demostraba que toda función $f : \mathbb{R} \longrightarrow \mathbb{R}$ es continua. Ante la objeción de, por ejemplo, la función que vale 0 salvo en $f(0) = 1$, Brouwer respondería que no está bien definida, porque hay números reales que no son ni iguales ni diferentes de 0.

Enseguida trataremos de explicar en qué consiste la teoría de la demostración, pero antes comentamos algunas apreciaciones que Hilbert hace en su charla respecto de las teorías alternativas a las suyas. Respecto al logicismo de Russell, dice:

> *La teoría de los fundamentos de Russell y Whitehead es una investigación lógica general de amplio alcance. Pero el fundamento que proporciona para las matemáticas se basa, primero, en el axioma del infinito y, luego, en lo que se denomina el axioma de reducibilidad, y ambos axiomas son suposiciones genuinas y con contenido que no están respaldadas por una prueba de consistencia; son suposiciones cuya validez de hecho sigue siendo dudosa y que, en cualquier caso, mi teoría no requiere.*

Más sutil es la crítica a Poincaré:

> *Poincaré ya hizo varias afirmaciones que entran en conflicto con mis puntos de vista; sobre todo, negó desde un principio la posibilidad de una prueba de consistencia para los axiomas aritméticos, sosteniendo que la consistencia del método de inducción matemática nunca podría ser probada sino a través del propio método inductivo.*
>
> *Pero, como muestra mi teoría, entran en juego dos métodos distintos que proceden recursivamente cuando se establecen los fundamentos de la aritmética: por un lado, la construcción intuitiva del número entero como numeral (a la que también corresponde, a la inversa, la descomposición de cualquier numeral dado, o la descomposición de cualquier arreglo dado concretamente y construido exactamente como un numeral), es decir, la inducción con contenido* [material]*; y, por otro lado, la inducción formal propiamente dicha, que se basa en el axioma de inducción y sólo a través de la cual la variable matemática puede comenzar a desempeñar su papel en el sistema formal.*
>
> *Poincaré llega a su convicción equivocada al no distinguir entre estos dos métodos de inducción, que son de índole completamente diferente.*

Parece ser que, para Hilbert, la diferencia es que una cosa es el principio formal de inducción que nos permite asegurar que todos (los infinitos) números naturales cumplen algo, con la inducción necesaria para razonar exclusivamente con objetos finitos. En una conferencia que daría en Bolonia el año siguiente lo explicaría con más detalle:

> *Por lo tanto, cuando quiero determinar si una fórmula, tomada como axioma, conduce a una contradicción, la pregunta es si se me puede presentar una prueba que conduzca a una contradicción. Si no se me puede presentar tal prueba, mucho mejor; me ahorro la molestia de tener que reaccionar. Si se me presenta tal prueba, tengo derecho a extraer ciertas partes de ella y considerarlas por sí mismas, y, en particular, a descomponer de nuevo los numerales que, compuestos y construidos, aparecen en ellas. Esto aún no emplea la inferencia de n a $n+1$ de ninguna manera.*

Es decir, Hilbert se plantea qué pasaría si alguien le presentara una prueba de una contradicción. Sería una prueba con un número fijo n de pasos, y la teoría de la demostración pretende dar un argumento que muestre que, ante una prueba así, llegaríamos a un absurdo, por lo que tal prueba no puede existir, pero eso no requiere razonar nada sobre todos los números naturales, sino sólo para todos los números naturales hasta un máximo determinado por la hipotética prueba concreta.

Jacques Herbrand explicaría esto así tres años más tarde diciendo que, en la teoría de la demostración, un argumento inductivo

> *no es más que la indicación en una fórmula de un procedimiento que habrá que aplicar un número finito de veces en cada caso particular.*

Respecto a Brouwer, a modo de resumen, Hilbert dice que *quitarle a un matemático el tercio excluso sería como, digamos, prohibirle el telescopio al astrónomo, o al boxeador el uso de sus puños.*

En su conclusión, Hilbert "se viene arriba" y predice cómo terminará su proyecto de fundamentación de las matemáticas:

> *Ya en este momento me gustaría afirmar cuál será el resultado final: las matemáticas son una ciencia sin presupuestos. Para fundamentarlas, no necesito a Dios, como Kronecker, ni la suposición de una facultad especial de nuestro entendimiento en sintonía con el principio de inducción matemática, como Poincaré, ni la intuición primordial de Brouwer, ni, finalmente, como Russell y Whitehead, axiomas de infinitud, reducibilidad o completitud, que de hecho son supuestos fácticos y con contenido que no pueden ser compensados por pruebas de consistencia.*

Es inevitable ver aquí un cierto grado de cabezonería por su parte, pues está diciendo que sus pruebas de consistencia finitistas no tienen presupuesto alguno, lo cual es simplemente absurdo. Lo máximo que se le puede conceder (como intención plausible, no como hecho) es que sus argumentos finitistas no requieren ninguna consideración sobre qué podemos decir —según la lógica, o según la intuición o según lo que sea— sobre conjuntos infinitos, porque nunca se tiene en consideración ningún conjunto infinito.

Ackerman ayudó a Hilbert a transformar en un libro las conferencias que había dado en los últimos años sobre lógica matemática en un libro, que fue publicado en **1928** con el título de *Fundamentos de la lógica teórica,* que puede considerarse el primer tratado moderno de la teoría de la demostración, y el primero en el que se presenta el concepto moderno de teoría axiomática formal (de primer orden).

Pero pasemos finalmente a analizar en qué consiste la teoría de la demostración de Hilbert.

Hasta hacía pocos años, los matemáticos interesados en el estudio del razonamiento, es decir, los lógicos, habían sido una reducida minoría. Los matemáticos siempre habían razonado "razonando", sin necesidad de consultar nada a los lógicos. Por ejemplo, Zermelo podía razonar que, dados dos conjuntos a y b, a partir de su axioma II se puede concluir que existe un conjunto $\{a, b\}$ cuyos elementos son a y b, y por su axioma V aplicado a este conjunto, existe un conjunto $a \cup b$ cuyos elementos son los que están en a y los que están en b. Y nadie en su sano uso de razón cuestionará que, en efecto, todos estos razonamientos son consecuencias lógicas de los axiomas, pero si escribimos las fórmulas que expresan estas afirmaciones una debajo de la otra:

1. $\bigwedge ab \bigvee x(\bigwedge u(u \in x \leftrightarrow u = a \vee u = b))$.
2. $\bigwedge x \bigvee y \bigwedge u(u \in y \leftrightarrow \bigvee v(u \in v \wedge v \in x))$.
3. $\bigwedge ab \bigvee y \bigwedge u(u \in y \leftrightarrow u \in a \vee u \in b)$.

¿podemos dar un criterio puramente formal que nos permita justificar que, en efecto, la tercera fórmula es consecuencia lógica de los dos primeros axiomas? Lo de "puramente formal" significa que no vale leer lo que significan los dos axiomas, entenderlo, leer lo que dice la conclusión, entenderlo y concluir: sí, si suponemos que esos dos axiomas son verdad, la conclusión también tiene que ser verdad. Se trata de dar un criterio que no aluda al significado pretendido de las fórmulas, aunque tal criterio requiriera que el argumento se detallara aún más intercalando varios pasos intermedios. Así, la cuestión es si todo razonamiento matemático se puede detallar lo suficiente (aunque fuera tedioso hacerlo) de modo que un algoritmo comprobara mecánicamente que corresponde a una deducción matemática correcta.

Lo que Hilbert había esbozado en Münster y desarrollado en sus *Fundamentos de la lógica* era una forma de hacer esto, con lo que las demostraciones matemáticas (incluso las que trataban sobre conjuntos infinitos) se convertían en objetos matemáticos susceptibles de ser analizados en un marco finitista. Para ello, Hilbert, además de los axiomas matemáticos, como los de Zermelo, introducía una lista de axiomas lógicos, que expresaban "verdades lógicas", que no dependían de la interpretación de ninguno de los signos no definidos de la teoría. En realidad, los axiomas lógicos eran infinitos, y se introducían mediante esquemas. Por ejemplo, un esquema axiomático de los que proponía Hilbert era:

$$(\alpha \to (\beta \wedge \neg\beta)) \to \neg\alpha$$

donde α y β son fórmulas cualesquiera. Para cada par de fórmulas concretas que pongamos en el esquema anterior, obtenemos un axioma lógico. Lo que expresa este esquema es el llamado principio de no contradicción:

> *Si suponemos que si una fórmula α es cierta también tienen que serlo otra fórmula β y su negación, entonces lo que es cierto es la negación de α.*

Éste era uno de los quince esquemas de axiomas lógicos que Hilbert proponía en su artículo de 1927. Pero estos axiomas serían inútiles si no se acompañan también de al menos una regla de inferencia, es decir, un criterio para añadir a un razonamiento una fórmula que no sea un axioma. Hilbert sólo necesitó una, la regla del *modus ponens*, según la cual, si en una demostración hemos escrito una fórmula de tipo $\alpha \to \beta$ y también la fórmula α, podemos añadir la fórmula β. De este modo, una *deducción formal* puede definirse como sigue:

> Una deducción formal a partir de unas premisas expresadas en un lenguaje formal prefijado es una sucesión finita de fórmulas $\alpha_1, \ldots, \alpha_n$ de dicho lenguaje formal de modo que, cada una de ellas es, o bien una premisa, o bien un axioma lógico, o bien se deduce por una regla de inferencia de dos fórmulas precedentes de la sucesión. Se dice que una fórmula α es una *consecuencia lógica* de unas premisas si existe una deducción formal con dichas premisas que termine con la fórmula α.

Esta definición se puede aplicar a distintos sistemas lógicos, con distintas elecciones de axiomas y reglas de inferencia, pero se planteaba entonces la cuestión de qué axiomas lógicos y qué reglas de inferencia era necesario adoptar para tener la garantía de que "ser una consecuencia lógica" en este sentido coincida con lo que un matemático entiende por "ser una consecuencia lógica" sin pensar en axiomas lógicos ni en unas reglas de inferencia prefijadas.

En efecto, un matemático entiende que una fórmula α es consecuencia lógica de unas premisas si razonando "como Dios le dé a entender" puede concluir que si las premisas son ciertas, la fórmula α también tiene que ser cierta. Cuando esto sucede, ¿tal razonamiento puede expresarse como una deducción en el sistema de Hilbert, o quizá en otro más adecuado?

Hilbert y Ackermann plantearon explícitamente el problema en su tratado eliminando el "como Dios le dé a entender", lo cual requiere una precisión. Hay que suponer que el matemático razona que α es una consecuencia necesaria de las premisas "como Dios le dé a entender" —es decir, sin poner límites *a priori* en el tipo de argumentos que está legitimado a usar— pero siempre y cuando sus argumentos sean puramente formales, es decir, que no tenga en cuenta para nada el posible significado de los signos no definidos del lenguaje formal que aparezcan en las fórmulas distintos de los signos lógicos (como $\wedge$, $\bigwedge$, $=$, etc.). En el supuesto de que las fórmulas tengan un significado claro y preciso, lo que se pueda deducir teniendo esto en cuenta es harina de otro costal.

Lo que Hilbert y Ackermann pretendían con su definición de deducción formal era capturar el concepto que los matemáticos tienen de deducción formal, es decir, lo que un matemático (sin ninguna restricción *a priori* más allá de ceñirse a lo que se lee en las fórmulas, sin atribuirles ningún significado específico) puede razonar lógicamente. Por ejemplo, si a un matemático se le dice que $x \in y \vee x \in z$ y que $x \notin y$ (es decir, que no $x \in y$), asegurará que de ahí puede concluir que $x \in z$ signifique lo que signifique el signo $\in$.

Así, cuando un matemático razona en términos puramente formales "como Dios le dé a entender" que si unas premisas $\alpha_1, \ldots, \alpha_r$ son verdaderas también tiene que serlo una conclusión α, lo que está argumentando es que, para cualquier interpretación de los signos no definidos del lenguaje formal que haga que las premisas sean verdaderas, la conclusión también tiene que serlo. Pero una interpretación de los signos de un lenguaje formal que haga verdaderas a unas fórmulas es lo que llamamos un modelo de dichas fórmulas, y así llegamos al enunciado que Hilbert y Ackermann dejaron planteado en su tratado:

> *Supongamos que $\alpha_1, \ldots, \alpha_r$ son fórmulas de un lenguaje formal, y que α es otra fórmula que es verdadera en todos los modelos de $\alpha_1, \ldots, \alpha_r$. ¿Puede entonces deducirse formalmente α a partir de $\alpha_1, \ldots, \alpha_r$?*

El "como Dios le dé a entender" está implícito aquí en que no imponemos ninguna restricción en cómo se convence un matemático de que α tiene que ser verdadera en todos los modelos de las premisas. La cuestión es: si aceptamos que un matemático ha demostrado esto "como Dios le dé a entender", ¿existirá necesariamente una deducción formal de α a partir de las premisas?

Hilbert y Ackermann plantearon la pregunta concretamente para la definición que habían dado de "deducción formal", con los axiomas lógicos y la regla de inferencia que habían propuesto. Habían constatado que prácticamente cualquier forma de razonamiento que emplean los matemáticos podía justificarse con sus axiomas, pero ese "cualquier forma" no admitía una concreción precisa (no estaba claro que abarcara el "como Dios le dé a entender" en toda su generalidad).

En el fondo, la pregunta era si los axiomas lógicos propuestos por Hilbert y Ackermann eran suficientes para demostrar todo lo que un matemático aceptará como demostrable o si, por el contrario, había algún razonamiento válido que requiriera incorporar más axiomas lógicos o más reglas de inferencia a la definición de demostración formal.

39 El teorema de completitud semántica En **1928** tuvo lugar en Bolonia el *Octavo Congreso Internacional de Matemáticos.* En los dos últimos, celebrados en 1920 y 1924, como consecuencia de la Primera Guerra Mundial, se había prohibido la presencia de matemáticos alemanes y de lo que habían sido las Potencias Centrales, mientras que en Bolonia los matemáticos alemanes fueron admitidos con restricciones. Brouwer, que era neerlandés, y no estaba afectado por las restricciones, exigió que éstas fueran eliminadas y, en caso contrario, animó a un boicot. Pero Hilbert, que encabezaba la delegación alemana y había sido uno de los principales responsables de las negociaciones para su readmisión, se molestó mucho por la actitud de Brouwer.

En Bolonia Hilbert anunció que, con sus técnicas se había logrado demostrar la consistencia de la aritmética, y que pronto se llegaría a una prueba de la consistencia del análisis (es decir, de la teoría sobre los números reales). En efecto, Ackermann creía haber resuelto el problema detectado en su tesis doctoral, pero, aunque entonces no se sabía, la demostración corregida seguía siendo inválida.

Hilbert estaba en el comité editorial de los *Anales matemáticos,* de la que Brouwer era editor adjunto, y maniobró para expulsar a Brouwer. Otros miembros del comité editorial, como Albert Einstein y Constantin Carathéodory, se opusieron indignados a lo que sin duda era un abuso de autoridad, pero la mayoría del comité no quiso enemistarse con Hilbert y, pese a las protestas de Brouwer, en **1929** el comité editorial fue disuelto para ser reconstruido inmediatamente, pero sin Brouwer (ni Einstein ni Carathéodory, que renunciaron).

A Brouwer le afectó mucho este incidente, que se unió al disgusto que se llevó cuando en un tranvía de Bruselas le robaron su maletín lleno de manuscritos que juzgó que nunca podría reconstruir, así como a una polémica que suscitó Karl Menger sobre quién había dado primero la definición correcta de dimensión topológica. La relación entre Hilbert y Brouwer se parecía cada vez más a la que habían mantenido Kronecker y Peano.

Al congreso de matemáticos de Bolonia había asistido un joven estudiante de la Universidad de Viena que había leído el libro de Hilbert y Ackermann y se había interesado enormemente por la lógica matemática. En **1929** eligió el problema de la suficiencia de los axiomas lógicos para su tesis doctoral, y ese mismo año, a sus 23 años, demostró lo que ahora se conoce como teorema de completitud semántica. Con sus 25 páginas, fue una de las tesis doctorales más breves de la historia. El joven se llamaba Kurt Gödel. Su demostración del teorema de completitud semántica se basaba en un resultado de gran interés en sí mismo, al que a menudo se le llama también teorema de completitud semántica:

> Si una colección de fórmulas de un lenguaje formal es consistente (es decir, si a partir de ellas no se puede deducir formalmente ninguna contradicción), entonces tiene un modelo de universo finito o numerable.

Conviene destacar algunas observaciones sobre este resultado:

1. En el enunciado hay que entender que "no se puede deducir una contradicción" hace referencia a una deducción a partir de los axiomas y reglas de inferencia de Hilbert y Ackermann, pero el argumento se podía adaptar fácilmente a cualquier otro cálculo deductivo, con otros axiomas o reglas de inferencia, que cumpliera unos requisitos mínimos, es decir, que permitiera expresar los razonamientos concretos que requería la prueba del teorema.

2. La colección de fórmulas podía ser finita o infinita. Por ejemplo, los axiomas de Zermelo, o de Zermelo-Fraenkel son infinitos, pero se les puede aplicar el teorema de completitud: si son consistentes, es decir, si a partir de ellos no se puede probar ninguna contradicción, entonces tienen un modelo, es decir, existen unos objetos que, con una relación de pertenencia definida adecuadamente, cumplen los axiomas de la teoría de conjuntos.

3. El recíproco del teorema es trivial: si una colección de fórmulas de un lenguaje formal admite un modelo, entonces es consistente, por lo que podemos afirmar que una teoría axiomática es consistente si y sólo si tiene un modelo.

   En efecto, si M es un modelo de una colección de fórmulas dada, es decir, si dichas fórmulas son verdaderas en M, también lo serán todas sus consecuencias lógicas, luego no es posible demostrar ninguna contradicción a partir de ellas, pues una misma fórmula no puede ser verdadera y falsa a la vez en un mismo modelo.

4. Esto reforzaba la postura de Hilbert, según la cual, lo único que hacía falta para legitimar la adopción de unos axiomas era justificar su consistencia, pues Gödel demostraba que si unos axiomas son consistentes, no hay peligro de que "no hablen de nada", es decir, de que no existan objetos que cumplan los axiomas considerados. Siempre los habrá. Cualquier teoría axiomática consistente habla de algo, tiene un significado posible.[53]

[53] La postura oficial de Hilbert en esa época era que las afirmaciones sobre conjuntos infinitos no tienen ningún significado, pero hacía unas décadas Hilbert había sostenido justamente lo que ahora demostraba Gödel. En una carta a Frege de 1899 decía:

Usted escribe "de la verdad de los axiomas se deduce que no se contradicen unos a otros". He leído con gran interés esta afirmación suya, porque, de hecho, siempre que he pensado, escrito y dado clases sobre estas cosas, he dicho justo lo contrario: Si unos axiomas elegidos arbitrariamente, junto con todas sus consecuencias, no se contradicen mutuamente, entonces son verdaderos, y las cosas definidas por los axiomas existen. Para mí, ése es el criterio de verdad y existencia.

5. Otra cosa es que ese significado sea el pretendido, pues el teorema de Gödel implica que, si la teoría de conjuntos es consistente, entonces tiene un modelo numerable, tal y como había señalado Skolem.[54] De hecho, el teorema de Gödel implica en particular el teorema de Löwenheim-Skolem, pues si una familia de fórmulas admite un modelo, entonces es consistente (porque todas las consecuencias lógicas de tales fórmulas serán verdaderas en el modelo, luego no puede demostrarse a partir de ellas ninguna contradicción) y si es consistente, entonces admiten un modelo finito o numerable.

No vamos a discutir la demostración de este teorema sobre existencia de modelos, porque más adelante se obtendrían demostraciones conceptualmente más simples, pero citamos un pasaje de la prueba:

> *Entonces existen sistemas satisfactorios de cada nivel. Pero, dado que para cada nivel sólo hay un número finito de sistemas satisfactorios (porque los dominios asociados de individuos son finitos) y dado que, además, todo sistema satisfactorio de nivel $n+1$ contiene uno de nivel n como parte(como se desprende del hecho de que los A_n se forman mediante conjunciones sucesivas), se deduce, por argumentos conocidos, que en este caso existe una sucesión de sistemas satisfactorios $S_1, S_2, \ldots, S_k, \ldots$ (siendo S_k de nivel k) tales que cada uno contiene al anterior como parte.*

Aun sin saber de qué está hablando Gödel, podemos adivinar que habla de un árbol formado por unos nodos que llama "sistemas satisfactorios" ordenados en niveles finitos por la inclusión, por lo que los "argumentos conocidos" que le dan una rama de dicho árbol son el teorema de Kőnig que hemos discutido en la sección 37. Esto es relevante porque cualquier demostración del teorema de incompletitud involucra el trato con conjuntos infinitos que exceden los límites de lo que podríamos llamar el finitismo más estricto, pero puede probarse que el teorema de Kőnig es el único ingrediente no estrictamente finitista que requiere la prueba del teorema de completitud (en el sentido de que se puede dar una prueba basada exclusivamente en principios finitistas más dicho teorema). El lector puede meditar ahora si le parece razonable afirmar que el teorema de Kőnig es un ejemplo de enunciado que, aunque no se lo tenga por estrictamente finitista, podemos afirmar que tiene un significado intuitivo claro y preciso y que es verdadero.

Lo que sí que podemos hacer es demostrar el teorema de completitud semántica a partir del teorema de Gödel que acabamos de comentar:

Demostración: Tenemos que probar que si una fórmula α es verdadera en todos los modelos de unas premisas $\alpha_1, \ldots, \alpha_r$, entonces es deducible de las premisas (en el sentido preciso de un cálculo deductivo, como por ejemplo el de Hilbert y Ackermann que tomó Gödel como referencia). Esto equivale a demostrar el recíproco: si α no es deducible a partir de $\alpha_1, \ldots, \alpha_r$, existe un modelo de las premisas en el que α es falso o, equivalentemente, existe un modelo de $\alpha_1, \ldots, \alpha_r, \neg\alpha$. Ahora bien, basta observar que si α no es deducible a partir de $\alpha_1, \ldots, \alpha_r$, entonces las fórmulas $\alpha_1, \ldots, \alpha_r, \neg\alpha$ son consistentes (pues entonces tienen un modelo por el teorema que probó Gödel), y esto es cierto, pues si se pudiera demostrar una contradicción a partir de ellas, eso significaría que, suponiendo $\alpha_1, \ldots, \alpha_r$, al suponer $\neg\alpha$ se llega a una contradicción, y eso es una demostración de α por reducción al absurdo (algo expresable en el cálculo deductivo de Hilbert y Ackermann), luego tendríamos una demostración de α a partir de $\alpha_1, \ldots, \alpha_r$, en contra de lo supuesto. ∎

40 El axioma de regularidad En **1929** von Neumann publicó un segundo artículo sobre su teoría de funciones, en el que sustituyó el axioma de limitación de tamaño por el axioma del reemplazo y el axioma de elección fuerte (que afirma que la clase V admite un buen orden), y demostró que si la teoría resultante era consistente, lo seguía siendo al añadir el axioma de limitación de tamaño.

Las ideas involucradas en la prueba son muy interesantes, pero explicarlas en términos de la exótica teoría de funciones de von Neumann sería artificioso. No obstante, las ideas más importantes aparecerían también en términos mucho más simples en un artículo que Zermelo publicó en **1930** titulado *Sobre números frontera y dominios de conjuntos. Nuevas investigaciones sobre los fundamentos de la teoría de conjuntos.*

Pero el artículo de Zermelo también es un tanto *sui generis,* porque en él se combinan algunas excentricidades, con algunas falsedades y con algunos resultados correctos, por lo que su análisis es delicado.

[54] Por esas fechas muchos matemáticos seguían viendo la paradoja de Skolem como una contradicción. El año anterior, en 1928, Fraenkel se había referido a ella como una "antinomia" y ese mismo año, en 1929, fue cuando Zermelo empezó a cuestionar que los lenguajes formales y el concepto de demostración que estaban estudiando Hilbert y sus colaboradores fueran adecuados para la teoría de conjuntos, precisamente porque permitían la paradoja de Skolem. Insistimos, no obstante, en que la llamada paradoja de Skolem no es realmente ninguna paradoja, en cuanto que no supone contradicción alguna.

En primer lugar, "por generalidad" —según explicaría Bernays— Zermelo se empeñó en admitir la existencia de un conjunto de elementos primitivos que no eran conjuntos, pese a que ya estaba claro que eran innecesarios.[55] En lo que sigue, particularizaremos las afirmaciones de Zermelo al caso en que no existen elementos primitivos. Por ejemplo, ahora Zermelo introducía los ordinales y los cardinales mediante las definiciones de von Neumann,[56] pero obtenía unos ordinales distintos (aunque todos equivalentes) en función de qué elemento primitivo tomara como conjunto vacío (o, equivalentemente, como ordinal 0). Nosotros consideraremos únicamente el caso en que hay un único conjunto vacío y omitiremos todos los tecnicismos que conlleva esta falta de unicidad.

Por otro lado, Zermelo omite el axioma de elección de su lista de axiomas, pero a la vez dice que lo supone como "un principio lógico general" por el que supondrá que todo conjunto puede ser bien ordenado.

Zermelo incorpora a su teoría el axioma de reemplazo y, siguiendo a von Neumann, se refiere a la teoría resultante como "el sistema de axiomas de Zermelo-Fraenkel". Aprovechamos este punto para presentar este axioma, que venimos mencionando desde hace un tiempo sin haberlo enunciado. Zermelo lo enuncia esencialmente así:

> *Si los elementos x de un conjunto a se reemplazan de forma única por conjuntos arbitrarios x', existe un conjunto cuyos elementos son esos conjuntos x'.*

Como sucedía con su enunciado del axioma de especificación, esta formulación deja abierta una "brecha" al no dejar claro cómo se define el "se reemplazan". Un enunciado riguroso requiere especificar que dicho reemplazo está determinado por una fórmula $\phi(x,y)$ del lenguaje de la teoría de conjuntos. Concretamente, el axioma de reemplazo es en realidad un esquema axiomático tal que, para cada fórmula $\phi(x,y)$ del lenguaje de la teoría de conjuntos, la fórmula siguiente es un axioma:

$$\bigwedge a(\bigwedge x \in a \overset{1}{\bigvee} y\, \phi(x,y) \to \bigvee b \bigwedge y(y \in b \leftrightarrow \bigvee x \in a\, \phi(x,y))),$$

donde $\overset{1}{\bigvee} y$ significa "existe un único y". Así, el axioma dice que si para cada $x \in a$ existe un único conjunto y que cumple $\phi(x,y)$, existe un conjunto b cuyos elementos son los que resultan de reemplazar cada $x \in a$ por el único conjunto y que cumple $\phi(x,y)$.

Otro punto insólito es que Zermelo omite el axioma de infinitud de su lista de axiomas, porque dice que no corresponde a "la teoría de conjuntos general". En realidad, lo que pretende Zermelo es estudiar la teoría de conjuntos con y sin el axioma de infinitud, por lo que va a usarlo a veces sí y a veces no.

Pero el punto más interesante es la introducción de un nuevo axioma que él llama *axioma de fundación,* del que nos ocupamos a continuación, pero al que nos referiremos como axioma de regularidad. (En la actualidad coexisten ambas denominaciones.)

Von Neumann había observado, al igual que Skolem, de forma independiente, que los axiomas de Zermelo no impedían la existencia de conjuntos "patológicos", como un conjunto x que fuera su único elemento (es decir, que cumpliera $x = \{x\}$) o de un par de conjuntos tales que $x = \{y\}$, $y = \{x\}$, o incluso una sucesión de conjuntos

$$x_0 = \{x_1\}, \quad x_1 = \{x_2\}, \quad x_2 = \{x_3\}, \quad \ldots$$

En su artículo de 1925, von Neumann había propuesto un axioma que eliminaba algunos de estos conjuntos, pero no todos, y en su artículo de 1929 había propuesto otro que los eliminaba todos, al que llamó axioma de fundación, pero, debido al exotismo de su teoría de funciones, la formulación del axioma de von Neumann era enrevesada.

Todos estos conjuntos tienen en común que permiten construir sucesiones infinitas respecto de la relación inversa de la pertenencia. Por ejemplo, si $x = \{x\}$ o, simplemente, si $x \in x$, podemos formar la sucesión

$$x \ni x \ni x \ni x \ni x \ni \cdots$$

Si $x = \{y\}$, $y = \{x\}$, o simplemente si $x \in y$, $y \in x$, tenemos

$$x \ni y \ni x \ni y \ni x \ni \cdots$$

Esto nos lleva a definir un conjunto *regular* como un conjunto tal que no existen sucesiones infinitas de este tipo que empiezan en x.

[55] Bernays atribuye este convenio a Paul Finsler.

[56] Esto suponía un cambio respecto a su construcción de los números naturales, pues en su artículo de 1908 se identificaban con los conjuntos $0 = \varnothing,\ 1 = \{0\},\ 2 = \{1\},\ 3 = \{2\}$, y ahora pasaban a ser $0 = \varnothing,\ 1 = \{0\}, 2 = \{0,1\},\ 3 = \{0,1,2\}$, etc.

Zermelo enunció el axioma de regularidad de dos formas equivalentes: como que todos los conjuntos son regulares, y también como que todo conjunto no vacío x posee un elemento $y \in x$ sin elementos en común con x. Formalmente:[57]

$$\bigwedge x(x \neq \varnothing \to \bigvee y(y \in x \wedge y \cap x = \varnothing)).$$

Así pues, si admitimos el axioma de regularidad, ningún conjunto se pertenece a sí mismo y, en términos de la teoría de von Neumann, la clase de todos los conjuntos que no se pertenecen a sí mismos coincide con la clase de todos los conjuntos.

Vamos a ver que el axioma de regularidad impone una estructura muy clara en el universo conjuntista. Para ello vamos a definir una sucesión transfinita de conjuntos. Empezamos con

$$V_0 = \varnothing, \quad V_1 = \mathcal{P}V_0 = \{\varnothing\}, \quad V_2 = \mathcal{P}V_1 = \{\varnothing, \{\varnothing\}\}, \quad V_3 = \mathcal{P}V_2 = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}, \quad \ldots$$

De este modo obtenemos una sucesión de conjuntos finitos, de cardinal $0, 1, 2, 4, 8, \ldots$ y, admitiendo el axioma de infinitud, con ellos podemos formar el conjunto infinito[58]

$$V_\omega = \bigcup_{n<\omega} V_n,$$

que acumula todos los conjuntos obtenidos hasta el momento. No es difícil ver que la sucesión es creciente:

$$V_0 \subset V_1 \subset V_2 \subset V_3 \subset \cdots \subset V_\omega.$$

Pero, al igual que sucedía con la sucesión de conjuntos derivados de Cantor, el hecho de que hayamos podido prolongar la sucesión de los V_n con V_ω nos permite continuar tomando conjuntos de partes:

$$V_{\omega+1} = \mathcal{P}V_\omega, \quad V_{\omega+2} = \mathcal{P}V_{\omega+1}, \quad V_{\omega+3} = \mathcal{P}V_{\omega+2}, \quad \ldots$$

y así tenemos una sucesión doblemente infinita que sigue siendo creciente:

$$V_0 \subset V_1 \subset V_2 \subset V_3 \subset \cdots \subset V_\omega \subset V_{\omega+1} \subset V_{\omega+2} \subset V_{\omega+3} \subset \cdots$$

Pero la sucesión no acaba ahí, sino que podemos definir $V_{\omega\cdot 2} = \bigcup_{\alpha<\omega\cdot 2} V_\alpha$, y de nuevo podemos continuar con $V_{\omega\cdot 2+1} = \mathcal{P}V_{\omega\cdot 2}$, etc.

En este punto el lector debe recordar lo que es una sucesión transfinita, una sucesión que no se detiene sólo porque llegue a una "cola infinita". Detrás de esa "cola" está definido un nuevo término de la sucesión.

En general, en la teoría de Zermelo-Fraenkel podemos asociar a cada ordinal α un conjunto V_α por recursión transfinita mediante

$$V_0 = \varnothing, \qquad V_{\alpha+1} = \mathcal{P}V_\alpha, \qquad V_\lambda = \bigcup_{\alpha<\lambda} V_\alpha,$$

donde λ hace referencia a un ordinal límite arbitrario.

Esta construcción aparece por primera vez en el artículo de Zermelo, pero se atribuye a von Neumann, y se conoce como la *jerarquía acumulativa de von Neumann.* Con palabras: partimos del conjunto vacío, en cada ordinal sucesor calculamos el conjunto de partes del término anterior de la jerarquía, y en los ordinales límite acumulamos todos los conjuntos obtenidos hasta el momento. En términos de la teoría de von Neumann (pero no en la de Zermelo-Fraenkel) podemos definir la clase (que no tiene nada que ver con la clase de Russell)

$$R = \bigcup_{\alpha\in\Omega} V_\alpha,$$

donde Ω es la clase de todos los ordinales y se puede demostrar que R no es sino la clase de todos los conjuntos regulares.

[57] Notemos que si existe una cadena decreciente

$$x_0 \ni x_1 \ni x_2 \ni x_3 \ni \cdots$$

el conjunto x formado por todos los x_n es no vacío y no tiene elementos disjuntos con él mismo (puesto que $x_{n+1} \in x \cap x_n$). Recíprocamente, si x no tiene elementos disjuntos con él mismo, podemos tomar un $x_0 \in x$ y, como $x_0 \cap x \neq \varnothing$, podemos tomar $x_1 \in x_0 \cap x$ y, como $x_1 \cap x \neq \varnothing$, podemos tomar $x_2 \in x_1 \cap x$, y así construimos una sucesión que prueba que x no es regular.

[58] Aquí tenemos un caso típico del uso del axioma del reemplazo. Sin él, podemos dar una definición precisa de $y = V_n$, es decir, esta igualdad se puede expresar como una fórmula $\phi(n, y)$ del lenguaje de la teoría de conjuntos, pero ninguno de los axiomas de Zermelo nos asegura que exista un conjunto X que contenga a todos los V_n. Esto nos lo asegura precisamente el axioma del reemplazo, que nos permite partir del conjunto ω de todos los números naturales y reemplazar cada n por V_n para formar un conjunto X, y entonces podemos definir $V_\omega = \bigcup X$.

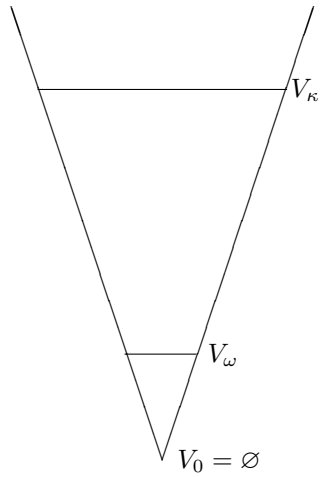
En efecto, por una parte, si $x \in R$ (o, en términos de ZF, si x pertenece a algún V_α), podemos considerar el menor ordinal α tal que $x \in V_\alpha$, que, obviamente, no puede ser $\alpha = 0$ y tampoco puede ser un ordinal límite, pues en tal caso V_α sería la acumulación de los conjuntos de los niveles precedentes de la jerarquía, y x estaría en un V_δ anterior, en contra de la minimalidad de α. Por lo tanto, dicho mínimo es de la forma $\alpha = \rho + 1$. u así tenemos que $x \in V_{\rho+1} = \mathcal{P}V_\rho$, pero $x \notin V_\rho$.

El ordinal ρ se llama *rango* del conjunto x (y se representa por $\operatorname{rang} x$), y es el mínimo ordinal tal que $x \in V_{\rho+1}$ o tal que $x \subset V_\rho$. En estos términos, V_α es el conjunto de los conjuntos de rango menor que α.

De este modo, el rango de un conjunto es una medida de su complejidad, es decir, del número de pasos que hay que dar para construirlo a partir del conjunto vacío. Se puede demostrar que si dos conjuntos cumplen $x \in y$, entonces $\operatorname{rang} x < \operatorname{rang} y$, y de aquí se sigue que todos los conjuntos de R son regulares, porque si $x \in R$ y existe una sucesión

$$x = x_0 \ni x_1 \ni x_2 \ni x_3 \ni \cdots$$

entonces tendríamos una sucesión decreciente de ordinales. También se puede probar el recíproco, es decir, que todo conjunto regular está en algún V_α, pero no vamos a dar aquí los detalles.



Lo importante es que así vemos que el axioma de regularidad equivale a que todo conjunto está en la en la jerarquía de von Neumann o, en términos de las clases de von Neumann, que $V = R$. En particular, todo conjunto tiene definido su rango, que mide su complejidad.

La figura ilustra la estructura de la clase R de los conjuntos regulares (o de la clase V de todos los conjuntos si admitimos el axioma de regularidad). Hay un "primer conjunto" (el único de rango 0) que es el conjunto vacío. Aplicando sucesivamente la operación "conjunto de partes" llegamos hasta el conjunto V_ω formado por los conjuntos *hereditariamente finitos,* es decir, los conjuntos finitos cuyos elementos son conjuntos finitos cuyos elementos son conjuntos finitos cuyos elementos son conjuntos finitos, etc. Y si continuamos aplicando el operador de partes una cantidad transfinita de veces (es decir, sin detenernos por el mero hecho de llegar a una "cola infinita", sino acumulándola para continuar) obtenemos sucesivamente todos los conjuntos.

Von Neumann y Skolem observaron de forma independiente que los axiomas de la teoría de conjuntos no dejan de cumplirse si nos quedamos únicamente con los conjuntos regulares, es decir, que si existen unos objetos que cumplen los axiomas de la teoría de conjuntos y nos deshacemos de los que no son regulares, los conjuntos que quedan siguen cumpliendo los axiomas de la teoría de conjuntos, y además cumplen el axioma de regularidad.

Por ejemplo, un axioma afirma que, dados dos conjuntos x, y, existe el conjunto $\{x, y\}$, pero si los conjuntos x, y son regulares, es fácil ver que también lo es $\{x, y\}$, por lo que alguien que sólo vea los conjuntos regulares no encontrará ningún fallo en el axioma del par: siempre que ve dos conjuntos (regulares), ve el par formado por ellos (porque también es regular), y lo mismo se puede razonar con los demás axiomas.

La consecuencia es que, si los axiomas de la teoría de conjuntos son consistentes, también lo son al añadir el axioma de regularidad (basta aplicar el teorema de completitud: si la teoría de conjuntos es consistente, tiene un modelo, y si en ese modelo eliminamos los conjuntos no regulares, obtenemos un modelo de la teoría más el axioma de regularidad, luego ésta es consistente).

El axioma de regularidad no tardó en ser considerado como uno más de los axiomas de la teoría de conjuntos de Zermelo-Fraenkel, aunque cabe resaltar que, para la mayor parte de las matemáticas, es irrelevante. A la hora de demostrar teoremas sobre álgebra, análisis, topología, etc., no importa lo más mínimo que haya o no haya conjuntos no regulares.

No obstante, von Neumann le sacó partido al axioma. Suponiendo que su teoría de funciones es consistente, demostró que también lo es si se le añade el axioma de regularidad y, entonces, usando este axioma y la versión fuerte del axioma de elección (el que afirma que la clase universal puede ser bien ordenada) pudo demostrar que la clase universal es biyectable con la clase Ω de todos los ordinales y, de ahí, que se cumple el axioma de limitación de tamaño. De este modo, tal y como indicábamos, obtuvo que si su teoría de funciones es consistente, también lo es al añadirle el axioma de limitación de tamaño.

41 Cardinales fuertemente inaccesibles Zermelo trató de llevar mucho más lejos el argumento de Skolem y von Neumann. Para explicar su propósito necesitamos introducir el concepto siguiente:

> Un cardinal *(fuertemente) inaccesible* es un cardinal límite regular no numerable κ tal que para todo cardinal $\mu < \kappa$ se cumple que $2^\mu < \kappa$.

Recordemos que Hausdorff ya había considerado los cardinales débilmente inaccesibles, que resultan de suprimir la última condición en la definición precedente. Hausdorff los había calificado de "exorbitantes", pero más como una forma ponderar lo grandes que debían ser que como una definición, pero Zermelo cita a Hausdorff para llamar *cardinales exorbitantes* a los débilmente inaccesibles, mientras que a los fuertemente inaccesibles los llama *cardinales frontera.* Ese mismo año de **1930** Sierpiński y Tarski publicaron un artículo en el que atribuían a Kuratowski el nombre de "cardinales inaccesibles" para los cardinales débilmente inaccesibles, pero a la vez advertían que ellos iban a llamar "inaccesibles" a los cardinales fuertemente inaccesibles. Desde entonces ha habido siempre cierta vacilación sobre si por "inaccesible" hay que entender débilmente o fuertemente inaccesible.

Volviendo al artículo de Zermelo, éste define un *dominio normal* como un conjunto cuyos elementos cumplen los axiomas de Zermelo-Fraenkel (sin exigir el axioma de infinitud), es decir, como un conjunto D tal que, si decidimos llamar "conjuntos" únicamente a los elementos de D (con la misma relación de pertenencia que estamos considerando), se siguen cumpliendo todos los axiomas de ZF. En términos modernos, esto es lo que se llama un *modelo natural* de ZF, donde "natural" indica que no redefinimos la relación de pertenencia, sino que mantenemos la misma.

Zermelo demuestra que si $\kappa = \omega = \aleph_0$, o bien κ es un cardinal fuertemente inaccesible, entonces V_κ es un dominio normal. Esto significa que si vamos construyendo la jerarquía de von Neumann, al llegar a V_ω ya tenemos suficientes conjuntos para que se cumplan los axiomas de ZF sin el axioma de infinitud, y esto explica por qué a partir de los demás axiomas de ZF no es posible demostrar el axioma de infinitud: los conjuntos de V_ω cumplen todos esos axiomas, pero no cumplen el axioma de infinitud. Si pudiéramos demostrarlo, tendríamos que concluir que hay un conjunto infinito en V_ω, y no lo hay.

Similarmente, si continuamos avanzando en la jerarquía de von Neumann y llegamos hasta un conjunto V_κ, donde κ es un ordinal fuertemente inaccesible, resulta que ahí "podemos parar", en el sentido de que no hacen falta más conjuntos. Con ellos ya se cumplen todos los axiomas de ZF (ahora incluyendo el axioma de infinitud), pero nada nos impide seguir prolongando la jerarquía de von Neumann y añadir más conjuntos, por innecesarios que sean. Los cardinales fuertemente inaccesibles son los puntos de la jerarquía en los que "podemos parar si queremos". Si paramos ahí, no echaremos en falta los conjuntos que podríamos añadir después, sino que con esos conjuntos ya se cumplirán todos los axiomas[59] de ZF.

El caso es que hasta aquí hemos ido filtrando los resultados de Zermelo para evitar cosas que afirma y que no son ciertas. De hecho, Zermelo creía haber demostrado que *los únicos* dominios normales eran V_ω y los V_κ, con κ fuertemente inaccesible, lo cual no es cierto. Por el contrario, si suponemos que existe un cardinal fuertemente inaccesible κ, las técnicas de Skolem permiten demostrar que existe un ordinal numerable $\lambda > \omega$ (que no es, ni de lejos, un cardinal inaccesible) tal que V_λ también es un dominio normal, y el propio teorema de Löwenheim-Skolem permite probar, más aún (siempre suponiendo que exista un cardinal fuertemente inaccesible), que existen dominios normales numerables.

Precisamente, la intención de Zermelo era burlar las consecuencias —que el juzgaba espeluznantes— del teorema de Löwenheim-Skolem, no exactamente cuestionando su validez, sino asegurándose de que no se aplicara a la teoría de conjuntos considerando en ésta lo que en los *Principia Mathematica* se llamarían "fórmulas de segundo orden", es decir, fórmulas en las que se cuantifica sobre relaciones arbitrarias de forma absoluta. Explicamos esto discutiendo uno de los errores típicos en los que incurre Zermelo.

Zermelo entiende que si M es un dominio y $x \in M$, el hecho de que M cumpla el axioma de partes se traduce en que el conjunto $\mathcal{P}x$ debe pertenecer a M (y esto bastaría para probar que M es necesariamente no numerable, en contra de lo que acabamos de señalar). Pero eso no es cierto. Para que M cumpla el axioma de partes basta con que $\mathcal{P}x \cap M \in M$. En efecto, si decidimos llamar "conjuntos" únicamente a los elementos

[59] Sin embargo, si nos conformamos con los axiomas de la teoría de Zermelo, es decir, si no consideramos el axioma del reemplazo, resulta que $V_{\omega+\omega}$ ya es suficiente para que se cumplan los axiomas de Zermelo. Vemos así que, sin el axioma del reemplazo no podemos probar la existencia de los ordinales de von Neumann desde $\omega+\omega$ (ése ya no está en $V_{\omega+\omega}$ y no hace falta que esté), pero, por otra parte, en $V_{\omega+\omega}$ hay buenos órdenes en ω de cualquier ordinal numerable, luego en $V_{\omega+\omega}$ no es cierto que todo conjunto bien ordenado sea similar a un ordinal de von Neumann. Eso a su vez indica que no se cumple el teorema de recursión transfinita para conjuntos bien ordenados. En la práctica, esto significa que estos hechos no son demostrables en la teoría de Zermelo.

de M, entonces el conjunto de todos los subconjuntos de x es $\mathcal{P}x \cap M$, pues cualquier $u \in \mathcal{P}x$ que no esté en M "era" un subconjunto de x, pero ha dejado de serlo en cuanto hemos redefinido los conjuntos como los elementos de M. Pero Zermelo se niega a admitir este último punto: para él, si admitimos que x es un conjunto, entonces sus subconjuntos son todos los y de los que podemos afirmar que $y \subset x$, sin que esté justificado excluir ninguno por el hecho de que no esté en M. Para Zermelo, si $\mathcal{P}x \cap M \in M$, pero no es cierto que $\mathcal{P}x \in M$, entonces M no cumple realmente el axioma del conjunto de partes.

Si expresamos formalmente el axioma de partes (cosa que Zermelo nunca hace)[60]:

$$\bigwedge x \bigvee y \bigwedge u(u \subset x \to u \in y)$$

la clave del asunto es que Zermelo pretende que ese "para todo u" se aplique a todos los conjuntos contenidos en x, sin restricción alguna de tipo "sólo consideramos conjuntos a los elementos de M". El caso concreto del axioma de partes Zermelo lo pasa sin comentario alguno (no es descartable que ni siquiera se hubiera dado cuenta de que ese punto en concreto era polémico), pero en otros puntos similares, donde los axiomas implicados son el de especificación o el del reemplazo, para justificarse, Zermelo remite a un artículo suyo del año anterior titulado *Sobre el concepto de buena definición en la axiomática,* donde trata de "incrustar" este tipo de "cuantificación absoluta" en la definición de "propiedad bien definida", pero lo único que pone de manifiesto con ello es que no entendía la lógica formal (cosa que también se hace patente en la correspondencia que mantendría con Gödel) y Skolem no había tardado en replicarle que lo que trataba de expresar "era vago", que era una forma elegante de decir que no tenía ni pies ni cabeza.

Con la precaución de tener en cuenta que Zermelo afirma algo más de lo que realente puede demostrar, podemos examinar ahora las consecuencias que extrae de sus resultados:

> *Y es esta clara distinción entre los diferentes modelos del sistema de axiomas (¡no categórico!) la que nos permite resolver las "antinomias ultrafinitas" a nuestra satisfacción presentando siempre los "no conjuntos" de un modelo como "conjuntos" propios en el modelo siguiente y en todos los modelos superiores.*

Así, aunque en un principio, Zermelo se había horrorizado ante la idea de que los axiomas de la teoría de conjuntos no fueran categóricos (es decir, admitieran modelos distintos, con interpretaciones distintas del concepto de "conjunto"), ahora le concedía a Skolem de buen grado que así era, pero no porque existieran modelos numerables espeluznantes (que existen, pero él seguía sin admitirlo y creía que lo acababa de refutar), sino porque pueden existir distintos modelos cada vez mayores, cada vez con más conjuntos.

Respecto a la existencia de cardinales fuertemente inaccesibles, Zermelo dice:

> *Por supuesto, no es posible "probar", es decir, deducir de los axiomas generales* ZF, *ni su existencia ni su no existencia, simplemente porque, por ejemplo, el número frontera ω, aunque existe en el dominio "cantoriano", no existe en el dominio "finitista"; porque, en otras palabras, la pregunta recibe diferentes respuestas en diferentes "modelos" de teoría de conjuntos y, por lo tanto, no se decide meramente por los axiomas solos.*

Aquí hay una mezcla de verdades y errores. En efecto, como ya hemos señalado, si no suponemos el axioma de infinitud, no podemos demostrar que exista el conjunto ω de los números naturales, porque V_ω es un modelo de los axiomas de ZF sin infinitud en el cual ω no existe, porque todos los conjuntos son finitos (a eso se refiere con "el dominio finitista"). Igualmente, aun suponiendo el axioma de infinitud, no podemos demostrar que exista un cardinal fuertemente inaccesible κ, porque si pudiéramos demostrar que existe uno, podríamos tomar el menor de todos, y considerar el conjunto V_κ, que es un modelo de ZF en el que no existen cardinales fuertemente inaccesibles, luego tendríamos una contradicción. Similarmente, aunque supongamos que existe un primer cardinal fuertemente inaccesible κ, no podemos demostrar que existe un segundo μ, porque en tal caso V_μ sería un modelo en el que hay un único cardinal fuertemente inaccesible, cuando estamos suponiendo que de ahí se sigue que tiene que haber un segundo, etc.

En cambio, Zermelo se extralimita cuando dice que no podemos demostrar que existan ω o cardinales fuertemente inaccesibles, *ni tampoco que no existan.* Esto último no tiene forma de justificarlo. Podría ser que la

[60] La forma usual de enunciar el axioma de partes es con una doble implicación, pero la implicación opuesta a la que hemos escrito se puede demostrar aplicando el axioma de especificación, y para lo que discutimos aquí es más claro centrarnos en esta implicación.

existencia de ω fuera contradictoria, que es tanto como decir que ZF es contradictorio, o podría ser consistente ZF pero ser contradictorio que exista un cardinal fuertemente inaccesible. Zermelo no tiene argumentos para descartarlo.[61] Pero, con este desliz, considera satisfactorio que sus axiomas no determinen si existen o no cardinales fuertemente inaccesibles, porque es lógico que así sea: puede haber un modelo donde los haya, y tomando en él V_κ, donde κ es el menor cardinal fuertemente inaccesible, tenemos otro donde no los hay. Como se pueden dar los dos casos, los axiomas no implican ni que existan ni que no existan. Más aún:

> *Después de todo, nuestro sistema de axiomas no es categórico, lo cual, en este caso, no constituye una desventaja, sino una ventaja. La enorme importancia y la aplicabilidad ilimitada de la teoría de conjuntos residen precisamente en este hecho. Por supuesto, siempre es posible forzar artificialmente la categoricidad deseada añadiendo más "axiomas", pero sólo a expensas de la generalidad.*

Zermelo cree haber demostrado que si tomamos como axioma que no existen cardinales fuertemente inaccesibles entonces ya sólo hay un modelo posible para la teoría de conjuntos, lo cual es falso. Pero, de todos modos, argumenta que no sería un axioma conveniente, porque sería negar la existencia de unos conjuntos que, si existen, no hay razón para desterrarlos de la matemática.

Finalmente Zermelo habla ya abiertamente en términos especulativos:

> *Planteemos ahora la hipótesis general de que todo dominio categóricamente determinado también puede concebirse como un "conjunto" de una forma u otra; es decir, que puede presentarse como un elemento de un dominio normal (adecuadamente elegido). De ello se deduce que a cualquier dominio normal le corresponde uno superior* [...] *y, por lo tanto, también a cualquier "número frontera" un número frontera mayor.* [...]
>
> *Una vez más, esto no es, por supuesto, demostrable con base en los axiomas* ZF, [...] *En cambio, debemos postular la existencia de una secuencia ilimitada de números frontera como un nuevo axioma para la metateoría de conjuntos, donde la cuestión de la consistencia aún requiere un análisis más detallado.*

Así pues, Zermelo considera plausible que el universo entero de cualquier modelo de la teoría de conjuntos pueda verse como un conjunto V_κ de otro modelo mayor, para un cierto cardinal fuertemente inaccesible κ, y en tal caso lo procedente es postular la existencia de infinitos cardinales fuertemente inaccesibles, para no desterrar de la matemática unos conjuntos que "están ahí", nos interesemos por ellos o no. Finalmente:

> *Aunque debo limitarme aquí a este esbozo preliminar y referirme a su posterior elaboración, lo siguiente, que puede considerarse el resultado esencial de la presente investigación, debería ser ya evidente:*
>
> *Las "antinomias ultrafinitas de la teoría de conjuntos", a las que los científicos reaccionarios y antimatemáticos apelan con tanta vehemencia en su lucha contra la teoría de conjuntos, son sólo "contradicciones" aparentes, debidas únicamente a una confusión entre la propia teoría de conjuntos —que no está determinada categóricamente por sus axiomas— y los modelos individuales que la representan: lo que en un modelo aparece como "no-conjunto" o "superconjunto ultrafinito", pasa a ser un "conjunto" plenamente válido con un cardinal y un ordinal asignados, en el modelo inmediatamente superior y, a su vez, sirve de base para la construcción del nuevo dominio. A la serie ilimitada de números ordinales cantorianos corresponde una doble serie, igualmente ilimitada, de modelos de teoría de conjuntos esencialmente diferentes, en cada uno de los cuales se expresa toda la teoría clásica.*

En conclusión, el axioma de regularidad estructura la clase V de todos los conjuntos en una jerarquía acumulativa, y Zermelo está acertado cuando considera que (supuesto que esto sea consistente) siempre podemos considerar que la clase Ω de todos los ordinales de un modelo dado de ZF (y recordemos que Zermelo incluye aquí tácitamente el axioma de elección) puede verse como un cardinal fuertemente inaccesible κ de otro modelo mayor, de forma que la clase V de todos los conjuntos del primer modelo es el conjunto V_κ del segundo. Esto proporciona una forma de tratar con las "multiplicidades inconsistentes" de Cantor sin contradicciones, considerándolas como conjuntos de un modelo mayor.

[61] Es verdad que, un poco más abajo, Zermelo dice que *"la cuestión de la consistencia todavía está pendiente de un examen más minucioso"*, por lo que se puede entender que aquí está conjeturando bajo el supuesto de que no haya ningún problema con la consistencia.

Cardinales $\mathbb{R}$-medibles Zermelo tenía razón en que no era sensato descartar por axioma los cardinales inaccesibles. Por ejemplo, Vitali había demostrado que es imposible definir una medida sobre todos los subconjuntos de la recta real (o de un intervalo) que fuera invariante por traslaciones. El año anterior, en 1929, Banach y Kuratowski habían publicado un artículo titulado *sobre una generalización del problema de la medida,* en el que se planteaban eliminar la condición de la invarianza por traslaciones. Más precisamente, llamando $X = [0,1]$, se plantearon si es posible definir una medida no trivial sobre todos los subconjuntos de X, donde "no trivial" significa que los puntos tengan medida nula,[62] pero haya conjuntos de medida no nula. Suponiendo la hipótesis del continuo, demostraron que tal medida no puede existir. Sin embargo, en **1930**, Stanisław Ulam, que, a sus 21 años, estaba cursando el doctorado con Kuratowski, publicó *Sobre la teoría de la medida en la teoría general de conjuntos,* donde abordó el mismo problema para un conjunto arbitrario X y, sin suponer la hipótesis del continuo. Un resultado elemental es el siguiente:

Teorema Si ν es un cardinal tal que existe una medida no trivial $\mu : \mathcal{P}X \longrightarrow [0,1]$ en un conjunto de cardinal ν, entonces existe un cardinal $\kappa \leq \nu$ tal que existe una medida $\mu' : \mathcal{P}\kappa \longrightarrow [0,1]$ no trivial que además es κ-aditiva, es decir, la unión de menos de κ conjuntos nulos es nula.

Demostración: Basta tomar como κ el menor cardinal tal que existe una medida no trivial $\mu : \mathcal{P}X \longrightarrow [0,1]$ en un conjunto X de cardinal κ. Claramente entonces $\kappa \leq \nu$. Tomamos una biyección $f : \kappa \longrightarrow X$, lo que nos permite definir $\mu'(A) = \mu(f[A])$, y claramente μ' es una medida no trivial en κ. Sólo tenemos que probar que es κ-aditiva. En caso contrario, sea $\xi < \kappa$ tal que existe una familia $\{A_\alpha\}_{\alpha<\xi}$ de subconjuntos nulos de κ cuya unión no sea nula. Cambiando cada A_α por $A_\alpha \setminus \bigcup_{\beta<\alpha} A_\beta$, podemos suponer que los A_α son disjuntos dos a dos.

Definimos $\mu^* : \mathcal{P}\xi \longrightarrow [0,1]$ mediante $\mu^*(U) = m(\bigcup_{\alpha\in U} A_\alpha)$. Basta probar que es una medida no trivial, y tendremos una contradicción.

Sea $\{U_n\}_{n=0}^\infty$ una familia de subconjuntos de ξ disjuntos dos a dos. Entonces

$$\mu^*(\bigcup_{n=0}^\infty U_n) = \mu'(\bigcup_{n=0}^\infty \bigcup_{\alpha\in U_n} A_\alpha) = \sum_{n=0}^\infty \mu'(\bigcup_{\alpha\in U_n} A_\alpha) = \sum_{n=0}^\infty \mu^*(U_n).$$

Esto (junto con que $\mu^*(\varnothing) = \varnothing$) prueba que μ^* es una medida. Claramente, además, $\mu^*(\{\alpha\}) = \mu'(A_\alpha) = 0$ y $\mu^*(\xi) = \mu'(\bigcup_{\alpha<\xi} A_\alpha) > 0$, luego la medida no es trivial. ∎

Un *cardinal* $\mathbb{R}$*-medible* es un cardinal κ tal que existe una medida κ-aditiva $\mu : \mathcal{P}\kappa \longrightarrow [0,1]$ no trivial.

En estos términos hemos demostrado que si existe una medida no trivial en un conjunto X de cardinal ν, existe un cardinal $\mathbb{R}$-medible $\kappa \leq \nu$. Y Ulam probó que hay dos posibilidades para estos cardinales:

Teorema (Ulam) κ es un cardinal $\mathbb{R}$-medible:

- o bien existe una medida no trivial en κ que es bivaluada (es decir, que sólo toma los valores $0, 1$), y en tal caso κ es fuertemente inaccesible,
- o bien $\kappa \leq 2^{\aleph_0}$ es débilmente inaccesible y existe una medida[63] no trivial definida sobre todos los subconjuntos del intervalo $[0,1]$.

En particular, si se cumple la hipótesis del continuo no puede haber cardinales inaccesibles menores o iguales que $2^{\aleph_0}$, luego el resultado de Ulam implica el de Banach y Kuratowski.

Más aún, si κ es fuertemente inaccesible, como $\aleph_0 < \kappa$, también se cumple $2^{\aleph_0} < \kappa$, luego la única posibilidad para que haya una medida no trivial en $[0,1]$ (o en $[0,1]^n$) es que se dé el segundo caso, es decir, que haya un cardinal débilmente inaccesible menor o igual que $2^{\aleph_0}$. Vemos así que, salvo que la potencia del continuo sea enorme, no es posible dar una definición de "longitud", "área", etc. que valga para todos los subconjuntos de la recta, plano, etc., ni siquiera sacrificando la condición de que se conserve por movimientos.

[62] Dado cualquier conjunto X no vacío se puede definir una medida sobre todos sus subconjuntos fijando un elemento x de X y estableciendo que los conjuntos que contienen a x tienen medida 1 y los que no contienen a x tienen medida 0. El concepto de "medida no trivial" descarta este caso y el de la medida que vale 0 en todos los conjuntos.

[63] Puede probarse que esta medida se puede manipular para que extienda a la medida de Lebesgue.

42 El álgebra de van der Waerden En **1930** el matemático neerlandés Bartel Leendert van der Waerden publicó el libro *Moderne Algebra,* considerado como el primer libro de álgebra abstracta, y que empezaba con un capítulo dedicado a la teoría de conjuntos, en el cual se basaban todos los demás (dedicados al estudio de grupos, anillos, cuerpos, etc.). La introducción de este primer capítulo empieza así:

> *Debido a que en este libro se utilizan ciertos conceptos lógicos y de la matemática general, en particular el concepto de conjunto, con los que el estudiante de matemáticas a menudo aún no está familiarizado, se incluirá una sección breve sobre estos conceptos al principio. No se abordarán las dificultades de los fundamentos: adoptamos consistentemente el "punto de vista ingenuo", eso sí, evitando las definiciones circulares que generan paradojas. El estudiante avanzado sólo necesita recordar de este capítulo el significado de los signos* $\in, \subset, \cup, \cap, \setminus$ *y* $\{\cdots\}$ *y puede omitir todo lo demás.*

Luego define los conceptos conjuntistas básicos (subconjuntos, uniones, intersecciones, funciones, etc.) El conjunto de los números naturales se presenta sin definición, aceptando que cumple los axiomas de Peano, a partir de los cuales se deducen los resultados básicos sobre los números naturales. La definición de los números enteros también se incluye en este capítulo preliminar. Seguidamente se definen y se demuestran las propiedades básicas de los conjuntos finitos y numerables. Para terminar se introducen los resultados básicos sobre relaciones de equivalencia y conjuntos cociente.

Éste era un ejemplo más de cómo los matemáticos se estaban convenciendo de que la teoría de conjuntos proporcionaba el marco más conveniente para presentar y desarrollar cualquier teoría matemática, hasta el punto de que la existencia de paradojas era algo irrelevante que no merecía ninguna atención: la forma práctica de evitar las paradojas no era ceñirse a los axiomas de Zermelo-Fraenkel, sino simplemente no meterse con ellas (sin perjuicio de que todos los teoremas del libro de van der Waerden eran, de hecho, consecuencias de los axiomas de Zermelo).

43 Conjuntos proyectivos También en **1930**, Lusin publicó su libro *Lecciones sobre los conjuntos analíticos y sus aplicaciones,* el primer libro en el que se exponía de forma sistemática la teoría de los conjuntos analíticos. En él adopta como definición lo que en su nota de 1917 era un teorema:

> Definición *Llamaremos "analítico" a todo conjunto E que admite una representación paramétrica $x = f(t)$ mediante una función continua sobre $\mathcal{I}$.*

Aquí $\mathcal{I}$ es lo que Lusin llama el "dominio fundamental", que es el conjunto de los números irracionales. ¿Y por qué aparece este conjunto en la definición de conjunto analítico? Recordemos que la teoría de los conjuntos analíticos había surgido en parte debido al error que Suslin detectó en un tratado de Lebesgue, el cual afirmaba que toda proyección ortogonal de un conjunto de Borel es un conjunto de Borel. Una proyección ortogonal es un caso de función continua, luego resulta que no es cierto en general que las imágenes continuas de los conjuntos de Borel sean conjuntos de Borel. Esencialmente, los conjuntos analíticos son las imágenes continuas de los conjuntos de Borel, sólo que Suslin había demostrado que todo conjunto analítico en $\mathbb{R}$ puede expresarse, más concretamente, como imagen continua de un subconjunto cerrado en $\mathbb{R}$. Ahora bien, cerrados en $\mathbb{R}$ hay muchos y muy variados, pero sucede que todos ellos son imágenes continuas de $\mathcal{I}$, así que este espacio sirve como dominio común para definir todos los conjuntos analíticos. (En cambio, no es cierto que todo conjunto analítico sea imagen continua del propio[64] $\mathbb{R}$.)

Lusin define los conjuntos analíticos en $\mathbb{R}^n$ como las imágenes continuas de $\mathcal{I}^n$, sin darse cuenta de que, en realidad, $\mathcal{I}^n$ es el mismo espacio que $\mathcal{I}$. En efecto, Baire había demostrado que el espacio de Baire $\mathcal{N}$ (formado por todas las sucesiones de números naturales) es homeomorfo al conjunto $\mathbb{I}$ de los números irracionales $0 < \alpha < 1$ (véase la sección 24), pero también es homeomorfo[65] a $\mathcal{I}$. Por lo tanto, un conjunto analítico en $\mathbb{R}$ puede definirse como una imagen continua del espacio de Baire $\mathcal{N}$. Si Lusin hubiera trabajado con $\mathcal{N}$ en lugar de $\mathcal{I}$, posiblemente se habría dado cuenta de que $\mathcal{N}^n$ es homeomorfo a $\mathcal{N}$, que es un hecho más que confirma la percepción que Baire tenía de este espacio como un espacio de dimensión 0.

[64] Porque las imágenes continuas de $\mathbb{R}$ son conexas, mientras que un conjunto analítico no tiene por qué serlo.

[65] La idea es que, si llamamos $\mathbb{I}_n$ al espacio de los números irracionales $n < \alpha < n+1$, entonces $\mathcal{I} = \bigcup_{n\in\mathbb{Z}} \mathbb{I}_n$, donde cada $\mathbb{I}_n$ es abierto y cerrado en $\mathcal{I}$ y, similarmente $\mathcal{N} = \bigcup_{n\in\mathbb{N}} \mathcal{N}_n$, donde $\mathcal{N}_n$ está formado por las sucesiones que empiezan por n, y también es abierto y cerrado en $\mathcal{N}$ y homeomorfo a $\mathcal{N}$. Por lo tanto, usando una biyección entre $\mathbb{N}$ y $\mathbb{Z}$, podemos considerar homeomorfismos que hagan corresponder cada $\mathcal{N}_n$ con un $\mathbb{I}_n$, y estos homeomorfismos se combinan en un único homeomorfismo entre $\mathcal{N}$ e $\mathcal{I}$.

En efecto, cada punto $(x, y) \in \mathcal{N}^2$ es un par de sucesiones de números naturales, que puede identificarse con la sucesión

$$(x_0, y_0, x_1, y_1, x_2, y_2, \ldots) \in \mathcal{N},$$

lo cual nos da una correspondencia biunívoca entre $\mathcal{N}^2$ y $\mathcal{N}$, y es fácil demostrar que es un homeomorfismo. Lo mismo vale con n factores, e incluso, apurando el argumento, con una cantidad numerable de ellos.

Lusin explica por qué eligió el nombre de "conjuntos analíticos" para los que originalmente se llamaban A-conjuntos, donde la A era por Alexandroff:

> *El motivo de esta denominación es muy claro: como toda función $x = f(t)$ continua en $\mathcal{I}$ es una función de clase 1 de la clasificación del Sr. Baire, existe una serie de polinomios en t con coeficientes racionales*[66]
>
> $$P_1(t) + P_2(t) + \cdots + P_n(t) + \cdots$$
>
> *convergente para todo valor de t entre 0 y 1 cuya suma es $f(t)$.*
>
> *Por lo tanto, cualquier conjunto analítico lineal es el conjunto de valores que toma en $(0, 1)$ la suma de una serie de polinomios con coeficientes racionales y, en consecuencia, está definido mediante una igualdad analítica.**
>
> *(*) El nombre de conjunto analítico se da a raíz de una propuesta del Sr. H. Lebesgue de llamar conjuntos analíticos a todos los conjuntos que pueden definirse mediante igualdades o desigualdades analíticas:*
>
> *"... De lo que se demostrará a continuación, se deduce que los conjuntos medibles B son aquellos que pueden definirse mediante igualdades o desigualdades analíticas; por esta razón, merecen ser llamados conjuntos analíticos."*
>
> [H. Lebesgue, *Sobre los conjuntos analíticamente representables, p. 165, nota (1)*]
>
> *La proposición inversa (es decir, que cualquier conjunto definido mediante igualdades o desigualdades analíticas es un conjunto medible B) nunca la ha enunciado. Lebesgue no había escrito ni una sola frase, ni una simple alusión a la posibilidad de esta inversión. Ésta es la razón por la que Suslin y yo, deseosos de ejecutar el programa del Sr. Lebesgue para el estudio de las funciones más generales que se pueden nombrar, tan pronto como nos dimos cuenta de que estábamos en presencia de una nueva clase de conjuntos íntimamente ligados a las series polinómicas, nos encontramos con la terminología ya establecida por el propio Sr. Lebesgue. Pero, al mismo tiempo, tuvimos cuidado de abstenernos de dar el mismo nombre de conjuntos analíticos a los conjuntos complementarios: éstos últimos, al estar definidos de manera puramente negativa como colecciones de "puntos que no...", no necesitaban una prueba especial de su analiticidad en el sentido del Sr. Lebesgue. Ahora bien, un ejemplo particular de un conjunto complementario obtenido por el propio Sr. Lebesgue (véase la página 202 de este libro) ha puesto claramente de manifiesto la imposibilidad de tener una definición positiva y completa para los conjuntos complementarios, lo cual ha sido demostrado posteriormente por la teoría, cuando ya estaba suficientemente desarrollada: cualquier definición positiva de un conjunto complementario implica infaliblemente todos los números transfinitos de la segunda clase (y no sólo aquellos inferiores a uno de ellos, fijado de antemano) o algo seguramente adecuado a esta totalidad ilegítima. La importancia de este hecho se nos hará particularmente evidente al abordar el estudio de los conjuntos que denomino proyectivos, cuya primera idea se remonta a M. Lebesgue.* [...]

En efecto, en el último capítulo del libro, Suslin llevaba más allá los límites de la teoría descriptiva de conjuntos presentando una clase aún más amplia de conjuntos, los llamados *conjuntos proyectivos,* que habían sido introducidos en 1925 por el propio Lusin y por Sierpiński. Con notación moderna, los conjuntos analíticos son los llamados conjuntos $\mathbf{\Sigma}^1_1$ y sus complementarios, los conjuntos *coanalíticos,* son los conjuntos $\mathbf{\Pi}^1_1$. Suslin había demostrado que los conjuntos de Borel son los conjuntos que son a su vez analíticos y coanalíticos. Lusin destaca que, en general, no son analíticos, pero, si aceptamos que al definirlos como complementarios de conjuntos "que se pueden nombrar" los estamos "nombrando en un sentido débil", a partir de ahí podemos obtener nuevos conjuntos tomando sus imágenes continuas, y los conjuntos que se obtienen así son los $\mathbf{\Sigma}^1_2$, cuyos complementarios son los $\mathbf{\Pi}^1_2$, y así sucesivamente. Si llamamos $\mathbf{\Delta}^1_n = \mathbf{\Sigma}^1_n \cap \mathbf{\Pi}^1_n$, con lo que $\mathbf{\Delta}^1_1$ es la clase de los conjuntos de Borel, estas clases de conjuntos están ordenadas así:

$$\begin{array}{ccccccccccc}
 & & \mathbf{\Sigma}^1_1 & & \mathbf{\Sigma}^1_2 & & \mathbf{\Sigma}^1_3 & & & \cdots \\
 & \subset & & \subset & & \subset & & \subset & \subset & \\
\mathbf{\Delta}^1_1 & & \subset & \mathbf{\Delta}^1_2 & & \subset & \mathbf{\Delta}^1_3 & & \mathbf{\Delta}^1_4 & \\
 & \subset & & \subset & & \subset & & \subset & \subset & \\
 & & \mathbf{\Pi}^1_1 & & \mathbf{\Pi}^1_2 & & \mathbf{\Pi}^1_3 & & & \cdots
\end{array}$$

[66] Que toda función continua puede expresarse como límite y, por consiguiente, como suma infinita de polinomios es algo que Weierstrass había demostrado en 1885 para funciones definidas en un intervalo en $\mathbb{R}$ y que Stone extendería a dominios más generales en 1937. Lusin conocía, no obstante, este caso intermedio.

La clase P de los conjuntos proyectivos es

$$P = \bigcup_n \mathbf{\Sigma}^1_n = \bigcup_n \mathbf{\Pi}^1_n,$$

donde n recorre los números naturales. Se llaman así porque, para construirlos, en lugar de tomar imágenes continuas generales, es suficiente tomar proyecciones ortogonales, es decir, que todo conjunto $\mathbf{\Sigma}^1_2$ es la proyección ortogonal de un conjunto $\mathbf{\Pi}^1_1$ (y todo conjunto $\mathbf{\Pi}^1_2$ es la proyección ortogonal de un conjunto $\mathbf{\Sigma}^1_1$).

Sin embargo, Lusin estaba algo desencantado con estos conjuntos. Él mismo había demostrado que los conjuntos $\mathbf{\Sigma}^1_1$ son medibles Lebesgue y, por consiguiente, sus complementarios, los conjuntos $\mathbf{\Pi}^1_1$, también lo son, pero el problema de si los conjuntos $\mathbf{\Sigma}^1_2$ son medibles Lebesgue resistía todo ataque. Lo más que pudo probar es que todo conjunto $\mathbf{\Sigma}^1_2$ es unión de $\aleph_1$ conjuntos de Borel (luego medibles Lebesgue), pero no pudo demostrar que la unión de $\aleph_1$ conjuntos medibles Lebesgue tuviera que ser medible. No obstante, esto implica que todo conjunto $\mathbf{\Sigma}^1_2$ tiene cardinal $\leq \aleph_1$ o cardinal $\mathfrak{c}$, lo que responde parcialmente al problema 9 de la página 55. De hecho, también responde al problema 4. Basta tomar un conjunto analítico A que no sea de Borel, con lo que $B = \mathbb{R} \setminus A$ es $\mathbf{\Pi}^1_1$. Como A y B son $\mathbf{\Sigma}^1_2$, podemos expresar ambos como unión de $\aleph_1$ conjuntos de Borel, y uniendo las dos descomposiciones, tenemos una descomposición de $\mathbb{R} = \bigcup_{\alpha<\omega_1} B_\alpha$ en $\aleph_1$ subconjuntos de Borel tal que ninguna unión numerable cubre $\mathbb{R}$, o A sería de Borel.

Basta tomar $C_\alpha = B_\alpha \setminus \bigcup_{\delta<\alpha} B_\delta$, pues los conjuntos C_α son de Borel, disjuntos dos a dos, cubren $\mathbb{R}$ y al menos una cantidad no numerable de ellos son no vacíos.

Igualmente, Lusin había demostrado que todo conjunto $\mathbf{\Sigma}^1_1$ no numerable contiene un subconjunto perfecto, luego todo conjunto analítico es numerable o tiene el cardinal del continuo. En cambio, el problema de si todo conjunto $\mathbf{\Pi}^1_1$ no numerable contiene un subconjunto perfecto parecía inabordable.

44 La lógica intuicionista En 1925 se había doctorado el matemático neerlandés Arend Heyting bajo la dirección de Brouwer. Su tesis trataba sobre una axiomatización intuicionista de la geometría proyectiva. En **1930** Heyting publicó su artículo *Las reglas formales de la lógica intuicionista,* en el que presentaba un sistema axiomático para la lógica intuicionista que luego aplicó a la aritmética de Peano en *Las reglas formales de la matemática intuicionista,* dando lugar a lo que hoy se denomina *Aritmética de Heyting.*

La lógica de Heyting es una variante del cálculo deductivo de Hilbert, pero modificado para excluir tanto el principio del tercio excluso (es decir, para que $\alpha \vee \neg\alpha$ deje de ser un teorema lógico) como la regla de doble negación (de modo que α ya no es equivalente a $\neg\neg\alpha$, aunque en algunos casos se pueda demostrar $\alpha \vee \neg\alpha$ o la equivalencia entre α y $\neg\neg\alpha$). Fue Heyting quien introdujo los signos $\neg$ y $\wedge$ con el significado de "no" e "y".

45 Los teoremas de incompletitud Del 5 al 7 de septiembre de **1930** se celebró en Königsberg el *Segundo Congreso sobre la Epistemología de las Ciencias Exactas,* en el que Rudolph Carnap habló sobre el logicismo de Bertrand Russell, Heyting sobre el intuicionismo de Brouwer, y von Neumann sobre el formalismo de Hilbert. Además, Kurt Gödel explicó su teorema de completitud semántica. El 8 de septiembre tuvo lugar un homenaje a David Hilbert, que a sus 68 años se acababa de jubilar. El día anterior había tenido lugar uno de los últimos actos del congreso, un debate sobre la fundamentación de la matemática en el que habían participado, entre otros, Carnap, Heyting, von Neumann y Gödel. En él, Gödel comentó de pasada unos resultados que había obtenido. Nadie le prestó atención excepto von Neumann, que en cuanto pudo se llevó aparte a Gödel para preguntarle más detalles al respecto.

Gödel presentó oficialmente sus resultados el 23 de octubre, en una breve comunicación a la Academia de Ciencias de Viena. Mientras tanto, von Neumann había estado desarrollando las ideas que le había esbozado Gödel en Königsberg y el 20 de noviembre le escribió una carta en la que le informaba que que había demostrado su teorema (lo que ahora se conoce como primer teorema de incompletitud de Gödel) y había obtenido consecuencias que iban mucho más allá (lo que ahora se conoce como segundo teorema de incompletitud de Gödel). Gödel le respondió que, en efecto, conocía esas consecuencias y que estaban recogidas en un artículo pendiente de publicación. El artículo fue publicado en **1931** con el título de *Sobre sentencias fomalmente indecidibles en los Principia Mathematica y sistemas afines.* En palabras de von Neumann:

> *El logro de Kurt Gödel en la lógica moderna es singular y monumental. De hecho, es más que un monumento. Es un punto de referencia que seguirá siendo visible en el espacio y en el tiempo. Sin duda, el objeto de la lógica ha cambiado completamente su naturaleza y sus posibilidades con el logro de Gödel.*

La cita siguiente es del propio anuncio de Gödel en Viena, con las únicas salvedades de que él enunció sus resultados para un cálculo deductivo S basado en la lógica de los *Principia Mathematica,* si bien luego aclaraba que se aplicaba igualmente a los axiomas de Zermelo-Fraenkel o a cualquiera de las teorías axiomáticas consideradas hasta entonces. Por otra parte hemos eliminado ciertas restricciones que más adelante se demostraría que eran innecesarias:

> I *El sistema S no es completo, es decir, contiene proposiciones A (de hecho podemos mostrar explícitamente tales proposiciones) para las que ni A ni $\neg A$ es demostrable y, en particular, contiene (incluso para propiedades decidibles F de los números naturales) problemas indecidibles con la simple estructura $\bigvee x\, Fx$, donde x recorre los números naturales.*
>
> II *Incluso se admitimos todas las herramientas lógicas de S en la metamatemática, en particular el axioma de elección, no existe una prueba de consistencia del sistema S (y mucho menos si restringimos los métodos de prueba de cualquier forma). Por lo tanto, una prueba de consistencia para el sistema S sólo puede llevarse a cabo mediante formas de razonamiento no formalizables en el sistema S.*
>
> III *El teorema* I *puede mejorarse para asegurar que, incluso si añadimos un número finito de axiomas a S, no obtenemos un sistema completo, bajo el supuesto de que sea consistente.*
>
> IV *El teorema* I *vale incluso para extensiones consistentes de S mediante infinitos axiomas bajo el supuesto de que la clase de los nuevos axiomas sea decidible, es decir, que sea metamatemáticamente decidible si una fórmula dada es o no un axioma.*

En resumen: Gödel había demostrado que el programa de Hilbert era inviable. No sólo no era posible demostrar la consistencia de ZFC[67] (o de cualquier teoría de conjuntos similar) mediante argumentos finitistas, sino que ni siquiera podía existir una prueba de consistencia aunque admitiéramos emplear todas las formas de razonamiento expresables en ZFC. Sucede que ZFC puede expresar cualquier razonamiento que un matemático considere aceptable, luego no existen pruebas de la consistencia de ZFC, salvo que presupongan algún principio más fuerte que la propia consistencia de ZFC, en cuyo caso no aportan nada a la hora de convencerse de que ZFC es consistente.

Por otro lado, ZFC es incompleto, no puede demostrar cualquier afirmación matemática o su negación. De hecho, existen afirmaciones indecidibles con la estructura más simple posible. Más adelante se probaría que las afirmaciones de Gödel pueden expresarse en forma de ecuaciones diofánticas del estilo de

$$\bigvee xyz \in \mathbb{N}\,(x^2y + 3xz + z^3 + 5z^2x + 23 = 0)$$

(con más variables y una expresión mucho más complicada, pero de este aspecto, es decir, que hablamos de fórmulas que afirman la existencia de unos números naturales que cumplen una ecuación polinómica).

Y nada de esto se puede arreglar añadiendo más axiomas a la teoría considerada. Aunque tomemos una fórmula indecidible y la añadamos como axioma, la teoría resultante tendrá otras fórmulas indecidibles, y esto no dejará de ser así por muchos axiomas que añadamos (siempre y cuando tengamos un procedimiento efectivo para saber qué fórmulas son axiomas y cuáles no).

46 Funciones recursivas Aunque, según hemos señalado, Gödel probó sus teoremas de incompletitud para un cálculo deductivo basado en la lógica de los *Principia Mathematica,* también dejó claro que, en realidad, sus argumentos eran válidos para cualquier teoría axiomática T que cumpliera unos requisitos mínimos. Uno de ellos es el que acabamos de parafrasear diciendo que debe existir un procedimiento efectivo para saber qué fórmulas son axiomas de T y cuáles no, pero esto es un anacronismo. En realidad la hipótesis que planteó Gödel era que el conjunto de los axiomas de T fuera recursivo. Vamos a ver lo que significa esta condición.

Gödel definió una clase de funciones aritméticas (es decir, funciones que a cada n números naturales $x_1, \ldots, x_n$ les hacen corresponder un número natural $f(x_1, \ldots, x_n)$) a las que llamó *funciones recursivas.* Su definición era como sigue:

1. La función cero, dada por $c(n) = 0$ es recursiva.
2. La función sucesor, dada por $s(n) = n + 1$ es recursiva.

[67] A partir de aquí adoptamos el convenio usual de indicar con la C de *choice* la teoría de conjuntos ZFC que resulta de incluir entre los axiomas ZF de Zermelo-Fraenkel el axioma de elección, aunque todavía no se usaba por estas fechas.

3. Las proyecciones,[68] dadas por $p_i^n(x_1, \ldots, x_n) = x_i$ son recursivas.

4. Si $g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n), h(x_1, \ldots, x_m)$ son funciones recursivas, la función dada por

$$f(x_1, \ldots, x_n) = h(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$$

es recursiva (y se dice que está definida por *composición* a partir de las funciones dadas).

5. Si $g(x_1, \ldots x_n), h(x_1, \ldots, x_n, x, y)$ son funciones recursivas, también lo es la función dada por

$$\begin{aligned} f(x_1, \ldots, x_n, 0) &= g(x_1, \ldots, x_n), \\ f(x_1, \ldots, x_n, x+1) &= h(x_1, \ldots, x_n, x, f(x_1, \ldots, x_n, x)), \end{aligned}$$

(y se dice que está definida por *recursión* a partir de las funciones dadas).

Para ilustrar esta definición vamos a demostrar que la función $f(x, y) = x + y$ es recursiva. Para ello consideramos las funciones siguientes:

$f_1(x) = x$	proyección
$f_2(x, y, z) = z$	proyección
$f_3(x) = x + 1$	sucesor
$f_4(x, y, z) = f_3(f_2(x, y, z)) = z + 1$	composición f_1, f_2
$f_5(x, 0) = f_1(x) = x$	
$f_5(x, y + 1) = f_4(x, y, f_5(x, y)) = f_5(x, y) + 1$	recursión f_1, f_4

Si en vez de escribir $f_5(x, y)$ escribimos $x + y$, vemos que esta función cumple:

$$x + 0 = x, \qquad x + (y + 1) = (x + y) + 1,$$

y es claro que estas relaciones determinan unívocamente a la suma de números naturales, por lo que la función f_5 no es sino la suma, y la forma en que la hemos construido muestra que es recursiva.

Similarmente se puede probar que la función $f(x, y) = xy$ es recursiva, al igual que $f(x, y) = x^y$. En realidad, la clase de las funciones recursivas es muy amplia, mucho más amplia de lo que podría parecer a juzgar por la definición.

Observemos ahora un hecho fundamental:

Todas las funciones recursivas se pueden calcular en la práctica mediante un algoritmo.

Esto es consecuencia de las observaciones siguientes:

1. Las funciones c, s y p_i^n se pueden calcular trivialmente.

2. Dadas unas funciones $g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n), h(x_1, \ldots, x_m)$ (en un orden fijado), existe una única función $f(x_1, \ldots, x_n)$ definida por composición a partir de ellas, y si sabemos calcular en la práctica las funciones dadas, también sabemos calcular la función f.

   En efecto, para calcular $f(x_1, \ldots, x_n)$, sólo tenemos que calcular $g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)$ y, cuando tenemos los resultados, calcular con ellos la función h, y el resultado será el valor de f.

3. Dadas unas funciones $g(x_1, \ldots x_n), h(x_1, \ldots, x_n, x, y)$, existe una única función $f(x_1, \ldots, x_n, x)$ definida por recursión a partir de ellas, y si sabemos calcular en la práctica las funciones dadas, también sabemos calcular la función f.

   En efecto, para calcular $f(x_1, \ldots, x_n, x)$, empezamos calculando $f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n)$, y luego vamos calculando sucesivamente los valores

$$f(x_1, \ldots, x_n, 0), \quad f(x_1, \ldots, x_n, 1), \quad f(x_1, \ldots, x_n, 2), \quad \ldots \quad , f(x_1, \ldots, x_n, x),$$

   donde cada una se calcula mediante la función h a partir de la anterior, por ejemplo:

$$f(x_1, \ldots, x_n, 1) = h(x_1, \ldots, x_n, 0, f(x_1, \ldots, x_n, 0)).$$

[68] En realidad, en su artículo sobre los teoremas de incompletitud, Gödel cometió el desliz de no incluir las proyecciones en su definición, si bien las usaba tácitamente)

Si A es un conjunto de números naturales, decimos que es *recursivo* si lo es su función característica, es decir, la dada por

$$f(x) = \begin{cases} 1 & \text{si } x \in A, \\ 0 & \text{si } x \notin A. \end{cases}$$

Gödel mostró cómo cualquier fórmula de un lenguaje formal se puede codificar mediante un número natural, y la hipótesis que exigió para que sus teoremas fueran aplicables a una teoría axiomática T era que el conjunto de sus axiomas (identificado con un conjunto de números naturales a través de una codificación) fuera recursivo.

En particular, esto implica que disponemos de un criterio para determinar si una fórmula dada es o no un axioma. Este requisito es exigible sin duda alguna, pues, ¿de qué serviría una teoría axiomática si no podemos saber cuáles son sus axiomas? Pero en este punto se vuelve crucial la pregunta siguiente:

Si podemos calcular una función en la práctica, ¿ésta es necesariamente recursiva?

Si la respuesta no fuera afirmativa, los teoremas de incompletitud tendrían una brecha, pues cabría la posibilidad de que existiera una teoría de conjuntos consistente y completa que no se viera afectada por los teoremas de incompletitud porque sus axiomas no formaran un conjunto recursivo. En cambio, si la recursividad de los axiomas equivale a que se pueda determinar qué es un axioma y qué no lo es, entonces esa hipotética teoría sería inútil, pues si no podemos saber si una fórmula dada es o no un axioma, no podemos saber si una demostración dada es correcta o no, y no podríamos demostrar nada en tal teoría.

Sucede que hay funciones calculables en la práctica que no son recursivas. Esbozamos una demostración:

Cada sucesión recursiva puede calcularse mediante una sucesión de funciones recursivas (como hemos mostrado con la suma). Sólo hay un número finito de funciones recursivas que pueden definirse con sucesiones de longitud a lo sumo N y usando proyecciones p_i^n con $i \le n \le N$. Por lo tanto, podemos enumerar todas las funciones recursivas empezando con las que pueden construirse con $N = 1$, luego las que pueden construirse con $N = 2$ y así sucesivamente. Esto nos da una sucesión

$$f_0, \quad f_1, \quad f_2, \quad f_3, \quad \ldots$$

de funciones recursivas que podemos calcular explícitamente. Cada función requerirá un número distinto de argumentos, pero pongamos que eliminamos de la sucesión todas las que requieran más de un argumento. Así tenemos una enumeración (tal vez con repeticiones) de todas las funciones recursivas con un argumento, y esta enumeración se puede calcular en la práctica, es decir, que podemos determinar cuál es exactamente la función recursiva $f_{214}(x)$, o cualquier otra. Esto nos permite definir la función

$$f(x) = f_x(x) + 1$$

que podemos calcular en la práctica sin ningún problema, pero no puede ser ninguna de las f_x, pues si fuera $f = f_n$, tendríamos que $f(n) = f_n(n) + 1 = f(n) + 1$, lo cual es imposible.

Jacques Herbrand escribió a Gödel señalándole que había procedimientos (algunos bastante intrincados) que permitían calcular funciones en la práctica y que no encajaban en la definición de función recursiva. Se refirió a ellas como *funciones recursivas generales*. Tras un intercambio de correspondencia, Gödel se dio cuenta de que todas las funciones recursivas generales de Herbrand se podían obtener sin más que añadir un nuevo criterio de generación de funciones a su definición de función recursiva:

6. Si $g(x_1, \ldots, x_n, x)$ es una función recursiva tal que, para todos los valores de $x_1, \ldots, x_n$, existe al menos un número x tal que $g(x_1, \ldots, x_n, x) = 0$, entonces también es recursiva la función dada por

   $$f(x_1, \ldots, x_n) = \text{el mínimo } x \text{ tal que } g(x_1, \ldots, x_n, x) = 0,$$

   y se dice que f está definida por *minimización* a partir de la función dada.

Notemos que, si sabemos calcular la función g, también podemos calcular la función f. Sólo tenemos que ir calculando

$$g(x_1, \ldots, x_n, 0), \quad g(x_1, \ldots, x_n, 1), \quad g(x_1, \ldots, x_n, 2), \quad \ldots$$

hasta llegar a un x que cumpla $g(x_1, \ldots, x_n, x) = 0$, y entonces $f(x_1, \ldots, x_n) = x$. Por lo tanto, todas las funciones recursivas generales son calculables en la práctica.

La función no recursiva que hemos construido antes es un ejemplo de función recursiva general que no es recursiva.

Ahora bien, estas definiciones no tardaron en cambiarse, y las funciones recursivas generales pasaron a llamarse funciones recursivas, mientras que las funciones recursivas que había definido Gödel originalmente pasaron a llamarse *funciones recursivas primitivas.*

La correspondencia entre Herbrand y Gödel tuvo lugar en los primeros meses de **1931**, pues Herbrand murió el 27 de julio de ese año, a los 23 años, mientras practicaba el alpinismo.

La incorporación de la posibilidad de definir funciones por minimización no suponía más que una modificación mínima en la demostración de los teoremas de incompletitud, por lo que éstos seguían siendo válidos para teorías cuyos axiomas formaran un conjunto recursivo en el nuevo sentido más general.

47 Matemática y metamatemática Las demostraciones de los teoremas de Gödel no eran fáciles de seguir (con el tiempo se encontrarían pruebas más simples y claras). El primero que las entendió plenamente fue, sin duda, von Neumann, que las había reconstruido por sí mismo a partir de las indicaciones que le había dado Gödel. Los que decididamente no entendieron nada fueron los filósofos. Bertrand Russell se había apartado de la lógica matemática desde que terminó sus *Principia,* pero hizo algunos comentarios sobre los teoremas de Gödel que han llevado a muchos a concluir que no los entendía, entre ellos al propio Gödel, a cuyas manos llegó una carta de Russell en la que decía:

> *Me di cuenta, por supuesto, de que el trabajo de Gödel es de una importancia fundamental, pero me desconcertaba. Hizo que me alegrara de no estar trabajando ya en la lógica matemática. Si un conjunto dado de axiomas lleva a una contradicción, está claro que al menos uno de los axiomas debe ser falso. ¿Se aplica esto a la aritmética escolar? Y si es así, ¿podemos creer en algo de lo que nos enseñaron en nuestra juventud? ¿Debemos pensar que* $2+2$ *no es* 4*, sino* 4.001*? Obviamente no es lo que se pretende.*

Gödel comentó:

> *Russell evidentemente malinterpreta mi resultado, pero lo hace de un modo muy interesante.*[69]

Algo similar sucedía con Ludwig Wittgenstein (que también era filósofo y matemático) y con el propio Zermelo. Al parecer, pensaban que los teoremas de incompletitud suponían una paradoja más en la fundamentación de las matemáticas, y el núcleo de su confusión era probablemente que no hacían una distinción fundamental que Hilbert ya había trazado vagamente, pero que Gödel fue el primero en manejar con absoluta precisión, y es la distinción entre lo que el propio Gödel llamó *matemática* y *metamatemática.*

Fue Hilbert quien planteó convertir al razonamiento matemático en objeto de estudio matemático, y la forma de hacerlo es a través del concepto de teoría axiomática formal. Pensemos concretamente en ZFC, una teoría axiomática capaz de expresar cualquier razonamiento que un matemático considere concluyente. Específicamente, ZFC consiste en:

1. El lenguaje formal de la teoría de conjuntos, que, además de las variables y los signos lógicos, consta únicamente del signo no definido $\in$.

2. La especificación de dos colecciones infinitas de axiomas: los axiomas lógicos, como

$$x \in y \to (u = v \to x \in y),$$

   y los axiomas propios de ZFC, como $\bigwedge xy \bigvee z \bigwedge u(u \in z \leftrightarrow u \in x \vee u \in y)$ (el axioma del par).

3. La especificación de unas reglas de inferencia, que determinan cuándo se puede deducir una fórmula de otras dadas, como la regla del *modus ponens,* que establece que si en una deducción tenemos α y $\alpha \to \beta$, podemos añadir β como una nueva línea de la deducción.

Con esto queda completamente especificado qué es un teorema de ZFC: Una fórmula del lenguaje de la teoría de conjuntos es un teorema de ZFC si y sólo si puede obtenerse como la última fórmula de una sucesión de fórmulas en las que cada una es un axioma o bien se deduce de las fórmulas precedentes mediante una de las reglas de inferencia establecidas.

En este contexto podemos —y debemos— distinguir cuidadosamente entre dos clases de afirmaciones:

[69] Lo del interés lo decía, probablemente, por una serie de ideas que Russell daba luego sobre una sucesión de lenguajes que podría "arreglar el problema".

Por una parte están las *afirmaciones matemáticas,* que son aquellas que, aunque por comodidad prefiramos expresar en castellano, o en cualquier otra lengua natural, pueden expresarse mediante una fórmula del lenguaje de la teoría de conjuntos y que serán teoremas de ZFC si satisfacen la definición que acabamos de dar.

Un ejemplo es *"Existen infinitos números primos".* Esta afirmación está expresada en castellano, pero es posible expresarla en el lenguaje de la teoría de conjuntos, por ejemplo así:

$$\bigvee Pf(f : \mathbb{N} \longrightarrow P \text{ biyectiva} \wedge \bigwedge x(x \in P \leftrightarrow x \text{ es primo})).$$

En esta fórmula aparecen muchos signos que no son signos lógicos y son distintos del relator $\in$, pero decimos que es una fórmula del lenguaje de la teoría de conjuntos porque cada signo no definido podría sustituirse por su definición de modo que, tras un número finito de sustituciones, llegaríamos a una expresión que no contuviera más que signos lógicos y el relator de pertenencia.

Por ejemplo, "x es primo" puede sustituirse por:

$$x \in \mathbb{N} \wedge x \neq 0 \wedge x \neq 1 \wedge \bigwedge uv(u \in \mathbb{N} \wedge v \in \mathbb{N} \wedge x = u \cdot v \to u = x \vee v = x),$$

donde a su vez podríamos eliminar las definiciones de $x \in \mathbb{N}$, $x = 0$, $x = 1$, $x = u \cdot v$, etc.

En la práctica nunca es necesario ir eliminando signos definidos. Basta con asegurarse de que no empleamos ningún signo distinto de $\in$ o de los signos lógicos que no haya sido definido previamente. Es por esto por lo que podemos decir —en el sentido moderno de la palabra— que "Existen infinitos números primos" es una afirmación matemática y, más aún, que es un teorema de ZFC, puesto que admite una demostración.

Por otra parte, tenemos las *afirmaciones metamatemáticas,* expresadas en castellano u otra lengua natural, y que *no tiene sentido* identificar con fórmulas del lenguaje de la teoría de conjuntos, sino que tienen que verse como afirmaciones sobre ZFC.

Ejemplos de afirmaciones metamatemáticas son "ZFC *tiene infinitos axiomas*" o "ZFC *es consistente*".

La distinción es fundamental y no tenerla en cuenta puede resultar catastrófico. Más precisamente, vamos a comparar tres afirmaciones:

1. *Hay infinitos axiomas*[70] *de* ZFC.
2. *Hay infinitos números primos.*
3. *Hay infinitos cardinales infinitos.*

La primera afirmación es de naturaleza metamatemática. No podemos identificarla con una fórmula de lenguaje formal de ZFC, por lo que no tiene sentido plantearse siquiera si es o no un teorema de ZFC. No obstante, podemos considerarla porque es una afirmación en castellano con un significado claro e inequívoco y, de hecho, es verdadera. Ello se debe a que, entre los axiomas de ZFC, se encuentra el axioma del reemplazo, que no es un axioma, sino un esquema que determina infinitos axiomas. Recordemos su formulación:

> *Para toda fórmula $\phi(x, y)$ del lenguaje de la teoría de conjuntos, la fórmula siguiente es un axioma de* ZFC *(un ejemplo de axioma de reemplazo):*
>
> $$\bigwedge a(\bigwedge x \in a \overset{1}{\bigvee} y\, \phi(x, y) \to \bigvee b \bigwedge y(y \in b \leftrightarrow \bigvee x \in a\, \phi(x, y))),$$
>
> donde —recordemos— $\overset{1}{\bigvee}$ significa "existe un único".

Como hay infinitas fórmulas posibles $\phi(x, y)$ y, para cada una de ellas, obtenemos un axioma distinto, resulta que hay infinitos axiomas de reemplazo. Más aún, a nivel matemático, la última línea del párrafo anterior (la que empieza por $\bigwedge a$) es un axioma, es decir, una afirmación expresada en el lenguaje de la teoría de conjuntos, algo que afirmamos sobre los conjuntos, aunque no sepamos qué son esos conjuntos de los que estamos afirmando esto; pero, a nivel metamatemático, esa misma línea no es una afirmación, sino que es el nombre de un objeto, el nombre de una sucesión de signos del lenguaje de la teoría de conjuntos que satisface la definición de fórmula.

La diferencia es la misma que hay entre *"nadar es un ejercicio saludable"* y *"nadar es una palabra de cinco letras".* No hay contradicción entre decir que "nadar" es una acción (cuando pensamos en el significado de la palabra "nadar") y decir que "nadar" es una cosa (una palabra castellana). *"Nadar con mayúscula"* es un sinsentido si pretendemos verlo como una forma de nadar, pero *"Nadar con mayúscula"* tiene sentido como precisión de que nos referimos a "Nadar" y no a "nadar".

[70] Aquí es necesario aclarar si cuando hablamos de axiomas de ZFC incluimos los axiomas lógicos o nos referimos exclusivamente a los axiomas propios. Aclaramos, pues, que nos referimos a los axiomas propios, como es habitual.

Alguien que confundiera la acción de nadar con la palabra nadar no entendería nada en cuanto se encontrara con varias afirmaciones seguidas que requieren entender "nadar" en un sentido o en otro según el caso, y lo mismo sucede con quien intenta entender la demostración de los teoremas de Gödel sin tener clara la distinción entre las afirmaciones matemáticas y las metamatemáticas.

Por ejemplo, volviendo a la definición que acabamos de dar del esquema axiomático del reemplazo, sería catastrófico confundir el $\bigwedge a$ con el que empieza el axioma (que podemos leer como "para todo conjunto a") con el "para toda fórmula ϕ" con el que hemos empezado la definición del esquema axiomático. El primer "para todo" (el $\bigwedge a$) es un "para todo" matemático, que especifica que la variable a recorre todos los conjuntos, mientras que el "para toda fórmula ϕ" es un "para todo" metamatemático, que indica que ϕ recorre las fórmulas del lenguaje de la teoría de conjuntos, y dichas fórmulas no son conjuntos, son cadenas de signos del lenguaje de la teoría de conjuntos que usamos para enunciar los axiomas y los teoremas de la teoría de conjuntos. Podemos emplear el primer $\bigwedge a$ formalmente, sin necesidad de especificar qué son esos conjuntos de los que hablamos cuando aludimos a "todos" los conjuntos. Para eso precisamente hemos definido ZFC, para hablar de "todos" los conjuntos sin necesidad de decir qué son. En cambio, el "para toda fórmula ϕ" sólo tiene sentido porque sabemos lo que queremos decir cuando hablamos de todas las fórmulas del lenguaje de la teoría de conjuntos. No es un "para todo" matemático formal, sino un "para todo" metamatemático material, un "para todo" que podemos usar sólo porque sabemos qué son "todas" esas fórmulas de las que hablamos. En particular, sería un despropósito escribir algo como:

$$\bigwedge \phi \in \mathrm{Form}\, \bigwedge a(\bigwedge x \in a \overset{1}{\bigvee} y\, \phi(x,y) \to \bigvee b \bigwedge y(y \in b \leftrightarrow \bigvee x \in a\, \phi(x,y))) \in \mathrm{Form}$$

Esta mezcla entre matemática y metamatemática es tan absurda como si alguien dijera que su nivel de natación llega hasta la "d" de "nadar", pero que las dos últimas letras se le resisten. No se puede mezclar la acción de nadar con las letras de la palabra nadar.

Pasamos ahora a la segunda afirmación. Ésta puede verse de dos formas distintas. Por un lado, puede verse como hemos explicado antes, como una afirmación en castellano que puede identificarse con una afirmación matemática, con una fórmula del lenguaje de la teoría de conjuntos. Vista así, no tiene sentido plantearse si es verdadera o falsa. Lo más que podemos decir es que es un teorema de ZFC, luego será verdadera en todos los modelos de ZFC, es decir, que si consideramos unos objetos cualesquiera que cumplan los axiomas de la teoría de conjuntos (sean lo que sean), la afirmación "existen infinitos primos" expresa un hecho que cumplirán necesariamente esos objetos (sean lo que sean).

Ahora bien, esa misma afirmación puede verse también como una propiedad estrictamente finitista[71] sobre los números naturales y podemos razonar que es absolutamente verdadera, sin hacer referencia a ningún modelo de ZFC. Se trata, pues, de una afirmación metamatemática finitista verdadera, expresada en castellano, que puede expresarse también mediante una afirmación matemática en el lenguaje de la teoría de conjuntos, igual que podríamos expresarla en alemán o en chino.

La tercera afirmación tiene, sin duda, sentido como afirmación matemática, es decir, como una fórmula del lenguaje de la teoría de conjuntos que, de hecho, puede demostrarse en ZFC, lo que a su vez implica que es verdadera en cada modelo posible de ZFC. Sin embargo, un formalista como Hilbert diría que, salvo que hagamos referencia a un modelo determinado de ZFC, en sí misma no tiene ningún significado absoluto. No tiene sentido decir si es verdadera o falsa. Son sólo palabras. Por el contrario, un platonista como Zermelo —o como Gödel— considerarán que sí que tiene un significado absoluto, y que es verdadera, sólo que no estamos en condiciones de razonar informalmente sobre afirmaciones de esa naturaleza no finitista, y para concluir que es verdadera tenemos que deducirlo de los axiomas de ZFC, que, al margen de que sean trivialmente verdaderos en todo modelo de ZFC, lo importante es que expresan hechos verdaderos sobre "los conjuntos de verdad".

En resumen, si excluimos de entre las frases en castellano aquellas que no tienen un contenido matemático objetivo (como "las matemáticas son difíciles"), nos quedan tres tipos de afirmaciones relevantes para un matemático:

1. Las *afirmaciones metamatemáticas* con un significado intuitivo preciso que hablan sobre ZFC, sobre sus signos, sus fórmulas, sus axiomas, sus teoremas, etc. (o sobre los de cualquier sistema deductivo formal que queramos estudiar), pero que no podemos considerar como afirmaciones matemáticas del lenguaje de la teoría de conjuntos.

[71] Aunque en ella aparezca la palabra "infinito", podríamos reformularla diciendo que, "dado cualquier conjunto finito de primos, siempre hay otro primo que no pertenece al conjunto", y así eliminamos toda referencia al infinito).

2. Las afirmaciones con un significado intuitivo preciso que no aluden a ZFC, que podemos considerar tanto como *afirmaciones metamatemáticas* materiales o como *afirmaciones matemáticas* formales (como por ejemplo $2 + 2 = 4$).

3. Las afirmaciones sin un contenido intuitivo preciso que, en principio, sólo podemos entender formalmente, como *afirmaciones matemáticas* formales expresables en el lenguaje de la teoría de conjuntos, a menos que seamos platonistas y estemos convencidos de que ZFC habla de una realidad objetiva, de unos "conjuntos de verdad", sin perjuicio de que admita otros modelos "patológicos" como los modelos numerables que se obtienen del teorema de Löwenheim-Skolem o de la prueba de Gödel del teorema de completitud.

En el tercer caso es importante señalar que, incluso un platonista razonable concederá que no está en condiciones de razonar informalmente sobre afirmaciones del estilo de "existen infinitos cardinales infinitos", sino que es necesario tratarlas en el marco de una teoría axiomática formal, por lo que la distinción entre si, pese a ello, se les atribuye un significado objetivo o se las considera como palabras sin sentido es algo que queda en el terreno de la filosofía personal de cada cual y que no tiene ninguna repercusión práctica.

Pero es fundamental que el lector entienda que esta distinción entre "matemática" y "metamatemática" no es una distinción filosófica de la que uno puede olvidarse tranquilamente como de cualquier distinción filosófica, sino que no tenerla presente es la razón principal por la que a muchos matemáticos les cuesta entender la metamatemática, o incluso fracasan en el intento.

48 Modelos no estándar Para ilustrar este hecho, vamos a analizar una consecuencia del teorema de completitud de Gödel.[72] Vamos a considerar la teoría ZFC, aceptando como hipótesis que es consistente, pero todo cuanto vamos a hacer se puede hacer igualmente partiendo de cualquier teoría axiomática formal consistente en la que se puedan demostrar las propiedades básicas de los números naturales.

Para entender el argumento es crucial distinguir entre los números naturales metamatemáticos, es decir, los números naturales "de verdad", los que conoce un niño de seis años, y los números naturales matemáticos, los definidos en ZFC. Los números naturales "de verdad" son $0, 1, 2, 3, \ldots$ y lo que vamos a ver es que es imposible garantizar que los números naturales definidos en términos de conjuntos no contengan otros además de éstos.

Precisando un poco, los números naturales metamatemáticos son el cero y los que se pueden obtener a partir del cero aplicando un número finito de veces la operación "siguiente de", que nos da cada vez un nuevo número natural, distinto de los anteriores. Así tenemos el cero 0, el siguiente de cero, que llamamos 1, el siguiente del siguiente de 0, que llamamos 2, etc., donde "etc." significa "etc.", es decir, que los números naturales no son ni más ni menos que los que se van obteniendo al ir añadiendo una y otra vez "el siguiente de" a las expresiones de la forma "el siguiente del siguiente del siguiente del siguiente de cero".

Cuando los matemáticos definen el conjunto $\mathbb{N}$ de los números naturales tratan de imitar esta idea, de modo que acaban teniendo definida una operación "siguiente de", que es una aplicación $S : \mathbb{N} \longrightarrow \mathbb{N}$, donde el conjunto $\mathbb{N}$ se define con la intención de que $\mathbb{N}$ no tenga más elementos que $0 \in \mathbb{N}$, $S(0) \in \mathbb{N}$, $S(S(0)) \in \mathbb{N}$, $S(S(S(0))) \in \mathbb{N}$, etc. Lo que vamos a ver es que, se defina $\mathbb{N}$ como se defina, nunca podremos asegurar que en $\mathbb{N}$ no hay más elementos, aparte de éstos.

Para marcar unas diferencias que son esenciales, si n es un número natural metamatemático (un número natural "de verdad"), vamos a llamar $\ulcorner n \urcorner$ al *numeral* que lo representa en ZFC, es decir, $\ulcorner 0 \urcorner$ es el único conjunto que en ZFC satisface la definición de "cero" (conjunto que normalmente representamos como 0, pero aquí vamos a llamarlo $\ulcorner 0 \urcorner$). Similarmente,

$$\ulcorner 1 \urcorner = S(\ulcorner 0 \urcorner), \quad \ulcorner 2 \urcorner = S(\ulcorner 1 \urcorner) = S(S(\ulcorner 0 \urcorner)), \quad \ulcorner 3 \urcorner = S(\ulcorner 2 \urcorner) = S(S(S(\ulcorner 0 \urcorner))), \quad \ldots$$

Esto hay que entenderlo bien, porque no es una definición, sino infinitas definiciones: hemos definido lo que es $\ulcorner 0 \urcorner$ (que es lo que normalmente llamamos 0), y también lo que es $\ulcorner 1 \urcorner$ (que es el conjunto que normalmente llamamos 1), y también lo que es $\ulcorner 2 \urcorner$, etc. Para cada número natural metamatemático n tenemos definido un conjunto $\ulcorner n \urcorner$. Concretamente, $\ulcorner n \urcorner$ es el conjunto que se obtiene de $\ulcorner 0 \urcorner$ aplicándole n veces la función S.

[72] El resultado que vamos a discutir fue publicado por primera vez por Skolem en 1934, en su artículo *Sobre la imposibilidad de caracterizar la sucesión numérica mediante una cantidad finita o infinita numerable de proposiciones que contengan variables únicamente para números,* mediante una técnica que anticipaba el concepto de "ultraproducto", pero Gödel señaló que en realidad ya se deducía de su teorema de completitud, y probablemente estaba pensando en el argumento que vamos a exponer aquí.

Así, por ejemplo, no debemos confundir una fórmula como $m = n$, donde m y n son variables del lenguaje de la teoría de conjuntos, con una fórmula como $m = \ulcorner n \urcorner$, donde ahora m es una variable y n un número natural metamatemático. Para cada número n, tenemos infinitas fórmulas

$$m = \ulcorner 0 \urcorner, \quad m = \ulcorner 1 \urcorner, \quad m = \ulcorner 2 \urcorner, \quad \ldots$$

cada una de las cuales tiene únicamente UNA (única) variable libre (la m). La fórmula $m = n$ tiene DOS variables libres, m y n, mientras que las fórmulas $m = \ulcorner n \urcorner$ tienen UNA (única) variable libre cada una (la m).

Ahora, el matemático familiarizado con ZFC sabe que no es admisible definir el conjunto $\mathbb{N}$ de los números naturales como

$$\mathbb{N} = \{\ulcorner 0 \urcorner, \quad \ulcorner 1 \urcorner, \quad \ulcorner 2 \urcorner, \quad \ldots \quad \},$$

porque esos puntos suspensivos no permiten traducir la fórmula $x \in \mathbb{N}$ en una fórmula del lenguaje de la teoría de conjuntos, luego eso no es una definición válida. En términos intuitivos sí que podemos decir que el conjunto de los números naturales está formado por los números $0, 1, 2, \ldots$, y ahí esos puntos suspensivos tienen un significado preciso, pero en el formalismo de ZFC la pregunta no es si los puntos suspensivos significan algo, sino a qué fórmula estamos haciendo referencia con $x \in \mathbb{N}$, y esos puntos suspensivos no concretan ninguna fórmula. Lo más parecido sería una "fórmula infinita" del estilo de

$$x = \ulcorner 0 \urcorner \quad \vee \quad x = \ulcorner 1 \urcorner \quad \vee \quad x = \ulcorner 2 \urcorner \quad \vee \quad \cdots$$

pero el lenguaje de la teoría de conjuntos no admite fórmulas infinitas. Tampoco tiene sentido definir $x \in \mathbb{N}$ como $\bigvee n\, x = \ulcorner n \urcorner$, porque esto último es un despropósito. Para que tuviera sentido $\bigvee n$, necesitaríamos que n fuera una variable del lenguaje de la teoría de conjuntos, pero entonces no tendría sentido $\ulcorner n \urcorner$, que requiere que n sea un número natural metamatemático. No obstante, hay muchas formas de definir rigurosamente los números naturales en ZFC, y el lector puede adoptar su favorita, no importa cual.[73] Lo que vamos a ver es que, elijamos la definición que elijamos, nunca podremos asegurar que el conjunto $\mathbb{N}$ no contenga un conjunto distinto de $\ulcorner 0 \urcorner, \quad \ulcorner 1 \urcorner, \quad \ulcorner 2 \urcorner, \quad \ldots$

En efecto, vamos a considerar el lenguaje formal que resulta de añadir al lenguaje de la teoría de conjuntos un nuevo signo c, una constante que interpretamos como un cierto conjunto, pero que no definimos cuál es, igual que no definimos la relación $\in$. Como sucede con todo signo formal no definido, cada vez que fijamos un modelo de este lenguaje, tenemos que especificar —además de cuáles son los objetos de su universo y con qué relación R se interpreta sobre ellos el relator $\in$— qué objeto del universo del modelo es el que nombra la constante c.

Llamamos ZFC′ a la teoría axiomática sobre este lenguaje extendido con la constante c cuyos axiomas son los de ZFC más los infinitos axiomas siguientes:

$$c \in \mathbb{N}, \quad c \neq \ulcorner 0 \urcorner, \quad c \neq \ulcorner 1 \urcorner, \quad c \neq \ulcorner 2 \urcorner, \quad c \neq \ulcorner 3 \urcorner, \quad c \neq \ulcorner 4 \urcorner, \quad c \neq \ulcorner 5 \urcorner, \quad \ldots$$

Así, los axiomas de ZFC′ afirman en primer lugar que se cumplen todas las propiedades básicas que los matemáticos postulan usualmente de los conjuntos, con lo que en particular en ZFC′ se pueden demostrar todos los teoremas que los matemáticos saben demostrar sobre los números naturales, y además tenemos un conjunto c que cumple $c \in \mathbb{N}$, es decir, que cumple la definición formal que hayamos elegido de número natural, pero que no cumple ni la definición de 0, ni la de 1, ni la de 2, etc.

Si en este punto el lector ha conjeturado que la teoría ZFC′ es contradictoria, debe ponerse en guardia porque se equivoca, y probablemente su error consiste en que no distingue debidamente entre matemática y metamatemática. Vamos a demostrar que ZFC′ es una teoría consistente (si es que ZFC lo es).

Si ZFC′ fuera contradictorio, significaría que a partir de sus axiomas se puede deducir lógicamente una contradicción, pero una deducción lógica es una sucesión finita de fórmulas que termina en la conclusión (en este caso en la contradicción), y sólo puede contener una cantidad finita de axiomas. En particular, habrá un número natural N tal que la contradicción se deducirá empleando a lo sumo algunos axiomas de ZFC, más algunos axiomas entre

$$c \in \mathbb{N}, \quad c \neq \ulcorner 0 \urcorner, \quad c \neq \ulcorner 1 \urcorner, \quad \ldots \quad c \neq \ulcorner N \urcorner.$$

Llamamos ZFC^N a la teoría axiomática que consta de los axiomas de ZFC más estos axiomas, que, según lo que acabamos de razonar, será contradictoria, pues la demostración que tenemos de una contradicción en ZFC′ usa únicamente los axiomas de ZFC^N. Ahora bien, si ZFC es consistente, por el teorema de completitud semántica tiene un modelo, y el punto clave es que dicho modelo se convierte en un modelo de ZFC^N sin más que interpretar la constante c como el número natural $N + 1$ del modelo.

[73] Una posibilidad es la definición de Dedekind, de 1888, que ya hemos discutido.

En efecto, si tenemos unos objetos que cumplen los axiomas de ZFC e interpretamos la constante c como el objeto de su universo que cumple la definición de $N+1$, entonces en el modelo definido de ese modo se cumplen los axiomas de ZFC, así como que c es un número natural distinto de $0, 1, \ldots N$, luego todos los axiomas de ZFC^N se cumplen en dicho modelo. Como ZFC^N tiene un modelo, concluimos que es consistente (por el recíproco del teorema de completitud semántica), pero bajo el supuesto de que ZFC′ es contradictorio habíamos llegado a que ZFC^N (para cierto N) debía ser contradictorio también. Como hemos visto que no es así, la conclusión final es que ZFC′ tiene que ser consistente.

Si el lector pensaba (o sigue pensando) que ZFC′ es contradictorio, tal vez se deba a que confunda los infinitos axiomas adicionales de esta teoría, que afirman que c es un número natural distinto de todos —con un "todos" metamatemático— los números naturales, con el (único) axioma:

$$c \in \mathbb{N} \wedge \bigwedge x \in \mathbb{N}\, c \neq x$$

que afirma que c es un número natural distinto de todos —con un "todos" matemático— los números naturales. Este axioma sí que es contradictorio, pues de él se puede deducir lógicamente que $c \neq c$.

El caso es que ZFC′ es consistente, luego tiene un modelo, y dicho modelo está formado por unos objetos que cumplen los axiomas de ZFC, y además entre ellos hay uno (un conjunto, el que interpreta a la constante c) para el que se cumple $c \in \mathbb{N}$, es decir, que cumple la definición de número natural, pero a la vez es diferente del número natural 0, y del 1, y del 2, etc. Dicho objetos es un número natural diferente de "todos" (metamatemático) los números naturales "de verdad", pero no es distinto de "todos" (matemático) los números naturales, ya que él mismo es un número natural y no es diferente de sí mismo.

No vamos a entrar en ello, pero puede demostrarse que $c > \ulcorner 0 \urcorner$ y $c > \ulcorner 1 \urcorner$, y $c > \ulcorner 2 \urcorner$, etc., por lo que es un número natural mayor que todos los números naturales de verdad. Esto es lo que se llama un *número natural no estándar,* y un modelo con números no estándar se dice que es un *modelo no estándar de* ZFC. Más aún, en ZFC puede probarse que

$$\bigwedge n \in \mathbb{N} \bigvee x(\bigwedge u(u \in x \leftrightarrow u \in \mathbb{N} \wedge u < n) \wedge x \text{ es finito}),$$

es decir, que para todo número natural n existe un conjunto cuyos elementos son los números naturales menores que n, y tal conjunto es finito (pues tiene n elementos). Como esto tiene que ser cierto en el modelo no estándar que estamos considerando, podemos considerar el conjunto X formado por los números naturales menores que c, que es un conjunto finito, pero contiene al 0, y al 1, y al 2, y al 3, etc. Tenemos, por lo tanto, un conjunto que satisface la definición de "conjunto finito" que se da en ZFC, pero que contiene infinitos elementos.

Ésta es la conclusión a la que llegó Skolem en su artículo de 1934: sea cual sea la definición formal que demos de "número natural" o de "conjunto finito" (con tal de que permitan demostrar las propiedades básicas de los números naturales y los conjuntos finitos, respectivamente) existe un modelo de ZFC en el que hay un conjunto que satisface la definición de "número natural" que hayamos elegido, pero es distinto de $0, 1, 2, 3, \ldots$ y existe un conjunto que satisface la definición de "conjunto finito" que hayamos elegido, pero que contiene a todos (con un "todos" metamatemático) los números $0, 1, 2, 3, \ldots$) Equivalentemente, es imposible forzar con una definición bien elegida a que los únicos números naturales sean $0, 1, 2, \ldots$ o a que los conjuntos finitos tengan únicamente una cantidad finita de elementos. En realidad Skolem probó esto para una teoría axiomática en concreto. El razonamiento a partir del teorema de completitud vale para cualquier teoría axiomática en la que se puedan definir los números naturales y el concepto de finitud.

Con esto Skolem rebatía la idea de Zermelo según la cual no había que presuponer los números naturales en una construcción de ZFC, sino que ZFC es el marco conceptual adecuado para dar una definición rigurosa del concepto de número natural. Para alguien que identifique los números naturales con los conjuntos que satisfacen la definición en ZFC de número natural, todo el argumento que acabamos de exponer se vuelve completamente ininteligible.

La existencia de modelos no estándar de ZFC pone en evidencia una vez más la imposibilidad de identificar "conjunto" con "colección de conjuntos". Por ejemplo, en un modelo no estándar de ZFC, la colección de los números naturales no estándar es una colección de conjuntos que no puede ser un conjunto, porque si lo fuera, un teorema de ZFC dice que todo conjunto no vacío de números naturales debe tener un mínimo elemento, y es imposible que exista un mínimo número natural no estándar.

En efecto, si un número natural n es estándar (es decir, si se obtiene del 0 mediante un número finito de aplicaciones de la operación "siguiente de"), se cumple que $n+1$ también es estándar (pues se obtiene aplicando

una vez más la operación "siguiente"), luego, recíprocamente, si n es un número natural no estándar, cumple que $n > 0$ y además $n - 1$ también tiene que ser no estándar, luego ningún número no estándar es el mínimo de todos ellos. La colección de todos los números naturales no estándar es una colección no vacía de números naturales sin mínimo elemento. No hay contradicción porque dicha colección no es un conjunto (y sabemos que no es un conjunto precisamente porque si lo fuera tendríamos una contradicción).

49 La formalización de la lógica El apartado precedente tenía como objetivo que el lector tuviera una primera aproximación de las dificultades que plantea la necesidad de distinguir entre matemática y metamatemática para entender la lógica matemática en general y los teoremas de incompletitud de Gödel en particular. Sin embargo, una primera aproximación no es ilustrativa, pues los teoremas de incompletitud requieren otra vuelta de tuerca.

La idea principal que hemos tratado de transmitir en el apartado precedente es que el estudio de la lógica matemática requiere trabajar a dos niveles bien diferenciados:

- El nivel 0 de la *metateoría,* en el que, en principio, razonamos informalmente, exigiendo que cada afirmación que hagamos tenga un significado intuitivamente preciso (y que para la demostración de los teoremas de incompletitud podemos exigir que dicho significado sea finitista en el sentido más estricto posible del término).
- El nivel 1 de la *teoría,* en el que razonamos deduciendo formalmente de unos axiomas arbitrarios, que pueden ser los axiomas de ZFC o cualesquiera otros, pues el razonamiento formal nos exime de la necesidad de atribuir un significado claro y preciso a las fórmulas consideradas.

Sin embargo, la prueba de los teoremas de incompletitud requiere trabajar, no a dos, sino a tres niveles bien diferenciados. La idea es que en ZFC pueden definirse todos los conceptos matemáticos: podemos definir los números, los polinomios, los grafos, los espacios vectoriales, las matrices, las variedades diferenciales, etc. y nada impide definir igualmente en ZFC los conceptos de "lenguaje formal", "teoría axiomática", "demostración", etc. En particular, en ZFC podemos definir ZFC. Vamos a desarrollar un poco esta idea:

Los signos del lenguaje de la teoría de conjuntos son los de la fila superior de la tabla siguiente:

$\neg$	$\to$	$\vee$	$\wedge$	$\leftrightarrow$	$\bigwedge$	$\bigvee$	$=$	$\in$	x_0	x_1	x_2	$\ldots$
0	1	2	3	4	5	6	7	8	9	10	11	$\ldots$

donde $x_0, x_1, x_2, \ldots$ son las variables, que a menudo nombramos con letras arbitrarias, como x, y, z.

Del mismo modo que si queremos abordar matemáticamente un problema sobre cinco ciudades podemos representarlas por el conjunto $\{1, 2, 3, 3, 5\}$, y decimos que 1 es "la primera ciudad", para hablar de estos signos en ZFC podemos identificar cada signo con el número natural que tiene debajo en la tabla.

A su vez, cada fórmula, como el axioma del conjunto vacío: $\alpha \equiv \bigvee x_0 \bigwedge x_1 \neg x_1 \in x_0$, se identifica con una sucesión de números naturales, en este caso $(6, 9, 5, 10, 0, 10, 8, 9)$ o, si queremos distinguir entre los números naturales y los numerales que los nombran, sería

$$\ulcorner\alpha\urcorner \equiv (\ulcorner 6\urcorner, \ulcorner 9\urcorner, \ulcorner 5\urcorner, \ulcorner 10\urcorner, \ulcorner 0\urcorner, \ulcorner 10\urcorner, \ulcorner 8\urcorner, \ulcorner 9\urcorner).$$

Así, del mismo modo que una cosa es el número natural 3 y otra el numeral $\ulcorner 3\urcorner = S(S(S(0)))$ definido en ZFC, una cosa es el axioma del conjunto vacío α, que es una cadena de signos del lenguaje de la teoría de conjuntos (y, en particular, no es un conjunto, sino una afirmación sobre conjuntos), y otra cosa el conjunto $\ulcorner\alpha\urcorner$ que nombra a α en ZFC.

Del mismo modo que en ZFC se puede definir el conjunto P de los números primos, y si p es un número primo, en ZFC se puede demostrar que $\ulcorner p\urcorner \in P$, también podemos definir el conjunto Form de las fórmulas del lenguaje de la teoría de conjuntos, y si α es una fórmula, en ZFC se puede demostrar que $\ulcorner\alpha\urcorner \in \mathrm{Form}$.

Igualmente podemos definir en ZFC los subconjuntos de Form formados por los axiomas lógicos y los axiomas de ZFC, y a su vez el conjunto de las demostraciones en ZFC, y el conjunto de los teoremas de ZFC, etc. En general, toda la lógica que se puede desarrollar metamatemáticamente sobre ZFC, se puede reinterpretar como una serie de teoremas de ZFC sobre la versión formalizada de ZFC. Más en general, en ZFC podemos definir el concepto general de "lenguaje formal" y de "teoría axiomática formal" y estudiar teorías axiomáticas en general

del mismo modo que podemos definir el concepto general de "espacio vectorial" y estudiar espacios vectoriales en general. Cuando hacemos esto, la lógica matemática se convierte en una rama más de la matemática que puede estudiarse desde ZFC, igual que el álgebra, la geometría, el análisis matemático, la estadística, etc.

Ahora tenemos tres niveles distintos de trabajo:

- El nivel 0 de la *metateoría,* en el que, en principio, razonamos informalmente, exigiendo que cada afirmación que hagamos tenga un significado intuitivamente preciso (y que para la demostración de los teoremas de incompletitud podemos exigir que dicho significado sea finitista en el sentido más estricto posible del término).
- El nivel 1 de la *teoría,* en el que razonamos deduciendo formalmente de unos axiomas arbitrarios, que pueden ser los axiomas de ZFC o cualesquiera otros, pues el razonamiento formal nos exime de la necesidad de atribuir un significado claro y preciso a las fórmulas consideradas.
- El nivel 2 de la *teoría formalizada,* en el que razonamos exactamente igual que en el nivel 1, con la diferencia de que en la metateoría para estudiar el nivel 1 razonamos intuitivamente, mientras que la metateoría para estudiar el nivel 2 es ZFC (o la teoría axiomática que estemos considerando en el nivel 1).

Aquí hemos tomado ZFC como ejemplo para ilustrar la situación, pero una de las muchas ideas brillantes que tuvo Gödel para demostrar los teoremas de incompletitud fue demostrar que no hace falta ZFC, sino que en cualquier teoría axiomática recursiva en la que se puedan definir los números naturales y en la que se puedan demostrar sus propiedades elementales es posible formalizar cualquier otra teoría axiomática. Por ejemplo, hemos visto cómo en teoría de conjuntos se puede definir el axioma del conjunto vacío como la sucesión finita

$$\ulcorner\alpha\urcorner \equiv (\ulcorner 6\urcorner, \ulcorner 9\urcorner, \ulcorner 5\urcorner, \ulcorner 10\urcorner, \ulcorner 0\urcorner, \ulcorner 10\urcorner, \ulcorner 8\urcorner, \ulcorner 9\urcorner).$$

Si queremos trabajar en una teoría aritmética T en la que no es posible definir sucesiones finitas de números, siempre podemos definir

$$\ulcorner\alpha\urcorner \equiv \ulcorner 2\urcorner^{\ulcorner 6\urcorner} \cdot \ulcorner 3\urcorner^{\ulcorner 9\urcorner} \cdot \ulcorner 5\urcorner^{\ulcorner 5\urcorner} \cdot \ulcorner 7\urcorner^{\ulcorner 10\urcorner} \cdot \ulcorner 11\urcorner^{\ulcorner 0\urcorner} \cdot \ulcorner 13\urcorner^{\ulcorner 10\urcorner} \cdot \ulcorner 17\urcorner^{\ulcorner 8\urcorner} \cdot \ulcorner 19\urcorner^{\ulcorner 9\urcorner},$$

es decir, considerando que cada número natural no nulo codifica la sucesión finita de los exponentes de su descomposición en factores primos.

Así pues, si llamamos *teorías aritméticas* a las teorías axiomáticas en las que es posible demostrar las propiedades básicas de los números naturales (los axiomas de la aritmética de Peano), Gödel demostró que cualquier teoría aritmética T' sirve como metateoría para estudiar formalmente cualquier teoría axiomática recursiva T. Y la demostración de su teorema se basa en el caso particular en que T se usa como metateoría para estudiar T.

En estos términos, el planteamiento de la demostración de los teoremas de incompletitud de Gödel es el siguiente:

1. En el nivel 0 (es decir, razonando intuitivamente), tomamos una teoría aritmética recursiva T de la que suponemos que es consistente, así como que tenemos un criterio que nos permite determinar si una fórmula dada de su lenguaje formal es o no un axioma.
2. En el nivel 1 (es decir, razonando en T) probamos que se puede definir la formalización $\ulcorner T\urcorner$ de la teoría T (y es en este punto en el que es fundamental que ésta sea recursiva).
3. En el nivel 0 mostramos que, a cada fórmula ψ del lenguaje formal de T (para cada afirmación de nivel 1) le podemos asociar un objeto $\ulcorner\psi\urcorner$ que en T (es decir, al nivel 1) se demuestra que es una fórmula de la teoría formalizada $\ulcorner T\urcorner$ (una afirmación de nivel 2).
4. Pero la idea más brillante subyacente a los teoremas de incompletitud (rayana en lo diabólico y demostrada a nivel 0) afirma que, para cada fórmula $\phi(x)$ del lenguaje de T con x como única variable libre, existe una sentencia ψ del lenguaje de T, de modo que en T (es decir, a nivel 1) se demuestra la equivalencia

   $$\psi \leftrightarrow \phi(\ulcorner\psi\urcorner).$$

   En otras palabras, para cualquier propiedad $\phi(x)$, existe una sentencia ψ (de nivel 1) que, a nivel 1, equivale a que su formalización $\ulcorner\psi\urcorner$ (a nivel 2) tiene la propiedad ϕ. Podríamos decir que ψ significa "yo tengo la propiedad ϕ", donde "yo" es en realidad "mi formalización".

5. Cuando se aplica este teorema tomando como $\phi(x)$ la propiedad "x no es una fórmula demostrable en $\ulcorner T\urcorner$", obtenemos una sentencia G (la *sentencia de Gödel* de T) tal que en T se puede demostrar:

$$G \leftrightarrow \ulcorner G\urcorner \text{ no es demostrable en } \ulcorner T\urcorner.$$

6. **Primer teorema de incompletitud de Gödel** Si T es consistente, la sentencia de Gödel no es demostrable en T y, bajo una hipótesis adicional (que se puede eliminar cambiando G por una fórmula un poco más sofisticada), su negación $\neg G$ tampoco lo es, por lo que la teoría T es incompleta. De hecho, la sentencia G es verdadera (porque afirma que ella misma no se puede demostrar y eso es cierto), pero no es demostrable en T.

7. **Segundo teorema de incompletitud de Gödel** En T se puede demostrar que

$$G \leftrightarrow \text{Consis}\ulcorner T\urcorner,$$

donde la sentencia de la derecha es la que afirma que $\ulcorner T\urcorner$ es una teoría consistente, es decir, que en ella no se pueden demostrar contradicciones. Por consiguiente, si T es consistente, la consistencia de $\ulcorner T\urcorner$ no puede ser demostrada en T.

En estos términos, Hilbert quería demostrar la consistencia de una teoría de conjuntos T del estilo de ZFC trabajando en una metateoría finitista, pero Gödel demostró que la consistencia de ZFC no puede demostrarse ni siquiera tomando como metateoría la propia ZFC. Puesto que cualquier razonamiento que un matemático considera aceptable es formalizable en ZFC, la conclusión es que la consistencia de ZFC es indemostrable.

Los teoremas de incompletitud darían que hablar a muchos filósofos que en realidad no los entendían. Una de las cosas que más les impactaba era que, como hemos dicho en 6, la sentencia de Gödel G es verdadera, pero no demostrable. Esto hizo correr ríos de tinta sosteniendo que la mente humana es superior a cualquier máquina, porque es capaz de concluir que una afirmación G es verdadera sin que ello pueda demostrarse formalmente. Pero eso es una tontería fruto de no haber entendido nada. Como señalamos en 7, la sentencia G es equivalente a la consistencia de la teoría, y esto es una de las hipótesis de los teoremas de incompletitud, luego no es que sepamos que G es verdadera, pero no es demostrable, sino que lo que se demuestra en realidad es que, *en el supuesto* de que G sea verdadera, no es demostrable. Pero no sabemos que G sea verdadera o, por lo menos, no lo sabemos en virtud del teorema de incompletitud.

La consistencia de los cardinales inaccesibles El segundo teorema de incompletitud tiene innumerables aplicaciones. Por ejemplo, llamemos FI a la fórmula que afirma que existe un cardinal fuertemente inaccesible. Según hemos visto, Zermelo había demostrado que si κ es un cardinal fuertemente inaccesible, entonces V_κ es un modelo de ZFC, y el hecho de que ZFC tenga un modelo implica que es consistente. Así pues, en ZFC+FI puede demostrarse la fórmula

$$\text{Consis}\ulcorner \text{ZFC}\urcorner.$$

También hemos visto que Zermelo había demostrado que si ZFC es consistente, también lo es suponer que no existen cardinales fuertemente inaccesibles (pues basta tomar un modelo de ZFC y, o bien no tiene cardinales fuertemente inaccesibles, o bien tiene uno mínimo κ, en cuyo caso V_κ es un modelo en el que no hay cardinales fuertemente inaccesibles), pero quedaba pendiente estudiar si la consistencia de ZFC implica también la consistencia de que existan cardinales fuertemente inaccesibles.

Supongamos que pudiéramos demostrar que es así. Supongamos que tenemos un argumento, no necesariamente finitista, sino que nos basta con que pueda ser expresado en ZFC, lo cual es mucho más de lo que sería razonable para que pudiéramos considerarlo "convincente". En tal caso, en ZFC podríamos demostrar la implicación

$$\text{Consis}\ulcorner \text{ZFC}\urcorner \to \text{Consis}\ulcorner \text{ZFC} + \text{FI}\urcorner.$$

Entonces, como en ZFC+FI se puede demostrar $\text{Consis}\ulcorner \text{ZFC}\urcorner$, en ZFC + FI podríamos demostrar también $\text{Consis}\ulcorner \text{ZFC} + \text{FI}\urcorner$, pero esto es justo lo que el segundo teorema de incompletitud dice que no es posible. Una teoría no puede demostrar su propia consistencia, a menos que sea contradictoria, luego podríamos concluir que ZFC + FI sería una teoría contradictoria y, si hemos probado que la consistencia de ZFC implica la consistencia de ZFC + FI, podremos concluir que ZFC también es contradictorio. En resumen:

> Si ZFC es consistente, aunque ZFC más la existencia de un cardinal fuertemente inaccesible sea consistente, es imposible demostrar que así es, incluso tomando como hipótesis la consistencia de ZFC.

El segundo teorema de incompletitud mostraba que la presunta prueba finitista de Ackermann de la consistencia de la aritmética de Peano tenía que estar mal (una prueba finitista tenía que poder formalizarse en la propia aritmética de Peano, en contra de lo que permite el teorema de incompletitud). En efecto, von Neumann la examinó con detalle y comprobó, de hecho, que la técnica principal en la que se basaba no era concluyente.

50 Representación de funciones recursivas Ahora estamos en condiciones de entender la relación entre las relaciones y funciones recursivas y la demostración de los teoremas de incompletitud. Para ello introducimos unas definiciones:

Se dice que una relación $R(x_1,\dots,x_n)$ definida sobre los números naturales es *expresable* en una teoría T (en la que se puedan definir los números naturales) por una fórmula $\phi(x_1,\dots,x_n)$ si:

1. Cuando se cumple $R(a_1,\dots,a_n)$, entonces en T se puede demostrar $\phi(\ulcorner a_1\urcorner,\dots,\ulcorner a_n\urcorner)$,
2. Cuando no se cumple $R(a_1,\dots,a_n)$, entonces en T se puede demostrar $\neg\phi(\ulcorner a_1\urcorner,\dots,\ulcorner a_n\urcorner)$.

Se dice que una función $f(x_1,\dots,x_n)$ definida sobre los números naturales es *representable* en T por una fórmula $\phi(x_1,\dots,x_n,x)$ si:

1. Cuando se cumple $f(a_1,\dots,a_n)=a$, entonces en T se puede demostrar $\phi(\ulcorner a_1\urcorner,\dots,\ulcorner a_n\urcorner,\ulcorner a\urcorner)$,
2. Cuando no se cumple $f(a_1,\dots,a_n)=a$, entonces en T se puede demostrar $\neg\phi(\ulcorner a_1\urcorner,\dots,\ulcorner a_n\urcorner,\ulcorner a\urcorner)$,
3. Para todos los números naturales $a_1,\dots,a_n$, en T se puede demostrar

$$\bigwedge xy(\phi(\ulcorner a_1\urcorner,\dots,\ulcorner a_n\urcorner,x)\wedge\phi(\ulcorner a_1\urcorner,\dots,\ulcorner a_n\urcorner,y)\to x=y).$$

Esto significa que los cálculos sobre si una relación se cumple o no para unos números, o sobre cuál es el valor que toma una función se pueden realizar razonando en la teoría T.

Una relación $R(x_1,\dots,x_n)$ se dice *recursiva* si la función

$$f(x_1,\dots,x_n)=\begin{cases}1 & \text{si se cumple } R(x_1,\dots,x_n),\\ 0 & \text{si no se cumple } R(x_1,\dots,x_n),\end{cases}$$

es recursiva, lo que en la práctica se interpreta como que existe un procedimiento efectivo para determinar si unos números dados cumplen o no la relación. Gödel demostró:

> Toda relación recursiva es expresable en cualquier teoría aritmética, y toda función recursiva es representable en cualquier teoría aritmética.

Para comprender la relevancia de este hecho, vamos a demostrar el resultado que hemos enunciado en el punto 4 de la página 104:

> **Lema de autorreferencia de Gödel** Si T es una teoría axiomática recursiva, para cada fórmula $\phi(x)$ del lenguaje de T con x como única variable libre, existe una sentencia ψ del lenguaje de T, de modo que en T se demuestra la equivalencia
>
> $$\psi\leftrightarrow\phi(\ulcorner\psi\urcorner).$$

Demostración: Aquí hay que entender que cada fórmula ψ del lenguaje de T se puede codificar con un número natural $\ulcorner\psi\urcorner$, de modo que en la práctica siempre podemos saber si un número natural dado es el código de una fórmula y, en caso afirmativo, de cual. A su vez, ese número natural $\ulcorner\psi\urcorner$ se representará en la teoría mediante un numeral[74] que, en principio, deberíamos llamar $\ulcorner\ulcorner\psi\urcorner\urcorner$, pero que por simplicidad llamaremos $\ulcorner\psi\urcorner$.

Esto nos permite definir una función F de modo que, si un número n es el código de una fórmula $\alpha(x)$ con x como única variable libre, entonces $F(n)=\ulcorner\alpha(\ulcorner n\urcorner)\urcorner$, y en caso contrario $F(n)=0$.

Más detalladamente: tomamos un número n, lo examinamos para ver si codifica una fórmula $\alpha(x)$, es decir, si es de la forma $n=\ulcorner\alpha(x)\urcorner$, donde $\alpha(x)$ tiene una única variable libre. Si no es así, concluimos que $F(n)=0$. En caso contrario, calculamos el numeral $\ulcorner n\urcorner$ y lo sustituimos en α, para formar la sentencia $\alpha(\ulcorner n\urcorner)$. Entonces $F(n)=\ulcorner\alpha(\ulcorner n\urcorner)\urcorner$ es el código de esta sentencia.

[74] Por ejemplo, una cosa es el axioma del conjunto vacío $\psi\equiv\bigvee x_0\bigwedge x_1\neg x_1\in x_0$, otra cosa es el número natural $\ulcorner\psi\urcorner=2^6\cdot3^9\cdot5^5\cdot7^{10}\cdot11^0\cdot13^{10}\cdot17^8\cdot19^9$ y otra cosa el numeral $\ulcorner\ulcorner\psi\urcorner\urcorner=S\cdots S0$, donde S aparece $\ulcorner\psi\urcorner$ veces, que nombra a $\ulcorner\psi\urcorner$ en T.

Puesto que sabemos codificar y decodificar fórmulas en la práctica (y también sustituir variables por numerales en la práctica), la función $F(x)$ puede calcularse en la práctica, y eso se traduce en que es recursiva.[75] Por lo tanto, existe una fórmula $\theta(x,y)$ que la representa en T.

Ahora consideramos la fórmula

$$\sigma(x) \equiv \bigwedge y(\theta(x,y) \to \phi(y)),$$

que es una fórmula con x como única variable libre. Calculamos su código $n = \ulcorner\sigma(x)\urcorner$, que es un número natural, calculamos su numeral $\ulcorner n\urcorner$ y lo sustituimos en $\sigma(x)$, para obtener la sentencia $\psi \equiv \sigma(\ulcorner n\urcorner)$. Vamos a ver que cumple lo requerido.

En primer lugar observamos que, ψ se obtiene sustituyendo la x de $\sigma(x)$ por el numeral de $n = \ulcorner\sigma(x)\urcorner$ y, por definición de F, eso significa que $F(n) = \ulcorner\psi\urcorner$. Como ϕ representa a F, en T podemos demostrar:

$$\theta(\ulcorner\sigma(x)\urcorner, \ulcorner\psi\urcorner), \qquad \bigwedge uv(\theta(\ulcorner\sigma(x)\urcorner, u) \wedge \theta(\ulcorner\sigma(x)\urcorner, v) \to u = v),$$

donde, hemos simplificado $\ulcorner\ulcorner\sigma(x)\urcorner\urcorner$ y $\ulcorner\ulcorner\psi\urcorner\urcorner$ a $\ulcorner\sigma(x)\urcorner$ y $\ulcorner\psi\urcorner$, respectivamente.

Esto significa que $\ulcorner\psi\urcorner$ es el único y que cumple $\theta(\ulcorner\sigma(x)\urcorner, y)$, luego $\psi \equiv \bigwedge y(\theta(\ulcorner\sigma(x)\urcorner), y) \to \phi(y))$, que afirma que todo y que cumple $\theta(\ulcorner\sigma(x)\urcorner, y)$ también cumple $\phi(y)$, está diciendo únicamente que se cumple $\phi(\ulcorner\psi\urcorner)$, luego ambas sentencia son equivalentes, como había que probar. ∎

La idea subyacente a la prueba es que $\sigma(x)$ significa "la fórmula que se obtiene de la fórmula x cuando se le aplica la función F cumple ϕ", y entonces ψ significa "la fórmula que se obtiene de $\sigma(x)$ cuando se le aplica la función F cumple ϕ", pero por construcción dicha fórmula es ψ, luego ψ está hablando de sí misma (o de su codificación, para ser más exactos).

Hasta aquí no hemos necesitado que la teoría T sea recursiva. Que sea recursiva significa que tenemos un criterio para determinar si una fórmula dada es o no un axioma de T, que es lo único que necesitamos para poder comprobar en la práctica si una sucesión de fórmulas $\alpha_1, \ldots, \alpha_n$ es o no una demostración en T.

Cada fórmula de la sucesión puede codificarse por un número natural, con lo que obtenemos una sucesión de números naturales $\ulcorner\alpha_1\urcorner, \ldots, \ulcorner\alpha_n\urcorner$, que a su vez, puede codificarse con un único número natural $\ulcorner D\urcorner$, donde D es el nombre de la sucesión de fórmulas dada.

De este modo, nada impide en la práctica determinar si un número natural dado codifica o no una sucesión de fórmulas del lenguaje de T y, si la teoría T es recursiva, podemos saber, más concretamente, si codifica o no una demostración en T.

Por lo tanto, si T es una teoría aritmética recursiva, la relación $\mathrm{Dem}(m,n)$ que se cumple si n codifica una fórmula α de T y m codifica una demostración de α en T es recursiva y, por consiguiente, está representada en T por una fórmula $\phi(x,y)$, que podemos representar, más descriptivamente, como $\overset{x}{\underset{\ulcorner T\urcorner}{\vdash}} y$. Si usamos igualmente la notación $\overset{D}{\underset{T}{\vdash}} \alpha$ para expresar que D es una demostración de α en T, lo que tenemos es que:

1. Si $\overset{D}{\underset{T}{\vdash}} \alpha$, entonces, en T se puede demostrar $\overset{\ulcorner D\urcorner}{\underset{\ulcorner T\urcorner}{\vdash}} \ulcorner\alpha\urcorner$,

   es decir, si D es una demostración de α en T, entonces en T se puede demostrar que el numeral $\ulcorner D\urcorner$ que representa a D es una demostración del numeral $\ulcorner\alpha\urcorner$ que representa a α en T. Y análogamente:

2. Si no $\overset{D}{\underset{T}{\vdash}} \alpha$, entonces, en T se puede demostrar $\neg \overset{\ulcorner D\urcorner}{\underset{\ulcorner T\urcorner}{\vdash}} \ulcorner\alpha\urcorner$.

Definimos la fórmula $\underset{\ulcorner T\urcorner}{\vdash} y \equiv \bigvee x \overset{x}{\underset{\ulcorner T\urcorner}{\vdash}} y$, que significa que existe una demostración de y en T o, equivalentemente, que y es demostrable en $\ulcorner T\urcorner$. Así se cumple:

[75] De hecho, es recursiva primitiva, y Gödel mostró explícitamente que cumple la definición de función recursiva primitiva.

3. Si α es demostrable en T, entonces en T se puede demostrar $\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\alpha\urcorner$.

   En efecto, basta considerar una demostración D de α, con lo que tenemos $\overset{D}{\underset{T}{\vdash}}\alpha$, luego en T se puede demostrar $\underset{\ulcorner T\urcorner}{\overset{\ulcorner D\urcorner}{\vdash}}\ulcorner\alpha\urcorner$, y esto implica trivialmente que $\bigvee x\,\underset{\ulcorner T\urcorner}{\overset{x}{\vdash}}\ulcorner\alpha\urcorner$, y esto es $\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\alpha\urcorner$.

El lema de autorreferencia nos da ahora una sentencia G tal que en T se puede demostrar

$$G \leftrightarrow \neg \underset{\ulcorner T\urcorner}{\vdash}\ulcorner G\urcorner.$$

Esta es la sentencia de Gödel de la teoría T, cuyo significado es que ella misma no es demostrable en T.

Y ciertamente, si T es consistente, no es demostrable, porque, si lo fuera, en T se podría demostrar $\underset{\ulcorner T\urcorner}{\vdash}\ulcorner G\urcorner$ y, por construcción de T, esto implica $\neg G$, luego en T se podrían demostrar G y $\neg G$, con lo que T sería contradictoria.

51 ω-consistencia Continuando con el argumento, tenemos que si la teoría T es consistente, entonces G no es demostrable en T, luego ningún número natural codifica una demostración de G, es decir, que

$$\text{no } \overset{\ulcorner 0\urcorner}{\underset{T}{\vdash}}\ulcorner G\urcorner, \quad \text{no } \overset{\ulcorner 1\urcorner}{\underset{T}{\vdash}}\ulcorner G\urcorner, \quad \text{no } \overset{\ulcorner 2\urcorner}{\underset{T}{\vdash}}\ulcorner G\urcorner, \quad \text{no } \overset{\ulcorner 3\urcorner}{\underset{T}{\vdash}}\ulcorner G\urcorner, \quad \text{no } \overset{\ulcorner 4\urcorner}{\underset{T}{\vdash}}\ulcorner G\urcorner, \quad \ldots$$

mientras que si $\neg G$ pudiera demostrarse en T, por la construcción de G también podría demostrarse $\underset{\ulcorner T\urcorner}{\vdash}\ulcorner G\urcorner$, es decir:

$$\bigvee n\,\overset{n}{\underset{T}{\vdash}}\ulcorner G\urcorner,$$

(lo que implica en particular que n es un número natural). En suma: por una parte en T se podría demostrar que existe un número natural que codifica una demostración de $\ulcorner G\urcorner$ y, por otra, se podría demostrar que dicho número natural no puede ser 0, ni 1, ni 2, ni ningún otro.

Esto se expresa diciendo que T sería una teoría ω-contradictoria. En general, una teoría aritmética es *ω-contradictoria* si hay una fórmula $\phi(x)$ tal que en T se puede demostrar $\phi(0), \phi(1), \phi(2), \ldots$ pero también se puede demostrar $\bigvee x \neg\phi(x)$. En caso contrario se dice que la teoría es *ω-consistente*.

En contra de lo que pueda parecer, una teoría ω-contradictoria no tiene por qué ser contradictoria. En efecto, una teoría ω-contradictoria puede tener un modelo y, por consiguiente, ser consistente. Para ello sólo hace falta que el modelo contenga números naturales no estándar, es decir, números naturales distintos de $0, 1, 2, 3, \ldots$. Así puede suceder que $0, 1, 2, 3, \ldots$ cumplan todos $\phi(x)$, pero que, a la vez, haya un número no estándar que no tenga esta propiedad.

Lo que sí que es inmediato es que toda teoría ω-consistente T es consistente. Basta aplicar la definición de ω-consistencia a la fórmula $\phi(x) \equiv x = x$. Puesto que se puede demostrar $\phi(0), \phi(1), \phi(2), \ldots$, la ω-consistencia implica que no se puede demostrar $\bigvee x\, x \neq x$, y esto implica que T es consistente, pues en una teoría contradictoria se pueden demostrar todas las fórmulas.

Así hemos demostrado la formulación original del primer teorema de incompletitud de Gödel:

Toda teoría aritmética recursiva ω-consistente es incompleta.

En efecto, hemos probado que, bajo estas hipótesis, podemos construir una sentencia G tal que, si G es demostrable en T, entonces T es contradictoria y, si $\neg G$ es demostrable en T, entonces T es ω-contradictoria.

Más adelante veremos que, usando una sentencia distinta, el teorema puede probarse suponiendo meramente la consistencia de la teoría en lugar de la ω-consistencia.

52 La teoría de von Neumann-Bernays I Tras este análisis de las ideas subyacentes a la prueba de los teoremas de incompletitud, volvemos al año **1931** en el que Gödel los publicó. Ese año Bernays escribió una carta a Gödel en la que le mostró una teoría axiomática aún no publicada que había diseñado reformulando la teoría de funciones de von Neumann para hacerla lo más parecida posible a ZFC, pero incorporando el desterrado concepto cantoriano de "multiplicidad inconsistente". Para ello Bernays considera cuatro nociones primitivas no definidas: "conjunto", "clase", una pertenencia entre conjuntos $x \in y$, y una pertenencia de conjuntos a clases $x\,\eta\,Y$. Su teoría no admite que una clase pueda pertenecer a otra clase. También distingue dos tipos de variables, las que recorren conjuntos (que representa por letras minúsculas) y las que recorren clases (que representa por letras mayúsculas).

Así pues, tanto los conjuntos como las clases son colecciones de conjuntos. Cuando un conjunto x tiene exactamente los mismos elementos que una clase X, se dice que el conjunto x *representa* a la clase X. Bernays demostraba que todo conjunto representa una clase, pero no toda clase es representada por un conjunto. Las clases que no son representadas por conjuntos son precisamente el equivalente en la teoría a las multiplicidades inconsistentes de Cantor. En la teoría de Bernays existe la clase de todos los conjuntos, la clase de todos los ordinales, la clase de todos los conjuntos que no se pertenecen a sí mismos, etc., pero no dan lugar a contradicciones, sino que las paradojas correspondientes se convierten en demostraciones de que dichas clases no están representadas por ningún conjunto.

La teoría de Bernays —como la de von Neumann y al contrario que la de Zermelo o la de Zermelo-Fraenkel— requiere sólo un número finito de axiomas. A partir de un número finito de axiomas de existencia de clases, Bernays demuestra un esquema teoremático de formación de clases, según el cual, para cada fórmula $\phi(x)$, con la única restricción de que no contenga cuantificadores de tipo "para toda clase u" ni "existe una clase u" (pero sí que puede contener "para todo conjunto u" o "existe un conjunto u") se demuestra el teorema de comprensión:

$$\bigvee X \bigwedge u(u\,\eta\, X \leftrightarrow \phi(u)),$$

en otras palabras, siempre existe la clase de todos los conjuntos que cumplen la propiedad ϕ. Así, tomando como $\phi(u)$ la fórmula $u = u$ obtenemos la clase V de todos los conjuntos, tomando $u \notin u$ obtenemos la clase R de todos los conjuntos que no se pertenecen a sí mismos, etc. Como indicábamos, la paradoja de Russell se traduce en que la clase R no está representada por ningún conjunto, pues si existiera un conjunto r con los mismos elementos que R, es decir, si existiera un conjunto r cuyos elementos son todos los conjuntos que no se pertenecen a sí mismos, llegaríamos a que $r \in r$ implica $r \notin r$ y viceversa. Pero esto no es una contradicción. Sólo una demostración de que no existe r.

Además de los axiomas de formación de clases que permiten demostrar el teorema general (esquema teoremático, en realidad) de formación de clases, la teoría de Bernays cuenta con axiomas que garantizan la existencia de determinados conjuntos, muchos de los cuales son análogos a los axiomas correspondientes de Zermelo.

En resumen, la teoría de Bernays permite hablar parcialmente de clases no representables como conjuntos de forma análoga a como Cantor podía hablar de "multiplicidades inconsistentes", con la diferencia esencial de que las limitaciones para hablar de "multiplicidades inconsistentes" eran puramente pragmáticas (no había que decir nada que lleve a contradicciones), mientras que en la teoría de Bernays estaba perfectamente estipulado qué cumplen y qué no cumplen las clases y los conjuntos.

Más aún (con una versión fuerte del axioma de elección) en ella se podía demostrar lo que von Neumann había tomado como axioma de limitación de tamaño, de modo que las clases que no estaban representadas por conjuntos eran justamente las biyectables con la clase V de todos los conjuntos.

53 Gödel y el intuicionismo En **1932** murió Peano a los 73 años, de un ataque al corazón. Ese año Gödel presentó una ponencia en un congreso en Viena, que **1933** sería publicada con el título de *Sobre la teoría de números y la aritmética intuicionista,* en la que comparaba una formalización de la aritmética elemental debida a Jacques Herbrand en el marco de la lógica clásica con una ligera variante de la Aritmética de Heyting, donde los cambios son por simplicidad, pero son intuicionistamente aceptables.

Recordemos que la lógica intuicionista de Heyting se diferencia de la clásica en que restringe los razonamientos válidos para descartar en toda su generalidad el principio del tercio excluso o el de la doble negación. Sin embargo, Gödel considera, para cada fórmula ϕ de la aritmética de Herbrand, una traducción ϕ' al lenguaje de la aritmética de Heyting que consiste en realizar las sustituciones siguientes:

Lógica clásica	Lógica intuicionista
$\neg p$	$\neg p$
$p \to q$	$\neg(p \wedge \neg q)$
$p \vee q$	$\neg(\neg p \wedge \neg q)$
$p \wedge q$	$p \wedge q$

y demuestra que si una fórmula ϕ es demostrable en la aritmética de Herbrand, entonces su traducción ϕ' (que significa lo mismo desde el punto de vista clásico) es demostrable en la de Heyting. Así pues, las restricciones de la lógica intuicionista son mera apariencia. En palabras de Gödel:

> *El teorema* I, *cuya prueba acabamos de completar, muestra que la teoría de números y la aritmética intuicionista sólo aparentemente son más reducidas que las versiones clásicas, y de hecho contienen la teoría de números y la aritmética clásicas, aunque con una interpretación algo distinta de la usual.* [...] *El intuicionismo sólo puede dar lugar a restricciones genuinas en el análisis y la teoría de onjuntos, y esas restricciones no son resultado de negar el* tertium non datur, *sino más bien de la prohibición de los conceptos impredicativos.*

54 El teorema de Tarski En **1933** Tarski publicó un artículo titulado *El concepto de verdad en los lenguajes de las ciencias deductivas,* donde se planteó el problema de la definición del concepto de "verdad". Era un tocho de 145 páginas en polaco con muchas vaguedades filosóficas y poco contenido matemático, y al final le añadió un epílogo (posiblemente influido por su descubrimiento del trabajo de Gödel) en el que se desdecía en parte de lo dicho y enfatizaba lo siguiente (que está traducido al castellano, aunque pueda parecer que sigue en polaco):

> *A′. La semántica de cualquier lenguaje formal puede establecerse como parte de la morfología del lenguaje basándose en definiciones adecuadamente construidas, siempre que el lenguaje en el que se expresa la morfología tenga un orden superior al de la lengua cuya morfología es expresada.*
>
> *B′. Es imposible establecer la semántica de un lenguaje de esta manera si el orden del lenguaje de su morfología es, como máximo, igual al del propio lenguaje.*

Benévolamente, esto puede verse como una forma "filosófica" de expresar el hecho concreto que vamos a tratar a continuación.

Consideremos una teoría axiomática T lo suficientemente potente como para poder formalizarse a sí misma. De acuerdo con el trabajo de Gödel, para eso basta con que pueda definir los números naturales y demostrar los axiomas de Peano. Esto nos permite trabajar con T a los tres niveles que considerábamos en la página 104: el nivel metateórico 0, el nivel teórico 1 y el nivel 2 de la teoría formalizada. Fijemos además un modelo[76] M de los axiomas de T.

Consideremos cualquier fórmula ϕ del lenguaje formal de T, por ejemplo, $\bigwedge x\, x \neq x$, o $2+2=4$, o

$$\bigwedge n \in \mathbb{N} \bigvee pq \in \mathbb{N}(p \text{ es primo} \wedge q \text{ es primo} \wedge 2n+4 = p+q).$$

- En el nivel 0 (la metateoría), tenemos que ϕ es una sucesión de signos del lenguaje formal de $\mathcal{L}$. Podemos decir que ϕ es una "cosa", no una afirmación, como "nadar" es una palabra, no una acción.
- En el nivel 1 (la teoría T), tenemos que ϕ es una afirmación, que expresa una contradicción lógica (si ϕ es el primer ejemplo que hemos puesto, un hecho aritmético elemental (si ϕ es el segundo), un hecho nada elemental (si es el tercero), o cualquier otro hecho, verdadero o falso en M, demostrable o no en T.
- En el nivel 1 tenemos definida también la formalización $\ulcorner\phi\urcorner$ de ϕ, que es un objeto, una cadena de signos de la formalización del lenguaje formal de T. Por ejemplo, si T es ZFC y ϕ es $\bigwedge x\, x \neq x$ (que es lo mismo que $\bigwedge x\, \neg x = x$), de acuerdo con la tabla de la página 103, tenemos que
$$\ulcorner\bigwedge x\, x \neq x\urcorner = (\ulcorner\bigwedge\urcorner, \ulcorner x\urcorner, \ulcorner\neg\urcorner, \ulcorner x\urcorner, \ulcorner=\urcorner, \ulcorner x\urcorner) = (5,9,0,9,7,9).$$
- En el nivel 2, en cambio $\ulcorner\phi\urcorner$ es una afirmación que tiene un significado (el mismo que ϕ).

Así, si a nosotros nos dan el conjunto $(5,9,0,9,7,9)$, sabemos "leerlo" y entendemos que se trata de la fórmula que dice que todo conjunto es distinto de sí mismo. La cuestión es: ¿podemos definir en T lo que es la "lectura" de una fórmula como ésta? Más precisamente: ¿es posible definir una fórmula $V(x)$ de modo que, por ejemplo, $V(5,9,0,9,7,9)$ signifique "todo conjunto es distinto de sí mismo", una fórmula que "lea" los conjuntos que satisfacen la definición de fórmula y nos dé su significado?

Una forma de concretar completamente la pregunta es plantearse si es posible definir una fórmula $V(x)$ del lenguaje formal de T de modo que, para cada fórmula metamatemática ϕ, la fórmula $V(\ulcorner\phi\urcorner)$ sea verdadera en M si y sólo si ϕ es verdadera en M, es decir, si es posible definir una fórmula $V(x)$ que signifique "x es una fórmula verdadera".

[76] Sería el propio Tarski quien años más tarde introduciría el concepto explícito de modelo en una revisión de este trabajo, pero éste ya estaba implícito en este artículo, como lo estaba en muchos otros anteriores de Skolem, Gödel, etc.

Otra versión más fuerte es si existe una fórmula $V(x)$ tal que, para toda fórmula metamatemática ϕ, en T se pueda demostrar

$$V(\ulcorner\phi\urcorner) \leftrightarrow \phi.$$

Si esto se puede demostrar en T, entonces la equivalencia será verdadera en M y tendremos, en efecto, que un miembro es verdadero en M si y sólo si lo es el otro, pero en principio no pedimos que la equivalencia tenga que demostrarse en M. Y mucho menos estamos pidiendo que se pueda determinar si una fórmula dada es verdadera en M o no. Por ejemplo, si ϕ es

$$\bigwedge n \in \mathbb{N} \bigvee pq \in \mathbb{N}(p \text{ es primo} \wedge q \text{ es primo} \wedge 2n + 4 = p + q),$$

lo único que se le exige a la fórmula $V(x)$ es que $V(\ulcorner\phi\urcorner)$ sea verdadera en M si y sólo si en M se cumple que todo número par mayor que dos es suma de dos primos, pero sin necesidad de que sepamos concluir (ni mucho menos demostrar en T) si eso es cierto o no. El caso es que la respuesta es negativa:

> **Teorema de Tarski de indefinibilidad de la verdad** Si T es una teoría aritmética y M es un modelo de T, no existe ninguna fórmula metamatemática $V(x)$ del lenguaje formal de T tal que, para toda fórmula metamatemática ϕ, la fórmula $V(\ulcorner\phi\urcorner)$ sea verdadera en M si y sólo si lo es ϕ.

En otras palabras, si formalizamos el lenguaje formal de T, de modo que en T podemos llamar "fórmulas" a determinados objetos, no hay forma de asignar en T a cada uno de esos objetos-fórmula su significado pretendido.

DEMOSTRACIÓN: Supongamos que existe la fórmula $V(x)$. Por el lema de autorreferencia de Gödel (véase la página 106), existe una fórmula ψ del lenguaje formal de T tal que en T se puede demostrar $\psi \leftrightarrow \neg V(\ulcorner\psi\urcorner)$.

Pero entonces esta equivalencia tiene que ser verdadera en M, luego tendremos que ψ es verdadera en M si y sólo si lo es $\neg V(\ulcorner\psi\urcorner)$, si y sólo si $V(\ulcorner\psi\urcorner)$ es falsa en M, si y sólo si ψ es falsa en M. Esta contradicción prueba que $V(x)$ no puede existir. ∎

En resumen: el lema de autorreferencia implica que si pudiéramos definir una fórmula $V(x)$ que significara "x es una fórmula verdadera", podríamos construir una fórmula ψ que significara "yo soy falsa" (o "mi formalización es falsa"), y eso da lugar a una contradicción.

El teorema de Tarski se llama así porque Tarski fue el primero en publicar algo que sonaba a lo mismo, pero lo cierto es que Gödel ya se lo había comunicado (en términos serios) a von Neumann en la correspondencia que mantuvieron ambos antes de la publicación de su artículo sobre los teoremas de incompletitud.

La indefinibilidad de la verdad está relacionada con la indefinibilidad de la definibilidad, que hace que la paradoja de Berry no sea demostrable en los sistemas aritméticos. Decir que un número natural n es definible en una teoría T significa que existe una fórmula $\phi(x)$ (de nivel 1, es decir, un objeto que cumple la definición de fórmula) tal que n es el único número natural que la hace verdadera, pero, como no podemos definir "que la hace verdadera", tampoco podemos definir "n es definible".

En 1933 Gödel viajó a los Estados Unidos, y en **1934** impartió un seminario en el Instituto de Estudios Avanzados de Princeton, donde explicó sus teoremas trabajando con teorías aritméticas "al estilo de Hilbert" en lugar de con la lógica de los *Principia Mathematica,* explicó la extensión del concepto de función recursiva y comentó de pasada el teorema de Tarski sin conocer la publicación de Tarski, pues sólo estaba disponible en polaco y pocos habían oído hablar de ella.

En particular, Gödel señaló la relación con su demostración del teorema de Tarski y la conocida paradoja de Epiménides. En su formulación clásica, Epiménides era un cretense que afirmó que todos los cretenses eran unos mentirosos. Si entendemos que uno es "mentiroso" cuando siempre miente (sin excepciones), el hecho de que Epiménides era cretense resultaba paradójico, aunque Gödel reformuló la paradoja en términos menos sutiles:

> *Supóngase que el 4 de mayo de 1934 X hace una única afirmación: "Cualquier afirmación que X haga el 4 de mayo de 1934 es falsa". Claramente esta afirmación no puede ser verdadera. Tampoco puede ser falsa, pues el único modo de que sea falsa es que X haya hecho una afirmación verdadera en el tiempo especificado, y en ese tiempo sólo hizo la afirmación citada.*

Pero lo que en estos términos es poco más que un "juego de palabras", en la demostración del Teorema de Tarski no hay ninguna ambigüedad ni nada cuestionable. Las fórmulas de un lenguaje formal son las que son, nos preguntamos si hay una que tenga una determinada propiedad, y vemos que no puede haberla.

55 Descripciones Hilbert no se había pronunciado sobre los teoremas de incompletitud y su impacto en su programa de fundamentación de las matemáticas. Sin embargo, en **1934** se publicó el primer volumen de *Los fundamentos de las matemáticas,* de Hilbert y Bernays, que ocupaba casi 500 páginas y comenzaba con esta breve introducción firmada por Hilbert:

> *Los principios rectores de mis investigaciones sobre los fundamentos de las matemáticas, que retomé en conversaciones con P. Bernays en 1917 basándome en enfoques anteriores, los he presentado con detalle en diversos lugares.*
>
> *A estas investigaciones, en las que también participó W. Ackermann, se han sumado desde entonces diversos matemáticos.*
>
> *La primera parte de este curso, escrita por Bernays y aún en desarrollo, tiene como objetivo presentar la teoría según sus resultados actuales.*
>
> *Este estado de resultados señala simultáneamente el camino para futuras investigaciones en teoría de la demostración hacia el objetivo final de reconocer la consistencia de todos nuestros métodos matemáticos habituales.*
>
> *Con respecto a este objetivo, quisiera enfatizar que la opinión emergente de que ciertos resultados recientes de Gödel implicaban la impracticabilidad de mi teoría de la demostración ha resultado ser errónea. De hecho, este resultado sólo demuestra que, para las demostraciones de consistencia más avanzadas, el punto de vista finito debe utilizarse con mayor precisión de la necesaria al considerar los formalismos elementales.*

En el prefacio, firmado por Bernays, se lee:

> *La implementación de este proyecto ha visto significativamente retrasada debido a que, cuando la presentación estaba a punto de finalizar, la publicación de las obras de Herbrand y Gödel provocó un cambio en el campo de la teoría de la demostración, lo que obligó a considerar nuevas perspectivas. Como resultado, el volumen del libro aumentó, por lo que una división en dos volúmenes pareció apropiada.*

Esta primera parte constaba de ocho capítulos. En el primero de ellos, de carácter introductorio, se explicaba el método axiomático tomando como ejemplo los *Grundlagen der Geometrie,* y se exponía de nuevo el programa finitista: cualquier teoría matemática que hable de conjuntos infinitos requiere una prueba de consistencia, y ésta no puede lograrse mostrando objetos que cumplan los axiomas, sino que es necesaria una prueba basada en la teoría de la demostración, un razonamiento finitista que justifique que a partir de los axiomas no es posible llegar a una contradicción.

En el segundo capítulo se explica lo que hay que entender por *razonamiento sustantivo elemental* (que también podríamos traducir como *razonamiento material elemental*), que no es sino el razonamiento finitista intuitivo, y se ilustra justificando puntillosamente los hechos básicos de la aritmética, para luego explicar que en matemáticas se emplean habitualmente técnicas de razonamiento que exceden con creces las posibilidades de este razonamiento material, y por ello se vuelve a la necesidad de una prueba finitista de la consistencia de estos métodos. Los capítulos siguientes son una exposición exhaustiva y minuciosa de la teoría de la demostración, aunque no contienen nada esencialmente novedoso.

Destacaremos únicamente el último capítulo, titulado *El concepto de 'el que' y su eliminabilidad,* en el que aborda un problema que ya había sido analizado en los *Principia Mathematica,* pero desde un punto de vista ligeramente distinto.

Se trata de las referencias a objetos a través de propiedades que los caracterizan, como "el padre de Beethoven" o "el mínimo común múltiplo de 12 y 18".

En su *Formulario de matemáticas,* Peano usaba la letra griega iota (la inicial de *ίσος*, igual) para indicar que ιx era el conjunto formado por los objetos iguales a x, es decir, el conjunto $\{x\}$, y usaba una iota invertida $\turnediota$ como una especie de operador inverso: si una propiedad P la cumple un único objeto —con lo que define un conjunto de la forma $\{x\}$— entonces $\turnediota P$ representaba el único objeto de dicha clase, es decir, el único objeto que cumple la propiedad P.

En los *Principia,* la letra ι se usa en un sentido completamente distinto, para nombrar el tipo de objetos llamados "individuos" (los objetos que no son conjuntos), pero se mantiene la iota invertida para nombrar "descripciones". Una descripción es una expresión de la forma $(\turnediota x)\,\phi(x)$, donde $\phi(x)$ es una fórmula, y representa "el único x que cumple $\phi(x)$".

A Hilbert no le gustaban estos giros y, del mismo modo que escribía Ex en lugar del $\exists x$ de Russell para indicar "existe", usó una iota al derecho: $\iota x\,\phi(x)$ para representar descripciones. Desde entonces distintos autores han representado las descripciones con iotas al derecho o al revés, según gustos. Puesto que esta iota ya no guarda ninguna relación con el *ίσος* de Peano, nosotros usaremos la notación $x|\phi(x)$ y leeremos "el (único) x tal que $\phi(x)$".

Esto supone añadir el *descriptor* $|$ a la lista de signos lógicos, junto con $\to, \wedge, \vee$, etc. Notemos que el descriptor liga la variable que le antecede, igual que lo hacen los cuantificadores.

El problema que plantean las descripciones es cómo interpretarlas cuando no hay un único objeto que cumple la propiedad considerada. Es famoso el ejemplo que puso Russell para ilustrar este caso:

El actual rey de Francia es calvo.

¿Esta afirmación es verdadera o falsa? Es evidente que, más que una respuesta, lo que esta pregunta requiere es un convenio.

- Russell adoptó el convenio más natural desde un punto de vista filosófico: cuando decimos que el actual rey de Francia es calvo, estamos dando por hecho que existe un único rey de Francia. Como esto no es cierto, la afirmación es falsa.

  Sin embargo, lo más natural desde un punto de vista filosófico no suele ser lo más conveniente desde un punto de vista matemático. Este convenio tiene dos inconvenientes. El primero es que no atribuye ningún significado en concreto a la expresión "el actual rey de Francia", y el segundo es que uno querría que identidades lógicas como $x = y \to y = x$ fueran siempre verdaderas, pero si sustituimos x e y por "el actual rey de Francia" y "el padre de próximo rey de Francia", (o por $\lim\limits_n (-1)^n$ y $\lim\limits_n (-1)^{n+1}$) respectivamente, obtenemos una afirmación falsa.

- Hilbert, en cambio, adoptó el convenio más natural según las costumbres de los matemáticos: no es aceptable escribir $x|\phi(x)$ si previamente no se ha demostrado que existe un único x que cumple $\phi(x)$. Con este convenio, "el actual rey de Francia es calvo" no es una afirmación verdadera ni falsa, porque no es una afirmación.

  Pero lo más natural según las costumbres de los matemáticos no es necesariamente lo más conveniente desde un punto de vista lógico. El inconveniente de este criterio es que la definición de fórmula deja de ser trivial: así no podemos saber si una cadena de signos es o no una fórmula sin más que analizar su estructura. Una cadena de signos puede ser una fórmula si aceptamos unos axiomas y no serlo si aceptamos otros. Es lo que le sucede, por ejemplo a $n|(n \in \mathbb{N} \wedge 2^{\aleph_0} = \aleph_n) < 20$.

- Un convenio más moderno (aunque próximo a lo que pensaba Frege al respecto) que evita todos estos inconvenientes[77] consiste en estipular que una descripción $x|\phi(x)$ nombra al único objeto que cumple $\phi(x)$ si es que existe tal objeto (y entonces se dice que la descripción es propia), o bien a un objeto predeterminado si no existe tal único objeto (y entonces se dice que la descripción es impropia). El objeto designado arbitrariamente como significado de las descripciones impropias puede ser aludido siempre mediante la descripción $x|x = x$. En efecto, en un modelo en el que no exista un único objeto, se cumple que la descripción $x|x = x$ es impropia (porque no hay un único objeto que cumpla $x = x$), por lo que se interpreta como el objeto designado como significado de las descripciones impropias, mientras que en un modelo en el que sólo haya un objeto, la descripción es propia, pero, precisamente porque no hay más que un objeto, su significado deberá coincidir con el objeto asignado a las descripciones impropias.

  Esto hace que, en general, no sea necesario especificar un objeto concreto como significado para las descripciones impropias, pero nada impide elegir uno. Así, por ejemplo, en la teoría de conjuntos podemos adoptar como axioma "semilógico" la fórmula $\bigwedge u\, u \notin x|x = x$, que especifica que todas las descripciones impropias nombran, por definición, al conjunto vacío. Esto hace que, por ejemplo, la fórmula

  $$\lim_n (-1)^n = \lim_n (-1)^{n+1}$$

  sea un teorema, ya que ambos miembros son $\varnothing$, donde entendemos que

  $$\lim_n x_n = x|\{x_n\}_n \to x,$$

  es decir, que el límite de una sucesión es "el x al cual converge la sucesión", con lo que es igual a $\varnothing$ cuando la sucesión no tiene límite.

[77] Propuesto por Richard Montague y Donald Kalish en su artículo de 1957 *Notas sobre descripciones y deducción natural.*

Fijado un tratamiento para las descripciones impropias, el descriptor resulta ser la forma más práctica de concebir las definiciones matemáticas. Por ejemplo, en la teoría de conjuntos se demuestra que, dados dos conjuntos x, y, existe un único conjunto cuyos elementos son los elementos comunes a ambos, y eso justifica que demos a dicho conjunto el nombre de $x \cap y$, ¿qué es concretamente $x \cap y$? La pregunta hay que entenderla a nivel metamatemático (pues a nivel matemático la respuesta es que $x \cap y$ es la intersección de x e y). Estamos preguntando cuál es la definición de $x \cap y$ en términos del lenguaje de la teoría de conjuntos.

- Si admitimos el descriptor como un signo lógico, la respuesta es muy simple: $x \cap y$ es, por definición, lo mismo que

$$z \mid \bigwedge u(u \in z \leftrightarrow u \in x \wedge u \in y).$$

En cualquier fórmula en la que aparezca $x \cap y$, podemos eliminar esta expresión sustituyéndola por la definición precedente.

Si no incluimos al descriptor entre los signos lógicos, todavía tenemos dos opciones:

- Podemos considerar que, al definir la intersección, estamos añadiendo un nuevo signo $\cap$ al lenguaje de la teoría de conjuntos, lo que requiere dejar claro que sólo es lícito añadir nuevos signos cuando éstos puedan ser definidos en términos de conceptos precedentes, como ocurre con la intersección.

- Y otra opción es considerar que $x \cap y$ no es nada, que lo que definimos realmente al definir la intersección es la fórmula $z = x \cap y$, que es, por definición,

$$\bigwedge u(u \in z \leftrightarrow u \in x \wedge u \in y).$$

Los dos últimos convenios requieren justificar que los signos definidos pueden eliminarse. Por ejemplo, si tenemos esta fórmula:

$$\bigwedge xy(x \in A \wedge y \in A \to x \cap y \in A)$$

y queremos eliminar la intersección, lo primero que tenemos que hacer es añadir una variable:

$$\bigwedge xy \bigvee z(z = x \cap y \wedge (x \in A \wedge y \in A \to z \in A))$$

y ahora ya se puede eliminar $z = x \cap y$ por su definición, con lo que llegamos a una fórmula equivalente a la dada en la que no hay signos definidos.

No obstante, el hecho de que con el descriptor no necesitemos demostrar nada sobre eliminación de signos definidos, pues siempre podemos sustituir los signos definidos por sus definiciones (como al cambiar $x \cap y$ por su definición $z \mid \bigwedge u(u \in z \leftrightarrow u \in x \wedge u \in y)$), lo cierto es que es posible (y muy conveniente) demostrar que toda fórmula con descriptores es equivalente[78] a otra que no tenga descriptores, y ése es el resultado principal del capítulo octavo del tratado de Hilbert y Bernays.

De este modo, el descriptor es la forma más cómoda de concebir en la práctica las definiciones matemáticas, y en teoría siempre podemos suponer que una fórmula matemática (o una demostración matemática) no contiene descriptores, lo cual es imprescindible en muchos argumentos metamatemáticos.

56 Deducción natural Hitler había llegado al poder en Alemania en 1933, e inmediatamente había iniciado una purga de judíos en las instituciones públicas. Hacía ya cuatro años que Abraham Fraenkel —viendo el auge del nazismo— se había trasladado a la Universidad Hebrea de Jerusalén. Von Neumann era ascendencia judía, aunque se declaraba agnóstico y en 1930 se había convertido al catolicismo. Ese año había marchado a los Estados Unidos para lo que iba a ser una estancia temporal, pero ya no regresó a Alemania. En 1932 Einstein siguió sus pasos. En 1933 Paul Bernays fue expulsado de la Universidad de Gotinga por ser "no ario". Durante seis meses trabajó contratado por Hilbert, hasta que se marchó a Suiza con su familia, desde donde seguiría colaborando con Hilbert. Emmy Noether había sido expulsada de la universidad al mismo tiempo por el mismo motivo, y ese mismo año se marchó a los Estados Unidos, aunque moriría en 1935, de un cáncer de mama.

[78] Si adoptamos el convenio de asignar un significado arbitrario a las descripciones impropias, es necesario suponer que el objeto asignado a ellas admite una caracterización sin descriptores, como le ocurre al conjunto vacío, que es el único conjunto x que cumple $\bigwedge u\, u \notin x$. Esta restricción es irrelevante en la práctica.

Bernays estaba entonces dirigiendo la tesis a un joven de 24 años llamado Gerhard Karl Erich Gentzen, por lo que, aunque éste siguió trabajando con Bernays, oficialmente su director de tesis pasó a ser Hermann Weyl, que ocupaba entonces la cátedra que Hilbert había dejado vacante al jubilarse.

Gentzen leyó su tesis ese mismo año, con el título de *Investigaciones sobre el razonamiento lógico.* No tardó en alistarse en las *Sturmabteilung,* la milicia de los "camisas pardas" vinculada al Partido Nacionalsocialista Obrero Alemán, pero a la vez siguió manteniendo correspondencia con Bernays y con Fraenkel, lo que le valió los recelos de las autoridades nazis. Weyl no era judío, pero su mujer sí, por lo que terminó emigrando también a los Estados Unidos, y su cátedra fue ocupada por Helmut Hasse, que no se llevaba mal con los nazis.[79]

Gentzen publicó los resultados de sus tesis en dos artículos con el mismo título en **1934** y **1935**. Ese año empezó a trabajar como ayudante de Hilbert en Gotinga. (Por su parte, Zermelo, a sus 64 años, renunció ese año a su cátedra, como expresión de su rechazo al nazismo.)

Gentzen se había propuesto desarrollar lo que llamó un *sistema de deducción natural,* es decir, un cálculo deductivo que fuera lo más similar posible al modo en que razonan los matemáticos en la práctica. Una deducción "al estilo de Hilbert" consistía en una sucesión de fórmulas que partían de las premisas de la deducción y de axiomas lógicos, y en los que cada nueva fórmula se obtenía de las anteriores por aplicación de unas pocas reglas de inferencia (a menudo una sola: el *modus ponens*). Los axiomas lógicos eran, sin duda, verdades lógicas, pero artificiosas, de modo que un matemático podía tener bien claro que, por ejemplo

$$(\alpha \vee (\beta \wedge \gamma)) \to (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$$

e incluso sabría razonárselo a cualquiera que lo cuestionara y, al mismo tiempo, no saber cómo deducirlo en el cálculo deductivo de Hilbert, porque ello requiere elegir los axiomas adecuados y la estrategia que hay que seguir para llegar a la conclusión deseada, y eso no es trivial en absoluto. Es como si tenemos una herramienta para hacer algo y sabemos exactamente qué queremos hacer y que nuestra herramienta basta para hacerlo, pero todavía nos falta aprender cómo funciona la herramienta.[80]

En su lugar, Gentzen propuso un cálculo deductivo que llamó NK (la N de natural y la K de (*klassische,* clásico) que era equivalente al de Hilbert, en cuanto que permitían demostrar exactamente lo mismo, pero que carecía de axiomas y, en su lugar, tenía unas reglas de inferencia que no sólo eran evidentes, sino que también era evidente cómo y cuándo había que usar cada una (al menos, si uno tiene claro el razonamiento que quiere formalizar).

Más aún, Gentzen notó que si al sistema NK se le eliminaba una única regla, precisamente la que expresa la ley de la doble negación, se obtenía un sistema que llamó NJ y que equivale al sistema de Heyting para la lógica intuicionista (por algún motivo desconocido, Gentzen eligió la J para hacer referencia al Intuicionismo).

Vamos a describir estos sistemas. En primer lugar, mientras las deducciones "a la Hilbert" son sucesiones finitas de fórmulas, Gentzen define sus deducciones como estructuras de fórmulas en forma de árbol, de modo que cada fórmula tiene inmediatamente por encima la premisa o las premisas de las cuales se deduce por una regla de inferencia. Por ejemplo, la fórmula que hemos puesto antes como ejemplo, se puede deducir en el sistema NJ mediante este árbol de fórmulas (que el propio Gentzen usa como ilustración):

$$\dfrac{\alpha \vee (\beta \wedge \gamma) \qquad \dfrac{\dfrac{\dfrac{\alpha}{\alpha \vee \beta} \qquad \dfrac{\alpha}{\alpha \vee \gamma}}{(\alpha \vee \beta) \wedge (\alpha \vee \gamma)} \qquad \dfrac{\dfrac{\dfrac{\beta \wedge \gamma}{\beta}}{\alpha \vee \beta} \qquad \dfrac{\dfrac{\beta \wedge \gamma}{\gamma}}{\alpha \vee \gamma}}{(\alpha \vee \beta) \wedge (\alpha \vee \gamma)}}{(\alpha \vee \beta) \wedge (\alpha \vee \gamma)}}{(\alpha \vee (\beta \wedge \gamma)) \to (\alpha \vee \beta) \wedge (\alpha \vee \gamma)}$$

Para entender la deducción (y apreciar su naturalidad), vamos a presentar las reglas de inferencia del sistema NJ. En total son 12, pero mostramos aquí únicamente 8 de ellas:

[79] No obstante, en 1937 solicitaría el ingreso en el partido nazi, pero le fue denegado porque le encontraron antepasados judíos.

[80] Cabe incidir en que esto no es exactamente un defecto de los cálculos deductivos "a la Hilbert", sino que esta reducción de la lógica a unos axiomas técnicos y unas pocas reglas de inferencia resulta en muchas ocasiones mucho más adecuado a efectos teóricos que otras alternativas más naturales, pues reducen los razonamientos sobre deducciones posibles a unas pocas comprobaciones rutinarias.

$$\frac{\alpha \quad \beta}{\alpha \wedge \beta}\, I- \wedge \qquad \frac{\alpha \wedge \beta}{\alpha}\quad \frac{\alpha \wedge \beta}{\beta}\, E- \wedge \qquad \frac{\alpha}{\alpha \vee \beta}\quad \frac{\beta}{\alpha \vee \beta}\, I- \vee \qquad \frac{\alpha \vee \beta \quad \begin{matrix}[\alpha]\\ \gamma\end{matrix} \quad \begin{matrix}[\beta]\\ \gamma\end{matrix}}{\gamma}\, E- \vee$$

$$\frac{\begin{matrix}[\alpha]\\ \beta\end{matrix}}{\alpha \to \beta}\, I- \to \qquad \frac{\alpha \quad \alpha \to \beta}{\beta}\, E- \to \qquad \frac{\begin{matrix}[\alpha]\\ \beta \wedge \neg\beta\end{matrix}}{\neg\alpha}\, I- \neg \qquad \frac{\alpha \quad \neg\alpha}{\beta}\, E- \neg$$

1. La primera regla es la *introducción del conjuntor,* que establece que si hemos deducido α y también β, de ahí podemos deducir $\alpha \wedge \beta$. En el ejemplo anterior se ha usado dos veces, al pasar del cuarto nivel del árbol (contando desde abajo) al tercero.

2. La segunda regla es la *eliminación del conjuntor,* que establece que de $\alpha \wedge \beta$ podemos deducir α y también β. En el ejemplo la hemos usado dos veces, en lo más alto del árbol.

3. La tercera regla es la *introducción del disyuntor,* que establece que si hemos deducido α o β, de ahí podemos deducir $\alpha \vee \beta$. En el ejemplo la hemos usado cuatro veces, al pasar del quinto al cuarto nivel.

4. La cuarta es la *eliminación del disyuntor,* que establece que si, suponiendo α hemos llegado a γ y suponiendo β, también, entonces a partir de $\alpha \vee \beta$ podemos concluir γ. Y, a partir de este punto, α y β ya no son hipótesis de la deducción, es decir, las fórmulas que aparezcan debajo de $\alpha \vee \beta$ serán válidas sin suponer que α y β lo son.

   En el ejemplo la hemos usado al pasar del tercer nivel al segundo: suponiendo α hemos llegado a la fórmula $(\alpha \vee \beta) \wedge (\alpha \vee \gamma)$ y suponiendo $\beta \wedge \gamma$ hemos llegado a la misma conclusión, luego suponiendo $\alpha \vee (\beta \wedge \gamma)$ tenemos esta misma conclusión, y a partir de aquí entendemos que esta conclusión no tiene más premisa que $\alpha \vee (\beta \wedge \gamma)$.

5. La quinta es la *introducción del implicador,* que afirma que si suponiendo α llegamos a deducir β, entonces podemos concluir que $\alpha \to \beta$ y a partir de ahí α deja de ser una premisa, es decir, que $\alpha \to \beta$ es válida sin necesidad de esa premisa.

   En el ejemplo es el paso final. Teníamos deducido $(\alpha \vee \beta) \wedge (\alpha \vee \gamma)$ bajo la única hipótesis $\alpha \vee (\beta \wedge \gamma)$ y llegamos a que la conclusión es válida sin hipótesis alguna.

6. La sexta es la *introducción del negador,* que no es sino el razonamiento por reducción al absurdo: si suponiendo α podemos llegar a una contradicción, de ahí se deduce $\neg\alpha$.

7. La séptima es la *eliminación del negador,* que establece que de una contrdicción se puede deducir cualquier cosa.

Las cuatro reglas que hemos omitido son la introducción y la eliminación del generalizador y del particularizador, y son igual de evidentes que las demás.[81] Gentzen no da reglas para el coimplicador $\leftrightarrow$, por lo que hay que considerar que una fórmula de tipo $\alpha \leftrightarrow \beta$ es una mera abreviatura de $(\alpha \to \beta) \wedge (\beta \to \alpha)$, por lo que una notación puede sustituirse en cualquier momento por la otra, pues son nombres distintos de la misma fórmula.

Señalemos únicamente que Gentzen usa $\exists x$ como particularizador, es decir, para expresar "existe un x". Se trata de la notación de Peano, que representa una E (de "existe") girada 180°. Ésta había sido adoptada también por Whitehead y Russell, mientras que Hilbert usaba una E. (Existe empieza por E tanto en castellano, como en italiano, como en inglés, como en alemán). Para el generalizador ("para todo"), tanto Whitehead y Russell como Hilbert usaban la notación (x) de Peano, pero Gentzen consideró que era preferible emplear un signo "más visible", para que fuera patente cómo sus reglas lo introducían y lo eliminaban, y para ello giró la letra A de *Alle* (todo) e inventó el signo $\forall$, que ahora es el más usado para representar el generalizador.

El propio Gentzen señalaba que expresar las demostraciones como árboles parecía ir en contra de su propósito declarado de definir un cálculo deductivo lo más próximo posible al modo usual de razonar de los matemáticos,

[81] El enunciado que hemos dado de las reglas $I- \neg$ y $E- \neg$ no coincide exactamente con el que formuló Gentzen, porque él empleaba el signo $\bot$ para representar una contradicción y aquí lo hemos omitido.

pues es un hecho que los matemáticos expresan sus razonamientos mediante sucesiones de afirmaciones, y no en forma de árbol. Frente a ello sólo indica que así resulta más conveniente y que no es esencial. Acudiendo en su defensa, podemos añadir que, aunque los matemáticos escriban sus razonamientos de forma sucesiva, a menudo hacen referencia en un punto a un fragmento demostrado anteriormente, y lo que hace la estructura de árbol es explicitar la conexión entre los distintos fragmentos de una demostración matemática usual, y esto resulta tener un gran valor teórico.

Observemos que el árbol del ejemplo precedente se puede obtener mecánicamente, incluso sin tener *a priori* un argumento que justifique la validez de la conclusión. Basta razonar de abajo hacia arriba: queremos que la última línea del árbol sea la que queremos probar y, como es una implicación, podemos pensar en obtenerla con la regla de la introducción del implicador. Ello nos permite escribir:

$$\dfrac{\dfrac{\alpha \vee (\beta \wedge \gamma)}{(\alpha \vee \beta) \wedge (\alpha \vee \gamma)}}{(\alpha \vee (\beta \wedge \gamma) \to (\alpha \vee \beta) \wedge (\alpha \vee \gamma)}$$

pero como la premisa es una disyunción, la forma más simple de llegar a la conclusión es mediante la regla de eliminación del disyuntor, lo que nos permite completar el tercer nivel del árbol, pues ésta exige tener al mismo nivel dos demostraciones de $(\alpha \vee \beta) \wedge (\alpha \vee \gamma)$, una bajo la premisa α y bajo la premisa $\beta \wedge \gamma$. A su vez, como se trata de una conjunción, la forma más simple de llegar a ella es mediante la regla de introducción del conjuntor, lo que nos permite completar el cuarto nivel del árbol. A su vez, pare deducir las disyunciones a partir de α, lo más simple es aplicar la regla de introducción del disyuntor con premisa α, y para deducirlas con premisa $\beta \wedge \gamma$, lo más simple es aplicar las reglas de introducción del disyuntor con premisas β y γ, con lo que completamos el quinto nivel del árbol. Por último, para deducir β y γ con premisa $\beta \wedge \gamma$ basta usar la regla de eliminación del conjuntor.

No todos los razonamientos lógicos son tan mecánicos como éste, pero este ejemplo sirve para ilustrar cómo el sistema de Gentzen ayuda a mecanizar el razonamiento lógico, de modo que sólo es necesario concentrarse en encontrar una estrategia general de razonamiento, y los detalles se completan de forma rutinaria.

Para obtener el sistema deductivo NK para la lógica clásica basta con añadir la regla de inferencia de la doble negación:

$$\dfrac{\neg\neg\alpha}{\alpha}$$

o, alternativamente, tomar como axiomas lógicos todos los casos del tercio excluso: $\alpha \vee \neg\alpha$, de modo que en cualquier deducción se puede partir de una fórmula de este tipo sin que cuente como premisa.

Señalemos, por último, que Gentzen está considerando lenguajes formales sin igualador. Para demostrar identidades lógicas que dependan de las propiedades del igualador, como $x = y \to y = x$, es necesario añadir axiomas que recojan las propiedades básicas del igualador, cosa de la que no se ocupa Gentzen en los artículos que estamos comentando.

57 El cálculo secuencial Una vez expuestos los sistemas NJ y NK, Gentzen pasa a presentar otros dos nuevos sistemas equivalentes, a los que llama LJ y LK, donde la L es de *logístico,* término con el que Gentzen se refería a los sistemas lógicos "a la Hilbert" habituales en la época, caracterizados por que en las deducciones no se establecían hipótesis provisionales, y cada fórmula de una deducción lógica era lógicamente válida, verdadera en sí misma, sin estar condicionada a premisas establecidas en líneas previas de la deducción. En palabras de Gentzen:

> *Lo que queremos hacer es formular un cálculo deductivo (para la lógica de predicados) que sea, por un lado, "logístico", es decir, en el que las derivaciones no contengan hipótesis, como en el cálculo* NJ*, pero que, por otro lado, tome del cálculo* NJ *la división de las formas de inferencia en introducciones y eliminaciones de los diversos signos lógicos.*
>
> *El método más obvio para convertir una derivación* NJ *en una logística es el siguiente: reemplazamos una fórmula β, que depende de las hipótesis $\alpha_1, \ldots, \alpha_n$ por la nueva fórmula $\alpha_1 \wedge \cdots \wedge \alpha_n \to \beta$. Hacemos esto con todas las fórmulas.*
>
> *Así obtenemos fórmulas que ya son verdaderas en sí mismas, es decir, cuya verdad ya no está condicionada a la verdad de ciertas hipótesis. Este procedimiento, sin embargo, introduce nuevos signos lógicos $\wedge$ y $\to$, lo que requiere reglas de inferencia adicionales para $\wedge$ y $\to$, y, por lo tanto, altera el carácter sistemático de nuestro método de introducción y eliminación de signos.*

Por esta razón, hemos introducido el concepto de secuente. *En lugar de una fórmula*

$$\alpha_1 \wedge \cdots \wedge \alpha_n \to \beta,$$

por ejemplo, escribimos el secuente

$$\alpha_1, \ldots, \alpha_n \Rightarrow \beta.$$

El significado informal de este secuente no difiere del de la fórmula anterior; las expresiones difieren meramente en su estructura formal.

Aun así, se requieren nuevas figuras de inferencia que no pueden integrarse en nuestro sistema de introducciones y eliminaciones; pero tenemos la ventaja de poder reservarles lugares especiales dentro de nuestro sistema, ya que ya no se refieren a signos lógicos, sino meramente a la estructura de los secuentes. Por lo tanto, a estas las llamamos "reglas de inferencia estructurales", y a las otras "reglas de inferencia operacionales".

En el cálculo clásico NK, *la ley del tercio excluso ocupaba un lugar especial entre las formas de inferencia porque no podía integrarse en nuestro sistema de introducciones y eliminaciones. En el cálculo logístico clásico* LK, *que enseguida presentaremos, esta característica se elimina.*

Esto es posible gracias a la admisión de secuentes con varias fórmulas en el consecuente (la parte derecha del secuente), mientras que la transición desde el cálculo NJ *que acabamos de describir sólo conducía a secuentes con una única fórmula en el consecuente. La simetría así obtenida es más adecuada para la lógica clásica. Por otro lado, la restricción de tener a lo sumo una fórmula en el consecuente se mantendrá para el cálculo intuicionista* LJ.

En resumen, Gentzen se había dado cuenta que las ventajas de la formulación de los sistemas NJ y NK, en las que cada signo lógico tenía una regla de introducción y otra de eliminación, se multiplicaban espectacularmente si las reglas de inferencia se reformulaban, no en términos de fórmulas, sino de secuentes, donde un *secuente* es una expresión de la forma

$$\gamma_1, \ldots, \gamma_m \Rightarrow \delta_1, \ldots, \delta_n,$$

cuya interpretación es la misma que la de la fórmula

$$\gamma_1 \wedge \cdots \wedge \gamma_m \to \delta_1 \vee \cdots \vee \delta_n,$$

es decir, que si se cumplen todas las fórmulas del *antecedente* $\gamma_1, \ldots, \gamma_m$ del secuente, entonces se cumple alguna de las fórmulas del *consecuente* $\delta_1, \ldots, \delta_n$ del secuente. Esto equivale también a la fórmula

$$\neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n,$$

pero esta expresión tiene la ventaja de que tiene sentido incluso si el antecedente o el consecuente es vacío. Así, un secuente de la forma

$$\Rightarrow \delta_1, \ldots, \delta_n$$

se interpreta como $\delta_1 \vee \cdots \vee \delta_n$, es decir, como que se cumple alguna de las fórmulas dadas, mientras que un secuente de la forma

$$\gamma_1, \ldots, \gamma_m \Rightarrow$$

se interpreta como

$$\neg\gamma_1 \vee \cdots \vee \neg\gamma_m,$$

es decir, como que no se cumple alguna de las fórmulas dadas. Finalmente, también se admite como secuente el *secuente vacío* $\Rightarrow$, que se considera siempre falso.

Los cálculos LJ y LK tienen ahora los mismos axiomas y las mismas reglas de inferencia, y sólo se diferencian en que las deducciones en LJ constan únicamente de secuentes con a lo sumo una fórmula en el consecuente, mientras que las de LK pueden tener secuentes con cualquier cantidad finita de fórmulas en el consecuente.

Los axiomas lógicos son los secuentes de la forma $\alpha \Rightarrow \alpha$, y las reglas de inferencia son las siguientes:

$$\textbf{Debilitación izquierda}\ \frac{\Gamma \Rightarrow \Delta}{\alpha, \Gamma \Rightarrow \Delta}, \quad \textbf{Debilitación derecha}\ \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \alpha},$$

$$\textbf{Corte}\ \ \frac{\Gamma \Rightarrow \Delta, \alpha \qquad \alpha, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta},$$

$$\begin{array}{c|ll}
\neg & \dfrac{\Gamma \Rightarrow \Delta, \alpha}{\neg\alpha, \Gamma \Rightarrow \Delta}, & \dfrac{\alpha, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\alpha}, \\[2ex]
\vee & \dfrac{\alpha,\ \Gamma \Rightarrow \Delta \qquad \beta,\ \Gamma \Rightarrow \Delta}{\alpha \vee \beta,\ \Gamma \Rightarrow \Delta}, & \dfrac{\Gamma \Rightarrow \Delta,\ \alpha\ [\text{o } \beta]}{\Gamma \Rightarrow \Delta,\ \alpha \vee \beta}, \\[2ex]
\wedge & \dfrac{\alpha\ [\text{o } \beta],\ \Gamma \Rightarrow \Delta}{\alpha \wedge \beta,\ \Gamma \Rightarrow \Delta}, & \dfrac{\Gamma \Rightarrow \Delta,\ \alpha \quad \Gamma \Rightarrow \Delta,\ \beta}{\Gamma \Rightarrow \Delta, \alpha \wedge \beta}, \\[2ex]
\rightarrow & \dfrac{\Gamma \Rightarrow \Delta, \alpha \qquad \beta, \Gamma \Rightarrow \Delta}{\alpha \rightarrow \beta,\ \Gamma \Rightarrow \Delta}, & \dfrac{\alpha, \Gamma \Rightarrow \Delta, \beta}{\Gamma \Rightarrow \Delta, \alpha \rightarrow \beta},
\end{array}$$

más otras cuatro reglas que omitimos aquí, dos asociadas al generalizador y otras dos al particularizador. Las tres primeras son las *reglas estructurales*[82] y las doce últimas (contando las cuatro que hemos omitido) son las *reglas operacionales.*

Antes de explicar estas reglas de inferencia vamos a ver el aspecto que tiene el ejemplo de deducción que hemos comentado en el apartado anterior, pero ahora en términos del cálculo secuencial:

$$\dfrac{\dfrac{\dfrac{\dfrac{\alpha \Rightarrow \alpha}{\alpha \Rightarrow \alpha \vee \beta} \quad \dfrac{\alpha \Rightarrow \alpha}{\alpha \Rightarrow \alpha \vee \gamma}}{\alpha \Rightarrow (\alpha \vee \beta) \wedge (\alpha \vee \gamma)} \quad \dfrac{\dfrac{\dfrac{\beta \Rightarrow \beta}{\beta \Rightarrow \alpha \vee \beta} \quad \dfrac{\gamma \Rightarrow \gamma}{\gamma \Rightarrow \alpha \vee \gamma}}{\beta \wedge \gamma \Rightarrow \alpha \vee \beta} \quad \dfrac{\beta \wedge \gamma \Rightarrow \alpha \vee \gamma}{}}{\beta \wedge \gamma \Rightarrow (\alpha \vee \beta) \wedge (\alpha \vee \gamma)}}{\alpha \vee (\beta \wedge \gamma) \Rightarrow (\alpha \vee \beta) \wedge (\alpha \vee \gamma)}}{\Rightarrow \alpha \vee (\beta \wedge \gamma) \rightarrow (\alpha \vee \beta) \wedge (\alpha \vee \gamma)}$$

Este árbol puede construirse de forma totalmente mecánica (sin preocuparse para nada del significado de la fórmula que queremos demostrar). Para ello lo vamos construyendo de abajo hacia arriba:

1. La línea inferior es el secuente que expresa la fórmula que queremos demostrar. En términos del cálculo secuencial, demostrar una fórmula θ equivale a demostrar el secuente $\Rightarrow \theta$.

2. Como la fórmula es una implicación, aplicamos (en sentido inverso) la regla de introducción del implicador en el consecuente, que nos da la segunda línea del árbol. En el enunciado de la regla hay que entender que Γ y Δ son dos conjuntos arbitrarios de fórmulas, que en este caso son vacíos. Esto significa que la regla se podría aplicar igualmente aunque hubiera otras fórmulas en el antecedente y en el consecuente. Lo mismo vale para todas las reglas.

3. Ahora aplicamos la regla de introducción del disyuntor en el antecedente, lo que requiere escribir dos premisas en el tercer nivel.

4. En las dos premisas, aplicamos la regla de introducción del conjuntor en el consecuente, lo que nos da las fórmulas del cuarto nivel.

5. En la parte izquierda del árbol, la regla de introducción del disyuntor en el consecuente nos da ya el axioma lógico $\alpha \Rightarrow \alpha$, que cierran dicha parte.

6. En la parte derecha, la regla de introducción del conjuntor en el antecedente nos da dos secuentes que se deducen a su vez de axiomas lógicos mediante la regla de introducción del disyuntor en el consecuente.

[82] En realidad, Gentzen consideraba que el antecedente y el consecuente de un secuente eran sucesiones de fórmulas, mientras que nosotros consideramos que son conjuntos de fórmulas. La diferencia es que Gentzen tenía que dar cuatro reglas estructurales adicionales, que expresaban que se pueden eliminar repeticiones en el antecedente y en el consecuente, y que se pueden reordenar las fórmulas en el antecedente y en el consecuente. Considerando a éstos como conjuntos, tales reglas resultan innecesarias.

En este ejemplo no hemos necesitado ninguna regla estructural, y todos los secuentes tienen una única fórmula en el consecuente (y en el antecedente también, pero eso es irrelevante), por lo que la deducción es válida en el sistema LJ, lo que significa que es válida para la lógica intuicionista.

Vemos así que el cálculo secuencial sólo tiene reglas de introducción y no de eliminación de signos lógicos. Por ello, a menudo, en lugar de decir, por ejemplo, "regla de introducción del disyuntor en el antecedente / consecuente" se dice más brevemente, "regla izquierda / derecha del disyuntor". La única regla que permite eliminar signos lógicos es la regla de corte.

El lector puede comprobar que todas las reglas de inferencia son correctas, en el sentido de que si sus premisas son secuentes verdaderos, su conclusión también tiene que serlo. Por ejemplo, la regla derecha del disyuntor dice que si α y otras fórmulas en Γ implican que se cumple la disyunción de las fórmulas de Δ y que β y las mismas fórmulas de Γ implican también que se cumple esa misma disyunción, entonces $\alpha \vee \beta$ y las mismas fórmulas de Γ implican también dicha disyunción, lo cual es cierto.

Conviene observar el significado de la regla de corte:

Si llamamos γ a la conjunción de las fórmulas de Γ y δ a la disyunción de las de Δ, las premisas son que $\gamma \to \delta \vee \alpha$ y que $\alpha \wedge \gamma \to \delta$. La conclusión es que $\gamma \to \delta$, lo cual es cierto, porque, supuesto γ, o bien se cumple α, o bien se cumple $\neg\alpha$. En el primer caso tenemos $\alpha \wedge \gamma$, luego la primera premisa nos da δ, y en el segundo caso la primera premisa nos da $\delta \vee \alpha$, pero, como es $\neg\alpha$, tiene que ser δ, y en ambos casos tenemos que $\gamma \to \delta$.

Notemos que hemos usado el principio del tercio excluso al suponer $\alpha \vee \neg\alpha$, lo cual no es intuicionistamente aceptable, pero aquí tenemos que recordar que en el cálculo LJ los consecuentes no pueden tener más de una fórmula, luego la regla del corte sólo es válida en LJ cuando Δ es vacío.

En tal caso, las premisas son que $\gamma \to \alpha$ y (por la interpretación de los secuentes con consecuente vacío) que $\neg\alpha \vee \neg\gamma$, mientras que la conclusión es $\neg\gamma$, y de nuevo es correcto (esta vez sin tercio excluso), ya que si suponemos γ, tiene que darse α por la primera premisa y $\neg\alpha$ o bien $\neg\gamma$ por la segunda, luego tiene que darse la conclusión requerida $\neg\gamma$.

Las justificaciones de que las reglas de inferencia son correctas pueden parecer más o menos artificiosas, pero eso es irrelevante. Lo que importa es que las reglas del cálculo secuencial son correctas y son formalmente simplicísimas, lo cual hace posibles numerosos argumentos en la teoría de la demostración que serían inviables considerando demostraciones "a la Hilbert".

Observemos por último cómo se demuestra en LK el principio del tercio excluso:

$$\dfrac{\dfrac{\dfrac{\dfrac{\alpha \Rightarrow \alpha}{\Rightarrow \alpha, \neg\alpha}}{\Rightarrow \alpha \vee \neg\alpha, \neg\alpha}}{\Rightarrow \alpha \vee \neg\alpha, \alpha \vee \neg\alpha}}{\Rightarrow \alpha \vee \neg\alpha}$$

Hemos aplicado (de arriba hacia abajo) la regla derecha del negador, la regla derecha del disyuntor dos veces y por último hemos eliminado la duplicación de $\alpha \vee \neg\alpha$ usando que el consecuente es un conjunto de fórmulas, por lo que la duplicación es redundante (para Gentzen esto era una aplicación de la regla estructural de contracción).

Notemos que la prueba no es válida en LJ desde el primer paso, que ya ha dado lugar a un secuente con dos fórmulas en el consecuente.

Genzten insiste una y otra vez en que muchas de las características del cálculo secuencial son preferibles a cualquier otra alternativa que podría parecer igualmente razonable (como sustituir algunas reglas por axiomas) porque así es como tienen que ser para que se cumpla lo que él llama el *Hauptsatz* (el teorema principal), que hoy se conoce como:

> **Teorema de eliminación de cortes.** Toda deducción en LJ o LK puede transformarse en otra deducción con el mismo secuente final en la que no se use la regla de corte.

Es imposible transmitir aquí la relevancia de este teorema.[83] Lo primero que podría plantearse el lector es qué sentido tiene incluir la regla de corte en el cálculo secuencial para luego demostrar que no hace falta usarla.

[83] En realidad, lo que es relevante es la posibilidad de demostrar teoremas análogos para teorías con más axiomas que los meros axiomas lógicos, pero no vamos a entrar en ello aquí. De todos modos, el teorema para LK y LJ también tiene su importancia.

Hay varias razones que lo explican. Ante todo, hay demostraciones que son naturales usando la regla de corte, pero que, si les aplicamos el teorema de eliminación de cortes, podemos obtener pruebas muchísimo más largas y enrevesadas.

En segundo lugar, la regla de corte hace falta para deducir consecuencias de premisas. Por ejemplo, si queremos tomar el secuente $\Rightarrow \alpha \wedge \beta$ como premisa y deducir $\Rightarrow \alpha$, la regla de corte es imprescindible. Una deducción es así:

$$\dfrac{\Rightarrow \alpha \wedge \beta \qquad \dfrac{\alpha \Rightarrow \alpha}{\alpha \wedge \beta \Rightarrow \alpha}}{\Rightarrow \alpha}$$

Sin la regla de corte sería imposible, porque —recordemos— la regla de corte es la única que permite eliminar fórmulas de una deducción. Si usamos la premisa $\Rightarrow \alpha \wedge \beta$ y queremos llegar a $\Rightarrow \alpha$, es imprescindible aplicar la regla de corte para eliminar $\alpha \wedge \beta$, porque cualquier otra regla de inferencia dejará invariante $\alpha \wedge \beta$ o la sustituirá por una fórmula más compleja, pero nunca la eliminará.

En tercer lugar, la regla de corte aparece, por ejemplo, en la demostración siguiente de que LK y LJ son consistentes, es decir, que no es posible demostrar un secuente de la forma $\Rightarrow \alpha \wedge \neg\alpha$.

En efecto, si fuera posible deducir tal secuente, podríamos prolongar la deducción así:

$$\dfrac{\Rightarrow \alpha \wedge \neg\alpha \qquad \dfrac{\alpha \Rightarrow \alpha}{\alpha \wedge \neg\alpha \Rightarrow}}{\Rightarrow}$$

con lo que en LJ o LK podríamos demostrar el secuente vacío. Esta demostración usaría la regla de corte (al menos en su paso final), pero, por el teorema de eliminación de cortes existiría otra demostración sin cortes del secuente vacío, pero eso es imposible, por el mismo motivo que antes: en una demostración sin cortes las fórmulas de los axiomas se quedan igual o se van sustituyendo por fórmulas más complejas, pero nunca se eliminan, luego no es posible llegar al secuente vacío.

Una ligera variante del argumento anterior nos da que si unas fórmulas $\gamma_1, \ldots, \gamma_n$ son contradictorias, es decir, si podemos deducir lógicamente un secuente de la forma $\gamma_1, \ldots, \gamma_n \Rightarrow \alpha \wedge \neg\alpha$, cortando la contradicción como antes llegaríamos a una deducción del secuente $\gamma_1, \ldots, \gamma_n \Rightarrow$, que a su vez podemos suponer que puede deducirse sin cortes, y esto puede usarse decisivamente en una prueba de la consistencia de $\gamma_1, \ldots, \gamma_n$.

Por ejemplo, Gentzen usó este método (con un refinamiento del teorema de eliminación de cortes) para demostrar la consistencia de la aritmética de Peano sin el principio de inducción.

Las posibilidades que ofrece el cálculo secuencial para analizar la estructura de una demostración no tienen parangón con lo que dan de sí los cálculos deductivos "a la Hilbert". Por eso muchos libros modernos de teoría de la demostración trabajan exclusivamente con el cálculo secuencial, ya que muchos de los resultados que presentan serían inabordables sin él.

58 El lema de Zorn Ya en 1914, en sus *Fundamentos de la teoría de conjuntos,* Hausdorff había demostrado lo que hoy se conoce como *principio maximal de Hausdorff:*

> Si $(P, \leq)$ es un conjunto parcialmente ordenado[84] y $C \subset P$ es un subconjunto totalmente ordenado (es decir, tal que, para cada $p, q \in P$, se cumple $p \leq q$ o bien $q \leq p$) entonces existe un conjunto totalmente ordenado $C \subset M \subset P$ que es maximal para la inclusión, es decir, que no está contenido en otro mayor.

La prueba usaba de forma esencial el axioma de elección. Hausdorff se interesó en este hecho a raíz de sus estudios sobre conjuntos bien ordenados y no pareció darle excesiva importancia. Sin embargo, en 1922 Kuratowski publicó un artículo titulado *Un método de eliminación de los números transfinitos en los razonamientos matemáticos* en el que demostraba varios resultados similares, como:

> Si E es un conjunto y sea $\mathcal{P}$ un conjunto no vacío formado por subconjuntos de E con la propiedad de que todo conjunto $C \subset \mathcal{P}$ no vacío y bien ordenado por la inclusión cumple $\bigcup C \in \mathcal{P}$. Entonces existe un conjunto $M \in \mathcal{P}$ que es maximal respecto de la inclusión, es decir, que no está contenido en otro conjunto mayor que pertenezca a $\mathcal{P}$.

[84] Esto significa que $\leq$ es una relación reflexiva, antisimétrica y transitiva en P.

Kuratowski demostró este resultado usando ordinales, pero a su vez mostró que podía usarse para demostrar resultados en topología sin necesidad de saber nada de ordinales. Varios trabajos posteriores usaron los teoremas de Kuratowski, pero siempre en el área de la topología. Hausdorff demostró el teorema anterior en la segunda edición de su *Teoría de conjuntos,* publicada en 1927, y Solomon Bochner lo usó en un artículo de 1928 titulado *Extensión de superficies de Riemann.* Copiamos la demostración de Hausdorff:

> *Se elige en el sistema $\mathcal{P}$, un conjunto cualquiera A_0, luego, si existen en $\mathcal{P}$ conjuntos que contienen estrictamente a A_0, entre éstos se elige un conjunto A_1; si aún existen conjuntos que contienen estrictamente a A_1, entre éstos se elige un conjunto A_2, y así sucesivamente. Si se llega para un n finito a un conjunto A_n tal que no existe ningún conjunto en $\mathcal{P}$ que contenga estrictamente a A_n, entonces tenemos un conjunto maximal. En caso contrario, nos encontramos con una sucesión estrictamente creciente de conjuntos $A_0 \subset A_1 \subset A_2 \subset \cdots$ de tipo ω. Ahora bien, puede ocurrir que no exista ningún conjunto A en el sistema $\mathcal{P}$ que contenga todos los A_n; entonces el intento ha fracasado. Por lo tanto, hacemos la suposición de que una sucesión ascendente de conjuntos sin último elemento siempre puede continuarse, es decir:*
>
> $(*)$ *Si η es un ordinal límite y*[85]
>
> $$A_0 \subset A_1 \subset \cdots \subset A_\xi \subset A_{\xi+1} \subset \cdots \qquad (\xi < \eta)$$
>
> *es una sucesión estrictamente creciente de conjuntos del sistema de tipo η, entonces existe en $\mathcal{P}$ un conjunto A_η que contiene a todos los A_ξ.*
>
> *Así el procedimiento anterior puede continuarse, y debe conducir finalmente a un conjunto maximal. Pues si definimos inductivamente* [es decir, por recursión transfinita] *A_η $(\eta > 0)$ como un conjunto que supera a todos los A_ξ $(\xi < \eta)$, suponiendo que todos los A_ξ ya están definidos y existe tal conjunto A_η, mientras que de lo contrario A_η no se define, entonces el conjunto de los A_η definidos no puede exceder la cardinalidad*[86] *del sistema $\mathcal{P}$, y existe un mínimo ordinal $\zeta > 0$ para el cual A_ζ no está definido. Según $(*)$, ζ no es un ordinal límite, luego $\zeta = \eta + 1$, el conjunto A_η está definido y no existe ningún conjunto en $\mathcal{P}$ que contenga estrictamente a A_η, ya que de lo contrario podría ser elegido como $A_{\eta+1}$. Así, A_η es un elemento maximal.*

En 1932 el estadounidense Robert Lee Moore publicó su libro *Fundamentos de la teoría de conjuntos de puntos* en el que citaba a Kuratowski y demostraba:

> *Si G es una familia no vacía de conjuntos y para cada subconjunto H de G totalmente ordenado por la inclusión existe un A en G tal que $A \subset B$, para todo B en H, entonces un elemento M de G no tiene subconjuntos propios en G.*

(Esta versión se sigue de aplicar la de Kuratowski al conjunto de los complementarios de los elementos de G respecto de un conjunto que los contenga a todos).

En 1930 había leído su tesis doctoral en Hamburgo un joven de 24 años llamado Max Zorn, bajo la dirección de Emil Artin. Más tarde, en 1933, Zorn emigró a los Estados Unidos, no mucho después de que un grupo de nazis le diera una paliza en la calle que le dañó para siempre la garganta (Zorn no era judío, pero sí comunista). Ese mismo año Bochner, que sí que era judío, emigró también a los Estados Unidos.

En **1935** Zorn publicó un artículo titulado *Una observación sobre el método en álgebra transfinita,* que empezaba así:

> *Los teoremas de Steinitz relativos a la clausura algebraica y el grado de trascendencia se ven obstaculizados, desde el punto de vista algebraico, por el teorema de buena ordenación y su teoría. Queremos mostrar cómo, introduciendo un axioma sobre conjuntos de conjuntos en lugar del teorema de buena ordenación, se pueden simplificar las demostraciones y hacerlas más algebraicas. Las demostraciones se presentarán desde el punto de vista no axiomático de la teoría de conjuntos.*

[85] Hausdorff no ha enunciado el teorema previamente, sino que parte de una familia de conjuntos $\mathcal{P}$ y ahora supone una hipótesis ligeramente más débil que la de Kuratowski: en lugar de suponer que la unión de los A_ξ está en $\mathcal{P}$, supone meramente que en $\mathcal{P}$ hay un conjunto que contiene a los A_ξ, sin necesidad de que sea su unión.

[86] Tenemos una aplicación inyectiva $\eta \longrightarrow \mathcal{P}$ dada por $\xi \mapsto A_\xi$, luego η tiene que ser menor o igual que el cardinal de $\mathcal{P}$. Esto prueba que la sucesión transfinita que hemos definido tiene que detenerse en algún ordinal ζ, que no puede ser un ordinal límtie, porque la hipótesis $(*)$ garantiza que la construcción siempre puede continuar en los ordinales límite.

DEFINICIÓN 1. *Un conjunto $\mathcal{B} = \{B\}$ de conjuntos B se llama una cadena si para cada par de conjuntos $B_1, B_2 \in \mathcal{B}$ se cumple $B_1 \subset B_2$ o $B_2 \subset B_1$.*

DEFINICIÓN 2. *Se dice que un conjunto $\mathcal{A}$ de conjuntos A es cerrado (cerrado por la derecha) si contiene la unión $\bigcup \mathcal{B}$ de cada cadena $\mathcal{B}$ contenida en $\mathcal{A}$.*

Entonces, nuestro principio maximal se puede expresar de la forma siguiente:

(PM). *En un conjunto cerrado $\mathcal{A}$ de conjuntos A, existe al menos un A^* que no está contenido como un subconjunto propio en ningún otro $A \in \mathcal{A}$.*

Así, el resultado de Zorn era el mismo de Kuratowski salvo que no requería que las cadenas estuvieran bien ordenadas por la inclusión, sino únicamente que estuvieran totalmente ordenadas (con lo cual el enunciado era conceptualmente más simple, pero no más general, sino todo lo contrario: el enunciado de Kuratowski implica trivialmente el de Zorn). Pero Zorn hablaba de "su" principio maximal, sin ninguna referencia a Kuratowski ni a ningún otro autor, y dijo que en un próximo artículo mostraría que era equivalente al axioma de elección, pero tal artículo nunca aparecería.

Cuando, años más tarde, se le preguntó a Zorn si no conocía las publicaciones previas sobre "su" lema, su respuesta fue muy sospechosa:

> *Hice mi trabajo sobre el principio maximal en Hamburgo, alrededor de 1933.* [...] *En algún momento tuve el libro de Moore en mis manos, pero no vi el teorema. Sólo lo vi cuando alguien me lo señaló mucho después, en los Estados Unidos.* [...] *Sabía de Kuratowski, pero me formé una impresión errónea de la idea de su artículo. Sólo en 1976 me di cuenta del contenido del libro de Hausdorff* [de 1927]. *De entre las personas con las que tenía contacto, tal vez fui el primero en advertirlo.*

Lo que hizo Zorn fue mostrar a los algebristas que, sin saber nada de ordinales ni de teoría de conjuntos, con "su" principio maximal, podían demostrar fácilmente teoremas como la existencia y unicidad de la clausura algebraica de un cuerpo (que Steinitz había demostrado en 1910 a partir del principio de buena ordenación) o la existencia de ideales maximales en un anillo unitario (que Wolfgang Krull había demostrado en 1929 mediante una inducción transfinita), etc.

Este resultado abrió las puertas del axioma de elección a los algebristas e hizo que muchos perdieran cualquier clase de inhibición hacia el axioma de elección. Con el tiempo se pasó a llamar *Lema de Zorn* a una versión un poco más general del resultado enunciado por Zorn, en la que no se exige que la relación de orden sea la inclusión (y que se demuestra exactamente con la misma prueba).

59 El platonismo Ya hemos hablado en varias ocasiones de la concepción platonista de las matemáticas, pero el término fue acuñado en **1935** por Bernays en un artículo titulado *Platonismo en matemáticas* (o, en realidad, el año anterior, pues era el texto de una conferencia que había dado en Ginebra en 1934). Empieza señalando un hecho que, en boca de otro matemático, podría tenerse por ignorancia, pero que en boca de Bernays ponía en evidencia que en realidad era la opinión contraria la que indicaba una ignorancia de lo que las matemáticas eran para los matemáticos:

> *Con su permiso, me dirigiré a ustedes ahora sobre el tema de la situación actual en la investigación de los fundamentos de las matemáticas. Dado que quedan preguntas abiertas en este campo, no estoy en posición de pintar una imagen definitiva del mismo para ustedes. Pero debe señalarse que la situación no es tan crítica como uno podría pensar al escuchar a quienes hablan de una crisis de los fundamentos. Desde ciertos puntos de vista, esta expresión puede justificarse; pero podría dar lugar a la opinión de que la ciencia matemática está tambaleándose en sus raíces. La verdad es que las ciencias matemáticas están creciendo con completa seguridad y armonía. Las ideas de Dedekind, Poincaré y Hilbert se han desarrollado sistemáticamente con gran éxito, sin ningún conflicto en los resultados. Es sólo desde el punto de vista filosófico que se han planteado objeciones. Se refieren a ciertas formas de razonamiento peculiares del análisis y la teoría de conjuntos.*

En efecto, la realidad era que no había ninguna crisis de fundamentos en las matemáticas. Los matemáticos estaban fundando sus libros y artículos en los principios de la teoría de conjuntos sin que las posibles contradicciones de la teoría les importaran lo más mínimo. Lo cierto es que la axiomática de ZFC eliminaba por completo en la práctica esas contradicciones, pero no es menos cierto que a la mayoría de los matemáticos les daba igual. Para evitar las contradicciones les bastaba con no hablar de ellas o, como se solía decir, les bastaba "adoptar la teoría ingenua de conjuntos" evitando cualquier razonamiento que llevara a una contradicción.

Tras poner un ejemplo sobre la fundamentación de la geometría, Bernays introduce así el concepto de platonismo:

> *Este ejemplo ya muestra que la tendencia de la que hablamos consiste en ver los objetos como desvinculados de todo vínculo con el sujeto que reflexiona. Puesto que esta tendencia se manifestó especialmente en la filosofía de Platón, permítanme llamarla "platonismo".*

Bernays argumenta que el platonismo, entendido como que las matemáticas tratan sobre unos objetos que existen objetivamente y tienen las propiedades que tienen, justifica el uso de la lógica clásica en matemáticas (en particular el uso del tercio excluso que cuestionaban los intuicionistas). Podría decirse que termina confundiendo el platonismo con el no poner objeciones al razonamiento matemático (lo cual es, en realidad, compatible con una concepción formalista de las matemáticas, al estilo de Hilbert):

> *Las concepciones platónicas del análisis y la teoría de conjuntos también se han aplicado en las teorías modernas del álgebra y la topología, donde han demostrado ser muy fértiles. Este breve resumen bastará para caracterizar el platonismo y su aplicación a las matemáticas. Esta aplicación está tan extendida que no es una exageración decir que el platonismo reina hoy en las matemáticas.*
>
> *Pero, por otro lado, vemos que esta tendencia ha sido criticada en principio desde su primera aparición y ha dado lugar a muchas discusiones. Esta crítica se vio reforzada por las paradojas descubiertas en la teoría de conjuntos, a pesar de que estas antinomias sólo refutan el platonismo extremo.* [...]
>
> *La importancia esencial de estas antinomias radica en poner de manifiesto la imposibilidad de combinar dos elementos: la idea de la totalidad de todos los objetos matemáticos y los conceptos generales de conjunto y función. Esto se debe a que la totalidad misma formaría un dominio de elementos para los conjuntos, y de argumentos y valores para las funciones.*[87] *Por lo tanto, debemos renunciar al platonismo absoluto.*
>
> *Sin embargo, debe observarse que ésta es casi la única indicación que se desprende de las paradojas. Algunos pensarán que esto es lamentable, ya que las paradojas son invocadas por doquier. Pero evitar las paradojas no constituye un programa unívoco. En particular, el platonismo restringido no se ve afectado en absoluto por las antinomias.*

Tras un buen trecho de críticas al intuicionismo, Bernays sigue describiendo su concepción del platonismo:

> [...] *debemos reconocer que las suposiciones del platonismo tienen un carácter trascendente que no se encuentra en el intuicionismo.*
>
> *Es también este carácter trascendente el que nos obliga a tomar ciertas precauciones con respecto a cada suposición platónica. Pues, aun cuando tal suposición no sea en absoluto arbitraria y se presente de forma natural a la mente, puede suceder que el principio del que procede sólo permita una aplicación restringida, fuera de la cual se caería en contradicción. Debemos ser aún más cuidadosos ante esta posibilidad, ya que el impulso por la simplicidad nos lleva a hacer nuestros principios lo más amplios posible. Y a menudo no se percibe la necesidad de una restricción. Éste fue el caso, como hemos visto, del principio de totalidad, que fue llevado demasiado lejos por el platonismo absoluto. Aquí, sólo el descubrimiento de la paradoja de Russell-Zermelo demostró que era necesaria una restricción.*
>
> *Así, es deseable encontrar un método para asegurar que las suposiciones platónicas en las que se basan las matemáticas no excedan los límites permisibles.* [...] *Y la condición que restringe la aplicación de estos principios no es otra que la de la consistencia de las consecuencias que se deducen de las suposiciones fundamentales.*
>
> *Como saben, Hilbert está tratando de encontrar formas de darnos tales garantías de consistencia, y su teoría de la demostración tiene este objetivo.*

En suma, lo que dice es que los objetos matemáticos son los que son y tienen las propiedades que tienen, que no dependen de lo que nuestra intuición nos permite representarnos. Si un matemático estudia, digamos, las funciones holomorfas, está estudiando unos conceptos que existían antes de que a nadie se le ocurriera pensar

[87] Bernays viene a decir que el platonismo restringido no es más que admitir que no existen las multiplicidades inconsistentes o, mejor aún —en términos de la teoría de von Neumann Bernays— que no hay que confundir conjuntos y clases propias.

en ellos. En cambio, si estudia "el conjunto de todos los conjuntos", no está estudiando nada, porque no existe tal cosa y nunca ha existido. Lo que ocurre es que, cuando un matemático se plantea estudiar un concepto, no tiene por qué distinguir inmediatamente si es un concepto matemático legítimo, correspondiente a algo que existe, o si, por el contrario, es un concepto imposible. De ahí la importancia de las pruebas de consistencia.

Seguidamente, Bernays describe el programa de Hilbert y su intención de probar la consistencia de las teorías matemáticas mediante técnicas de la teoría de la demostración. Y añade:

> *Partiendo de esta idea fundamental, Hilbert esbozó un programa detallado de una teoría de la prueba, indicando las ideas principales de los argumentos (para las principales pruebas de consistencia). Su intención era limitarse a consideraciones intuitivas y combinatorias; su "punto de vista finitista" se restringía a estos métodos.*
>
> *Dentro de este marco, la teoría se desarrolló hasta cierto punto. Varios matemáticos contribuyeron a ella: Ackermann, von Neumann, Skolem, Herbrand, Gödel, Gentzen. Sin embargo, estas investigaciones permanecieron dentro de un dominio relativamente restringido. De hecho, ni siquiera lograron una prueba de la consistencia de la teoría axiomática de los números naturales.*

Para terminar explica las limitaciones que los teoremas de incompletitud de Gödel imponen al programa de Hilbert y menciona el resultado de Gödel (también obtenido por Gentzen) que reduce la consistencia de la aritmética de Peano clásica a la de la aritmética intuicionista de Heyting.

60 La consistencia de la aritmética Las últimas palabras que hemos citado de Bernays perdieron vigencia apenas un par de años después de cuando fueron pronunciadas, pues en **1936** Gentzen publicó un artículo titulado *La consistencia de la teoría de números elemental,* en el que presenta una demostración de la consistencia de la aritmética de Peano.

Como ya hemos señalado en varias ocasiones, la forma natural de justificar que unos axiomas son consistentes es encontrar unos objetos que los satisfagan, pero Hilbert había incidido en que no es posible seguir esa vía para probar la consistencia de la teoría de conjuntos, pues ello requeriría definir unos objetos abstractos inimaginablemente complejos cuya existencia el propio Hilbert ponía en cuestión. En su lugar, quedaba la posibilidad de demostrar la consistencia a través de la teoría de la demostración, es decir, demostrando la imposibilidad de que existe una demostración de una contradicción a partir de los axiomas, que es un problema puramente finitista (al menos en su planteamiento). Sin embargo, eso es razonable si hablamos de los axiomas de la teoría de conjuntos, pero no si hablamos de la aritmética de Peano. En este caso, es razonable concluir que la aritmética de Peano es obviamente consistente porque existen unos objetos que cumplen sus axiomas, a saber, los números naturales.[88] Pero la demostración de Gentzen era interesante porque se basaba enteramente en técnicas de la teoría de la demostración, susceptibles de ser aplicadas a otras teorías axiomáticas en las que no quepa la posibilidad de justificar la existencia intuitiva de unos objetos que cumplan los axiomas.

De hecho, Gentzen no contempla más que la posibilidad de una prueba de consistencia basada en al teoría de la demostración:

> *Veamos más de cerca la situación en el caso de los números naturales: Estos números obviamente no pueden ser determinados a partir de un dominio más simple de objetos. Tampoco nos concierne de hecho la consistencia del dominio de los números en sí, es decir, con la consistencia de las relaciones básicas entre los números según lo determinado por los 'axiomas' (p. ej., los 'axiomas de Peano' de la teoría de números). Probar la consistencia de estos axiomas sin invocar otras suposiciones equivalentes parece inconcebible. Nos concierne más bien la consistencia de nuestro razonamiento lógico sobre los números naturales (partiendo de sus axiomas) tal como ocurre en las demostraciones de la teoría de números.*

Por otro lado, Gentzen es plenamente consciente de la limitación que plantean los teoremas de incompletitud de Gödel, y no trata de burlarlos en modo alguno:

> *Sigue siendo bastante concebible que la consistencia de la teoría elemental de números pueda, de hecho, ser verificada mediante técnicas que, en parte, ya no pertenecen a la teoría elemental de números, pero que sin embargo pueden considerarse más fiables que los componentes dudosos de la propia teoría elemental de números.*

[88] Años más tarde, Gaisi Takeuti, que trabajo en Princeton con Gödel, diría al respecto de la prueba de Gentzen en su libro *Teoría de la demostración* de 1975: *Por supuesto, la importancia de este teorema reside en su demostración* [...] *¡Nadie alberga sospechas sobre la consistencia de la aritmética de Peano!*

No es posible entender esto sin entender previamente lo que Gentzen pretendía.[89] Para ello definimos

$$\omega^{(0)} = 1, \quad \omega^{(1)} = \omega, \quad \omega^{(2)} = \omega^\omega, \quad \omega^{(3)} = \omega^{\omega^\omega}, \quad \omega^{(4)} = \omega^{\omega^{\omega^\omega}}, \quad \ldots$$

En general, $\omega^{(n+1)} = \omega^{\omega^{(n)}}$. Tenemos así una sucesión estrictamente creciente de ordinales numerables, pero sabemos que esto nunca "agota" los ordinales, sino que por encima de todos los términos de una serie infinita de ordinales siempre hay un mínimo ordinal, que en este caso es el que Cantor había llamado[90] ϵ_0:

$$1 = \omega^{(0)} < \omega^{(1)} < \omega^{(2)} < \omega^{(3)} < \omega^{(4)} < \cdots < \epsilon_0.$$

En principio, todo esto se define y se demuestra a partir de los axiomas de la teoría de conjuntos, pero sucede que los ordinales menores que ϵ_0 pueden ser definidos en la aritmética de Peano. La clave para ello está en el teorema de la forma normal de Cantor, según el cual, todo ordinal puede expresarse de forma única como

$$\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_n},$$

para ciertos ordinales $\eta_0 \geq \eta_1 \geq \cdots \geq \eta_n$.

Para ordinales $\alpha < \epsilon_0$ se cumple además que $\alpha > \eta_0$, de odo que la forma normal de Cantor permite expresar α en términos de ordinales menores que α. En general esto no es cierto. Por ejemplo, la forma normal de Cantor de $\alpha = \epsilon_0$ es $\epsilon_0 = \omega^{\epsilon_0}$, que no aporta nada. La situación es similar a la de las fórmulas de un lenguaje formal, donde cada una de ellas puede construirse a partir de subfórmulas de menor longitud, hasta llegar a las fórmulas atómicas. Así, con las mismas técnicas con las que Gödel expresó en términos de números naturales las fórmulas de un lenguaje formal, y expresó sus propiedades en términos aritméticos, es posible expresar los ordinales menores que ϵ_0 en términos de números naturales, y definir en términos aritméticos la relación de orden entre estos ordinales.

Más precisamente, esto puede hacerse, no ya en la aritmética de Peano (AP), sino incluso en la Aritmética Recursiva Primitiva de Skolem (ARP), que no permite expresar más que conceptos y razonamientos finitistas en el sentido más estricto.

En resumen, en ARP podemos definir lo que es un ordinal (menor que ϵ_0) a la vez que la relación de orden entre los ordinales, y se puede demostrar que ésta es una relación de orden total. Por ejemplo, se cumple que

$$\omega^5 + \omega^4 + \omega + \omega + \omega + \omega + 1 + 1 + 1 + 1 + 1 < \omega^5 + \omega^5 + \omega^3 + \omega^2 + \omega^2 + 1 + 1 + 1$$

y esto no sólo se puede demostrar en ZFC, sino que también es posible demostrarlo en ARP y, en particular, en AP.

Con esto tenemos el primer ingrediente de la prueba de consistencia de Gentzen. El segundo consiste en que es posible asignar un ordinal menor que ϵ_0 a cada demostración en AP expresada en términos del cálculo secuencial LK de Gentzen. Esto puede hacerse de forma explícita (formalizable en ARP). Si nos dan una demostración de un teorema de AP en términos del sistema LK, a partir de ella podemos calcular un ordinal menor que ϵ_0 y escribirlo explícitamente en un papel (al menos, supuesto que el universo sea suficientemente grande como para contener un papel del tamaño adecuado, pero esta hipótesis es irrelevante en nuestro contexto).

El tercer ingrediente de la prueba consiste en que Gentzen demostró que si la aritmética de Peano es contradictoria, es decir, si existe una deducción en LK del secuente vacío $\Rightarrow$ tomando como premisas los axiomas de Peano (y los axiomas que expresan las propiedades lógicas del igualador, que no figuran en LK), es posible transformarla en otra de ordinal estrictamente menor. Nuevamente, este proceso es formalizable en ARP. En esta teoría podemos demostrar que si nos dan una demostración del secuente vacío en AP (el concepto de demostración es completamente finitista, y por ello formalizable en ARP), a partir de ella, una determinada construcción expresable en términos aritméticos nos da otra demostración del secuente vacío, y es posible demostrar en ARP que su ordinal es menor que el de la demostración dada.

Por lo tanto, si alguien encontrara una demostración de una contradicción en AP, podríamos formalizarla en LK y calcular su ordinal, digamos α_0. El proceso de Gentzen nos daría otra demostración de ordinal $\alpha_1 < \alpha_0$, y volviendo a aplicarlo obtendríamos otra demostración de ordinal $\alpha_2 < \alpha_1 < \alpha_0$, y procediendo del mismo modo obtendríamos una sucesión infinita estrictamente decreciente de ordinales menores que ϵ_0.

[89] Gentzen mejoraría su demostración en los años siguientes, y posteriormente otros autores obtendrían versiones más conceptuales y clarificadoras, de modo que tratar de describir su prueba de consistencia en los términos de este primer artículo en la que fue expuesta no sería lo más ilustrativo, así que en la exposición que sigue nos alejaremos bastante del planteamiento original.

[90] Cantor llamó *números épsilon* a los ordinales que cumplen $\omega^\epsilon = \epsilon$. El ordinal ϵ_0 es el menor número épsilon.

Y el cuarto y último ingrediente es justificar que no existen sucesiones decrecientes de ordinales menores que ϵ_0. Esto es un teorema de ZF, pero no queremos justificar la consistencia de AP a partir de la consistencia de ZF, pues eso sería trivial. La cuestión es dar un argumento "creíble" de que no existen sucesiones decrecientes de ordinales menores que ϵ_0 que no dependa de la consistencia de ZF.

Para precisar más el problema, igual que en AP (y, de hecho, en ARP) se puede definir una fórmula $P(n)$ que signifique "n es un número primo", también es posible definir una fórmula $D(\alpha)$ que signifique "α es un ordinal (menor que ϵ_0) y existe una demostración del secuente vacío en AP de ordinal α". Y en ARP se puede demostrar:

$$\bigwedge\alpha(D(\alpha) \to \bigvee\beta(\beta \prec \alpha \wedge D(\beta))),$$

donde $\beta \prec \alpha$ es la relación de orden entre los ordinales, definida en términos aritméticos (que no coincide con la relación de orden usual $<$ entre números naturales). Esto implica (y de hecho es lógicamente equivalente a)

$$\bigwedge\alpha(\alpha \in E \wedge \bigwedge\beta(\beta \prec \alpha \to \neg D(\beta)) \to \neg D(\alpha)),$$

donde $\alpha \in E$ es la fórmula (definida en términos aritméticos) que expresa que α es un ordinal (menor que ϵ_0). En efecto, si α es un ordinal (menor que ϵ_0) y suponemos que todo $\beta \prec \alpha$ cumple $\neg D(\beta)$, necesariamente se cumple $\neg D(\alpha)$, pues si fuera $D(\alpha)$, por la afirmación precedente, existiría un $\beta \prec \alpha$ que cumpliría $D(\beta)$, en contra de lo supuesto.

Así pues, esta última fórmula también es demostrable en ARP. Recordemos que existe consenso en que ARP es una teoría estrictamente finitista, luego ni siquiera un intuicionista cuestionaría que lo que expresa la fórmula precedente es verdad: si todos los ordinales menores que uno dado α cumplen la propiedad $\neg D(\beta)$, entonces α también la cumple.

El punto crucial de la demostración es si esta otra fórmula también es verdadera:

$$\mathrm{IND}(\epsilon_0) : \bigwedge\alpha(\alpha \in E \wedge \bigwedge\beta(\beta \prec \alpha \to \neg D(\beta)) \to \neg D(\alpha)) \to \bigwedge\alpha(\alpha \in E \to \neg D(\alpha)).$$

Lo que expresa $\mathrm{IND}(\epsilon_0)$ no es más que (un caso particular de) el principio de inducción transfinita hasta ϵ_0:

> Si α es un ordinal (menor que ϵ_0) y, bajo el supuesto de que todos los ordinales $\beta \prec \alpha$ cumplen $\neg D(\beta)$, podemos asegurar que también se cumple $\neg D(\alpha)$, entonces podemos concluir que todos los ordinales (menores que ϵ_0) cumplen $\neg D(\alpha)$.

Según acabamos de observar, en ARP se puede demostrar la hipótesis de $\mathrm{IND}(\epsilon_0)$, es decir, podemos demostrar lo que requiere una demostración por inducción transfinita para concluir que todo ordinal cumple $\neg D(\alpha)$. Lo que falta por analizar es si ese principio de inducción transfinita es válido. Equivalentemente, en ARP podemos demostrar:

$$\mathrm{IND}(\epsilon_0) \to \bigwedge\alpha(\alpha \in E \to \neg D(\alpha)),$$

pero lo que dice el miembro derecho es que ningún ordinal es el ordinal de una demostración de una contradicción en AP. Eso implica (siempre en ARP) que no existen demostraciones de contradicciones en AP (pues a cada demostración de una contradicción siempre podemos asignarle un ordinal). Como diría Gödel:

$$\mathrm{IND}(\epsilon_0) \to \mathrm{Consis}(\ulcorner\mathrm{AP}\urcorner).$$

Esto es un teorema de ARP, luego hasta un intuicionista aceptará que es verdad:

> Si el principio de inducción transfinita[91] hasta ϵ_0 (en su interpretación aritmética) es verdadero, entonces AP es consistente.

Para terminar con los hechos "incuestionables", conviene observar lo siguiente:

> Si no se cumple $\mathrm{IND}(\epsilon_0)$, existe una sucesión infinita decreciente de ordinales con la propiedad $D(\alpha)$.

[91] El principio de inducción transfinita hasta ϵ_0 sería en realidad la afirmación $\mathrm{IND}(\epsilon_0)$, no concretamente para la propiedad $\neg D(\alpha)$, sino para cualquier propiedad $P(\alpha)$ o, al menos, para cualquier propiedad definible en AP, pero aquí sólo necesitamos el caso particular correspondiente a la propiedad concreta $\neg D(\alpha)$, es decir, la propiedad de no ser el ordinal asociado a una demostración de una contradicción en AP.

En efecto, estamos suponiendo que se cumple la hipótesis:

$$\bigwedge\alpha(\alpha \in E \wedge \bigwedge\beta(\beta \prec \alpha \to \neg D(\beta)) \to \neg D(\alpha)),$$

pero que falla la tesis, es decir, que existe un ordinal α_0 tal que $D(\alpha_0)$. Aplicando la fórmula anterior a α_0, concluimos que existe un $\alpha_1 \prec \alpha_0$ tal que $D(\alpha_1)$, y aplicando la fórmula a α_1 resulta que existe un $\alpha_2 \prec \alpha_1$ que cumple $D(\alpha_2)$, y así vamos obteniendo una sucesión infinita:

$$\alpha_0 \succ \alpha_1 \succ \alpha_2 \succ \alpha_3 \succ \cdots$$

Así pues, Genzten dio una demostración estrictamente finitista de que $\mathrm{IND}(\epsilon_0)$ (o, alternativamente, de que la no existencia de sucesiones decrecientes de ordinales menores que ϵ_0) implica la consistencia de AP.

Es en este punto cuando Gödel tiene algo que decir: en AP no puede demostrarse $\mathrm{IND}(\epsilon_0)$, porque, si se pudiera, también podríamos demostrar en AP la fórmula $\mathrm{Consis}(\ulcorner \mathrm{AP} \urcorner)$ que expresa la consistencia de AP, y eso es justo lo que el segundo teorema de incompletitud asegura que no puede ocurrir.

Tenemos pues, una afirmación puramente aritmética, sobre los números naturales, que es demostrable en ZF (donde puede demostrarse el teorema de inducción transfinita para ordinales cualesquiera), pero que no es demostrable en AP. Pero esta afirmación concreta sobre los números naturales implica —incuestionablemente— la consistencia de AP.

Para analizar hasta qué punto podemos considerar intuitivamente verdadera la inducción hasta ϵ_0, nos planteamos antes una cuestión ligeramente más simple:

Supongamos que aceptamos de salida que la aritmética de Peano es consistente, simplemente porque los números naturales cumplen los axiomas de Peano y, por consiguiente, todos los teoremas de AP expresan afirmaciones verdaderas sobre los números naturales. Pero sucede que $\mathrm{IND}(\epsilon_0)$ no es demostrable en AP. ¿Tiene motivos para cuestionarse si $\mathrm{IND}(\epsilon_0)$ es verdad alguien que acepte que los teoremas de AP son todos verdaderos?

Para analizar esta pregunta definimos, para cada número natural metamatemático n y cada fórmula ϕ del lenguaje de la aritmética, la fórmula:

$$\phi - \mathrm{Ind}(\omega^{(n)}) : \bigwedge\alpha(\alpha \prec \omega^{(n)} \wedge \bigwedge\beta(\beta \prec \alpha \to \phi(\beta)) \to \phi(\alpha)) \to \bigwedge\alpha(\alpha \prec \omega^{(n)} \to \phi(\alpha)),$$

que expresa el principio de inducción hasta el ordinal $\omega^{(n)}$: si, para un ordinal $\alpha \prec \omega^{(n)}$, el hecho de que todo ordinal $\beta \prec \alpha$ cumpla una propiedad $\phi(\beta)$ implica que α también la tiene, entonces todos los ordinales menores que $\omega^{(n)}$ tienen dicha propiedad.

Pues bien: sucede que en AP se puede demostrar $\phi - \mathrm{Ind}(\omega^{(n)})$ para cada fórmula ϕ y para cada número natural (metamatemático) n.

Por lo tanto, si alguien acepta como verdaderos todos los teoremas de AP, aceptará que la inducción transfinita hasta cualquier $\omega^{n)}$ es verdadera, es decir, que si podemos demostrar

$$\bigwedge\alpha(\alpha \in E \wedge \bigwedge\beta(\beta \prec \alpha \to \phi(\beta)), \qquad (*)$$

como $\phi - \mathrm{Ind}(\omega^{(1)})$ es verdadera, $(*)$ implica $\bigwedge\alpha(\alpha \prec \omega^{(1)} \to \phi(\alpha))$, pero, como $\phi - \mathrm{Ind}(\omega^{(2)})$ también es verdadera, $(*)$ implica $\bigwedge\alpha(\alpha \prec \omega^{(2)} \to \phi(\alpha))$, pero, como $\phi - \mathrm{Ind}(\omega^{(3)})$ también es verdadera, $(*)$ implica $\bigwedge\alpha(\alpha \prec \omega^{(3)} \to \phi(\alpha))$ y, en general, podemos concluir que $\phi(\alpha)$ se cumple para todo $\alpha \prec \omega^{(1)}$, y para todo $\alpha \prec \omega^{(2)}$, y para todo $\alpha \prec \omega^{(3)}$, etc.

Ahora bien, ϵ_0 es el supremo de los ordinales $\omega^{(1)}$, $\omega^{(2)}$, $\omega^{(3)}$, etc. Todo ordinal α menor que ϵ_0 es menor que algún $\omega^{(n)}$, luego afirmar que $\phi(\alpha)$ se cumple para todo ordinal α menor que cada uno de los ordinales $\omega^{(1)}, \omega^{(2)}, \omega^{(3)}$, etc. equivale a afirmar que se cumple para todo ordinal menor que ϵ_0, que es lo que requiere $\phi - \mathrm{IND}(\epsilon_0)$. Por lo tanto, concluimos que la fórmula $\phi - \mathrm{IND}(\epsilon_0)$ es verdadera.

En resumen: hemos razonado que cualquiera que acepte que los teoremas de AP son verdaderos, debe aceptar que las fórmulas $\phi - \mathrm{IND}(\epsilon_0)$ son verdaderas (decimos "las fórmulas" porque hay una para cada fórmula ϕ). Pero entonces, si podemos deducir que $\phi - \mathrm{IND}(\epsilon_0)$ es verdadera sin más que aceptar que los axiomas de Peano (junto con sus consecuencias) son verdaderos, ¿por qué no podemos demostrar $\phi - \mathrm{IND}(\epsilon_0)$ a partir de los axiomas de Peano?

La respuesta es que en el argumento precedente hemos usado un hecho que no se deduce de los axiomas de Peano, y es que todo número natural es, o bien 0, o bien 1, o bien 2, etc. Concretamente, en AP (o en ARP) se puede demostrar que

$$\bigwedge\alpha(\alpha \in E \to \bigvee n\, \alpha \prec \omega^{(n)}),$$

pero lo que NO podemos demostrar es que $\alpha \prec \omega^{(1)}$ o $\alpha \prec \omega^{(2)}$ o $\alpha \prec \omega^{(3)}$, etc., y no lo podemos demostrar porque no lo podemos enunciar. Esto no es expresable mediante una fórmula del lenguaje de la aritmética.[92]

En términos del teorema de completitud semántica, para que la fórmula $\phi - \mathrm{IND}(\epsilon_0)$ fuera demostrable a partir de los axiomas de Peano haría falta que fuera verdadera en todos los modelos de los axiomas de Peano, pero lo único que hemos demostrado es que $\phi - \mathrm{IND}(\epsilon_0)$ es verdadera en el modelo natural, formado por los números naturales. Sabemos que $\phi - \mathrm{IND}(\epsilon_0)$ no puede demostrarse a partir de los axiomas de Peano, y eso, en virtud del teorema de completitud, se traduce en que existirá un modelo no estándar de AP en el cual $\phi - \mathrm{IND}(\epsilon_0)$ es falso. Será un modelo en el que existe un número natural k distinto de $0, 1, 2, 3, \ldots$, de modo que $\phi - \mathrm{IND}(\omega^{(n)})$ se cumple para $n = 0, 1, 2, 3, \ldots$, pero falla para k. Pero esto no afecta a la prueba de consistencia de Gentzen:

Si AP fuera contradictoria, podríamos escribir en un papel una demostración de una contradicción en AP, a partir de la cual podríamos calcular un ordinal en concreto α asociado a ella, un ordinal que cumpliría $D(\alpha)$, así como que $\alpha \prec \omega^{(n)}$ para un número natural concreto, fuera $0, 1, 2, 3, \ldots$ o quince millones, pero sería un número en concreto para el cual sabemos que $\neg D - \mathrm{IND}(\omega^{(n)})$ es verdadera, y esto implica que todo ordinal $\alpha \prec \omega^{(n)}$ cumple $\neg D(\alpha)$, con lo que tendríamos una contradicción: por un lado tendríamos un ordinal $\alpha \prec \omega^{(n)}$ que podríamos comprobar que cumple $D(\alpha)$, y por otro lado sabríamos que es verdad que no existe ningún ordinal así.

Por lo tanto, si aceptamos que la aritmética de Peano es consistente porque sus teoremas son verdaderos respecto de su interpretación natural, tenemos que aceptar que la inducción hasta ϵ_0 es una forma válida de razonamiento y, recíprocamente, aceptar la inducción hasta ϵ_0 supone aceptar (por un razonamiento finitista incuestionable) que la aritmética de Peano es consistente.

La cuestión es si hay un argumento que pueda convencer de que la inducción hasta ϵ_0 es válida a alguien que dude de la consistencia de la aritmética de Peano.

Por ejemplo, se dice que Tarski dijo en cierta ocasión que la prueba de Gentzen mediante inducción hasta ϵ_0 había aumentado su confianza en la consistencia de la aritmética "en un ϵ" (es decir, que el incremento fue insignificante), pero esto se entiende más bien como que ya confiaba en la consistencia de la aritmética y que la prueba de Gentzen no añadió nada a esta confianza.

Más mordaz fue Hermann Weyl cuando afirmó que Gentzen había demostrado la consistencia de la aritmética, es decir, de la inducción hasta el ordinal ω, mediante la inducción hasta ϵ_0 (un ordinal mucho mayor).

La crítica que encierra la frase de Tarski supone una acusación de circularidad trivial: "no tengo objeción alguna a tus argumentos porque acepto de entrada la conclusión a la que quieres llegar, y ella los justifica todos", mientras que la de Weyl sugiere una circularidad destructiva: "pretendes convencerme de algo pidiéndome que acepte de entrada algo mucho más fuerte que tu conclusión".

Sin embargo, Gentzen estaba convencido de que podía justificar satisfactoriamente la validez de la inducción transfinita hasta ϵ_0. Pero antes de entrar en este punto, conviene entender cómo concebía Gentzen el aporte global de su demostración:

> *El objetivo de la demostración de consistencia será justificar las formas de inferencia discutibles (incluidos los conceptos y axiomas derivados) sobre la base de inferencias indiscutibles. Para una comprensión adecuada de mi demostración de consistencia para la teoría elemental de números tendremos que examinar precisamente qué formas de inferencia y otras técnicas de demostración de la teoría elemental de números son de hecho discutibles, y cuáles otras pueden aceptarse como indudablemente correctas. Una delimitación inequívoca no es posible; pero ciertamente podemos presentar argumentos que harán muy plausible la admisibilidad de algunos métodos de demostración, mientras que una justificación correspondiente falla para otros métodos en los casos en que existe una analogía remota con las falacias que surgen en las antinomias de la teoría de conjuntos, y que hacen que estas técnicas parezcan discutibles.*

[92] He aquí un ejemplo de hecho que no puede entender alguien que no distinga entre los números naturales y su formalización.

Gentzen se refiere a las objeciones de los intuicionistas, que, a raíz de las contradicciones surgidas en la teoría de conjuntos, cuestionaron que la lógica clásica fuera aplicable a los razonamientos que involucran el infinito:

> *Pasemos ahora a las proposiciones esencialmente transfinitas, es decir, proposiciones en las que los conectores "todo" o "existe" se refieren a la totalidad de los números naturales. Aquí nos enfrentamos a un estado de cosas fundamentalmente nuevo.*
>
> *Primero debemos señalar que la regla de decisión aplicable en el caso de un dominio finito no se extiende a tales proposiciones transfinitas. En el caso de una proposición sobre todos los números naturales, por ejemplo, tendríamos que probar infinitos casos individuales, lo cual es imposible. No se conoce ninguna regla de decisión para proposiciones transfinitas arbitrarias y es dudoso que alguna vez pueda darse tal regla. Si existiera tal regla, podríamos decidir, por ejemplo, mediante cálculo si el "último teorema de Fermat" (así como la conjetura de Goldbach, etc.) es verdadero o falso. ¿Qué sentido puede atribuirse entonces a una proposición cuya verdad no puede verificarse?*
>
> *La visión tradicional sostiene que, independientemente de si lo sabemos o lo sabremos alguna vez, está realmente predeterminado si una proposición transfinita, como el último teorema de Fermat, es 'verdadera' o 'falsa'.* Se considera que toda proposición transfinita tiene un sentido real y definido.[93] *En particular, el sentido de una proposición universal se interpreta como: "Para cada uno de los infinitos números naturales, la proposición en cuestión es válida". El sentido de una proposición existencial es: "En la totalidad infinita de los números naturales, existe en algún lugar un número para el cual la proposición en cuestión es válida".*
>
> *De esta interpretación se infiere además que, para las proposiciones transfinitas, son válidas las mismas formas lógicas de inferencia que para el caso finito, ya que el sentido "actualista" de los conectores lógicos en las proposiciones transfinitas corresponde exactamente al del caso finito.*

Frente a esta posición "clásica", Gentzen contrapone la posición intuicionista:

> *En este punto existe ahora un amplio espacio para la crítica, siempre y cuando hayamos decidido extraer las últimas consecuencias de las ideas obtenidas al considerar las antinomias de la teoría de conjuntos. Esto es lo que haré ahora y, como resultado de un examen crítico de la antinomia de Russell, estableceré el principio siguiente:*
>
> Una totalidad infinita no debe considerarse como algo existente y cerrado de manera actual (infinito actual), sino sólo como algo que se está formando, que puede extenderse constructivamente cada vez más a partir de algo finito (infinito potencial).
>
> [...] *Sin embargo, la interpretación "actualista" tradicional de las proposiciones transfinitas que hemos descrito no es compatible con este principio, porque se basa en la idea de la secuencia numérica infinita cerrada. Al mismo tiempo, debe rechazarse la opinión de que las formas lógicas de inferencia pueden simplemente transferirse de dominios finitos a dominios infinitos de objetos.*
>
> *Recuerdo al lector un caso similar, aunque más trivial, de generalización inadmisible de lo finito a lo infinito, a saber, la conocida falacia: "Todo conjunto (finito) de números naturales contiene un número mayor; por lo tanto, el conjunto (infinito) de todos los números naturales contiene un número mayor". Este argumento lleva a contradicciones ya que, de hecho, no es válido.*
>
> *Habiendo rechazado la interpretación actualista de las proposiciones transfinitas, nos queda aún la posibilidad de atribuir un sentido "finitista" a tales proposiciones, es decir, de interpretarlas en cada caso como expresiones de estados de cosas definidos y caracterizables finitamente. Una vez adoptada esta perspectiva, las formas lógicas de inferencia relevantes deben examinarse en cuanto a su compatibilidad con esta interpretación de las proposiciones.* [...]

A partir de aquí Gentzen expone y justifica lo que esencialmente es la interpretación intuicionista de las afirmaciones aritméticas para justificar que toda la demostración de

$$\mathrm{IND}(\epsilon_0) \to \mathrm{Consis}(\ulcorner \mathrm{AP} \urcorner)$$

[93] Esta afirmación (que, como se ve justo a continuación, Gentzen restringe a proposiciones sobre números naturales) es relevante, pues se trata de la condición fundamental para la validez del razonamiento material: éste sólo puede tratar sobre proposiciones que tengan un significado intuitivo bien definido, es decir, que podamos considerarlas verdaderas o falsas, aunque no sepamos cómo determinar cuál de los dos casos se da. Por ejemplo, no podemos afirmar que una proposición como "toda función derivable es continua" tiene un significado preciso y definido porque no tenemos un concepto intuitivo de "función derivable" que sea tan general como el concepto matemático al que nos referimos.

es intuicionistamente aceptable. De este modo, sólo quedará justificar aceptablemente la validez de la inducción hasta ϵ_0 para concluir la consistencia de la aritmética de Peano clásica sin presuponer la posición clásica según la cual toda afirmación aritmética tiene un significado intuitivo "actualista" objetivo respecto al cual la lógica clásica es correcta (siempre lleva de premisas verdaderas a conclusiones verdaderas), lo cual ya de por sí implica trivialmente la consistencia (pues los axiomas de Peano son verdaderos y de ellos sólo se pueden deducir consecuencias verdaderas).

Con esto pasamos ya al punto delicado: la justificación de la inducción transfinita hasta ϵ_0, y ahora podemos entender a qué se refería Gentzen cuando hablaba de emplear *técnicas que, en parte, ya no pertenecen a la teoría elemental de números, pero que sin embargo pueden considerarse más fiables que los componentes dudosos de la propia teoría elemental de números.* Gentzen expresa su prueba en términos del concepto de "accesibilidad":

> *Todos los ordinales* [menores que ϵ_0] *son* accesibles, *en el sentido siguiente, al recorrerlos en orden de magnitud creciente: el primer ordinal,* 0*, se considera accesible y, si todos los números menores que un número β han sido reconocidos como accesibles, entonces β también se considera accesible.*

Aquí es importante recordar que cuando hablamos de ordinales, no nos estamos refiriendo a un concepto conjuntista abstracto, sino que es posible definir aritméticamente los ordinales (menores que ϵ_0) como determinados números naturales, junto con una relación de orden $m \prec n$, también definida aritméticamente, de modo que los primeros ordinales respecto a esta relación sean

$$0 \prec 1 \prec 2 \prec \cdots \omega \prec \omega+1 \prec \cdots \omega\cdot 2 \prec \cdots,$$

donde hay que entender que todos estos objetos son números naturales. Por ejemplo, con un convenio en particular para codificar los ordinales, se tiene esta identificación:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	1	ω	2	ω^ω	–	3	ω^2	$\omega+1$	–	4	ω^{ω^ω}	–	–	–	5	–	$\omega\cdot 2$	–	–	–

Las rayas indican que el número natural correspondiente, como el 5, no codifica ningún ordinal. Todos estos conceptos son decidibles: es posible programar un ordenador para que, dado un número natural, nos diga si corresponde a un ordinal o no y, en caso afirmativo, nos lo exprese en forma normal de Cantor, así como para que, si le damos dos ordinales, nos diga cuál de los dos es el mayor respecto a $\prec$ (tampoco hay dificultad alguna en probar que dos ordinales cualesquiera son comparables). Así, los primeros ordinales son los números naturales $0 \prec 1 \prec 3 \prec 6 \prec 10 \prec 15 \prec \ldots$ y Gentzen quiere demostrar que todos los ordinales son accesibles, en el sentido que ha definido.

Por ejemplo, por definición, el ordinal 0 (es decir, el número natural 0, según la tabla anterior) es accesible, pero éste es el único ordinal menor que el ordinal 1 (el número natural 1), luego éste también es accesible, y $0, 1$ son los únicos ordinales menores que el ordinal 2 (el número natural 3), luego éste también es accesible, y de este modo se puede justificar que son accesibles los ordinales $0, 1, 2, 3, \ldots$ (es decir, los números naturales $0, 1, 3, 6, \ldots$), que son todos los ordinales menores que ω (el número natural 2), luego éste también es accesible, y todos éstos son los únicos ordinales menores que el ordinal $\omega+1$ (el número natural 8), luego éste también es accesible.

Se trata de probar que, de este modo, se puede concluir que todos los ordinales (todos los números naturales que no tienen un $-$ en la tabla anterior) son accesibles. Justificar esto es equivalente a justificar la legitimidad de la inducción transfinita hasta ϵ_0. En efecto, si podemos razonar que todos los ordinales son accesibles, el mismo razonamiento valdrá si en la definición de accesibilidad añadimos cualquier propiedad P compatible con la definición de accesibilidad, es decir, cualquier propiedad para la que podamos asegurar que si todos los ordinales menores que uno β tienen la propiedad P, entonces β también la tiene. Y entonces, al probar que todos los ordinales son accesibles, habremos probado que todos tienen la propiedad P.

No vamos a dar aquí los detalles del argumento de Gentzen para justificar la inducción hasta ϵ_0, principalmente porque no representaba los ordinales exactamente a través de su forma normal del Cantor, por lo que tendríamos que profundizar un poco en la aritmética ordinal para explicar su planteamiento, pero, por otra parte, el caso es que Gödel no lo consideró concluyente. En efecto, Gentzen resumía así la situación:

> *Podemos, por ejemplo, visualizar los casos iniciales con características*[94] *1, 2, 3 con detalle. A medida que la característica crece, no se añade nada básicamente nuevo, el método de progresión es*

[94] Con la codificación de los ordinales que usa Gentzen, los ordinales de característica 0 son los finitos, los de característica 1 llegan hasta $\omega\cdot 2$, los de característica 2 hasta ω^2, los de característica 3 hasta $\omega^\omega = \omega^{(2)}$, y a partir de ahí ya siguen la sucesión $\omega^{(4)}, \omega^{(5)}$, etc.

siempre el mismo. Desde luego, hay que admitir que la complejidad de los infinitos múltiplemente anidados que hay que recorrer crece considerablemente; este recorrido debe considerarse siempre como potencial [...] *La dificultad reside en que, aunque el sentido finitista preciso de "recorrer" los ordinales es razonablemente claro en los casos iniciales, se vuelve de tal complejidad en el caso general que apenas es remotamente visualizable; sin embargo, esto constituye una base adecuada que justifica la posibilidad de recorrer los números de la característica siguiente.*

Pero Gödel no estuvo de acuerdo:

La situación, a grandes rasgos, puede ser descrita como sigue: La inducción transfinita hasta ϵ_0 *podría probarse finitistamente si y sólo si la consistencia de la teoría de números pudiera probarse finitistamente. Por otra parte, la validez de esta inducción no puede hacerse inmediatamente evidente, como sucede, por ejemplo, en el caso de* ω^2*. Es decir, uno no puede captar de un vistazo las diversas posibilidades estructurales que existen para las sucesiones decrecientes y no existe, por lo tanto, un conocimiento concreto inmediato de la terminación de cada una de dichas sucesiones. Pero, más aún, tal conocimiento concreto (en el sentido de Hilbert) no puede alcanzarse a través de una transición gradual de ordinales menores a otros mayores, porque los pasos concretamente evidentes, como* $\alpha \mapsto \alpha^2$ *son tan pequeños que tendrían que repetirse* ϵ_0 *veces para llegar hasta* ϵ_0*.*

Por otro lado, como ya hemos señalado y como Gentzen demostraría más adelante, es posible demostrar la validez de la inducción transfinita hasta cualquier ordinal $\omega^{(n)}$ a partir de los axiomas de Peano (tal cual están enunciados en la página 60), lo que significa que cualquier matemático que no desconfíe de las propiedades elementales de la suma y el producto de números naturales ni del principio de inducción usual, aceptará como un hecho rigurosamente probado que la inducción transfinita hasta cualquier ordinal $\omega^{(n)}$ es válida. Y si a eso le sumamos el hecho intuitivamente evidente (aunque no demostrable en AP) de que todo ordinal concreto α cumple $\alpha \prec \omega$, o bien $\alpha \prec \omega^{(2)}$, o bien $\alpha \prec \omega^{(3)}$, etc., la conclusión es que ningún matemático sin prejuicios intuicionistas cuestionará la validez de la inducción transfinita hasta ϵ_0. Otra cosa es que su justificación se pueda considerar finitista.

Por ejemplo, si identificamos los argumentos finitistas con los que pueden formalizarse en la Aritmética Recursiva Primitiva, entonces sucede que la inducción transfinita hasta $\omega^{(2)}$, es decir, hasta ω^ω, no es demostrable en ARP. Más precisamente, la asignación de ordinales a demostraciones puede hacerse de modo que toda demostración en ARP tenga ordinal menor que ω^ω, por lo que el mismo argumento de Gentzen prueba que

$$\mathrm{IND}(\omega^\omega) \to \mathrm{Consis}(\ulcorner \mathrm{ARP} \urcorner).$$

Otra cosa es que decidamos extender la noción de "razonamiento finitista", aunque tal vez sería más claro expresar la situación diciendo que un argumento metamatemático aceptable no tiene por qué ser finitista, sino que basta con que tenga un contenido intuitivo objetivo. Esto está en consonancia con lo que el propio Bernays publicó en 1967 en un artículo sobre David Hilbert:

Por lo tanto, se hizo evidente que el "punto de vista finito" no es la única alternativa a las formas clásicas de razonamiento y no está necesariamente implícito en la idea de la teoría de la demostración. Por lo tanto, se sugirió una ampliación de los métodos de la teoría de la demostración: en lugar de una reducción a métodos finitistas de razonamiento, sólo se requería que los argumentos fueran de carácter constructivo, lo que nos permitiera tratar con formas más generales de inferencia.

No está de más señalar que el hecho de que —como señala Gödel— la inducción transfinita hasta ϵ_0 no pueda considerarse como intuitivamente evidente no está reñido con que sea intuitivamente demostrable. (El teorema de Pitágoras tampoco es intuitivamente evidente, pero sí intuitivamente demostrable.)

Por otro lado, también cabe destacar que la crítica de Gödel al argumento de Gentzen para justificar la inducción hasta ϵ_0 no estaba reñida con que Gödel admirara el trabajo de Gentzen, y lo admiraba hasta el punto de que llegó a declarar que Gentzen era mejor lógico que él, cuando Gödel no se caracterizaba precisamente por las alabanzas a sus colegas.

Al margen del valor epistemológico que se le quiera conceder a la prueba de consistencia de Gentzen (es decir, a lo que aporta a la hora de convencer de la consistencia de la aritmética de Peano, más allá de que el argumento es técnicamente correcto) Gentzen lo concebía también como un paso previo de cara a un programa más ambicioso. Ese mismo año de **1936** dio una charla titulada *El concepto de infinito en matemáticas,* en la que dijo:

> *Primero presentaré una clasificación de las matemáticas en tres niveles distintos, según el grado en que se utiliza la noción de "infinito" en sus diversas ramas. El primer y más bajo nivel está representado por la teoría elemental de números, es decir, por la teoría de números que no emplea técnicas del análisis. El infinito aparece aquí en su forma más simple: se trata de una secuencia infinita de objetos, en este caso, los números naturales.* [...]
>
> *El segundo nivel de las matemáticas está representado por el análisis. En lo que respecta a la aplicación del concepto de infinito, la característica esencialmente nueva aquí es el hecho de que incluso los objetos individuales de la teoría pueden ser ellos mismos conjuntos infinitos. Los números reales, es decir, los objetos del análisis, se definen, al fin y al cabo, como conjuntos infinitos, por lo general como secuencias infinitas de números racionales. En este sentido, no importa si la definición particular elegida es la de intervalos encajados, cortes de Dedekind o cualquier otro medio. Toda la teoría de funciones complejas también pertenece a este nivel; aquí no se añade nada esencialmente nuevo.*
>
> *El tercer nivel de aplicación del concepto de infinito, finalmente, se encuentra en la teoría general de conjuntos. Aquí se admiten como objetos no sólo los números naturales y otras cantidades finitamente describibles, como en el primer nivel, así como conjuntos infinitos de estos, como en el segundo nivel, sino, además, conjuntos infinitos de conjuntos infinitos y, de nuevo, conjuntos de tales conjuntos, etc., con la máxima generalidad concebible.*

Y la conclusión de su charla era:

> *Espero —aunque esto es sólo una conjetura por el momento— que la consistencia del análisis —y, en la medida de lo posible, de la teoría de conjuntos— se pueda probar de la misma manera. En cada caso, por supuesto, tendremos que avanzar una distancia considerablemente mayor en la secuencia de números de la segunda clase numérica.*
>
> *En conjunto, la situación podría ser ésta: el aumento en la complejidad del concepto de infinito en los tres niveles de las matemáticas descritos al principio de este artículo —teoría elemental de números, análisis y teoría de conjuntos— va acompañado de una extensión correspondiente de la secuencia de números ordinales transfinitos. De la misma manera en que el número ϵ_0 constituye el límite superior para la teoría elemental de números, tendríamos un número específico de la segunda clase numérica como límite superior para el análisis, y otro número como límite superior para una teoría de conjuntos formalmente delimitada —en la medida en que dicha teoría de conjuntos tenga sentido.*

La distinción entre los tres niveles (aritmética, análisis y teoría de conjuntos) no es original de Gentzen, sino que se manejaba desde hacía tiempo en el entorno de Hilbert. La prueba de Gentzen se veía como un paso previo a una demostración de la consistencia del análisis, y como un indicio de que el programa de Hilbert podía ofrecer resultados no triviales.

La idea de Gentzen de reducir la consistencia de diversas teorías al principio de inducción hasta ordinales cada vez mayores acabaría cristalizando en lo que hoy se conoce como *análisis ordinal,* que es una parte relevante de la teoría de la demostración moderna.

61 El problema de la decisión En el seminario que Gödel había dado en Princeton sobre sus teoremas de incompletitud se había planteado la pregunta crítica:

> Si podemos calcular una función en la práctica, ¿ésta es necesariamente recursiva (en el sentido general de Gödel-Herbrand)?

La diferencia con las funciones recursivas primitivas era que ahora nadie conocía ningún ejemplo que desmintiera la conjetura. Podría pensarse que el mismo argumento por el que hemos construido una función recursiva que no es recursiva primitiva (página 96) se podría aplicar para construir una función calculable en la práctica, pero no recursiva. Sin embargo, no es así. Esta vez el argumento falla.

La razón es que no podemos enumerar las funciones recursivas de modo que podamos saber en la práctica cuál es la función f_n para un n dado. En efecto, ante una posible definición de una función recursiva en la que se use la definición por minimización, necesitamos saber si, dada una función $g(x_1, \ldots, x_n, x)$, para cada $x_1, \ldots, x_n$ existe o no un x tal que $g(x_1, \ldots, x_n, x) = 0$. Y no está claro cómo podemos comprobar que sea así.

Ahora se da la situación peculiar de que, si f es una función recursiva, podemos calcular sus valores en la práctica, pero lo que no podemos hacer siempre en la práctica es determinar si una definición dada corresponde o no a una función recursiva. Podemos pensar en una enumeración de todas las funciones recursivas con un argumento y repetir la construcción del ejemplo anterior, pero la función que obtendremos, que ciertamente no será recursiva, no sabremos cómo calcularla para algunos números naturales.[95]

En la práctica, parecía claro que cualquier función calculable explícitamente se ajustaba a la nueva definición de función recursiva, pero hacía falta un teorema análogo al teorema de completitud: Hilbert había dado una definición teórica de "deducción lógica" y Gödel había demostrado que cualquier cosa que un matemático aceptara como "deducción lógica" podía expresarse en los términos de la definición de Hilbert. Ahora faltaba justificar que cualquier función calculable en la práctica podía expresarse en los términos de la definición de función recursiva. Gödel tenía serias dudas de que eso fuera cierto.

Hay otra razón por la que tiene interés encontrar una caracterización de las funciones que pueden calcularse en la práctica. En su programa de la fundamentación de la matemática, Hilbert había incidido en un aspecto que nosotros hemos pasado por alto hasta ahora, y es *el problema de la decisión.* Hilbert esperaba que la teoría de la demostración acabara proporcionando un algoritmo para determinar si una fórmula es demostrable o refutable en una teoría axiomática.

No hemos incidido en ello porque la decidibilidad es consecuencia inmediata de la completitud: toda teoría completa es decidible. Si tenemos la garantía de que toda afirmación puede demostrarse o refutarse a partir de unos axiomas, para saber cuál es el caso sólo necesitamos ir enumerando todas las demostraciones en la teoría (cosa que, al menos en teoría, puede hacerse en la práctica) hasta encontrar una que pruebe o refute la afirmación deseada. Pero ahora que estaba claro que no se puede aspirar en general a que una teoría axiomática sea completa, se volvía relevante el problema de la decisión, es decir, si al menos podemos determinar qué afirmaciones son demostrables y cuáles refutables, al menos suponiendo la consistencia de la teoría (porque si la teoría es contradictoria, todas las fórmulas son demostrables).

Dos de los asistentes al seminario eran Stephen Cole Kleene y John Barkley Rosser, que ese mismo año leerían sus respectivas tesis doctorales, dirigidas ambas por Alonzo Church, el cual llevaba ya un tiempo estudiando el problema de la computabilidad efectiva de funciones. En 1932 y 1933 había publicado dos artículos en los que había introducido lo que llamó *cálculo λ,* un lenguaje formal aparentemente muy simple, pero capaz de definir una amplia clase de funciones, todas ellas calculables mediante algoritmos, en particular una clase de funciones definidas sobre los números naturales de la que no era descabellado conjeturar que eran todas las funciones que podían calcularse en la práctica.

Precisamente, la tesis de Kleene, titulada *Una teoría sobre los enteros positivos en la lógica formal,* mostraba cómo definir en el cálculo λ los números naturales y las operaciones aritméticas.

Sin embargo, en 1935 Kleene y Rosser publicaron un artículo titulado *La inconsistencia de ciertas lógicas formales,* en el que probaban que el cálculo λ era contradictorio formalizando en él la llamada *paradoja de Kleene-Rosser,* que venía a ser una variante de la paradoja de Richard.

Las lógicas formales a las que hacía referencia el título del artículo eran dos: el cálculo λ de Church y la *lógica combinatoria* de Haskell Brooks Curry, un matemático estadounidense que se había doctorado en 1930 en Gotinga bajo la dirección de Hilbert, quien pocos años antes había dirigido también la tesis del soviético Moses Schönfinkel, y ambos (Schönfinkel y Curry), habían creado independientemente la ya mencionada lógica combinatoria, muy relacionada con el cálculo lambda de Church.

En **1936** Church publicó su artículo *Un problema insoluble de la teoría de números elemental,* en el que presentaba una versión reducida del cálculo λ no afectada por la paradoja de Church-Kleene y a la vez mostraba un ejemplo de problema matemático que no podía resolverse, lo que resolvía negativamente el problema de la decisión, que Hilbert y Ackermann habían planteado años atrás, es decir, el problema de encontrar un algoritmo para determinar si cualquier afirmación matemática era demostrable o no. En sus propias palabras:

[95] Hay otra sutileza que conviene tener en cuenta respecto de estos conceptos. La función

$$f(n) = \begin{cases} 1 & \text{si ZFC es consistente,} \\ 0 & \text{si ZFC es contradictoria,} \end{cases}$$

es recursiva primitiva, pero no la sabemos calcular en la práctica. Es recursiva primitiva porque, o bien es la función constante igual a 1, o bien es la función constante igual a 0, y las dos se pueden calcular fácilmente, pero no sabemos cuál de las dos es.

> *El propósito del presente artículo es proponer una definición de calculabilidad efectiva que se considera que corresponde satisfactoriamente a la noción intuitiva, un tanto vaga, en términos de la cual a menudo se plantean problemas de esta clase, y mostrar, mediante un ejemplo, que no todo problema de esta clase es soluble.*
>
> *Como se verá, esta definición de calculabilidad efectiva puede expresarse en cualquiera de dos formas equivalentes: (1) una función de enteros positivos se llamará efectivamente calculable si es λ-definible en el sentido de la Sección 2, y (2) una función de enteros positivos se llamará efectivamente calculable si es recursiva en el sentido de la Sección 4. La noción de λ-definibilidad se debe conjuntamente al presente autor y a S.C. Kleene, habiéndose dado los pasos sucesivos hacia ella por el presente autor en los Annals of Mathematics, vol. 34 (1933), p. 863, y por Kleene en el American Journal of Mathematics, vol. 57 (1935), p. 219. La noción de recursividad en el sentido de la Sección 4 se debe conjuntamente a Jacques Herbrand y Kurt Gödel, como allí se explica. Y la prueba de la equivalencia de ambas nociones se debe principalmente a Kleene, pero también en parte al presente autor y a J. B. Rosser, como se explica más adelante. La propuesta de identificar estas nociones con la noción intuitiva de calculabilidad efectiva se hace por primera vez en el presente artículo (pero véase la primera nota a pie de página de la Sección 7).*
>
> *Con la ayuda de los métodos de Kleene (American Journal of Mathematics, 1935), las consideraciones del presente artículo podrían, con una modificación comparativamente ligera, llevarse a cabo enteramente en términos de λ-definibilidad, sin hacer uso de la noción de recursividad. Por otro lado, desde que se obtuvieron los resultados del presente artículo, Kleene ha demostrado (véase su próximo artículo, "General recursive functions of natural numbers") que se pueden obtener resultados análogos enteramente en términos de recursividad, sin hacer uso de la λ-definibilidad. El hecho, sin embargo, de que dos definiciones de calculabilidad efectiva tan ampliamente diferentes y (en opinión del autor) igualmente naturales resulten ser equivalentes, aumenta la fuerza de las razones aducidas a continuación para creer que constituyen una caracterización tan general de esta noción como es consistente con el concepto intuitivo habitual de la misma.*

Gödel discrepaba de la convicción de Church sobre que la λ-definibilidad pudiera identificarse con la calculabilidad efectiva. En los últimos años Church había mantenido correspondencia con Gödel y éste había calificado su propuesta como *absolutamente insatisfactoria.*

Ese mismo año de **1936**, poco después de la publicación del artículo de Church, un joven matemático británico de 24 años publicó el artículo *Sobre los números computables con una aplicación al problema de la decisión.* Se llamaba Alan Mathison Turing, y en él presentaba una nueva propuesta de caracterización del concepto intuitivo de "función calculable en la práctica". En el último momento conoció el trabajo de Church y añadió un apéndice a su artículo en el que esbozaba una demostración de que las funciones calculables en el sentido de Church eran las mismas que las calculables según su propia definición.

Se tenían entonces tres definiciones equivalentes de funciones definidas sobre los números naturales y con valores naturales que supuestamente caracterizaban la noción intuitiva de "función calculable" (la de Gödel-Herbrand, la de Church y la de Turing), pero la de Turing era, con diferencia, la más convincente de todas. Se basaba en lo que Turing llamó "máquinas calculadoras", pero que hoy se conocen como *máquinas de Turing.* Una máquina de Turing no es una máquina en el sentido usual de la palabra, sino un concepto matemático que simula el comportamiento de una máquina. Turing presenta a sus máquinas como un análogo de "un hombre realizando un cálculo", pero unos años más tarde todo el mundo vería en una máquina de Turing una versión ideal de un ordenador. (Esto no era posible en 1936 porque no existían aún los ordenadores.)

En términos de ordenadores, el cálculo λ de Church puede verse como un lenguaje de programación ideal de bajo nivel (en el sentido técnico de que admite muy pocas operaciones básicas, pero que con ellas se pueden definir conceptos y operaciones más complejas hasta convertirlo en un lenguaje de alto nivel, en el que se puede programar cualquier cosa), mientras que las máquinas de Turing eran modelos de ordenadores, dotados, eso sí, de infinita memoria, para no descartar como no computables funciones cuyo cálculo excediera una cantidad limitada de memoria fijada de antemano.

El concepto de máquina de Turing es muy simple: una máquina de Turing consta de una cinta infinita (sin principio ni fin) dividida en casillas, y cada casilla puede estar en blanco o bien tener impreso un signo de entre un número finito de signos posibles, digamos $s_1, \ldots, s_n$, que constituyen el *alfabeto de la máquina.* Sólo un número finito de casillas de la cinta pueden tener un signo impreso. Podemos representar así la cinta de una máquina de Turing:

	s_1			s_2	s_2	s_3		s_1	s_1			s_4	s_1		

En cada instante, sólo una casilla de la cinta está "dentro" de la máquina, y a esta casilla se la llama la *casilla escrutada.* La máquina puede estar en un número finito de estados distintos $q_0, \ldots, q_m$, de los cuales, al menos uno, por ejemplo q_0 es un *estado pasivo* y exactamente uno, por ejemplo q_1 es el *estado inicial,* que es el estado en el que se encuentra la máquina cuando empieza a actuar. Si la máquina se encuentra en un estado pasivo, no hace nada. Pero, si se encuentra en un estado activo, realiza un *acto,* que depende del estado q_i en que se encuentra y del signo s_j impreso en la casilla escrutada (que puede ser s_0, interpretado como que la casilla está en blanco). Un acto consiste en:

- Imprimir un signo s_k en la casilla escrutada.
- Mover la casilla escrutada un lugar a la izquierda o a la derecha (o no realizar ningún movimiento).
- Cambiar a un nuevo estado.

De este modo, un *programa* (o *matriz de transiciones*) para una máquina de Turing es una función que a cada par posible (q_i, s_j) de un estado y un signo de la casilla escrutada le asocia un signo impreso, un movimiento y un nuevo estado. La tabla siguiente muestra la matriz de transiciones de una máquina de Turing B con tres estados activos q_1, q_2, q_3 y un alfabeto de un único signo 1, aparte del signo 0 que representa la casilla en blanco:

B	q_1	q_2	q_3
0	$1Dq_2$	$0Dq_3$	$1Iq_3$
1	$1Rq_0$	$1Dq_2$	$1Iq_1$

Por ejemplo, si la máquina se encuentra en el estado q_1 y el signo de la casilla escrutada es 0, realiza el acto $1Dq_2$, que significa: imprimir un 1, mover la cinta para que la nueva casilla escrutada sea la de la Derecha de la actual y pasar al estado q_2.

El lector puede comprobar el funcionamiento de la máquina B cuando empieza con la cinta en blanco (en el estado inicial q_1) escrutando la casilla indicada con [0]:

0	q_1	0	[0]	0	0	0	0
1	q_2	0	1	[0]	0	0	0
2	q_3	0	1	0	[0]	0	0
3	q_3	0	1	[0]	1	0	0
4	q_3	0	[1]	1	1	0	0
5	q_1	[0]	1	1	1	0	0
6	q_2	1	[1]	1	1	0	0
7	q_2	1	1	[1]	1	0	0

8	q_2	1	1	1	[1]	0	0
9	q_2	1	1	1	1	[0]	0
10	q_3	1	1	1	1	0	[0]
11	q_3	1	1	1	1	[0]	1
12	q_3	1	1	1	[1]	1	1
13	q_1	1	1	[1]	1	1	1
14	q_0	1	1	1	[1]	1	1

Según hemos indicado, el acto correspondiente a esta situación es imprimir un 1, moverse a la derecha y pasar al estado q_2, que corresponde a la segunda línea de la tabla (donde está el resultado del primer paso). Según el programa, cuando en el estado q_2 se lee un 0, se imprime un 0, se mueve a la derecha y se pasa al estado q_3. Si el lector sigue ejecutando la máquina, verá que tras decimotercer paso se llega al estado q_1 con un 1 en la casilla escrutada, por lo que el acto es imprimir un 1, moverse a la derecha y pasar al estado pasivo q_0, con lo que la máquina se detiene al cabo de 14 pasos, dejando 6 unos impresos en la cinta.

Una máquina de Turing no es nada más que esto, y puede usarse para hacer cálculos matemáticos. No vamos a seguir de cerca el artículo de Turing porque él usaba sus máquinas para calcular las expansiones decimales binarias de números reales (y llamaba números computables a aquellos cuyas cifras decimales podía calcular una máquina de Turing). Fue Kleene quien aplicaría las máquinas de Turing al cálculo de funciones $f(x_1, \ldots, x_n)$ que toman argumentos naturales y dan valores naturales. Para ello Kleene adoptaría el convenio de representar una sucesión finita de números naturales $x_1, \ldots, x_n$ en la cinta de una máquina de Turing eligiendo un signo s cualquiera del alfabeto y formando como n series de $x_1 + 1, x_2 + 1, \ldots, x_n + 1$ signos s separados por un espacio en blanco. Por ejemplo, la sucesión $2, 0, 3$ se representa así:

		s	s	s		s		s	s	s	s		

Además convenimos en que, para que una máquina de Turing empiece a calcular con estos datos, se la situará de modo que la casilla escrutada sea la que ocupa la última s del último número (la que en la figura está marcada con una barra). Decimos que una máquina de Turing *computa* una función $f(x_1, \ldots, x_n)$ si cuando empieza con los números $x_1, \ldots, x_n$ según el convenio que acabamos de describir y el resto de la cinta en blanco, termina con $x_1, \ldots, x_n, f(x_1, \ldots, x_n)$ y el resto de la cinta en blanco.[96]

En el apéndice de su artículo, Turing esbozó la prueba (aunque en otros términos, pues este convenio es posterior) de que las funciones que pueden calcularse de este modo mediante una máquina de Turing coinciden con las funciones que Church consideraba calculables (y, por lo tanto, con las funciones recursivas de Gödel y Herbrand).

Uno de los resultados más notables de Turing en su primer artículo sobre sus máquinas es la existencia de una máquina de Turing universal. Es claro que la matriz de transiciones de una máquina de Turing puede codificarse en forma de un número natural, y Turing demostró que existe una máquina $\mathcal{U}$ tal que, si empieza con un número natural en la cinta que codifica a (la matriz de transiciones de) una máquina de Turing M, se comporta igual que M cuando comienza con la cinta en blanco. Una ligera generalización permite construir una máquina $\mathcal{U}$ tal que si empieza con una cinta que contiene los datos M, D, donde M es un número natural que codifica a una máquina de Turing M y D es una sucesión finita de números naturales, se comporta igual que la máquina M cuando empieza con los datos D.

Cuando decimos "se comporta igual" hay que entender que si M no se detiene, la máquina universal tampoco lo hace, porque una máquina de Turing no tiene por qué detenerse nunca. Por ejemplo, cualquier máquina que tenga en su matriz de transiciones las asignaciones $(q_1, 0) \mapsto (1Dq_1)$, $(q_1, 1) \mapsto (1Dq_1)$ se desplazará hacia la derecha escribiendo unos en la cinta sin parar. Turing demostró que el *problema de la detención* no es resoluble, es decir:

> No existe ningún algoritmo que determine si una máquina M se detiene o no cuando empieza con unos datos D en la cinta.

En efecto, admitiendo que las funciones calculables en la práctica son las que pueden calcular las máquinas de Turing, si existiera un algoritmo para determinar si una máquina M se para o no cuando empieza con los datos D en la cinta, la función que —identificando M con un número natural que codifique su matriz de transiciones— asigna a M, D el valor 1 o 0 según si la máquina M se detiene o no cuando empieza con los datos D sería calculable por una máquina de Turing $\mathcal{D}$.

Ahora observamos que las máquinas de Turing pueden encadenarse. Cuando la matriz de transiciones de $\mathcal{D}$ establece que tiene que pasar a un estado pasivo, podemos modificarla para que pase al estado inicial de la máquina siguiente C (la raya indica que no importa qué instrucción tenga en esa posición, porque no se va a usar):

C	q_1	q_2	q_3
0	$-$	$0Dq_0$	$1Dq_3$
1	$1Iq_2$	$1Dq_3$	$1Dq_3$

Si la máquina M se detiene cuando empieza con D, la máquina $\mathcal{D}$ terminará con $M, D, 1$ en la cinta, es decir, con 1[1] a la derecha y la máquina C verá el primer 1, pasará al estado 3 y se pondrá a escribir unos sin parar. En cambio, si M no se detiene cuando empieza con D, la máquina $\mathcal{D}$ terminará con $M, D, 0$ en la cinta, es decir, con 0[1] a la derecha, y la máquina C, al ver el primer 0, se detendrá.

En definitiva, la concatenación $\mathcal{D}^* = \mathcal{D}C$ se detiene cuando empieza con M, D si y sólo si M no se detiene cuando empieza con D.

Por otro lado, no es difícil definir una máquina C^* que copia un número dado, es decir, que cuando empieza con un número D en la cinta, se detiene con D, D en la cinta. Si llamamos $\mathcal{D}^{**} = C^*\mathcal{D}^*$, tenemos una máquina que, cuando empieza con un número M que codifica a una máquina de Turing, hace actuar $\mathcal{D}^*$ sobre M, M, la cual se detiene si y sólo si M no se detiene cuando empieza con el número M en la cinta.

[96] Un resultado técnico que resulta útil es que si una máquina de Turing calcula una función f, es posible definir otra máquina de Turing que calcula la misma función y además nunca examina las casillas de la cinta situadas a la izquierda de los datos (o, más exactamente, a la izquierda de las dos primeras casillas en blanco a la izquierda de los datos, para que pueda saber dónde terminan los datos), con lo cual es irrelevante que la cinta esté o no en blanco a la izquierda de los datos. Y podemos restringirnos a considerar máquinas con esta propiedad.

Pero entonces, ¿qué hará $\mathcal{D}^{**}$ cuando empiece con el número $\mathcal{D}^{**}$ que la codifica a ella misma? Debería detenerse si y sólo si la máquina $\mathcal{D}^{**}$ no se detiene cuando empieza con $\mathcal{D}^{**}$ en la cinta. Esto es imposible, lo cual demuestra que no existe la máquina $\mathcal{D}$, es decir, que no existe ningún algoritmo para decidir si una máquina de Turing se detiene o no cuando empieza con unos datos dados.

Esto implica una versión más fuerte:

> No existe ningún algoritmo que determine si una máquina de Turing se detiene o no cuando empieza con la cinta en blanco.

En efecto, si existiera tal algoritmo, para saber si una máquina de Turing M se detiene o no cuando empieza con unos datos D en la cinta, bastaría aplicar el algoritmo a la máquina de Turing M' que escribe los datos D cuando empieza con la cinta en blanco y luego, deja actuar a la máquina M.

A su vez, Turing relaciona el problema de la detención con el problema de la decisión y, del hecho de que el primero no tiene solución, deduce que el segundo tampoco. No detallamos el argumento de Turing porque hay otros más simples. Por ejemplo:

> Si T es una teoría aritmética consistente, el problema de la decisión es insoluble para T, es decir, que no existe ningún algoritmo que determine si una fórmula dada es o no un teorema de T.

Demostración: Supongamos que existe tal algoritmo. Cada fórmula ϕ puede codificarse con un número natural $\ulcorner\phi\urcorner$, y entonces (aceptando, como supone Turing, que las funciones calculables en la práctica son calculables por una máquina de Turing y, por lo tanto, recursivas) tendríamos que la relación R que cumple un número natural si es el código de una fórmula demostrable en T sería recursiva, luego representable en T (véase la sección 50).

Esto significa que existe una fórmula ϕ de T tal que:

1. Si la fórmula α es demostrable en T, entonces en T se puede demostrar $\phi(\ulcorner\alpha\urcorner)$.
2. Si la fórmula α no es demostrable en T, entonces en T se puede demostrar $\neg\phi(\ulcorner\alpha\urcorner)$.

Aplicando el lema de autorreferencia (página 106), existe una fórmula ψ tal que en T se demuestra

$$\psi \leftrightarrow \neg\phi(\ulcorner\psi\urcorner).$$

Así, si ψ no se puede demostrar en T, entonces $\neg\phi(\ulcorner\psi\urcorner)$ se puede demostrar en T, con lo que ψ (que es equivalente) también se puede demostrar en T y tenemos una contradicción.

Por lo tanto ψ se tiene que poder demostrar en T, pero entonces $\phi(\ulcorner\psi\urcorner)$ se puede demostrar en T, luego $\neg\psi$ (que es equivalente) también se puede demostrar en T, y así T es contradictoria. ∎

Church fue uno de los revisores del artículo de Turing, y antes de que terminara el año Turing estaba ya en Princeton para doctorarse bajo la dirección de Church. Para éste, el trabajo de Turing ya no dejaba margen de duda para la identificación de las funciones calculables en cualquiera de los sentidos técnicos equivalentes y las funciones calculables en la práctica.

Sin embargo, no todos estaban de acuerdo. Poco antes de que se publicara el artículo de Turing, Emil Leon Post publicó otro artículo titulado *Procesos combinatorios finitos-Formulación 1* donde definía un concepto muy similar al de máquina de Turing y llegaba a resultados análogos que lo llevaban a conjeturar que las funciones que cumplían lo que él llamaba "formulación 1" coincidían con las funciones calculables en la práctica, pero termina su artículo insistiendo en que identificar las funciones calculables en cualquiera de los sentidos equivalentes conocidos y el concepto intuitivo de función calculable en la práctica debe tomarse como una hipótesis de trabajo y no como una definición:

> *En realidad, el trabajo ya realizado por Church y otros lleva esta identificación considerablemente más allá del* status *de hipótesis de trabajo. Pero enmascarar esta identificación bajo una definición oculta el hecho de que se ha hecho un descubrimiento fundamental en las limitaciones del poder matematizador del* Homo sapiens *y nos ciega ante la necesidad de su verificación continua.*

Es decir, por una parte, definir una función calculable como una función λ-definibile en el sentido de Church, o como una función recursiva, o como una función calculable por una de las máquinas de Post, suponía trivializar un hecho nada trivial, que expresa las limitaciones de los cálculos matemáticos y, por otra parte, supondría perder de vista que cabe la posibilidad de que se descubrieran en cualquier momento nuevas técnicas de cálculo explícito que no cupieran en las definiciones consideradas en ese momento. Post afirmaba a continuación que, incluso si la hipótesis se podía en algún momento dar por confirmada, eso no la convertiría en un axioma o una definición, sino más bien en una "ley natural". Church criticó duramente esta idea.

En otro orden de cosas, en **1936** Rosser publicó un artículo titulado *Extensiones de unos teoremas de Gödel y Church,* donde demostraba que el primer teorema de incompletitud de Gödel era válido sin la hipótesis de ω-consistencia.

Volviendo a la computabilidad, en **1937** Turing publicó un artículo titulado *Computabilidad y λ-definibilidad* en el que detallaba la demostración de que las funciones computables por máquinas de Turing coinciden con las funciones λ-definibles. Más precisamente, demostraba que las funciones λ-definibles son Turing-computables y que las funciones Turing-computables son recursivas (lo que da la equivalencia, porque Kleene ya había demostrado que las funciones recursivas son λ-definibles).

Para entonces seguían sin existir ordenadores,[97] pero si hubieran existido habría sido evidente que el argumento que daba Turing para probar que toda función Turing-computable es recursiva se podía aplicar en general a toda función calculable por cualquier ordenador, por cualquier dispositivo que sólo admita un número finito de estados que determinen su comportamiento juntamente con la lectura de una memoria potencialmente ilimitada (no necesariamente accesible secuencialmente, como la cinta de una máquina de Turing). Y entonces nadie habría cuestionado que las funciones Turing-computables coinciden con las funciones que puede calcular cualquier ordenador y, por consiguiente, con las funciones calculables en la práctica.

62 La teoría de von Neumann-Bernays II Hasta el momento, la única teoría de conjuntos que manejaban los matemáticos era ZFC, pues los *Principia Mathematica* eran demasiado exóticos y no interesaban más que a unos pocos lógicos (y en muchos casos sólo porque Gödel los había usado para exponer sus teoremas de incompletitud) y la teoría de funciones de von Neumann era demasiado atípica. Estaba la reformulación de Bernays, mucho más natural, pero no fue publicada hasta **1937** en un artículo titulado *Un sistema de teoría axiomática de conjuntos-Parte I.* Bernays pone por delante su platonismo:

> *La teoría no se concibe como un mero formalismo, sino más bien siguiendo el método usual de la teoría axiomática elemental, donde tratamos con proposiciones que se entienden con un significado inherente, y donde los nombres para los tipos de individuos y para los predicados fundamentales ya sugieren la referencia al ámbito de los hechos que se busca axiomatizar.*

Como ya sabemos, la teoría de Bernays distingue entre conjuntos y clases. Bernays la explica así:

> *Según la idea principal de la teoría de conjuntos de von Neumann, debemos manejar dos tipos de individuos, que podemos distinguir como conjuntos y clases. La distinción puede entenderse de la siguiente manera: un conjunto es una multitud que forma una entidad propia, mientras que una clase es un predicado considerado sólo con respecto a su extensión.*

Quiere decir que los conjuntos son cosas, mientras que las clases son una forma de referirse a propiedades de las cosas (de los conjuntos). Por ejemplo, la clase Ω de todos los ordinales no es una "cosa", es una propiedad que pueden tener los conjuntos, la propiedad de "ser un ordinal", de modo que escribir $x \in \Omega$ (o $x\,\eta\,\Omega$, como escribía Bernays para dejar claro que hablamos de pertenencia de un conjunto a una clase) sólo es una forma conveniente de decir que el conjunto x tiene la propiedad de ser un ordinal.

En esta primera parte, Bernays sólo daba los axiomas básicos de la teoría: dos axiomas de extensionalidad (uno para conjuntos y otro para clases), dos axiomas de formación de conjuntos (uno que afirma la existencia del conjunto vacío y otro que afirma que, dados dos conjuntos x, u, existe $x \cup \{u\}$) y nueve axiomas de existencia de clases, con los que demuestra el esquema teoremático de comprensión, del que ya hemos hablado:

[97] Fue en 1938 cuando el ingeniero alemán Konrad Zuse construyó la primera calculadora eléctrica parcialmente programable, la Z1, aunque tenía muchos fallos, y en 1943 construyó la Z3, que fue el primer ordenador que, al menos en teoría, podía calcular cualquier función Turing-computable. En 1944 IBM construyó la *Harvard Mark 1,* que, salvando las distancias, ya era equiparable a un ordenador en el sentido moderno de la palabra. Los primeros lenguajes de programación de alto nivel, que evidenciaban que un ordenador podía calcular cualquier cosa calculable, no aparecieron hasta 1949.

Si $\phi(u)$ es una fórmula (con posibles parámetros) en la que todos los cuantificadores se refieren a conjuntos (son de la forma "para todo conjunto" o "existe un conjunto", pero nunca de la forma "para toda clase" o "existe una clase"), entonces la fórmula siguiente es un teorema:

$$\bigvee Y \bigwedge u(u \in Y \leftrightarrow \phi(u)).$$

El axioma de extensionalidad para clases implica que la clase Y es única, y es la que habitualmente se representa por $\{u \mid \phi(u)\}$.

Sin más detalles, las ventajas de esta teoría no resultaban nada apreciables para los matemáticos en general.

63 Los Nuevos Fundamentos de Quine En 1924, Whitehead, a sus 63 años, había aceptado una plaza de profesor de filosofía en Harvard, y allí había dirigido la tesis a Willard Van Orman Quine, leída en 1932 y que versaba sobre la lógica de los *Principia Mathematica.* En **1937** Quine publicaba un artículo titulado *Nuevos fundamentos para la lógica matemática,* en el que proponía una forma de eliminar la lógica de tipos de los *Principia* conservando la idea subyacente. Apenas desarrolló su propuesta (apenas le dedica las dos últimas páginas de su artículo), pero ésta consistía en partir únicamente de dos axiomas (o, mejor dicho, de un axioma y de un esquema de axioma):

Extensionalidad Si dos conjuntos tienen los mismos elementos, entonces son iguales:

$$\bigwedge xy(\bigwedge u(u \in x \leftrightarrow u \in y) \to x = y)$$

Comprensión Para toda fórmula estratificada $\phi(x)$, la fórmula siguiente es un axioma:

$$\bigvee y \bigwedge x(x \in y \leftrightarrow \phi(x)),$$

es decir, existe el conjunto de todos los conjuntos que cumplen $\phi(x)$, que es único por el axioma de extensionalidad y que podemos representar por $\{x \mid \phi(x)\}$.

La clave está en el requisito de que la fórmula $\phi(x)$ esté estratificada. Sin él, podríamos definir, por ejemplo, el conjunto $\{x \mid x \notin x\}$ y tendríamos la paradoja de Russell. ¿Y en qué consiste la estratificación?

Una fórmula está estratificada si podemos asignar un número a cada variable (llamado su *tipo*) de modo que en cada fórmula atómica $x = y$ las dos variables tengan el mismo tipo, mientras que en cada fórmula $x \in y$ la x tenga tipo una unidad inferior a la y.

Por ejemplo, el axioma de extensionalidad es una fórmula estratificada, como muestra la asignación de tipos siguiente:

$$\bigwedge x_1 y_1(\bigwedge u_0(u_0 \in x_1 \leftrightarrow u_0 \in y_1) \to x_1 = y_1).$$

En cambio, obviamente, la fórmula $x \notin x \equiv \neg x \in x$ no está estratificada, por lo que no define un conjunto y la paradoja de Russell no da lugar a ninguna contradicción.

La teoría propuesta por Quine pasó a ser conocida como NF (por Nuevos Fundamentos), y lo más sorprendente es que permite definir el conjunto de todos los conjuntos: $V = \{x \mid x = x\}$, ya que la fórmula $x = x$ sí que está estratificada. En particular tenemos que $V \in V$.

Para todo conjunto X, podemos definir

$$\mathcal{P}X = \{Y \mid \bigwedge u_0(u_0 \in Y_1 \to u_0 \in X_1)\},$$

donde los subíndices prueban que la fórmula está estratificada.[98]

En particular está definido el conjunto $\mathcal{P}V$, de todos los subconjuntos de V, y es inmediato que $\mathcal{P}V = V$.

Todo apunta entonces a que la teoría NF es contradictoria, porque en ella se tiene que poder demostrar la paradoja de Cantor, pero no es así. En efecto, si representamos, por $|X|$ al cardinal de un conjunto X, en NF no se puede demostrar que $|X| < |\mathcal{P}X|$. ¡Ni siquiera se puede demostrar que $|X| \leq |PX|$!

[98] Nótese que Y_1 sólo indica que a la variable Y le asignamos el tipo 1. No ha de entenderse como que Y_1 es una variable distinta de Y, como es frecuente en otros contextos.

En efecto, el argumento usual que demuestra que $|X| \leq |\mathcal{P}X|$ consiste en considerar la aplicación inyectiva $f : X \longrightarrow \mathcal{P}X$ dada por $u \mapsto \{u\}$, es decir, el conjunto

$$f = \{z \mid \bigvee u(u \in X \wedge z = (u, \{u\})\} = \{z \mid \bigvee uv(u \in X \wedge v = \{u\} \wedge z = (u, v))\} =$$
$$\{z \mid \bigvee u_0 v_1(u_0 \in X_1 \wedge \bigwedge w_0(w_0 \in v_1 \leftrightarrow w_0 = u_0) \wedge z = (u_0, v_1))\}.$$

En la última expresión hemos tratado de estratificar la fórmula que define a f, pero no hemos acabado, porque necesitamos que el tipo de v sea una unidad mayor que el de u, pero es imposible estratificar $z = (u, v)$ sin asignar el mismo tipo a u y a v. En efecto:

$$z = (u, v) = \{\{u\}, \{u, v\}\} \leftrightarrow \bigwedge s(s \in z \leftrightarrow \bigwedge t(t \in s \leftrightarrow t = u) \vee \bigwedge t(t \in s \leftrightarrow t = u \vee t = v)),$$

y para estratificar $t = u \vee t = v$ necesitamos que u y v tengan el mismo tipo. Por lo tanto, no podemos[99] definir f en NF.

Para enunciar el teorema de Cantor en NF tenemos que definir el conjunto de todos los subconjuntos de X con un elemento:

$$\mathcal{P}_1 X = \{\{x\} \mid x \in X\} = \{z \mid \bigvee x_0(x_0 \in X_1 \wedge \bigwedge u_0(u_0 \in z_1 \leftrightarrow u_0 = x_0))\},$$

y así es inmediato que $\mathcal{P}_1 X \subset \mathcal{P}X$, por lo que $|\mathcal{P}_1 X| \leq |\mathcal{P}X|$. Con esto se puede demostrar:

Teorema de Cantor Para todo conjunto X, se cumple que $|\mathcal{P}_1 X| < |\mathcal{P}X|$.

Demostración: La prueba es exactamente igual que la del teorema de Cantor: si existiera una biyección $f : \mathcal{P}_1 X \longrightarrow \mathcal{P}X$, podríamos definir el conjunto

$$R = \{x \mid x \in X \wedge \{x\} \not\subset f(\{x\})\}.$$

Se puede comprobar que la definición es correcta, porque la fórmula que define a R está estratificada, y por lo tanto $R \in \mathcal{P}X$, luego existe un $x \in X$ tal que $f(x) = R$. Este conjunto x debería cumplir que

$$x \in R \leftrightarrow \{x\} \subset R \leftrightarrow \{x\} \subset f(\{x\}) \leftrightarrow x \notin R,$$

con lo que tenemos una contradicción. ∎

Sin embargo, no es cierto en general que $|X| = |\mathcal{P}_1 X|$. Un ejemplo es el conjunto V de todos los conjuntos, para el que $|V| = |\mathcal{P}V| > |\mathcal{P}_1 V|$. Esto demuestra que la biyección $f : V \longrightarrow \mathcal{P}_1 V$ dada por $x \mapsto \{x\}$ no existe.

No damos más detalles sobre NF. Lo visto es suficiente para que el lector de haga una idea de lo "pintoresca" que es esta teoría y no hace falta mucha perspicacia para adivinar que ningún matemático no interesado por las curiosidades lógicas se la iba a tomar en serio. Pese a todo, Quine parece hablar en serio cuando, al comparar su teoría con la de Zermelo, dice:

> *Pero estos métodos conllevan la mayoría de las incómodas limitaciones que conlleva la teoría de tipos. El método que propongo para evitar las contradicciones, si es que las evita, parece ser el menos restrictivo sugerido hasta ahora.*

Al parecer, para Quine, unos axiomas que niegan la existencia de la aplicación $x \mapsto \{x\}$ son menos restrictivos que otros que niegan la existencia del conjunto de todos los conjuntos (para entender esto hay que recordar que Quine era filósofo).

64 Funciones recursivas parciales En **1937** Church y Kleene publicaron un artículo titulado *Definiciones formales en la teoría de ordinales,* en el que iniciaron el estudio de los ordinales recursivos, es decir, de los buenos órdenes que se pueden definir en el conjunto de los números naturales mediante relaciones recursivas, relaciones calculables en la práctica. En particular definieron lo que hoy se conoce como el ordinal de Church-Kleene ω_1^{CK}, que es el menor ordinal no recursivo.

En **1938** continuaron este estudio con los artículos *La segunda clase numérica constructible* (de Church) —en el que presenta a los ordinales constructibles como un análogo efectivo de lo que Cantor había llamado la segunda clase numérica, es decir, el conjunto de los ordinales numerables— y *Sobre la notación para números ordinales* (de Kleene), en el que prueba algunos resultados profundos de la teoría de la recursión. No vamos a entrar en ellos, pero sí en un concepto básico que introduce en este trabajo y que es fundamental en la teoría: el de las funciones recursivas parciales. Más adelante Kleene diría:

[99] Este argumento sólo muestra que no podemos definir f aplicando el axioma de comprensión de forma natural, pero la prueba de que f no puede definirse de ningún modo nos la da el teorema de Cantor (véase la observación posterior).

Esta generalización (¿debería decir "parcialización"?) de la noción de función recursiva general había sido evitada deliberadamente por Church 1936 y Turing 1936-37.

Sin embargo, la noción de "función parcial" es esencial en la teoría de la computación, y no se podía evitar durante mucho más tiempo. Si queremos hablar de "funciones calculables mediante un algoritmo", tenemos que enfrentarnos al hecho de que cuando un algoritmo arbitrario empieza con unos datos dados, cabe la posibilidad de que el algoritmo entre en un bucle infinito y nunca llegue a detenerse (sin perjuicio de que, para algoritmos concretos, sea posible demostrar que no puede darse ese caso).

Si nos fijamos en la definición de función recursiva, veremos que esta posibilidad de que el cálculo de una función no termine nunca está contemplada en la definición por minimización. Hemos establecido que una función $f(x_1,\dots,x_n)$ está definida por minimización a partir de otra función $g(x_1,\dots,x_n,x)$ si viene dada por

$$f(x_1,\dots,x_n) = \text{el mínimo } x \text{ tal que } g(x_1,\dots,x_n,x) = 0,$$

y en la definición hemos incluido el requisito de que, para todos los valores $x_1,\dots,x_n$, siempre exista un x que cumpla $g(x_1,\dots,x_n,x) = 0$, pero esta exigencia es delicada, porque, aunque la función g sea recursiva y dispongamos de un algoritmo para calcularla en la práctica para todos los valores $x_1,\dots,x_n,x$, eso no nos garantiza que podamos asegurar si siempre va a existir un x que cumpla lo requerido. Si eliminamos esta exigencia, llegamos a la definición de función recursiva parcial.

En primer lugar, hablando siempre de funciones $f(x_1,\dots,x_n)$ definidas sobre números naturales y que toman valores naturales, una *función parcial* es simplemente una función que no está definida sobre todos los valores posibles $(x_1,\dots,x_n)$ de argumentos, sino que puede quedar indefinida en algunos de ellos (incluso en todos). Y las funciones *recursivas parciales* se definen como sigue:

1. La función cero, dada por $c(n) = 0$ es recursiva parcial.
2. La función sucesor, dada por $s(n) = n+1$ es recursiva parcial.
3. Las proyecciones, dadas por $p_i^n(x_1,\dots,x_n) = x_i$ son recursivas parciales.
4. Si $g_1(x_1,\dots,x_n),\dots,g_m(x_1,\dots,x_n),h(x_1,\dots,x_m)$ son funciones recursivas parciales, la función dada por
$$f(x_1,\dots,x_n) = h(g_1(x_1,\dots,x_n),\dots,g_m(x_1,\dots,x_n))$$
es recursiva parcial, entendiendo que $f(x_1,\dots,x_n)$ está definida si lo están todas las funciones
$$g_1(x_1,\dots,x_n),\quad \dots,\quad g_m(x_1,\dots,x_n),\quad h(g_1(x_1,\dots,x_n),\dots,g_m(x_1,\dots,x_n))$$
(y se dice que está definida por *composición parcial* a partir de las funciones dadas).
5. Si $g(x_1,\dots x_n),h(x_1,\dots,x_n,x,y)$ son funciones recursivas parciales, también lo es la función dada por
$$\begin{aligned} f(x_1,\dots,x_n,0) &= g(x_1,\dots,x_n),\\ f(x_1,\dots,x_n,x+1) &= h(x_1,\dots,x_n,x,f(x_1,\dots,x_n,x)),\end{aligned}$$
entendiendo que $f(x_1,\dots,x_n,x)$ está definida si lo están todas las funciones
$$\begin{aligned} f(x_1,\dots,x_n,0) &= g(x_1,\dots,x_n),\\ f(x_1,\dots,x_n,1) &= h(x_1,\dots,x_n,0,f(x_1,\dots,x_n,0)),\\ &\vdots \qquad\quad \vdots\\ f(x_1,\dots,x_n,x) &= h(x_1,\dots,x_n,x-1,f(x_1,\dots,x_n,x-1)),\end{aligned}$$
(y se dice que está definida por *recursión parcial* a partir de las funciones dadas).
6. Si $g(x_1,\dots,x_n,x)$ es una función recursiva parcial, también lo es la función dada por
$$f(x_1,\dots,x_n) = \text{el mínimo } x \text{ tal que } g(x_1,\dots,x_n,x) = 0,$$
entendiendo que $f(x_1,\dots,x_n)$ está definida si lo están
$$g(x_1,\dots,x_n,0)\neq 0,\quad \dots,\quad g(x_1,\dots,x_n,x-1)\neq 0,\quad g(x_1,\dots,x_n,x) = 0$$
y se dice que f está definida por *minimización parcial* a partir de la función dada.

Así, la diferencia esencial con la definición de función recursiva es que admitimos que toda función recursiva parcial defina una función por minimización, sin exigir que siempre existan los mínimos necesarios. Cuando no existen, la función definida por minimización queda indefinida.

De este modo, las funciones recursivas parciales se corresponden mucho más fielmente con las funciones calculables mediante un algoritmo, porque contemplan la posibilidad de que un algoritmo no termine nunca.

En estos términos podemos decir que toda máquina de Turing M calcula una función parcial f de cualquier número prefijado n de argumentos. Si M empieza a actuar con los números $x_1, \ldots, x_n$ en la cinta (de modo que la casilla escrutada es la de más a la derecha ocupada por los datos) y el resto de la cinta en blanco, y se detiene con los números $x_1, \ldots, x_n, k$ en la cinta y el resto en blanco, entonces, por definición, $f(x_1, \ldots, x_n) = k$, mientras que si M se detiene con la cinta en otra situación o no se detiene, entonces $f(x_1, \ldots, x_n)$ no está definida.

Si llamamos *funciones parciales Turing-computables* a las funciones parciales computables de este modo mediante una máquina de Turing, éstas resultan ser las mismas que las funciones recursivas parciales y la demostración es una variación mínima de la correspondiente a *funciones totales* (es decir, definidas para todos los argumentos).

Notemos que esto no corrige la convicción de Church de que las funciones calculables en la práctica mediante algoritmos coinciden con las funciones recursivas (o λ-definibles o Turing-computables), sino que meramente la extiende a funciones parciales y a algoritmos parciales (que pueden no terminar).

Observemos que si en la definición de función recursiva parcial eliminamos la definición por minimización parcial, lo que obtenemos es la definición de función recursiva primitiva, pues una función definida exclusivamente por composición parcial o recursión parcial (a partir de las funciones cero, sucesor y proyecciones) es necesariamente total.

Además, en términos de computabilidad, la diferencia entre las funciones recursivas primitivas y las funciones recursivas parciales (es decir, entre las que pueden definirse sin minimización y las que la requieren) tiene una interpretación muy simple:

- Una función es recursiva (pero no recursiva primitiva) cuando para programar su cálculo es necesario usar bucles de la forma WHILE, es decir, bucles que tienen que repetirse hasta que deje de cumplirse una determinada condición, pero de modo que no existe *a priori* ninguna garantía de que vaya a dejar de cumplirse nunca. Si nunca deja de cumplirse, el algoritmo entra en un bucle infinito y no termina nunca.

  Esto se corresponde con el uso de la minimización en la definición de una función recursiva. Salvo que podamos garantizar que siempre va a existir el mínimo requerido, puede ocurrir que una función definida por minimización quede indefinida para algunos argumentos.

- Una función es recursiva primitiva cuando puede programarse su cálculo usando a lo sumo bucles de tipo FOR, es decir, bucles en los que una variable tiene que tomar todos los valores posibles entre un mínimo y un máximo especificados de antemano, de modo que tenemos la garantía de que el bucle siempre terminará.

Para terminar observemos que, al eliminar en la definición de minimización parcial el requisito no comprobable en general de que la minimización siempre esté definida, desaparece el problema que señalábamos en la página 133, por el que no podemos enumerar explícitamente las funciones recursivas. En efecto, las definiciones de funciones recursivas parciales pueden ser ordenadas para determinar una enumeración $f_0,\ f_1, f_2,\ \ldots$ de todas las funciones recursivas parciales.

Ahora, si tratamos de reproducir el argumento dado en la página 96 que prueba la existencia de una función recursiva que no es recursiva primitiva, tenemos que restringir la enumeración a funciones con un argumento (lo cual siempre es factible en la práctica) y definir la función (parcial) dada por $f(n) = f_n(n) + 1$ (cuando $f_n(n)$ está definido), pero no podemos concluir que se trata de una función "nueva" no incluida en la sucesión dada. Al contrario, dicha función f es calculable en la práctica y nada impide que exista un k tal que $f = f_k$.

La contradicción del argumento de la página 96 venía de razonar que tiene que ser $f_k(k) = f(k) = f_k(k) + 1$, pero en nuestro contexto cabe otra posibilidad que no da lugar a contradicción alguna, y es simplemente que la función parcial f_k no tiene por qué estar definida en k.

65 La Segunda Guerra Mundial Wilhelm Blaschke era nazi, pero también era amigo de su colega Emil Artin, y en cierta ocasión le había sugerido que mantuviera cerrada la puerta de su aula, para evitar que cualquiera que pasara por el pasillo pudiera oír los comentarios nada agradables sobre los nazis que solía intercalar en sus clases. Artin no era judío, pero su esposa era "de raza mixta en primer grado", porque su padre era judío, y esto hacía que sus hijos fueran a su vez "de raza mixta en segundo grado". En 1937 (a sus 39 años) Artin fue "jubilado forzosamente" y aprovechó la ocasión para emigrar con su familia a los Estados Unidos. Ese mismo año Gentzen ingresó en el Partido Nacionalsocialista Obrero Alemán.

En **1938** Gentzen publicó un artículo titulado *Nueva versión de la prueba de consistencia para la teoría de números elemental,* más detallada y conceptual que la anterior (mucho más próxima a lo que hemos comentado sobre ella en el apartado correspondiente), en la que se pone de manifiesto el papel esencial que desempeña el proceso de eliminación de cortes. También simplificó el uso de los ordinales menores que ϵ_0 usando sistemáticamente su expresión en forma normal de Cantor (mientras en su artículo anterior los representaba como ciertos números decimales), lo que a su vez le permitía identificarlos con números naturales. Sobre la justificación de la inducción hasta ϵ_0 no aportó nada nuevo, sino que se remitió a su artículo anterior.

El filósofo Edgar Zilsel había organizado un seminario en Viena y Gödel dio en él una conferencia en la que expuso una reinterpretación de la demostración de Gentzen conocida como "interpretación sin contraejemplo". Zilsel era judío y marxista, así que cuando ese año Hitler ocupó Austria, huyó a Gran Bretaña. Gödel visitó Princeton de nuevo, e impartió otra charla sobre el mismo tema, pero luego regresó a Viena.

En **1939** Tarski salió de Varsovia para participar en un congreso en la Universidad de Harvard, y unos días después Hitler invadió Polonia, lo que desencadenó la Segunda Guerra mundial. Tarski era judío, así que es muy probable que ese viaje le salvara la vida. Su mujer y sus hijos quedaron en Polonia, aunque lograrían reunirse con él después de la guerra. La mayor parte de su familia moriría durante la ocupación nazi.

Stanisław Ulam se las arregló para salir de Polonia ese año con su hermano y se estableció en los Estados Unidos con la ayuda de von Neumann. El resto de su familia moriría en el holocausto.

Gentzen tuvo que dejar su trabajo junto a Hilbert al ser llamado a filas.

Ese año Alan Turing leyó su tesis doctoral, dirigida por Church en Princeton. En ella Turing definió el concepto de "función calculable en la práctica" como "función calculable con una máquina de Turing", y afirmó sin vacilación que tal definición formal era la correcta, con lo que se unía así a Church, que había afirmado lo mismo hacía ya cinco años (y contradecía la postura de Post, que seguía sosteniendo que la equiparación entre ambos conceptos debía verse como una hipótesis de trabajo). Para entonces Gödel, convencido por el trabajo de Turing, también se había sumado a esta postura. En un artículo de divulgación, Rosser también habló ese año de tres "definiciones" equivalentes.

Luego Turing regresó a Cambridge, donde asistió a un curso impartido por Wittgenstein sobre los fundamentos de las matemáticas, y ambos discutieron abiertamente. Turing se declaró formalista, es decir, consideraba que los conceptos matemáticos no computables estaban vacíos de contenido, pero eran matemáticas válidas igualmente. Wittgenstein, en cambio, sostenía que los matemáticos no descubrían verdades absolutas, sino que las matemáticas eran como una sinfonía, algo que inventa el compositor y que no existía antes de que fuera compuesta. En cuanto Gran Bretaña declaró la guerra a Alemania Turing empezó a trabajar para la Escuela Gubernamental de Código y Cifrado, en un programa con el objetivo de descifrar los códigos secretos alemanes.

66 Nicolas Bourbaki En 1934 dos jóvenes matemáticos franceses, Henri Cartan (de 30 años) y André Weil (de 28), que habían obtenido recientemente plazas de profesores en la universidad de Estrasburgo, debatían sobre cómo enseñar el cálculo diferencial e integral. A ninguno de ellos les gustaba el texto recomendado, el *Curso de Análisis Matemático,* de Édouard Goursat, cuya primera edición databa de 1902 (el primer tomo) y 1917 (el tercero). Goursat tenía entonces 76 años, con lo que sus planteamientos no eran muy modernos. Cartan y Weil iban todas las semanas a París a asistir a un seminario, así que tenían ocasión de verse con antiguos compañeros de la *École Normale Supérieur,* y a finales de año convocaron una reunión en un café para tratar la posibilidad de redactar un nuevo tratado de análisis que sirviera de referencia a las universidades francesas. Los asistentes fueron, además de ellos dos, Claude Chevalley, Jean Delsarte, Jean Dieudonné, René de Possel.

Todos lamentaron que durante la Primera Guerra Mundial, una buena parte de los matemáticos franceses había muerto en las trincheras, por lo que se había perdido prácticamente una generación de matemáticos y los jóvenes estaban siendo instruidos por profesores a punto de jubilarse. La idea de redactar el libro fue acogida

con entusiasmo y se propusieron escribir un libro de unas mil páginas que estaría listo para su publicación en seis meses. Sin embargo, no tardaron en darse cuenta de que había muchas decisiones que tomar y que no iba a ser cosa fácil. El *Comité para el tratado de análisis* (como se llamaban a sí mismos) fue reuniéndose periódicamente. Se añadieron algunos matemáticos más, otros abandonaron, y en 1935 habían decidido que escribirían bajo el pseudónimo de Nicolas Bourbaki.[100] Ese año el tratado de análisis ya había sido sustituido por un proyecto mucho más ambicioso de seis libros, que estarían ordenados de modo que cada uno de ellos hiciera referencia únicamente a resultados de los libros precedentes, pero nunca de los posteriores. Además, todo tenía que desarrollarse desde cero, de modo que tampoco se podría hacer referencia a otros trabajos, salvo en notas históricas. Los libros proyectados eran:

Libro I	Teoría de conjuntos,
Libro II	Álgebra,
Libro III	Topología,
Libro IV	Funciones de una variable real,
Libro V	Espacios vectoriales topológicos,
Libro VI	Integración.

En 1938 se dio título a la obra en su conjunto: *Elementos de matemática,* donde "matemática" en singular era tan inusual en francés como lo es en castellano, pero fue decidido intencionadamente para subrayar el propósito de mostrar las matemáticas como una disciplina unitaria. No era necesario redactar los libros en ese mismo orden, sino que se podían ir elaborando capítulos de cada libro en el orden más conveniente, con tal de que finalmente encajaran y pudieran leerse en orden. La primera publicación tuvo lugar en **1939**, y era un "fascículo de resultados" del futuro libro de teoría de conjuntos, pendiente de desarrollar, que sirviera de referencia a los demás libros.

El fascículo de resultados era una exposición de algo más de treinta páginas de una teoría ingenua de conjuntos (es decir, sin basarse en ninguna axiomática en particular y evitando las paradojas simplemente no metiéndose en ellas). Cumplía a la perfección su papel de servir de referencia para los conceptos conjuntistas básicos y demostraba que la crisis de los fundamentos sólo existía para quien quería creer en ella. Constaba de ocho apartados. El primero se titulaba *Elementos y partes de un conjunto.* Copiamos el principio para que el lector pueda captar el espíritu de la obra:

> *1. Un conjunto está formado por elementos susceptibles de poseer ciertas propiedades y de mantener ciertas relaciones entre sí o con elementos de otros conjuntos.*
>
> *2. Los conjuntos y los elementos se designan en los razonamientos mediante signos gráficos, que generalmente son letras (de diversos alfabetos) o combinaciones de letras y otros signos. Las relaciones entre los elementos de uno o más conjuntos se indican insertando los signos que los designan en un diagrama característico de la relación en cuestión; lo mismo aplica a las propiedades.*
>
> *Una letra puede designar un elemento específico o un elemento arbitrario (también llamado variable o argumento) de un conjunto. Cuando, en una relación, un elemento arbitrario se reemplaza por un elemento específico (del mismo conjunto), decimos que le damos por valor este elemento específico.*

Tras hablar un poco de propiedades y relaciones (no en el sentido conjuntista, sino en el puramente lógico de conexiones entre cosas), presenta los signos $=$, $\neq$ y define los subconjuntos en términos de propiedades:

> *7. Dado un conjunto E y una propiedad de un elemento de E, los elementos de E que poseen esta propiedad forman un nuevo conjunto, que se denomina parte o subconjunto de E. Por lo tanto, dos propiedades equivalentes definen la misma parte de E, y viceversa.*
>
> *Sea A una parte de E; si x es un elemento de E, la propiedad "x pertenece a A" (es decir, x es un elemento de A) se escribe $x \in A$; evidentemente, el conjunto de elementos que poseen esta propiedad no es otro sino A.*
>
> *La negación de esta propiedad se denota $x \notin A$ y se lee "x no pertenece a A" el conjunto de elementos de E que poseen esta propiedad se denomina complementario de A y se denota por $\complement A$ o $E \setminus A$.*

[100] Cuando Weil ingresó en la *École Normale Supérieur,* se organizó a modo de novatada una conferencia en la que un alumno de un curso superior se disfrazó con una barba postiza y enunció en la pizarra varios teoremas absurdos a los que dio nombres de generales franceses, y el último fue el "Teorema de Bourbaki", por el general Charles Soter Bourbaki. Weil recordaba ese nombre y le pareció apropiado para un "falso matemático".

Bourbaki usa el signo $\in$ moderno, y no ϵ, y a continuación incorpora un nuevo signo que se ha convertido en estándar: el signo $\varnothing$ para nombrar al conjunto vacío, que fue una invención de Weil.

También usa con su sentido actual los signos $\subset$, $\{x\}$, $x \cup y$, $x \cap y$, y $\mathfrak{P}(E)$ para nombrar al conjunto de las partes de E. El primer apartado termina enunciando las propiedades básicas del álgebra de conjuntos (sobre uniones, intersecciones, complementos e inclusiones), pero sin mencionar, naturalmente, nada que se parezca al "conjunto de todos los conjuntos".

En el segundo apartado se introducen así las funciones:

> *1. Sean E y F dos conjuntos, distintos o no. Una relación entre una variable x de E y una variable y de F se denomina relación funcional en y si, cualquiera que sea $x \in E$, existe un elemento y de F, y sólo uno, que se encuentra en la relación considerada con x.*
>
> *Se denomina función a la operación que asocia a cualquier elemento $x \in E$ el elemento $y \in F$ que se encuentra en la relación dada con x; decimos que y es el valor de la función para el elemento x, y que la función está determinada por la relación funcional considerada. Dos relaciones funcionales equivalentes determinan la misma función.*

A continuación introduce la notación moderna $f : E \longrightarrow F$, se introduce "aplicación" como sinónimo de "función", se introduce $f(x)$ para nombrar a la imagen de x y se presentan los conceptos básicos sobre funciones (como el de composición, imágenes y antiimágenes de conjuntos, etc.) con mínimas variaciones respecto a la notación actual, como el uso de $\overset{-1}{f}$ en lugar de f^{-1}. Los términos "aplicación inyectiva, suprayectiva, biyectiva". Fueron acuñados por Bourbaki.

En el tercer apartado se introduce el producto cartesiano $E \times F$ de dos conjuntos (llamado simplemente "producto") y se estudian varias aplicaciones entre productos (como las proyecciones, biyecciones canónicas entre productos como $X \times Y$ e $Y \times X$, etc.)

En el cuarto apartado se estudian familias de conjuntos $\{X_i\}_{i\in I}$ y se definen y estudian las uniones, intersecciones y productos

$$\bigcup_{i\in I} X_i, \qquad \bigcap_{i\in I} X_i, \qquad \prod_{i\in I} X_i,$$

enunciando sus propiedades principales con mucho detalle, como

$$\big(\bigcap_{i\in I} X_i\big) \times \big(\bigcap_{k\in K} Y_k\big) = \bigcap_{(i,k)\in I\times K} (X_i \times Y_k),$$

por poner un ejemplo típico.

En el quinto apartado se definen las relaciones de equivalencia y los conjuntos cociente y el en sexto las relaciones de orden y se definen los preórdenes como relaciones reflexivas y transitivas.

De repente se menciona el conjunto $\mathbf{N}$ de los números naturales, con una nota al pie que dice:

> *De acuerdo con el espíritu de este fascículo, suponemos conocida la teoría de los números enteros. Sin embargo, no se debe pensar que esta teoría sea necesaria para la construcción de la teoría de conjuntos; al consultar el Libro de Teoría de Conjuntos, el lector verá, por el contrario, que a partir de los resultados de la teoría de conjuntos se pueden definir los números enteros y demostrar todas sus propiedades conocidas.*
>
> *En nuestra terminología, 0 pertenece a $\mathbf{N}$ y, por lo tanto, se considera positivo; los números enteros positivos y $\neq 0$ se consideran estrictamente positivos.*

Luego se introducen los conceptos de conjunto totalmente ordenado, intervalos abiertos, cerrados y semiabiertos, los conceptos de "elemento más grande" y "elemento más pequeño" (en lugar de máximo y mínimo), se introduce el concepto de buen orden y se menciona que

> *Se demuestra, utilizando el axioma de elección, que en cada conjunto existe una estructura de conjunto bien ordenada (teorema de Zermelo).*

Es la primera vez que se menciona un axioma. Luego se definen las cotas superiores e inferiores, el supremo y el ínfimo. De nuevo se menciona el axioma de elección antes de enunciar el "teorema de Zorn". El sexto apartado termina estudiando los conceptos de límite inductivo y límite proyectivo de un sistema inductivo / proyectivo de conjuntos.

El séptimo apartado está dedicado a los conceptos de equipotencia y numerabilidad. Se enuncian las propiedades básicas de los conjuntos finitos y numerables, así como algunos resultados sobre sucesiones.

Por último, en el apartado octavo se introducen algunas nociones generales sobre estructuras matemáticas e isomorfismos entre ellas.

Hemos detallado el contenido del fascículo tal vez más de lo necesario con la intención de transmitir al lector varias de sus características:

- El fascículo contiene sobradamente todo lo necesario para que un lector pueda entender el lenguaje conjuntista que emplea prácticamente cualquier libro moderno, con los términos y la notación actuales salvo detalles mínimos.
- La forma en que Bourbaki introduce ingenuamente[101] los conceptos conjuntistas más elementales, hablando de "propiedades", "relaciones", "criterios", etc. en un sentido indefinido para a continuación formular explícitamente los resultados concretos sobre tales conceptos que se van a usar. Técnicamente, podríamos considerar a estos tesultados, formulados a partir de conceptos vagos, como una amplia familia de axiomas, en cuanto que su propósito es que en las referencias posteriores se haga referencia a tales propiedades, enunciadas con total precisión, y no a las nociones indefinidas con las que se han presentado.

Ese mismo año de **1939** estalló la Segunda Guerra Mundial, y esto frenó notablemente el proyecto Bourbaki.[102]

67 Las condiciones de Hilbert-Bernays En **1939** se publicó la segunda parte de *Los fundamentos de las matemáticas,* de Hilbert y Bernays, cinco años después de que apareciera la primera parte, y con una extensión de casi seiscientas páginas. En ella, además de exponerse las técnicas de Hilbert y Ackerman para obtener pruebas de consistencia, se presentan sistemáticamente los resultados más recientes sobre la teoría de la demostración, incluyendo los teoremas de incompletitud de Gödel y la solución negativa de Church al problema de la decisión. En la introducción, firmada por Bernays, se lee:

> *El segundo tema principal es el análisis del hecho que ha dado lugar a la necesidad de ampliar el alcance de las inferencias sustantivas permitidas para la teoría de la demostración, en comparación con la delimitación previa del "punto de vista finito". Un aspecto central de estas consideraciones es el descubrimiento de Gödel de la incompletitud deductiva de todo formalismo claramente definido y suficientemente expresivo. Los dos teoremas de Gödel que expresan este hecho se analizan en detalle, tanto en lo que respecta a su relación con las paradojas semánticas, las condiciones de su validez, la ejecución de la demostración —que sólo se insinúa para el segundo de estos teoremas en Gödel— como a su aplicabilidad al formalismo teórico de números completo.*

En efecto, en su artículo, Gödel había sido muy meticuloso con la demostración de su primer teorema de incompletitud, pero en la del segundo afirma vagamente que la demostración del primero se puede formalizar (al menos parcialmente) en cualquier teoría aritmética recursiva. Hilbert y Bernays precisan esa idea enunciando y demostrando lo que hoy se conoce como *condiciones de Hilbert-Bernays*,[103] a partir de las cuales demuestran fácilmente los teoremas de incompletitud. Vamos a enunciarlas:

[101] El propio Bourbaki habla de un "punto de vista *naïf*". En este contexto "ingenuo" no tiene ningún matiz peyorativo, sino que le damos el significado habitual en filosofía de "no basado en ninguna consideración previa" (por ejemplo, un "realista ingenuo" en filosofía es quien da por hecho que existen los objetos que percibe sin haberse planteado la posibilidad de que sean una mera imaginación suya, por oposición al "realista crítico", que es quien sostiene lo mismo, pero después de haber descartado tal alternativa por unas razones u otras). Con esto no insinuamos que Bourbaki no fuera consciente de todos los problemas que plantea una presentación de la teoría de conjuntos a prueba de contradicciones —eso sería falso—, sino meramente que presenta los conceptos más elementales eludiendo deliberadamente cualquier consideración previa u objeción que se pudiera plantear, lo cual es totalmente adecuado para su propósito.

[102] Weil huyó a Finlandia, donde fue arrestado al poco tiempo acusado de espiar para los soviéticos. Fue deportado a Francia, donde en 1940 fue juzgado, acusado de deserción y condenado a cinco años de cárcel, de los que se libró a cambio de alistarse en el ejército. Cuando Francia cayó ante la invasión alemana, Weil huyó a los Estados Unidos. Chevalley se encontraba en Princeton cuando estalló la guerra y allí se quedó hasta que terminó.

[103] También se las llama *condiciones de Hilbert-Bernays-Löb*, porque la formulación actual —que es la que presentamos aquí— la publicó Martin Löb en 1955.

Si T es una teoría aritmética recursiva, y ϕ es una fórmula de su lenguaje formal, representaremos por $\underset{T}{\vdash}\phi$ la afirmación metamatemática "ϕ es demostrable en T". La definición metamatemática de demostración puede formalizarse a través de la fórmula que llamamos $\underset{\ulcorner T\urcorner}{\vdash}\phi$ (donde ϕ es una variable libre). Recordemos también que si ϕ es una fórmula metamatemática del lenguaje formal de T, representamos por $\ulcorner\phi\urcorner$ el número natural que la formaliza en la teoría T.

En estos términos, las condiciones de Hilbert-Bernays son:

1. Si $\underset{T}{\vdash}\phi$, entonces $\underset{T}{\vdash}\ \underset{\ulcorner T\urcorner}{\vdash}\ulcorner\phi\urcorner$,
2. $\underset{T}{\vdash}(\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\phi\urcorner \to \underset{\ulcorner T\urcorner}{\vdash}\ulcorner\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\phi\urcorner\urcorner)$,
3. $\underset{T}{\vdash}(\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\phi\urcorner \wedge \underset{\ulcorner T\urcorner}{\vdash}\ulcorner\phi\to\psi\urcorner \to \underset{\ulcorner T\urcorner}{\vdash}\ulcorner\psi\urcorner)$.

Para entender estas condiciones es fundamental distinguir los tres niveles de discurso descritos en la página 104. La situación es más simple si pensamos en el caso en que T es una teoría de conjuntos, como ZF. La única diferencia con el caso general es que en una teoría aritmética recursiva arbitraria hay que emplear métodos indirectos para hablar de conjuntos finitos y sucesiones finitas, codificándolos adecuadamente como números naturales.

Recordemos, pues, que si T es una teoría aritmética, en la propia teoría T podemos definir lo que son las fórmulas de su lenguaje formal, pero entonces es esencial distinguir entre una fórmula metamatemática, como $\phi \equiv \bigvee x \bigwedge y\, y \notin x$, de su formalización $\ulcorner\phi\urcorner \equiv (6,9,5,10,0,10,8,9)$, donde identificamos cada signo con un número natural según la tabla de la página 103.

Igualmente podemos definir en T el conjunto[104] de todos los axiomas lógicos, y —si T es recursiva— el conjunto de todos los axiomas específicos de $\ulcorner T\urcorner$, y así podemos definir el concepto de demostración en $\ulcorner T\urcorner$, donde usamos la notación $\ulcorner T\urcorner$ para distinguir a T de la teoría $\ulcorner T\urcorner$ definida en T.

Con más detalle, en T podemos definir que una fórmula ϕ (en el sentido definido en T) es demostrable en $\ulcorner T\urcorner$ si existe una sucesión finita D de fórmulas de $\ulcorner T\urcorner$ tal que cada una de ellas es un axioma (lógico o de $\ulcorner T\urcorner$) o bien se deduce de fórmulas precedentes por una de las reglas de inferencia de $\ulcorner T\urcorner$.

Entonces, la fórmula $\underset{\ulcorner T\urcorner}{\vdash}\phi$ se define como "existe una demostración D en $\ulcorner T\urcorner$ cuya última fórmula es ϕ. Se trata de una fórmula del lenguaje formal de T con ϕ como única variable libre (es decir, susceptible de ser sustituida por cualquier término que nombre a una fórmula). Notemos que, en los términos explicados en la página 104, a nivel 0 tenemos que ϕ es una variable, mientras que a nivel 1 podemos decir[105] que ϕ es una fórmula del lenguaje de $\ulcorner T\urcorner$.

Si ϕ es una fórmula metamatemática, como $\bigvee x \bigwedge y\, y \notin x$, una cosa es que $\underset{T}{\vdash}\phi$, cosa que es cierta, como lo es si T es ZF, y otra relacionada, pero distinta, es $\underset{T}{\vdash}\ \underset{\ulcorner T\urcorner}{\vdash}\ulcorner\phi\urcorner$.

La relación básica entre ambas es la que expresa la primera condición de Hilbert-Bernays: si se cumple la primera, se cumple la segunda. Esto lo hemos demostrado en la página 108 (enunciado como punto 3), bajo el supuesto de que la teoría T sea recursiva, como estamos suponiendo aquí.

El recíproco de la primera condición no es cierto en general, pero se cumple si T es ω-consistente. En efecto, supongamos que en T se puede demostrar

$$\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\phi\urcorner \equiv \bigvee n\ \overset{n}{\underset{\ulcorner T\urcorner}{\vdash}}\ulcorner\phi\urcorner.$$

Entonces se tiene que poder demostrar ϕ, porque en caso contrario ningún número natural cumpliría $\overset{n}{\underset{T}{\vdash}}\phi$ y, como esta relación es recursiva (y está representada por la fórmula correspondiente), en T podríamos demostrar

$$\neg\ \underset{\ulcorner T\urcorner}{\vdash}^{\ulcorner 0\urcorner}\ulcorner\phi\urcorner, \qquad \neg\ \underset{\ulcorner T\urcorner}{\vdash}^{\ulcorner 1\urcorner}\ulcorner\phi\urcorner, \qquad \neg\ \underset{\ulcorner T\urcorner}{\vdash}^{\ulcorner 2\urcorner}\ulcorner\phi\urcorner, \qquad \neg\ \underset{\ulcorner T\urcorner}{\vdash}^{\ulcorner 3\urcorner}\ulcorner\phi\urcorner, \qquad \neg\ \underset{\ulcorner T\urcorner}{\vdash}^{\ulcorner 4\urcorner}\ulcorner\phi\urcorner, \qquad \ldots$$

y esto significa que T es ω-contradictoria.

[104] En una teoría aritmética arbitraria, en lugar de conjuntos, tenemos fórmulas que expresan cuándo una fórmula es un axioma.

[105] Es la misma situación que se da si consideramos la fórmula $\bigwedge x \in \mathbb{N}\ x+1 \in \mathbb{N}$. A nivel 0, tenemos que x es una variable, mientras que, a nivel 1, x es un número natural.

La condición de Hilbert-Bernays más sutil es la segunda. Según hemos dicho, a cada fórmula metamatemática ψ le podemos asociar su formalización $\ulcorner\psi\urcorner$, y esto en particular vale si partimos de una fórmula metamatemática ϕ y, a partir de ella, construimos la fórmula metamatemática $\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\phi\urcorner$. Tomando esta fórmula como ψ, podemos construir su formalización $\ulcorner\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\phi\urcorner\urcorner$.

A nivel 1, esto es una sucesión finita de números naturales (como cualquier fórmula de $\ulcorner T\urcorner$), mientras que, como cualquier fórmula de $\ulcorner T\urcorner$, a nivel 2 es una afirmación que tiene un significado que, en este caso expresa que la fórmula $\ulcorner\phi\urcorner$ es demostrable en $\ulcorner T\urcorner$.

En estos términos la primera condición de Hilbert-Bernays es una afirmación metamatemática que puede formalizarse en T. Descomponemos la formalización en varios pasos:

1. La formalización de $\underset{T}{\vdash}\phi$ es $\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\phi\urcorner$,
2. La formalización de $\underset{T}{\vdash}\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\phi\urcorner$ es $\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\phi\urcorner\urcorner$,
3. Por lo tanto, la formalización de la primera condición es $\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\phi\urcorner\to\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\phi\urcorner\urcorner$.

Esto es una fórmula del lenguaje formal de T cuyo significado es precisamente que ϕ cumple la primera condición de Hilbert-Bernays. Lo que afirma la segunda condición es que esta fórmula es demostrable en T. La demostración no es trivial. Una forma de probarla es demostrar que, si una fórmula α cumple cierta hipótesis,[106] entonces en T se puede demostrar $\alpha\to\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\alpha\urcorner$, y aplicar esto al caso en que $\alpha\equiv\underset{\ulcorner T\urcorner}{\vdash}\ulcorner\phi\urcorner$, que cumple la hipótesis requerida.

En cambio, la tercera condición de Hilbert-Bernays es trivial: sólo expresa que la definición de demostración en T incluye la regla del modus ponens, es decir, que si tenemos una prueba de $\ulcorner\phi\urcorner$ y otra de $\ulcorner\phi\to\psi\urcorner$, poniendo una demostración a continuación de la otra y añadiendo la línea $\ulcorner\psi\urcorner$ al final, obtenemos una prueba de $\ulcorner\psi\urcorner$.

Como ilustración vamos a demostrar de nuevo que la sentencia de Gödel es indecidible. Recordemos que la sentencia de Gödel de una teoría aritmética recursiva T es una sentencia G que cumple:

$$\underset{T}{\vdash}(G\leftrightarrow\neg\underset{\ulcorner T\urcorner}{\vdash}\ulcorner G\urcorner),$$

es decir, que G equivale a que su formalización no es demostrable.

Admitiendo esto, ahora es fácil demostrar el primer teorema de incompletitud:

Demostración: Se cumple que G no es demostrable en T. En efecto, si se pudiera demostrar, es decir, si se cumpliera $\underset{T}{\vdash}G$, por la primera condición de Hilbert-Bernays tendríamos $\underset{T}{\vdash}\underset{\ulcorner T\urcorner}{\vdash}\ulcorner G\urcorner$, pero por la construcción de G esto implica $\underset{T}{\vdash}\neg G$, y así T sería contradictoria, pues permitiría demostrar G y $\neg G$.

Para demostrar que $\neg G$ tampoco es demostrable hace falta suponer que T es ω-consistente (la alternativa es usar otra fórmula en lugar de G, debida a Rosser). En tal caso, si $\underset{T}{\vdash}\neg G$, por construcción de G tenemos $\underset{T}{\vdash}\underset{\ulcorner T\urcorner}{\vdash}\ulcorner G\urcorner$ y, por el recíproco de la condición 1 (que se cumple si T es ω-consistente), se cumple $\underset{T}{\vdash}G$, con lo que nuevamente llegamos a que T es contradictoria, pues demuestra G y $\neg G$. ∎

Pero ahora también podemos demostrar fácilmente el segundo teorema de incompletitud. Podemos definir

$$\mathrm{Consis}\ulcorner T\urcorner\equiv\neg\underset{\ulcorner T\urcorner}{\vdash}\ulcorner 0\neq 0\urcorner.$$

Esta sentencia dice que en T no se puede demostrar $0\neq 0$, y eso equivale a la consistencia de T, pues si en T se pudiera demostrar $0\neq 0$, como también se puede probar $0=0$, tendríamos una contradicción. Recíprocamente, si en T no se puede demostrar $0\neq 0$, entonces T es consistente, pues en una teoría contradictoria se puede demostrar cualquier fórmula.

Lo que afirma el segundo teorema de completitud es que si T es consistente, entonces no $\underset{T}{\vdash}\mathrm{Consis}\ulcorner T\urcorner$.

[106] Tiene que ser una fórmula de tipo Σ_1, y el resultado se conoce como teorema de Σ_1-completitud.

DEMOSTRACIÓN: Supongamos que $\underset{T}{\vdash}\mathrm{Consis}^{\ulcorner}T^{\urcorner}$, es decir,

$$\neg\underset{T}{\vdash}{}^{\ulcorner}0 \neq 0^{\urcorner}.$$

Entonces, para cualquier fórmula ϕ, se cumple $\underset{T}{\vdash}(\neg\phi \to (\phi \to 0 \neq 0))$, pues esto es un teorema lógico. Por la condición 1:

$$\underset{T}{\vdash}\ \underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}\neg\phi \to (\phi \to 0 \neq 0)^{\urcorner},$$

por la condición 3:

$$\underset{T}{\vdash}\ (\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}\neg\phi^{\urcorner} \wedge \underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}\neg\phi \to (\phi \to 0 \neq 0)^{\urcorner} \to \underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}\phi \to 0 \neq 0^{\urcorner}), \qquad \underset{T}{\vdash}\ (\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}\phi^{\urcorner} \wedge \underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}\phi \to 0 \neq 0^{\urcorner} \to \underset{T}{\vdash}{}^{\ulcorner}0 \neq 0^{\urcorner}),$$

De aquí se sigue trivialmente[107]

$$\underset{T}{\vdash}\ (\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}\neg\phi^{\urcorner} \to \neg\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}\phi^{\urcorner}).$$

Ahora aplicamos esto a $\phi \equiv \underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}G^{\urcorner}$, con lo que tenemos la primera fórmula de la demostración siguiente (todas las fórmulas son teoremas de T, por las razones que se indican a la derecha):

1	$\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}\neg\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}G^{\urcorner}{}^{\urcorner} \to \neg\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}G^{\urcorner}{}^{\urcorner}$	Lo que acabamos de probar.
2	$G \to \neg\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}G^{\urcorner}$	Por construcción de G.
3	$\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}G \to \neg\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}G^{\urcorner}{}^{\urcorner}$	Por 2 y la condición 1.
4	$\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}G^{\urcorner} \to \underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}\neg\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}G^{\urcorner}{}^{\urcorner}$	Por 3 y la condición 3.
5	$\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}G^{\urcorner} \to \neg\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}G^{\urcorner}{}^{\urcorner}$	Por 1 y 4.
6	$\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}G^{\urcorner} \to \ \underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}G^{\urcorner}{}^{\urcorner}$	Condición 2.
7	$\neg\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}G^{\urcorner}$	Por 5 y 6 (reducción al absurdo).
8	$\neg\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}G^{\urcorner} \to G$	Por construcción de G.
9	G	Por 7 y 8.
10	$\underset{\ulcorner T\urcorner}{\vdash}{}^{\ulcorner}G^{\urcorner}$	Por 9 y la condición 1.

Las líneas 7 y 10 muestran que T es contradictoria. De hecho, por la construcción de G podemos llegar también a una demostración de G y $\neg G$. ∎

Sobre la prueba de consistencia de Gentzen, en la introducción de los "Fundamentos" Bernays dice:

> *El análisis de la extensión del punto de vista finito conduce a considerar la prueba de consistencia más reciente de Gentzen para el formalismo numérico. Sin embargo, de esta prueba, sólo se presenta y analiza con más detalle aquí el aspecto metodológicamente novedoso, a saber, la aplicación de un tipo especial de la "inducción transfinita" de Cantor. El hecho de que no se presentara la prueba completa se debió principalmente a que la versión más reciente, la única verdaderamente transparente, de la prueba de Gentzen aún no había aparecido cuando este volumen se publicó.*

Al discutir la prueba de Gentzen ya habíamos señalado que la validez de la inducción transfinita hasta cualquier ordinal menor que ϵ_0 es demostrable en AP. Esto fue probado por primera vez en el libro de Hilbert-Bernays. En la sección correspondiente, se da por válida la inducción transfinita:

[107] Esto es cálculo proposicional: tenemos $\neg p, q, r \wedge q \to s, t \wedge s \to p$, y de estas premisas se deduce $r \to \neg t$.

> *La inferencia indirecta utilizada en esta demostración es, hasta cierto punto, no problemática desde el punto de vista finitista, ya que la suposición de una derivación con ordinal α, que tiene como secuente final el secuente vacío, posee una determinación intuitiva.* [...]
>
> *Sin embargo, el método de la demostración de Gentzen no está diseñado meramente para la prueba de consistencia del formalismo de la teoría de números que se ha llevado a cabo hasta ahora, sino también, y esencialmente, con vistas a la posibilidad de su aplicación a formalismos más amplios, en particular los del análisis. De hecho, la idea fundamental de la demostración de Gentzen no depende de que en el formalismo a considerar exista un tipo de eliminabilidad de los medios transfinitos, sino sólo de que, por un lado, las derivaciones puedan ordenarse bien, por así decirlo, según su grado de complicación, y de que para aquellas derivaciones cuya fórmula final no representa algo intuitivamente verdadero en sentido elemental, se pueda definir un paso de reducción mediante el cual, por así decirlo, se descompone un paso de la demostración, reduciéndose el número ordinal de la derivación.*
>
> *Pero hay que tener en cuenta —y esto es una consecuencia del teorema de indemostrabilidad de Gödel— que cuanto más amplio sea el formalismo a considerar, mayores tipos de orden, es decir, mayores formas del principio de inducción generalizado deben utilizarse, y las exigencias metodológicas para la demostración de contenido de ese principio de inducción superior establecen el estándar para las suposiciones metodológicas que deben subyacer a la configuración de contenido si se quiere que la prueba de consistencia del formalismo en cuestión tenga éxito.*

Hilbert tenía puestas sus esperanzas en que la técnica de Gentzen permitiera demostrar la consistencia del análisis (objetivo que el propio Gentzen se había marcado a sí mismo). En la introducción, Bernays dice:

> *Si esto tiene éxito — lo cual hay muchas perspectivas de que ocurra—, entonces el planteamiento original de Hilbert habrá sido rehabilitado en cuanto a su efectividad. En cualquier caso, ya basándose en la prueba de Gentzen, se puede sostener la opinión de que el fracaso temporal de la teoría de la demostración se debió únicamente a un exceso en la exigencia metodológica que se le había planteado a la teoría. Ciertamente, la decisión crucial sobre el destino de la teoría de la demostración sólo se dará a partir de la tarea de demostrar la consistencia del análisis.*

68 La consistencia del axioma de elección y de la hipótesis del continuo En 1938 Gödel había publicado en una revista estadounidense una breve nota titulada *La consistencia del axioma de elección y de la hipótesis del continuo generalizada,* con este anuncio (donde hemos actualizado la notación en los puntos 3 y 4):

> Teorema. *Sea T el sistema de axiomas para la teoría de conjuntos obtenido del sistema S^* de von Neumann al omitir el axioma de elección; entonces, si T es consistente, sigue siéndolo si las siguientes proposiciones 1-4 se adjuntan simultáneamente como nuevos axiomas:*
>
> 1. *El axioma de elección.*
> 2. *La hipótesis del continuo generalizada, (es decir, la afirmación de que se cumple $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ para todo ordinal α).*
> 3. *La existencia de conjuntos lineales $\mathbf{\Delta}^1_2$ no medibles Lebesgue.*
> 4. *La existencia de conjuntos $\mathbf{\Pi}^1_1$ que tienen la potencia del continuo y no contienen ningún subconjunto perfecto.*
>
> *Un teorema correspondiente se cumple si T denota el sistema de* Principia Mathematica *o el sistema de axiomas de Fraenkel para la teoría de conjuntos, omitiendo en ambos casos el axioma de elección, pero incluyendo el axioma del infinito.*
>
> *La prueba de los teoremas anteriores es constructiva en el sentido de que, si se obtuviera una contradicción en el sistema ampliado, se podría exhibir una contradicción en T.*

En **1939** publicó en la misma revista un esbozo en cuatro páginas de la demostración de los dos primeros hechos (para las teorías de Zermelo y de Zermelo-Fraenkel), bajo el título de *Prueba de la consistencia de la hipótesis del continuo generalizada.*

Gödel no era judío, pero muchos de sus amigos sí, así que desde la anexión de Austria a Alemania, su situación den Viena se había vuelto cada vez más precaria. Tras el estallido de la Segunda Guerra Mundial, cabía incluso

la posibilidad de que fuera obligado a alistarse en el ejército alemán. A finales de **1939** él y su esposa decidieron emigrar a los Estados Unidos, pero los submarinos alemanes hundían barcos constantemente en en Atlántico y en el Mediterráneo, por lo que a Gödel le aterraba la idea de embarcar. En su lugar, atravesaron la Unión Soviética en el ferrocarril Transiberiano, luego embarcaron hasta Japón y, ya en **1940** llegaron hasta los Estados Unidos atravesando el Pacífico, que estaba en paz, pues entonces la Unión Soviética era aliada de Alemania y Japón todavía no había entrado en la guerra.

En Princeton fue recibido como agua de mayo, porque su esbozo de demostración de la consistencia del axioma de elección y de la hipótesis del continuo generalizada era un tanto críptica, y había muchos matemáticos deseosos de entender los detalles. Gödel no tardó en impartir una serie de conferencias sobre su demostración, y ese mismo año publicó un librito de 66 páginas titulado *La consistencia del axioma de elección y de la hipótesis del continuo generalizada con los axiomas de la teoría de conjuntos,* donde explica su prueba con claridad meridiana, accesible prácticamente a cualquier matemático, aunque no estuviera muy familiarizado con la lógica.

En su primer anuncio de 1938, Gödel había hecho referencia a la teoría de von Neumann, mientras que en el esbozo de 1939 hablaba de las teorías de Zermelo y Zermelo-Fraenkel. En su exposición definitiva, consideró una simplificación de la teoría de von Neumann-Bernays que hoy se conoce como *teoría de von Neumann-Bernays-Gödel* (NBG).

La diferencia fundamental de NBG con la teoría de Bernays es que en ésta hay dos tipos de objetos: clases y conjuntos, que son distintos entre sí: una clase nunca es un conjunto, pero lo que sí puede suceder es que una clase y un conjunto tengan exactamente los mismos elementos, y entonces se dice que el conjunto representa a la clase. Todo conjunto representa a una clase, pero hay clases que no están representadas por ningún conjunto.

En cambio, en NBG no hay más que un tipo de objetos: las clases, entre las que se da la relación de pertenencia (no definida). Los conjuntos se definen como las clases que no pertenecen a otras clases. De este modo, el lenguaje de NBG tiene un único concepto no definido, el de pertenencia y los cuantificadores "para todo" y "existe" se interpretan como "para toda clase" y "existe una clase", respectivamente.[108] En NBG no hay clases representadas por conjuntos, sino que una clase o es un conjunto o no lo es. Una *clase propia* se define como una clase que no es un conjunto, es decir, como una clase que no pertenece a ninguna clase.

En este marco, Gödel introduce cuatro grupos de axiomas. Los axiomas del grupo A son simplemente el axioma de extensionalidad y el axioma del par:

$$\bigwedge XY(\bigwedge u(u \in X \leftrightarrow u \in Y) \to X = Y), \qquad \bigwedge xy\bigvee z\bigwedge u(u \in x \leftrightarrow u \in x \vee u \in y)).$$

Aquí adoptamos el convenio de que las letras minúsculas nombran conjuntos. El axioma de extensionalidad afirma que dos clases con los mismos elementos son iguales, y el axioma del par dice que, para cada par de conjuntos, hay otro que los tiene a ellos dos como únicos elementos.

El grupo de axiomas B consta de ocho axiomas de formación de clases, a partir de los cuales, análogamente a Bernays, demuestra el teorema de comprensión:[109]

> **Esquema teoremático de comprensión** Si $\phi(u)$ es una fórmula (con posibles parámetros) en la que todos los cuantificadores se refieren a conjuntos (son de la forma "para todo conjunto" o "existe un conjunto", pero nunca de la forma "para toda clase" o "existe una clase"), entonces la fórmula siguiente es un teorema:
>
> $$\bigvee Y\bigwedge u(u \in Y \leftrightarrow \phi(u)).$$

[108] En realidad, Gödel no lo plantea así, sino que introduce tres conceptos no definidos: Cls, $\mathcal{C}$ y $\in$, de modo que $\mathrm{Cls}\, X$ se lee "X es una clase", $\mathcal{C}x$ se lee "x es un conjunto" y $X \in Y$ se lee "X pertenece a Y", pero toma como un axioma tácito que sólo va a hablar de clases (cuando especifica el convenio que las variables mayúsculas recorren clases y las minúsculas conjuntos, con lo que $\bigwedge X$ significa "para toda clase" y $\bigwedge x$ significa "para todo conjunto"), a lo que añade explícitamente los axiomas que estipulan 1) que todo conjunto es una clase, y 2) que toda clase que pertenece a otra clase es un conjunto.

Esto es equivalente a tomar $\in$ como único concepto primitivo y adoptar como definición $\mathcal{C}X \equiv \bigvee Y X \in Y$ (una clase es un conjunto si pertenece a otra clase). Éste es el planteamiento usual hoy en día de NBG. Probablemente, Gödel adoptó un marco formal ligeramente más complicado de lo necesario porque así luego podía hacer corresponder más limpiamente los conceptos de "clase" y "conjunto" con los conceptos de "clase constructible" y "conjunto constructible" que iba a definir. En lo sucesivo, cuando hablamos de los axiomas de NBG, no incluimos los axiomas 1) y 2), que son innecesarios.

[109] En realidad, por razones técnicas, Gödel demuestra una versión para n-tuplas, pero que es equivalente a ésta.

Los axiomas del grupo C son cuatro axiomas de formación de conjuntos (sería más coherente que el axioma del par estuviera aquí, pero Gödel lo necesitaba antes para demostrar el teorema de comprensión): el axioma de infinitud, el axioma de la unión, el axioma del conjunto de partes y el axioma del reemplazo (que aquí es un único axioma y no un esquema axiomático). Finalmente, el grupo D consta de un único axioma, que es el axioma de regularidad de von Neumann, expresado como que toda clase no vacía posee un elemento disjunto de ella.

En realidad Gödel incluye en NBG una versión fuerte del axioma de elección (el axioma E), que afirma que existe una función $F : V \longrightarrow V$ que a cada conjunto no vacío le escoge uno de sus elementos, pero en lo sucesivo lo usa sólo en unos pocos teoremas claramente señalados, que sólo empleará en la parte final del trabajo, cuando ya haya demostrado la consistencia del axioma de elección. En lo que sigue y mientras no digamos lo contrario, cuando hablemos de NBG se entenderá que no incluimos el axioma de elección.

Tras dedicar unas páginas a explicar el convenio de que cada definición añade un signo al lenguaje formal, pero que todos los signos definidos son eliminables, Gödel introduce sistemáticamente todos los conceptos conjuntistas básicos (uniones, intersecciones, productos cartesianos, etc.) y demuestra los teoremas básicos que determinan qué clases son conjuntos y cuáles son clases propias. Con esto termina la sección 2 del trabajo (en la sección 1 ha introducido los axiomas).

En la sección 3 presenta con todo rigor, precisión y sencillez la teoría de ordinales, y en la sección 4 hace lo mismo con la teoría de cardinales. En particular, define la clase Ω de todos los ordinales (de von Neumann) y la clase $K \subset \Omega$ de todos los cardinales (los ordinales no biyectables con ningún ordinal anterior), así como la función $\aleph$, que biyecta en orden creciente los ordinales con los cardinales infinitos.

Esta primera parte de la monografía de Gödel es relevante en sí misma, porque mostró a muchos matemáticos que deducir con rigor lógico los resultados conjuntistas básicos a partir de unos axiomas dados no era algo sutil y artificioso, sólo accesible a los expertos en lógica, sino que se podía hacer de forma rutinaria, siguiendo las costumbres habituales de los matemáticos, sin necesidad de filosofar más allá de lo justo para dejar claro el lenguaje formal empleado, con sus conceptos no definidos, y cómo hay que entender las definiciones de los demás conceptos.

En la sección 5 Gödel introduce los conceptos principales de su prueba de consistencia, pero nos vamos a apartar de su exposición porque, para que resulte natural a los matemáticos no familiarizados con la lógica, Gödel oculta la idea de fondo, que está patente en el esbozo de prueba que había presentado el año anterior, y más claramente aún en su nota del año precedente:

> *El método de demostración consiste en construir, a partir de los axiomas de T, un modelo para el cual las proposiciones 1-4 sean verdaderas. Este modelo, en términos generales, consta de todos los conjuntos "matemáticamente constructibles", donde el término "constructible" debe entenderse en un sentido semiintuicionista que excluye los procedimientos impredicativos. Esto significa que los conjuntos "constructibles" se definen como aquellos que pueden obtenerse mediante la jerarquía ramificada de tipos de Russell, si se extiende para incluir órdenes transfinitos. La extensión a órdenes transfinitos tiene como consecuencia que el modelo satisface los axiomas impredicativos de la teoría de conjuntos, ya que se puede demostrar un axioma de reducibilidad para órdenes suficientemente altos. Además, se puede demostrar que la proposición "Todo conjunto es constructible" (que abrevio como "A") es consistente con los axiomas de T, ya que A resulta ser verdadera para el modelo compuesto por los conjuntos constructibles.*

Vamos a explicar esta cita. Si X es un conjunto cualquiera, podemos definir (sin usar el axioma de elección, ni siquiera el de partes) el conjunto $\mathcal{D}X$ de las *partes definibles* de X, que está formado por todos los subconjuntos de X que pueden definirse mediante fórmulas con parámetros en X y cuyos cuantificadores recorren únicamente los elementos de X. En otras palabras, los elementos de $\mathcal{D}X$ son los conjuntos de la forma

$$\{x \in X \mid \phi(x, x_1, \ldots, x_n)\},$$

donde $x_1, \ldots, x_n \in X$ y los cuantificadores que pueda haber en la fórmula[110] ϕ se interpretan como "para todo $u \in X$" o "existe un $u \in X$".

[110]Técnicamente, aquí hay que entender que ϕ no es una fórmula metamatemática, sino una fórmula "de nivel 1" en el sentido de la página 104, y esto requiere asociar a ϕ la relación $R_\phi \subset X^{n+1}$ que cumplen las $n+1$-tuplas $(x, x_1, \ldots, x_n)$ que cumplen ϕ, cosa que puede hacerse, pero obliga a distinguir entre el nivel matemático y el metamatemático, y esto es justamente lo que Gödel evitó con el enfoque que empleó en su monografía.

Así $\mathcal{D}X \subset \mathcal{P}X$ y, de hecho, para conjuntos finitos se da la igualdad, pero para conjuntos infinitos la diferencia es sustancial: usando el axioma de elección se demuestra que $|\mathcal{D}X| = |X|$, mientras que $|\mathcal{P}X| > |X|$.

Conviene observar que si X es un conjunto transitivo, es decir, si todo $x \in X$ cumple $x \subset X$, entonces $X \subset \mathcal{D}X$ y $\mathcal{D}X$ también es transitivo.

DEMOSTRACIÓN: Si $x \in X$, entonces $x = \{u \in X \mid \phi(u, x)\}$, donde $\phi(u, x) \equiv u \in x$, luego, en efecto, $x \in \mathcal{D}X$. Además, si $A \in \mathcal{D}X$, tenemos que probar que $A \subset \mathcal{D}X$, para lo cual tomamos $x \in A \subset X$ y, por la parte ya probada, $x \in \mathcal{D}X$, luego, ciertamente, $A \subset \mathcal{D}X$. ∎

Y un hecho clave es que si tenemos dado un buen orden $\leq$ de X, a partir de él podemos definir explícitamente un buen orden $\leq^*$ en $\mathcal{D}X$ (sin necesidad del axioma de elección).

La idea es que, a partir de un buen orden en X, podemos definir un buen orden $\leq'$ el el conjunto X^* de todas las sucesiones finitas $(x_1, \ldots, x_n)$ de elementos de X (por ejemplo el orden lexicográfico, el mismo que se usa para ordenar las palabras en un diccionario a partir de un orden prefijado de las letras en el alfabeto). Por otro lado, las fórmulas $\phi(x, x_1, \ldots, x_n)$ que podemos usar para definir elementos de $\mathcal{D}X$ forman un conjunto numerable que podemos enumerar explícitamente, y esto a su vez nos permite ordenar bien todos los pares (ϕ, s), donde ϕ es una fórmula con n parámetros y s es una sucesión de elementos de X con n elementos. Entonces, podemos definir $A \leq^* B$ si y sólo si el menor par (ϕ, s) que define a A es menor o igual que el menor par (ψ, t) que define a B. Y esto resulta ser un buen orden en $\mathcal{D}X$.

Más aún, si X es transitivo, y se cumple, pues, que $X \subset \mathcal{D}X$, podemos retocar el buen orden $\leq^*$ para exigir que coincida con el orden dado $\leq$ sobre los elementos de X, así como que todos ellos sean anteriores a los elementos de $\mathcal{D}X$ que no están en X.

Por ejemplo, el conjunto ω de todos los números naturales es un conjunto transitivo[111] y está bien ordenado por el orden usual $\leq$. Entonces es posible definir un buen orden $\leq^*$ en $\mathcal{D}\omega$ que empiece así:

$$0 \quad \leq^* 1 \quad \leq^* 2 \quad \leq^* 3 \quad \leq^* \quad \cdots \quad \leq^* \quad A_\omega \quad \leq^* \quad A_{\omega+1} \quad \leq^* \quad A_{\omega+2} \quad \leq^* \quad \cdots$$

Primero van los números naturales (que son subconjuntos definibles de ω) y luego los restantes subconjuntos definibles.

Podríamos decir que $\mathcal{D}X$ es el conjunto de los "subconjuntos predicativos" de X, es decir, los que pueden definirse cuantificando únicamente sobre los conjuntos "ya definidos" sin ningún compromiso de que los conjuntos que definamos tengan que estar ya entre los elementos de X, sino que, en principio, estarán en un nivel superior $\mathcal{D}X$.

A continuación, lo que hacemos es imitar la jerarquía acumulativa de von Neumann (véase la página 85), pero sustituyendo el operador $\mathcal{P}$ por $\mathcal{D}$:

$$L_0 = \varnothing, \qquad L_{\alpha+1} = \mathcal{D}L_\alpha, \qquad L_\lambda = \bigcup_{\delta<\lambda} L_\delta,$$

con lo que obtenemos *la clase de los conjuntos constructibles:*

$$L = \bigcup_{\alpha\in\Omega} L_\alpha.$$

Con más detalle: partimos de un nivel[112] 0 que es simplemente $L_0 = \varnothing$. Supuestos definidos los conjuntos de nivel α, donde α es un ordinal arbitrario, definimos $L_{\alpha+1}$ como el conjunto de las partes definibles de L_α y, supuestos definidos todos los niveles L_δ anteriores a un ordinal límite λ, definimos el nivel L_λ acumulando todos los conjuntos definidos hasta el momento. Finalmente, la clase L de todos los conjuntos constructibles se obtiene acumulando todos los conjuntos obtenidos en este proceso.

Como L_0 es trivialmente un conjunto transitivo, se razona por inducción transfinita que todos los conjuntos L_α son transitivos, lo que a su vez hace que la jerarquía constructible sea creciente respecto de la inclusión, es decir, que si $\alpha \leq \beta$, entonces $L_\alpha \subset L_\beta$.

[111] Por el convenio según el cual cada ordinal es el conjunto de los ordinales anteriores a él, de modo que, por ejemplo, se cumple que $5 = \{0, 1, 2, 3, 4\} \subset \omega$.

[112] Probablemente, la letra L proviene de *"level"*.

Como L_0 es finito, en los primeros pasos de la jerarquía es indistinto usar $\mathcal{D}$ o $\mathcal{P}$, por lo que la jerarquía constructible empieza igual que la jerarquía de von Neumann: $L_n = V_n$, para todo número natural n, y de aquí a su vez que, al acumular, obtenemos también $L_\omega = V_\omega$.

Pero a partir de aquí la jerarquía de Gödel se distancia de la de von Neumann, y en general sólo se da la inclusión $L_\alpha \subset V_\alpha$ para todo ordinal α.

A su vez, Gödel define las clases constructibles como las que cumplen:

$$\mathcal{L}A \equiv A \subset L \wedge \bigwedge x \in L\ A \cap x \in L.$$

En otros términos: una clase es constructible si todos sus elementos son conjuntos constructibles y su intersección con cada conjunto constructible es un conjunto constructible.

Tras demostrar algunos resultados técnicos sobre los conjuntos y las clases constructibles, en la sección 6 Gödel demuestra que si pasamos a llamar "clases" a las clases constructibles y "conjuntos" a los conjuntos constructibles, todos los axiomas de NBG siguen cumpliéndose. En otras palabras, que si alguien sólo ve los conjuntos y las clases constructibles, no verá que falle por ello ninguno de los axiomas de NBG.

Veamos un par de ejemplos de lo que esto supone. Por ejemplo, tomemos el axioma del par, que afirma que, dados dos conjuntos, existe un tercer conjunto que los tiene a ambos por elementos. Lo que tenemos que probar es que, dados dos conjuntos constructibles x, y, el conjunto $\{x, y\}$ también es constructible, de modo que alguien que sólo vea los conjuntos constructibles no dejará de ver los pares de todos los conjuntos que ve.

Ahora bien, si $x, y \in L$, existe un ordinal α tal que $x, y \in L_\alpha$ (en principio, cada uno pertenecerá a un L_α distinto, pero basta tomar el mayor de los dos ordinales). Pero entonces

$$\{x, y\} = \{u \in L_\alpha \mid u = x \vee u = y\} \in \mathcal{D}L_\alpha = L_{\alpha+1} \subset L.$$

Consideremos ahora el axioma del conjunto de partes, que dice que si existe un conjunto x, existe un conjunto $\mathcal{P}x$ formado por todos sus subconjuntos. Lo que tenemos que probar en este caso es que si $x \in L$, existe un conjunto constructible que contiene a todos los subconjuntos constructibles de x, es decir, que $\mathcal{P}x \cap L \in L$. Así, alguien que sólo vea los conjuntos constructibles, verá el conjunto $\mathcal{P}x \cap L$ y considerará que es el conjunto de todos los subconjuntos de x, ya que contiene todos los subconjuntos de x que él ve.

Para probarlo tenemos que considerar la aplicación de $\mathcal{P}x \cap L \longrightarrow \Omega$ que a cada $u \in \mathcal{P}x \cap L$ le asigna el mínimo ordinal α tal que $x \in L_\alpha$. El axioma del reemplazo asegura que la imagen de esta aplicación es un subconjunto de Ω, y todo subconjunto de Ω tiene un supremo γ, que en este caso es un ordinal tal que todo $u \in \mathcal{P}x \cap L$ está en L_γ o, equivalentemente, tal que $\mathcal{P}x \cap L \subset L_\gamma$. Entonces

$$\mathcal{P}x \cap L = \{u \in L_\gamma \mid \bigwedge v \in L_\gamma(v \in u \to v \in x)\} \in \mathcal{D}L_\gamma = L_{\gamma+1} \subset L.$$

Aquí usamos que si $u \in L_\gamma$ cumple $\bigwedge v \in L_\gamma(v \in u \to v \in x)$, entonces $u \subset x$, pues si $v \in u$, como $u \subset L_\gamma$ (ya que L_γ es transitivo) tenemos que $v \in L_\gamma$, luego, por hipótesis, $v \in x$.

Gödel demostró que esto sucede con todos los axiomas de NBG: para que se cumplan los axiomas de NBG podemos desprendernos de todas las clases y conjuntos no constructibles.

De aquí se desprende lo siguiente:

> Si NBG es consistente, también lo es la teoría que resulta de añadirle el *axioma de constructibilidad:* $V = L$, es decir, la afirmación "todo conjunto es constructible".

La idea es la siguiente: es imposible demostrar en NBG que existe un conjunto no constructible, porque si pudiera demostrarse, como alguien que sólo vea las clases y los conjuntos constructibles ve que se cumplen los axiomas de NBG, también tendría que ver un conjunto no constructible, lo cual es absurdo.[113]

La demostración es constructiva, en el sentido de que se puede programar a un ordenador para que, si le damos la demostración de una contradicción en NBG + $V = L$, nos devuelva la demostración de una contradicción en NBG. Esta demostración se obtiene cambiando "clase" por "clase constructible" y "conjunto" por "conjunto constructible" en la demostración dada.

[113] En realidad hay una sutileza que hay que tener en cuenta. Falta demostrar que alguien que sólo vea las clases y conjuntos constructibles podrá reconocer que todos los conjuntos que ve son constructibles. En otras palabras, que para comprobar que un conjunto x es constructible no hace falta ver ningún conjunto o clase que no sea constructible. Gödel dedica la sección 7 de su trabajo a demostrar que esto es así.

En resumen, la idea es que un conjunto no constructible es un conjunto "raro", "indefinible", y los axiomas de la teoría de conjuntos (distintos del axioma de elección, que no estamos considerando aquí) postulan la existencia de conjuntos, pero no se pronuncian sobre si existen o no conjuntos "raros". Si los eliminamos, en el supuesto de que los haya, no dejan de cumplirse.

Finalmente, Gödel dedica la última sección a demostrar que el axioma de constructibilidad $V = L$ implica el axioma de elección y la hipótesis del continuo generalizada. Aceptando esto, tenemos ya su consistencia: si se pudiera demostrar una contradicción en NBG incluyendo el axioma de elección o la hipótesis del continuo generalizada, tendríamos una contradicción en NBG + $V = L$, y ya hemos visto que eso implica que NBG es contradictorio.

La prueba de que $V = L$ implica el axioma de elección es conceptualmente muy simple: si definimos $\trianglelefteq_0 = \varnothing$, tenemos trivialmente que $\trianglelefteq_0$ es un buen orden en el conjunto vacío, y hemos razonado antes que cada buen orden en un conjunto transitivo X se extiende a un buen orden en $\mathcal{D}X$ que prolonga al dado, por lo que podemos definir una sucesión transfinita de buenos órdenes:

$$\trianglelefteq_0 = \varnothing, \qquad \trianglelefteq_{\alpha+1} = \trianglelefteq_\alpha^*, \qquad \trianglelefteq_\lambda = \bigcup_{\delta<\lambda} \trianglelefteq_\delta, \qquad \trianglelefteq = \bigcup_{\alpha\in\Omega} \trianglelefteq_\alpha,$$

de modo que cada $\trianglelefteq_\alpha$ es un buen orden en L_α y $\trianglelefteq$ es un buen orden en L.

Más detalladamente: $L_0 = \varnothing$ está trivialmente bien ordenado. Supuesto definido un buen orden en L_α, hemos visto cómo extenderlo a un buen orden en $L_{\alpha+1}$, de modo que los elementos "nuevos" de $L_{\alpha+1}$ van detrás de los de L_α. Y supuesto que hemos ordenado todos los L_δ, con $\delta < \lambda$, de modo que cada buen orden prolonga a los anteriores, entonces L_λ queda trivialmente bien ordenado por los buenos órdenes dados (no hay en él conjuntos nuevos que ordenar). Por último, todos estos buenos órdenes $\trianglelefteq_\alpha$ determinan un único buen orden en toda la clase L, que hemos construido sin usar en ningún momento el axioma de elección, definiendo explícitamente el orden de cada nivel de la jerarquía.

En particular, si $V = L$ sabemos ordenar bien la clase universal (mediante una fórmula explícita, que no depende del axioma de elección!), y podemos definir una función de elección $F : V \longrightarrow V$ que a cada conjunto no vacío le asigne su mínimo respecto de la relación $\trianglelefteq$. Esto prueba que $V = L$ implica el axioma de elección de Gödel (que es más fuerte que el de Zermelo, pues no sólo afirma que cada conjunto tiene una función de elección, o que todo conjunto puede ser bien ordenado, sino que la clase universal tiene una función de elección, y puede ser bien ordenada).

Más aún, puede probarse que existe una única biyección $F : \Omega \longrightarrow L$ que conserva el orden. Si suponemos $V = L$, para cada clase propia A existe una única biyección $F : \Omega \longrightarrow A$ que conserva el orden, por lo que todas las clases propias son biyectables entre sí.

A partir de aquí ya podemos considerar al axioma de elección como uno más de los axiomas de NBG. En particular, podemos contar con el hecho de que, si X es un conjunto infinito, entonces $|\mathcal{D}X| = |X|$, y de ahí se deduce que, si α es un ordinal infinito, entonces $|L_\alpha| = |\alpha|$.

En particular, los niveles $L_\omega, L_{\omega+1}, \ldots$ son numerables. En la jerarquía de von Neumann, $V_{\omega+1} = \mathcal{P}V_\omega$ contiene todos los subconjuntos de V_ω, pero $L_{\omega+1}$ es numerable, así que no puede contener a todo $\mathcal{P}V_\omega$, que es no numerable. En $L_{\omega+1}$ sólo están los subconjuntos de L_ω que pueden definirse sin hacer referencia a nada que no esté en L_ω, y no son todos. En $L_{\omega+2}$ habrá más, pues ahí estarán todos los que pueden definirse sin hacer referencia a nada que no esté en $L_{\omega+1}$, pero seguirán siendo una cantidad numerable, luego no están todos.

Así, mientras en la jerarquía de von Neumann, todos los subconjuntos de L_ω aparecen "de golpe" en $V_{\omega+1}$, en la jerarquía de Gödel, los subconjuntos de L_ω van apareciendo poco a poco en los niveles $L_{\omega+1}, L_{\omega+2}, L_{\omega+3}, \ldots$ ya que todos estos (primeros) conjuntos son numerables y no cabe todo $\mathcal{P}L_\omega$ en ninguno de ellos.

En este punto obtenemos uno de los resultados más profundos del trabajo de Gödel (aunque no lo enuncia en estos términos):

> Si $V = L$ y κ es un cardinal infinito, entonces se cumple $\mathcal{P}L_\kappa \subset L_{\kappa^+}$, donde κ^+ representa el cardinal siguiente a κ.

Es decir, los subconjuntos de L_κ van apareciendo sucesivamente en los niveles $L_{\kappa+1}, L_{\kappa+2}, \ldots$, pero al llegar a L_{κ^+} ya han aparecido todos. De nuevo la prueba que da Gödel es técnicamente muy simple, pero oculta las ideas de fondo. No vamos a discutirlas aquí.[114] El caso es que esto implica inmediatamente:

[114] Tales ideas están en la base de lo que años más tarde se llamaría "estructura fina de L", una teoría muy profunda sobre la clase de los conjuntos constructibles.

Si $V = L$, se cumple la hipótesis del continuo generalizada.

En efecto, si κ es un cardinal infinito, tenemos que $|L_\kappa| = \kappa$, luego

$$\kappa^+ \leq 2^\kappa = |\mathcal{P}L_\kappa| \leq |L_{\kappa^+}| = \kappa^+,$$

luego $2^\kappa = \kappa^+$ es el cardinal siguiente a 2^κ, y eso es justo lo que afirma la hipótesis del continuo generalizada.

Podemos pensar que, al quedarnos sólo con los conjuntos constructibles, a cada conjunto le estamos dejando el mínimo número posible de subconjuntos, y la hipótesis del continuo generalizada afirma precisamente eso: que cada conjunto tiene el menor número de subconjuntos posible, teniendo en cuenta el teorema de Cantor, que exige que sea un cardinal mayor que el del conjunto.

La conclusión es la misma que con el axioma de elección: si NBG es consistente, también lo es si le añadimos como axioma la hipótesis del continuo generalizada, porque si alguien pudiera llegar a una contradicción a partir de ella, también tendríamos una contradicción si suponemos que $V = L$, pero ya hemos visto que esto implicaría que NBG es contradictorio.

Cabe insistir en que las pruebas son todas constructivas: si alguien encuentra una contradicción suponiendo el axioma de constructibilidad, o el axioma de elección, o la hipótesis del continuo generalizada, o todo a la vez, a partir de ella podríamos construir mecánicamente una demostración de contradicción a partir de los axiomas de NBG sin el axioma de elección. El argumento se puede adaptar a ZF. Gödel prefirió trabajar con NBG para hablar de la clase L "cómodamente", sin tener que recurrir a artificios lógicos que pudieran hacer que algún matemático arrugara la nariz.

Con la demostración de Gödel quedaba descartada cualquier objeción al uso del axioma de elección fundada en la posibilidad de que sea contradictorio, pero seguían vigentes las objeciones relacionadas con que introduce conjuntos "raros", "caóticos", "indefinibles". Sobre esto, la prueba de Gödel también tiene algo que decir:

Observación Gödel no demostró la consistencia del axioma de elección viendo que es posible definir conjuntos "raros", sino todo lo contrario, viendo que si descartamos los conjuntos "raros" (los no constructibles) si entendemos que, cuando hablamos de conjuntos, nos referimos únicamente a conjuntos que pueden obtenerse mediante un proceso más o menos "constructivo", entonces el axioma de elección es un teorema, es decir, si un conjunto es constructible, tenemos un criterio para elegirle un elemento. La fórmula $x \trianglelefteq y$ es una fórmula explícita del lenguaje de la teoría de conjuntos que no tiene ningún parámetro aparte de x, y, y define explícitamente un buen orden de la clase L. Si no se puede demostrar que la clase V de todos los conjuntos admite un buen orden, ello se debe a que los axiomas de la teoría de conjuntos no concretan si $V = L$, pero si suponemos que $V = L$, lo cual sólo supone descartar conjuntos "raros" (como deberían aprobar los suspicaces con el axioma de elección), entonces tenemos un criterio explícito para elegir elementos de cualquier conjunto. ∎

En su anuncio de 1938 Gödel había dicho:

> *La proposición A* [es decir, $V = L$]*, añadida como un nuevo axioma, parece completar de forma natural los axiomas de la teoría de conjuntos, ya que determina la vaga noción de un conjunto infinito arbitrario de forma definida. En este sentido, es importante que la prueba de consistencia para A sigue siendo válida si se añaden axiomas de infinitud más fuertes (por ejemplo, la existencia de números inaccesibles) a T. Por lo tanto, la consistencia de A parece ser absoluta en cierto sentido, aunque, en la situación actual, no es posible dar un significado preciso a esta frase.*

No obstante, como veremos enseguida, unos años más tarde Gödel cambiaría de opinión y dejaría de considerar al axioma de constructibilidad como una "compleción natural" de los axiomas de la teoría de conjuntos.

Lo que dice sobre cardinales inaccesibles es lo siguiente: si κ es un cardinal (débilmente) inaccesible, no es difícil ver que sigue siendo débilmente inaccesible cuando eliminamos los conjuntos no constructibles. Pero como entonces se cumple la hipótesis del continuo generalizada, κ es de hecho un cardinal fuertemente inaccesible, y en la página 105 hemos visto que la existencia de un cardinal fuertemente inaccesible implica $\mathrm{Cons}\ulcorner\mathrm{ZFC}\urcorner$. Por lo tanto, ahora podemos afirmar que la mera existencia de un cardinal débilmente inaccesible ya implica $\mathrm{Cons}\ulcorner\mathrm{ZFC}\urcorner$, por lo que las consecuencias que extraíamos en la página 105 sobre la consistencia de que existan cardinales fuertemente inaccesibles valen ahora para cardinales débilmente inaccesibles.[115]

[115] Sin suponer $V = L$, puede probarse que si κ es un cardinal débilmente inaccesible, entonces L_κ es un modelo de ZFC.

Gödel no llegó a publicar ninguna demostración de la consistencia de las dos últimas afirmaciones que había hecho en su anuncio de 1938, pero lo cierto es que, suponiendo $V = L$, es posible demostrar ambas: existen subconjuntos de $\mathbb{R}$ de tipo $\mathbf{\Delta}^1_2$ que no son medibles Lebesgue, y existen subconjuntos coanalíticos (es decir, de tipo $\mathbf{\Pi}^1_1$ que tienen el cardinal del continuo (es decir, $\aleph_1$), pero no contienen subconjuntos perfectos.

La razón es que el buen orden constructible $x \trianglelefteq y$ es una fórmula con una estructura relativamente simple, y Gödel demostró que si $V = L$, entonces la restricción de $\trianglelefteq$ a $\mathbb{R}$, es decir, el conjunto $\{(x, y) \in \mathbb{R}^2 \mid x \trianglelefteq y\}$ es de tipo $\mathbf{\Delta}^1_2$ y a partir de este hecho[116] se pueden construir los ejemplos requeridos.

Estos ejemplos ponían de manifiesto que la lógica matemática tenía algo que decir incluso en problemas correspondientes a ramas de la matemática distintas de la teoría de conjuntos pura, como era el caso de la teoría descriptiva de conjuntos, que partía de la idea de no estudiar "conjuntos abstractos", sino conjuntos que, en cierto sentido, podían construirse.

En 1947 Gödel publicaría un artículo de divulgación titulado *¿Qué es el problema del continuo de Cantor?*, en el que explicó su punto de vista sobre el problema en general y sobre lo que aportaba su demostración en particular. Merece la pena comentarlo: primero Gödel formula el problema y señala lo poco que se sabe sobre la exponenciación de cardinales, pues ni siquiera se puede probar que $2^{\aleph_0} < 2^{\aleph_1}$. Sobre esto apunta:

> *Esta escasez de resultados, incluso en lo tocante a las cuestiones más fundamentales en esta área, puede deberse hasta cierto punto a dificultades puramente matemáticas, pero parece que hay también razones más profundas tras ella y que una solución completa de estos problemas sólo puede obtenerse por un análisis más profundo (de lo que es habitual entre los matemáticos) del significado de los términos involucrados (como "conjunto", "biyección", etc.) y de los axiomas subyacentes a su uso.*

Gödel se refiere a que la hipótesis del continuo podría ser indecidible, y que, en tal caso, para decidirla, sería necesario reconsiderar los axiomas de la teoría de conjuntos. Para tratar el posible significado de los axiomas, empieza describiendo la postura de los intuicionistas, y sobre ella dice:

> *Esta actitud negativa hacia la teoría de conjuntos de Cantor y hacia la matemática clásica, de la que es una generalización natural, no es de ningún modo, sin embargo, un resultado necesario de un examen detallado de sus fundamentos, sino únicamente una consecuencia de una cierta concepción filosófica de la naturaleza de las matemáticas, que admite objetos matemáticos sólo en la medida en que sean (o se crea que son) interpretables como construcciones nuestras o, al menos, completamente accesibles a nuestra intuición. Para quien no comparta estos puntos de vista, existe una fundamentación satisfactoria de la teoría de conjuntos de Cantor en toda su extensión original, a saber, la teoría axiomática de conjuntos.* [...]
>
> *Podría pensarse en un primer momento que las paradojas de la teoría de conjuntos obstaculizarían tal intento, pero un examen detallado muestra que no suponen problema alguno. Son un problema muy serio, pero no para la teoría de conjuntos de Cantor. En la medida en que los conjuntos aparecen y se necesitan en las matemáticas (al menos en las matemáticas actuales, incluyendo toda la teoría de conjuntos de Cantor), son conjuntos de enteros, o de números racionales (es decir, de pares de enteros), o de números reales (es decir, de conjuntos de números racionales), o de funciones de números reales (es decir, de conjuntos de pares de números reales), etc.; Cuando se enuncian teoremas sobre todos los conjuntos (o sobre la existencia de conjuntos) en general, siempre pueden interpretarse sin dificultad como que se cumplen para conjuntos de enteros, así como para conjuntos de números reales, o ... etc., que tienen la propiedad enunciada. Sin embargo, este concepto de conjunto, según el cual un conjunto es algo obtenible a partir de los enteros (u otros objetos bien definidos) por la aplicación iterada de la operación "conjunto de", y no algo obtenido dividiendo la totalidad de los objetos existentes en dos categorías, nunca ha llevado a antinomia alguna; es decir, que el trabajo completamente "ingenuo" y acrítico con este concepto de conjunto ha resultado hasta ahora completamente autoconsistente.*

Esto significa que las contradicciones surgen del supuesto de que podemos definir conjuntos mediante propiedades arbitrarias (dividiendo a todos los objetos en dos categorías: los que pertenecen a un conjunto dado y los que no), pero no surge ninguna contradicción cuando pensamos en los conjuntos como los objetos que produce la jerarquía acumulativa de von Neumann. (Gödel habla de partir del conjunto de los números naturales y no del conjunto vacío para no tener que explicar cómo pueden surgir todos los conjuntos del conjunto vacío).

[116] En 1951, en una segunda edición de su libro, añadió una nota señalando este hecho.

> *Pero, más aún, los axiomas que subyacen en este uso irrestricto de este concepto de conjunto o, al menos, de una porción de ellos que basta para todas las demostraciones matemáticas conocidas hasta ahora han sido formulados de forma tan precisa en la teoría axiomática de conjuntos que la cuestión de si una proposición determinada se sigue de ellos puede transformarse, a través del simbolismo lógico, en un problema puramente combinatorio sobre la manipulación de signos que hasta el intuicionista más radical tiene que reconocer como significativo. Así, el problema del continuo de Cantor, independientemente de la posición filosófica que uno adopte, conserva innegablemente este sentido: determinar si de los axiomas de la teoría de conjuntos se puede derivar una respuesta y, si es así, cuál.*

En efecto, incluso un intuicionista tiene que admitir como un problema con un sentido preciso y concreto el de si la hipótesis del continuo se puede demostrar o refutar a partir de los axiomas de la teoría de conjuntos (esto es un problema estrictamente finitista), independientemente de que admita que las afirmaciones involucradas en la prueba signifiquen algo o no.

> *Por supuesto, si se interpreta de este modo, hay* a priori *(suponiendo la consistencia de los axiomas) tres posibilidades para la conjetura de Cantor: puede ser demostrable, refutable o indecidible. La tercera alternativa (que es sólo una formulación precisa de la conjetura enunciada antes de que las dificultades del problema no son quizá puramente matemáticas) es la más plausible, y buscar una demostración de ello es actualmente una de las vías más prometedoras de abordar el problema. Un resultado en esta dirección ya ha sido obtenido, a saber, que la conjetura de Cantor no es refutable a partir de los axiomas de la teoría de conjuntos, supuesto que éstos sean consistentes.*

A continuación Gödel declara su punto de vista platonista:

> *Debe señalarse, no obstante, que incluso si se lograra demostrar esta indemostrabilidad, esto no zanjaría en modo alguno la cuestión de forma definitiva (al contrario de lo que sucede, por ejemplo, con una demostración de la trascendencia de π). Sólo alguien que (como los intuicionistas) niegue que los axiomas y los conceptos de la teoría de conjuntos clásica tengan significado (o algún significado bien definido)*[117] *quedaría satisfecho con tal solución, pero no quien crea que éstos describen una realidad bien definida. Y tal creencia no es en modo alguno quimérica, ya que es posible señalar caminos por los que podría, no obstante, decidirse el problema, aunque éste sea indecidible a partir de los axiomas en su forma actual.*
>
> *En primer lugar, los axiomas de la teoría de conjuntos no forman en absoluto un sistema cerrado en sí mismo, sino que, más bien al contrario, el mismo concepto de conjunto en el que se basan sugiere su extensión mediante nuevos axiomas que afirman la existencia de más iteraciones del operador "conjunto de". Estos axiomas pueden formularse también como proposiciones que afirman la existencia de cardinales muy grandes o (lo que es lo mismo) de conjuntos que tengan dichos cardinales. El más simple de estos "axiomas de infinitud" fuertes afirma la existencia de cardinales inaccesibles (y de cardinales fuertemente inaccesibles). Este último axioma, simplificando, sólo significa*[118] *que la totalidad de los conjuntos obtenibles por los procesos de formación de conjuntos expresados en los otros axiomas forma a su vez un conjunto (y, por consiguiente, una nueva base para nuevas aplicaciones de estos procesos).* [...] *Poco se sabe de esta parte de la teoría de conjuntos, pero, en cualquier caso, estos axiomas muestran claramente, no sólo que el sistema axiomático de la teoría de conjuntos, en su estado actual, es incompleto, sino también que puede ser suplementado sin arbitrariedad por nuevos axiomas que son sólo la prolongación natural de la serie de axiomas formulados hasta ahora.*
>
> *Puede probarse que estos axiomas tienen consecuencias muy alejadas del dominio de los cardinales transfinitos muy grandes, que son su objeto inmediato. Puede probarse que cada uno de ellos, hasta*

[117] El matiz es que alguien podría admitir que todo sistema de axiomas consistente tiene un significado (pues, como el propio Gödel había demostrado, admite un modelo, pero puede no tener ningún modelo "natural", sino distintos modelos, en algunos de los cuales la hipótesis del continuo podría ser cierta y en otros falsa, sin que se pueda decir cuál de ellos corresponde a los conjuntos "de verdad". No es el punto de vista de Gödel, que sostiene que sí que existe una interpretación "bien definida", distinta de cualquier otra "impostora", como los modelos no estándar de la aritmética de Peano son modelos "impostores" no equiparable al modelo natural, formado por los números naturales "de verdad", $0, 1, 2, \ldots$, sin añadidos.

[118] Esto lo hemos tratado en el apartado sobre cardinales fuertemente inaccesibles, en la página 87.

donde sabemos, bajo el presupuesto de su consistencia, aumenta el número de proposiciones decidibles incluso en el campo de las ecuaciones diofánticas.[119]

En lo que respecta al problema del continuo, hay pocas esperanzas de que pueda resolverse mediante estos axiomas de infinitud que pueden formularse tomando como base los principios conocidos hasta la fecha (la prueba antes mencionada de la irrefutabilidad de la hipótesis del continuo, por ejemplo, sigue valiendo con ellos sin cambio alguno). Pero es probable que existan otros basados en principios desconocidos hasta ahora; y también puede que existan, además de los axiomas ordinarios y los axiomas de infinitud, otros axiomas de la teoría de conjuntos (desconocidos hasta ahora) que un entendimiento más profundo de los conceptos subyacentes a la lógica y las matemáticas nos permitiría reconocer como consecuencias de dichos conceptos.

Además, incluso ignorando la necesidad intrínseca de algún nuevo axioma, e incluso en el caso de que no hubiera ninguna necesidad intrínseca en absoluto, es posible determinar su verdad también de otra manera, a saber, inductivamente, estudiando su "éxito", es decir, su fecundidad en consecuencias, y en particular en consecuencias "verificables", es decir, consecuencias demostrables sin el nuevo axioma, pero cuyas demostraciones mediante éste son, sin embargo, considerablemente más sencillas y fáciles de descubrir, y permiten condensar en una sola demostración muchas demostraciones diferentes. Los axiomas para el sistema de números reales, rechazados por los intuicionistas, se han verificado hasta cierto punto en este sentido, debido a que la teoría analítica de números con frecuencia nos permite demostrar teoremas teóricos de números que posteriormente pueden verificarse mediante métodos elementales. Sin embargo, es concebible un grado de verificación mucho mayor. Podrían existir axiomas con tantas consecuencias verificables, que arrojaran tanta luz sobre toda una disciplina y proporcionaran métodos tan poderosos para resolver problemas dados (e incluso resolverlos, en la medida de lo posible, de manera constructivista) que, independientemente de su necesidad intrínseca, tendrían que asumirse al menos en el mismo sentido que cualquier teoría física bien establecida.

A partir de aquí Gödel pasa a extraer conclusiones de su prueba de consistencia.

¿Son estas consideraciones apropiadas para el problema del continuo? ¿Existen realmente indicios sólidos de su insolubilidad mediante los axiomas conocidos? Creo que hay al menos dos.

El primero consiste en que existen dos clases de objetos definidas de forma muy diferente, que satisfacen todos los axiomas de la teoría de conjuntos escritos hasta la fecha. Una clase consiste en los conjuntos definibles de cierta manera por las propiedades de sus elementos,[120] *la otra en los conjuntos en el sentido de multitudes arbitrarias, independientemente de si pueden definirse o cómo. Así, sin determinar qué objetos deben contarse y en función de qué correspondencias biunívocas, difícilmente se podría esperar determinar su número (excepto quizás en caso de alguna coincidencia afortunada).*[121] *Si, sin embargo, alguien cree que no tiene sentido hablar de conjuntos excepto en el sentido de extensiones de propiedades definibles, o, al menos, que no existen otros conjuntos, entonces, también, difícilmente puede esperar que más de una pequeña fracción de los problemas de la teoría de conjuntos sean resolubles sin hacer uso de esta característica, en su opinión esencial, de los conjuntos: que todos se derivan de (o, en cierto sentido, incluso son idénticos a) propiedades definibles. Esta característica de los conjuntos, sin embargo, no está formulada explícitamente ni contenida implícitamente en los axiomas aceptados de la teoría de conjuntos. Así pues,* [...] *es plausible que el problema del continuo no se pueda resolver con los axiomas establecidos hasta ahora, pero que, por otro lado, pueda resolverse mediante un nuevo axioma que establezca o al menos implique algo sobre la definibilidad de los conjuntos.*

La segunda mitad de esta conjetura ya se ha verificado; es decir, el concepto de definibilidad recién mencionado (que es a su vez definible en términos de las nociones primitivas de la teoría de conjuntos) permite derivar la hipótesis del continuo generalizada a partir del axioma de que todo

[119] Se refiere a que, por ejemplo, si admitimos que existe un cardinal inaccesible, podemos demostrar Consis$^{\ulcorner}ZFC^{\urcorner}$, que es equivalente a una ecuación diofántica, es decir, a que una ecuación polinómica con coeficientes enteros no tiene soluciones enteras. Esto, tal cual, no estaba demostrado en ese momento, pero sí para una afirmación ligeramente más complicada (que una familia de ecuaciones diofánticas dependiente de unos parámetros no admitiera soluciones enteras).

[120] Aquí, en una nota al pie, Gödel aclara que se refiere a los conjuntos constructibles, y resume su construcción.

[121] Quiere decir que no podemos determinar cuántos números reales hay sin fijar si nos referimos sólo a los constructibles o a otros más generales, salvo que se dé la coincidencia de que haya $\aleph_1$ de todos modos.

> *conjunto es definible en este sentido. Dado que este axioma (llamémoslo "A") resulta demostrablemente consistente con los demás axiomas bajo el supuesto de la consistencia de estos axiomas, este resultado (independientemente de cualquier opinión filosófica) muestra la consistencia de la hipótesis del continuo con los axiomas de la teoría de conjuntos, siempre que estos axiomas sean consistentes.* [...]
>
> *Un segundo argumento a favor de la insolubilidad del problema del continuo sobre la base de los axiomas ordinarios puede fundamentarse en ciertos hechos (desconocidos o inexistentes en la época de Cantor) que parecen indicar que la conjetura de Cantor resultará errónea;*[122] *en caso de una decisión negativa, la cuestión es (como se acaba de explicar) demostrablemente imposible sobre la base de los axiomas tal como se conocen hoy.* [...]
>
> *Se podría decir que muchos de los resultados de la teoría de conjuntos puntuales obtenidos sin utilizar la hipótesis del continuo también son altamente inesperados e implausibles.*[123] *Pero, por cierto que esto sea, la situación es diferente en este caso, ya que en esos casos (como, por ejemplo, las curvas de Peano) la apariencia contraria puede, en general, explicarse por una falta de concordancia entre nuestros conceptos geométricos intuitivos y los de la teoría de conjuntos que aparecen en los teoremas.*[124] *Además, es muy sospechoso que, frente a las numerosas proposiciones plausibles que implican la negación de la hipótesis del continuo, no se conozca ninguna proposición plausible que implique la hipótesis del continuo. Por lo tanto, se puede sospechar con razón que el papel del problema del continuo en la teoría de conjuntos será el siguiente: que finalmente conducirá al descubrimiento de nuevos axiomas que permitirán refutar la conjetura de Cantor.*

Recordemos que Gödel escribió esto en 1947. Vemos así que, como habíamos adelantado, en unos años había dejado de considerar al axioma de constructibilidad una extensión plausible de la axiomática de la teoría de conjuntos.

Ese mismo año de **1940** Quine publicó su libro *Lógica Matemática* en el que expuso LM, una versión de su teoría NF que incluía clases propias, al estilo de NBG, pero en 1942 Rosser demostró que era contradictoria, pues permitía formalizar la antinomia de Burali-Forti.

En **1941** Bernays publicó *Un sistema de teoría axiomática de conjuntos-Parte II,* en el que añade los axiomas que faltaban para completar la teoría de conjuntos de von-Neumann-Bernays y los usa para construir los ordinales y —como caso particular— los números naturales. La definición que da de ordinal, aunque es equivalente a la de von Neumann o a la que había adoptado Gödel, es especialmente simple, pues no hace referencia a la buena ordenación, y había aparecido por primera vez en 1937 en un trabajo[125] de Raphael Mitchel Robinson sobre la teoría de von Neumann. Según esta definición, un conjunto α es un ordinal si cumple dos propiedades:

1. α es transitivo (es decir, que si $u \in v$ y $v \in \alpha$, entonces $u \in \alpha$).
2. Si $u, v \in \alpha$ son dos elementos distintos, o bien $u \in v$ o bien $v \in u$.

El lector puede comprobar que los ordinales finitos:

$$0 = \varnothing, \quad 1 = \{0\}, \quad 2 = \{0, 1\}, \quad 3 = \{0, 1, 2\}, \quad 4 = \{0, 1, 2, 3\}, \quad \dots$$

cumplen estas dos propiedades. Aunque no es trivial, sucede que bastan para definir los ordinales.

En **1942** Bernays publicó la tercera y la cuarta parte de este trabajo. En la tercera discute la formalización en su teoría del análisis matemático y señala que, en este contexto, en muchas ocasiones algunos axiomas y, en especial, el axioma de elección pueden ser restringidos a otras formas más débiles. Concretamente, para el axioma de elección considera dos de ellas, que, con la nomenclatura y formulación modernas son:

Axioma de elección numerable Si $\{A_n\}_{n=0}^{\infty}$ es una familia numerable de conjuntos no vacíos, existe una función que a cada número natural n le asigna un elemento de A_n.

[122] En una nota al pie, Gödel cita un artículo de Lusin, donde considera "fuera de duda" que todo subconjunto de $\mathbb{R}$ de cardinal $\aleph_1$ es coanalítico. Pero hay $2^{\aleph_0}$ subconjuntos coanalíticos de $\mathbb{R}$ y $2^{\aleph_1}$ subconjuntos de cardinal $\aleph_1$ luego la hipótesis de Lusin implica que $2^{\aleph_0} = 2^{\aleph_1} > \aleph_1$. Luego cita en el texto algunas propiedades más que omitimos, porque no se relacionan con lo que hemos visto aquí.

[123] Aquí Gödel cita un artículo que explica la paradoja de Banach-Tarski y algunos resultados relacionados.

[124] Ésta es una idea muy importante —que ya hemos discutido— a la hora de no distorsionar el papel que es razonable conceder a la intuición en el razonamiento matemático (véase la página 77).

[125] *La teoría de clases: una modificación del sistema de von Neumann.*

Principio de elecciones dependientes Si R es una relación en una clase A tal que, para cada $a \in A$, existe un $b \in A$ de modo que $b\,R\,a$, entonces para cada $a \in A$ existe una sucesión $\{a_n\}_{n=0}^{\infty}$ tal que $a = a_0$ y $a_{n+1}\,R\,a_n$.

Esto significa que es posible llevar a cabo una cantidad numerable de elecciones, pero de modo que el conjunto en el que se realiza la elección n-sima depende de las elecciones precedentes.

En la cuarta parte expone los hechos básicos sobre cardinales y en la quinta, publicada en **1943**, demuestra el teorema de recursión transfinita y lo usa para demostrar el lema de Zorn y otras formas del axioma de elección, y para introducir la aritmética ordinal. En 1948 publicaría una sexta parte dedicada al axioma de regularidad.

69 El problema de Suslin El problema número 3 publicado póstumamente por Suslin en el primer número de *Fundamenta Mathematicae* (véase la página 55) puede reformularse así:

> **Problema de Suslin** Si R es un conjunto totalmente ordenado completo (en el sentido de que todo subconjunto no vacío tiene supremo) y denso en sí mismo (es decir, de modo que entre dos cualesquiera de sus puntos haya un tercero) y en el que toda familia de intervalos no vacíos disjuntos dos a dos es a lo sumo numerable, ¿es R similar en cuanto al orden al intervalo $[0, 1]$ de la recta real?

Una variante equivalente es:

> **Problema de Suslin** Si R es un conjunto totalmente ordenado completo (en el sentido de que todo subconjunto no vacío a acotado superiormente tiene supremo), sin máximo ni mínimo y denso en sí mismo (es decir, de modo que entre dos cualesquiera de sus puntos haya un tercero) y en el que toda familia de intervalos no vacíos disjuntos dos a dos es a lo sumo numerable, ¿es R similar en cuanto al orden a la recta real?

Cantor había demostrado (véase la página 23) que la respuesta es afirmativa si sustituimos la condición sobre los intervalos por la condición de que R tenga un subconjunto denso numerable D (es decir, un conjunto tal que entre dos puntos de R haya siempre uno de D). Notemos que esta condición implica que toda familia de intervalos no vacíos disjuntos dos a dos es a lo sumo numerable, pues cada intervalo de la familia debe contener al menos un elemento distinto de D y sólo hay una cantidad numerable de posibilidades. El problema de Suslin es si se da el recíproco, es decir, si la condición de que las familias de intervalos disjuntos sean numerables implica la existencia de un subconjunto denso numerable.

En **1943** se publicó un artículo titulado *Una nota sobre el problema de Suslin,* de Edwin W. Miller, un profesor de la universidad de Michigan que había fallecido el año anterior, a los 37 años. En este artículo póstumo, Miller mostraba que el problema de Suslin era equivalente a un problema conceptualmente mucho más simple sobre conjuntos parcialmente ordenados:

> *Como es bien sabido, las siguientes propiedades caracterizan al continuo lineal L como un tipo de orden lineal.*
>
> *(*1) *L no tiene primer ni último elemento.*
>
> (2) *L es continuo; es decir, cada corte en L es un corte de Dedekind.*
>
> (3) *Existe un subconjunto numerable D de L tal que entre dos elementos cualesquiera de L hay un elemento de D.*
>
> *Como consecuencia inmediata de (3), tenemos:*
>
> (4) *Todo conjunto de intervalos en L que no se solapen es numerable.*
>
> *Suslin planteó la pregunta siguiente: ¿Caracterizan las propiedades* (1), (2) *y* (4) *el continuo lineal? En otras palabras, ¿las propiedades* (1), (2) *y* (4) *implican la propiedad* (3)*?*
>
> *El propósito del presente artículo es demostrar el siguiente*
>
> Teorema. *Para que exista un orden lineal que posea las propiedades* (1), (2) *y* (4) *sin poseer la propiedad* (3)*, es necesario y suficiente que exista un orden parcial P de potencia $\aleph_1$, tal que:*
>
> (a) *si $Q \subset P$ y $\overline{\overline{Q}} = \aleph_1$, entonces Q contiene dos elementos comparables y dos elementos no comparables;*
>
> (b) *si x e y son elementos no comparables de P, entonces no existe ningún z en P tal que $x < z$ e $y < z$.*

Conviene reformular un poco el enunciado. Los conjuntos L que cumplen (1), (2) y (4) pero no (3) se llaman[126] *rectas de Suslin.* Un subconjunto de un conjunto parcialmente ordenado es una *cadena* si todos sus elementos son comparables, y es una *anticadena* si sus elementos son incompatibles (es decir, no comparables) dos a dos. En estos términos, el resultado de Miller puede enunciarse así:

> Existe una recta de Suslin si y sólo si existe un conjunto parcialmente ordenado P tal que:
>
> (a) Todas las cadenas y todas las anticadenas de P son a lo sumo numerables.
>
> (b) Si $z \in P$, la sección inicial $\{x \in P \mid x < z\}$ está totalmente ordenada.

Sin embargo, lo cierto es que, cuando Miller parte de una recta de Suslin y construye un conjunto P en estas condiciones, de hecho construye uno en el que las secciones iniciales están bien ordenadas. Esto nos lleva a su vez a las definiciones siguientes:

> Un *árbol* es un conjunto parcialmente ordenado A cuyas secciones iniciales están bien ordenadas. Un *árbol de Suslin* es un árbol de cardinal $\aleph_1$ cuyas cadenas y anticadenas son a lo sumo numerables.

En estos términos, Miller había demostrado que existe una recta de Suslin si y sólo si existe un árbol de Suslin. Una implicación es muy sencilla:

DEMOSTRACIÓN: Supongamos que existe una recta de Suslin L y vamos a construir a partir de ella un árbol de Suslin A. Los elementos de P serán intervalos cerrados $[a, b]$ en L con $a < b$, y la relación de orden será la inversa de la inclusión, es decir, $I_1 \leq I_2$ si y sólo si $I_2 \subset I_1$.

Vamos a definir, por recursión transfinita, una familia $\{I_\alpha\}_{\alpha<\omega_1}$, de intervalos cerrados de L. Tomamos como $I_0 = [a_0, b_0]$ cualquier intervalo, con $a_0 < b_0$. Supongamos definidos $\{I_\beta\}_{\beta<\alpha}$, para cierto ordinal numerable $\alpha < \omega_1$, donde $I_\beta = [a_\beta, b_\beta]$. El conjunto E formado por todos los extremos a_β y b_β es numerable, y estamos suponiendo que L no tiene subconjuntos densos numerables. Por lo tanto no es denso, lo cual significa que existe un intervalo $I_\alpha = [a_\alpha, b_\alpha]$, con $a_\alpha < b_\alpha$ que no contiene puntos de E. Esto hace que, si $\beta < \alpha$, o bien $I_\alpha \subset I_\beta$ (con una inclusión estricta), o bien I_α e I_β son disjuntos.

Entonces, si consideramos a $P = \{I_\alpha \mid \alpha < \omega_1\}$ con el orden dado por la inversa de la inclusión, tenemos ciertamente que P tiene cardinal $\aleph_1$ y, fijado $x = I_\alpha \in P$, la sección inicial $P_x = \{y \in P \mid y < x\}$ está formada por intervalos $y = I_\beta$ tales que $x = I_\alpha \subset I_\beta = y$ (con una inclusión estricta) lo cual sólo puede suceder si $\beta < \alpha$, y si $I_\alpha \subset I_\beta$ e $I_\alpha \subset I_{\beta'}$, necesariamente $I_\beta \subset I_{\beta'}$ o bien $I_{\beta'} \subset I_\beta$, ya que la alternativa es que I_β e $I_{\beta'}$ sean disjuntos, y entonces no contendrían a I_α.

Por lo tanto, la sección P_x está totalmente ordenada y, de hecho, está bien ordenada, pues la aplicación $I_\beta \mapsto \beta$ es una aplicación $P_x \longrightarrow \alpha$ inyectiva que conserva el orden, ya que si $\beta < \beta' < \alpha$, la única inclusión que puede darse por construcción es $I_{\beta'} \subset I_\beta$ (es decir, $I_\beta < I_{\beta'}$) y no la contraria. Como α está bien ordenado, esto implica que P_x también lo está. Así pues, P es un árbol.

Toda anticadena en P es una familia de intervalos de L disjuntos dos a dos, luego es numerable porque L cumple la propiedad (4). Por último, si $\{J_\alpha\}_{\alpha<\omega_1}$ fuera una cadena no numerable en P, donde $J_\alpha = [c_\alpha, d_\alpha]$, los intervalos $]c_\alpha, c_{\alpha+1}[$ serían disjuntos dos a dos, pues si $\alpha < \beta$, entonces $\alpha + 1 \leq \beta$, luego

$$[c_{\beta+1}, d_{\beta+1}] \subset [c_\beta, d_\beta] \subset [c_{\alpha+1}, d_{\alpha+1}] \subset [c_\alpha, d_\alpha]$$

y entonces $c_\alpha < c_{\alpha+1} \leq c_\beta < c_{\beta+1}$ (porque, por construcción, ningún intervalo de P tiene un extremo en común con otro). Por lo tanto, $]c_\alpha, c_{\alpha+1}[$ es disjunto de $]c_\beta, c_{\beta+1}[$, en contra de la propiedad (4) de L. ∎

La prueba del recíproco es más técnica, porque, en primer lugar, requiere "podar" el árbol de Suslin quitándole todos los nodos que no tiene $\aleph_1$ elementos por encima, luego se construye un conjunto totalmente ordenado L_0 formado por las ramas (numerables) del árbol y luego hay que completar L_0 hasta una recta de Suslin L por el mismo procedimento con el que Dedekind construyó $\mathbb{R}$ a partir de $\mathbb{Q}$.

Observemos que en cualquier árbol A (en el sentido que le hemos dado aquí) se puede hablar de la altura de un nodo x, definida como el ordinal de la sección inicial A_x, así como del nivel de altura α, formado por todos los elementos de altura α, que necesariamente es una anticadena (pero no toda anticadena tiene por qué ser un nivel). Recordemos que el teorema de Kőnig (sección 37) afirma que si un árbol de cardinal $\aleph_0$ tiene niveles de cardinal $< \aleph_0$, entonces tiene una rama de cardinal $\aleph_0$. El enunciado análogo cambiando $\aleph_0$ por $\aleph_1$ sería: "Si un árbol de cardinal $\aleph_1$ tiene niveles numerables, entonces tiene una rama no numerable." Un árbol de Suslin contradice esta generalización, pues tiene niveles numerables, pero no tiene ramas no numerables).

[126] Hay que entender (2) como equivalente a que L es denso en sí mismo y completo en el sentido de Dedekind.

En 1935 habían leído su tesis dos matemáticos yugoslavos de 28 años bajo la dirección de Fréchet. Se llamaban Đuro Kurepa y Nachman Aronszajn. El segundo se había doctorado también en Varsovia en 1930 bajo la dirección de Mazurkiewicz. La tesis de Kurepa se titulaba *Conjuntos ordenados y ramificados,* y se dice que en ella ya estaba demostrado el teorema de Miller, sólo que hace falta mucha paciencia para encontrarlo y reconocerlo, por la oscuridad de la presentación, que acumula una definición sobre otra, así que es disculpable que Miller no hubiera estado al tanto. Kurepa no supo decidir si existen o no árboles de Suslin, pero sí que mostró una construcción que atribuyó a Aronszajn de un árbol de cardinal $\aleph_1$ con niveles numerables y sin ramas no numerables. Para que fuera un árbol de Suslin le faltaría que sus anticadenas (no sólo los niveles) fueran numerables. La existencia de *árboles de Aronszajn* muestra, de todos modos, que el análogo para $\aleph_1$ del teorema de Kőnig es falso. Un árbol puede tener niveles numerables y elementos de cualquier altura numerable, pero a la vez puede que no haya en él ninguna rama que permita subir hasta cualquier altura. Si una rama llega, digamos, hasta altura α, será necesario salirse de ella para llegar a una altura β mayor.

70 El fin de la guerra Hausdorff se había librado de ser expulsado de la universidad de Bonn cuando Hitler llegó al poder debido a que de joven había servido como voluntario en el ejército alemán, y permaneció dos años en su puesto hasta que se jubiló en 1935, con 67 años. Pero en 1939, *tras la noche de los cristales rotos,* su situación empeoró. En 1940 pidió permiso para emigrar, pero le fue denegado. Tuvo que soportar confiscaciones e impuestos abusivos que lo llevaron a pasar hambre. En 1941 fue obligado a llevar la estrella de David. En 1942 le comunicaron que debía trasladarse al gueto de Bonn, lo que era un paso previo para que fuera enviado a un campo de exterminio. Unos días antes de que venciera el plazo se suicidó junto a su esposa y su cuñada, mediante una sobredosis de un barbitúrico.

En **1943**, doce días después de la derrota alemana en Stalingrado, Hilbert murió en Gotinga, a los 81 años. A su funeral asistió apenas una docena de personas, de las cuales sólo dos eran matemáticos. La mayor parte de sus antiguos colegas estaba en los Estados Unidos, donde se le rindieron múltiples homenajes.

En **1944** fue Dénes Kőnig el que se suicidó (a los 60 años) para no caer en manos de los nazis (su padre había sido judío, pero se había convertido al cristianismo a los 40 años). Tras el alzamiento de Varsovia, Mostowki evitó ser internado en un campo de concentración gracias a la ayuda de unas enfermeras y huyó a Canadá.

Gentzen terminó ese año su servicio militar y obtuvo una plaza en la Universidad Alemana de Praga a la vez que trabajaba en el proyecto de cohetes V-2, que era la última esperanza de Hitler para cambiar el curso de la guerra. Para muchos checos, Gentzen era un nazi que les había sido impuesto por el invasor alemán. En **1945** los praguenses se rebelaron contra la ocupación nazi. Los estadounidenses estaban muy cerca, pero los soviéticos exigieron que se respetaran los acuerdos previos según los cuales les correspondía a ellos ocupar esa zona. Esperaron a que los nazis acabaran con todos los rebeldes no comunistas y finalmente entraron en la ciudad. Gentzen, igual que el resto de profesores alemanes, fue capturado por los comunistas e internado en un campo de concentración, en el que moriría de hambre unos meses más tarde, a los 35 años. Un amigo que estuvo con él en sus últimos días contaría más adelante:

> *Aún puedo verlo tumbado en su litera de madera pensando todo el día en los problemas matemáticos que le preocupaban. Una vez me confesó que estaba muy contento, pues por fin tenía tiempo para pensar en una prueba de consistencia para el análisis.* [...] *También se ocupaba de otras cuestiones, como la de un lenguaje artificial, etc. De vez en cuando charlaba un rato.* [...] *Nos aseguraban constantemente que los trámites de nuestra liberación sólo tardarían unos días más.* [...] *Esperaba poder regresar a Gotinga y dedicarse de lleno al estudio de la lógica matemática y los fundamentos de las matemáticas. Soñaba con un instituto para este fin.*

Banach había sobrevivido a la ocupación nazi de Polonia gracias en gran parte a la protección del biólogo polaco Rudolf Weigl.[127] Sin embargo, murió en **1945**, a los 53 años, de un cáncer de pulmón.

Los nazis habían ocupado los Países Bajos en 1940, y unos meses después, ese mismo año, Brouwer fue nombrado rector de la Universidad de Amsterdam. Apenas ocupó el cargo un año, pero dio la imagen de ser más sumiso a las directrices nazis de lo que hubiera sido disculpable en el contexto histórico, especialmente por su cooperación en la expulsión de estudiantes y profesores judíos. En **1945** fue investigado en el "proceso de purificación" que tuvo lugar tras la guerra y en 1946 fue suspendido de su puesto en la Universidad por el

[127] Weigl era de ascendencia alemana, y los nazis estaban interesados en su trabajo en el diseño de una vacuna contra el tifus, y lo aprovechó para emplear a miles de judíos e intelectuales en su Instituto de Investigación sobre el Tifus y los Virus, en muchos casos como donantes de sangre para alimentar a piojos.

ministro de Educación. También tuvo que dimitir del comité editorial de la revista *Compositio Mathematica,* de la que había sido un miembro fundador en 1934 y que había dejado de publicarse durante la guerra. En 1947 fue readmitido en la Universidad, pero su imagen pública quedó muy dañada. El comité editorial de *Compositio Mathematica* se negaba a readmitirlo y, finalmente, tras varios años de tensiones, se acordó que su nombre continuara figurando en la portada de la revista, pero en la práctica no fue readmitido en el comité editorial.

71 Categorías Entre los judíos polacos que habían abandonado a tiempo su país se encontraba Samuel Eilemberg, que se había doctorado en 1936 bajo la dirección de Kuratowski y Karol Borsuk, y en 1939, a los 26 años, había emigrado a los Estados Unidos siguiendo el consejo de su padre (sus padres acabarían sus días en un campo de exterminio nazi). En 1941 conoció a Saunders Mac Lane, que era estadounidense, pero se había doctorado en Gotinga en 1934, bajo la dirección de Bernays hasta que éste fue expulsado de la universidad, y entonces, como en el caso de Gentzen, su director había pasado a ser oficialmente Weyl.

La tesis de Mac Lane trataba sobre lógica, pero al regresar a los Estados Unidos se dedicó al álgebra, y al conocer a Eilenberg se interesó por su trabajo en topología algebraica. En particular, ambos se interesaron en presentar axiomatizar el álgebra homológica (axiomatizar en el sentido de dar definiciones análogas a las definiciones de "grupo, anillo, cuerpo, etc." que axiomatizan el álgebra y permiten un tratamiento unificado de resultados correspondientes a contextos distintos). En 1942 publicaron el artículo *Extensiones de grupos y homología* en el que hablan repetidamente de definiciones "naturales" (con las comillas incluidas) de homomorfismos, indicando que esa "naturalidad" hace referencia a que se definen sin elecciones arbitrarias, que podrían dar a objetos distintos según la elección de cada cual.[128] Sin embargo, en una de las secciones del artículo demuestran un teorema que pretende expresar en qué se plasma concretamente esa "naturalidad". Eilenberg y Mac Lane se dieron cuenta de que en su trabajo, y en muchos otros del área de la topología algebraica e incluso del álgebra en general, había ciertas ideas comunes que nunca habían sido aisladas adecuadamente para entenderlas a fondo. Finalmente, en **1945** publicaron su artículo *Teoría general de las equivalencias naturales,* en el que introdujeron lo que hoy se conoce como la *teoría de categorías.*

Es difícil entender el aporte que suponía la teoría de categorías sin conocer el estado en ese momento de varias ramas de la matemática como la topología algebraica y el álgebra homológica, pero, dado que la teoría demostró ser relevante en un área mucho mayor, que prácticamente abarca toda la matemática, trataremos de describir brevemente sus ideas fundamentales. Ilustramos las definiciones con el mismo ejemplo que Eilenberg y Mac Lane usan en la introducción de su artículo.[129]

Una *categoría* $\mathcal{C}$ está determinada por los objetos siguientes:

- Una clase $\mathrm{ob}(\mathcal{C})$ de *objetos.* Por ejemplo, podemos considerar la categoría $\mathcal{V}$ cuyos objetos son los espacios vectoriales de dimensión finita[130] sobre $\mathbb{R}$.

- Para cada par de objetos A y B, un conjunto $\hom(A,B)$ de *morfismos* de A en B. Si f es un morfismo de A en B, esto se expresa con la notación $f : A \longrightarrow B$ o $A \xrightarrow{f} B$.

  En principio un morfismo puede ser cualquier cosa, aunque en la mayor parte de los casos los morfismos serán aplicaciones entre objetos. Cada morfismo determina unívocamente su objeto inicial A y su objeto final B. Por ejemplo, los morfismos de la categoría $\mathcal{V}$ son las aplicaciones lineales $f : V \longrightarrow W$ entre espacios vectoriales.[131]

- Para cada terna de objetos A, B, C, una aplicación $\circ : \hom(A,B)\times\hom(B,C) \longrightarrow \hom(A,C)$. En nuestro ejemplo, si $V \xrightarrow{f} W \xrightarrow{g} X$ son dos aplicaciones lineales, la composición $V \xrightarrow{f\circ g} X$ es la aplicación lineal dada por[132] $(f \circ g)(v) = g(f(v))$.

[128] Por ejemplo, una aplicación lineal entre dos espacios vectoriales es "natural" si no depende de ninguna elección de una base de cada espacio, de modo que una elección distinta de lugar a otra aplicación distinta.

[129] Las definiciones que vamos a dar difieren ligeramente de las que aparecen en el artículo.

[130] En términos conjuntistas, un objeto de $\mathcal{V}$ es una terna $(V, +, \cdot)$, donde $+ : V \times V \longrightarrow V$ y $\cdot : \mathbb{R} \times V \longrightarrow V$.

[131] En teoría de conjuntos, si $B \subset C$, toda aplicación $f : A \longrightarrow B$ es también una aplicación $f : A \longrightarrow C$, por lo que una aplicación no determina su espacio final. Por ello tenemos que entender que un objeto de $\hom(V,W)$ es una terna (f, V, W), donde $f : V \longrightarrow W$ es una aplicación lineal.

[132] Aquí nos desviamos del convenio estándar de definir $(g \circ f)(v) = g(f(v))$. Hay que elegir entre la naturalidad de pasar de $g(f(v))$ a $g \circ f$ o la naturalidad de pasar de $V \xrightarrow{f} W \xrightarrow{g} X$ a $f \circ g$. Nosotros elegimos la segunda opción, pues no cuesta nada, al calcular, invertir las letras al pasar de $g(f(v))$ a $(f \circ g)(v)$ o viceversa, pero para pasar de $V \xrightarrow{f} W \xrightarrow{g} X$ a $g \circ f$ hay que leer siempre los diagramas en el sentido opuesto a las flechas.

Para que estos objetos determinen una categoría debe cumplirse que la composición sea asociativa, es decir, que $(f \circ g) \circ h = f \circ (g \circ h)$ siempre que las composiciones están definidas y que, para cada objeto A, exista un morfismo $A \xrightarrow{1_A} A$ (que es fácil probar que es único) tal que, para todos los morfismos $A \xrightarrow{f} B$, $B \xrightarrow{g} A$, se cumpla $1_A \circ f = f$, $g \circ 1_A = g$. El morfismo 1_A se llama *identidad* en A.

Pero, como señalan Eilenberg y Mac Lane:

> *Cabe observar, en primer lugar, que el concepto de categoría es esencialmente auxiliar; nuestros conceptos básicos son, en esencia, los de funtor y transformación natural (éste último se define en el capítulo siguiente). La idea de categoría sólo se requiere por el precepto de que toda función debe tener una clase definida como dominio y una clase definida como rango, y así las categorías se introducen como los dominios y rangos de los funtores.*

Un *funtor covariante / contravariante* $F : \mathcal{A} \longrightarrow \mathcal{B}$ entre dos categorías es una aplicación tal que:

- A cada objeto A de $\mathcal{A}$ le asigna un objeto $F(A)$ de $\mathcal{B}$.
- A cada morfismo $A \xrightarrow{f} B$ le asigna un morfismo $F(A) \xrightarrow{F(f)} F(B)$ (si F es covariante) o $F(B) \xrightarrow{F(f)} F(A)$ (si F es contravariante), de modo que $F(1_A) = 1_{F(A)}$ y $F(f \circ g) = F(f) \circ F(g)$ (o $F(f \circ g) = F(g) \circ F(f)$ para funtores contravariantes).

Veamos tres ejemplos de funtores sobre la categoría $\mathcal{V}$ que hemos definido:

1. El *funtor identidad* $I : \mathcal{V} \longrightarrow \mathcal{V}$ es el funtor covariante que a cada objeto V le hace corresponder $I(V) = V$ y a cada morfismo $V \xrightarrow{f} W$ le hace corresponder $I(f) = f$.
2. El *funtor dual* $* : \mathcal{V} \longrightarrow \mathcal{V}$ es el funtor contravariante que a cada espacio vectorial V le hace corresponder su espacio dual V^*, formado por todas las aplicaciones lineales $V \longrightarrow \mathbb{R}$, y que a cada aplicación lineal $V \xrightarrow{f} W$ le hace corresponder la aplicación dual $W^* \xrightarrow{f^*} V^*$ dada por $f^*(g) = f \circ g$.
3. El *funtor bidual* $** : V \longrightarrow V$ es el funtor covariante que a cada espacio vectorial V le hace corresponder su bidual V^{**} y a cada aplicación lineal $V \xrightarrow{f} W$ le hace corresponder su bidual $V^{**} \xrightarrow{f^{**}} W^{**}$.

Y con esto podemos introducir el concepto fundamental de la teoría:

Dados dos funtores covariantes $F, G : \mathcal{A} \longrightarrow \mathcal{B}$ entre dos categorías (la definición para funtores contravariantes es análoga) una *transformación natural* $\eta : F \longrightarrow G$ es una aplicación que a cada objeto A de $\mathcal{A}$ le asigna un morfismo $F(A) \xrightarrow{\eta_A} G(A)$, de modo que, para todo morfismo $A \xrightarrow{f} B$, el diagrama siguiente es conmutativo:

$$\begin{array}{ccc} F(A) & \xrightarrow{F(f)} & F(B) \\ {\scriptstyle \eta_A}\downarrow & & \downarrow{\scriptstyle \eta_B} \\ G(A) & \xrightarrow[G(f)]{} & G(B) \end{array}$$

(es decir, $F(f) \circ \eta_B = \eta_A \circ G(f)$).

Por ejemplo, podemos definir una transformación natural $\eta : I \longrightarrow **$ definiendo, para cada espacio vectorial V, la aplicación lineal $\eta_V : V \longrightarrow V^{**}$ que a cada $v \in V$ le asigna $\eta_V(v) \in V^{**}$, es decir, la aplicación lineal $\eta_V(v) : V^* \longrightarrow \mathbb{R}$, dada por $\eta_V(v)(f) = f(v)$.

Como los espacios vectoriales son de dimensión finita, cada η_V es un isomorfismo. Lo que hemos hecho es definir "de forma natural" un isomorfismo η_V entre cada espacio vectorial de dimensión finita (sobre $\mathbb{R}$, aunque vale cualquier cuerpo) y su bidual. Cuando se dice que un espacio vectorial de dimensión finita es "naturalmente isomorfo" a su bidual, esto significa informalmente que es posible definir el isomorfismo mediante $\eta_V(v)(f) = f(v)$, de modo que la definición no depende de ninguna elección arbitraria de una base en V. Pero en la teoría de categorías esto se plasma en el hecho de que η es una transformación natural en el sentido que acabamos de definir. En cambio, aunque cada espacio vectorial de dimensión finita V es isomorfo a su dual V^*, esto se debe a que ambos tienen la misma dimensión, pero no es posible definir un isomorfismo $V \longrightarrow V^*$ sin fijar arbitrariamente una base en V. Un espacio vectorial de dimensión finita es isomorfo, pero no naturalmente isomorfo, a su dual.

No es posible hacerse una idea de la potencia de la teoría de categorías a partir de las meras definiciones que hemos dado (como tampoco podría alguien formarse una idea fiel de lo que puede hacerse en ZFC sin más que ver sus axiomas). Del mismo modo que la teoría de conjuntos permite definir objetos matemáticos cuya complejidad no puede adivinarse a partir del carácter elemental de sus axiomas, lo mismo sucede con la teoría de categorías, que permite definir conceptos muy sofisticados y demostrar resultados profundos sobre ellos.

De hecho, esto tampoco se entendía plenamente en esta época, y durante algunos años la teoría de categorías fue vista meramente como un lenguaje útil para expresar de forma unificada una serie de resultados válidos en diversos contextos matemáticos.

En nuestro contexto, lo que más nos interesa es que la teoría de categorías plantea un problema no trivial, y es que no es evidente cómo encaja en una teoría axiomática de conjuntos. Las categorías más interesantes son "demasiado grandes" para "caber" en ZFC. Por ejemplo, hemos hablado de la categoría $\mathcal{V}$ de todos los espacios vectoriales sobre $\mathbb{R}$ de dimensión finita, pero en ZFC se demuestra que no existe ningún conjunto que contenga a todos los objetos de $\mathcal{V}$. Eilenberg y Mac Lane eran conscientes de ello, y a este respecto dicen:

> *En el apartado 3 señalamos que ejemplos como la "categoría de todos los conjuntos" y la "categoría de todos los grupos" son ilegítimos. Las dificultades y antinomias aquí implicadas son exactamente las de la teoría de conjuntos intuitiva ordinaria; aparentemente no hay paradojas esencialmente nuevas. Cualquier fundamento riguroso capaz de sustentar la teoría ordinaria de clases sustentaría igualmente nuestra teoría. Por lo tanto, hemos optado por adoptar el punto de vista intuitivo, dejando al lector la libertad de insertar cualquier tipo de fundamento lógico (o la ausencia del mismo) que prefiera.*

No obstante, plantean varias posibilidades, como formalizar la teoría en NBG, donde las categorías pueden definirse como clases propias. Sin embargo, a medida que se desarrolló la teoría surgieron contextos que no podían formalizarse de forma natural (por ejemplo, porque involucran definir aplicaciones sobre categorías o funtores, y NBG no permite definir funciones que actúen sobre clases propias).

72 La hipótesis del continuo generalizada implica el axioma de elección En 1926 Adolf Lindenbaum (un estudiante polaco de 22 años que estaba preparando su tesis bajo la dirección de Sierpiński) publicó junto con Tarski una comunicación titulada *Comunicación sobre las investigaciones en teoría de conjuntos,* donde presentaban sin demostraciones una serie de resultados sobre la aritmética cardinal demostrables en su mayor parte sin usar el axioma de elección. Entre ellos figuraba que la hipótesis del continuo generalizada (enunciada como que, para todo conjunto infinito X, no hay ningún cardinal intermedio entre el cardinal de X y el de $\mathcal{P}X$) implica el axioma de elección. Lindenbaum leyó su tesis en 1928, pero en 1941 murió a los 37 años, víctima de los nazis (era judío). Nunca se publicó la demostración de su afirmación sobre la hipótesis del continuo y el axioma de elección, y en **1947** Sierpiński publicó su propia demostración en *La hipótesis del continuo generalizada y el axioma de elección.*

73 Henkin y el teorema de completitud En **1947** se doctoró en Princeton un estudiante de 26 años llamado Leon Albert Henkin, bajo la dirección de Church. En **1949** publicó el artículo *La completitud del cálculo funcional de primer orden,* en el que exponía uno de los resultados de su tesis, que no era sino una nueva demostración del teorema de completitud de Gödel, pero distinta tanto de la que había dado el propio Gödel como de la que después habían presentado Hilbert y Bernays. La prueba de Henkin era conceptualmente más simple que las anteriores y, con algunas variantes, simplificaciones y generalizaciones, es la que presentan habitualmente los libros modernos de lógica. Según hemos visto en la página 82, para probar el teorema de completitud basta demostrar el teorema siguiente (que a menudo recibe también el nombre de teorema de completitud):

> Si una colección de fórmulas de un lenguaje formal es consistente (es decir, si a partir de ellas no se puede deducir formalmente ninguna contradicción), entonces tiene un modelo de universo finito o numerable.

Vamos a esbozar las ideas de la demostración de Henkin (no de la demostración tal cual la presenta Henkin, sino de una de las versiones modernas basadas en ella). Por claridad vamos a considerar el caso concreto de los axiomas de ZFC, aunque el argumento es completamente general y aplicable a cualquier teoría axiomática (de primer orden).

Llamamos Γ_0 al conjunto de los axiomas de ZFC, que es un conjunto infinito de fórmulas del lenguaje formal $\mathcal{L}$ de la teoría de conjuntos, cuyo único signo no definido es el relator de pertenencia $\in$. Cambiando

cada axioma por su clausura universal, podemos suponer que todos ellos son sentencias. Suponemos que Γ_0 es consistente, es decir, que a partir de sus sentencias no es posible demostrar ninguna contradicción. Tenemos que encontrar un conjunto numerable de objetos de modo que, definiendo adecuadamente sobre él una relación de pertenencia, las sentencias de Γ_0 resulten verdaderas cuando se interpretan como afirmaciones sobre tales objetos.

Lo primero que hacemos es extender $\mathcal{L}$ a un nuevo lenguaje formal $\mathcal{L}'$ que conste de los mismos signos que $\mathcal{L}$ más un conjunto infinito de constantes $c_0, c_1, c_2, \ldots$, es decir, de signos que nombran objetos, y enumeramos las sentencias de $\mathcal{L}'$: $\alpha_0, \alpha_1, \alpha_2, \ldots$ Por ejemplo, podría ser $\alpha_0 \equiv \bigvee x\, x \in c_7 \wedge c_3 = c_5$.

De este modo, Γ_0 es un conjunto consistente de sentencias de $\mathcal{L}'$ en el que no aparece ninguna de las nuevas constantes c_i. Vamos a realizar una construcción recurrente. Supongamos que ya tenemos definido un conjunto consistente Γ_n de sentencias de $\mathcal{L}'$ en el que a lo sumo aparezca un número finito de las constantes nuevas. Vamos a construir Γ_{n+1} distinguiendo varios casos:

1. Si al añadir α_n a Γ_n obtenemos un conjunto contradictorio, entonces tomamos como Γ_{n+1} el propio Γ_n, que sigue siendo un conjunto consistente de sentencias de $\mathcal{L}'$ en el que aparece a lo sumo un número finito de constantes nuevas.

2. Si al añadir α_n a Γ_n seguimos teniendo un conjunto consistente, distinguimos dos subcasos:

   (a) Si α_n no es de la forma $\bigvee x\, \beta(x)$, entonces definimos $\Gamma_{n+1} = \Gamma_n \cup \{\alpha_n\}$, que es un conjunto consistente de sentencias y tiene un número finito de constantes nuevas (las que estaban en Γ_n y las que pueda haber en la fórmula α_n).

   (b) Si α_n es de la forma $\bigvee x\, \beta(x)$, tomamos la menor constante c_i que no aparezca en Γ_n ni en α_n y definimos $\Gamma_{n+1} = \Gamma_n \cup \{\alpha_n, \beta(c_i)\}$. Puede probarse que Γ_{n+1} es consistente y cumple todo lo requerido.

La idea del último apartado es que si es consistente que exista un x que cumple $\beta(x)$, no hay ninguna contradicción en tomar un nombre nuevo c_i (del que no se dice nada en $\Gamma_n \cup \{\alpha_n\}$) y añadir como axioma que c_i es un ejemplo de x que cumple $\beta(x)$.

Un aspecto esencial de esta construcción no puede realizarse en la práctica, es decir, no podemos saber qué fórmulas contiene cada Γ_n. Para saberlo tendríamos que saber distinguir si varios conjuntos de fórmulas son consistentes o contradictorios, pero no tenemos ningún procedimiento para saberlo, así que, aunque Γ_n está bien definido, no podemos determinar qué conjunto es concretamente.

Observemos que, por construcción, cada Γ_n contiene a los conjuntos precedentes. Llamamos Γ_∞ a la unión de todos los conjuntos Γ_n. Ahora observamos lo siguiente:

1. Γ_∞ es consistente.

   En efecto, supongamos que a partir de las sentencias de Γ_∞ pudiera deducirse una contradicción. Una deducción es una sucesión finita de fórmulas, luego en ella sólo cabe un número finito de premisas. Esto quiere decir que, en realidad, en la deducción sólo intervendría un número finito de sentencias de Γ_∞, luego existiría un n tal que todas ellas estarían en Γ_n (en principio, cada una estaría en un Γ_n distinto, pero, como la sucesión es creciente, tomando el mayor n resulta que Γ_n las contiene a todas). Por lo tanto, de las sentencias de Γ_n se deduciría una contradicción, pero esto es imposible porque, por construcción, cada Γ_n es consistente.

2. Γ_∞ es completo en el sentido de que si α es cualquier sentencia de $\mathcal{L}'$, o bien α está en Γ_∞, o bien $\neg\alpha$ está en Γ_∞.

   En efecto, supongamos, por ejemplo, que $\alpha \equiv \alpha_5$ y que $\neg\alpha \equiv \alpha_9$. Si α no está en Γ_∞, tampoco está en Γ_6 y, según la construcción, si no hemos incluido $\alpha \equiv \alpha_5$ en Γ_6 es porque $\Gamma_5 \cup \{\alpha\}$ es contradictorio.

   En otras palabras, suponiendo las sentencias de Γ_5, si suponemos α llegamos a una contradicción, pero esto es una demostración (por reducción al absurdo) de $\neg\alpha$ a partir de Γ_5.

   Pero si a partir de Γ_5 se puede deducir $\neg\alpha$, lo mismo vale para Γ_9 (pues contiene a Γ_5). Y si de Γ_9 se deduce $\alpha_9 \equiv \neg\alpha$, podemos afirmar que $\Gamma_9 \cup \{\alpha_9\}$ es consistente.[133] Por lo tanto, $\alpha_9 \equiv \neg\alpha$ está en Γ_{10}, luego en Γ_∞. Si $\neg\alpha$ aparece antes que α en la enumeración se razona análogamente.

[133] En efecto, si a partir de $\Gamma_9 \cup \{\alpha_9\}$ se pudiera demostrar una contradicción, también podríamos demostrarla a partir de Γ_9 únicamente, demostrando α_9 a partir de Γ_9 y luego continuando la demostración hasta llegar a la contradicción, pero Γ_9 es consistente.

Así pues, Γ_∞ es el sueño de Hilbert: un sistema completo de sentencias matemáticas que extiende a los axiomas de ZFC. Lo malo es que no es recursivo (no existe un algoritmo para saber si una fórmula está o no en Γ) y por eso no se le aplica el teorema de incompletitud de Gödel. Además, ni siquiera podemos decir que, si conociéramos explícitamente Γ_∞, habríamos resuelto cualquier problema indecidible en ZFC, pues que α esté o no en Γ_∞ depende esencialmente del orden que hayamos seguido para enumerar las sentencias de $\mathcal{L}'$. Por ejemplo, si tomamos $\alpha_0 \equiv 2^{\aleph_0} = \aleph_1$, entonces la hipótesis del continuo estará en Γ_∞, pero si tomamos $\alpha_0 \equiv 2^{\aleph_0} = \aleph_7$ entonces será la negación de la hipótesis del continuo la que estará en Γ_∞.

El conjunto Γ_∞ es lo que Henkin llamó un conjunto *maximalmente consistente* de sentencias de $\mathcal{L}'$ (que contiene a Γ_0). Eso quiere decir que es consistente, pero se vuelve contradictorio si tratamos de añadirle cualquier sentencia que no esté ya en Γ_∞ (porque si una sentencia α no está, es que está $\neg\alpha$, por lo que en $\Gamma_\infty \cup \{\alpha\}$ contendría a α y $\neg\alpha$, luego sería contradictorio).

Pero además, por construcción, Γ_∞ tiene una propiedad adicional:

3. Si Γ_∞ contiene una sentencia de tipo $\bigvee x\, \beta(x)$, entonces contiene también una sentencia $\beta(c)$, donde c es una de las constantes nuevas.

Esto se expresa diciendo que Γ_∞ está *ejemplificada:* si una de sus sentencias afirma que existe un x que cumple, algo, hay una constante que nombra a un x con tal propiedad. En otras palabras, las nuevas constantes son ejemplos de todo lo que se puede demostrar que existe a partir de Γ_∞.

Por ejemplo, como a partir de los axiomas de ZFC (que están contenidos en Γ_∞) se puede demostrar que existe un número real positivo cuyo cuadrado es 2, en Γ_∞ está la fórmula $c \in \mathbb{R} \wedge c > 0 \wedge c^2 = 2$, para cierta constante c. Pero no sólo hay constantes para cada concepto que podemos definir (como $\sqrt{2}$), sino también para cualquier concepto del que podamos probar la existencia, aunque no la unicidad. Por ejemplo, en ZFC se puede demostrar que existe un subconjunto de $\mathbb{R}$ no medible Lebesgue (aunque no se puede definir ninguno en concreto) y Γ_∞ tiene que contener una sentencia "$c \subset \mathbb{R} \wedge c$ no es medible Lebesgue".

Llamamos M_0 al conjunto (numerable) de todas las constantes nuevas. Tenemos que M_0 es un conjunto de nombres para cualquier cosa de la que pueda hablar un matemático en ZFC. Por ejemplo, para algunos de los elementos de M_0, se cumplirá que la fórmula $c \in \mathbb{R}$ estará en Γ_∞. Las constantes que cumplan esto son las que —según Γ_∞— nombran números reales. En Γ_∞ estará sin duda la sentencia que expresa que $\mathbb{R}$ no es numerable, pero esto no contradice que, como el lenguaje $\mathcal{L}'$ contiene sólo una cantidad numerable de sentencias, sólo se puede decir una cantidad numerable de cosas sobre los números reales, por lo que basta una cantidad numerable de números reales para atestiguar cualquier cosa que un matemático pueda decir sobre los números reales.

La idea "bruta" de Henkin es definir un modelo cuyo universo sea M_0, de modo que cada constante se nombre a sí misma, pero esta idea hay que refinarla un poco, porque, dadas dos constantes c y d en M_0, puede ocurrir que la sentencia $c = d$ esté en Γ_∞, y eso significa que ambas constantes deben nombrar el mismo objeto en cualquier modelo de Γ_∞. Por ello, si pretendiéramos que c y d fueran dos "conjuntos" distintos, la sentencia $c = d$ de Γ_∞ sería falsa si interpretamos que c y d se nombran a sí mismas.

Esto se arregla fácilmente considerando en M_0 la relación dada por $c \sim d$ si y sólo si la sentencia $c = d$ está en Γ_∞. Usando que Γ_∞ es máximalmente consistente, el lector no debería tener mucha dificultad en demostrar que se trata de una relación de equivalencia, es decir, que, para todas las constantes c, c', c'' de M_0, se cumple:

1. $c \sim c$
2. Si $c \sim d$, entonces $d \sim c$.
3. Si $c \sim d$ y $d \sim e$, entonces $c \sim e$.

Diremos que una constante c_i es mínima, si no se cumple $c_i \sim c_j$ para ningún $j < i$, y llamamos M al conjunto de todas las constantes mínimas. Es claro entonces que toda constante c de M_0 está relacionada con una única constante c^* de M (la de menor índice relacionada con ella).

Ahora ya podemos definir un modelo de Γ_∞:

1. El universo del modelo es M, es decir, llamamos "conjuntos" a las constantes nuevas mínimas.
2. Diremos que un elemento c de M pertenece a otro d si la sentencia $c \in d$ está en Γ_∞.
3. Definimos el objeto denotado por una constante c de $\mathcal{L}'$ como la constante mínima c^* relacionada con ella. Así, dos constantes c y d nombran el mismo objeto de M si y sólo si están relacionadas, es decir, si y sólo si la sentencia $c = d$ está en Γ_∞.

De este modo, hemos llamado "conjuntos" a unos meros signos lógicos, pero de manera que dos "conjuntos" c y d son iguales si y sólo si $c = d$ está en Γ_∞ (es decir, si y sólo si Γ_∞ afirma que son iguales) y uno "pertenece" a otro si y sólo si $c \in d$ está en Γ_∞ (si y sólo si Γ_∞ afirma que así sucede). Omitimos los detalles, pero la completitud y la ejemplificación de Γ_∞ permiten demostrar a partir de aquí que todas las sentencias de Γ_∞ (y en particular, todas las de Γ_0, es decir, todos los axiomas de ZFC) son verdaderas en este modelo (numerable).

Insistimos en que, aunque hemos ilustrado el argumento con ZFC, el procedimiento es general, y se aplica a cualquier teoría axiomática (de primer orden) sobre cualquier lenguaje formal (numerable).

Al margen de los detalles técnicos de la prueba, que hemos omitido, hay algunos aspectos sobre los que el lector debería meditar:

- En primer lugar está la idea general: el hecho de que sólo podamos hacer una cantidad numerable de afirmaciones hace que una cantidad numerable de objetos baste para que se cumplan todas ellas.

- En segundo lugar observemos que hemos usado notación conjuntista en la prueba, como al decir que $\Gamma_{n+1} = \Gamma_n \cup \{\alpha_n, \beta(c_i)\}$, etc., pero eso no significa que la prueba deba entenderse como un teorema de ZFC. De hecho, tal y como la hemos planteado, cada α_n es una fórmula metamatemática, por lo que no tiene ningún sentido interpretar $\Gamma_{n+1} = \Gamma_n \cup \{\alpha_n, \beta(c_i)\}$ como si α_n fuera un conjunto. Toda la demostración debe entenderse en términos "materiales" (no formales) intuitivos.

  Así, cuando hablamos de Γ_0, nos estamos refiriendo a un conjunto en el sentido intuitivo de la palabra, en este caso la colección de todos los axiomas de ZFC, que es algo perfectamente definido y de lo que podemos hablar sabiendo de qué estamos hablando exactamente.

  También podemos calcular explícitamente la sucesión $\alpha_0, \alpha_1, \ldots$, en el sentido de que (adoptando los convenios arbitrarios oportunos para fijar una ordenación) podemos determinar exactamente qué fórmula es α_0, cuál es α_1, etc. No necesitamos ninguna teoría axiomática de conjuntos para atribuir un significado preciso a esta enumeración.

  Supongamos que, con el convenio de ordenación que hemos adoptado, resulta que

$$\alpha_0 \equiv \bigvee x(x \text{ es un cardinal fuertemente inaccesible}).$$

  Entonces sabemos exactamente qué es el conjunto $\Gamma_0 \cup \{\alpha_0\}$. La notación empleada para hacer referencia a él es irrelevante. Nos referimos al conjunto formado por los axiomas de ZFC y además α_0, que es un conjunto perfectamente determinado en términos intuitivos.

  No sabemos si $\Gamma_0 \cup \{\alpha_0\}$ es consistente o no, pero sabemos perfectamente lo que significa que lo sea. Diga lo que diga un intuicionista, o bien es posible deducir una contradicción partiendo de algunos axiomas de ZFC y de α_0, o bien no es posible hacerlo. (Y, cuando hablamos de "deducir", nos referimos a un concepto perfectamente definido en términos intuitivos finitistas.)

  Por lo tanto, se nos plantean dos casos y no sabemos cuál es el correcto. Si $\Gamma_0 \cup \{\alpha_0\}$ es contradictorio, definimos $\Gamma_1 = \Gamma_0$, lo cual significa que llamamos Γ_1 exactamente a lo mismo a lo que llamábamos Γ_0.

  Por el contrario, si $\Gamma_0 \cup \{\alpha_0\}$ es consistente, llamamos

$$\Gamma_1 = \Gamma_0 \cup \{\bigvee x(x \text{ es un cardinal fuertemente inaccesible}),\ c_0 \text{ es un cardinal fuertemente inaccesible}\},$$

  es decir, llamamos Γ_1 al conjunto formado por los axiomas de ZFC y dos fórmulas más, una que afirma que existe un cardinal fuertemente inaccesible y otra que afirma que c_0 es un ejemplo de cardinal fuertemente inaccesible.

  Todo esto tiene un significado intuitivo preciso e inequívoco, de modo que podemos afirmar que Γ_1 está perfectamente definido, pese a que no podemos saber qué conjunto es exactamente, ya que no sabemos cuál de los dos casos se aplica a su definición.

  El lector tendrá que decidir si está de acuerdo con Brouwer y Heyting y niega que nada de esto tenga sentido alguno, o si está de acuerdo con Hilbert, Gödel, Henkin y prácticamente todos los matemáticos que hemos nombrado en estas páginas con pocas excepciones más (Kronecker, etc.) Incluso cabe conjeturar que hasta Skolem —que era finitista— reconocería que todo este argumento tiene sentido, puesto que su demostración del teorema de Löwenheim-Skolem requiere argumentos similares.

- Si el lector está dispuesto a aceptar como "materialmente válido" el argumento de Henkin, tiene dos opciones: o bien entender que la noción de "finitismo" es más amplia que lo que Hilbert pretendía que fuera, es decir, que tiene sentido hablar "finitistamente" de (algunos) conjuntos numerables, o bien aceptar que la metamatemática requiere argumentos que trascienden el finitismo en su sentido más estricto, y que no hay inconveniente con dicho requisito, pues es posible razonar intuitivamente con rigor sobre (algunos) conjuntos infinitos numerables, siempre y cuando los podamos considerar bien definidos, de modo que sepamos exactamente de qué estamos hablando y qué estamos diciendo cuando hablamos de ellos, sin necesidad de aceptar los postulados intuicionistas sobre lo que es o no intuitivamente aceptable. Cuando en la página 74 y siguientes hemos explicado cómo se puede concebir un razonamiento intuitivo, hemos considerado razonamientos mucho más generales que los que Hilbert reclamaba para su finitismo, pero que, desde que Gentzen apelara a la inducción hasta ϵ_0, los lógicos estaban empezando a admitir.

- Dicho esto, nada impide formalizar todo el argumento de Henkin en ZFC o en cualquier otra teoría de conjuntos, lo que supone considerar que las fórmulas α_n no son ya fórmulas metamatemáticas, sino conjuntos que satisfacen una definición formal de fórmula en ZFC (o la definición formal general en ZFC de fórmula de una teoría axiomática formal T). Así, la razón por la que alguien que lea el argumento anterior puede pensar que se trata de una demostración normal y corriente en ZFC es que, en efecto, nada impide considerarlo como tal. Lo que hemos enfatizado en el punto precedente es que *no es necesario* considerarlo como tal, pero también es cierto que nada nos impide considerarlo como tal.

  Lo que sucede es que, si queremos ver el teorema de completitud como parte del proceso que nos permite concluir que un cálculo deductivo es adecuado para formalizar la matemática y tomarlo como base de la definición de demostración en ZFC, necesitamos concebirlo como un teorema previo a ZFC y no como un teorema de ZFC (sin perjuicio de que posteriormente lo consideremos también como teorema de ZFC).

Cuando consideramos la lógica formalizada en ZFC, u otra teoría de conjuntos, podemos considerar lenguajes formales con una cantidad arbitraria de signos no definidos. Por ejemplo, con una cantidad no numerable de constantes, etc. En este contexto formalizado, si consideramos un conjunto Γ de axiomas de un lenguaje formal con una cantidad κ de signos (donde κ es un cardinal infinito), Henkin mostró que su argumento se adapta para demostrar esta versión del teorema de Löwenheim-Skolem:[134]

> **Teorema de Löwenheim-Skolem** Si κ es un cardinal infinito y Γ es un conjunto de fórmulas de un lenguaje formal con κ signos que admite un modelo infinito, entonces admite un modelo de cualquier cardinal infinito prefijado mayor o igual que κ.

Notemos que hay que exigir que Γ admita un modelo infinito, porque, por ejemplo, si

$$\Gamma = \{\bigvee yz \bigwedge x(x = y \vee x = z)\},$$

todos los modelos de Γ tienen a lo sumo dos elementos.

74 Álgebras de Boole El concepto de álgebra de Boole se remonta a un libro de George Boole de 1847 titulado *El análisis matemático de la lógica,* y había sido estudiado después por Schröder en 1890 o por Whitehead en 1898, entre otros, pero el nombre de "álgebra de Boole" lo acuñó Henry Maurice Sheffer en su artículo de 1913 titulado *Un conjunto de cinco postulados independientes para las álgebras de Boole, con aplicación a las constantes lógicas.* Hasta entonces lo que se consideraba en realidad era un "algebra" entendida como una especie de "cálculo lógico algebraico" basado en distintos juegos de postulados. Sheffer fue el primero en pensar en las álgebras de Boole como una estructura algebraica en un sentido similar al moderno. Por ejemplo, dice que emplea la expresión "álgebras de Boole", en plural, entre otras cosas porque:

> *Ninguno de los conjuntos de postulados equivalentes aquí mencionados es, en términos de sus entidades indefinidas, unívoco ("categórico"), es decir, cada uno determina no una sola álgebra, sino una clase de álgebras; por lo tanto, no se debería hablar de "el cálculo de la identidad" (Schröder) o "el álgebra de la lógica simbólica" (Whitehead).*

Es decir, que hay distintas álgebras de Boole, igual que hay distintos grupos, anillos, cuerpos, etc., aunque estén definidos por unas propiedades comunes.

[134] Se dice Skolem que lamentaba que se asociara su nombre con un teorema que para él, de acuerdo con su concepción finitista de la matemática, no tenía significado alguno.

Así como hay un consenso generalizado en qué axiomas definen el concepto de grupo, anillo, etc., en el caso de las álgebras de Boole hay muchos sistemas de axiomas equivalentes. Uno de los más naturales es definir un álgebra de Boole como un conjunto en el que hay definidas una operación unitaria: a' y dos operaciones binarias $a \wedge b$ y $a \vee b$ y en el que hay dos elementos distinguidos 0 y 1, de modo que se cumplen las propiedades siguientes:

$a \vee (b \vee c) = (a \vee b) \vee c$	$a \wedge (b \wedge c) = (a \wedge b) \wedge c$	asociatividad
$a \vee b = b \vee a$	$a \wedge b = b \wedge a$	conmutatividad
$a \vee (a \wedge b) = a$	$a \wedge (a \vee b) = a$	absorción
$a \vee 0 = a$	$a \wedge 1 = a$	identidad
$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$	$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$	distributividad
$a \vee a' = 1$	$a \wedge a' = 0$	complementos

Aunque no es especialmente relevante en nuestro contexto, Sheffer dedicaba su artículo a demostrar que, para definir un álgebra de Boole, bastaba considerar una única operación, que el representaba por $a \mid b$ (hoy conocidda como el trazo de Sheffer) y cinco axiomas. A partir del trazo de Sheffer, los conectores usuales pueden definirse como

$$\neg a = a \mid a, \quad a \wedge b = (a \mid b) \mid (a \mid b), \qquad a \vee b = (a \mid a) \mid (b \mid b).$$

Recíprocamente, $a \mid b = \neg(a \wedge b)$.

La relación entre las álgebras de Boole y la lógica formal en el sentido de Hilbert fue explicitada por el matemático polaco Adolf Lindenbaum, aunque no publicó apenas nada al respecto. Fue Tarski quien, hacia 1930 definió lo que llamó *álgebra de Lindembaum* de una teoría axiomática (por lo que también se conoce hoy como *álgebra de Lindembaum-Tarski*), y que consiste en establecer una relación de equivalencia entre las sentencias del lenguaje formal de una teoría axiomática T, de modo que dos sentencias α y β son equivalentes si en T se puede demostrar $\alpha \to \beta$. El álgebra de Lindembaum $B(T)$ está formada por las clases de equivalencia $[\alpha]$ de sentencias del lenguaje de T, de modo que $[\alpha] = [\beta]$ si y sólo si en T se puede demostrar que $\alpha \leftrightarrow \beta$.

En el conjunto $B(T)$ se pueden definir las operaciones

$$[\alpha]' = [\neg\alpha], \qquad [\alpha] \wedge [\beta] = [\alpha \wedge \beta], \qquad [\alpha \vee \beta] = [\alpha] \vee [\beta],$$

así como los elementos $0 = [\bigvee x\, x \neq x]$, $1 = [\bigwedge x\, x = x]$.

Como $\bigwedge x\, x = x$ es demostrable en T, la clase 1, que está formada por las fórmulas que en T son equivalentes a ésta, es en realidad la clase de todas las sentencias demostrables en T, mientras que 0 está formada por todas las sentencias refutables en T. En particular, se cumple $1 \neq 0$ si y sólo si la teoría T es consistente, y se cumple $B(T) = \{0, 1\}$ si y sólo si es completa. El resto de clases de $B(T)$ corresponden a sentencias que no son ni demostrables ni refutables en T.

Por otra parte, las álgebras de Boole aparecieron en diversos contextos matemáticos no relacionados con la lógica a través de la noción de *álgebra de conjuntos,* definida como una familia $\mathcal{B}$ de subconjuntos de un conjunto X tal que:

1. $\varnothing, X \in \mathcal{B}$
2. Si $A \in \mathcal{B}$, entonces $X \setminus A \in \mathcal{B}$.
3. Si $A, B \in \mathcal{B}$, entonces $A \cup B, A \cap B \in \mathcal{B}$.

El caso más simple es el de las álgebras $\mathcal{P}X$, para cualquier conjunto X, pero hay muchos otros casos de interés. Por ejemplo, la familia $\mathcal{B}$ de los conjuntos de Borel en $\mathbb{R}^n$ forman un álgebra de subconjuntos de $\mathbb{R}^n$, al igual que la familia $\mathcal{M}$ de los conjuntos medibles Lebesgue.

Es fácil ver que toda álgebra de conjuntos es un álgebra de Boole tomando como operaciones $A' = X \setminus A$, $A \wedge B = A \cap B$, $A \vee B = A \cup B$, además de $0 = \varnothing$, $1 = X$.

En un álgebra de conjuntos, la inclusión $A \subset B$ es una relación de orden parcial que puede definirse en términos de la estructura de álgebra, pues en un álgebra de Boole cualquiera se puede definir la relación

$$a \leq b \quad \leftrightarrow \quad a \wedge b = a \quad \leftrightarrow \quad a \vee b = b,$$

y, en el caso de un álgebra de conjuntos, esta relación es precisamente la inclusión.

De hecho, las álgebras de Boole se pueden caracterizar en términos de su estructura de orden:

Un *retículo* se define como un conjunto R dotado de una relación $\leq$ de orden parcial, es decir, tal que

1. $a \leq a$
2. Si $a \leq b$ y $b \leq a$ entonces $a = b$
3. si $a \leq b$ y $b \leq c$ entonces $a \leq c$

en el que cada par de elementos a y b tienen un (único) supremo $a \vee b$ y un (único) ínfimo $a \wedge b$.

Esto significa que $a \vee b$ es el menor elemento mayor o igual que a, b, es decir, que

$$a \leq a \vee b,\ b \leq a \vee b \text{ y si } a \leq c \text{ y } b \leq c, \text{ entonces } a \vee b \leq c,$$

así como que $a \wedge b$ es el mayor elemento menor o igual que a, b:

$$a \wedge b \leq a,\ a \wedge b \leq b \text{ y si } c \leq a \text{ y } c \leq b, \text{ entonces } c \leq a \wedge b.$$

Un retículo es *distributivo* si cumple las leyes de distributividad

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c), \qquad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Un retículo está complementado si tiene un máximo elemento 1 y un mínimo 0 de modo que cada elemento a tiene un *complemento*[135] a' que cumple $a \vee a' = 1$, $a \wedge a' = 0$.

En estos términos, las álgebras de Boole coinciden con los retículos distributivos complementados.

La teoría sobre las álgebras de Boole experimentó una revolución con la obra de Marshall Harvey Stone, entre cuyos artículos a este respecto cabe destacar *Álgebras de Boole y su aplicación a la topología,* de 1934, y *La teoría de representaciones para álgebras de Boole,* de 1936 (el segundo de los cuales ocupaba 75 páginas). Uno de sus descubrimientos básicos era el siguiente:

Las álgebras de Boole se pueden identificar con los *anillos booleanos,* es decir, con los anillos conmutativos y unitarios en los que todo elemento es idempotente,[136] es decir, cumple $a \cdot a = 0$.

En efecto, en un anillo idempotente podemos definir

$$a' = 1 + a, \qquad a \wedge b = ab, \qquad a \vee b = 1 + (1 + a)(1 + b) = a + b + ab$$

y estas operaciones cumplen la definición de álgebra de Boole. Recíprocamente, toda álgebra de Boole es un anillo booleano con las operaciones dadas por[137]

$$a + b = (a \vee b) \wedge (a \wedge b)', \qquad ab = a \wedge b.$$

Esto permitía trasvasar a la teoría de álgebras de Boole toda la teoría de anillos, que para entonces ya estaba muy desarrollada. En particular, daba pie a hablar de ideales de un álgebra de Boole, y de álgebras cociente, isomorfismos, etc., conceptos que resultaron tener una interpretación natural específica en el contexto de las álgebras de Boole y que Stone estudió a fondo.

Por ejemplo, el concepto de "ideal", que Dedekind había introducido en 1871 y se había convertido en un concepto fundamental en la teoría de anillos, tenía esta caracterización en el contexto de las álgebras de Boole:

Un ideal (propio) en un álgebra de Boole B es un conjunto $I \subset B$ con las propiedades siguientes:

1. $0 \in I$, $1 \notin I$.
2. Si $a \in B$, $b \in I$ y $a \leq b$, entonces $a \in I$.
3. Si $a, b \in I$, entonces $a \vee b \in I$.

[135] El complemento no tiene por qué ser único, pero sí que lo es si el retículo es distributivo.
[136] Esto implica a su vez que $a + a = 0$, pues $a + a = (a + a)(a + a) = a + a + a + a$.
[137] Notemos que, en un álgebra de conjuntos, esta suma es lo que se conoce como *diferencia simétrica:* $A + B = (A \cup B) \setminus (A \cap B)$.

Estas propiedades pueden interpretarse como que I define una familia de "elementos pequeños" de B:

1. El 0 es pequeño, pero el 1 no lo es.
2. Todo elemento menor o igual que uno pequeño es pequeño.
3. El supremo de dos elementos pequeños sigue siendo pequeño.

Por ejemplo, si X es un conjunto inifinito, la familia F de los subconjuntos finitos de X forma un ideal del álgebra de conjuntos $\mathcal{P}X$ o, en el álgebra de Boole de los conjuntos medibles Lebesgue, los conjuntos de medida nula también forman un ideal, pues cumplen trivialmente las condiciones anteriores.

En la teoría de anillos también son fundamentales los conceptos de ideal maximal y de ideal primo. En el contexto de las álgebras de Boole ambos son equivalentes, y admiten esta caracterización:

Un ideal P en un álgebra de Boole B es *primo* si y sólo si todo elemento a de B cumple $a \in P$ o bien $a' \in B$.

De hecho, no se pueden dar los dos casos a la vez, pues entonces $1 = a \vee a' \in I$, en contra de la definición de ideal (propio).

Así pues, un ideal primo P parte un álgebra de Boole B en dos mitades disjuntas: $B = P \cup P'$, donde $P' = \{p' \mid p \in P\}$. Por una parte están los elementos de P ("próximos" a 0) y, por otra, sus complementos ("próximos" a 1).[138]

Entre los muchos resultados que Stone obtuvo sobre álgebras de Boole, estaba el siguiente:

Toda álgebra de Boole es isomorfa a un álgebra de conjuntos.[139]

En 1937 Henri Cartan introdujo los conceptos de *filtro* y *ultrafiltro* como una forma de sustituir la convergencia de sucesiones en espacios topológicos en los que éstas no sirven para caracterizar la topología.[140] Aquí no necesitamos nada sobre las aplicaciones de los filtros y ultrafiltros en topología, pero conviene observar que el concepto de filtro no es sino el caso particular para álgebras de conjuntos de esta definición general, válida para álgebras de Boole:

Definición Un filtro (propio) en un álgebra de Boole B es un conjunto $F \subset B$ con las propiedades siguientes:

1. $1 \in F$, $0 \notin F$
2. Si $a \in B$, $b \in F$ y $b \leq a$, entonces $a \in F$.
3. Si $a, b \in F$, entonces $a \wedge b \in F$.

Exactamente igual que los ideales expresan la idea de "conjunto pequeño", los filtros expresan la de "conjunto grande". Los conceptos de "ideal" y "filtro" son duales, en el sentido de que si I es un ideal en un álgebra de Boole $\mathcal{B}$, entonces el conjunto $I' = \{p' \mid p \in I\}$ es un filtro, y viceversa.

Un filtro U es un *ultrafiltro* si cumple la condición adicional de que todo elemento a de B cumple $a \in U$ o bien $a' \in U$.

Los ultrafiltros son los duales de los ideales primos, es decir, U es un ultrafiltro de un álgebra de Boole si y sólo si U' es un ideal primo.

Esto significa que si P es un ideal primo en un álgebra de Boole $\mathcal{B}$, entonces ésta se descompone en una unión disjunta $\mathcal{B} = P \cup U$, donde U es el ultrafiltro dual de P.

En 1939 había leído su tesis en Varsovia Andrej Mostowski, teóricamente bajo la dirección de Kuratowski, pero en la práctica bajo la de Tarski (que no era profesor en Polonia en ese momento y no podía dirigir tesis oficialmente). A su vez, Mostowski dirigió la tesis de Roman Sikorski, que la leyó en 1949, y éste, en **1950** publicó un artículo junto con *Helena Rasiowa,* que ese año leería también su tesis bajo la dirección de Mostowski. El artículo se titulaba *Una demostración del teorema de completitud de Gödel,* y en él Rasiowa y Sikorski daban una demostración alternativa del teorema de completitud basada en la teoría de álgebras de Boole.

[138] En general, el anillo cociente de un álgebra de Boole por un ideal es un álgebra de Boole, y el ideal es primo si y sólo si el anillo cociente es el álgebra trivial $B/P = \{0, 1\}$.

[139] Más precisamente, Stone demostró que, si B es un álgebra de Boole, el conjunto $S(B)$ de sus ideales primos puede dotarse de forma natural de estructura de espacio de Hausdorff compacto cerodimensional (es decir, con una base formada por abiertos-cerrados), que es lo que hoy se conoce como el *espacio de Stone* de B, y toda álgebra de Boole B resulta ser isomorfa al álgebra (de conjuntos) de abiertos-cerrados de su espacio de Stone $S(B)$.

[140] Las sucesiones sólo caracterizan la topología de espacios topológicos en los que cada punto tiene una base numerable de entornos.

Más precisamente, si una teoría T es consistente, podemos considerar su álgebra de Lindenbaum $B(T)$, y Rasiowa y Sikorski usaban la existencia de un ideal primo P en $B(T)$ para construir una familia maximalmente consistente y ejemplificada de sentencias de T, a saber, las formada por las sentencias cuyas clases estaban en el ultrafiltro dual de P (las "próximas" a 1), que se convertían en las sentencias verdaderas del modelo construido, mientras que las sentencias con clase en P eran las fórmulas falsas en el modelo. (Un ideal primo P "parte" las sentencias en verdaderas y falsas.)

75 ZFC y NBG Hao Wang había cursado un máster en filosofía en China, y en 1945 se había trasladado a los Estados Unidos para continuar sus estudios. En 1948 se doctoró bajo la dirección de Quine. En 1949 publicó su artículo *Sobre los axiomas para la teoría de conjuntos de Zermelo y von Neumann.* En él observa que es fácil probar que si la teoría de conjuntos NBG es consistente (sin el axioma de elección), también lo es ZF, pero que no es obvio que el recíproco sea cierto. En la línea de relacionar ambas teorías, Wang muestra cómo se puede obtener NBG a partir de ZF añadiendo un nuevo juego de variables y unos axiomas que las regulan.

Esto sugería que todo modelo de ZF se puede extender a un modelo de NBG añadiéndole unos nuevos objetos que hicieran de clases propias, pero Wang no justificaba que esto pudiera hacerse de modo que los nuevos objetos cumplieran sus axiomas, y de hecho nunca llega a afirmar que sus resultados demostraran la consistencia de NBG a partir de la de ZF.

Ilse Lisl Novak, había nacido en Viena en el seno de una familia judía y, en 1938, a sus 14 años, tras la anexión de Austria a la Alemania nazi, había huido con su familia a los Estados Unidos. Allí estudió matemáticas y en 1948 leyó su tesis bajo la dirección de Quine y Lynn Harold Loomis. En **1950** publicó un artículo con los contenidos de su tesis titulado *Una construcción de modelos de sistemas consistentes,* en el que mejoraba los resultados de Wang y demostraba que la consistencia de ZF implica la consistencia de NBG. Más aún, Novak señala en una nota que Mostowski había generalizado sus resultados demostrando lo siguiente:

> Las teorías ZF y NBG pueden demostrar exactamente los mismos resultados[141] sobre conjuntos, es decir, si una sentencia tiene todas sus variables restringidas a conjuntos, entonces es demostrable en ZF si y sólo si lo es en NBG.

Ese mismo año, Wang y Rosser publicaron *Modelos no estándar para lógicas formales,* donde afirman que:

> *Mediante el mismo método utilizado para demostrar (1) anteriormente, podemos demostrar que si la teoría de conjuntos de Zermelo-Fraenkel es consistente, entonces también lo es la teoría de conjuntos de Gödel. (Para una prueba alternativa de este resultado, véase* [Novak].)

Las demostraciones de Novak y Wang eran complicadas en comparación con argumentos más modernos. Vamos a esbozar aquí un argumento más sencillo:

Demostración: Supongamos que ZF es consistente, con lo que tiene un modelo M. Esto significa que M es un conjunto en el que hay definida una relación de pertenencia R de modo que, si entendemos por "conjuntos" los elementos de M y por "pertenencia" la relación R, todos los axiomas de ZF son verdaderos.

Consideramos entonces la colección[142] C_0 formada por todos los $\Phi = (\phi, (a_1, \ldots, a_n))$, donde $\phi(x_0, x_1, \ldots, x_n)$ es una fórmula con las variables libres indicadas y $a_1, \ldots, a_n$ son elementos de M.

A cada $\Phi = (\phi, (a_1, \ldots, a_n))$ podemos asociarle la colección C_Φ formada por todos los "conjuntos" c tales que $\phi(x_0, \ldots, x_n)$ es verdadera en M cuando sus variables se interpretan como $c, a_1, \ldots, a_n$.

Podemos pensar que C_Φ es lo que en un modelo de NBG sería la clase

$$\{x_0 \mid \phi(x_0, x_1, \ldots, x_n)\}$$

cuando los parámetros $x_1, \ldots, x_n$ se interpretan como $a_1, \ldots, a_n$ o, en otras palabras, que C_Φ es la clase definida por ϕ cuando sus parámetros se definen como $a_1, \ldots, a_n$.

Nuestra intención es añadirle a M las clases C_Φ que no sean conjuntos, es decir, que no estén ya en M. Más precisamente, llamaremos P_0 a la colección de los elementos Φ de C_0 tales que no existe ningún c en M de modo que C_Φ coincida con el conjunto de todos los d en M que cumplen $d\,R\,c$, es decir, tales que C_Φ no esté formada por los conjuntos que "pertenecen" a c. Esto se interpreta como que C_Φ es una "clase propia" en M.

[141] Se considera NBG sin el axioma de elección, pero el resultado es igualmente válido si consideramos ZFC y NBG con el axioma de elección de Zermelo y no el de Gödel, es decir, el axioma que afirma que todo conjunto puede ser bien ordenado y no que la clase universal puede ser bien ordenada. Para el axioma de elección de Gödel también es cierto, pero requiere afinar más el argumento.

[142] Usamos aquí "colección" en el sentido de conjunto metamatemático, para que no se confunda con los "conjuntos" en el sentido de elementos de M.

Por otra parte, puede haber elementos Φ y Ψ en P_0 tales que $C_\Phi = C_\Psi$, con lo que ambos deben definir la misma clase, por lo que definimos en P_0 la relación dada por $\Phi \sim \Psi$ si y sólo si $C_\Phi = C_\psi$. Para cada Φ en P_0, llamamos $[\Phi]$ a la colección de todos los Ψ equivalentes a Φ, de modo que $[\Phi] = [\Psi]$ si y sólo si $\Phi \sim \Psi$, si y sólo si $C_\Phi = C_\Psi$. Llamamos P a la colección de todas las clases de equivalencia $[\Phi]$.

Así, cada $[\Phi]$ en P determina una "clase propia" A_Φ, que es una subcolección de M cuyos elementos están determinados por la fórmula ϕ y los parámetros $a_1, \ldots, a_n$ que forman Φ y de modo que ninguna "clase propia" en este sentido es un conjunto y no hay dos clases iguales.

Ahora podemos definir un modelo de NBG tomando como universo M^* los objetos de M y los de P, y extendiendo la relación de pertenencia R de M de modo que un "conjunto" c "pertenece" a una "clase" $[\Phi]$, es decir, cumple $c\,R\,[\Phi]$, si y sólo si c está en C_Φ (mientras que una "clase" nunca pertenece a otra "clase").

Se puede probar que M^* con la relación de pertenencia R así extendida es un modelo para NBG (con el axioma de elección de Zermelo) en el que los "conjuntos", es decir, las clases que no pertenecen a otras clases, son justamente los elementos de M. Por lo tanto, si ZFC es consistente, también lo es NBG.

Más aún, es fácil ver que la observación de Mostowski es cierta: supongamos que α es una sentencia que sólo habla de conjuntos y que es demostrable en NBG. Vamos a ver que es demostrable en ZFC. Por el teorema de completitud de Gödel, para que esto suceda basta[143] con que α sea verdadera en todos los modelos de ZFC. Tomamos un modelo arbitrario M de ZFC. Por la construcción anterior obtenemos un modelo M^* de NBG en el que α tiene que ser verdadera, porque es un teorema de NBG, pero, como α sólo habla de conjuntos, de hecho α es verdadera en M.

La otra implicación es trivial: todo teorema (necesariamente sobre conjuntos) demostrable en ZFC es demostrable también en NBG. Esto puede demostrarse sin recurrir a modelos, pero el argumento con modelos es inmediato: en NBG se demuestra que los conjuntos satisfacen los axiomas de ZFC, por lo que si M es un modelo de NBG, el modelo M_* que resulta de eliminar de M los objetos que son clases propias es un modelo de ZFC, y podemos razonar exactamente igual que antes. ∎

En realidad todo el argumento vale igualmente si donde hemos dicho "modelo" decimos más concretamente "modelo numerable" y entonces la prueba es tan intuitivamente válida como lo es la prueba del teorema de completitud (en el sentido de que no es estrictamente finitista, pero hay (o no) los mismos motivos para ponerle objeciones a una o a la otra).

Por supuesto, la demostración es formalizable en ZFC y en NBG, por lo que en cualquiera de las dos teorías se puede demostrar

$$\mathrm{Consis}(\ulcorner \mathrm{ZFC} \urcorner) \leftrightarrow \mathrm{Consis}(\ulcorner \mathrm{NBG} \urcorner).$$

Clases en ZF El argumento que hemos dado puede traducirse a algo mucho más práctico y tangible: es posible hablar con rigor de clases propias en ZF.

En efecto, partiendo de la idea de que, para añadirle clases propias a un modelo de ZF, basta con asociar una a cada fórmula del lenguaje formal a la vez que se fijan valores para sus parámetros, trabajando en ZF, podemos convenir en llamar "clases" simplemente a las fórmulas. Por ejemplo —siempre trabajando en ZF—, podemos definir la fórmula "x es un ordinal", y con ella podemos definir la clase

$$\Omega = \{x \mid x \text{ es un ordinal}\},$$

¿cómo hay que entender esto? Simplemente como el convenio de que, si escribimos $x \in \Omega$, esto ha de entenderse simplemente como que "x es un ordinal".

En general, si consideramos dos fórmulas y definimos clases,

$$A = \{x \mid \phi(x, x_1, \ldots, x_n)\}, \qquad B = \{x \mid \psi(x, y_1, \ldots, y_m)\},$$

estas definiciones se pueden entender como entradas de un "diccionario" que nos permite traducir cualquier fórmula en la que aparezcan A y B en otra en la que no estén. Concretamente, las fórmulas atómicas se traducen así:

[143] El teorema afirma que si α es verdadera siempre que los axiomas de ZFC son verdaderos, entonces α puede deducirse lógicamente de dichos axiomas.

- $x \in A \equiv \phi(x, x_1, \ldots, x_n)$.
- $x = A \equiv \bigwedge u(u \in x \leftrightarrow u \in A)$.
- $A \in x \equiv \bigvee u\,(u \in x \wedge u = A)$.
- $A = B \equiv \bigwedge x(x \in A \leftrightarrow x \in B)$.
- $A \in B \equiv \bigvee x(x \in B \wedge x = A)$.

Y cualquier otra fórmula se traduce sustituyendo las apariciones de clases en las fórmulas atómicas que contienen. Por ejemplo, la inclusión se define como

$$x \subset y \equiv \bigwedge u(u \in x \to u \in y),$$

luego si en una inclusión aparecen una o dos clases, podemos usar esta definición para "traducirlas":

$$x \subset A \equiv \bigwedge u(u \in x \to u \in A), \qquad A \subset B \equiv \bigwedge u(u \in A \to u \in B),$$

etc. Entendiendo así cualquier afirmación que involucre clases propias, nos encontramos con que las clases se comportan exactamente como NBG afirma que se comportan.

Por ejemplo, ahora podemos afirmar (y demostrar) en ZF que Ω no es un conjunto, entendiéndolo como que no existe ningún conjunto x tal que $\Omega = x$, cosa que es cierta, porque partiendo de $\Omega = x$ se puede probar la antinomia de Burali-Forti, luego esa contradicción nos da que, en efecto, Ω no es un conjunto.

En general, si una clase A no es un conjunto (si $\neg\bigvee x(x = A)$), entonces A no pertenece a ningún conjunto ni a ninguna clase, pues las definiciones que hemos dado de $A \in x$ o $A \in B$ requieren que A sea igual a un conjunto. ∎

Ahora observamos que, si adoptamos este convenio de expresar fórmulas del lenguaje de ZF empleando clases, lo que nunca nos vamos a encontrar es un cuantificador sobre clases. En ZF, $\bigwedge x$ significa "para todo conjunto x", y no tenemos forma de definir un "para toda clase X". Por eso, al definir una clase en la forma que acabamos de plantear, $A = \{x \mid \phi(x, x_1, \ldots, x_n)\}$, la fórmula ϕ puede contener clases (eliminables como hemos visto), pero no cuantificadores de tipo "para toda clase" o "existe una clase", porque a eso no podemos darle ningún sentido en ZF. Vemos así que la restricción a fórmulas que no tengan cuantificadores sobre clases en el teorema de comprensión de NBG hace que el uso de clases en NBG no exceda las posibilidades que tenemos de hablar de clases de este modo en ZF.

En términos modernos, NBG es lo que se conoce como la *extensión predicativa* de ZFC, lo cual significa que un modelo de NBG se obtiene añadiendo a un modelo de ZFC nuevas colecciones de conjuntos definidas por fórmulas que especifican algunos de los conjuntos del modelo dado. La prohibición de definir clases mediante fórmulas que cuantifican sobre la totalidad de las clases es una prohibición de naturaleza predicativa: no permite definir una clase en función de la totalidad de las clases a la cual debería pertenecer la clase definida.

Justo a continuación del artículo de Novak, en la misma revista de **1950**, venía un artículo de Mostowski titulado *Algunas definiciones impredicativas en la teoría de conjuntos axiomática,* en el que analiza las limitaciones que impone a NBG la prohibición de las definiciones impredicativas de clases.

Tras citar el resultado de Novak y Rosser-Wang sobre la equiconsistencia de ZFC y NBG, Mostowski observa que, por el segundo teorema de incompletitud de Gödel, en NBG no es posible demostrar la consistencia de $\ulcorner$ZFC$\urcorner$, pues esto equivaldría a demostrar su propia consistencia, que es equivalente.

Esto lo lleva a plantearse cómo es posible que en NBG no pueda demostrarse la consistencia de ZFC si en NBG se puede demostrar la existencia de la clase universal V y ésta es un modelo de ZFC, es decir, que cuando llamamos "conjuntos" a los conjuntos (a los elementos de V), se cumplen todos los axiomas de ZFC. ¿No basta la existencia de un modelo para justificar la consistencia de ZFC?

En efecto, justamente en este contexto, lo dicho no basta para demostrar la consistencia de ZFC y vamos a analizar el porqué siguiendo (no muy de cerca) a Mostowski:

Recordemos, ante todo, por qué se dice que la existencia de un modelo M de una teoría T implica que T es consistente. Para el caso en que T es una teoría de conjuntos, un modelo es simplemente un conjunto M en el que hay definida una relación R de modo que, cuando interpretamos "conjunto" como "elemento de M" y "pertenencia" como la relación R, todos los axiomas de T resultan verdaderos.

Por concretar, supongamos que en NBG hemos demostrado que existe un modelo M de $\ulcorner\mathrm{ZFC}\urcorner$, donde escribimos $\ulcorner\mathrm{ZFC}\urcorner$ para dejar claro que estamos razonando en NBG, por lo que no hablamos del ZFC metamatemático, intuitivo, sino de $\ulcorner\mathrm{ZFC}\urcorner$ definido en NBG, que es un concepto conjuntista como pueda serlo $\mathbb{R}$ o $\mathcal{P}\mathbb{N}$.

Queremos demostrar Consis($\ulcorner\mathrm{ZFC}\urcorner$), es decir, que

$$\neg \underset{\ulcorner\mathrm{ZFC}\urcorner}{\vdash} \ulcorner 0 \neq 0\urcorner.$$

Para ello suponemos lo contrario, es decir, que en $\ulcorner\mathrm{ZFC}\urcorner$ se puede demostrar $\ulcorner 0 \neq 0\urcorner$. Entonces, por definición de "ser demostrable", tiene que existir una sucesión de fórmulas $\{\gamma_i\}_{i=0}^n$ de modo que cada $\gamma_i \in \mathrm{Form}(\ulcorner\mathrm{ZFC}\urcorner)$, $\gamma_n = \ulcorner 0 \neq 0\urcorner$ y cada γ_i es un axioma lógico, un axioma de $\ulcorner\mathrm{ZFC}\urcorner$, o bien se deduce de fórmulas anteriores por una regla de inferencia lógica.

Basta concluir que esto implica que $\ulcorner 0 \neq 0\urcorner$ tiene que ser verdadera en M porque, por otra parte, es fácil probar justo lo contrario, y así tendremos la contradicción de que $\ulcorner 0 \neq 0\urcorner$ es verdadera y falsa en M y quedará probado que $\ulcorner\mathrm{ZFC}\urcorner$ es consistente.

¿Y cómo podemos concluir que $\ulcorner 0 \neq 0\urcorner$ es verdadera en M? Para ello usamos los hechos siguientes:

1. Todos los axiomas lógicos son verdaderos en M.
2. Todos los axiomas de $\ulcorner\mathrm{ZFC}\urcorner$ son verdaderos en M.
3. Si una fórmula se deduce de otras por una regla de inferencia lógica, si las premisas son verdaderas en M, entonces también lo es la conclusión.

Usando estos hechos, partiendo de la demostración $\{\gamma_i\}_{i=0}^n$, una simple inducción demuestra que cada γ_i tiene que ser verdadera en M, por lo que en particular lo es $\gamma_n = \ulcorner 0 \neq 0\urcorner$.

Éste es el argumento y la pregunta que se hizo Mostowski es qué falla en él para que no podamos demostrar en NBG que $\ulcorner\mathrm{ZFC}\urcorner$ es consistente tomando como modelo M la clase universal V con la relación de pertenencia usual. Y la respuesta es que todo el argumento anterior funciona bien si M es un conjunto, pero no tan bien si M es una clase propia, como le sucede a V.

El primer punto que hay que analizar es que hace falta dar una definición precisa de qué significa que una fórmula $\alpha \in \mathrm{Form}(\ulcorner\mathrm{ZFC}\urcorner)$ sea verdadera en un modelo M. Esto lo hizo esencialmente Tarski en su artículo de 1933 y la definición se formaliza bien en NBG siempre y cuando M sea un conjunto. Si consideramos el caso de la clase V, en principio algo podemos hacer. Mostowski demuestra:

> **Teorema I** Existe una fórmula $V(x)$ con x como única variable libre tal que si ϕ es una sentencia metamatemática cuyos cuantificadores sean todos de tipo "para todo conjunto" o "existe un conjunto" y $\ulcorner\phi\urcorner$ es su formalización en NBG, entonces en NBG se puede demostrar $\phi \leftrightarrow V(\ulcorner\phi\urcorner)$. Dicha fórmula es de la forma $V(x) \equiv \bigvee Y\, \alpha(x, Y)$, donde α es una fórmula cuyos cuantificadores son todos de la forma "para todo conjunto" o "existe un conjunto", pero en el cuantificador final $\bigvee Y$, la variable Y es una clase arbitraria.

De este modo, si ϕ es una sentencia (metamatemática), con cuantificadores restringidos a conjuntos (para que tenga sentido interpretarla en la clase V) su formalización $\ulcorner\phi\urcorner$ pasa a ser una mera sucesión finita de números naturales, pero la fórmula $V(x)$ es capaz de "recuperar" su significado, de modo que $V(\ulcorner\phi\urcorner)$ "vuelve a ser" ϕ.

Si la fórmula $V(x)$ se pudiera definir en ZFC y la equivalencia se pudiera demostrar en ZFC, esto contradiría el teorema de Tarski de indefinibilidad de la verdad, al igual que si la equivalencia demostrada en NBG fuera válida para fórmulas ϕ cualesquiera (sin la restricción sobre sus cuantificadores), pero —por poco— no estamos delinquiendo. La fórmula $V(x)$ cumple las propiedades siguientes:

1. Si ϕ es un axioma lógico, se cumple $V(\phi)$.
2. Si ϕ es un axioma[144] de $\ulcorner\mathrm{ZFC}\urcorner$, se cumple $V(\phi)$.
3. Si ϕ se deduce de otras fórmulas α, β mediante reglas de inferencia lógica y se cumple $V(\alpha), V(\beta)$, entonces también se cumple $V(\phi)$.

[144] Notemos que en estas tres propiedades escribimos ϕ y no $\ulcorner\phi\urcorner$ porque aquí ϕ es una variable, no la formalización de una fórmula metamatemática. Concretamente, esta propiedad se formaliza así: $\bigwedge \phi \in \ulcorner\mathrm{ZFC}\urcorner\, V(\phi)$, donde $\ulcorner\mathrm{ZFC}\urcorner$ es aquí el conjunto de los axiomas de ZFC.

Estas tres propiedades nos bastan para demostrar un caso particular del teorema I que es suficiente para lo que nos ocupa:

Teorema $\mathbf{I_0}$ Si ϕ es una fórmula metamatemática tal que $\underset{\text{ZFC}}{\vdash} \phi$, entonces $\underset{\ulcorner\text{NBG}\urcorner}{\vdash} V(\ulcorner\phi\urcorner)$.

Demostración: Sea $\gamma_0, \ldots, \gamma_n$ (con $\gamma_n \equiv \phi$) una demostración de ϕ en ZFC. Entonces, una simple inducción sobre i demuestra que $\underset{\ulcorner\text{NBG}\urcorner}{\vdash} V(\ulcorner\gamma_i\urcorner)$. En efecto, si γ_i es un axioma lógico o un axioma de ZFC, entonces en NBG se demuestra que $\ulcorner\gamma_i\urcorner$ es un axioma lógico o un axioma de $\ulcorner\text{ZFC}\urcorner$, y por las propiedades 1 y 2 precedentes, $\underset{\ulcorner\text{NBG}\urcorner}{\vdash} V(\ulcorner\gamma_i\urcorner)$. Si, por el contrario, γ_i se deduce de fórmulas anteriores γ_j por una regla de inferencia y, por hipótesis de inducción, en NBG podemos demostrar $V(\ulcorner\gamma_j\urcorner)$, la propiedad 3 nos da $\underset{\ulcorner\text{NBG}\urcorner}{\vdash} V(\ulcorner\gamma_i\urcorner)$.

En particular, para $i = n$, tenemos que $\underset{\ulcorner\text{NBG}\urcorner}{\vdash} V(\ulcorner\phi\urcorner)$. ∎

Aplicando esto a $\phi \equiv 0 = 0$ (que es un teorema de ZFC), tenemos que en NBG se demuestra $V(\ulcorner 0 = 0\urcorner)$ y, de la definición de V, también se sigue que

$$V(\ulcorner 0 \neq 0\urcorner) \leftrightarrow \neg V(\ulcorner 0 = 0\urcorner).$$

¿Y con todo esto, no podemos demostrar $\underset{\text{NBG}}{\vdash} \text{Consis}(\ulcorner\text{ZFC}\urcorner)$? Intentémoslo:

Demostración: Razonamos en NBG y queremos demostrar $\text{Consis}(\ulcorner\text{ZFC}\urcorner)$, es decir, que

$$\neg \underset{\ulcorner\text{ZFC}\urcorner}{\vdash} \ulcorner 0 \neq 0\urcorner.$$

Para ello suponemos lo contrario, es decir, que en $\ulcorner\text{ZFC}\urcorner$ se puede demostrar $\ulcorner 0 \neq 0\urcorner$. Entonces, por definición de "ser demostrable", tiene que existir una sucesión de fórmulas $\{\gamma_i\}_{i=0}^n$ de modo que cada $\gamma_i \in \text{Form}(\ulcorner\text{ZFC}\urcorner)$, $\gamma_n = \ulcorner 0 \neq 0\urcorner$ y cada γ_i es un axioma lógico, un axioma de $\ulcorner\text{ZFC}\urcorner$, o bien se deduce de fórmulas anteriores por una regla de inferencia lógica.

Basta concluir que esto implica que $V(\ulcorner 0 \neq 0\urcorner)$ porque esto equivale a $\neg V(\ulcorner 0 = 0\urcorner)$ y así tendremos la contradicción $V(\ulcorner 0 = 0\urcorner)$ y $\neg V(\ulcorner 0 = 0\urcorner)$.

Las propiedades 1, 2, 3 anteriores nos dan trivialmente que

$$\bigwedge i \leq n(\bigwedge j < i\ V(\gamma_j) \to V(\gamma_i)),$$

es decir, que si suponemos por hipótesis de inducción que todo $j < i$ cumple $V(\gamma_j)$, lo mismo vale para i. Esto prueba que $\bigwedge i \leq n\, V(\gamma_i)$, luego en particular, para $i = n$, tenemos que $V(\ulcorner 0 \neq 0\urcorner)$ y hemos probado (en NBG) $\text{Consis}(\ulcorner\text{ZFC}\urcorner)$. Por el segundo teorema de incompletitud, NBG es contradictorio, y ZFC también. ¿∎?

Como el lector sospechará, este argumento tiene un fallo que no depende de nada "oculto" (de la definición de $V(x)$ que no hemos dado, ni de ninguna consideración que requiera poner en juego cartas que no estén sobre la mesa).

Por simplificar la notación, vamos a llamar $\Phi(i) \equiv V(\gamma_i)$. En estos términos, hemos demostrado en NBG (¡y la demostración es correcta!) que

$$\bigwedge i \leq n(\bigwedge j < i\ \Phi(j) \to \Phi(i)).$$

es decir, que si suponemos por hipótesis de inducción que todos los números naturales menores que un $i \leq n$ cumplen la propiedad Φ, entonces i también la cumple. Y de ahí, hemos pretendido deducir, por el principio de inducción fuerte, que todo $i \leq n$ cumple Φ. ¡Eso es lo que está mal!

¿Cómo se demuestra el principio de inducción fuerte? Por concretar en nuestro caso, suponemos que existe un $k \leq n$ que no cumple $\Phi(k)$, y consideramos el conjunto

$$X = \{i \leq n \mid \neg\Phi(i)\}.$$

Así $k \in X$, luego X es un subconjunto no vacío de $\mathbb{N}$ (finito, de hecho), por lo que tiene que tener un mínimo elemento i, el menor número natural que cumple $\neg\Phi(i)$. Pero por la minimalidad se cumple $\bigwedge j < i\ \Phi(j)$, luego, por lo que hemos demostrado, también se cumplirá $\Phi(i)$ y así tenemos una contradicción, lo que prueba que no existe tal k, es decir, que todo $i \leq n$ cumple $\Phi(i)$. ¿∎?

Pues bien, ¡este argumento también está mal! ¡Esto no es una demostración válida en NBG!

Si llamáramos a Hercules Poirot para que nos resuelva el misterio, nos recordaría que Φ se ha definido a partir de la fórmula $V(x)$, y en el teorema I se ha indicado que $V(x)$ tiene un cuantificador no restringido a conjuntos y que en la página 152 se ha indicado que el teorema de comprensión en NBG sólo afirma que las fórmulas con cuantificadores restringidos a conjuntos definen clases en NBG, pero no dice nada de las fórmulas con cuantificadores arbitrarios. Por lo tanto, la definición de X no es válida en NBG. No podemos asegurar que exista tal conjunto X y mucho menos que tenga un mínimo elemento (y el lector tenía todas las pistas para descubrir al asesino).

De hecho, retocando un poco las fórmulas que estamos considerando, Mostowski demuestra que el principio de inducción usual también falla en NBG para fórmulas arbitrarias:

> **Teorema II** Existe una fórmula metamatemática $\Phi(n) \equiv \bigvee Y\, \alpha(n, Y)$, con n como única variable libre, donde α es una fórmula cuyos cuantificadores son todos de la forma "para todo conjunto" o "existe un conjunto", para la cual en NBG se puede demostrar:
>
> $$\Phi(0) \wedge \bigwedge n \in \mathbb{N}(\Phi(n) \to \Phi(n+1))$$
>
> pero, si NBG es consistente, no se puede demostrar $\bigwedge n \in \mathbb{N}\, \Phi(n)$.

El "truco" es el que ya hemos explicado: las fórmulas con cuantificadores no acotados no definen necesariamente clases, por lo que no se puede demostrar para ellas ninguna forma del principio de inducción.

En el enunciado del teorema I que da Mostowski hay una parte que habíamos omitido por no anticipar acontecimientos, y es que, como hemos demostrado, si NBG es consistente, no es posible demostrar

$$\bigwedge \phi((\underset{\ulcorner \mathrm{ZFC} \urcorner}{\vdash} \phi) \to V(\phi)).$$

Esto sí que permitiría demostrar $\mathrm{Consis}(\ulcorner \mathrm{ZFC} \urcorner)$ en NBG y, por consiguiente, NBG y ZFC serían contradictorios.

Pero¡ Mostowski recalca la diferencia que hay entre esta (única) sentencia, que no es un teorema de NBG, y el teorema I_0, que en realidad es un esquema teoremático que agrupa infinitos teoremas: para cada teorema (metamatemático) ϕ de ZFC se cumple que en NBG se puede demostrar $V(\ulcorner \phi \urcorner)$, con lo que tenemos un teorema distinto (con una demostración distinta) para cada ϕ.

Mostowski destacó también que —como hemos visto— hay fórmulas que no definen clases en NBG:

> **Teorema III** Existe una fórmula metamatemática $\Psi(x) \equiv \bigvee Y\, \alpha(x, Y)$, con x como única variable libre, donde α es una fórmula cuyos cuantificadores son todos de la forma "para todo conjunto" o "existe un conjunto", tal que, si NBG es consistente, no se puede demostrar
>
> $$\bigvee A \bigwedge x(x \in A \leftrightarrow \Psi(x)),$$
>
> (donde $\bigwedge x$ significa "para todo conjunto x").

Como hemos visto, estas restricciones al principio de inducción o a la definición de clases no son gratuitas, sino que si pudiéramos saltárnoslas podríamos demostrar contradicciones en NBG. Pero esto no significa exactamente que si eliminamos la restricción en el teorema de comprensión de NBG obtengamos necesariamente una teoría contradictoria.

En su artículo de 1949, Wang presentaba NBG mediante los axiomas de Gödel excepto los de formación de clases, regularidad y elección, y tomando el teorema de comprensión como esquema axiomático, y llamó NQ a la teoría que resulta de extender el axioma de comprensión a fórmulas arbitrarias, sin exigir que los cuantificadores estuvieran restringidos a conjuntos. La N era por von Neumann y la Q por Quine, porque decía que la versión general del axioma de comprensión "se debía a Quine", que lo había formulado en su contradictoria teoría LM. Sobre NQ dice:

> *A diferencia de* N7 [el esquema de comprensión con cuantificadores restringidos]*, aún no se sabe si* N7′ [el esquema de comprensión general] *es reducible a un número finito de axiomas. Sin embargo, este sistema* NQ *parece ser una extensión interesante del de von Neumann, ya que en él podemos formar clases sin preguntarnos si el predicado definitorio es una "expresión constitutiva"* [tiene los cuantificadores restringidos]*, y la mera sustitución de* N7 *por* N7′ *no parece afectar la consistencia del sistema.*

Pero se notaba que Wang (como Quine o Russell) tenía la perspicacia propia de los filósofos, porque, aparte de que escribe varias veces mal el axioma de extensionalidad (formula la implicación opuesta a la correcta), como le señala Mostowski, la extensión del esquema de comprensión *sí* que tiene consecuencias sobre la consistencia del sistema. La discusión precedente muestra que, sin la restricción en el axioma de comprensión, se cumple

$$\vdash_{\ulcorner \mathrm{NQ} \urcorner} \mathrm{Consis}(\ulcorner \mathrm{ZFC} \urcorner), \qquad \text{o, equivalentemente,} \qquad \vdash_{\ulcorner \mathrm{NQ} \urcorner} \mathrm{Consis}(\ulcorner \mathrm{NBG} \urcorner),$$

lo cual no supone contradicción alguna, pero muestra que la consistencia de NQ *no* es equivalente a la de NBG, ya que si fueran equivalentes sí que tendríamos

$$\vdash_{\ulcorner \mathrm{NQ} \urcorner} \mathrm{Consis}(\ulcorner \mathrm{NQ} \urcorner)$$

y NQ se sumaría a la lista de teorías que se vuelven contradictorias en cuanto se les incorpora una idea de Quine. Más precisamente, mientras que es posible demostrar que NBG es consistente suponiendo que ZFC lo es, no es posible demostrar que NQ es consistente ni siquiera suponiendo que NBG lo es, porque entonces la implicación

$$\mathrm{Consis}(\ulcorner \mathrm{NBG} \urcorner) \to \mathrm{Consis}(\ulcorner \mathrm{NQ} \urcorner)$$

sería demostrable en NQ y nos permitiría demostrar $\mathrm{Consis}(\ulcorner \mathrm{NQ} \urcorner)$, con lo que NQ sería contradictoria.

76 La Introducción a la metamatemática de Kleene En **1952** Kleene publicó su *Introducción a la metamatemática,* dirigida a los matemáticos no especialistas en lógica, y que durante muchos años sería la referencia básica para entender los resultados metamatemáticos obtenidos en la primera mitad del siglo XX. En el prefacio Kleene destaca especialmente los *Fundamentos de las matemáticas,* de Hilbert y Bernays, como una de sus referencias principales, pero su libro es mucho más "moderno" en muchos sentidos, desde la elección de los contenidos hasta por la forma de exponerlos.

El libro está dividido en cuatro partes. La primera, *El problema de los fundamentos,* consta de los tres primeros capítulos, y en ella trata de explicar a un lector matemático los problemas que plantea la fundamentación de las matemáticas.

En el capítulo I empieza hablando de la paradoja de Galileo y de conjuntos numerables, y llega incluso a demostrar el teorema de Cantor-Bernstein sin hacer referencia a ninguna teoría axiomática de conjuntos en particular. Luego sigue hablando de los cardinales $\aleph_0$, $2^{\aleph_0}$ y $2^{2^{\aleph_0}}$. En el capítulo II discute (siempre informalmente) algunos conceptos mucho más elementales: los números naturales, funciones, etc., mientras que en el capítulo III habla de las paradojas de la teoría de conjuntos para explicar la necesidad de precisar lo que se entiende por un razonamiento matemático.

Planteada la pregunta de cómo se explica que el razonamiento matemático dé lugar a paradojas, afirma:

> *Decir que ahora estos temas deberían establecerse sobre una base axiomática no resuelve el problema. Tras la axiomatización, debe existir un nivel de verdad y falsedad. Si la axiomática es informal, los axiomas deben ser verdaderos. Si la axiomática es formal, al menos debemos creer que los teoremas se derivan de los axiomas; y también debe existir alguna relación entre estos resultados y alguna realidad ajena a la teoría axiomática, para que la actividad de los matemáticos no se reduzca al sinsentido. Las proposiciones formalmente axiomatizadas de las matemáticas no pueden constituir la totalidad de las matemáticas; también debe haber una matemática intuitivamente entendida. Si debemos abandonar nuestra creencia anterior de que ésta abarca toda la aritmética, el análisis y la teoría de conjuntos, no estaremos completamente satisfechos a menos que aprendamos en qué era errónea esa creencia y dónde, en cambio, trazar una línea de separación.*
>
> *El problema inmediato de eliminar las paradojas se fusiona así con el problema más amplio de los fundamentos de las matemáticas y la lógica.*
>
> *¿Cuál es la naturaleza de la verdad matemática? ¿Qué significado tienen las proposiciones matemáticas y en qué evidencia se basan? Este amplio problema, o complejo de problemas, existe para la filosofía independientemente de la circunstancia de que las paradojas hayan surgido en la frontera de las matemáticas. Históricamente, esta circunstancia ha llevado a los matemáticos a un estudio más intensivo del problema de lo que habría sido probable que hicieran de no haber sido por ello; y las paradojas obviamente imponen condiciones a la solución del problema.*

Luego describe cómo Poincaré y Russell atribuyeron las paradojas a la admisión de definiciones impredicativas, y presenta las tres posturas básicas ante la fundación de las matemáticas: el logicismo de Russell, el intuicionismo de Brouwer y el formalismo de Hilbert.

Sobre el logicismo explica que el axioma de reducibilidad de los *Principia* arruinaba el programa logicista, pues no tenía más justificación que el hecho de que sin él no era posible formalizar aspectos fundamentales de las matemáticas en el sistema:

> *Weyl (1946) afirma que, en el sistema de los* "Principia mathematica", *"las matemáticas ya no se fundamentan en la lógica, sino en una especie de paraíso para los lógicos..." ; y observa que quien esté dispuesto a creer en este "mundo trascendental" también podría aceptar el sistema de la teoría axiomática de conjuntos (Zermelo, Fraenkel, etc.), que, para la deducción de las matemáticas, tiene la ventaja de ser más simple en su estructura.*

Del intuicionismo concluye:

> *Como sustituto de las matemáticas clásicas, ha resultado ser menos potente y, en muchos sentidos, más complejo de desarrollar. Por ejemplo, en la teoría del continuo de Brouwer, no podemos afirmar que dos números reales cualesquiera a y b sean iguales o desiguales. Nuestro conocimiento sobre la igualdad o desigualdad de a y b puede ser más o menos específico. Por $a \neq b$, se entiende que $a = b$ conduce a una contradicción, mientras que $a\#b$ es un tipo de igualdad más fuerte, lo que significa que se puede dar un ejemplo de un número racional que separa a y b. Por supuesto, $a\#b$ implica $a \neq b$. Pero hay pares de números reales a y b para los que no se sabe que $a = b$ o $a \neq b$ (o $a\#b$). Es evidente que tales complicaciones sustituyen la teoría clásica del continuo por otra mucho menos clara. A pesar de ello, no se descarta la posibilidad de una reconstrucción intuicionista de las matemáticas clásicas de una manera diferente que implique una reinterpretación (recientemente emprendida).*[145]

Sobre el formalismo dice:

> *Un veredicto sobre el pensamiento de los formalistas dependerá en parte de los frutos del programa que proponen. Este programa requiere una materia llamada "metamatemática", cuyo objetivo principal es establecer la consistencia de las matemáticas clásicas.*
>
> *Adelantamos que la metamatemática proporcionará una técnica matemática rigurosa para investigar una gran variedad de problemas fundamentales para las matemáticas y la lógica, entre los cuales el problema de la consistencia es sólo uno más. Por ejemplo, los métodos metamatemáticos se aplican actualmente en estudios de sistematizaciones matemáticas derivadas de las escuelas logicista e intuicionista, así como de la de Hilbert. (Y a la inversa, la metamatemática debe su origen a las investigaciones logicista e intuicionista). Nuestro objetivo en el resto de este libro no es emitir un veredicto que apoye o rechace el punto de vista formalista en ninguna versión preasignada, sino comprender en qué consiste el método metamatemático y aprender algunos de los descubrimientos que se han obtenido al aplicarlo.*

Observemos ahora cómo explica Kleene lo que es la metamatemática:

> *A Hilbert se debe, en primer lugar, el énfasis en que la formalización estricta de una teoría implica la abstracción total del significado, denominándose al resultado un sistema formal o formalismo (o, a veces, una teoría formal o matemáticas formales); y, en segundo lugar, su método para convertir el sistema formal en su conjunto en objeto de un estudio matemático llamado metamatemáticas o teoría de la demostración.*
>
> *La metamatemática incluye la descripción o definición de sistemas formales, así como la investigación de sus propiedades. Al tratar un sistema formal particular, podemos llamarlo teoría objeto, y a las metamatemáticas relacionadas con él, metateoría.*
>
> *Desde el punto de vista de la metateoría, la teoría objeto no es propiamente una teoría en absoluto, tal como entendíamos anteriormente el término, sino un sistema de objetos sin sentido, como las posiciones en una partida de ajedrez, sujetos a manipulaciones mecánicas como las jugadas en el*

[145] Aquí remite a la sección en la que presenta los resultados de Gödel y Gentzen que permiten reinterpretar la lógica clásica en términos intuicionistas.

ajedrez. La teoría objeto se describe y estudia como un sistema de signos y de objetos construidos a partir de signos. Los signos se consideran simplemente como diversos tipos de objetos reconocibles. Para fijar ideas, podemos pensar en ellos concretamente como marcas en el papel; o, más precisamente, como abstraídos de nuestra experiencia con signos como marcas en el papel. (La teoría de la demostración debe ser hasta cierto punto abstracta, ya que supone que se pueden construir secuencias de signos arbitrariamente largas, aunque la cantidad de papel y tinta en el mundo sea finita). Los demás objetos del sistema se analizan únicamente en términos de cómo se componen a partir de los signos. Por definición, esto es todo lo que un sistema formal debe ser como objeto de estudio para la metamatemática.

La metateoría pertenece a la matemática intuitiva e informal (a menos que la metateoría se formalice en una metametateoría, cosa que aquí no consideramos). La metateoría se expresará en lenguaje ordinario, con signos matemáticos, como variables metamatemáticas, introducidos según sea necesario. Las afirmaciones de la metateoría deben tener un significado. Las deducciones deben ser convincentes. Deben proceder mediante inferencias intuitivas y no, como las deducciones en la teoría formal, mediante la aplicación de reglas establecidas. Se han establecido reglas para formalizar la teoría objeto, pero ahora debemos comprender, sin reglas, cómo funcionan esas reglas. Una matemática intuitiva es necesaria para definir la matemática formal.

(Entendemos esto como que la apelación final para justificar una inferencia metamatemática debe basarse en el significado y la evidencia, más que en cualquier conjunto de reglas convencionales. Esto no nos impedirá, en la práctica, sistematizar nuestros resultados metamatemáticos en teoremas o reglas, que luego pueden aplicarse cuasiformalmente para abreviar el razonamiento intuitivo. Este es un procedimiento familiar en la matemática informal).

Los métodos empleados en la metateoría se restringirán a los métodos —denominados finitistas por los formalistas— que emplean únicamente objetos concebibles intuitivamente y procesos realizables. (Traducimos el alemán "finit" como "finitista", ya que "finito" se usa para el alemán "endlich"). Ninguna clase infinita puede considerarse un todo completo. Las pruebas de existencia proporcionarán, al menos implícitamente, un método para construir el objeto cuya existencia se está demostrando.

Esta restricción es necesaria para el propósito por el cual Hilbert introduce las metamatemáticas. Las proposiciones de una teoría matemática dada pueden no tener un significado claro, y las inferencias en ella pueden no aportar evidencia indudable. Al formalizar la teoría, su desarrollo se reduce a forma y regla. Ya no existe ambigüedad sobre qué constituye un enunciado de la teoría o qué constituye una prueba en la teoría. Entonces, la cuestión de si los métodos formalizados en ella conducen a contradicciones, y otras cuestiones sobre el efecto de dichos métodos, deben investigarse en la metateoría, mediante métodos que no estén sujetos a las mismas dudas que los métodos de la teoría original. [...]

(Algunos autores usan "meta-" para identificar un lenguaje o teoría en el que otro lenguaje o teoría se convierte en objeto de estudio no restringido a métodos finitistas. También se discute en este contexto la diferencia entre "lenguaje sintáctico" frente a "lenguaje objeto". [...] *En este libro, sólo usamos "meta-" cuando los métodos son finitistas).*

Los sistemas formales que se estudian en la metamatemática suelen elegirse de modo que sirvan de modelos para partes de las matemáticas y la lógica informales con las que ya estamos más o menos familiarizados y de las que surgieron por formalización. Los significados que se pretenden adjuntar a los signos, fórmulas, etc., de un sistema formal dado, al considerar el sistema como una formalización de una teoría informal, los llamamos la interpretación (prevista) del sistema (o de sus signos, fórmulas, etc.). En otras palabras, las interpretaciones de los signos, fórmulas, etc., son los objetos, proposiciones, etc., de la teoría informal que se correlacionan según el método por el cual el sistema constituye un modelo para la teoría informal.

En el caso de una fórmula que representa un enunciado ideal de las matemáticas clásicas, la interpretación no puede constituir un significado totalmente intuitivo (o finitista), sino que debe consistir en todo aquello en lo que el matemático clásico piensa en el desarrollo informal (o no estrictamente formalizado) de las matemáticas clásicas, es decir, en el desarrollo que ha tenido lugar históricamente y que tiene lugar actualmente, cuando el procedimiento no se está formalizando conscientemente en el sentido estricto de la teoría de la demostración.

La interpretación motiva al metamatemático en su elección del sistema formal particular que introduce mediante sus definiciones, lo guía en la elección de los problemas relacionados con el sistema que investiga. Incluso puede proporcionarle pistas esenciales para lograr la solución de esos problemas. Sólo en la declaración final y la prueba de sus resultados se le prohíbe (como metamatemático) usar la interpretación.

¿Cuán restrictiva es esta prohibición? La metamatemática debe estudiar el sistema formal como un sistema de signos, etc., que se consideran de forma totalmente objetiva. Esto significa simplemente que esos signos, etc., son en sí mismos los objetos últimos, y no se usan para referirse a algo distinto de sí mismos. El metamatemático los mira a ellos, no a través ni más allá de ellos; así, son objetos sin interpretación ni significado.

Ahora bien, al estudiar esos objetos, la metamatemática debe aplicar sus propios métodos y herramientas. Éstos pueden ser cualesquiera con tal de que sean finitistas. Por ejemplo, la metamatemática puede emplear los números naturales de forma finitista. En el caso de fórmulas que admiten (fuera de la metamatemática) una interpretación finitista, es posible dentro de la metamatemática definir propiedades de esos objetos formales que (desde fuera de la metamatemática) son equivalentes a sus interpretaciones. Así, las interpretaciones finitistas pueden introducirse por la puerta de atrás. Sin embargo, la metamatemática no puede en modo alguno tratar con las interpretaciones no finitistas de las proposiciones ideales de las matemáticas clásicas.

Para dejar claro en todo momento por qué nos interesan los sistemas formales que estamos considerando, y cómo constituyen formalizaciones de porciones de la lógica y las matemáticas con las que ya estamos familiarizados informalmente, en este libro indicaremos las posibilidades de interpretación y usaremos terminología sugestiva, como "prueba" para las derivaciones formales, e "y" para el nombre del signo $\wedge$. Esto es necesario para nuestro propósito completo, aunque la interpretación sea ajena a la metamatemática misma.

La segunda parte del libro comprende los capítulos V, VI, VII y VIII, y en ella Kleene expone y analiza el cálculo deductivo. En el capítulo cuarto introduce los lenguajes formales, con los signos lógicos

$$\neg, \qquad \supset, \qquad \&, \qquad \vee, \qquad \forall, \qquad \exists, \qquad =,$$

y plantea los siguientes axiomas y reglas de inferencia (y que transcribimos con los signos que usamos aquí habitualmente):

- Axiomas para el cálculo proposicional:[146]

  1. $\alpha \to (\beta \to \alpha)$
  2. $(\alpha \to \beta) \to ((\alpha \to (\beta \to \gamma)) \to (\alpha \to \gamma))$
  3. $\alpha \to (\beta \to \alpha \wedge \beta)$
  4. $\alpha \wedge \beta \to \alpha, \quad \alpha \wedge \beta \to \beta$
  5. $\alpha \to \alpha \vee \beta, \quad \beta \to \alpha \vee \beta$
  6. $(\alpha \to \gamma) \to ((\beta \to \gamma) \to (\alpha \vee \beta \to \gamma))$
  7. $(\alpha \to \beta) \to ((\alpha \to \neg\beta) \to \neg\alpha)$
  8. $\neg\neg\alpha \to \alpha$

- Reglas de inferencia para el cálculo proposicional:

$$\frac{\alpha, \quad \alpha \to \beta}{\beta}$$

- Axiomas (adicionales) para el cálculo de predicados:

  9. $\bigwedge x\, \alpha(x) \to \alpha(t)$
  10. $\alpha(t) \to \bigvee x\, \alpha(x)$

[146] Si se reemplaza el axioma 8 por $\alpha \to (\neg\alpha \to \beta)$ obtenemos el cálculo deductivo intuicionista.

- Reglas de inferencia (adicionales) para el cálculo de predicados:

$$\frac{\gamma \to \alpha(x)}{\gamma \to \bigwedge x \alpha(x)} \qquad \frac{\alpha(x) \to \gamma}{\bigvee \alpha(x) \to \gamma}$$

- Axiomas (adicionales) para la aritmética (extendiendo el lenguaje con los signos 0, $(\ )'$, $+$, $\cdot$):

11. $a = b \to (a = c \to b = c)$
12. $a = b \to a' = b'$
13. $a' = b' \to a = b$
14. $a' \neq 0$
15. $a + 0 = a, \qquad a + b' = (a + b)'$
16. $a \cdot 0 = 0, \qquad a \cdot b' = a \cdot b + a$
17. $(\alpha(0) \wedge \bigwedge x(\alpha(x) \to \alpha(x'))) \to \bigwedge x\, \alpha(x)$

Notemos que cada "axioma" es en realidad un esquema de axioma. Por ejemplo, $\alpha \to (\beta \to \alpha)$ representa las infinitas fórmulas que pueden construirse sustituyendo las metavariables α y β por fórmulas concretas. Puesto que hay infinitas fórmulas posibles, hay infinitos axiomas lógicos de esta forma.

Hemos detallado los axiomas y reglas de inferencia para que el lector se haga una idea del aspecto global que tiene un cálculo deductivo "a la Hilbert" moderno. Notemos que Kleene no considera axiomas lógicos generales para el igualador, sino que las propiedades básicas del igualador sólo pueden deducirse usando los axiomas de Peano. Por ejemplo, ¿sabría el lector deducir que $a = a$ a partir de estos axiomas? SOLUCIÓN[147].

El capítulo IV contiene las definiciones y resultados necesarios para dar sentido a estos axiomas y reglas de inferencia e introducir el concepto de deducción formal que ya conocemos: una deducción formal a partir de unas premisas es una sucesión finita de fórmulas tal que cada una de ellas es una premisa, o bien uno de los axiomas anteriores, o bien se deduce de fórmulas anteriores por alguna de las reglas de inferencia. En el capítulo V prueba resultados generales sobre deducciones formales, en el capítulo VI obtiene resultados específicos para el cálculo proposicional (que sólo usa el primer grupo de axiomas y reglas de inferencia), el capítulo VII obtiene resultados para el sistema completo y en el capítulo VIII estudia la aritmética de Peano[148] El capítulo termina explicando los teoremas de incompletitud de Gödel y demostrándolos admitiendo un lema técnico que demostrará en la tercera parte.

La tercera parte trata de la teoría de la recursión. En el capítulo IX se estudian las funciones recursivas primitivas, en el capítulo X se presenta la formalización de la matemática necesaria para demostrar los teoremas de incompletitud, en el capítulo XI se estudian las funciones recursivas generales y se demuestra el teorema de Church sobre el problema de la decisión, en el capítulo XII se estudian las funciones recursivas parciales y en el capítulo XIII se estudian las máquinas de Turing.

Mientras Church, Turing y Gödel estaban de acuerdo en considerar las tres definiciones equivalentes de computabilidad como una definición formal de lo que es una función calculable en la práctica, Kleene adopta una postura mucho más próxima al punto de vista de Post. En el capítulo XI, previamente a la demostración del teorema de Church enuncia:

> TESIS DE CHURCH *Toda función efectivamente calculable es recursiva.*

y añade:

> *La tesis y su recíproco proporcionan la* definición *exacta de la noción de procedimiento o algoritmo de cálculo (decisión).*

pero en el capítulo XII afirma:

[147] En 11 tomamos damos a a, b, c los valores $a + 0, a, a$, respectivamente, con lo que obtenemos $a + 0 = a \to (a + 0 = a \to a = a)$ y, considerando también 15, aplicamos la regla del modus ponens dos veces.

[148] Al contrario que Peano o Dedekind, Kleene toma al 0 y no al 1 como primer número natural.

> **Tesis de Church.** *Uno de los principales objetivos de este capítulo y del siguiente es presentar la evidencia de la tesis de Church.*
>
> *Dado que nuestra noción original de calculabilidad efectiva de una función es intuitivamente algo vaga, la tesis no puede demostrarse.*

A su vez, en el capítulo XIII presenta la *Tesis de Turing* como la afirmación de que toda función calculable en la práctica es Turing-computable, y afirma que es equivalente a la tesis de Church porque previamente ha demostrado que las funciones Turing-computables coinciden con las funciones recursivas parciales.

A partir de ahí habla siempre de la *Tesis de Church,* salvo en una ocasión, en la que la llama *Tesis de Church-Turing,* y así es como se la ha conocido tradicionalmente desde entonces. Aunque Kleene expuso las abundantes evidencias en favor de la "tesis", la forma en que la presentó extendió la idea de que lo "ortodoxo" es considerar la "tesis de Chuch-Turing" como una suerte hipótesis indemostrable, cuando ni Church ni Turing entraban en tal "ortodoxia".

En **1953** Rosser publicó su libro *Lógica para matemáticos,* y en su primer capítulo plantea un hipotético diálogo entre Descartes y un matemático moderno, el profesor X. Éste convence a Descartes de que la definición $\epsilon - \delta$ de continuidad es preferible a la noción vaga de continuidad que tiene Descartes, pero entonces Descartes le plantea este problema:

> *Tengo aquí un concepto importante al que llamo continuidad. Actualmente, mi noción es bastante vaga; no lo suficiente como para no poder decidir qué curvas son continuas, pero sí demasiado vaga como para permitir demostraciones precisas. Usted propone una definición precisa de esta misma noción. Sin embargo, dado que mi definición es demasiado vaga para servir de base a una demostración precisa, ¿cómo vamos a verificar que mi definición vaga y su definición precisa son definiciones de lo mismo?*

Sin embargo, Descartes y el profesor X acaban estando de acuerdo en que es razonable adoptar como definición el concepto $\epsilon - \delta$ de continuidad, sin necesidad de llamarlo "tesis" en vez de "definición".[149]

Pero, para terminar con el libro de Kleene, la cuarta parte (Temas adicionales) consta de dos capítulos (pero que abarcan más de la cuarta parte del libro). El capítulo XIV trata, entre otros temas, el teorema de completitud de Gödel,[150] la paradoja de Skolem y la existencia de modelos no estándar de la aritmética. El capítulo XV presenta el cálculo secuencial de Gentzen con algunas aplicaciones. Por ejemplo, demuestra la consistencia del sistema aritmético que ha definido en la primera parte restringiendo el principio de inducción a fórmulas sin cuantificadores. Luego explica sin detalles la prueba de Gentzen de la consistencia de la aritmética y da la prueba de Gentzen de que la lógica clásica puede expresarse en la lógica intuicionista.

77 La Lógica para matemáticos de Rosser Volviendo al libro de Rosser, estaba en las antípodas del de Kleene. Su título y su prólogo son muy alentadores:

> *La lógica moderna se ha convertido en un campo de estudio amplio y diversificado, con numerosas ramas bien desarrolladas. Muchas de estas ramas tienen poco valor para el matemático como herramienta de razonamiento matemático. Un texto sobre dicha rama de la lógica, por excelente que sea, resultaría de poco interés para un lector principalmente matemático. Por el contrario, ciertos temas de gran valor como herramientas de razonamiento matemático resultan poco interesantes para los estudiantes de lógica y casi nunca se abordan en libros de lógica. Por lo tanto, entre los muchos libros de lógica, ninguno es completamente adecuado para el matemático.*

Y, en efecto, el libro está adornado ejemplos sobre geometría, cálculo diferencial, etc., pero ya en el prólogo aparece una frase inquietante:

> *En el presente texto utilizamos la lógica simbólica porque de otra manera no sabemos cómo lograr la precisión deseada.*

[149] En realidad, Rosser no pone este ejemplo para abordar el problema de qué hay que entender por "función calculable en la práctica", sino el de qué hay que entender por "razonamiento matemático preciso", pero es innegable que viene como anillo al dedo como réplica a Kleene.

[150] Kleene señala que la prueba no es "intuicionista", lo que viene a significar que no es estrictamente finitista, pero no le pone ninguna objeción.

Y, en efecto, Rosser usa el "peaniano" de los *Principia Mathematica* en todo momento. He aquí un ejemplo de "enunciado preciso":

Theorem XI.2.2.

I. $\vdash (n):n \in \mathrm{NC}. \equiv .(\mathrm{E}\alpha).n = \mathrm{Nc}(\alpha).$

II. $\vdash (\alpha,\beta):\alpha \mathrm{\ sm\ } \beta. \equiv .\mathrm{Nc}(\alpha) = \mathrm{Nc}(\beta).$

III. $\vdash (n):.n \in \mathrm{NC}: \supset :(\alpha):\alpha \in n. \equiv .n = \mathrm{Nc}(\alpha).$

IV. $\vdash (m,n):m,n \in \mathrm{NC}.m \cap n \neq \Lambda. \supset .m = n.$

V. $\vdash (\alpha)(\mathrm{E}_1 n).\alpha \in n.n \in \mathrm{NC}.$

VI. $\vdash (n):n \in \mathrm{NC}. \supset .n \neq \Lambda.$

(Por ejemplo, II afirma que si dos clases α y β son biyectables, entonces tienen el mismo cardinal. Con esta pista, el lector puede tratar de desencriptar el resto de apartados. Nótese que Λ es el conjunto vacío.)

Pero lo peor no son las formas, sino el fondo: Rosser consideró que lo que mejor le venía a los matemáticos era estudiar los Nuevos Fundamentos de Quine. A la hora de decidirse entre una teoría como la de Zermelo o NF, su valoración final es:

> *Todas las sugerencias actuales para evitar las paradojas conservan un matiz de artificialidad. Ciertamente, la teoría de tipos es artificial. En la teoría de conjuntos de Zermelo, la distinción entre conjuntos y no conjuntos es engorrosa, y los diversos criterios para decidir entre conjuntos y no conjuntos no son intuitivamente muy naturales.*
>
> *En el sistema del presente texto, los Nuevos Fundamentos de Quine, resulta engorroso que no todas las condiciones determinen clases, y que el criterio de estratificación para decidir qué condiciones las determinarán no sea intuitivamente natural.*
>
> *Tanto la teoría de conjuntos como los Nuevos Fundamentos de Quine reproducen el razonamiento matemático con una aproximación notablemente cercana a los métodos sin trabas utilizados antes del descubrimiento de las paradojas. Ciertas regiones de la teoría de cardinales y ordinales están demasiado cerca de las paradojas como para sobrevivir sin cambios, pero ha sido posible amputar las paradojas conocidas con un daño notablemente mínimo al cuerpo principal de las matemáticas.*

Por ejemplo, para enunciar el teorema de Cantor, en lugar de expresarlo como hemos hecho nosotros en la página 141, Rosser define un *conjunto cantoriano* como un conjunto X que es biyectable con el conjunto $\mathcal{P}_1 X = \{\{u\} \mid u \in X\}$, y entonces demuestra:

$$\vdash (\alpha) : \mathrm{Can}(\alpha). \supset . \sim (\alpha \mathrm{\ sm\ } \mathrm{SC}(\alpha)).$$

es decir, que si α es un conjunto cantoriano, entonces no es biyectable con $\mathcal{P}\alpha$.

Tal y como hemos visto al comentar NV, la paradoja de Cantor implica que el conjunto universal V no es cantorniano, pero a Kleene no le chirría mucho:

> *Este teorema establece* $\vdash \neg(V \mathrm{\ sm\ } \mathrm{USC}(V))$, [es decir, que V no puede biyectarse con $\mathcal{P}_1 V$] *lo cual parece intuitivamente erróneo, ya que tenemos la sensación de que para cualquier clase* α *deberíamos poder demostrar* $\alpha \mathrm{\ sm\ } \mathrm{USC}(\alpha)$ *haciendo que* x *corresponda a* $\{x\}$ *para cada* x *de* α. *En realidad, nuestras restricciones de estratificación claramente impiden esto, afortunadamente.*
>
> *Tenemos aquí el primer caso en el que nuestro sistema formal se desvía en algún aspecto importante de nuestras ideas intuitivas. De hecho, demostraremos* $\mathrm{Can}(\alpha)$ *para las clases más comunes de las matemáticas (como la clase de los enteros, la clase de los números reales, etc.), de modo que, para la mayoría de los propósitos matemáticos, nuestra lógica formal sigue bastante bien la lógica intuitiva.*
>
> *De hecho, las clases* α *para las que aparentemente no podemos demostrar* $\mathrm{Can}(\alpha)$ *son las clases con un gran número de elementos, como* V*, o la clase de todos los números ordinales, o clases de este tipo, que, desde un punto de vista intuitivo, no están definidas con precisión. Para clases tan grandes y vagas, en la frontera de nuestra comprensión, no es realmente sorprendente que algunas propiedades, como* $\mathrm{Can}(\alpha)$*, que hemos extrapolado de clases finitas, no se cumplan.*

Ese año de **1953** murió Zermelo, a los 81 años, pero, como en el caso de Poincaré, no hay evidencias de que la lectura del libro de Rosser hubiera precipitado el fin de sus días.

El capítulo XIV está dedicado al axioma

$$(\lambda) :: (\alpha) : \alpha \in \lambda. \supset .\alpha \neq \Lambda : .(\alpha, \beta) : \alpha, \beta \in \lambda.\alpha \neq \beta. \supset .\alpha \cap \beta = \Lambda. :\supset: .(E\gamma)(\alpha) : \alpha \in \lambda. \supset .(E_1 x).x \in \alpha \cap \gamma.$$

que, como el lector habrá reconocido, no es más que el axioma de elección,[151] y demuestra su equivalencia con el principio de buena ordenación, el lema de Zorn, etc. Sin embargo, ese mismo año el matemático suizo Ernst Paul Specker asestó el golpe definitivo a la propuesta de Rosser con su artículo *El axioma de elección en los Nuevos Fundamentos de Quine para la lógica matemática,* donde demuestra que NF es contradictorio si incluimos en la teoría el axioma de elección.

Aunque el lector ya tiene suficiente información como para formarse una opinión sobre el libro de Rosser, copiamos aquí algunos fragmentos de una reseña que Curry —que se declaraba formalista— hizo de él:

> *Este libro constituye, sin duda, una importante aportación a la literatura de lógica matemática. Sin embargo, no es precisamente la aportación que cabría esperar de su título, su prólogo y la reputación de su autor. El prólogo afirma que el libro está concebido como un libro de texto para matemáticos experimentados; que, como tal, pretende ser relativamente completo; y que se omiten deliberadamente cuestiones de considerable importancia lógica que no resultan de interés para el matemático. El libro resulta ser una exposición detallada, basada en los Principia Mathematica, de un sistema logicista particular.*

Tras explicar que Rosser trabaja en la teoría de Quine y resumir su historia, Curry señala:

> *Por otra parte, pronto se hicieron evidentes ciertas anomalías. Como el propio Quine demostró en 1937, la paradoja de Cantor sólo se evita porque una clase α no siempre tiene el mismo cardinal que el conjunto de sus subconjuntos unitarios (que Rosser llama* USC*(α)). Existen varias anomalías relacionadas con la inducción matemática; así, en este libro se necesita un axioma especial que establezca que los primeros n números naturales forman un conjunto de cardinal n. La restricción a propiedades estratificadas es peculiarmente molesta; el criterio no sólo es tedioso de verificar (mucho más que la restricción a subconjuntos de un conjunto dado) en caso de que haya términos definidos, sino que tiende a fallar en los lugares más inesperados. Sin embargo, la anomalía más sorprendente es la mostrada recientemente por Specker (cuya exposición se basa en este libro). Specker demostró que el axioma de elección es incompatible con* NF.

Luego Curry señala que los conjuntos grandes tienen un comportamiento patológico en NF, pero:

> *Sólo los conjuntos ordinarios tienen interés en matemáticas. Parece claro que, para desarrollar una matemática remotamente similar a la que conocemos, será necesario introducir en algún momento una restricción a los conjuntos ordinarios. Dicha restricción será similar a las de la teoría de conjuntos más ortodoxa; y en tal caso, la restricción a las propiedades estratificadas constituye una complicación innecesaria y molesta.*
>
> *A pesar de todo esto —de hecho, debido a ello—, el sistema* NF *reviste gran interés lógico. Su publicación contribuyó significativamente a profundizar nuestra comprensión. Al presentar el tratamiento más elaborado de este sistema hasta la fecha, Rosser ha prestado un verdadero servicio a la lógica. Sin embargo,* NF *es una extraña elección para una lógica para matemáticos. Incluso antes del descubrimiento de Specker, se sabía lo suficiente sobre el carácter anómalo y peligroso del sistema como para que Rosser hubiera advertido los riesgos que corría.*

La conclusión final es:

> *En conclusión, el revisor encuentra tanto méritos como defectos en esta obra de Rosser. Es el tratamiento más completo de los Nuevos fundamentos de Quine que existe ahora; y hace varias contribuciones menores a la lógica técnica. Tiene varias virtudes desde el punto de vista expositivo. Sin embargo, como lógica para matemáticos, es algo decepcionante. Hace una elección desafortunada del sistema logicista y se excede en su compromiso con él. Además, al revisor le parece un poco anticuado; contrariamente a lo afirmado en el prólogo, considera varios temas cuyo interés parece técnico y especial; mientras que otros temas de la lógica moderna, cuyo interés matemático parece mucho mayor, se pasan por alto.*

---

[151] Desencriptado: $\bigwedge\lambda(\bigwedge\alpha(\alpha \in \lambda \to \alpha \neq \varnothing) \wedge \bigwedge\alpha\beta \in \lambda(\alpha \neq \beta \to \alpha \cap \beta = \varnothing) \to \bigvee\gamma\bigwedge\alpha(\alpha \in \lambda \to \overset{1}{\bigvee} x\, x \in \alpha \cap \gamma))$.

Pero, para hacerle justicia a Rosser, hay que decir que también tuvo sus admiradores. Skolem escribió otra reseña en 1954 en términos muy diferentes:

> *Este libro aborda cuestiones lógicas de interés para los matemáticos en activo. Se omiten las ramas de la lógica moderna de escaso interés para los matemáticos comunes. Se puede decir que el libro es una versión modernizada de los* Principia Mathematica *de Russell y Whitehead; la exposición simbólica se ha simplificado y se han tenido en cuenta desarrollos modernos, como el lema de Zorn. Una característica del libro es que los principios lógicos se ilustran con numerosos ejemplos y cuenta con numerosos ejercicios que hacen especialmente valioso su estudio.* [...]
>
> *Como es bien sabido, la negación del requisito de que toda condición formulada arbitrariamente determine una clase o un "conjunto" es el método utilizado en los sistemas lógicos aceptados hasta la fecha. En la teoría de conjuntos de Zermelo, la restricción respecto a este requisito es bastante artificial y nada intuitiva. En la teoría de tipos, la restricción es quizás algo menos artificial. El autor elige un tercer procedimiento, inspirado en W. V. Quine. Según éste, una condición sólo define una clase cuando está estratificada, es decir, cuando se pueden añadir subíndices a las variables de la condición de modo que, en cada relación $x \in y$ que aparece en la condición, y tenga el subíndice $n+1$ siempre que con la que x tiene el subíndice n.* [...]
>
> *Cabe señalar, sin embargo, que no todos los teoremas de las matemáticas clásicas se mantienen válidos sin cambios en la teoría actual. Así, el teorema de Cantor, que establece que el conjunto de todos los subconjuntos de un conjunto S tiene una cardinalidad mayor que S, no es válido en general. Por otro lado, sigue siendo válido en los casos realmente relevantes para las matemáticas. El revisor considera muy acertado que se haya desarrollado una teoría de conjuntos modificada de este tipo, ya que la actitud de la mayoría de los matemáticos con respecto a este tema ha sido demasiado dogmática. El libro es muy claro y fácil de leer, aunque las partes más técnicas requieren cierta paciencia. El revisor recomienda encarecidamente su estudio.*

Skolem tenía ya 67 años. Parece ser que, tras las disputas continuas que había mantenido con Zermelo, cuanto menos se pareciera una teoría a la de Zermelo, más razonable le parecía, por estrafalaria que fuera.

Turing tenía 41 años, pero en 1954, apenas un mes antes de que hubiera cumplido 42 fue hallado muerto en su casa, envenenado por arsénico. La policía concluyó que había sido un suicidio, aunque algunos no descartaron que hubiera sido un accidente.[152]

En 1956 Church publicaría su *Introducción a la lógica matemática,* en la misma línea "sensata" de Kleene.

Ese mismo año Kleene dio un curso de verano para profesores de enseñanza secundaria y universitaria siguiendo su libro, pero en los apuntes del curso, que fueron "mimeografiados" y distribuidos por uno de los asistentes, se lee:

> `Este razonamiento nos da el teorema siguiente, en el que escribimos ''|='' como abreviatura de ''E es válida''.`

Es, probablemente, el primer uso registrado del signo $\models$. En su *Lógica matemática,* de 1964, Kleene dice:

> *El signo "$\vdash$" se remonta a Frege, 1879; su uso actual se remonta a Rosser, 1935 y Kleene, 1934. (Rosser lo propuso para expresar la deducibilidad mediante las reglas de inferencia, y Kleene sugirió incluir también el uso de los axiomas). El uso paralelo de "$\models$" es quizás original de Kleene, 1956a.*

Así, $\vdash$ significa "es demostrable" y $\models$ significa "es verdadero".[153]

[152] Sus últimos dos años no habían sido muy agradables. En 1952 entraron a robar a su casa, y poco después su amante (Arnold Murray, de 19 años) le confesó que había sido cómplice del robo. Turing lo denunció a la policía, y durante la investigación no ocultó su homosexualidad, que era un delito en Gran Bretaña. Fue condenado por "indecencia grave" y el juez le dio a elegir entre una pena de cárcel o la libertad condicional, siempre y cuando accediera a someterse a una castración química. Turing la aceptó y el tratamiento lo dejó impotente y con alteraciones fisiológicas. Trató de emigrar a los Estados Unidos, pero le fue denegada la entrada.

[153] Estos signos se denominan "trinquete" y "doble trinquete".

78 Determinación Oskar Morgenstern era un economista alemán que había obtenido una plaza en la universidad de Viena, pero se encontraba en Princeton cuando Hitler se anexionó Austria, y ya no volvió. No tardó en leer un artículo que von Neumann había publicado unos años antes, en 1928, titulado *Teoría de los juegos de mesa.* Se pusieron en contacto y empezaron a colaborar hasta que en 1944 publicaron *Teoría de juegos y comportamiento económico,* que sentó las bases de la *teoría de juegos.* En esta disciplina destacó el matemático canadiense Albert William Tucker, que dirigió la tesis de David Gale (leída en 1948) y la de John Forbes Nash (leída en 1950), entre otros. En 1950 Tucker analizó lo que llamó el *dilema del prisionero,* que es una de las paradojas más famosas de la teoría de juegos. En **1953** Tucker y Harold William Kuhn (un amigo y compañero de estudios de Nash, que tenía entonces 28 años) publicaron como editores una recopilación de artículos de teoría de juegos, entre los que había uno del propio Kuhn, titulado *Juegos extensivos y el problema de la información,* en el que introdujo una formalización matemática de cierto tipo de juegos, y también otro de Gale junto con Frank M. Stewart (un compañero de Gale en la universidad de Brown, doctorado en Harvard), en el que extendían las definiciones de Kuhn a "juegos infinitos" de dos jugadores, en los que hay que hacer infinitas jugadas para determinar quién es el ganador.

El interés que estos juegos infinitos pudieran tener en la teoría de juegos (como disciplina orientada a la economía y a otros casos prácticos) era más que dudoso. De hecho, los autores tratan de justificarse:

> *Finalmente, cabe mencionar las razones para considerar juegos del tipo descrito. Si bien es cierto que un juego de este tipo no puede jugarse en su forma extensiva, se espera que las técnicas empleadas aquí puedan aplicarse a juegos infinitos en la forma normalizada. Además, la consideración del contraejemplo y los resultados positivos en el caso infinito arrojan luz sobre la demostración de von Neumann para juegos finitos. Finalmente, en ciertos problemas tácticos y de persecución se dispone de mucha información, aunque no perfecta, sobre las jugadas pasadas del oponente. Para tales problemas, una forma extensiva puede ser más útil que la forma normal. Esperamos que este estudio de juegos con información perfecta pueda sugerir métodos útiles para el estudio de algunos juegos con información parcial.*

Todo esto eran vaguedades y, en efecto, el interés del artículo de Gale y Stewart en el contexto de la teoría de juegos era más que dudoso. Sin embargo, a la larga resultaría ser de gran interés en el contexto de la fundamentación de la matemática. No era el primer juego de estas características que se consideraba en matemáticas. En 1935 Stalisław Mieczysław Mazur había planteado un problema sobre un juego de características similares a los de Gale-Stewart que Banach resolvió poco después (y hoy se conoce como el *juego de Banach-Mazur*).

Para entender el planteamiento de Kuhn, Gale y Stewart, vamos a analizar matemáticamente el juego del tres en raya (en su versión en la que cada jugada es inamovible). Tenemos un tablero 3×3 cuyas casillas podemos numerar así:

1	2	3
4	5	6
7	8	9

En general, consideramos un conjunto X de *jugadas posibles,* que en este caso será $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Llamamos $X^{<\omega}$ al conjunto de todas las sucesiones finitas en X, a cuyos elementos llamaremos *situaciones.* Por ejemplo, la situación $(5, 3, 6, 4, 1)$ corresponde a

$\times$		$+$
$+$	$\times$	$\times$

en la que el jugador I ha marcado $\times$ en la casilla 5, luego el jugador II ha marcado $+$ en la casilla 3, etc.

Dentro del conjunto de situaciones seleccionamos un conjunto $R \subset X^{<\omega}$ de *situaciones legales,* que está determinado (y determina) las reglas del juego.

Por ejemplo, en el tres en raya, $(5, 1, 2, 5)$ no es una situación legal, porque el jugador II no puede jugar en la casilla 5, porque está ya marcada por I. El conjunto R para el tres en raya está formado por las situaciones en las que no se repite ninguna jugada y en las que no hay una situación previa en la que ya se ha formado un tres en raya. Por ejemplo, $(5, 3, 6, 4, 1, 7, 9, 2)$ no es una situación legal, porque en la situación previa $(5, 3, 6, 4, 1, 7, 9)$ el jugador I ya ha hecho tres en raya (en la diagonal $1, 5, 9$) y la partida termina. Esto significa que $(5, 3, 6, 4, 1, 7, 9) \in R$, pero no hay ninguna situación en R que prolongue a ésta.

Una situación legal que no admita prolongaciones legales es una *partida.* Kuhn consideró juegos en los que el conjunto R de situaciones legales es finito, de modo que toda situación legal se prolonga necesariamente hasta una o varias partidas.

En total, un juego J está determinado por unos conjuntos $J = (X, R, V_1, V_2)$, donde X es un conjunto de jugadas no vacío, $R \subset X^{<\omega}$ es un conjunto de situaciones legales que contiene, como mínimo, a la situación vacía $\varnothing$ (la situación al inicio de la partida) y V_1, V_2 son conjuntos disjuntos de partidas, de modo que V_1 es el conjunto de las partidas en las que gana el jugador I y V_2 es el conjunto de las partidas en las que gana el jugador II. Puede haber partidas que no estén en ninguno de los dos conjuntos, que corresponden a empates.

Por ejemplo, en el tres en raya, el conjunto V_1 contiene todas las partidas en las que el jugador I ha conseguido un tres en raya, como $(5, 3, 6, 4, 1, 7, 9)$, y el conjunto V_2 contiene todas las partidas en las que el jugador II ha hecho tres en raya.

Jugar a un juego J consiste en partir de la situación vacía $\varnothing$, y dejar que los dos jugadores I y II vayan haciendo jugadas por turnos. El jugador I es, por definición, el jugador que empieza, y lo hace eligiendo una jugada x_0 tal que la situación (x_0) sea legal. Luego juega II eligiendo una jugada x_1 tal que la situación (x_0, x_1) sea legal. El juego termina cuando un jugador ya no puede hacer ninguna jugada legal, con lo que se ha completado una partida x, en la que gana I, o gana II, o hay empate, según si x está en V_1, en V_2 o no está en ninguno de los dos conjuntos.

La definición de juego de Kuhn era mucho más general, porque admitía un número finito de jugadores y además contemplaba que cada uno de ellos no tuviera información completa sobre la situación del juego (por ejemplo porque cada jugador tenga unas cartas que no muestra a los demás, o porque las jugadas posibles dependen de lo que salga en un dado, etc.). Aquí estamos considerando lo que se llama un juego para dos jugadores con información perfecta.

Uno de los resultados básicos para este tipo de juegos es que están determinados, es decir, o bien el jugador I tiene una estrategia ganadora, es decir, unas instrucciones de juego tales que, si las sigue, gana seguro, haga lo que haga el jugador II, o bien es el jugador II el que tiene dicha estrategia, o bien ambos jugadores tienen estrategias que garantizan que no perderán la partida, de modo que, si uno la aplica, el otro jugador no tiene más opciones que aplicar también la suya y la partida acaba en empate, o bien pierde. En el caso del tres en raya se da la tercera opción: cada jugador tiene una estrategia que garantiza que no va a perder, de modo que, si los dos la aplican, las partidas siempre acaban en tablas.

La situación es más simple si $V_1 \cup V_2$ incluye todas las partidas posibles, es decir, si las reglas del juego no permiten que haya empates. En tal caso, necesariamente uno de los dos jugadores tiene una estrategia ganadora. Es el caso, por ejemplo, del nim.

Podríamos haber formalizado el concepto de estrategia, pero no lo hemos hecho porque nos interesa realmente la variante planteada por Gale y Stewart, en la que las partidas pueden tener longitud infinita. Por simplicidad, vamos a considerar únicamente el caso en el que las reglas del juego no contemplan la posibilidad de partidas finitas, es decir, que nunca se da el caso de que un jugador gane la partida tras un número finito de jugadas, ni de que un jugador se encuentre en una situación en la que ya no haya jugadas legales posibles. Tampoco vamos a admitir la posibilidad de empates.

Concretamente, un juego $J = (X, R, A)$ está determinado por un conjunto X de jugadas posibles, un árbol de reglas $R \subset X^{<\omega}$ con la propiedad de que $\varnothing \in R$ y toda situación $s \in R$ admite al menos una prolongación $s^\frown x \in R$ (donde $s^\frown x$ representa la sucesión que resulta de añadir $x \in X$ a la sucesión $s \in X^{<\omega}$) y un conjunto $A \subset X^\omega$, donde X^ω es el conjunto de todas las sucesiones (infinitas) en X. El conjunto A es el conjunto de las partidas en las que gana el jugador I (de modo que II gana todas las partidas legales que no están en A).

En estos términos, jugar a un juego J consiste en el proceso siguiente:

Empezamos con la situación vacía $\varnothing \in R$. El jugador I elige una jugada $x_0 \in X$ tal que la situación (x_0) sea legal (que existe, por la definición de juego que hemos dado). Entonces el jugador II elige otra jugada x_1 tal que la situación (x_0, x_1) sea legal, y el proceso continúa infinitamente, hasta completar una partida

$$x = (x_0, x_1, x_2, \ldots) \in X^\omega.$$

Si $x \in A$, el jugador I gana el juego, y en caso contrario lo gana II.

Vamos a definir ahora el concepto de estrategia en este contexto, que es el que nos interesa:

Dado un juego $J = (X, R, A)$, una *estrategia* para el jugador I (resp. para el II) es cualquier función $\sigma : E \subset R \longrightarrow X$ que cumpla las propiedades siguientes:

1. $\varnothing \in E$.
2. Si $s \in E$ tiene longitud par (resp. impar), entonces $s^\frown\sigma(s) \in E$.
3. Si $s \in E$ tiene longitud impar (resp. par), entonces, para todo $x \in X$ que cumpla $s^\frown x \in R$, se cumple también $s^\frown x \in E$.

Por ejemplo, para el caso del jugador I, esto significa que si le toca jugar a él y se encuentra con una situación $s \in E$, la estrategia σ le elige una jugada $\sigma(s)$ que cumple que $s^\frown\sigma(s) \in E \subset R$, luego es una jugada legal. Y si es el jugador II el que se encuentra en su turno con una situación $s \in E$ (necesariamente de longitud impar), sea cual sea la jugada legal x que elija, la situación resultante $s^\frown x$ estará en E.

Esto se traduce en que si el jugador I decide aplicar una estrategia σ, todas las jugadas de la partida estarán siempre en E, por lo que nunca se encontrará con que σ no le diga qué debe jugar.

Fijada una estrategia σ (por ejemplo, para el jugador I), una sucesión $y \in X^\omega$ es *legal para* σ si todas las situaciones de la partida:

$$\sigma * y = (x_0, y_0, x_1, y_2, x_2, y_2, \ldots)$$

donde $x_0 = \sigma(\varnothing)$, $x_1 = \sigma(x_0, y_0)$, $x_2 = \sigma(x_0, y_0, x_1, y_1)$, etc. son legales. (Notemos que, por definición de estrategia, las únicas situaciones que podrían ser ilegales son las de longitud par, es decir, las que dependen del jugador II.)

Similarmente, si τ es una estrategia para II, una sucesión $x \in X^\omega$ es *legal para* τ si todas las situaciones de la partida

$$x * \tau \in X^\omega = (x_0, y_1, x_1, y_2, \ldots),$$

$y_1 = \tau(x_0)$, $y_2 = \tau(x_0, y_1, x_1)$, etc. son legales.

Además, si σ es una estrategia para I y τ es una estrategia para II, está definida la partida $\sigma * \tau$ que resulta cuando cada jugador aplica su estrategia.

Una estrategia para I es *ganadora* si para toda sucesión $y \in X^\omega$ que sea legal para σ se cumple que $\sigma * y \in A$. Una estrategia τ para II es *ganadora* si para toda sucesión $x \in X^\omega$ que sea legal para τ se cumple que $x * \tau \notin A$.

Se dice que un juego J está *determinado* si uno de los dos jugadores tiene una estrategia ganadora.

Podría pensarse que, dado que estamos considerando juegos cuyas reglas no contemplan empates, si un jugador no tiene una estrategia ganadora, es decir, si un jugador no puede asegurarse la victoria con ningún criterio de juego, es porque es el otro el que tiene una estrategia ganadora, tal y como sucede necesariamente en los juegos finitos, pero lo primero que demuestran Gale y Stewart es que, para juegos infinitos, esto ya no es así. Basta considerar los juegos infinitos más simples, $J_X(A) = (X, X^{<\omega}, A)$ en los que las jugadas son números naturales y no hay reglas, es decir, todas las jugadas son legales.

Teorema (Gale-Stewart) Hay un conjunto $A \subset \mathbb{N}^\omega$ tal que en el juego $J_\mathbb{N}(A)$ no está determinado.

DEMOSTRACIÓN: Sea $\mathfrak{c} = 2^{\aleph_0}$, el cardinal del continuo, que es también el cardinal de $\mathbb{N}^\omega$. En cambio, el cardinal del conjunto $\mathbb{N}^{<\omega}$ de las situaciones posibles es $\aleph_0$. Toda estrategia $\sigma : S \subset \mathbb{N}^{<\omega} \longrightarrow \mathbb{N}$ puede extenderse a una aplicación $\sigma : \mathbb{N}^{<\omega} \longrightarrow \mathbb{N}$, y de aquí se sigue fácilmente que hay $\mathfrak{c}$ estrategias posibles para cada jugador.

Por otro lado, fijada una estrategia σ para el jugador I, toda sucesión $y \in \mathbb{N}^\omega$ es legal para σ (porque no hay reglas que excluyan ninguna jugada), y el conjunto $[\sigma] = \{\sigma * y \mid y \in \mathbb{N}^\omega\}$ de todas las partidas que se pueden jugar con la estrategia σ tiene cardinal $\mathfrak{c}$ (exactamente $\mathfrak{c}$, porque sucesiones distintas y_1, y_2 dan lugar a partidas distintas $\sigma * y_1 \neq \sigma * y_2$). Igualmente, si τ es una estrategia para el jugador II, el conjunto $[\tau] = \{x * \tau \mid x \in \mathbb{N}^\omega\}$ tiene cardinal $\mathfrak{c}$.

Sea Σ el conjunto formado por todos los conjuntos $[\sigma]$, donde σ es una estrategia para cualquiera de los dos jugadores. Acabamos de razonar que Σ tiene cardinal $\mathfrak{c}$, por lo que podemos numerarlo en la forma $\Sigma = \{P_\alpha\}_{\alpha<\mathfrak{c}}$. Tenemos así una sucesión de $\mathfrak{c}$ subconjuntos de $\mathbb{N}^\omega$, cada uno de los cuales tiene cardinal $\mathfrak{c}$.

Ahora vamos a definir, por recursión transfinita, una sucesión de pares $\{(a_\alpha, b_\alpha)\}_{\alpha<\mathfrak{c}}$. Para ello, suponemos que la sucesión está definida hasta $\{(a_\alpha, b_\alpha)\}_{\alpha<\beta}$, con $\beta < \mathfrak{c}$, y vamos a definir el par (a_β, b_β).

En este punto debemos recordar que $\mathfrak{c}$ es un cardinal, y esto significa que es un ordinal no biyectable con ningún ordinal anterior, es decir, que β tiene cardinal estrictamente menor que $\mathfrak{c}$, por lo que el conjunto

$$C = \{a_\alpha \mid \alpha < \beta\} \cup \{b_\alpha \mid \alpha < \beta\}$$

tiene cardinal estrictamente menor que $\mathfrak{c}$. Como P_β tiene cardinal $\mathfrak{c}$, el conjunto $P_\beta \setminus C$ tiene también cardinal $\mathfrak{c}$, luego en particular podemos elegir en él dos elementos distintos a_β, b_β.

Así tenemos definida la sucesión $\{(a_\alpha, b_\alpha)\}_{\alpha<\mathfrak{c}}$, que tiene dos propiedades fundamentales:

1. $a_\alpha, b_\alpha \in P_\alpha$.
2. Cada a_α y cada b_α es distinto de todos los anteriores, luego de hecho todos ellos son distintos entre sí dos a dos.

En particular, los conjuntos $A = \{a_\alpha \mid \alpha < \mathfrak{c}\}$ y $A' = \{b_\alpha \mid \alpha < \mathfrak{c}\}$ son subconjuntos disjuntos de $\mathbb{N}^\omega$.

Ahora es fácil concluir que el juego $J(A)$ no tiene estrategias ganadoras. En efecto, si σ es cualquier estrategia para el jugador I, existe un $\alpha < \mathfrak{c}$ tal que $[\sigma] = P_\alpha$, y entonces $b_\alpha \in [\sigma] \cap A'$, es decir, es una partida jugada con la estrategia σ en la que gana el jugador II, luego σ no es una estrategia ganadora. Similarmente, si τ es una estrategia para el jugador II, existe un $\alpha < \mathfrak{c}$ tal que $[\tau] = P_\alpha$, y entonces $a_\alpha \in [\tau] \cap A$ es una partida jugada con la estrategia τ en la que gana el jugador I, luego τ tampoco es una estrategia ganadora. ∎

Un juego no determinado es un objeto extraño. Es un juego en el que, por ejemplo, cada estrategia del jugador I tiene una réplica, una posible contraestrategia del jugador II que hace que I termine perdiendo, pero II necesita conocer la estrategia que va a emplear I para determinar la contraestrategia. No hay ninguna contraestrategia que valga para toda estrategia. En cuanto un jugador se compromete a seguir un criterio, el otro siempre puede encontrar la contraestrategia adecuada.

Por otro lado la prueba que hemos visto usa fuertemente el axioma de elección,[154] por lo que Gale y Stewart se plantearon si no sería posible demostrar que los juegos $J_X(A)$ están determinados cuando A no es un conjunto "salvaje", construido con el axioma de elección, sino un conjunto "razonable". Esto los llevó a considerar a X^ω como espacio topológico, esencialmente con la misma topología que Baire consideró en el espacio $\mathcal{N} = \mathbb{N}^\omega$ de las sucesiones de números naturales (véase la sección 24). La distancia entre dos sucesiones se puede definir como

$$d(x, y) = \sum_{n=0}^{\infty} \frac{[x_n, y_n]}{2^{n+2}},$$

donde $[x_n, y_n]$ vale 0 o 1 según si $x_n = y_n$ o $x_n \neq y_n$. Exactamente igual que en el caso de $\mathcal{N}$, esto hace que la bola abierta de centro x y radio $1/2^n$ está formada por las sucesiones y tales que $y|_n = x|_n$, es decir, que tienen los primeros n términos iguales a los de x. De aquí se desprende el hecho siguiente, que el lector puede tomar directamente como definición:

> Un conjunto $A \subset X^\omega$ es *abierto* si cuando $x \in A$, existe un número natural n tal que todas las sucesiones $y \in X^\omega$ que comparten con x los n primeros términos están también en A. Un subconjunto de X^ω es *cerrado* cuando su complementario es abierto.

En estos términos podemos demostrar:

> **Teorema (Gale-Stewart)** Si $A \subset X^\omega$ es un conjunto abierto o cerrado, entonces el juego $J_X(A)$ está determinado.

Demostración: Consideremos en primer lugar el caso en que A es cerrado. Suponemos que II no tiene una estrategia ganadora y vamos a demostrar que I sí que la tiene.

Para cada situación $s = (a_0, \ldots, a_n) \in X^{<\omega}$, podemos considerar el conjunto $A_s \subset X^\omega$ formado por las sucesiones $(x_0, x_1, x_2, \ldots)$ tales que $(a_0, \ldots, a_n, x_0, x_1, x_2, \ldots) \in A$.

[154] Pero esto es engañoso. En ZF se puede demostrar que existe un juego $J_{\omega_1}(A)$ no determinado (véase la página 260).

Dada una situación s de longitud par, es decir, una situación en la que le toca jugar a I, diremos que s *no está perdida para* I si II no tiene una estrategia ganadora para el juego $J_X(A_s)$.

Esto significa que, para cualquier estrategia τ que adopte II en el juego $J_X(A_s)$, existe una contraestrategia $x \in X^\omega$ tal que

$$x * \tau = (x_0, y_0, x_1, y_1, \ldots) \in A_s$$

o, lo que es lo mismo, $(a_0, \ldots, a_n, x_0, y_0, x_1, y_1, \ldots) \in A$. En otras palabras, que si la partida ha llegado a la situación s, el jugador I puede responder a cualquier estrategia que aplique II a partir de ese momento y ganarle la partida en $J_X(A)$. En particular, podemos afirmar que la jugada vacía $s = \varnothing$ no está perdida para I, pues (como $A_s = A$), esto significa que II no tiene una estrategia ganadora para $J_X(A)$, que es lo que estamos suponiendo.

Ahora vamos a probar lo siguiente:

> Si una situación $s = (x_0, \ldots, x_{2n-1})$ de longitud par no está perdida para I, existe una cierta jugada $\sigma(s) \in X$ para I con la propiedad de que, si I juega $x_{2n} = \sigma(s)$, para cualquier jugada $x_{2n+1} \in X$ que haga II, la situación $(x_0, \ldots, x_{2n-1}, x_{2n}, x_{2n+1})$ no está perdida para I.

En efecto, supongamos lo contrario, es decir, que, dada una situación s no perdida para I, para cualquier jugada x_{2n} que haga I, existe una jugada x_{2n+1} que puede hacer II con la que la situación $(x_0, \ldots, x_{2n-1}, x_{2n}, x_{2n+1})$ está perdida para I. Más precisamente, para cada número natural k, si I juega $x_{2n} = k$, existe una jugada $t(k) \in X$ de modo que si II juega $x_{2n+1} = t(k)$ el jugador II tiene una estrategia ganadora τ_k para $J_X(A_{(x_0,\ldots,x_{2n+1})}) = J_X(A_{(x_0,\ldots,x_{2n-1},k,t(k))})$.

Pero entonces es fácil construir una estrategia ganadora para II en el juego $J_X(A_s)$. La estrategia τ con la que II gana seguro es esperar a que I haga su primera jugada k, entonces jugar $t(k)$ y a partir de ahí aplicar la estrategia τ_k a la situación que resulta de eliminar las dos primeras jugadas $(k, t(k))$ en la situación en curso. Más detalladamente, la partida de $J_X(A_s)$ según la estrategia τ es:

$$(k, t(k), a_1, b_1, a_2, b_2, a_3, b_3, \ldots)$$

donde $b_1 = \tau_k(a_1)$, $b_2 = \tau_k(a_1, b_1, a_2)$, $b_3 = \tau_k(a_1, b_1, a_2, b_2, a_3)$, etc. La estrategia ganadora τ_k garantiza que $(a_1, b_1, a_2, b_2, \ldots) \in J_X(A_{(x_0,\ldots,x_{2n-1},k,t(k))})$, luego $(x_0, \ldots, x_{2n-1}, k, t(k), a_1, b_1, a_2, b_2, \ldots) \in A$, luego $(k, t(k), a_1, b_1, a_2, b_2, \ldots) \in A_s$ y así II gana el juego $J_X(A_s)$. Por lo tanto, la situación s está perdida para I, en contra de lo supuesto.

Así pues, si llamamos $E \subset X^{<\omega}$ al conjunto de situaciones no perdidas para I, acabamos de probar que existe una estrategia $\sigma : E \longrightarrow X$ (es decir, que cuando I aplica E, juegue lo que juegue II, se obtiene una nueva situación en E). Vamos a probar que se trata de una estrategia ganadora. Para ello tenemos que ver que, para toda réplica $y \in X^\omega$, se cumple que $\sigma * y \in A$. Supongamos, por el contrario, que

$$\sigma * y = (x_0, y_0, x_1, y_1, x_2, y_2, \ldots) \in X^\omega \setminus A.$$

Por hipótesis A es cerrado, luego su complementario es abierto, luego existe un número natural (que podemos tomar par pasando al siguiente, si fuera impar) digamos $2n$, de modo que todas las sucesiones que empiezan por

$$s = (x_0, y_0, \ldots, x_{2n-1}, y_{2n-1})$$

están en $X^\omega \setminus A$. Pero esto significa que $A_s = X^\omega$, por lo que II tiene trivialmente una estrategia ganadora en el juego $J_X(A_s)$ (gana seguro, sin que importe lo que juegue), luego la situación s está perdida para I, pero eso es imposible porque la estrategia σ proporciona siempre situaciones no perdidas para I.

Esto termina la prueba cuando A es cerrado. Si A es abierto se razona análogamente intercambiando los papeles de I y II. Suponemos que I no tiene una estrategia ganadora y construimos una para II. Para ello consideramos el conjunto E de las situaciones (ahora de longitud impar) no perdidas para II y demostramos que ninguna situación de longitud 1 está perdida, así como que existe una estrategia $\tau : E \longrightarrow X$ para II que resulta ser ganadora por el mismo motivo (porque si existe una réplica x tal que $x * \tau \in A$, podemos usar que A es abierto igual que antes hemos usado que lo era $X^\omega \setminus A$). ∎

La demostración anterior también usa el axioma de elección y, de hecho, el teorema es equivalente al axioma:

Teorema (ZF) Si para todo conjunto X y todo cerrado $A \subset X^\omega$ el juego $J_X(A)$ está determinado, entonces se cumple el axioma de elección.

DEMOSTRACIÓN: Sea E un conjunto formado por conjuntos no vacíos y vamos a demostrar que tiene una función de elección. Para ello llamamos $X = E \cup \bigcup E$, y consideramos el juego $J_X(A)$ en el que $A \subset X^\omega$ está formado por las sucesiones x tales que si $x_0 \in E$, entonces $x_1 \in x_0$. Se trata de un conjunto cerrado (de hecho es abierto y cerrado), pues si $x \in X^\omega \setminus A$, eso significa que $x_0 \in E$ y $x_1 \notin x_0$, luego cualquier sucesión $y \in X^\omega$ que coincida con x en sus dos primeros términos cumple también $y \in X^\omega \setminus A$. Esto prueba que $X^\omega \setminus A$ es abierto.

Por hipótesis, el juego $J_X(A)$ está determinado, pero es imposible que el jugador I tenga una estrategia ganadora: si empieza con una jugada $x_0 \notin E$, ya ha perdido la partida y, si empieza con $x_0 \in E$, entonces II sólo tiene que jugar un $x_1 \in x_0$ y ya ha ganado la partida.

Por lo tanto, II tiene que tener una estrategia ganadora τ, la cual se restringe una función de elección para E, pues cada $x_0 \in E$ es una posible jugada inicial de I, para la que τ nos da una respuesta $\tau(x_0) \in x_0$, luego $x_0 \mapsto \tau(x_0)$ es una función de elección en E. ∎

Un poco más allá, Gale y Stewart demostraron que si A pertenece a la menor álgebra de Boole que contiene a los abiertos de X^ω, entonces el juego $J_X(A)$ está determinado, y terminaron su artículo con varias preguntas abiertas, entre ellas si también están determinados los juegos definidos por conjuntos $\mathbf{\Sigma}^0_2$ y $\mathbf{\Pi}^0_2$ (es decir, intersecciones numerables de abiertos y uniones numerables de cerrados), incluso especularon con la posibilidad de que los conjuntos A para los que el juego $J_X(A)$ estuviera determinado fueran precisamente los conjuntos de Borel (los elementos de la menor álgebra de subconjuntos de X^ω que contiene a los abiertos y que es cerrada para uniones e intersecciones numerables).

En 1954 leyó su tesis en Berkeley Philip Wolfe, quien demostró que, en efecto, cuando A es $\mathbf{\Sigma}^0_2$ o $\mathbf{\Pi}^0_2$, el juego $J_X(A)$ está determinado. Pero no se haría ningún progreso en esta línea durante muchos años.

79 La aritmética de Robinson En el *Undécimo Congreso Internacional de Matemáticos,* celebrado en Cambridge en 1950, Raphael Robinson había presentado una ponencia titulada *Un sistema de axiomas esencialmente indecidible,* del que publicó únicamente un breve resumen en las actas del congreso. Su aportación aparecería desarrollada en **1953** en un artículo firmado conjuntamente por Tarski y Mostowski con el título de *Indecibilidad e indecibilidad esencial en aritmética.*

Robinson consideró la teoría axiomática sobre el lenguaje formal de la aritmética de Peano (cuyos signos no definidos son 0, S, $+$, $\cdot$) que hoy se conoce como la *aritmética de Robinson,* que está determinada por los axiomas siguientes:[155]

Q1 $Sx = Sy \to x = y$,

Q2 $Sx \neq 0$,

Q3 $x \neq 0 \to \bigvee y\, x = Sy$,

Q4 $x + 0 = x$,

Q5 $x + Sy = S(x + y)$,

Q6 $x \cdot 0 = 0$,

Q7 $x \cdot Sy = x \cdot y + x$.

Si el lector los compara con los axiomas de la aritmética de Peano (página 60), verá que los axiomas de Robinson resultan de eliminar a los de la aritmética de Peano el esquema axiomático de inducción y de añadir el axioma Q3, que no es necesario en la aritmética de Peano porque se demuestra trivialmente por inducción. Notemos que, a diferencia de la aritmética de Peano, la aritmética de Robinson admite un número finito de axiomas.

Si el lector se pregunta qué interés puede tener una teoría tan débil, lo cierto es que los resultados que obtuvo Robinson (que eran una simplificación de resultados previos de Tarski y Mostowski, de ahí que los tres firmaran el artículo) son aplicables a una teoría aún más débil. Si llamamos

$$\ulcorner 0 \urcorner \equiv 0, \quad \ulcorner 1 \urcorner \equiv S0, \quad \ulcorner 2 \urcorner \equiv SS0, \quad \ulcorner 3 \urcorner \equiv SSS0, \quad \ldots$$

[155] Tarski, Mostowski y Robinson usan los cuantificadores $\bigwedge$ y $\bigvee$ que usamos aquí.

la teoría R es la determinada por los esquemas axiomáticos siguientes (donde $x \leq y \equiv \bigvee z\, z + x = y$):

R1 $\ulcorner m \urcorner + \ulcorner n \urcorner = \ulcorner m + n \urcorner$,

R2 $\ulcorner m \urcorner \cdot \ulcorner n \urcorner = \ulcorner mn \urcorner$,

R3 $\ulcorner m \urcorner \neq \ulcorner n \urcorner$ (sólo para $m \neq n$),

R4 $x \leq \ulcorner n \urcorner \to x = \ulcorner 0 \urcorner \vee x = \ulcorner 1 \urcorner \vee \cdots \vee x = \ulcorner n \urcorner$,

R5 $x \leq \ulcorner n \urcorner \vee \ulcorner n \urcorner \leq x$.

Por ejemplo, R1 es un esquema que abarca infinitos axiomas, como $\ulcorner 2 \urcorner + \ulcorner 3 \urcorner = \ulcorner 5 \urcorner$, etc. La aclaración en R3 indica que $\ulcorner 3 \urcorner \neq \ulcorner 7 \urcorner$ es un axioma de R, pero $\ulcorner 3 \urcorner \neq \ulcorner 3 \urcorner$ no lo es. Un axioma de tipo R4 es, por ejemplo,

$$x \leq \ulcorner 2 \urcorner \to x = \ulcorner 0 \urcorner \vee x = \ulcorner 1 \urcorner \vee x = \ulcorner 2 \urcorner.$$

Puede comprobarse que todos los axiomas de R son demostrables en Q, por lo que R es una teoría (mucho) más débil que Q. Lo que probó Robinson es que el teorema de Gödel que enunciamos en la sección 50, en virtud del cual en toda teoría aritmética (es decir, que pueda demostrar los axiomas de Peano) son expresables todas las relaciones recursivas y son representables todas las funciones recursivas es válido, más en general, para teorías en las que se puedan demostrar los axiomas de R o, en particular, los de Q.

Esto hace que el primer teorema de incompletitud[156] de Gödel valga, de hecho, para teorías aritméticas recursivas entendiendo "aritméticas" en el sentido más débil de que puedan demostrar los axiomas de R.

En particular, Tarski, Mostowski y Robinson demuestran que toda teoría consistente T en la que se puedan demostrar los axiomas de R (o los de Q) es indecidible, es decir, que no existe ningún algoritmo para determinar si una fórmula dada es o no un teorema de T. El argumento con el que lo demuestran es el que hemos empleado nosotros en la página 138.

Para no repetir argumentos que ya hemos analizado, vamos a aprovechar para demostrar la versión de Rosser del primer teorema de incompletitud:

Primer teorema de incompletitud de Gödel (versión de Rosser) Toda teoría aritmética (en el sentido de que demuestre los axiomas de R) recursiva y consistente es incompleta.

Demostración: Sea T una teoría en las condiciones del enunciado. El hecho de que sea recursiva implica que la relación $\overset{x}{\underset{T}{\vdash}} y$ que se cumple cuando x codifica una demostración de la fórmula codificada por y, es recursiva y, como T es aritmética, es expresable en T por una fórmula $\overset{x}{\underset{\ulcorner T \urcorner}{\vdash}} y$.

También se cumple el lema de autorreferencia (página 106), que nos da la existencia de una sentencia R (la *sentencia de Rosser*) con la propiedad de que en T se demuestra la equivalencia

$$R \leftrightarrow \bigwedge y(\overset{y}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner R \urcorner \to \bigvee x(x \leq y \wedge \overset{x}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner \neg R \urcorner))$$

Así, la fórmula de Rosser afirma que si ella misma admite una demostración de código n, entonces su negación es demostrable con una demostración de código menor.

Vamos a ver que R no es demostrable ni refutable en T. Supongamos en primer lugar que es demostrable, y sea n el código de una demostración de R. Entonces, como se cumple $\overset{n}{\underset{T}{\vdash}} \ulcorner R \urcorner$ y esta relación está expresada en T por la fórmula correspondiente, en T se puede demostrar

$$\overset{\ulcorner n \urcorner}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner R \urcorner.$$

Pero, como R también es demostrable en T, podemos concluir que

$$\bigvee x(x \leq \ulcorner n \urcorner \wedge \overset{x}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner \neg R \urcorner).$$

[156] La prueba del segundo teorema de incompletitud requiere algo más, para que sean válidas las condiciones de Hilbert-Bernays, pero con un argumento específico se puede probar que también vale para Q: la teoría Q no puede demostrar su propia consistencia.

Siempre razonando en T, fijamos un x tal que

$$x \leq \ulcorner n \urcorner \wedge \overset{x}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner \neg R \urcorner.$$

El axioma R4 (que es un teorema de T) nos da que

$$(*) \qquad x = \ulcorner 0 \urcorner \vee x = \ulcorner 1 \urcorner \vee \cdots \vee x = \ulcorner n \urcorner.$$

Como T es consistente y demuestra R, no puede demostrar $\neg R$, luego ninguno de los números naturales $0, 1, \ldots, n$ codifica una demostración de $\neg R$ en T. Como la relación $\overset{x}{\underset{T}{\vdash}} y$ es expresable, en T podemos demostrar

$$\neg \overset{\ulcorner 0 \urcorner}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner \neg R \urcorner \wedge \neg \overset{\ulcorner 1 \urcorner}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner \neg R \urcorner \wedge \cdots \wedge \neg \overset{\ulcorner n \urcorner}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner \neg R \urcorner$$

y esto, junto con $(*)$, implica $\neg \overset{x}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner \neg R \urcorner$, con lo que T es contradictorio.

Concluimos que R no es demostrable en T. Supongamos ahora que $\neg R$ es demostrable en T. Por construcción de R, también podemos demostrar

$$\bigvee y(\overset{y}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner R \urcorner \wedge \bigwedge x(x \leq y \to \neg \overset{x}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner \neg R \urcorner)).$$

Fijamos un y tal que

$$\overset{y}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner R \urcorner \wedge \bigwedge x(x \leq y \to \neg \overset{x}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner \neg R \urcorner).$$

Sea n el código de una demostración de $\neg R$. Entonces en T se demuestra $\overset{\ulcorner n \urcorner}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner \neg R \urcorner$. Por R5 tenemos que $\ulcorner n \urcorner \leq y \vee y \leq \ulcorner n \urcorner$, pero descartamos la primera opción por la elección de y. Así pues, $y \leq \ulcorner n \urcorner$. Por R4 tenemos que

$$y = \ulcorner 0 \urcorner \vee y = \ulcorner 1 \urcorner \vee \cdots \vee y = \ulcorner n \urcorner.$$

Pero como T es consistente y demuestra $\neg R$, no puede demostrar R, luego ningún número $0, 1, \ldots, n$ es el código de una demostración de R, luego en T se demuestra

$$(**) \qquad \neg \overset{\ulcorner 0 \urcorner}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner \neg R \urcorner \wedge \neg \overset{\ulcorner 1 \urcorner}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner \neg R \urcorner \wedge \cdots \wedge \neg \overset{\ulcorner n \urcorner}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner \neg R \urcorner.$$

Esto, junto con $(**)$, implica $\neg \overset{y}{\underset{\ulcorner T \urcorner}{\vdash}} \ulcorner \neg R \urcorner$, luego T es contradictoria. ∎

80 La aritmética recursiva primitiva Un hecho obvio que no se prestaba a discusión entre los interesados en la fundamentación de las matemáticas era en el hecho de que, para fundamentar la matemática existente en términos de una teoría axiomática formal, es necesario estudiar dicha teoría (o toda una familia de teorías candidatas a tomarse como marco de razonamiento) en términos intuitivos informales. Hilbert y los logicistas habían tratado de reducir estos presupuestos intuitivos necesarios a un mínimo finitista poco menos que insignificante, pero las certeras críticas de Poincaré habían puesto en evidencia que pretender que las construcciones lógicas no requerían un uso intuitivo de la aritmética básica era ilusorio, y los trabajos posteriores de Gödel y Gentzen habían mostrado que, para probar resultados metamatemáticos más profundos, lo que procede no es reducir el razonamiento intuitivo a un mínimo, sino determinar el alcance máximo en el que podemos considerar fiables los razonamientos intuitivos.

Algunos matemáticos recelan del razonamiento intuitivo porque, mientras en el caso de un razonamiento formal podemos examinar cuáles son exactamente los axiomas que se presuponen y cuáles son las reglas de inferencia que damos por válidas, parece que razonar intuitivamente significa tener licencia para sacarse cualquier afirmación de la manga en cualquier momento oportuno, de modo que es imposible "fiscalizar" esta forma de razonamiento, lo que redunda en su falta de fiabilidad.

Ahora bien, esto no es así. Sí que es posible "fiscalizar" el razonamiento metamatemático intuitivo, porque el razonamiento metamatemático puede formalizarse, y en muchos casos en teorías mucho más débiles que la teoría axiomática de conjuntos.

Por ejemplo, toda la metamatemática concerniente al estudio de los lenguajes formales en términos puramente sintácticos (no semánticos), es decir, sin hacer referencia a modelos, pueden formalizarse en la Aritmética Recursiva Primitiva de Skolem, lo que significa que esta parte de la metamatemática no requiere más presupuestos intuitivos que los necesarios para reconocer que los axiomas de ARP son verdaderos y que las reglas de inferencia de ARP son lógicamente válidas, es decir, llevan siempre de premisas verdaderas a conclusiones verdaderas.

El lector podría objetar que no sólo es necesario aceptar los axiomas y reglas de inferencia de ARP, sino también *la construcción* de ARP, la cual podría requerir que se acepten otros principios intuitivos no formalizables en ARP, pero no es así, porque sucede que la construcción de ARP puede ser formalizada en ARP (ya que es parte de la metamatemática que no requiere teoría de modelos), por lo que dicha construcción no añade presupuestos intuitivos a los que vienen expresados en sus axiomas y reglas de inferencia.

No hay que confundir esto con que, naturalmente, no es posible demostrar en ARP la consistencia de ARP. Si reconocemos que sus axiomas son verdaderos y que sus reglas de inferencia son válidas, con esto estamos admitiendo ya la consistencia de ARP, pero esto no es formalizable en ARP, aunque casi.

Lo que se puede formalizar en ARP es que la inducción transfinita hasta ω^ω implica la consistencia de ARP, y en ARP se puede demostrar el principio de inducción transfinita hasta ω, y hasta ω^2, y hasta ω^3, etc., y ω^ω no es más que el menor ordinal mayor que todas estas potencias. El hecho de que la inducción transfinita hasta ω, y hasta ω^2, y hasta ω^3, etc. sea verdadera implica que también lo es la inducción transfinita hasta ω^ω y, por consiguiente, la consistencia de ARP, pero esto no es demostrable en ARP porque en ARP no podemos demostrar (ni siquiera formular) que si $\alpha \prec \omega^\omega$, entonces existe un numeral n (es decir, el nombre de un número natural concreto: $0, 1, 2, \ldots$) tal que $\alpha \prec \omega^n$.

En 1941 Curry había mostrado una axiomática alternativa mucho más elemental para ARP en un artículo titulado *Una formalización de la aritmética recursiva,* y en 1945 Reuben Louis Goodstein presentó otra propuesta más simple en *Teoría de funciones en un cálculo de ecuaciones sin axiomas,* que era parte de la tesis doctoral que estaba elaborando en Cambridge bajo la dirección de Wittgenstein y que leería en 1946. Finalmente, en **1954** Goodstein publicó *Formalizaciones sin lógica de la aritmética recursiva,* donde simplificaba aún más su propuesta.

Vamos a detallar el formalismo, los axiomas y las reglas de inferencia de ARP según la propuesta de Goodstein (algo más desarrollada que su presentación, que da algunas cosas por supuestas) porque, según hemos dicho, el contenido intuitivo de dichos axiomas y reglas de inferencia son todo lo que uno necesita aceptar para dar por válida toda la metamatemática intuitiva concerniente a la construcción de teorías axiomáticas formales (sin entrar en consideraciones sintácticas).

Vamos a construir un lenguaje formal a partir de ocho signos,[157] que representaremos por

$$0, \qquad S, \qquad C, \qquad p, \qquad \kappa, \qquad \rho, \qquad x, \qquad =$$

ARP es una teoría axiomática formal, lo cual significa que puede construirse sin hacer referencia en ningún momento al posible significado de sus signos o cadenas de signos, pero aquí estamos interesados justamente en atribuir un significado intuitivo preciso a algunas cadenas construidas con estos signos para constatar que todos los axiomas que vamos a enunciar formalmente son de hecho intuitivamente verdaderos, y que todas las reglas de inferencia que vamos a especificar son intuitivamente válidas (siempre llevan a afirmaciones verdaderas cuando se aplican a afirmaciones verdaderas).

Así, para empezar, estipulamos que el signo 0 nombra al número natural cero y que el signo S nombra a la función sucesor, que a cada número natural n le hace corresponder su sucesor. Llamaremos *numerales* a las cadenas de signos

$$0, \quad S0, \quad SS0, \quad SSS0, \quad SSSS0, \quad \ldots$$

que nombrarán a cada uno de los números naturales. Más precisamente, si n es un número natural, llamaremos N_n a la cadena de signos formada por n signos S seguidos de un 0, de modo que[158] $N_7 \equiv SSSSSSS0$, y convenimos en que cada numeral N_n es el nombre en nuestro lenguaje del número natural n.

[157] El lector puede añadir a la lista los paréntesis "(" y ")" y las comas, aunque técnicamente su uso se puede suprimir.

[158] Usamos el signo metamatemático $\equiv$ (que no es un signo de ARP) para indicar que los dos miembros son la misma cadena de signos.

Si $1 \leq i \leq n$ son números naturales, la cadena de signos $P_k^n \equiv pN_kN_n$ recibe el nombre de *proyección* n-ádica k-ésima. Por ejemplo, $P_2^4 \equiv pSS0SSSS0$ es una proyección, mientras que $P_4^2 \equiv pSSSS0SS0$ no lo es, porque no cumple el requisito de que $k \leq n$.

Convenimos en que el signo c nombra a la función nula, dada por $c(n) = 0$, para todo número natural n, y que las proyecciones P_k^n nombran a las proyecciones p_k^n dadas por $p_k^n(x_1, \ldots, x_n) = x_k$.

Ahora definimos inductivamente una familia de cadenas se signos a las que llamaremos *funtores* (sin relación alguna con los funtores de la teoría de categorías). A cada funtor le asociaremos un número natural al que llamaremos su *rango,* y a los funtores de rango n los llamaremos funtores n-ádicos. A cada funtor n-ádico le asignaremos como significado una función de n argumentos:

- S y C son funtores monádicos (de rango 1), que nombran, como ya hemos establedido, a la función sucesor y a la función nula, respectivamente, y P_k^n es un funtor n-ádico que nombra a la proyección p_k^n.
- Si H es un funtor n-ádico que nombra a la función h y $G_1, \ldots, G_n$ son funtores k-ádicos que nombran a las funciones $g_1, \ldots, g_n$, entonces $\kappa(H, G_1, \ldots, G_n) \equiv \kappa HG_1 \ldots G_n$ es un funtor k-ádico que nombra a la función definida por composición a partir de las funciones h, $g_1, \ldots, g_n$, en el sentido de la página 94.
- Si G es un funtor n-ádico que nombra a la función g y H es un funtor $n+2$-ádico que nombra a la función G, entonces $\rho(G, H) \equiv \rho GH$ es un funtor $n+1$-ádico que nombra a la función definida por recursión a partir de G y H en el sentido de la página 94.

Estas reglas determinan completamente las cadenas de signos que son funtores, en el sentido de que es posible programar un ordenador para que, si le damos una cadena de signos,[159] nos diga si corresponde a un funtor o no y en caso afirmativo nos diga su rango. Es inmediato que los funtores nombran a todas las funciones recursivas primitivas. Más aún, podemos programar un ordenador para que si le damos un funtor n-ádico F y n números naturales, nos calcule el valor que toma la función que nombra F sobre los números naturales dados.

Por ejemplo, repetimos aquí la prueba de que la suma de números naturales es recursiva primitiva, pero indicando ahora el nombre de cada una de las funciones empleadas en la justificación:

$$\begin{array}{ll}
f_1(x) = x & P_1^1 \\
f_2(x, y, z) = z & P_3^3 \\
f_3(x) = x + 1 & S \\
f_4(x, y, z) = f_3(f_2(x, y, z)) = z + 1 & \kappa(S, P_3^3) \\
f_5(x, 0) = f_1(x) = x & \\
f_5(x, y + 1) = f_4(x, y, f_5(x, y)) = f_5(x, y) + 1 & \rho(P_1^1, \kappa(P_1^1, P_3^3))
\end{array}$$

Así pues, el funtor diádico

$$+ \equiv \rho(P_1^1, \kappa(P_1^1, P_3^3)) \equiv \rho P_1^1 \kappa P_1^1 P_3^3 \equiv \rho pS0S0\kappa pS0S0pSSS0SSS0$$

nombra a la suma de números naturales. Del mismo modo podemos calcular un funtor que nombre a cada función recursiva primitiva. Veamos, por ejemplo, el caso del producto:

$$\begin{array}{ll}
f_1(x) = 0 & C \\
f_2(x, y, z) = z & P_3^3 \\
f_3(x, y, z) = x & P_1^3 \\
f_4(x, y) = x + y & + \\
f_5(x, y, z) = f_4(f_2(x, y, z), f_3(x, y, z)) = z + x & \kappa(+, P_3^3, P_1^3) \\
f_5(x, 0) = f_1(x) = 0 & \\
f_5(x, y + 1) = f_4(x, y, f_5(x, y)) = f_5(x, y) + x & \rho(C, \kappa(+, P_3^3, P_1^3))
\end{array}$$

Si llamamos $\cdot \equiv \rho(C, \kappa(+, P_3^3, P_1^3))$, se trata de un funtor diádico que nombra a la función que cumple $x \cdot 0 = 0$ y $x \cdot (y + 1) = x \cdot y + x$, luego es necesariamente el producto usual de números naturales.

[159] Cuando en la definición anterior hemos escrito $\kappa(H, G_1, \ldots, G_n) \equiv \kappa HG_1 \ldots G_n$ y $\rho(G, H) \equiv \rho GH$, con esto indicamos que no hay problema en suprimir los paréntesis. El mero orden de los signos ya determina completamente la estructura del funtor, de modo que los paréntesis sólo hace falta ponerlos para facilitar la lectura. De todos modos, para nuestro objetivo este tecnicismo es irrelevante.

Llamaremos *variables* a las cadenas de signos de la forma $x_n \equiv xN_n$, es decir:

$$x_0 \equiv x0, \qquad x_1 \equiv xS0, \qquad x_2 \equiv xSS0, \qquad x_3 \equiv xSSS0, \qquad \ldots$$

Las variables son las únicas cadenas de signos a las que no les vamos a asociar un significado en concreto, pues las usaremos para hacer referencia a números naturales arbitrarios.

Ahora definimos los *términos* de forma recurrente:

- 0 es un término.
- Las variables son términos.
- Si $t_1, \ldots t_n$ son términos y F es un funtor n-ádico, entonces $F(t_1, \ldots, t_n) \equiv Ft_1 \cdots t_n$ es un término.

Ejemplos:

1. 0 es un término.
2. $1 \equiv S0$ es un término.
3. $2 \equiv S1$ es un término.
4. $x \equiv x_0$, $y \equiv x_1$ son términos.
5. $x^2 \equiv \cdot(x,x)$, $\quad y^2 \equiv \cdot(y,y)$, $\quad xy \equiv \cdot(x,y)$ son términos.
6. $2xy \equiv \cdot(2,xy)$ es un término.
7. $x^2 + 2xy \equiv +(x^2, 2xy)$ es un término.
8. $x^2 + 2xy + y^2 \equiv +(x^2 + 2xy, y^2)$ es un término.

Por ejemplo, la línea 6 dice que, como $\cdot$ es un funtor diádico y ya hemos visto que $2, xy$ son términos, se cumple que $2xy$ (definido como $\cdot(2,xy)$) es también un término. Lo mismo vale para las líneas restantes, excepto para 1 y 4, que se basan en que 0 y las variables son términos por definición.

En general, los términos son cadenas de signos que se construyen a partir de las variables y el 0 aplicando funtores (de modo que cada funtor n-ádico se aplica a n términos).

La presencia de variables hace que no podamos asignar ningún significado específico a un término como $x^2 + 2xy + y^2$, pero, si llamamos *valoraciones* a las funciones v que a cada variable x_i le asignan un número natural $v(x_i)$, podemos definir el *significado* $N(t)[v]$ de un término t respecto de una valoración v como el número natural que se calcula según las reglas siguientes:

- $N(0)[v] = 0$.
- $N(x_i)[v] = v(x_i)$.
- Si $t_1, \ldots t_n$ son términos y F es un funtor n-ádico que nombra a la función f, entonces
$$N(F(t_1, \ldots, t_n))[v] = f(N(t_1)[v], \cdots, N(t_n)[v]).$$

Por ejemplo, si consideramos una valoración v que cumpla $v(x_0) = 3$ y $v(x_1) = 2$, tenemos que

1. $N(0)[v] = 0$.
2. $N(1)[v] = N(S0)[v] = s(N(0)[v]) = s(0) = 1$.
3. $N(2)[v] = N(S1)[v] = s(N(1)[v]) = s(1) = 2$.
4. $N(x)[v] = v(x_0) = 3$, $N(y)[v] = v(x_1) = 2$.
5. $N(x^2)[v] = N(\cdot(x,x))[v] = N(x)[v] \cdot N(x)[v] = 3 \cdot 3 = 9$,
   $N(y^2)[v] = N(\cdot(y,y))[v] = N(y)[v] \cdot N(y)[v] = 2 \cdot 2 = 4$,
   $N(xy)[v] = N(\cdot(x,y))[v] = N(x)[v] \cdot N(y)[v] = 3 \cdot 2 = 6$.
6. $N(2xy)[v] = N(\cdot(2,xy))[v] = N(2)[v] \cdot N(xy)[v] = 2 \cdot 6 = 12$.
7. $N(x^2 + 2xy)[v] = N(+(x^2, 2xy))[v] = N(x^2)[v] + N(2xy)[v] = 9 + 12 = 21$.
8. $N(x^2 + 2xy + y^2)[v] = N(+(x^2 + 2xy, y^2)) = N(x^2 + 2xy)[v] + N(y^2)[v] = 21 + 4 = 25$.

Por ejemplo, en la línea 6, tenemos que $2xy$ se define como $\cdot(2,(xy))$, luego para calcular $N(2xy)[v]$, aplicamos la función que nombra el funtor $\cdot$ (que es el producto de números naturales) a los significados de 2 y xy respecto de v, que ya hemos visto que son 2 y 6, luego $2xy$ significa 12 cuando x significa 3 e y significa 2.

En general, el significado de un término t respecto de una valoración v es el número que resulta de ir calculando las funciones nombradas por los funtores que aparecen en t cuando las variables se interpretan como indica la valoración. Para calcular $N(x^2+2xy+y^2)[v]$ no hacía falta todo el proceso que hemos seguido, sino que basta sustituir $x=3$ e $y=2$ y operar. La definición que hemos dado de significado de un término respecto de una valoración sirve únicamente para que quede claro que éste está unívocamente definido para cualquier término t y cualquier valoración v, pero en la práctica no es más que el resultado de calcular t cuando las variables se interpretan como v.

Similarmente, el lector puede comprobar que $(x+y)^2 \equiv (x+y)\cdot(x+y)$ es un término, y que, respecto de la misma valoración, $N((x+y)^2)[v]=25$.

En particular, $N(t)[v]$ depende únicamente de los valores que asigna v a las variables que realmente aparecen en el término t.

Finalmente, llamaremos *fórmulas* (del lenguaje de ARP) a las cadenas de signos de la forma $t_1=t_2$, donde t_1 y t_2 son términos. Por ejemplo, teniendo en cuenta las definiciones precedentes,

$$(x+y)^2 = x^2+2xy+y^2$$

es una fórmula, como también lo es $x^2=4$.

Diremos que una fórmula es *verdadera* si sus dos miembros significan lo mismo respecto de cualquier valoración y diremos que es *falsa* si sus dos miembros no significan lo mismo respecto de ninguna valoración.

Aquí es importante tener en cuenta que, para determinar si una fórmula es verdadera o falsa, sólo necesitamos considerar valoraciones definidas sobre las variables que aparecen realmente en ella, pues el valor que se asigne a otras variables es irrelevante. Por ejemplo:

- La fórmula $(x+y)^2 = x^2+2xy+y^2$ es verdadera, pues los dos miembros toman el mismo valor cualquiera que sea la valoración que usemos para calcularlos (es decir, cualquiera que sea el valor que toman sus variables).
- La fórmula $x = x+1$ es falsa, porque no es posible dar ningún valor a x que haga que se cumpla la igualdad.
- La fórmula $x^2=4$ no es ni verdadera ni falsa, porque sus dos miembros toman el mismo valor respecto de las valoraciones que cumplen $v(x)=2$, pero no respecto a las demás valoraciones.

Aunque hemos asociado inmediatamente un significado a cada concepto que hemos definido, el lector puede observar que es posible eliminar todo cuanto hemos dicho sobre significados y eso no impide definir las fórmulas del lenguaje de ARP, por lo que la definición de fórmula es puramente formal. Podemos programar a un ordenador para que, si le damos una cadena de signos del lenguaje de ARP, nos determine si se trata o no de una fórmula simplemente analizando su forma, es decir, la disposición de sus signos. Pero además hemos asignado a cada fórmula un significado intuitivo preciso que nos permite clasificar las fórmulas en tres categorías: verdaderas, falsas y ni verdaderas ni falsas.

Con esto estamos en condiciones de formular los axiomas de ARP:

- $C(x_0)=0$
- Si $1 \le k \le n$ son números naturales, la fórmula

  $$P^n_k(x_1,\ldots,x_n) = x_k$$

  es un axioma.
- Si $F \equiv \kappa(H,G_1,\ldots,G_n)$ es un funtor k-ádico, la fórmula siguiente es un axioma:

  $$F(x_1,\ldots,x_k) = H(G_1(x_1,\ldots,x_k),\ldots,G_n(x_1,\ldots,x_k)).$$
- Si $F \equiv \rho(G,H)$ es un funtor $n+1$-ádico, las fórmulas siguientes son axiomas:

  $$F(x_1,\ldots,x_n,0) = G(x_1,\ldots,x_n), \qquad F(x_1,\ldots,x_n,Sx_0) = H(x_1,\ldots,x_n,x_0,F(x_1,\ldots,x_n,x_0)).$$

En resumen: los axiomas de ARP son simplemente las fórmulas que definen sus funtores (excepto el funtor S, que no tiene ningún axioma asociado). Todos ellos son trivialmente verdaderos, por la propia definición que hemos dado del significado de una fórmula.

Por ejemplo, la fórmula $C(x_0) = 0$ es verdadera porque el significado de su miembro izquierdo respecto de cualquier valoración v es $c(v(x_0)) = 0$, que coincide con el significado de su miembro derecho. Igualmente se puede razonar que cualquier otro de los axiomas es verdadero.

Más precisamente: admitir que los axiomas de ARP son verdaderos sólo supone admitir que las funciones recursivas primitivas están bien definidas, es decir, que cada definición de una función recursivamente primitiva (distinta de la función sucesor) define realmente una función que cumple lo que exige su definición.[160]

Veamos ahora las cuatro reglas de inferencia que enuncia Goodstein para la Aritmética Recursiva Primitiva:

$$(S_1) \quad \frac{t_1(x_0) = t_2(x_0)}{t_1(t) = t_2(t)}$$

Aquí hay que entender que t_1, t_2 y t son términos arbitrarios y que $t_1(t)$ y $t_2(t)$ son los términos que resultan de sustituir la variable x_0 por t en t_1 y t_2, respectivamente.

Por ejemplo, un caso particular de esta regla es:

$$\frac{(x+y)^2 = x^2 + 2xy + y^2}{(x+3zx)^2 = x^2 + 2x(3zx) + (3zx)^2}$$

Si admitimos que la fórmula de arriba es verdadera, en el sentido de que se cumple para todo x, y, tenemos que admitir que sigue siéndolo si cambiamos y por $3zx$, o por cualquier otro término que queramos.

En general, si, de algún modo, estamos convencidos de que la igualdad $t_1(x_0) = t_2(x_0)$ se cumple sea cual sea el valor que tomen sus variables (en particular, x_0), podemos asegurar que seguirá cumpliéndose si en lugar de x_0 ponemos concretamente el término[161] t.

Por lo tanto, lo único que expresa la regla S_1 es que ARP no tiene cuantificadores, pero que, en su defecto, hemos adoptado el convenio de que, si los tuviera, $t_1(x_0) = t_2(x_0)$ significaría lo mismo que $\bigwedge x_0\, t_1(x_0) = t_2(x_0)$, y si esto es cierto, también lo es $t_1(t) = t_2(t)$.

$$(S_2) \quad \frac{t_1 = t_2}{t(t_1) = t(t_2)}$$

Aquí t_1, t_2 y $t(x_0)$ son de nuevo términos arbitrarios, y $t(t_1), t(t_2)$ son los términos que resultan de sustituir en t la variable x_0 por t_1 y t_2, respectivamente.

Por ejemplo, un caso particular es

$$\frac{(x+y)^2 = x^2 + 2xy + y^2}{(x+y)^2 + z = (x^2 + 2xy + y^2) + z}$$

donde hemos tomado $t(x_0) = x_0 + z$.

Lo que dice esta regla es que, si estamos seguros de que la igualdad $t_1 = t_2$ se cumple para cualquier valor de las variables, el resultado de sustituir x_0 por t_1 en un término $t(x_0)$ será el mismo que el de sustituir x_0 por t_2.

$$(T) \quad \frac{t_1 = t_2 \qquad t_1 = t_3}{t_2 = t_3}$$

Esta regla no necesita comentario alguno. Las dos últimas reglas son las que dejan constancia en ARP como teoría formal de que el signo $=$ significa "igual".

$$(I_0) \quad \frac{s_1(0) = s_2(0) \qquad s_1(Sx_0) = h(x_0, s_1(x_0)) \qquad s_2(Sx_0) = h(x_0, s_2(x_0))}{s_1(x_0) = s_2(x_0)}$$

Aquí $s_1(x_0), s_2(x_0)$ y $h(x_0, x_1)$ son términos arbitrarios (que pueden tener más variables aparte de las indicadas).

[160] Todo lo que hemos dicho hasta aquí es lo que Goodstein da por supuesto en su artículo de 1954, que en realidad empieza presentando las reglas de inferencia que plantea para ARP.

[161] Técnicamente, fijada una valoración v, se puede razonar que $N(t_i(t))[v] = N(t_i)[w]$, donde w es la valoración que coincide con v salvo por que $w(x_0) = N(t)[v]$, por lo que $t_1(x_0) = t_2(x_0)$ es verdadera si, para toda valoración v, se cumple la igualdad $N(t_1(t))[v] = N(t_2(t))[v]$, lo cual equivale a $N(t_1)[w] = N(t_2)[w]$, lo cual es cierto si la fórmula $t_1 = t_2$ es verdadera, ya que entonces sus miembros deben significar lo mismo respecto de cualquier valoración, en particular respecto de w.

El significado de esta regla es el siguiente: si suponemos que

1. s_1 y s_2 coinciden en $x_0 = 0$ (para todos los valores de las demás variables que aparezcan en estos términos),
2. El valor de $s_1(Sx_0)$ se puede calcular a partir de x_0 y $s_1(x_0)$ mediante un término h,
3. El valor de $s_2(Sx_0)$ se puede calcular a partir de x_0 y $s_2(x_0)$ mediante el mismo término h,

entonces s_1 y s_2 coinciden para todo valor de x_0.

Esto es un caso particular del principio de inducción. Fijados unos valores arbitrarios para el resto de las variables, tenemos que $s_1(0) = s_2(0)$ y, supuesto que $s_1(x_0) = s_2(x_0)$, entonces

$$s_1(Sx_0) = h(x_0, s_1(x_0)) = h(x_0, s_2(x_0)) = s_2(Sx_0),$$

luego por inducción la igualdad vale para todo x_0. Decimos que es un caso particular del principio de inducción porque sólo estamos afirmando que éste se puede aplicar para justificar que todos los números naturales tienen propiedades del tipo $s_1(x_0) = s_2(x_0)$, que son una familia muy restringida de propiedades posibles (ya que están definidas por funciones recursivas primitivas, luego son propiedades que, para cada valor concreto de las variables, se pueden calcular en la práctica).

Y no hay más. Si el lector admite que los axiomas de ARP (que no son más que las definiciones de las funciones recursivas primitivas) son verdaderos cuando se interpretan intuitivamente como hemos convenido, y que estas cuatro reglas de inferencia de ARP (que no son más que el convenio de que las variables representan números arbitrarios, las propiedades elementales de la igualdad y un caso muy particular del principio de inducción) son lógicamente válidas (es decir, que llevan siempre de fórmulas intuitivamente verdaderas a fórmulas intuitivamente verdaderas), entonces tiene que aceptar que todos los teoremas de ARP —que, por definición, son las fórmulas que se pueden deducir de los axiomas sin más que aplicar estas reglas de inferencia— son intuitivamente verdaderos.

Pero sucede que, para cualquier afirmación metamatemática sobre teorías axiomáticas formales que no involucre modelos, incluyendo toda la construcción de ARP como teoría formal (es decir, sin hablar del significado de sus fórmulas) puede expresarse como un teorema de ARP, lo cual reduce los presupuestos intuitivos de esta parte de la metamatemática a lo que expresan los axiomas y las reglas de inferencia de ARP.

En este punto, sin duda la pregunta que se formulará el lector es cómo va a ser posible formalizar la metamatemática en una teoría cuyas fórmulas sólo pueden expresar igualdades entre funciones recursivas primitivas, sin signos lógicos de ningún tipo salvo los "para todo" implícitos en el convenio por el que las fórmulas verdaderas deben cumplirse para todos los valores posibles de las variables.

La respuesta está en que ARP es bastante más potente de lo que parece. Recordemos que el artículo de Goodstein se titulaba *Formalizaciones sin lógica de la aritmética recursiva,* porque su aportación fue precisamente mostrar que era posible axiomatizarla *sin lógica,* porque la lógica puede ser definida a partir de la aritmética.

En efecto, consideremos la función

$$f(x,y) = \begin{cases} 0 & \text{si } x = y, \\ 1 & \text{si } x \neq y, \end{cases}$$

que claramente se puede calcular en la práctica, y no es difícil probar que cumple la definición de función recursiva primitiva. Consecuentemente, podemos referirnos a ella mediante un funtor F del lenguaje de ARP que podríamos escribir explícitamente.

Ahora, para cada fórmula $\alpha \equiv t_1 = t_2$ del lenguaje de ARP, llamamos

$$t_\alpha \equiv F(t_1, t_2),$$

que es un término cuyo significado respecto de una valoración v es

$$N(t_\alpha)[v] = f(N(t_1)[v], N(t_2)[v]) = \begin{cases} 0 & \text{si } N(t_1)[v] = N(t_2)[v], \\ 1 & \text{si } N(t_1)[v] \neq N(t_2)[v] \end{cases}.$$

Pero, en estos términos, la fórmula α es verdadera si y sólo si $N(t_1)[v] = N(t_2)[v]$ para toda valoración v, lo cual equivale a que $N(t_\alpha)[v] = 0$ para toda valoración v, lo cual equivale a que la fórmula $t_\alpha = 0$ sea verdadera.

Y el núcleo del artículo de Goodstein consiste en demostrar que esto puede demostrarse en ARP, es decir, que las reglas de inferencia siguientes son demostrables en ARP:

$$\frac{\alpha}{t_\alpha = 0} \qquad \frac{t_\alpha = 0}{\alpha}$$

Más precisamente, si en ARP se puede demostrar α, la demostración se puede prolongar para demostrar $t_\alpha = 0$, y viceversa. Esto nos permite definir

$$\neg\alpha \equiv F(t_\alpha, 1) = 0,$$

de modo que α es verdadera si y sólo si $t_\alpha = 0$ es verdadera, si y sólo si $F(t_\alpha, 1) = 0$ es falsa, es decir, si y sólo si $\neg\alpha$ es falsa.

A su vez, podemos definir

$$\alpha \vee \beta \equiv t_\alpha \cdot t_\beta = 0, \qquad \alpha \wedge \beta \equiv t_\alpha + t_\beta = 0, \qquad \alpha \to \beta \equiv \neg\alpha \vee \beta, \qquad \alpha \leftrightarrow \beta \equiv t_\alpha = t_\beta,$$

y en ARP se pueden demostrar todos los teoremas del cálculo proposicional, así como los axiomas de Peano:

1. $Sx \neq 0$,
2. $Sx = Sy \to x = y$,
3. $x + 0 = x$,
4. $x + Sy = S(x + y)$,
5. $x \cdot 0 = 0$,
6. $x \cdot Sy = x \cdot y + x$.

El principio de inducción no se puede formular como un axioma porque no tenemos cuantificadores, pero se puede demostrar la regla de inferencia siguiente:

$$(I) \qquad \frac{\alpha(0) \qquad \alpha(x) \to \alpha(Sx)}{\alpha(x)}$$

esto significa que si podemos demostrar $\alpha(0)$ y $\alpha(x) \to \alpha(Sx)$, la demostración se puede prolongar hasta una demostración de $\alpha(x)$.

Aun así, conviene tener presente que esto NO es el principio de inducción en toda su generalidad, pues sólo es aplicable a propiedades expresables mediante fórmulas del lenguaje de ARP, que estamos viendo que son más de las que se podría haber pensado, pero siguen siendo propiedades que se pueden comprobar en la práctica para números naturales concretos dados.

Más aún, Goodstein demostró que en ARP se pueden definir las fórmulas

$$\bigwedge u \le x\, \alpha(x_1, \dots x_n, u), \qquad \bigvee u \le x\, \alpha(x_1, \dots, x_n, u),$$

cuyo significado es el que sugiere la notación, es decir, que la primera es verdadera si la fórmula $\alpha(x_1, \dots, x_n, u)$ se cumple cuando damos a u todos los valores posibles menores o iguales que x, y la segunda cuando $\alpha(x_1, \dots, x_n, u)$ se cumple para algún valor de $u \le x$.

Esto se expresa diciendo que ARP tiene cuantificadores acotados. La clave está en que una fórmula con cuantificadores acotados siempre puede comprobarse si se cumple o no para unos valores concretos de sus variables, mientras que si tiene cuantificadores no acotados esto ya no es necesariamente cierto.

Pero conviene tener presente que no estamos añadiendo signos lógicos al lenguaje de ARP. Una fórmula de ARP sigue siendo una mera igualdad de términos aritméticos. Lo que sucede es que una fórmula del estilo de

$$x \mid y \equiv \bigvee u \le y\, y = x \cdot u,$$

que expresa que x es un divisor de y, puede expresarse en el lenguaje de ARP sustituyendo el cuantificador acotado por su definición (que no la hemos dado aquí porque es técnica, pero que es de la misma naturaleza que las definiciones que hemos dado de los conectores lógicos).

Con esto ya resulta plausible (y, de hecho, es cierto) que en ARP puede formalizarse toda la aritmética elemental y la construcción de cualquier teoría axiomática recursiva, incluida la propia ARP. Y por ello podemos afirmar que los presupuestos inductivos de esta parte de la metamatemática no son más que los que expresan los axiomas y las reglas de inferencia de ARP. Por ejemplo, la prueba del teorema demostrado en el apartado siguiente se puede formalizar en ARP.

81 El teorema de Löb Martin Hugo Löb había huido de Alemania con 18 años, poco antes del inicio de la Segunda Guerra Mundial. Tras la guerra estudió matemáticas en Londres y en 1953 se doctoró bajo la dirección de Goodstein. En **1955** publicó su artículo *Solución a un problema de Leon Henkin,* en el que, como su título indica, resolvía un curioso problema que Henkin había planteado en 1952.

El problema era el siguiente: Gödel había demostrado que si una sentencia G en una teoría axiomática aritmética recursiva consistente T cumple

$$\underset{T}{\vdash}(G \leftrightarrow \neg \underset{\ulcorner T \urcorner}{\vdash} \ulcorner G \urcorner),$$

es decir, si afirma que no puede ser demostrada, entonces, en efecto, G no puede ser demostrada. Pero igualmente se puede construir una sentencia H que cumpla

$$\underset{T}{\vdash}(H \leftrightarrow \underset{\ulcorner T \urcorner}{\vdash} \ulcorner H \urcorner),$$

es decir, que equivalga a que ella misma puede ser demostrada. Estas sentencias se llaman *sentencias de Henkin* y, en principio, no parece haber ningún problema con que H sea verdadera (y demostrable) ni con que sea falsa (y no demostrable). Lo que Henkin había preguntado es si las sentencias de Henkin son siempre verdaderas, siempre falsas, o si se pueden dar los dos casos, según la sentencia considerada. Löb demostró que siempre son verdaderas. Más aún:

> **Teorema de Löb** Si T es una teoría aritmética recursiva y H es una sentencia de su lenguaje formal tal que
>
> $$\underset{T}{\vdash}(\underset{\ulcorner T \urcorner}{\vdash} \ulcorner H \urcorner \to H),$$
>
> entonces $\underset{T}{\vdash} H$.

Vamos a dar una prueba que no es exactamente la que dio Henkin, sino que se basa en el segundo teorema de incompletitud de Gödel:

Demostración: Podemos suponer que T es consistente, porque si no, H es trivialmente demostrable en T. Llamamos T^* a la teoría que resulta de añadir $\neg H$ a los axiomas de T. Suponemos, por reducción al absurdo, que H no es demostrable en T. Entonces T^* es consistente pues si en T^* se pudiera probar una contradicción, en T se podría demostrar que $\neg H$ implica una contradicción, y eso sería una demostración de H por reducción al absurdo. Vamos a formalizar este argumento.

Observemos que si en T^* se puede demostrar una contradicción, como $0 \neq 0$, entonces en T se puede demostrar que $\neg H \to 0 \neq 0$ (pues sirve la misma demostración, considerando en un caso $\neg H$ como axioma y en el otro como hipótesis para probar la implicación). Así pues:

$$\text{si} \quad \underset{T^*}{\vdash} 0 \neq 0 \quad \text{entonces} \quad \underset{T}{\vdash}(\neg H \to 0 \neq 0).$$

Esto es un hecho elemental que se deduce inmediatamente de la definición de deducción, luego puede formalizarse en cualquier teoría aritmética, como T. La formalicación es

$$(*) \qquad \underset{T}{\vdash}(\underset{\ulcorner T^* \urcorner}{\vdash} \ulcorner 0 \neq 0 \urcorner \to \underset{\ulcorner T \urcorner}{\vdash}(\neg \ulcorner H \urcorner \to \ulcorner 0 \neq 0 \urcorner)).$$

Por otro lado, es inmediato que $\underset{T}{\vdash}(\neg H \to 0 \neq 0) \to H)$ (si suponiendo $\neg H$ se llega a una contradicción, entonces se cumple H). Por la primera condición de Hilbert-Bernays (página 148):

$$\underset{T}{\vdash} \underset{\ulcorner T \urcorner}{\vdash}((\neg \ulcorner H \urcorner \to \ulcorner 0 \neq 0 \urcorner) \to \ulcorner H \urcorner)$$

y, por la tercera:

$$\underset{T}{\vdash} \underset{\ulcorner T \urcorner}{\vdash}(\neg \ulcorner H \urcorner \to \ulcorner 0 \neq 0 \urcorner) \to \underset{\ulcorner T \urcorner}{\vdash} \ulcorner H \urcorner).$$

Combinando esto con $(*)$):

$$\underset{T}{\vdash}(\underset{\ulcorner T^*\urcorner}{\vdash}\ulcorner 0\neq 0\urcorner\to\underset{\ulcorner T^*\urcorner}{\vdash}\ulcorner H\urcorner),$$

y negando la implicación

$$\underset{T}{\vdash}(\neg\underset{\ulcorner T^*\urcorner}{\vdash}\ulcorner H\urcorner\to\neg\underset{\ulcorner T^*\urcorner}{\vdash}\ulcorner 0\neq 0\urcorner),$$

pero esto es lo mismo que

$$\underset{T}{\vdash}(\neg\underset{\ulcorner T^*\urcorner}{\vdash}\ulcorner H\urcorner\to \mathrm{Consis}\ulcorner T^*\urcorner).$$

Esto se puede probar en T, luego también en T^*, pero, por el segundo teorema de incompletitud, como T^* es consistente, en T^* no es posible demostrar $\mathrm{Consis}(\ulcorner T^*\urcorner)$, luego en T^* no es posible demostrar $\neg\underset{\ulcorner T^*\urcorner}{\vdash}\ulcorner H\urcorner$, luego en T no es posible demostrar

$$\neg H\to\neg\underset{\ulcorner T^*\urcorner}{\vdash}\ulcorner H\urcorner$$

(pues si esto se pudiera demostrar en T, al tomar $\neg H$ como axioma, en T^*, podríamos demostrar la consecuencia de la implicación precedente), y, negando la implicación, esto equivale a que en T no se puede demostrar

$$\underset{\ulcorner T^*\urcorner}{\vdash}\ulcorner H\urcorner\to H,$$

cuando estamos suponiendo lo contrario. ∎

82 La teoría de conjuntos de Morse-Kelley Como ya habíamos señalado, la monografía de Gödel sobre la consistencia del axioma de elección y la hipótesis del continuo generalizada había mostrado a los matemáticos que no hacían falta grandes tecnicismos y sutilezas lógicas para presentar un fundamento axiomático riguroso de cualquier teoría matemática. La primera prueba tangible de esta nueva actitud hacia la axiomática fue el libro *Topología general,* de John Leroy Kelley, publicado en **1955**. En el prólogo se lee:

> *Por otro lado, como es un libro de texto, la exposición en los primeros capítulos avanza a un ritmo bastante lento. Por la misma razón, hay un capítulo preliminar que no forma parte de la exposición sistemática y que cubre aquellos temas que, según he notado, son nuevos para muchos estudiantes y que son requisitos para el cuerpo principal del trabajo. Los resultados más importantes de este capítulo son teoremas de teoría de conjuntos, cuya exposición sistemática se presenta en el apéndice. Este apéndice es completamente independiente del resto del libro, pero con esta excepción, cada parte del libro presupone todo lo desarrollado en las partes anteriores.*

Así, Kelley incluye en su libro un Capítulo 0 de preliminares en el que presenta una teoría ingenua de conjuntos, como hacían ya muchos otros libros de la época, pero incluye también un apéndice en el que demuestra a partir de un sistema de axiomas los resultados conjuntistas básicos y define con rigor los ordinales y los cardinales. En dicho apéndice se lee:

> *El sistema de axiomas adoptado es una variante de los sistemas de Skolem y de A. P. Morse, y se inspira en gran medida en el sistema de Hilbert-Bernays-von Neumann, formulado por Gödel. La formulación empleada aquí está diseñada para proporcionar una base matemática rápida y natural, libre de las paradojas más obvias. Por esta razón, se abandona un sistema axiomático finito y el desarrollo se basa en ocho axiomas y un esquema axiomático (es decir, todos los enunciados de una forma prescrita se aceptan como axiomas).*

A.P. Morse es Anthony Perry Morse, que trabajaba junto a Kelley en la Universidad de Berkeley.

Cuando habla de "abandonar un sistema axiomático finito" se refiere a que, para ahorrarse el trabajo tedioso de demostrar el esquema teoremático de comprensión a partir de los axiomas de formación de clases de Gödel, Kelley decidió tomar este esquema como esquema axiomático y, ya puestos a simplificar, eliminó la condición de que los cuantificadores de las fórmulas estuvieran restringidos a conjuntos. Su esquema axiomático de comprensión (que él llama de clasificación, o de formación de clases), enunciado en términos menos farragosos que los que él emplea, queda así:

> Si $\phi(u)$ es una fórmula (con posibles parámetros) del lenguaje de la teoría de conjuntos, la fórmula siguiente es un axioma:
>
> $$\bigvee Y\bigwedge u(u\in Y\leftrightarrow\phi(u)).$$

Kelley introduce la notación $\{x \mid \alpha(x)\}$ y explica que este esquema axiomático afirma que, para cualquier fórmula $\phi(x)$, podemos afirmar que

$$u \in \{x \mid \alpha(x)\} \text{ si y sólo si } u \text{ es un conjunto y } \alpha(u).$$

Y a este respecto, con una curiosa falta de confianza en sus propios axiomas, comenta:

> *Este esquema axiomático es precisamente la construcción intuitiva habitual de clases, excepto por el requisito 'u es un conjunto'. Este requisito es evidentemente antinatural e intuitivamente bastante indeseable. Sin embargo, sin él, se puede construir una contradicción basándose simplemente en el axioma de extensionalidad. Esta complicación, que requiere bastante trabajo técnico para probar la existencia de conjuntos, es simplemente el precio que hay que pagar para evitar inconsistencias obvias. Es muy posible que persistan inconsistencias menos obvias.*

Por lo demás, los otros ocho axiomas son esencialmente los mismos que los de NBG distintos de los axiomas de formación de clases.[162] Así pues, la teoría de Kelley es la misma[163] que la que Wang había mencionado en su artículo de 1949 y a la que había dado el nombre de NQ (por von Neumann-Quine). Afortunadamente, para entonces Quine y sus discípulos habían arrebatado a Russell el título de "filósofo famoso metido en matemáticas al que menos atención prestaban los matemáticos", y nadie recordó que hubiera habido alguien que alguna vez hubiera llamado NQ a esa teoría, que acabó conociéndose como *teoría de conjuntos de Morse-Kelley* (MK), pues ellos fueron los primeros que hicieron algo de provecho con ella, más allá de decir que "parecía interesante".

Según hemos visto, Mostowski había demostrado que en MK puede demostrarse Consis($\ulcorner$ZFC$\urcorner$) o, equivalentemente Consis($\ulcorner$NBG$\urcorner$), por lo que la consistencia de MK no puede demostrarse ni siquiera suponiendo que ZFC o NBG son consistentes.

Añadimos ahora un hecho adicional: razonamos en ZFC más el supuesto de que existe un cardinal fuertemente inaccesible κ. En la sección 41 hemos visto que Zermelo había demostrado que V_κ es un modelo de ZFC. Las mismas ideas que hemos empleado en la sección 75 para construir un modelo de NBG a partir de uno de ZFC permiten probar que el conjunto $\mathcal{D}V_\kappa$ de las partes definibles de V_κ (véase la página 153) es un modelo de NBG, mientras que $\mathcal{P}V_\kappa$ es un modelo de MK. Por lo tanto, si llamamos FI a la sentencia que afirma la existencia de un cardinal fuertemente inaccesible, en ZFC se pueden probar las implicaciones

$$\text{Consis}(\ulcorner\text{ZFC} + \text{FI}\urcorner) \to \text{Consis}(\ulcorner\text{MK}\urcorner) \to \text{Consis}(\ulcorner\text{NBG}\urcorner) \leftrightarrow \text{Consis}(\ulcorner\text{ZFC}\urcorner).$$

La topología conjuntista se había desarrollado mucho desde los tiempos de Hausdorff. Por ejemplo, en 1951 el canadiense Clifford Hugh Dowker se había planteado si todo espacio topológico normal es numerablemente paracompacto. No necesitamos aquí saber qué son estos conceptos, sino que nos bastará saber que los topólogos llamaban *espacios de Dowker* a los espacios topológicos normales no numerablemente paracompactos, de modo que la conjetura de Dowker era que no existen espacios de Dowker. En 1949 se había doctorado bajo la dirección de Moore una joven de 25 años llamada Mary Ellen Estill, que ahora era conocida como Mary Eller Rudin, porque en 1953 se había casado con el también matemático Walter Rudin.[164] En **1955** Mary Ellen Rudin observó que una recta de Suslin sería un ejemplo de espacio de Dowker (si existieran las rectas de Suslin), lo que suscitó un cierto interés por el problema de Suslin. No obstante, la conjetura al respecto, conocida como la *Hipótesis de Suslin,* era que no existen rectas de Suslin.

83 La teoría de conjuntos de Bourbaki Tras la publicación del Fascículo de resultados de Teoría de Conjuntos en 1939, durante la Segunda Guerra Mundial Bourbaki publicó únicamente los capítulos 1–4 de la *Topología general* (los dos primeros en 1940 y los dos últimos en 1942) y los capítulos 1–3 del *Álgebra* (también en 1942).

La publicación no se reanudó hasta 1947 con los capítulos 5–8 de la *Topología general,* a los que siguió en 1948 el capítulo 9 y luego los capítulos 4–5 del *Álgebra.* Para entonces se habían incorporado al grupo matemáticos como Roger Godement, Pierre Samuel, Jacques Dixmier y Jean-Pierre Serre. En 1949 se publicaron los capítulos 1–7 del libro de *Funciones de una variable real.*

[162] Salvo que enuncia el axioma de partes diciendo que si x es un conjunto existe un conjunto $\mathcal{P}x$ que contiene a todas las subclases de x, de donde deduce que todas las subclases de x son conjuntos, luego deduce que si x es un conjunto también lo es $\{x\}$ porque $\{x\} \subset \mathcal{P}x$ y esto le permite sustituir el axioma del par por el axioma que afirma que si x, y son conjuntos, también lo es $x \cup y$.

[163] No exactamente la misma, porque, por alguna razón difícil de imaginar, Wang no había incluido en NQ ni el axioma de regularidad ni el de elección (tal vez porque el de regularidad no lo entendía y el de elección volvía contradictoria a NF y no quería arriesgarse a que le pasara lo mismo).

[164] De familia judía, en 1938, cuando tenía 17 años, su familia huyó de Viena a Francia tras la anexión de Austria a la Alemania Nazi, y luego en 1940, huyeron de Francia a Gran Bretaña cuando Hitler ocupó Francia. Rudin sirvió en el ejército británico durante la guerra y luego emigró a los Estados Unidos.

En 1951 se publicó el capítulo 10 de la *Topología general* y en 1952 los capítulos 6–7 de *Álgebra* y los capítulos 1–4 del libro de *Integración.* Por esa época se habían incorporado Armand Borel, Eilenberg, Jean-Louis Koszul y Laurent Schwartz. En 1953 se publicaron los capítulos 1–5 del libro sobre *Espacios vectoriales topológicos.*

En 1948 Bourbaki publicó un artículo titulado *La arquitectura de las matemáticas* en el que explicaba las directrices que guiaban la elaboración de sus *Elementos de matemática,* el principal de los cuales era lo que llamaba *el método axiomático,* pero esto hay que entenderlo bien, pues no se refería a razonar en el marco de una teoría axiomática (eso era secundario), sino a axiomatizar las distintas partes de la matemática para unificarlas:

> *Para ilustrar con un ejemplo el procedimiento que acabamos de esbozar, tomaremos una de las teorías axiomáticas más antiguas (y también una de las más sencillas), a saber, la de los "grupos abstractos". Consideremos, por ejemplo, las tres operaciones siguientes:*
>
> *1. la suma de números reales, cuya suma (positiva, negativa o cero) se define de la manera habitual;*
>
> *2. la multiplicación de enteros módulo un número primo p (donde los elementos considerados son los números enteros* $1, 2, \dots p-1$*) y el "producto" de dos de estos números se define, por convenio, como el resto de la división de su producto habitual entre p;*
>
> *3. la "composición" de desplazamientos en el espacio euclidiano tridimensional, definiéndose la "resultante" (o "producto") de dos desplazamientos S, T (tomados en este orden) como el desplazamiento obtenido al realizar primero el desplazamiento T y luego el desplazamiento S.*
>
> *En cada una de estas tres teorías, se hace corresponder, mediante un procedimiento definido para cada teoría, a dos elementos x, y (tomados en ese orden) del conjunto considerado (en el primer caso, el conjunto de los números reales, en el segundo, el conjunto de los números* $1, 2, \dots, p-1$*, en el tercero, el conjunto de todos los desplazamientos) un tercer elemento bien determinado; acordaremos designar este tercer elemento en los tres casos por* $x\tau y$ *(esto será la suma de x e y si x e y son números reales, su producto "módulo p" si son enteros* $\leq p-1$*, su resultante si son desplazamientos). Si ahora examinamos las diversas propiedades de esta "operación" en cada una de las tres teorías, descubrimos un notable paralelismo; pero, en cada una de las teorías por separado, las propiedades están interconectadas, y un análisis de sus conexiones lógicas nos lleva a seleccionar un pequeño número de ellas que son independientes (es decir, ninguna de ellas es una consecuencia lógica de todas las demás).*

Y a continuación Bourbaki presenta las tres propiedades (a), (b), (c) que definen el concepto de grupo y muestra cómo, razonando a partir de ellas, se pueden obtener resultados aplicables a los tres casos.

> *Aunque sólo fuera para evitar repeticiones molestas, se ve fácilmente que sería conveniente desarrollar de una vez por todas las consecuencias lógicas de las tres propiedades (a), (b), (c). Por conveniencia lingüística, es deseable, por supuesto, adoptar una terminología común para los tres conjuntos. Se dice que un conjunto en el que se ha definido una operación* $x\tau y$ *con las tres propiedades (a), (b), (c) está provisto de una estructura de grupo (o, brevemente, que es un grupo); las propiedades (a), (b), (c) se denominan axiomas* de las estructuras de grupo, y el desarrollo de sus consecuencias constituye el establecimiento de la teoría axiomática de grupos.*
>
> ** No hace falta decir que ya no hay conexión alguna entre esta interpretación de la palabra "axioma" y su significado tradicional de "verdad evidente"* [ni tampoco con la de axioma de una teoría axiomática formal, más allá del hecho de que, naturalmente, es posible tomar los axiomas de la definición de grupo y formar a partir de ellos una teoría axiomática formal independiente de la teoría de conjuntos, pero no es eso lo que hace Bourbaki].

Bourbaki aplicó este "método axiomático" hasta las últimas consecuencias, partiendo de estructuras tan generales como fuera necesario para abarcar todos los casos particulares que iba a considerar más adelante, y demostrando en el caso general todo lo que podía valer, de ese modo, para todos los casos particulares.

Por ejemplo, en el capítulo 2 de la *Topología general* se define el concepto de *estructura uniforme,* que "axiomatiza" las nociones de continuidad uniforme y de convergencia uniforme, en el seno de la cual se puede definir el concepto de *filtro de Cauchy,* (que es una generalización del de *sucesión de Cauchy*) y con este concepto de filtro de Cauchy define el concepto de compleción de un espacio uniforme. Luego, tras haber usado estos conceptos para estudiar los grupos topológicos en el capítulo 3, Bourbaki considera que ya es el momento de pasar al capítulo 4 (*Los números reales*), donde define $\mathbb{R}$ como la compleción del grupo topológico de los números

racionales, al que posteriormente se le dota de estructura de cuerpo ordenado, y sólo en el capítulo 9 (*Uso de los números reales en la topología general*) es cuando se introducen los espacios métricos, cuyas propiedades se deducen principalmente de las propiedades generales de las estructuras uniformes. Y todo esto forma parte del libro III, previo al libro IV (el de *Funciones de una variable real*), en el que se introducen las derivadas, la integral de Riemann-Stieltjes, las funciones elementales, etc.

Este orden es justo el opuesto al que siguen los libros de análisis o de topología usuales, que empiezan construyendo $\mathbb{R}$ y estudiando el análisis de las funciones de una variable real, luego se pasa a las funciones de varias variables, y paralelamente se van introduciendo los conceptos de espacio métrico en primer lugar y posteriormente el de espacio topológico (y más tarde aún el de espacio uniforme), de modo que $\mathbb{R}$ y $\mathbb{R}^n$ sirven como ejemplos motivadores para estudiar los espacios métricos en general, y éstos para estudiar los espacios topológicos, y sólo en última instancia se aprecia el interés de axiomatizar el concepto de "uniformidad".

A esta "contradirección" tan poco didáctica había que añadir su estilo enciclopédico, por el que los contenidos se exponen en una fría sucesión de "definición-teorema-corolario" sin ejemplos, sin figuras, sin gráficas, sin motivaciones, sin aplicaciones a la física ni a nada. Esto suscitó muchas críticas. Por poner una de las más moderadas,[165] citamos a Gustave Choquet:

> *La mayoría de los matemáticos franceses de mi generación adquirieron gran parte de su formación matemática de Bourbaki. Bourbaki influyó en su estilo y su obra, transmitiendo algunas de sus cualidades y defectos. ¿Cuáles eran estos defectos? Parece que cualquier grupo que trabaje aislado durante mucho tiempo está condenado al dogmatismo. Creo que esta es la principal crítica a Bourbaki: las definiciones y teoremas básicos se presentan sin justificación ni explicación heurística alguna. Tienen la desecación y la escasez de huesos cuya carne, a pesar de ser deliciosa, se ha echado a los ejercicios. El lector que no los hace todos termina sólo con una caricatura de la actividad matemática.*

Asi, en algunos círculos "bourbakista" haya sido considerado un término despectivo para describir las matemáticas expuestas de forma innecesariamente fría, abstracta e inmotivada. Pero, al margen de su idiosincrasia, los *Elementos de matemática* se convertirían pronto en una referencia para la matemática en general en cuanto al nivel de rigor en las presentaciones, hasta el punto de que prácticamente todo libro y todo artículo moderno de matemáticas es bourbakista en ese sentido. Para definir lo que se entiende por una demostración rigurosa en sentido moderno, habría que decir que es una demostración formalizable en ZFC, pero, evidentemente, pocos matemáticos tienen en cuenta para nada ZFC a la hora de hacer su trabajo y exponer sus resultados. El criterio práctico que aplican para dar una exposición por rigurosa, el estándar de rigor matemático actual (al margen de todas las motivaciones, ilustraciones y aplicaciones que estimen oportuno adjuntar), es el que Bourbaki, no inventó —sin duda— pero sí oficializó.

La publicación de los seis libros proyectados por Bourbaki estaba casi terminada salvo por el primero, el de *Teoría de conjuntos,* del que no se había publicado nada más allá del fascículo de resultados que, no obstante, había sido suficiente para basar en él todos los libros posteriores. Sólo en 1954 se publicaron los dos primeros capítulos, titulados *Descripción de la matemática formal* y *Teoría de conjuntos,* en **1956** se publicó el tercer capítulo, titulado *Conjuntos ordenados, cardinales, números enteros* (y también el capítulo 5 del libro de *Integración*) y en **1957** el cuarto y último, *Estructuras.*

El capítulo primero describe un lenguaje formal compuesto por variables, cinco signos lógicos $(\square, \tau, \vee, \neg, =)$ y el signo no definido $\in$.

El signo τ es el operador que Hilbert llamaba ϵ, de modo que $\tau_x \alpha(x)$ significa "un x ejemplo de conjunto x que cumple $\alpha(x)$" (y no está definido cuando no existe ninguno), lo que le permite, entre otras cosas, definir los cuantificadores como hemos explicado en la página 78, y también puede usarse como descriptor.

[165] Entre las menos moderadas, ésta es de Siegel:

Desafortunadamente, hay muchos "compañeros de viaje" que ya han desprestigiado gran parte del álgebra y la teoría de funciones; sin embargo, hasta ahora, la teoría de números no se había tocado. Esta gente me recuerda el comportamiento cínico de los nacionalsocialistas que cantaban: "¡Seguiremos marchando hasta que todo se derrumbe!". Me temo que las matemáticas perecerán antes de que termine este siglo si la actual tendencia a la abstracción sin sentido —la teoría del conjunto vacío, como yo la llamo— resulta irrefrenable.

El signo $\square$ da lugar a una forma peculiar de concebir las variables ligadas. Por ejemplo, Bourbaki explica que la expresión "$\tau_x(x \in y)$" es en realidad una forma de referirse a la fórmula[166]

$$\tau_x(x \in y) \equiv \overbrace{\tau \in \square y}$$

que no contiene en realidad ninguna variable x.

Veamos un ejemplo más sofisticado. Si definimos $\varnothing \equiv x|\bigwedge y\, y \notin x$, usando la definición del generalizador:

$$\bigwedge y\, \alpha(y) \equiv \neg\bigvee y \neg\alpha(y) \equiv \neg\neg\alpha(\tau_y(\neg\alpha(y)))$$

para el caso $\alpha(y) \equiv y \notin x$, tenemos:

$$\varnothing \equiv \tau_x \bigwedge y\, y \notin x \equiv \tau_x \neg\neg(\tau_y(\neg y \notin x) \notin x) \equiv \tau_x \neg\neg\neg(\tau_y(\neg\neg y \in x) \in x) \equiv \tau_x \neg\neg\neg \in \tau_y \neg\neg \in yxx,$$

y, eliminando las variables ligadas queda:

$$\varnothing \equiv \overbrace{\tau \neg\neg\neg \in \overbrace{\tau \neg\neg \in \square\square}\square}$$

Bourbaki define los conectores $\wedge$, $\Rightarrow$, $\Leftrightarrow$ a partir de $\neg$ y $\vee$ y los cuantificadores $\forall$, $\exists$ a partir del operador τ.

Luego introduce unos axiomas lógicos y el concepto de demostración formal, discutiendo las técnicas básicas de demostración (suponer una hipótesis para probar una implicación, la reducción al absurdo, la distinción de casos, etc.) Entre los axiomas que regulan el igualador, introduce el siguiente, que asegura la coherencia del operador τ:

$$\forall x(R \Leftrightarrow S) \Rightarrow \tau_x R = \tau_x S.$$

En el capítulo segundo se introduce una teoría axiomática de conjuntos que es equivalente a ZFC sin el axioma de regularidad. Tras afirmar que la teoría de conjuntos considera fórmulas del tipo $T \in U$, explica:

> *Desde una perspectiva ingenua (*naïf*), muchos entes matemáticos pueden considerarse colecciones o conjuntos de objetos. No intentaremos formalizar esta noción, y en la interpretación formalista de lo que sigue, la palabra "conjunto" debe considerarse estrictamente sinónimo de "término"; en particular, oraciones como "sea X un conjunto" son, en principio, completamente superfluas, ya que cada letra es un término; dichas oraciones se introducen únicamente para facilitar la interpretación intuitiva del texto.*

Bourbaki expresa los axiomas sobre existencia de conjuntos en términos de "relaciones colectivizantes", es decir, plantea que no todas las fórmulas definen conjuntos, y llama *colectivizantes* a las que sí que lo hacen. Por ejemplo, el axioma del par lo enuncia así:

$$(\forall x)(\forall y)\mathrm{Col}_z(z = x \text{ o } z = y),$$

que significa que la fórmula $\alpha(z) \equiv z = x \vee z = y$ define un conjunto. Previamente ha puesto $x \notin x$ como ejemplo de relación no colectivizante, y lo demuestra mediante la paradoja de Russell. Más adelante mostrará también que $x = x$ no es colectivizante razonando que, si lo fuera, toda fórmula lo sería.

El axioma más escondido en su formulación es el axioma de reemplazo, que aparece enunciado en un esquema axiomático que lo engloba con el axioma de la unión:

$$(\forall y)(\exists X)(\forall x)(R \Rightarrow (x \in X)) \Rightarrow (\forall Y)\mathrm{Col}_x((\exists y)(y \in Y \text{ y } R)).$$

Si hacemos $R \equiv x \in y$, obtenemos

$$(\forall y)(\exists X)(\forall x)((x \in y) \Rightarrow (x \in X)) \Rightarrow (\forall Y)\mathrm{Col}_x((\exists y)(y \in Y \text{ y } (x \in y))).$$

La hipótesis se cumple tomando $X = y$, y la conclusión es la que la fórmula $\alpha(x) \equiv \exists y(x \in y \wedge y \in Y)$ define un conjunto, que no es sino $\bigcup Y$.

[166] Aquí vemos también que "oficialmente" $x \in y$ es la cadena de signos $\in xy$. La idea es que si cada signo se escribe delante de sus argumentos, los paréntesis se vuelven innecesarios. Por ejemplo, hacen falta paréntesis para distinguir $\neg(\alpha \vee \beta)$ de $\neg\alpha \vee \beta$, pero si escribimos el disyuntor delante, las dos fórmulas son $\neg\vee\alpha\beta$ y $\vee\neg\alpha\beta$, respectivamente, por lo que no se confunden. Por eso, Bourbaki conviene en que una disyunción es una fórmula de tipo $\vee\,\alpha\beta$, aunque, en la práctica, la escribimos como $\alpha \vee \beta$, añadiendo paréntesis cuando haga falta. Lo mismo vale para $\in, =$.

Por otro lado, a partir de este mismo esquema es posible demostrar la versión siguiente del axioma de reemplazo:

$$\bigwedge y \overset{1}{\bigvee} x\, \phi(x,y) \to \bigwedge Y \bigvee z \bigwedge x(x \in z \leftrightarrow \bigvee y(y \in Y \wedge \phi(y,x))).$$

En efecto, si suponemos $\bigwedge y \overset{1}{\bigvee} x\, \phi(x,y)$ y aplicamos el esquema de Bourbaki sustituyendo R por $\phi(y,x)$, obtenemos

$$(\forall y)(\exists X)(\forall x)(\phi(y,x) \Rightarrow (x \in X)) \Rightarrow (\forall Y)\mathrm{Col}_x((\exists y)(y \in Y \text{ y } \phi(y,x))).$$

Ahora, fijado un y, si llamamos x al único conjunto que cumple $\phi(y,x)$, la hipótesis se cumple con $X = \{x\}$, y la conclusión es que, para todo conjunto Y, la fórmula $\alpha(x) \equiv \exists y(y \in Y \wedge \phi(y,x))$ define un conjunto, que es justo el que requiere el axioma de reemplazo.

Por lo demás (salvo que están enunciados en términos de relaciones colectivizantes), en los axiomas de Bourbaki se reconocen claramente los axiomas de ZFC sin el axioma de regularidad, excepto el axioma de elección, que no necesita enunciarlo porque está implícito en la lógica del operador τ, que ya elige un elemento de cada conjunto no vacío.

A partir de aquí Bourbaki dedica el resto del segundo capítulo a los teoremas enunciados en su fascículo de resultados, salvo los relativos a las relaciones de orden y la teoría de ordinales, que se presentan en el tercer capítulo.

Las únicas consideraciones metamatemáticas sobre la teoría axiomática presentada en los dos primeros capítulos aparece en la introducción del libro, donde leemos:

> *Huelga decir que la descripción del lenguaje formalizado se realiza en lenguaje cotidiano, como las reglas del ajedrez; no entraremos en la discusión de los problemas psicológicos o metafísicos que plantea la validez del uso del lenguaje cotidiano en tales circunstancias (por ejemplo, la posibilidad de reconocer que una letra del alfabeto es "la misma" en dos lugares diferentes de una página, etc.). Tampoco es posible realizar dicha descripción sin utilizar la numeración; aunque algunas mentes brillantes pueden haberse sentido incómodas por este hecho, hasta el punto de considerarlo una petición de principio, es evidente que en este caso los números sólo se utilizan como referencias (que además podrían sustituirse por otros signos como colores o letras), y que no se realiza ningún razonamiento matemático al contar los signos que aparecen en una fórmula explícita. No analizaremos la posibilidad de enseñar los principios del lenguaje formalizado a seres cuyo desarrollo intelectual no llega a saber leer, escribir y contar.*
>
> *Si las matemáticas formalizadas fueran tan sencillas como el ajedrez, una vez descrito el lenguaje formalizado elegido, sólo quedaría escribir nuestras demostraciones en él, como el autor de un tratado de ajedrez escribe en su notación las partidas que pretende enseñar, acompañándolas con comentarios si es necesario. Pero las cosas están lejos de ser tan fáciles, y no se necesita mucha práctica para darse cuenta de que tal proyecto es absolutamente irrealizable; la más mínima demostración del inicio de la teoría de conjuntos ya requeriría cientos de signos para formalizarse por completo. Por lo tanto, desde el Libro 1 de este tratado, se impone la imperiosa necesidad de abreviar el texto formalizado mediante la introducción de nuevas palabras (llamadas "signos de abreviatura") y reglas sintácticas adicionales (llamadas "criterios deductivos") en un número considerable. De este modo, obtenemos lenguajes mucho más manejables que el propio lenguaje formalizado, y que un matemático con poca experiencia está convencido de que pueden considerarse transcripciones taquigráficas de éste último.*

La justificación del razonamiento metamatemático es bastante rudimentaria:

> *Como verá el lector, la introducción de este lenguaje condensado va acompañada de razonamientos de un tipo particular, propios de la llamada metamatemática. Esta disciplina, haciendo abstracción de cualquier significado que pudiera haberse atribuido originalmente a las palabras o frases de textos matemáticos formalizados, considera estos textos como objetos particularmente simples, conjuntos de objetos previamente dados, de los cuales sólo importa el orden asignado. Y, así como, por ejemplo, un tratado de química anuncia con antelación el resultado de un experimento realizado en condiciones dadas, los razonamientos metamatemáticos suelen afirmar que, tras una sucesión de operaciones sobre un texto de un tipo determinado, el texto final será de otro tipo. En los casos más*

> *simples, estas afirmaciones son, de hecho, puras verdades (que podrían compararse, por ejemplo, con lo siguiente: "cuando, en una bolsa de canicas que contiene canicas negras y blancas, todas las canicas negras son reemplazadas por canicas blancas, sólo quedan canicas blancas en la bolsa". Pero encontramos desde el principio ejemplos en los que el argumento toma un cariz típicamente matemático, con el uso predominante de números enteros arbitrarios y razonamiento por recurrencia. Si hemos descartado anteriormente la objeción contra el uso de la numeración en la descripción de un lenguaje formalizado, ya no es posible negar aquí el peligro de incurrir en una petición de principio, ya que, desde el principio, parecen emplearse todos los recursos de la aritmética, mientras que la intención, entre otras cosas, es exponer sus fundamentos. A esto algunos creen poder responder que, en este tipo de razonamientos, sólo describen operaciones susceptibles de ser realizadas y controladas, y por ello extraen de ellos una convicción de un orden diferente al que otorgan a las matemáticas propiamente dichas. Parece más sencillo decir que se podría prescindir de estos razonamientos metamatemáticos si las matemáticas formalizadas se escribieran realmente: en lugar de utilizar los "criterios deductivos", se comenzaría de nuevo cada vez las secuencias de operaciones que pretenden acortar prediciendo su resultado. Pero las matemáticas formalizadas no pueden escribirse en su totalidad; por lo tanto, es necesario, en última instancia, confiar en lo que podríamos llamar el sentido común del matemático; confianza análoga a la que un contable o un ingeniero otorga a una fórmula o una tabla numérica sin sospechar la existencia de los axiomas de Peano, y que, en última instancia, se basa en el hecho de que nunca ha sido contradicha por los hechos.*

Vemos así que Bourbaki "quiere pensar" que sus *Elementos* proporcionan el fundamento de la aritmética, pero al mismo tiempo se da cuenta de que la metamatemática de sus *Elementos* ya presupone la aritmética, y simplemente lo deja pasar. Lo que ocurre en el fondo es que, a Bourbaki, la lógica matemática y la teoría axiomática de conjuntos le traían sin cuidado. En 1949 se había fundado en Rumanía el *Instituto de Matemáticas Simion Stoilow,* y se cuenta que, en una visita, Dieudonné declaró que los capítulos 1 y 2 del libro de Teoría de conjuntos se habían incluido principalmente para satisfacer a los filósofos molestos. La introducción continúa explicando que nunca se van a usar (de hecho, que nunca se habían usado, porque los libros restantes estaban ya publicados, salvo unos pocos capítulos):

> *Por lo tanto, abandonaremos las matemáticas formalizadas desde el principio, pero no sin antes trazar con precisión el camino para retomarlas. Las facilidades que ofrecen los primeros "abusos del lenguaje" así introducidos nos permitirán escribir el resto de este Tratado (y en particular el fascículo de resultados del Libro 1) como se hace en la práctica con todos los textos matemáticos, es decir, en parte en lenguaje cotidiano y en parte mediante fórmulas que constituyen formalizaciones parciales, particulares e incompletas, de las cuales las del cálculo algebraico constituyen el ejemplo más conocido. A menudo, el lenguaje cotidiano se utilizará con mucha más libertad aún, mediante abusos deliberados del lenguaje, mediante la simple omisión de pasajes que se presumen fáciles de recuperar para un lector incluso con poca experiencia, mediante indicaciones intraducibles al lenguaje formal y destinadas a facilitar dicha recuperación. Otros pasajes igualmente intraducibles contendrán comentarios destinados a aclarar la progresión de las ideas, si es necesario apelando a la intuición del lector. El uso de recursos retóricos se vuelve entonces legítimo, siempre que se mantenga inalterada la posibilidad de formalizar el texto.*

En suma, que en el resto de los *Elementos,* se va a razonar como han razonado siempre los matemáticos, sin rastro de lógica o de axiomas conjuntistas, y que esto está legitimado porque todo cuando se dice es claramente formalizable en la teoría propuesta. De hecho, el Libro I incluye como apéndice el fascículo de resultados, con una nota al pie en la que se lee:

> *El lector no dejará de observar que el punto de vista ingenuo que se adopta en este fascículo para exponer los principios de la teoría de conjuntos es directamente opuesto al punto de vista formalista adoptado en el libro sobre teoría de conjuntos del que este fascículo es un resumen; por supuesto, esta oposición es intencional y corresponde a los diferentes objetivos para los cuales se escribieron estas dos partes de nuestro trabajo.*

En efecto, en el tercer capítulo, donde se demuestran, entre otras cosas, el principio de buena ordenación y el lema de Zorn, apenas se ven unos pocos cuantificadores aislados en algún que otro lugar y algunas apariciones del operador τ en puntos decisivos, como en la demostración del principio de buena ordenación, donde explicita el uso del axioma de elección, y, sobre todo, en la definición del cardinal de un conjunto.

En efecto, para definir el cardinal de un conjunto, Bourbaki evita la teoría de ordinales gracias a su operador τ, que le permite definir

$$\mathrm{Card}(X) \equiv \tau_Z(\mathrm{Eq}(X, Z)),$$

es decir, que el cardinal de X es un "ejemplo de " conjunto Z equipotente a X. Esto le evita tener que elegir uno en concreto, y puede demostrar que dos conjuntos son equipotentes si y sólo si tienen el mismo cardinal.

Ésta es la auténtica motivación para la introducción del operador τ. El hecho de que permita definir los cuantificadores o expresar implícitamente el axioma de elección es algo anecdótico, incluso la posibilidad de usarlo como descriptor sería prescindible, pero esta definición de cardinal resuelve al instante el mayor problema técnico que presenta la formalización de la teoría de cardinales sin pasar por la solución de von Neumann, que sigue vigente hoy en día, pero que obliga a construir los ordinales simplemente para definir el concepto de cardinal, aunque no se necesiten para nada más.

Bourbaki, en cambio, relega los ordinales a la colección de ejercicios del capítulo 3, donde enuncia también muchas propiedades más de los cardinales.

Naturalmente, los números naturales se definen como los cardinales finitos, de modo que la suma y el producto de números naturales se presentan como un caso particular de la suma y el producto de cardinales.

Finalmente el capítulo cuarto demuestra resultados generales sobre estructuras algebraicas, morfismos, etc. En este capítulo los restos de notación lógica son todavía más escasos que en el anterior, y son prácticamente nulos en el resto de libros de la serie.

El retraso en la aparición de los capítulos sobre teoría de conjuntos se debió a que éste fue el libro que más controversias suscitó entre los miembros del grupo. La versión inicial había sido presentada para su discusión por Cartan en 1935, y era una teoría ingenua de conjuntos, en la línea del fascículo de resultados que se publicaría más tarde, pero no se consideró satisfactoria y el trabajo en este libro se suspendió provisionalmente. En 1939 Dieudonné publicó un artículo titulado *Los métodos axiomáticos modernos y la fundamentación de las matemáticas,* en el que suscribe el programa formalista de Hilbert como vía para superar la crisis de los fundamentos. En 1943 Cartan publicó *Sobre el fundamento lógico de las matemáticas,* en el que presenta los axiomas de Zermelo (sin reemplazo), pero se refiere a ellos como axiomas de Zermelo-Fraenkel y afirma que *todas las matemáticas que existen hoy en día pueden expresarse en el sistema que acabo de esbozar.*

En 1949 fue el propio Bourbaki el que publicó un artículo titulado *Fundamentos de las matemáticas para la labor del matemático,* donde no se muestra preocupado por la posibilidad de que surjan contradicciones en matemáticas:

> *Históricamente hablando, es, por supuesto, completamente falso que las matemáticas estén libres de contradicciones; la no contradicción aparece como una meta a alcanzar, no como una cualidad divina que nos ha sido otorgada de una vez por todas. Desde los tiempos más remotos, todas las revisiones críticas de los principios de las matemáticas en su conjunto, o de cualquiera de sus ramas, han seguido casi invariablemente a períodos de incertidumbre, donde surgieron contradicciones que tuvieron que resolverse. Es difícil juzgar si la necesidad de demostraciones sistemáticas en las matemáticas griegas primitivas surgió o no de las paradojas relacionadas con el descubrimiento de magnitudes inconmensurables, como han sugerido varios historiadores. Pero ejemplos más modernos, como el desarrollo del cálculo infinitesimal, la teoría de series y la teoría de conjuntos, apuntan a la misma conclusión. Las contradicciones ocurren, pero no se puede permitir que subsistan si se pretende que la distinción entre verdadero y falso, probado y no probado, conserve su significado. No existe una línea nítida entre las contradicciones que surgen en el trabajo diario de todo matemático, principiante o experto, como resultado de errores más o menos fáciles de detectar, y las grandes paradojas que alimentan la reflexión lógica durante décadas y, a veces, siglos. La ausencia de contradicción, en las matemáticas en su conjunto o en cualquier rama de ellas, aparece así como un hecho empírico, más que como un principio metafísico. Cuanto más se ha desarrollado una rama, menos probable es que se encuentren contradicciones en su desarrollo posterior. Al mismo tiempo, incluso en las ramas más consolidadas de nuestra ciencia, todos sabemos que un uso torpe o demasiado astuto de la terminología y las notaciones existentes puede generar ambigüedades y, finalmente, contradicciones. No me refiero simplemente a esos "abusos de lenguaje" sin los cuales ningún texto matemático sería legible; un examen superficial de muchas notaciones existentes mostrará que pocas son completamente infalibles, en el sentido de que las ambigüedades inherentes a la mayoría de ellas no pueden*

eliminarse sin complicarlas hasta el punto de hacerlas inútiles. Como ejemplo, se puede mencionar el uso de paréntesis y corchetes, y los acuerdos entre caballeros en virtud de los cuales estos pueden ser frecuentemente ignorados.

¿Cuál será la actitud del matemático en activo ante tales dilemas? Creo que no tiene por qué ser otra que estrictamente empírica. No podemos esperar que pueda probarse que toda definición, todo signo, toda abreviatura que introduzcamos esté libre de posibles ambigüedades, que no genere la posibilidad de una contradicción que de otro modo no existiría. Exijamos que las reglas se formulen y las definiciones se expongan de tal manera que cada contradicción pueda rastrearse fácilmente hasta su causa, y que ésta sea eliminada o rodeada de señales de advertencia para evitar problemas graves. Esto, para el matemático, debería ser suficiente; y es con este objetivo comparativamente modesto y limitado en mente que he tratado de sentar las bases de mi tratado matemático, de la manera que describiré a continuación.

La manera que presenta a continuación es una paupérrima teoría de conjuntos —claramente insuficiente— formada por parte de los axiomas de Zermelo (extensionalidad, el esquema de especificación, el axioma de elección y unos axiomas que afirmaban la existencia de pares ordenados (tomados como un concepto primitivo) y de productos cartesianos, además del axioma de infinitud, que formula verbalmente. Tras ello concluía:

Sobre estas bases, afirmo que puedo construir toda la matemática actual; y, si hay algo original en mi procedimiento, reside únicamente en el hecho de que, en lugar de contentarme con tal afirmación, procedo a demostrarla de la misma manera que Diógenes demostró la existencia del movimiento; y mi demostración se hará cada vez más completa a medida que avance mi tratado.

En una traducción al inglés de *La arquitectura de las matemáticas,* publicada en 1950, se añade una nota al pie en la que se lee:

No consideramos aquí las objeciones que han surgido de la aplicación de las reglas de la lógica formal al razonamiento en teorías axiomáticas; estas están relacionadas con las dificultades lógicas encontradas en la teoría de conjuntos. Baste señalar que estas dificultades pueden superarse de una manera que no deja la más mínima duda sobre la corrección del razonamiento; [2] *y* [3] *son valiosas referencias a este respecto.*

Las referencias son los dos artículos que hemos mencionado previamente. En este mismo artículo se incide en el carácter secundario de la lógica matemática:

Los términos "formalismo" y "método formalista" también se utilizan con frecuencia; pero es importante estar en guardia desde el principio contra la confusión que puede causar el uso de estos términos imprecisos, y que con demasiada frecuencia utilizan quienes se oponen al método axiomático. Es sabido que, superficialmente, las matemáticas aparecen como esta "larga cadena de razones" de la que habló Descartes; toda teoría matemática es una concatenación de proposiciones, cada una derivada de las anteriores de conformidad con las reglas de un sistema lógico, que es esencialmente el codificado, desde la época de Aristóteles, bajo el nombre de "lógica formal", convenientemente adaptado a los objetivos particulares del matemático. Por lo tanto, es una obviedad decir que este "razonamiento deductivo" es un principio unificador de las matemáticas. Así que una observación superficial no puede explicar la evidente complejidad de las diferentes teorías matemáticas, como tampoco se podría, por ejemplo, unir la física y la biología en una sola ciencia basándose en que ambas utilizan el método experimental. El método de razonamiento mediante cadenas de silogismos no es más que un mecanismo transformador, aplicable tanto a un conjunto de premisas como a otro; por lo tanto, no podría servir para caracterizar estas premisas. En otras palabras, es la forma externa que el matemático da a su pensamiento, el vehículo que lo hace accesible a otros, en resumen, el lenguaje adecuado para las matemáticas; esto es todo, no se le debe atribuir mayor importancia. Establecer las reglas de este lenguaje, configurar su vocabulario y aclarar su sintaxis, todo eso es realmente extremadamente útil; de hecho, esto constituye un aspecto del método axiomático, el que puede llamarse con propiedad formalismo lógico (o "logística", como a veces se le llama). Pero enfatizamos que este es sólo un aspecto de este método, de hecho, el menos interesante. Lo que el método axiomático establece como objetivo esencial es precisamente aquello que el formalismo lógico por sí solo no puede proporcionar, a saber, la profunda inteligibilidad de las matemáticas. Así como el método experimental parte de la creencia* a priori *en la permanencia de las leyes naturales,*

> *el método axiomático tiene su piedra angular en la convicción de que las matemáticas no sólo no son una concatenación aleatoria de silogismos, sino que tampoco son una colección de trucos más o menos "astutos", obtenidos mediante combinaciones afortunadas, en los que la habilidad puramente técnica triunfa. Donde el observador superficial sólo ve dos o varias teorías muy distintas, que se prestan mutuamente un "apoyo inesperado" gracias a la intervención de un matemático genial, el método axiomático*[167] *nos enseña a buscar las razones profundas de tal descubrimiento, a encontrar las ideas comunes de estas teorías, ocultas bajo la acumulación de detalles propios de cada una de ellas, a sacar a la luz estas ideas y a exponerlas bajo su luz adecuada.*
>
> ∗ De hecho, todo matemático sabe que una demostración no ha sido realmente "comprendida" si uno no ha hecho más que verificar paso a paso la exactitud de las deducciones que la componen, y no ha intentado comprender claramente las ideas que han llevado a la construcción de esta particular cadena de deducciones con preferencia a cualquier otra.

Estas citas son interesantes porque, por un lado, ponen en evidencia el escaso interés que los miembros de Bourbaki tenían por la lógica matemática[168] y también el conocimiento limitado que tenían de ella (aunque, sin duda, se estaban documentando), lo cual, a su vez, es interesante porque es el mismo punto de vista sobre la fundamentación de las matemáticas que sostenían —o iban a sostener, por la influencia que tuvo Bourbaki— muchos matemáticos, especialmente en Francia, que fueron educados bajo estos criterios bourbakistas:

- Hacer matemáticas es razonar a partir de unas propiedades básicas sobre conjuntos, que a su vez pueden precisarse mediante axiomas y leyes lógicas, pero que cualquiera que lea un texto como el *fascículo de resultados* (o cualquier exposición más didáctica de una teoría ingenua de conjuntos) puede emplear competentemente y con pleno rigor sin necesidad de preocuparse por la lógica y los axiomas.

- No hay razón para preocuparse por si los axiomas implican contradicciones. No parece que las haya y, si alguna vez se encuentra alguna, ya se resolverá, como los matemáticos han resuelto sus contradicciones numerosas veces en la historia, pero es inviable tratar de resolver un problema que no se ha planteado. La situación es análoga a la de los físicos que trabajan con una teoría física sin la absoluta certeza de que algún experimento futuro no obligará a cambiarla, pero si eso ocurre, no será un drama, sino un avance en el conocimiento. En el caso de las matemáticas se puede decir lo mismo.

- Toda la matemática, incluyendo la aritmética, puede justificarse a partir de los resultados conjuntistas básicos de la teoría ingenua de conjuntos, donde las paradojas se evitan simplemente no planteándoselas, sabiendo que se pueden evitar con rigor mediante el marco teórico adecuado. El hecho de que ese marco teórico adecuado que es en teoría previo a la teoría de conjuntos que sirve de fundamento a la aritmética requiere ya de la aritmética es un círculo vicioso en el que es mejor no pensar. Simplemente, ahí entra en juego el "sentido común".

- En principio, todo razonamiento matemático debería desarrollarse según los cánones de rigor de la matemática moderna, razonando a partir de axiomas. Y si los lógicos no parten de axiomas para estudiar esos axiomas, eso muestra que son unos chapuceros que no saben lo que es hacer matemáticas bien hechas, razón de más para no leer libros de lógica, porque no son serios. E incluso parece que sus autores tratan deliberadamente de engañar al lector con filosofías baratas y otros ardides para disimular la falta de solidez y de solvencia de sus argumentos.

Este último punto no es atribuible a Bourbaki, obviamente, pero sí a la versión distorsionada que surgió inevitablemente con su difusión de boca en boca en un amplio sector de varias generaciones de matemáticos.

No fue hasta 1950 cuando Chevalley presentó al grupo una propuesta (la quinta versión) para el capítulo 1 que ya era similar a la que sería la versión definitiva, con la inclusión del operador τ, y unos meses más tarde otra del capítulo 2, que mencionaba los axiomas meramente por dejar constancia de ellos, pero sin usarlos realmente para nada.

[167] Recordemos que por "método axiomático" Bourbaki entiende la exposición de las matemáticas en términos de estructuras generales (grupos, anillos, etc.) que permitan aplicar las mismas ideas a contextos muy diferentes.

[168] Años más tarde, Dieudonné escribiría:

Al noventa y cinco por ciento de los matemáticos les importa un comino la lógica matemática [...] *cuando alguien viene y nos habla de lógica de primer y segundo orden, de funciones recursivas y de modelos, que son teorías muy bonitas y muy hermosas que han dado resultados notables, nosotros, los matemáticos, no vemos ninguna razón por la que la gente no debiera estudiar estos temas, pero por otro lado no nos atraen nada.* [De donde se sigue que Hilbert, von Neumann, etc. no eran matemáticos.]

Desde ese año de 1950 asistía como oyente a las reuniones de Bourbaki un joven matemático de 22 años llamado Alexander Grothendieck[169] En 1951 se propuso adoptar los axiomas de NBG, como medio para incluir un capítulo adicional sobre teoría de categorías. Sin embargo, la idea fue acogida con desconfianza. En una nota histórica al final del libro de Teoría de conjuntos se lee:

> *La eliminación de paradojas parece haberse logrado con los sistemas anteriores, pero a costa de restricciones que inevitablemente resultan muy arbitrarias. En defensa del sistema de Zernielo-Fraenkel, cabe decir que se limita a formular prohibiciones que sólo sancionan la práctica habitual en la aplicación de la noción de conjunto a diversas teorías matemáticas. Los sistemas de von Neumann y Gödel se alejan aún más de las concepciones habituales; por otra parte, no se descarta que sea más fácil insertar ciertas teorías matemáticas aún incipientes en el marco proporcionado por dichos sistemas que en el marco más restringido del sistema de Zermelo-Fraenkel.*

Parece ser que a Bourbaki, como a Kelley (página 207) le chirriaba la distinción entre conjuntos y clases propias (y, efectivamente, en el "bourbakismo popular" muchos matemáticos veían las clases propias como unos "objetos sospechosos", que en el momento menos pensado le podían dar a uno un disgusto). Que a uno no le dejen hablar del conjunto V de todos los conjuntos era aceptable, pues, al fin y al cabo, no era necesario para nada, pero que a uno le digan que existe la clase V de todos los conjuntos, pero que no puede decirse que $V \in V$, eso ya era más difícil de tragar.

Ese año de 1951 se unió al grupo Serge Lang. En 1953 Dieudonné y Dixmier presentaron la versión definitiva del segundo capítulo de la teoría de conjuntos, y en 1954 se publicaron finalmente los dos primeros capítulos, como ya habíamos indicado.

En 1955 Grothendieck ingresó en Bourbaki, junto con Pierre Cartier, y fue uno de los que más abogó por la inclusión de un capítulo sobre categorías. En **1957** publicó su artículo *Sobre algunos puntos del álgebra homológica,* en el que definió el concepto de *categoría abeliana* y mostró cómo en términos de estas categorías podía unificar muchas construcciones del álgebra homológica que inicialmente se habían demostrado para módulos a un contexto más general aplicable a otras categorías, como la de haces de grupos abelianos sobre un espacio topológico, lo cual a su vez fue un paso previo para la introducción del concepto de *esquema.* No importa si el lector no está familiarizado con estos conceptos. Lo relevante de lo que acabamos de decir es que Grothendieck usó la teoría de categorías para unificar varias teorías matemáticas, mientras que el "método axiomático" de Bourbaki se quedaba corto. En otras palabras, Grothendieck puso en evidencia que la teoría de categorías era mucho más que un lenguaje más o menos conveniente, pero prescindible en última instancia.

En **1957** murió von Neumann, a los 57 años. Bernays entonces tenía 69. En 1954 había publicado la última parte de su artículo sobre su teoría de conjuntos, y en 1958 la publicó de nuevo en forma de libro, con una introducción de Fraenkel. No hay mucho que comentar. Bernays —que no menciona a Gödel en ningún momento— hace complicado lo que Gödel había hecho sencillo.

Bourbaki publicó el capítulo 8 del libro de *Álgebra* y en 1959 el capítulo 9, así como el capítulo 6 del libro de *Integración.* Los dos últimos capítulos de este libro aparecerían en 1963 y con ellos se completaría la primera versión de los seis libros previstos inicialmente (aunque el grupo ya estaba trabajando en otros nuevos).

En 1960 Grothendieck, con la ayuda de Dieudonné, empezó a publicar sus *Elementos de Geometría Algebraica,* una obra equiparable a la de Bourbaki para esta rama específica de las matemáticas. Además de los avances que contenía, tuvo también un papel fundacional muy importante, pues la geometría algebraica clásica era una de las partes menos rigurosas de la matemática, principalmente por su uso de los conceptos indefinidos de "punto genérico", "curva genérica", etc., que debían entenderse como objetos generales, sin ninguna característica particular. Durante décadas hubo un debate entre Francesco Severi y Oscar Zariski sobre si cierta demostración del primero era válida o no. Zariski insistía en que Severi usaba el concepto de "punto genérico" de forma ambigua y atribuyéndole propiedades mal definidas. En 1935 Zariski publicó su libro *Superficies algebraicas,* en el que evitaba estos conceptos, mientras que en 1946 André Weil publicó sus *Fundamentos de la Geometría algebraica,* en los que formalizaba el concepto de "punto genérico", pero su marco conceptual acabaría relegado por el que propuso Grothendieck, que resultó ser mucho más conveniente. La transición de la geometría algebraica al patrón moderno de rigor conceptual fue una de las más traumáticas y que más esfuerzo requirieron a los especialistas del área.

[169] Grothendieck había llegado a París en 1949 y propuso a Dieudonné y Schwartz que le dirigieran la tesis. Éstos, para librarse de él, le dieron una copia de su último artículo, que terminaba con 14 problemas abiertos sobre espacios vectoriales topológicos. Grothendieck los resolvió en apenas unos meses, desarrollando para ello nuevas técnicas. Grothendieck se doctoró en 1953 bajo la dirección de Dieudonné y Schwartz.

Ese mismo año de 1960 Patrick Suppes publicó su *Teoría axiomática de conjuntos,* que presenta una versión de ZFC con elementos primitivos (que no son conjuntos). No es muy profunda, pues no llega a demostrar los teoremas principales sobre suma y producto de cardinales infinitos, pero es una exposición legible hoy en día, lo que no puede decirse del libro de Bernays.

Estos teoremas sí que se encuentran, en cambio, en la *Teoría ingenua de conjuntos* que publicó Paul Richard Halmos también en 1960. Merece la pena leer la introducción completa, que probablemente contiene lo que Bourbaki nunca se atrevió a decir:

> *Todos los matemáticos coinciden en que deben conocer algo de teoría de conjuntos; el desacuerdo surge al intentar decidir cuánto es algo. Este libro contiene mi respuesta a esa pregunta. Su propósito es explicar al estudiante principiante de matemáticas avanzadas los fundamentos de la teoría de conjuntos, con el mínimo discurso filosófico y formalismo lógico. El punto de vista general es el de un futuro matemático deseoso de estudiar grupos, integrales o variedades. Desde esta perspectiva, los conceptos y métodos de este libro son sólo algunas de las herramientas matemáticas estándar; el especialista experto no encontrará nada nuevo aquí.*
>
> *Los créditos y referencias bibliográficas académicas están fuera de lugar en un libro puramente expositivo como este. Sin embargo, el estudiante que se interese por la teoría de conjuntos en sí misma debe saber que hay mucho más sobre el tema que lo que hay en este libro. Una de las fuentes más hermosas de sabiduría conjuntista sigue siendo la teoría de conjuntos de Hausdorff. Una adición reciente a la literatura y de fácil lectura, con una bibliografía extensa y actualizada, es la Teoría Axiomática de Conjuntos de Suppes.*
>
> *En teoría de conjuntos, "ingenuo" y "axiomático" son términos opuestos. El presente estudio podría describirse mejor como teoría axiomática de conjuntos desde una perspectiva ingenua. Es axiomática en el sentido de que algunos axiomas de la teoría de conjuntos se enuncian y se utilizan como base de todas las demostraciones posteriores. Es ingenua en el sentido de que el lenguaje y la notación son los de las matemáticas informales ordinarias (pero formalizables). Una forma más importante en la que predomina la perspectiva ingenua es que la teoría de conjuntos se considera un conjunto de hechos, de los cuales los axiomas son un resumen breve y práctico; en la perspectiva axiomática ortodoxa, las relaciones lógicas entre diversos axiomas son los objetos centrales de estudio. Análogamente, un estudio de geometría podría considerarse puramente ingenuo si se basara únicamente en la intuición del tipo "plegado de papel". El otro extremo, el puramente axiomático, es aquel en el que los axiomas de las diversas geometrías no euclidianas se estudian con la misma atención que los de Euclides. El punto de vista análogo de este libro es el estudio de un único conjunto juicioso de axiomas con la intención de describir únicamente la geometría euclidiana.*
>
> *En lugar de "Teoría ingenua de conjuntos", un título más sincero para el libro habría sido "Un esbozo de los elementos de la teoría ingenua de conjuntos". "Elementos" advertiría al lector de que no todo está aquí; "esbozo" le advertiría de que incluso lo que hay aquí necesita ser completado. El estilo suele ser informal, casi coloquial. Hay muy pocos teoremas expuestos; la mayoría de los hechos se exponen simplemente, seguidos de un esbozo de una demostración, de forma muy similar a como se haría en una lección descriptiva general. Sólo hay unos pocos ejercicios oficialmente etiquetados como tales, pero, de hecho, la mayor parte del libro no es más que una larga cadena de ejercicios con pistas. El lector debería preguntarse continuamente si sabe cómo pasar de una pista a otra y, por lo tanto, no debería desanimarse si descubre que su ritmo de lectura es considerablemente más lento de lo normal.*
>
> *Esto no significa que el contenido de este libro sea inusualmente difícil o profundo. Lo cierto es que los conceptos son muy generales y abstractos, por lo que puede llevar tiempo acostumbrarse a ellos. Sin embargo, es una obviedad matemática que cuanto más general sea la aplicación de un teorema, menos profundo será. La tarea del estudiante al aprender la teoría de conjuntos es empaparse de generalidades desconocidas, pero esencialmente superficiales, hasta que se familiaricen tanto que puedan usarse casi sin esfuerzo consciente. En otras palabras, la teoría general de conjuntos es bastante trivial, pero si quieres ser matemático, necesitas algo, y aquí está: léelo, absórbelo y olvídalo.*

Como bien dice Halmos, el contenido del libro es en realidad ZFC, sólo que desprovisto de tecnicismos lógicos. El libro sigue siendo una referencia interesante hoy en día para quien quiera familiarizarse con las ideas básicas de la teoría de conjuntos. He aquí un ejemplo de las observaciones con las que acompaña la introducción de conceptos:

Por muy importante que sea la teoría de conjuntos ahora, en sus inicios algunos académicos la consideraron una enfermedad de la que, con suerte, las matemáticas se recuperarían pronto.[170] *Por esta razón, muchas consideraciones de la teoría de conjuntos se calificaron de patológicas, y el término perdura en el uso matemático; a menudo se refiere a algo que desagrada al hablante. La definición explícita de un par ordenado ($(a,b) = \{\{a\},\{a,b\}\}$) se relega con frecuencia a la teoría de conjuntos patológica. Para quienes creen que en este caso el nombre es merecido, observamos que la definición ya ha cumplido su propósito y nunca se volverá a utilizar. Necesitamos saber que los pares ordenados están determinados por sus coordenadas primera y segunda, y que estas las determinan de forma única, que se pueden formar productos cartesianos, y que cada conjunto de pares ordenados es un subconjunto de algún producto cartesiano; el enfoque particular utilizado para lograr estos fines es irrelevante.*

Es fácil localizar el origen de la desconfianza y la sospecha que muchos matemáticos sienten hacia la definición explícita de par ordenado dada anteriormente. El problema no es que haya algo incorrecto o que falte algo; las propiedades relevantes del concepto que hemos definido son todas correctas (es decir, son acordes con las exigencias de la intuición) y se cumplen todas las propiedades requeridas. El problema es que el concepto tiene algunas propiedades irrelevantes que son accidentales y distraen. El teorema de que $(a,b) = (x,y)$ si y sólo si $a = x$ y $b = y$ es el tipo de cosas que esperamos aprender sobre pares ordenados. El hecho de que $\{a,b\} \in (a,b)$, por otro lado, parece accidental; una propiedad caprichosa de la definición en lugar de una propiedad intrínseca del concepto.

La acusación de artificialidad es cierta, pero no un precio demasiado alto a pagar por la economía conceptual. El concepto de par ordenado podría haberse introducido como un concepto primitivo adicional, dotado axiomáticamente con las propiedades adecuadas, ni más ni menos. En algunas teorías esto se hace. El matemático tiene que elegir entre tener que recordar algunos axiomas más y tener que olvidar algunos hechos accidentales; la elección es claramente una cuestión de gusto. Decisiones similares ocurren con frecuencia en matemáticas; en este libro, por ejemplo, las encontraremos de nuevo en relación con las definiciones de números de varios tipos.

Halmos llega a introducir los ordinales y los cardinales, y demuestra las propiedades básicas de la aritmética cardinal (que la suma y el producto de dos cardinales infinitos es igual al mayor de ellos).

84 La teoría de modelos El "método axiomático" impulsado por Bourbaki conectaba muy bien con una teoría que estaba más allá de las fronteras que Bourbaki establecía para las "matemáticas interesantes", y es la teoría que, aunque se remonta, como mínimo, a 1915, cuando Löwenheim publicó su teorema, sólo en 1954 recibió el nombre de *teoría de modelos* en un artículo de Tarski, y aún tardaría un tiempo en generalizarse este nombre.

Durante décadas, cuando los matemáticos querían hablar de objetos que cumplieran sus axiomas, hablaban más bien de "dominios", aunque con el tiempo se extendió el uso de la palabra "modelo", en principio por analogía con casos como el de los puntos de una esfera y sus círculos máximos, que constituían un modelo para la geometría riemanniana. Y aun así, el término "modelo" para hacer referencia a la determinación de un significado para las fórmulas de un lenguaje formal coexistió con otros como "sistema relacional". Tarski había sido el principal impulsor de la teoría de modelos, pero ésta venía exponiéndose en el típico estilo "prebourbakista", sin definiciones explícitas, o con definiciones que se explicitaban por conveniencia, pero que luego no se usaban explícitamente, dando por obvias —sin mencionarlas siquiera— sus primeras consecuencias.

Robert Lawson Vaught se había doctorado en 1954 bajo la dirección de Tarski, y en **1957** ambos publicaron un artículo[171] conjunto titulado *Extensiones aritméticas de sistemas relacionales,* en el que se introdujeron varias ideas y resultados que iban a tener muchas repercusiones, a la vez que se apreciaba un esfuerzo por precisar las definiciones empleadas. Para empezar, se presentó de una forma mucho más simple y clara la definición de "verdad" que Tarski había dado en 1933 (aunque se remite como referencia a una traducción al alemán de 1936) y, aun así, no se presenta en general, sino a través de un ejemplo típico.

Nosotros la explicaremos a través de un ejemplo un poco más sofisticado que ilustra mejor la situación general, así como la conexión con el "método axiomático" bourbakista a la que hemos hecho referencia al principio de la sección. Consideremos para ello el concepto algebraico de "cuerpo ordenado". En términos bourbakistas, un

[170] La cita se atribuye a Poincaré, aunque no es segura: *Las generaciones futuras verán la Mengenlehre como una enfermedad de la que uno se ha recuperado.*

[171] En este artículo, por cierto, se usan los cuantificadores $\bigwedge, \bigvee$ que nosotros usamos.

cuerpo ordenado es una cuádrupla $(K, +, \cdot, \leq)$, donde K es un conjunto, $+$ y $\cdot$ son aplicaciones $K \times K \longrightarrow K$ y $\leq$ es una relación en K, de modo que se cumplen los hechos siguientes:[172]

1. $\bigwedge xyz \in K\,(x + y) + z = x + (y + z)$,
2. Existe un elemento $0 \in K$ tal que $\bigwedge x \in K\, x + 0 = x$,
3. $\bigwedge x \in K \bigvee y \in K\,(x + y = 0)$,
4. $\bigwedge xy \in K\, x + y = y + x$,
5. $\bigwedge xyz \in K\,(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
6. $\bigwedge xyz \in K\, x \cdot (y + z) = x \cdot y + x \cdot z$,
7. Existe un elemento $1 \in K$ tal que $1 \neq 0 \wedge \bigwedge x \in K\, x \cdot 1 = x$,
8. $\bigwedge xy \in K\, x \cdot y = y \cdot x$,
9. $\bigwedge x \in K(x \neq 0 \to \bigvee y \in K(x \cdot y = 1))$,
10. $\bigwedge x \in K\, x \leq x$,
11. $\bigwedge xy \in K\,(x \leq y \wedge y \leq x \to x = y)$,
12. $\bigwedge xyz \in K\,(x \leq y \wedge y \leq z \to x \leq z)$,
13. $\bigwedge xy \in K\,(x \leq y \vee y \leq x)$,
14. $\bigwedge xyz \in K(x \leq y \to x + z \leq y + z)$,
15. $\bigwedge xy \in K(x \geq 0 \wedge y \geq 0 \to x \cdot y \geq 0)$.

Bourbaki llamaría a estas 15 afirmaciones los "axiomas" de la teoría de cuerpos ordenados, si bien, técnicamente, no son axiomas, sino parte de una definición en el seno de la teoría de conjuntos.[173] Ahora bien, estos "falsos axiomas" pueden convertirse en auténticos axiomas sin más que definir el *lenguaje formal de la teoría de cuerpos ordenados,* que es el lenguaje formal que, aparte de las variables y los signos lógicos, consta de los signos no definidos siguientes:

Constantes : $0, 1$,

Relatores diádicos $\leq$ (además del igualador $=$),

Funtores diádicos $+, \cdot$.

Declarar los signos $0, 1$ como constantes significa que los vamos a usar como nombres de objetos, declarar $\leq$ como un relator diádico significa que lo usaremos para construir fórmulas añadiéndole dos complementos, como $x \leq 1$ y declarar $+, \cdot$ como funtores diádicos signifca que los usaremos para nombrar un objeto a partir de otros dos dados, como $x + 1$, $x \cdot (y + 1)$.

Ahora, los axiomas anteriores pueden transformarse en sentencias de este lenguaje formal, concretamente en las que llamaremos *axiomas de la teoría de cuerpos ordenados:*

1. $\bigwedge xyz\,(x + y) + z = x + (y + z)$,
2. $\bigwedge x\, x + 0 = x$,
3. $\bigwedge x \bigvee y\, x + y = 0$,

[172]Para ser estrictos, un bourbakista quitaría todos los chirimbolitos lógicos de la definición (que nosotros hemos puesto para relacionar esta definición con la lógica, pero, si no fuera por ello, sin duda estarían de más), y además no daría todas las propiedades de golpe, sino que diría que $(K, +, \cdot)$ es un cuerpo, que $(K, \leq)$ es un conjunto totalmente ordenado y que además se cumplen las dos últimas propiedades de compatibilidad, donde a su vez, un cuerpo se define como un anillo conmutativo y unitario que cumple la propiedad 9, etc.

[173]Con esto no estamos sugiriendo que el uso de Bourbaki de la palabra "axioma" sea incorrecto o poco recomendable, sino que meramente recalcamos que no hay que confundir este sentido de la palabra "axioma" con su sentido en lógica.

4. $\bigwedge xy\, x + y = y + x$,
5. $\bigwedge xyz\, (x \cdot y) \cdot z = x \cdot (y \cdot z)$,
6. $\bigwedge xyz\, x \cdot (y + z) = x \cdot y + x \cdot z$,
7. $1 \neq 0 \wedge \bigwedge x\, x \cdot 1 = x$,
8. $\bigwedge xy\, x \cdot y = y \cdot x$,
9. $\bigwedge x(x \neq 0 \to \bigvee y(x \cdot y = 1))$,
10. $\bigwedge x\, x \leq x$,
11. $\bigwedge xy\, (x \leq y \wedge y \leq x \to x = y)$,
12. $\bigwedge xyz\, (x \leq y \wedge y \leq z \to x \leq z)$,
13. $\bigwedge xy\, (x \leq y \vee y \leq x)$,
14. $\bigwedge xyz(x \leq y \to x + z \leq y + z)$,
15. $\bigwedge xy(x \geq 0 \wedge y \geq 0 \to x \cdot y \geq 0)$.

Tenemos así unas sentencias "puramente formales" que no especifican en absoluto de qué objetos hablan. Si nos preguntan si son verdaderas o falsas, no podremos responder a menos que nos especifiquen:

0. De qué objetos estamos hablando, es decir, qué significa "$\bigwedge x$" (o qué significaría "$\bigvee x$", si hubiera alguno).
1. De entre todos esos objetos, cuáles son los que estamos llamando 0 y 1.
2. Dados dos de esos objetos x, y, qué quiere decir $x \leq y$.
3. Dados dos objetos x, y, a qué llamamos $x + y$ y a qué llamamos $x \cdot y$.

Sólo cuando esto esté especificado tendrá sentido plantearse si las sentencias anteriores son verdaderas o falsas. Pues esto justamente es el concepto de modelo de un lenguaje formal:

Un *modelo* del lenguaje formal de la teoría de cuerpos ordenados es un par (K, I), donde K es un conjunto no vacío e I es una aplicación que determina:

1. dos objetos $I(0), I(1) \in K$,
2. una relación $I(\leq) \subset K \times K$,
3. dos funciones $I(+), I(\cdot) : K \times K \longrightarrow K$.

Así pues, un modelo fija el conjunto K de los objetos en el que hay que interpretar los cuantificadores, así como los objetos, relaciones y funciones necesarios para interpretar cada signo del lenguaje.

Por aligerar la notación escribiremos $I(0) = \mathbf{0}$, $I(1) = \mathbf{1}$, es decir, que $\mathbf{0}$ y $\mathbf{1}$ son los significados de las constantes $0, 1$ en el modelo (K, I), e igualmente $\leq$ será la relación $I(\leq)$ que interpreta a $\leq$ en el modelo (K, I) y $+, \cdot$ serán las funciones que interpretan a $+, \cdot$.

En general, un *modelo* de un lenguaje formal está determinado por un conjunto M (llamado *universo* del modelo, y una aplicación de interpretación I que asigna a cada signo del lenguaje una interpretación, de un tipo u otro según la categoría del signo (a cada constante un objeto, a cada relator una relación, etc.).[174]

[174] Algunos libros de teoría de modelos prefieren definir el concepto de "estructura", que es un conjunto dotado de ciertas relaciones, funciones y elementos distinguidos, y definir luego que un modelo de un lenguaje formal es una estructura junto con una aplicación que asigna a cada signo del lenguaje uno de sus objetos. Por ejemplo, Tarski y Vaught lo hacen al revés: primero definen el concepto de estructura (y lo llaman "sistema relacional", porque sólo consideran relaciones) y asocian a cada sistema relacional una "teoría formal", que es un lenguaje formal con los signos necesarios para que se correspondan con las relaciones del sistema. Son distintas formas de plasmar la misma idea: tenemos lenguajes formales y estructuras, y cada lenguaje formal se puede interpretar en una estructura cuyas relaciones, funciones y objetos distinguidos se correspondan con los signos no definidos del lenguaje formal (es decir, que haya una relación n-ádica para cada relator n-ádico, una función n-ádica para funtor n-ádico y un objeto asociado a cada constante.)

Y, en estos términos, podemos decir que un cuerpo ordenado es un modelo de las 15 sentencias precedentes, es decir, un modelo del lenguaje formal de la teoría de cuerpos ordenados en el que las 15 sentencias son verdaderas.

Presentamos la definición de verdad de Tarski y Vaught generalizada a nuestro ejemplo, pero introduciendo además una notación que, al parecer, introdujo en su tesis doctoral Simon Bernahrd Kochen, nacido en Bélgica en 1934, pero cuya familia huyó a Gran Bretaña (y luego a Canadá) cuando los nazis invadieron su país. En **1958** se doctoró bajo la dirección de Church con la tesis titulada *Productos con ultrafiltros y extensiones aritméticas,* cuyos resultados publicaría más tarde, en 1961 en un artículo titulado *Ultraproductos en la teoría de modelos,* probablemente el primer trabajo que trata plenamente la teoría de modelos al estilo algebraico moderno.

Fijado un modelo (K, I) del lenguaje formal de la teoría de cuerpos ordenados, una *valoración* v en el modelo es una aplicación que a cada variable le asigna un objeto de K.

Definimos el *objeto denotado*[175] por un término[176] t del lenguaje respecto de una valoración v como el objeto $K(t)[v]$ calculado a partir de las reglas siguientes:

1. Si $t \equiv x$ es una variable, $K(x)[v] = v(x)$ (es decir, el objeto denotado por una variable es el que le asigna la valoración v).
2. Si $t \equiv 0, 1$ es una constante, entonces $K(0)[v] = \mathbf{0}$, $K(1)[v] = \mathbf{1}$ (el objeto denotado por una constante es el objeto que le asigna el modelo).
3. Si $t \equiv t' + t''$ o $t \equiv t' \cdot t''$, entonces

$$K(t' + t'')[v] = K(t')[v] + K(t'')[v], \qquad K(t' \cdot t'')[v] = K(t')[v] \cdot K(t'')[v]$$

(el objeto denotado por $t + t'$ es el que resulta de aplicar la interpretación de $+$ dada por el modelo a los objetos denotados por t' y t'', e igualmente con $t' \cdot t''$).

Se dice que una fórmula α *es satisfecha* por el modelo respecto de v (y se representa $K \vDash \alpha[v]$) si se puede justificar a partir de las reglas siguientes:

1. $K \vDash (t_1 = t_2)[v]$ si y sólo si $K(t_1)[v] = K(t_2)[v]$ (una fórmula de tipo $t_1 = t_2$ es satisfecha cuando sus dos miembros denotan el mismo objeto).
2. $K \vDash (t_1 \leq t_2)[v]$ si y sólo si $K(t_1)[v] \leq K(t_2)[v]$ (una fórmula de tipo $t_1 \leq t_2$ es satisfecha si los objetos denotados por sus miembros satisfacen la relación $\leq$ que el modelo asocia a $\leq$).
3. $K \vDash \neg\alpha[v]$ si y sólo si no $K \vDash \alpha[v]$ (una fórmula de tipo $\neg\alpha$ es satisfecha si α no es satisfecha).
4. $K \vDash (\alpha \to \beta)[v]$ si y sólo si no $K \vDash \alpha[v]$ o bien $K \vDash \beta[v]$ (una fórmula de tipo $\alpha \to \beta$ es satisfecha si su antecedente no es satisfecho o su consecuente sí que lo es, o, dicho de otro modo, si cuando se satisface su antecedente se satisface también su consecuente).
5. $K \vDash (\alpha \vee \beta)[v]$ o $K \vDash (\alpha \wedge \beta)[v]$ si $K \vDash \alpha[v]$ y/o $K \vDash \beta[v]$.
6. $K \vDash (\alpha \leftrightarrow \beta)[v]$ si y sólo si $K \vDash \alpha[v]$ y $K \vDash \beta[v]$, o bien no $K \vDash \alpha[v]$ y no $K \vDash \beta[v]$ (una equivalencia es satisfecha cuando sus dos miembros son satisfechos o ambos no son satisfechos).
7. $K \vDash \bigwedge x\alpha(x)[v]$ si para todo elemento a en K, se cumple $K \vDash \alpha(x)[v_x^a]$, donde v_x^a es la valoración que coincide con v salvo que la variable x tiene asignado el valor a. (Una fórmula $\bigwedge x\,\alpha(x)$ es satisfecha si la fórmula $\alpha(x)$ es satisfecha con cualquier interpretación que se le dé a la variable x.)
8. $K \vDash \bigvee x\alpha(x)[v]$ si existe un elemento a en K tal que $K \vDash \alpha(x)[v_x^a]$. (Una fórmula $\bigvee x\,\alpha(x)$ es satisfecha si la fórmula $\alpha(x)$ es satisfecha si elegimos adecuadamente la interpretación que le damos a la variable x.)

Una fórmula α es *verdadera* en el modelo,[177] y se representa por $K \vDash \alpha$, si es satisfecha con cualquier valoración en el modelo, y es falsa si no es satisfecha con ninguna valoración.

[175] Toda esta parte no aparece en la definición de Tarski y Vaught porque sólo consideran lenguajes con relatores, sin constantes ni funtores.

[176] Un término es una cadena de signos construida a partir de variables y constantes mediante la aplicación de funtores.

[177] Tarski y Vaught sólo definen el concepto de verdad para sentencias, y señalan que una sentencia es satisfecha por una valoración si y sólo si es satisfecha por todas. Esto se debe a que la denotación y satisfacción sólo dependen del significado que se atribuye a las variables libres en la expresión analizada, por lo que si no hay variables libres, la asignación de significado a las variables es irrelevante.

Esta definición puede parecer sofisticada, pero simplemente expresa que una sentencia es verdadera si cuando leemos lo que dice como hacemos normalmente (sin pensar en esta definición), lo que entendemos es verdad.

Por ejemplo, consideremos el modelo formado por el conjunto $\mathbb{R}$ de los números reales donde cada signo se interpreta de la forma usual (la suma es la suma usual de números reales, etc.). Entonces, se cumple que

$$\mathbb{R} \vDash \bigwedge xy(x \geq 0 \wedge y \geq 0 \to x \cdot y \geq 0).$$

Hay dos formas de comprobar esto: una es leer lo que pone y entender que dice que, si x, y son dos números reales mayores o iguales que 0, su producto también es mayor o igual que 0, lo cual es verdad. La otra forma es aplicar las definiciones precedentes, que es un camino más largo, pero lleva a la misma conclusión.

Ejemplo Como ilustración, vamos a comprobar que el significado de esta sentencia es el que hemos dicho aplicando la definición de Tarski de "verdad". Observemos, ante todo, que $\bigwedge xy$ es una abreviatura de $\bigwedge x \bigwedge y$. Fijamos una valoración v, es decir, un criterio que asigne un número real a cada variable.

1. $\mathbb{R} \vDash \bigwedge x \bigwedge y(x \geq 0 \wedge y \geq 0 \to x \cdot y \geq 0)[v]$ significa que, para todo número real a, se cumple
$$\mathbb{R} \vDash \bigwedge y(x \geq 0 \wedge y \geq 0 \to x \cdot y \geq 0)[v_x^a].$$
2. A su vez, esto significa que, para todo número real b, se cumple
$$\mathbb{R} \vDash (x \geq 0 \wedge y \geq 0 \to x \cdot y \geq 0)[v_{xy}^{ab}].$$
3. Esto significa que, si se cumple $\mathbb{R} \vDash (x \geq 0 \wedge y \geq 0)[v_{xy}^{ab}]$, se tiene que cumplir también $\mathbb{R} \vDash (x \cdot y \geq 0)[v_{xy}^{ab}]$.
4. Esto significa que si se cumple $\mathbb{R} \vDash (x \geq 0)[v_{xy}^{ab}]$ y $\mathbb{R} \vDash (y \geq 0)[v_{xy}^{ab}]$, entonces $\mathbb{R} \vDash (x \cdot y \geq 0)[v_{xy}^{ab}]$.
5. Esto significa que si $\mathbb{R}(x)[v_{xy}^{ab}] \geq \mathbb{R}(0)[v_{xy}^{ab}]$ y $\mathbb{R}(y)[v_{xy}^{ab}] \geq \mathbb{R}(0)[v_{xy}^{ab}]$, entonces $\mathbb{R}(x \cdot y)[v_{xy}^{ab}] \geq \mathbb{R}(0)[v_{xy}^{ab}]$,
6. o también que si $\mathbb{R}(x)[v_{xy}^{ab}] \geq \mathbb{R}(0)[v_{xy}^{ab}]$ y $\mathbb{R}(y)[v_{xy}^{ab}] \geq \mathbb{R}(0)[v_{xy}^{ab}]$, entonces $\mathbb{R}(x)[v_{xy}^{ab}] \cdot \mathbb{R}(y)[v_{xy}^{ab}] \geq \mathbb{R}(0)[v_{xy}^{ab}]$,
7. o también que si $v_{xy}^{ab}(x) \geq 0$ y $v_{xy}^{ab}(y) \geq 0$, entonces $v_{xy}^{ab}(x) \cdot v_{xy}^{ab}(y) \geq 0$,
8. o también que si $a \geq 0$ y $b \geq 0$, entonces $ab \geq 0$.

En total, la sentencia significa que, para todo par de números reales a y b, si se cumple $a \geq 0$ y $b \geq 0$, entonces $ab \geq 0$. Como esto es cierto, pues la sentencia es verdadera en el modelo, cosa que ya sabíamos sin más que "haberla leído". ∎

En general, podemos comprobar (así o simplemente leyendo) que $\mathbb{R}$ cumple los 15 axiomas de la teoría de cuerpos ordenados y, más en general, que los modelos que cumplen los axiomas de la teoría de cuerpos ordenados no son ni más ni menos que los cuerpos ordenados, porque, si leemos los axiomas, veremos que no dicen ni más ni menos que lo que exige la definición de cuerpo ordenado. De este modo, hemos transformado unos axiomas en el sentido bourbakista de "condiciones que se exigen en una definición de estructura" a axiomas en el sentido lógico de la palabra, axiomas de una teoría axiomática de los que podemos deducir consecuencias formalmente.

Por ejemplo, si llamamos CO a la teoría de cuerpos ordenados, se puede probar que

$$\underset{\text{CO}}{\vdash} \bigwedge xy(xy = 0 \to x = 0 \vee y = 0),$$

en el sentido de que existe una demostración formal de esta sentencia a partir de los axiomas. A su vez, esto se traduce en que si K es cualquier cuerpo ordenado, se cumple que

$$K \vDash \bigwedge xy(xy = 0 \to x = 0 \vee y = 0),$$

porque las demostraciones formales se definen de modo que si parten de premisas verdaderas, llegan siempre a conclusiones verdaderas.[178]

Por curiosidad copiamos aquí la definición de "verdad" tal y como la dio Tarski en 1933:

[178] Este trabajo de Kochen parece ser la primera publicación en la que apareció el signo $\vDash$, y hay quienes le atribuyen su invención. Kochen (que ha cumplido 91 años pocos días antes de que estas líneas fueran escritas), declara que no recuerda si inventó él el signo $\vDash$ o si lo copió de algún sitio, pero el hecho es que lo usó Kleene en el curso que dio en 1956.

> *La sucesión f satisface la función proposicional x si y sólo si tenemos fRx para cada relación R que satisface la siguiente condición:*
>
> *Para cualquier g e y, para que gRy es necesario y suficiente que g sea una sucesión infinita de clases, y sea una función proposicional y (α) existan números naturales k y l tales que $y = \iota_{k,l}$, y $g_k \subset g_l$ o (β) exista una función proposicional z tal que $y = \bar{z}$ y la fórmula gRz no se cumpla; o (γ) existan funciones proposicionales z y t tales que $y = z + t$ y gRz o gRt; o finalmente (δ) exista un número natural k y una función proposicional z tal que $y = \bigcap_k z$ y hRz para cada sucesión infinita h que difiere de g a lo sumo en el lugar k-ésimo.*

Antes de seguir avanzando en la descripción de los conceptos básicos de la teoría de modelos, hay un punto que el lector debería tener claro desde un principio: como toda la lógica, la teoría de modelos puede estudiarse desde un marco metamatemático intuitivo, o en el seno de una teoría axiomática formal, preferentemente una teoría de conjuntos.

Si analizamos la definición de "modelo", vemos que un modelo es un conjunto en el que se han fijado unas relaciones y funciones. Podría pensarse que nada de esto tiene sentido si no es en el marco de una teoría de conjuntos o, por lo menos, aunque uno crea en la existencia de "los conjuntos", que no podemos permitirnos el lujo de razonar sobre conjuntos, relaciones, funciones, etc. si no es en el marco de una teoría axiomática formal, pues precisamente para eso se han inventado las teorías de conjuntos, para hablar de conjuntos sin caer en contradicciones inexplicables.

Ahora bien, salvo que uno sea un finitista muy, muy radical, que no le encuentre sentido a nada que involucre conjuntos infinitos, es razonable admitir que sí que podemos hablar intuitivamente con rigor, sabiendo de lo que estamos hablando, sin riesgo de caer en contradicciones, de algunos conjuntos infinitos. Por ejemplo, no hace falta ninguna teoría axiomática para afirmar que los números naturales (que son un conjunto perfectamente determinado en términos intuitivos y, de hecho, mucho mejor determinado, como mostró Skolem, de lo que puede determinarse con cualquier teoría axiomática), con la suma y el producto de números naturales, que son dos funciones definidas en el conjunto de los números naturales, también determinadas perfectamente en términos intuitivos, forman un modelo de la aritmética de Peano, lo que nos permite concluir que es consistente.

Más aún, los números racionales están tan bien determinados intuitivamente como los números naturales, y podemos afirmar, siempre en términos intuitivos, que el cuerpo ordenado de los números racionales (cuyas operaciones y cuya relación de orden se pueden definir perfectamente en términos intuitivos) son un modelo de la teoría axiomática CO, por lo que ésta es consistente.

De hecho, tanto los números racionales (con sus operaciones) como la teoría CO pueden definirse en la Aritmética Recursiva Primitiva. Lo que no puede definirse en ella es la relación $\mathbb{Q} \vDash \alpha[v]$, pues se trata de una definición recurrente que necesita tratar de forma esencial con el conjunto infinito (numerable) de todas las valoraciones definidas al menos sobre un conjunto finito de variables, y eso excede las capacidades de ARP, pero eso sólo significa que el concepto de satisfacción no es finitista en el sentido más estricto de la palabra, no que sea inmanejable en términos intuitivos.

Concebir intuitivamente (al menos la parte más básica de) la teoría de modelos no es un capricho. Por ejemplo, el teorema de completitud de Gödel perdería una parte crucial de su valor si se considerara como un mero teorema de ZFC. Aunque también puede concebirse como tal y tiene interés concebirlo como tal, buena parte de su relevancia reside en que también puede verse como una afirmación general sobre el cálculo deductivo que, en particular, es aplicable a ZFC "desde fuera". Recordemos su enunciado:[179]

> **Teorema de completitud semántica** Si Γ es una colección de fórmulas de un lenguaje formal y $\Gamma \vDash \alpha$ (es decir, α es verdadera en todos los modelos de Γ de universo numerable) entonces $\Gamma \vDash \alpha$ (es decir, α se puede deducir lógicamente de Γ).

Recordemos que Hilbert y Ackerman lo formularon para modelos arbitrarios, pero al restringir la hipótesis a modelos numerables estamos pasando a una afirmación más fuerte (que fue la que demostró Gödel) y así posibilitamos que pueda ser concebido intuitivamente, pues no podemos hablar intuitivamente de modelos arbitrarios, no necesariamente numerables.

Antes de plantearnos si este resultado es cierto o no, la pregunta es si podemos asignarle un significado intuitivo o no. Y la respuesta *a priori* sería que no. ¿Cómo hay que entender que una fórmula α sea verdadera

[179] Véase la página 81, donde está enunciado sin nombre, porque todavía no era más que una conjetura.

en *todos* los modelos numerables de Γ? Decir que una propiedad la cumplen *todos* los números naturales tiene pleno sentido intuitivo, pues significa que la cumple el 0, y el 1, y el 2, etc., con independencia de que sepamos o no cómo verificarlo. Pero, ¿qué significa que una propiedad la cumplan *todos* los modelos numerables de Γ. No tenemos nada que se parezca a una representación intuitiva de la totalidad de los modelos numerables de Γ, como para que podamos asegurar que una afirmación sobre tal totalidad tiene que tener un significado y que, en particular, o es verdadera, o es falsa.

Pero el enunciado del teorema de incompletitud adquiere pleno sentido intuitivo *a posteriori,* es decir, tras conocer su demostración, pues la demostración (hemos visto una en la sección 73) consiste en un método para definir de una forma intuitivamente bien determinada (aunque no efectiva) cómo construir un modelo en concreto de Γ que no cumple α bajo el supuesto de que α no es deducible de Γ. Decir que si α no es deducible a partir de Γ existe un modelo de Γ en el que α es falsa, no en el sentido de que "existe" vaya usted a saber dónde, sino en el de que podemos construir uno explícitamente (aunque no efectivamente) tiene pleno sentido intuitivo. Dicho modelo consiste en unos objetos que podemos definir sin necesidad de fiarnos de los axiomas de ninguna teoría de conjuntos y de unas relaciones y funciones que podemos definir explícitamente sobre esos objetos, sin construcciones impredicativas sospechosas, para las que no se echa de menos a la teoría de conjuntos formal, por más que estemos hablando de conjuntos, relaciones y funciones.

Por ello, podemos concluir que el teorema de completitud —entendido en términos intuitivos— nos garantiza que nuestro concepto de cálculo deductivo es justo lo que tiene que ser, en cuanto que no permite deducir ni más ni menos que lo que es lícito deducir de unas premisas, lo que es necesariamente cierto cuando las premisas son ciertas.

Pero, más allá de algunos usos esencialmente metamatemáticos de la teoría de modelos, ésta se presta a desarrollarse en el seno de la teoría de conjuntos como una teoría matemática más y, en cierto sentido, como una teoría que permite tratar de forma unificada todas las estructuras algebraicas en el sentido bourbakista, pues, igual que hemos definido la "teoría de los cuerpos ordenados", podemos definir la "teoría de grupos", la "teoría de anillos", la "teoría de anillos conmutativos y unitarios", la "teoría de los conjuntos parcialmente ordenados", la "teoría de las álgebras de Boole", etc., cada una con su lenguaje formal y sus axiomas correspondientes. Ahora bien, esto requiere un matiz para ser bien entendido.

Sería un error pensar que, por ejemplo, estudiar la teoría de cuerpos ordenados desde el punto de vista de la teoría de la demostración o de la teoría de modelos (en el seno de ZFC) es equivalente a lo que hacen los algebristas cuando estudian los cuerpos ordenados en ZFC. No es lo mismo porque la expresividad de los lenguajes formales es limitada, y no pueden plasmar cualquier cosa que un algebrista pueda definir sobre las estructuras que maneja.

Por ejemplo, un algebrista puede definir un cuerpo ordenado *pitagórico* como un cuerpo en el que toda suma de cuadrados es un cuadrado. Esta propiedad puede expresarse en CO mediante la sentencia[180]

$$\bigwedge xy \bigvee z(x \cdot x + y \cdot y = z \cdot z)$$

y podemos observar que es verdadera en $\mathbb{R}$, pero es falsa en $\mathbb{Q}$.

En cambio, un algebrista puede definir un cuerpo ordenado completo como un cuerpo ordenado K tal que todo subconjunto $X \subset K$ no vacío y acotado superiormente tiene supremo, pero esta propiedad no es expresable en la teoría CO. Lo más parecido a una definición de completitud sería esto:

$$\bigwedge X(\bigvee x\, x \in X \wedge \bigvee c \bigwedge x(x \in X \to x \leq c) \to \bigvee s(\bigwedge x(x \in X \to x \leq s) \wedge \bigwedge c(\bigwedge x(x \in X \to x \leq c) \to s \leq c)))$$

Ahí dice que, para todo subconjunto X del cuerpo, si no es vacío y tiene una cota superior c, entonces existe un s que es cota superior de X y es menor o igual que cualquier cota superior de X.

Pero para enunciar esto hemos tenido que suponer que hay dos clases de variables, las variables de primer orden, como x o c, que varían en los elementos del cuerpo, y las variables de segundo orden, como X, que varían en todos los subconjuntos del cuerpo. Y además necesitamos un relator $\in$ que establezca la pertenencia de un objeto de primer orden a uno de segundo orden. Pero nada de esto está en nuestro lenguaje formal de la teoría de cuerpos ordenados. Estamos considerando *lenguajes de primer orden,* que sólo tienen variables de primer orden que recorren objetos, pero no variables de segundo orden que recorran conjuntos de objetos.

[180] Obviamente, nada impide introducir la notación $x^2 = x \cdot x$ y expresar la propiedad de forma más natural.

Esto se expresa diciendo que la completitud de un cuerpo ordenado es una *propiedad de segundo orden,* que no puede expresarse mediante un lenguaje formal de primer orden, sino que requiere de una variable de segundo orden que recorra todos los posibles conjuntos de objetos (en este caso, todos los posibles subconjuntos del cuerpo).[181]

Por ello, lo que hemos llamado teoría de cuerpos ordenados, a veces se llama la *teoría elemental de cuerpos ordenados,* porque sólo estudia las *afirmaciones elementales* sobre cuerpos ordenados, es decir, las que pueden expresarse mediante un lenguaje de primer orden (cuyas variables están restringidas a los elementos del cuerpo). Así, por ejemplo, el carácter pitagórico de un cuerpo es una propiedad elemental de los cuerpos ordenados, mientras que la completitud no lo es.

Hechos estas matizaciones, seguimos comentando los aspectos más destacados del artículo de Tarski y Vaught y del de Kochen. Es el segundo quien define explícitamente os conceptos de *submodelo,*[182] *homomorfismo de modelos, isomorfismo de modelos* e *inmersión de modelos.*

Submodelos Concretamente, si M y N son dos modelos del mismo lenguaje formal (o, en otros términos, dos estructuras similares, es decir, con el mismo tipo de relaciones, funciones, etc., por ejemplo, ambas con dos relaciones diádicas y tres funtores monádicos, etc.) se dice que M es un submodelo de N si $M \subset N$, ambos interpretan las constantes igual, cada relación en M es la restricción de la relación correspondiente en N y cada función de M es la restricción de la función correspondiente de N. ∎

Por ejemplo, si hablamos de modelos del lenguaje de la teoría de cuerpos ordenados, para que (M, I) sea un submodelo de (N, I') hace falta que:

1. $I(0) = I'(0)$, $I(1) = I'(1)$ (lo cual a su vez requiere que $I'(0), I'(1) \in M$),
2. Para todo par de elementos $a, b \in M$, se cumple:
   (a) $I(\leq)(a, b)$ si y sólo si $I'(\leq)(a, b)$,
   (b) $I(+)(a, b) = I'(+)(a, b)$, $\quad I(\cdot)(a, b) = I'(\cdot)(a, b)$ (la suma y el producto se calculan igual en M que en N, lo que en particular requiere que al sumar en N elementos de M, la suma esté en M).

De este modo, un submodelo es simplemente un subconjunto cerrado para las operaciones algebraicas. Si además M y N son modelos de la teoría de cuerpos ordenados (es decir, de sus axiomas, no sólo de su lenguaje), esto equivale a que M sea un subcuerpo de N en el sentido algebraico usual.

Inmersiones Similarmente, un *homomorfismo* $i : M \longrightarrow N$ entre dos modelos de un mismo lenguaje formal es una aplicación que conserva todas las interpretaciones. Por ejemplo, en el caso del lenguaje de la teoría de cuerpos ordenados, esto se reduce a

1. $i(\mathbf{0}) = \mathbf{0}, \qquad i(\mathbf{1}) = \mathbf{1}$,
2. $\bigwedge ab \in M(a = b \leftrightarrow i(a) = i(b))$,
3. $\bigwedge ab \in M(a \leq b \leftrightarrow i(a) \leq i(b))$,
4. $\bigwedge ab \in M(i(a + b) = i(a) + i(b) \wedge i(a \cdot b) = i(a) \cdot i(b))$.

Observemos que, si consideramos siempre lenguajes formales con igualador, el cual se interpreta como la relación de igualdad en el modelo, en todos los casos tendremos la propiedad 2, que se traduce en que todos los homomorfimos de modelos son inyectivos, y por eso se llaman *inmersiones.* Las inmersiones biyectivas son *isomorfismos.* ∎

[181] Pero, a su vez, esto también hay que entenderlo bien. No se puede deducir de aquí que, puesto que en ZFC sí que es posible definir los cuerpos ordenados completos, eso significa que la lógica de ZFC es de segundo orden. Esto no es cierto. ZFC es una teoría axiomática formal de primer orden, porque sólo admite un tipo de variables, las cuales recorren los (presuntos) objetos de la teoría, que son los conjuntos. Hay que entender que la completitud es una propiedad de segundo orden porque *cuando nos limitamos a considerar un lenguaje de primer orden cuyas variables estén restringidas a los elementos del cuerpo,* es decir, cuando establecemos que "para todo" significa "para todo elemento del cuerpo", es imposible expresar en él la completitud. ZFC es una teoría de primer orden, pero en ella "para todo" no significa "para todo elemento de un cuerpo prefijado", sino "para todo conjunto", y los conjuntos pueden recorrer tanto los elementos de un cuerpo como sus subconjuntos.

[182] Kochen habla de sistemas, subsistemas, etc., pero es lo mismo. Por otro lado, sólo considera sistemas con relaciones, sin funciones ni objetos distinguidos que interpreten constantes.

Inmersiones elementales Pero las inmersiones y los isomorfismos no son las aplicaciones realmente interesantes entre modelos. Kochen introduce el concepto de *inmersión elemental* $i : M \longrightarrow N$, que es una inmersión tal que, para toda fórmula $\phi(x_1, \ldots, x_n)$ del lenguaje formal y para todos los objetos $a_1, \ldots, a_n \in M$, se cumple que[183]

$$M \vDash \phi[a_1, \ldots, a_n] \leftrightarrow N \vDash \phi[i(a_1), \ldots, i(a_n)].$$

Es decir, una inmersión elemental, no sólo conserva los conceptos básicos que definen la estructura, sino todas las propiedades elementales de la estructura, es decir, todas las propiedades expresables mediante las fórmulas (de primer orden) del lenguaje formal asociado a ellas.

Se dice que M es un *submodelo elemental* de un modelo N, y se representa por $M \prec N$, si es un submodelo tal que la inclusión $i : M \longrightarrow N$ es una inmersión elemental. También se dice entonces que N es una *extensión elemental* de M.

Dos modelos se dicen *elementalmente equivalentes*[184] si satisfacen las mismas sentencias. En particular, si existe una inmersión elemental entre dos modelos, éstos son elementalmente equivalentes, pues basta aplicar la definición de inmersión elemental al caso de las sentencias ($n = 0$).

Por ejemplo, la inclusión $i : \mathbb{Q} \longrightarrow \mathbb{R}$ es una inmersión, pero no es una inmersión elemental, pues $\mathbb{Q}$ y $\mathbb{R}$, aunque cumplen ambos los axiomas de la teoría de cuerpos ordenados, no cumplen las mismas sentencias (no son elementalmente equivalentes). Por ejemplo, difieren en ésta:

$$\bigvee x\, x \cdot x = 1 + 1.$$

Un resultado notable que aparece por primera vez en el artículo de Tarski y Vaught es lo que hoy se conoce como *criterio de Tarski-Vaught.* Observemos que, en principio, para que un submodelo M de un modelo N sea un submodelo elemental, lo que tiene que suceder es que:

> Para toda fórmula $\phi(x_1, \ldots, x_n)$ y todos los elementos $a_1, \ldots, a_n \in M$, se cumple:
>
> $$M \vDash \phi[a_1, \ldots, a_n] \leftrightarrow N \vDash \phi[a_1, \ldots, a_n].$$

Sin embargo:

> **Criterio de Tarski-Vaught** Si N es un modelo de un lenguaje formal y $M \subset N$ es un submodelo, se cumple que M es un submodelo elemental de N si y sólo si, para toda fórmula $\phi(x_0, x_1, \ldots, x_n)$ y todos los elementos $a_1, \ldots, a_n \in M$, se cumple que
>
> $$\bigvee a \in N\, N \vDash \phi[a, a_1, \ldots, a_n] \to \bigvee a \in M\, N \vDash \phi[a, a_1, \ldots, a_n].$$

Es decir, la condición se reduce a que si existe un objeto a en N que cumple una fórmula con parámetros en M, se puede encontrar uno de tales objetos a en M, pero en este criterio sólo interviene la satisfacción en N, al contrario que en la definición, donde intervienen tanto la satisfacción en N como en M.

Esto simplifica drásticamente la construcción de submodelos elementales. El enunciado siguiente es una leve variante de un enunciado de Tarski y Vaught, con la misma demostración (salvo una variante para admitir lenguajes con funtores):

> **Teorema** Si M es un modelo infinito de un lenguaje formal y $X \subset M$, entonces existe un submodelo elemental $X \subset N(X) \prec M$ tal que $|N(X)| \leq \aleph_0 |X|$ y que recibe el nombre de *núcleo de Skolem* de X en M.

Demostración: Llamamos X_0 a la unión de X y las interpretaciones en M de todas las constantes del lenguaje formal, que es un conjunto a lo sumo numerable X_0, pues a lo sumo hay una cantidad numerable de constantes. Si es finito, lo extendemos como sea para que sea infinito numerable. Supongamos definido $X_k \subset M$ con el mismo cardinal que X y entonces tomamos como X_{k+1} el conjunto que resulta de añadir a X_k los objetos siguientes:

[183] Aquí usamos la notación $M \vDash \alpha[a_1, \ldots, a_n]$ para indicar que $M \vDash \alpha[v]$, donde v es cualquier valoración que cumpla $v(x_i) = a_i$.

[184] Tarski y Vaught hablan de modelos elementalmente equivalentes y de extensiones elementales, pero no llegan a introducir el concepto de inmersión elemental. Además, dicen "aritméticamente equivalentes" y "extensiones aritméticas", pero finalmente se impondría el término "elemental".

1. Para cada función n-ádica que interprete en M un funtor n-ádico del lenguaje formal y cada n-tupla $(a_1, \ldots, a_n) \in X_k$, incluimos $f(a_1, \ldots, a_n)$ en X_{k+1}.

2. Para cada fórmula $\phi(x_0, x_1, \ldots, x_n)$ con al menos una variable libre y cada n-tupla $(a_1, \ldots, x_n) \in X_k$, en el caso de que exista un $a \in M$ que cumpla $M \vDash \phi(a, a_1, \ldots, a_n)$, elegimos uno y lo incluimos en X_{k+1}.

Es fácil ver que, con estos añadidos, teniendo en cuenta que sólo hay una cantidad numerable de funtores y de fórmulas que considerar, el cardinal de X_{k+1} sigue siendo el de X_0.

Finalmente, llamamos $N(X)$ a la unión de todos los conjuntos X_k. Así $|N(X)| = |X|$ y, por construcción, $N(X)$ contiene a todas las interpretaciones de las constantes, y si f es una función n-ádica que interpreta a un funtor del lenguaje y $a_1, \ldots, a_n$ son elementos de $N(X)$, estarán en un X_k, con lo que $f(a_1, \ldots, a_n)$ está en X_{k+1}, luego en $N(X)$. Esto basta para concluir que $N(X)$ es un submodelo de M.

Y, dada una fórmula $\phi(x_0, x_1, \ldots, x_n)$ y unos parámetros $a_1, \ldots, a_n \in N(X)$, éstos estarán en un X_k, luego si existe un $a \in M$ tal que $M \vDash \phi[a, a_1, \ldots, a_n]$, uno de tales a estará en X_{k+1}, luego en $N(X)$, y el criterio de Tarski-Vaught implica que $N(X)$ es un submodelo elemental de M. ∎

Esto implica la versión de Henkin del teorema de Löwenheim-Skolem formulado en la página 171.

En 1957 se había doctorado bajo la dirección de Tarski un filósofo llamado Richard Montague, con la tesis titulada *Contribuciones a la fundamentación axiomática de la teoría de conjuntos.* En ella demostraba que ZFC no es finitamente axiomatizable. El argumento requiere unos resultados que fueron publicados en **1959** por Montague y Vaught en un artículo titulado *Modelos naturales de teorías de conjuntos.* En el estudian la jerarquía acumulativa $\{V_\alpha\}_\alpha$ de von Neumann.

En el supuesto de que exista un cardinal fuertemente inaccesible, podemos tomar el mínimo de ellos, digamos θ. Zermelo ya había señalado que V_θ es un modelo de ZFC. Más aún, se puede demostrar que θ es el mínimo ordinal tal que $V_{\theta+1}$ es un modelo de NBG. Sin embargo:

> *Nuestro resultado principal en este artículo es que, por otro lado, existen ordinales $\theta' < \theta$ tales que $V_{\theta'}$ es un modelo de* ZF. *(Luego, la afirmación, que a veces se ha hecho, de que los axiomas de* ZF *aseguran la existencia de todos los "ordinales accesibles" se diría que es injustificada.)*

Montague y Vaught trabajan sin el axioma de elección, pero el resultado vale sin cambio alguno con el axioma de elección y así es incluso más fuerte.

Cardinales sin el axioma de elección Incidentalmente, para trabajar sin el axioma de elección muestran una forma de definir el concepto de "cardinal" en ZF. Recordemos que al principio de la sección 35 hemos señalado que esto era un problema, pues a la hora de definir el cardinal de un conjunto no podemos usar un ordinal equipotente (ya que un conjunto no es biyectable con un ordinal si no puede ser bien ordenado) ni tampoco definirlo como el conjunto de todos los conjuntos equipotentes a él, porque no existe tal conjunto. La solución de Montague y Vaught es definir el cardinal de un conjunto x como el conjunto $\bar{\bar{x}}$ de todos los conjuntos y equipotentes a x de rango mínimo, donde el rango de y es el menor ordinal α tal que $y \subset V_\alpha$. De este modo $\bar{\bar{x}}$ es un subconjunto de $V_{\alpha+1}$ y se cumple que dos conjuntos son equipotentes si y sólo si tienen el mismo cardinal, que es lo único que se requiere para que un concepto de "cardinal de un conjunto" se comporte según lo esperado. ∎

Pero, volviendo al objetivo del trabajo, la idea de fondo es muy simple:

> *Vamos a ver que, bajo ciertas circunstancias, un modelo V_λ de* ZF *es una extensión elemental de un modelo menor $V_{\lambda'}$. A grandes rasgos, esto puede verse como sigue: En las pruebas del teorema de Löwenheim-Skolem (como la de Tarski y Vaught) el universo B del submodelo de V_λ se construye en un número infinito de pasos, uno elige y pone en B un elemento con una determinada propiedad. Aquí seguimos el mismo procedimiento, pero, en cada paso, tomamos como γ el menor ordinal tal que un $x \in V_\gamma$ tiene la propiedad en cuestión, y ponemos todos los elementos de V_γ en B.*

Luego de decir que ésta es la idea, anuncian que van a probar el resultado por otro camino, pero nosotros vamos a explicar esta idea, que es conceptualmente más simple. Montague y Vaught demuestran resultados más detallados, pero aquí nos conformamos con el principal:

> **Teorema** Si θ es un cardinal fuertemente inaccesible y $\alpha < \theta$, existe un ordinal $\alpha \leq \theta' < \theta$ tal que $V_{\theta'}$ es un submodelo elemental de V_θ.

DEMOSTRACIÓN: Sólo tenemos que imitar la prueba del teorema precedente, simplificada por el hecho de que ahora consideramos modelos del lenguaje de la teoría de conjuntos, que no tiene constantes ni funtores. Partimos de $X_0 = V_\alpha$ y, supuesto construido $X_k = V_{\alpha_k}$, con $\alpha_k < \theta$, construimos como sigue $X_{k+1} = V_{\alpha_{k+1}}$:

Para cada fórmula $\phi(x_0, \ldots, x_n)$ y cada n-tupla $(a_1, \ldots, a_n) \in X_{k+1}$, si $\bigvee a \in V_\theta\, \phi(a, a_1, \ldots, a_n)$, elegimos el menor ordinal $\delta < \theta$ tal que $\bigvee a \in V_\delta\, \phi(a, a_1, \ldots, a_n)$ (recordemos que V_θ es la unión de los V_δ, con $\delta < \theta$). Con esto obtenemos un conjunto $A \subset \theta$ de ordinales δ elegidos de este modo, y el cardinal de A es a lo sumo el de V_{α_k}. El hecho de que θ sea fuertemente inaccesible se traduce en que el cardinal de cualquier V_α con $\alpha < \theta$ es estrictamente menor[185] que el cardinal de V_θ, que es θ. La inaccesibilidad implica tambien que, si tomamos como α_{k+1} el supremo de A, se cumple que $\alpha_{k+1} < \theta$, así como que si llamamos θ' al supremo de los ordinales α_k, se sigue cumpliendo que $\theta' < \theta$, y entonces $V_{\theta'}$ cumple lo requerido, exactamente por el mismo argumento que en el teorema de Tarski-Vaught que hemos visto antes. ∎

En particular $V_{\theta'}$ cumple las mismas sentencias que V_θ, luego también es un modelo[186] de ZFC (el argumento anterior no requiere el axioma de elección, porque, en lugar de elegir ejemplos, elegimos ordinales, pero si suponemos el axioma de elección, entonces V_θ es un modelo de ZFC, mientras que sin él sólo lo es de ZF).

85 El teorema de reflexión Pero Montague y Vaught llevan esta idea mucho más allá, y la aplican incluso a la clase universal V, en lugar de a un V_θ. Esto es delicado y, de hecho, dan muchos rodeos para enunciarlo sin pillarse los dedos. Lo que no se puede decir es que existe un ordinal λ tal que $V_\lambda \prec V$, y no se puede decir porque no se puede enunciar. No podemos afirmar que, para toda fórmula $\phi(x_1, \ldots, x_n)$, y todos los $a_1, \ldots, a_n \in V_\lambda$, se cumple

$$V_\lambda \vDash \phi[a_1, \ldots, a_n] \leftrightarrow V \vDash \phi[a_1, \ldots, a_n],$$

y no podemos decir esto porque el miembro derecho no está definido. Eso es justo lo que afirma el teorema de Tarski. Decir que V satisface una fórmula ϕ es lo mismo que decir que ϕ es verdadera. Podemos definir qué significa que una fórmula ϕ sea verdadera en un conjunto M (precisamente a través de la definición de Tarski de $M \vDash \phi[v]$), pero no en todo el universo de discurso. De hecho, si la expresión anterior tuviera sentido, podríamos demostrar que V_λ es un modelo de ZFC, con lo que podríamos demostrar Consis($\ulcorner$ZFC$\urcorner$) en ZFC, en contra del segundo teorema de incompletitud.

Hasta aquí hemos estado trabajando con fórmulas de lenguajes formales definidos en ZFC, incluyendo, en el caso del último teorema, fórmulas del lenguaje $\ulcorner$ZFC$\urcorner$ definido en ZFC, pero, si consideramos una fórmula metamatemática $\phi(x_1, \ldots, x_n)$, sí que tiene sentido la equivalencia:

$$\bigwedge a_1 \cdots a_n (V_\lambda \vDash \ulcorner\phi\urcorner[a_1, \ldots, a_n] \leftrightarrow \phi(a_1, \ldots, a_n)),$$

y, usando la misma idea de la prueba anterior, se puede probar lo que se hoy conoce como teorema de reflexión:[187]

> **Teorema de reflexión** Si $\phi_1(x_1, \ldots, x_n), \ldots, \phi_k(x_1, \ldots, x_n)$ son fórmulas metamatemáticas cuyas variables libres están entre las indicadas, la fórmula siguiente es un teorema de ZF:
>
> $$\bigvee\lambda \bigwedge a_1 \cdots a_n ((V_\lambda \vDash \ulcorner\phi_1\urcorner[a_1, \ldots, a_n] \leftrightarrow \phi_1(a_1, \ldots, a_n)) \wedge \cdots \wedge (V_\lambda \vDash \ulcorner\phi_k\urcorner[a_1, \ldots, a_n] \leftrightarrow \phi_k(a_1, \ldots, a_n))).$$

[185] Si θ es fuertemente inaccesible, una simple inducción transfinita demuestra que $|V_\alpha| < \theta$, pues, trivialmente vale para $\alpha = 0$, si vale para α, entonces $|V_{\alpha+1}| = |\mathcal{P}V_\alpha| = 2^{|V_\alpha|} < \theta$ (por definición de cardinal fuertemente inaccesible) y si $|V_\delta| < \theta$ para todo $\delta < \lambda < \theta$, donde λ es un ordinal límite, entonces $|V_\lambda| < \theta$, porque, de nuevo por la inaccesibilidad, la unión de menos de θ conjuntos de cardinal menor que θ tiene cardinal menor que θ. A su vez esto implica que $|V_\theta| \leq \theta$, porque la unión de una cantidad $\leq \theta$ de conjuntos de cardinal menor que θ es $\leq \theta$. Como $\theta \subset V_\theta$, tenemos la igualdad.

[186] Observemos que es un modelo peculiar, porque, para alguien que sólo vea los conjuntos de $V_{\theta'}$, la clase de todos los ordinales es $\Omega = \theta'$, pero θ' es el supremo del conjunto numerable $N = \{\alpha_k \mid k < \omega\}$, y eso no puede suceder en ZFC (o en NBG). Esto significa que alguien que sólo vea los conjuntos de $V_{\theta'}$ no puede ver N, no ya como conjunto (que no lo ve, porque $N \in V_{\theta'+1} \setminus V_{\theta'}$), sino tampoco como clase. Para alguien que "viva" en $V_{\theta'}$ la "colección" N no existe en absoluto. Puede pensar en la propiedad "ser un conjunto", que no define ningún conjunto, pero con ella está pensando en $V_{\theta'}$, o en la propiedad "ser un ordinal", que no define ningún conjunto, pero con ella está pensando en θ', pero no hay ninguna fórmula que defina N cuantificando sólo sobre conjuntos de $V_{\theta'}$ (ninguna fórmula en la que nuestro "habitante" pueda pensar). Hemos visto que el conjunto de las partes definibles $\mathcal{D}V_{\theta'}$ es un modelo de NBG, pero $V_{\theta'+1} = \mathcal{P}V_{\theta'}$ no puede serlo. Alguien que sólo viera las clases de $V_{\theta'+1}$ vería la clase $F = \{(k, \alpha_k) \mid k < \omega\} \in V_{\theta'+1}$, que es una biyección entre ω y una clase no acotada en Ω, y eso no sucede en NBG. Siguiendo esta línea es fácil probar que para que un conjunto $V_{\theta+1}$ sea un modelo de NBG es necesario que θ sea fuertemente inaccesible. Por ejemplo, si hubiera un cardinal $\kappa < \theta$ tal que $2^\kappa \geq \theta$, entonces en $V_{\theta+1}$ habría una clase $F : \mathcal{P}\kappa \longrightarrow \Omega$ suprayectiva, y eso no puede pasar en NBG (porque la imagen de un conjunto es un conjunto).

[187] Montague y Vaught lo demuestran con un argumento algo distinto porque también han seguido un camino algo distinto para demostrar el teorema anterior.

Se trata de definir una sucesión creciente de ordinales $\alpha_0 < \alpha_1 < \cdots$ cuyo supremo es λ, de modo que cada α_{k+1} es un ordinal lo suficientemente grande como para que $V_{\alpha_{k+1}}$ cumpla el criterio de Tarski-Vaught para las fórmulas ϕ_i con parámetros en V_{α_k}. En realidad hay que hacer un ajuste técnico porque el criterio no es aplicable a unas fórmulas aisladas, por lo que hay que añadir a la lista de fórmulas todas sus subfórmulas (con lo que seguimos teniendo una lista finita), pero no altera en nada el argumento central.

A este mismo resultado llegó en **1960** Azriel Lévy en un artículo titulado *Esquemas axiomáticos de infinitud fuerte en teoría de conjuntos.* Lévy se había doctorado en 1958 en la Universidad Hebrea de Jerusalén bajo la dirección de Fraenkel y Abraham Robinson. En **1961** Fraenkel cumplió 70 años, y en su honor se publicó un libro titulado *Ensayos sobre la fundación de las matemáticas,* con contribuciones de varios autores. Entre ellos estaba Montague, que presentó su artículo *La adición de Fraenkel a los axiomas de Zermelo,* en el que incluyó su demostración de que ZFC no es finitamente axiomatizable. Es una consecuencia inmediata del teorema de reflexión:

Ninguna extensión consistente de ZFC es finitamente axiomatizable.

DEMOSTRACIÓN: El enunciado significa que no existe ningún conjunto finito de sentencias $\alpha_1, \ldots, \alpha_n$ del lenguaje de la teoría de conjuntos que sean consistentes y a partir de las cuales se puedan demostrar todos los axiomas de ZFC (luego también todos sus teoremas), sin que importe que ellas mismas no sean necesariamente teoremas de ZFC.

Si existieran, llamemos T a la teoría que tiene a estas sentencias por axiomas o, equivalentemente, a la sentencia $\phi \equiv \alpha_1 \wedge \cdots \wedge \alpha_n$. Estamos suponiendo que T es una teoría consistente. Pero el teorema de reflexión nos daría que en ZF, luego en la teoría T, se puede demostrar

$$\bigvee\lambda(V_\lambda \vDash \ulcorner\phi\urcorner \leftrightarrow \phi).$$

Pero ϕ es demostrable en T, luego en realidad tenemos $\underset{T}{\vdash} \bigvee\lambda\, V_\lambda \vDash \ulcorner\phi\urcorner$, pero esto significa que existe un modelo de $\ulcorner\phi\urcorner$, o sea de $\ulcorner T\urcorner$, y así tenemos que $\underset{T}{\vdash} \mathrm{Consis}(\ulcorner T\urcorner)$, con lo que, por el segundo teorema de incompletitud, la teoría T es contradictoria, en contra de lo supuesto. ∎

El mismo argumento prueba que si T es la teoría que tiene por axiomas un número finito $\alpha_1, \ldots, \alpha_n$ de axiomas (o de teoremas) de ZFC, entonces

$$\underset{\mathrm{ZFC}}{\vdash} \bigvee\lambda\, V_\lambda \vDash \ulcorner T\urcorner,$$

luego también

$$\underset{\mathrm{ZFC}}{\vdash} \mathrm{Consis}(\ulcorner T\urcorner),$$

es decir, que en ZFC (supuesto que sea consistente) no se puede demostrar que exista un conjunto que sea un modelo de ZFC (pues eso contradiría al segundo teorema de incompletitud), pero sí que se puede demostrar que existe un conjunto que es un modelo de cualquier conjunto finito de axiomas de ZFC prefijado.

Notemos que la diferencia práctica es insignificante: cada teorema de ZFC se demuestra a partir de un número finito de axiomas, luego todos los teoremas demostrados jamás en cualquier libro de álgebra, de análisis, de geometría, etc., publicado hasta la fecha, se demuestran a partir de un número finito de axiomas de ZFC, y en ZFC se puede demostrar que existe un modelo de esos axiomas, en el que, por consiguiente, se cumplen todos los teoremas conocidos. Eso sí, en él no se cumplirá al menos alguno de los axiomas necesarios para demostrar que existe tal modelo.

Conviene observar que el teorema de reflexión demuestra algo ligeramente más fuerte que la existencia de modelos de cualquier conjunto finito de axiomas de ZFC. Tomando como ϕ_1 la conjunción de un conjunto finito T de axiomas de ZFC y como ϕ_2 una sentencia cualquiera α, obtenemos que existe un ordinal λ tal que

$$(V_\lambda \vDash \ulcorner\phi_1\urcorner \leftrightarrow \phi_1) \wedge (V_\lambda \vDash \ulcorner\alpha\urcorner \leftrightarrow \alpha),$$

pero ϕ_1 es un teorema de ZFC, luego

$$\bigvee\lambda(V_\lambda \vDash \ulcorner T\urcorner \wedge (V_\lambda \vDash \ulcorner\alpha\urcorner \leftrightarrow \alpha)).$$

Esto significa que podemos demostrar que existe un modelo V_λ de cualquier subteoría finita T de ZFC de modo que α es verdadera en V_λ si y sólo si es verdadera. A su vez, tomando un núcleo de Skolem $N \prec V_\lambda$ obtenemos un conjunto numerable N tal que, si llamamos Sent al conjunto de todas las sentencias del lenguaje de la teoría de conjuntos,

$$\bigwedge \phi \in \mathrm{Sent}(N \vDash \phi \leftrightarrow V_\lambda \vDash \phi).$$

En particular $N \vDash \ulcorner T \urcorner \wedge (N \vDash \ulcorner \alpha \urcorner \leftrightarrow \alpha)$. Es decir, en ZFC se puede demostrar que existe un modelo numerable de cualquier subteoría finita de ZFC que cumple una sentencia prefijada si y sólo si es cierta. Notemos que se trata de un submodelo de V_λ, donde en éste interpretamos la relación de pertenencia como la propia relación de pertenencia, luego lo mismo vale para N. Estamos hablando del modelo que resulta de llamar "conjuntos" únicamente a los elementos de N y de tomar como relación de pertenencia la misma que estábamos considerando antes de "desterrar" a los conjuntos que no están en N. Los modelos con esta propiedad, es decir, los modelos que consisten en un conjunto y la relación de pertenencia usual, se llaman *modelos naturales*.

Sin embargo, el modelo N carece de una propiedad que sí que tiene V_λ y que es muy conveniente al tratar con modelos de ZFC: no es necesariamente transitivo. En efecto, supongamos que un modelo natural M de ZFC (o de un conjunto finito de axiomas de ZFC tan grande que no se note la diferencia) no es transitivo. Alguien que "viva" en M, es decir, alguien sólo vea los conjuntos que están en M, verá un conjunto $a \in M$ al que llamará "conjunto vacío", pero dicho conjunto no tiene por qué ser realmente el conjunto vacío. Podría tener incluso infinitos elementos, a condición de que ninguno de ellos esté en M. En tal caso, para los habitantes de M (que no verán los elementos de a) el conjunto a será el vacío. En cambio, si M es transitivo, eso significa que los habitantes de M ven todos los elementos de los conjuntos que ven (si $a \in M$, entonces $a \subset M$, luego todos los elementos de a están a la vista de los habitantes de M), luego el conjunto al que los habitantes de M llamen "conjunto vacío" será el auténtico conjunto vacío, porque si tuviera algún elemento, lo verían.

Conceptos absolutos En general, un concepto conjuntista se dice *absoluto* para un modelo natural M de ZFC (o de un número finito de axiomas) si los "habitantes" del modelo no se equivocan cuando hablan de ese concepto. Por ejemplo, acabamos de observar que el conjunto vacío es absoluto para modelos transitivos de ZFC, pero no lo es necesariamente para modelos naturales no transitivos. Y hay muchos más conceptos que resultan ser absolutos para cualquier modelo transitivo del suficiente ZFC (en muchos casos ni siquiera hace falta el axioma de elección). Algunos ejemplos:

- Las operaciones conjuntistas básicas $x \cup y, x \cap y, x \setminus y$ son absolutas, al igual que la inclusión $x \subset y$.

  Esto quiere decir que si un habitante de M ve dos conjuntos x, y, llamará $x \cup y$ a la auténtica unión de esos dos conjuntos.

- La propiedad "ser un ordinal" es absoluta.

  Esto quiere decir que si un habitante de M ve un ordinal, lo reconocerá como tal, y si dice que un conjunto que ve es un ordinal, es que ciertamente lo es.

  No obstante, hay que tener en cuenta que M no tiene por qué contener todos los ordinales. La situación es la siguiente:

  1. Si M es un conjunto, entonces $\lambda = M \cap \Omega$, el conjunto de los ordinales que están en M, es un ordinal límite, de modo que, para un habitante de M, los ordinales son los ordinales menores que λ.
  2. Si M es una clase propia, como la clase L de los conjuntos constructibles, o en el caso trivial de la clase V de todos los conjuntos, entonces necesariamente $\Omega \subset M$ y los habitantes de M llaman ordinales a los ordinales, ni más ni menos.

- La propiedad "ser un número natural" es absoluta, al igual que las operaciones aritméticas con números naturales.

  Un habitante de M calculará $2 + 2 = 4$ exactamente igual que los que ven todos los conjuntos. De hecho, toda la aritmética ordinal es absoluta.

- La propiedad "ser un conjunto finito" es absoluta.

  Esto significa que, cuando un habitante de M ve un conjunto, nunca se equivoca al juzgar si es finito o infinito.

- Las propiedades "ser un número entero, racional, real,[188] complejo" son absolutas, así como las operaciones aritméticas de suma, producto, etc.

  En el caso de los números enteros y racionales, un habitante de M los ve siempre todos, pero con los números reales y complejos sucede lo mismo que con los ordinales: un habitante de M juzga correctamente si un conjunto que ve es o no un número real o un número complejo, pero no ve necesariamente todos los números reales o complejos. Por ejemplo, si el modelo M es numerable, necesariamente habrá muchos números reales que no estarán en M.

En cambio, otras propiedades no son necesariamente absolutas para modelos transitivos. Algunos ejemplos (que ciertamente no son absolutos para modelos numerables):

- La operación $\mathcal{P}x$ no es absoluta.

  Si un habitante de M ve un conjunto x, hay que distinguir entre el auténtico conjunto $\mathcal{P}x$, que contiene todos los subconjuntos de x, y el conjunto $\mathcal{P}^M x = \mathcal{P}x \cap M$, que contiene a los subconjuntos de x que ve el habitante. Si x es infinito y M es numerable, entonces $\mathcal{P}^M x$ será numerable, mientras que $\mathcal{P}x$ no lo será.

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ son absolutos, pero $\mathbb{R}$ y $\mathbb{C}$ no lo son.

  Un habitante de M ve todos los números racionales, y sabe distinguir cuándo son enteros o naturales, por lo que llama $\mathbb{N}, \mathbb{Z}$ o $\mathbb{Q}$ a estos mismos conjuntos. Sin embargo, no verá necesariamente todos los números reales y complejos, por lo que hay que distinguir los conjuntos $\mathbb{R}$ y $\mathbb{C}$, que contienen todos los números reales y complejos, de los conjuntos $\mathbb{R}^M = \mathbb{R} \cap M$ y $\mathbb{C}^M = \mathbb{C} \cap M$ que contienen los números reales y complejos visibles para los habitantes de M. Si M es numerable, entonces $\mathbb{R}^M$ es numerable, mientras que $\mathbb{R}$ no lo es.

- La propiedad "ser numerable" no es absoluta.

  No es lo mismo "x es numerable" (es decir, que exista una biyección $f : \mathbb{N} \longrightarrow x$) que "$x$ es numerable^M" (es decir, que exista una tal biyección $f \in M$). Por ejemplo, si M es numerable, el conjunto $\mathbb{R}^M$ es numerable, pero no es numerable^M.

- $\aleph_0$ es absoluto, pero $\aleph_1$ no lo es.

  Un habitante de M llamará $\aleph_0$ al conjunto correcto (que no es sino el conjunto de todos los números naturales), pero hay que distinguir entre $\aleph_1^M$, que es el menor ordinal que alguien que viva en M juzga no numerable, y $\aleph_1$, que es el menor ordinal no numerable. En general $\aleph_1^M \leq \aleph_1$, pero la igualdad no es necesariamente cierta.

En resumen, si un modelo natural M es transitivo, hay que hacer "un esfuerzo" para ponerse en el lugar de "un habitante de M" y tener claro qué entenderá por cada concepto conjuntista alguien que sólo vea los conjuntos de M, pero este es fuerzo es mucho menor que el que hace falta para ponerse en el lugar de un habitante de un modelo natural no transitivo, y mucho más para ponerse en el lugar de un habitante de un modelo en el que la relación de pertenencia se interpreta como otra relación R distinta de la pertenencia usual. ∎

Por ello, volviendo al modelo N no necesariamente transitivo que habíamos obtenido de V_λ, sucede que hay una forma de convertirlo en un modelo transitivo mucho más manejable. La técnica para ello había aparecido en un artículo de Mostowski de 1949 titulado *Una sentencia aritmética indecidible,* en el que, suponiendo que es consistente la existencia de un cardinal fuertemente inaccesible, demostraba que la sentencia "existe un modelo transitivo de NBG" es indecidible en NBG, y que puede expresarse en términos aritméticos. Pero como paso intermedio demostraba un resultado de gran interés en sí mismo, y que últimamente estaba siendo empleado con frecuencia:

Consideremos un conjunto M en el que hay definida una relación binaria R:

1. Si $A \subset M$, un *minimal* de A es un $x \in A$ tal que no exista ningún $y \in A$ que cumpla $y\,R\,x$.
2. R está *bien fundada* en M si todo subconjunto A de M no vacío tiene un minimal.
3. La *extensión* de un $a \in M$ es el conjunto $E(a) = \{x \in M \mid x\,R\,a\}$.

[188] En realidad "ser un número real/complejo es absoluto si los números reales se definen según Dedekind, pero no si se definen según Cantor.

4. R es *extensional* en M si elementos distintos en M tienen extensiones distintas, es decir, si cada elemento de M está completamente determinado por su extensión. Alternativamente, si

$$\bigwedge ab \in M(\bigwedge x \in M(x\,R\,a \leftrightarrow x\,R\,b) \to a = b).$$

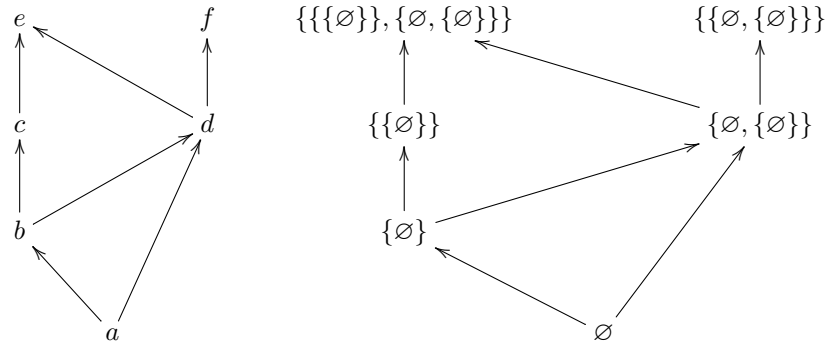
Por ejemplo, el axioma de extensionalidad afirma que la relación de pertenencia es extensional en cualquier conjunto, y el axioma de regularidad afirma que está bien fundada en cualquier conjunto. Lo que probó Mostowski es lo siguiente:

Teorema del colapso de Mostowski Si R es una relación extensional y bien fundada en un conjunto M, existe un único conjunto transitivo M^* y una única aplicación $\pi : M \longrightarrow M^*$ biyectiva tal que

$$\bigwedge xy \in M(x\,R\,y \leftrightarrow \pi(x) \in \pi(y)).$$

El conjunto M^* se conoce hoy en día como *colapso de Mostowski* o *colapso transitivo* de (M, R), y la función π como la *función colapsante de Mostowski*.

Por ejemplo, la figura siguiente muestra a la izquierda un ejemplo de conjunto $M = \{a, b, c, d, e, f\}$ en el que hay definida una relación R extensional y bien fundada, y a la derecha tenemos su colapso de Mostowski:



La idea subyacente a la construcción del colapso es que, para cada $x \in M$, su colapso $\pi(x) \in M^*$ tiene que estar formado exclusivamente por elementos de M^*, porque M^* es transitivo, luego cada elemento de $\pi(x)$ tiene que ser de la forma $\pi(y)$, para cierto $y \in M$, y si $\pi(y) \in \pi(x)$, según el enunciado del teorema de Mostowski, tiene que ser $y\,R\,x$. En suma, tiene que cumplirse la relación recurrente

$$\pi(x) = \{\pi(y) \mid y\,R\,x\}.$$

Esta relación determina completamente la función colapsante. Por ejemplo, en la figura vemos que a es el minimal de M (el único posible, porque dos minimales tendrían extensión vacía, luego tendrían que ser iguales, por la extensionalidad de R), luego su imagen es necesariamente $\pi(a) = \varnothing$. A su vez, esto determina el valor de $\pi(b) = \{\pi(a)\} = \{\varnothing\}$ y $\pi(d) = \{\pi(a), \pi(b)\} = \{\varnothing, \{\varnothing\}\}$, etc.

Mostowski demostró que la buena fundación de R garantiza que la definición recurrente de π define realmente una única función, y que la extensionalidad hace que π sea inyectiva. Los demás requisitos se deducen de la definición recurrente.

Con esto podemos enunciar el teorema de reflexión como se enuncia hoy en día:

Teorema de reflexión Si $\phi_1(x_1, \ldots, x_n), \ldots, \phi_k(x_1, \ldots, x_n)$ son fórmulas metamatemáticas cuyas variables libres están entre las indicadas, la fórmula siguiente es un teorema de ZF:

$$\bigvee \lambda \bigwedge a_1 \cdots a_n((V_\lambda \vDash \ulcorner\phi_1\urcorner[a_1, \ldots, a_n] \leftrightarrow \phi_1(a_1, \ldots, a_n)) \wedge \cdots \wedge (V_\lambda \vDash \ulcorner\phi_k\urcorner[a_1, \ldots, a_n] \leftrightarrow \phi_k(a_1, \ldots, a_n))).$$

Si $\phi_1, \ldots, \phi_n$ son sentencias, la fórmula siguiente es un teorema de ZFC:

$$\bigvee M(M \text{ transitivo numerable} \wedge ((M \vDash \ulcorner\phi_1\urcorner) \leftrightarrow \phi_1) \wedge \cdots \wedge (M \vDash \ulcorner\phi_k\urcorner) \leftrightarrow \phi_k)).$$

En particular, dada cualquier sentencia ϕ, existe un modelo transitivo numerable M de cualquier conjunto finito prefijado de axiomas de ZFC tal que $(M \vDash \ulcorner\phi\urcorner) \leftrightarrow \phi$.

La segunda parte se prueba tomando un V_λ que cumpla la primera parte, tomando un núcleo de Skolem numerable $M_0 \prec V_\lambda$ y calculando su colapso de Mostowski M, que será transitivo y numerable.

Esto es posible, porque siempre podemos exigir que entre los axiomas elegidos esté el de extensionalidad, con lo que V_λ cumple el axioma de extensionalidad, y M_0 también, y eso significa que la relación de pertenencia es extensional en M_0, y ésta está bien fundada en cualquier conjunto, luego podemos calcular el colapso de Mostowski $\pi : M_0 \longrightarrow M$. Éste es obviamente un isomorfismo de modelos del lenguaje de la teoría de conjuntos (pues al ser biyectivo conserva la interpretación del igualador, y por definición conserva la relación de pertenencia), luego M es elementalmente equivalente a M_0, que a su vez es elementalmente equivalente a V_λ. Por lo tanto, ϕ_i equivale a $V_\lambda \vDash \ulcorner\phi_i\urcorner$, que a su vez equivale a que M_0 cumpla lo mismo y a su vez a que M cumpla lo mismo.

Esto tiene una consecuencia notable:

> Una forma de demostrar un teorema ϕ en ZFC es demostrar que todo modelo transitivo numerable M de un conjunto finito suficientemente grande de axiomas de ZFC cumple $M \vDash \ulcorner\phi\urcorner$.

En efecto, el teorema de reflexión nos da que existe un modelo M que cumple todos los axiomas que queramos de ZFC (en número finito) y además $(M \vDash \ulcorner\phi\urcorner) \leftrightarrow \phi$, luego si hemos probado que M debe cumplir $M \vDash \ulcorner\phi\urcorner$, podemos concluir que se cumple ϕ.

86 La consistencia de la hipótesis del continuo generalizada Antes de seguir avanzando, vamos a ver que los resultados que hemos discutido en las secciones precedentes nos permiten entender por qué el axioma de constructibilidad $V = L$ implica la hipótesis del continuo generalizada. Según vimos en la página 156, esto es una consecuencia directa de este hecho, que se demuestra suponiendo $V = L$:

> Si $V = L$ y κ es un cardinal infinito, entonces se cumple $\mathcal{P}L_\kappa \subset L_{\kappa^+}$, donde κ^+ representa el cardinal siguiente a κ.

Esto significa que un subconjunto $x \subset L_\kappa$, no tiene por qué entrar en la jerarquía constructible en el paso siguiente $L_{\kappa+1} = \mathcal{D}L_\kappa$, pues ahí sólo entran los subconjuntos de L_κ definibles mediante una fórmula con parámetros en L_κ, y x no tiene por qué ser de esta forma. Pero sucede que x entra en la jerarquía constructible antes del paso κ^+, y eso implica (como vimos) que $2^\kappa = \kappa^+$. Ahora estamos en condiciones de entender por qué sucede esto.

Si M es un modelo transitivo de una cantidad finita suficientemente grande de axiomas de ZFC, ya hemos visto que $\mathcal{P}X$ no tiene por qué ser absoluto para M, es decir, que alguien que sólo vea los conjuntos de M, tomará por conjunto de partes de X a $\mathcal{P}^M X = \mathcal{P}X \cap M$, el conjunto de los subconjuntos de X que puede ver, que no tienen por qué ser todos. En cambio, sucede que $\mathcal{D}X$ sí que es absoluto para modelos transitivos. Si $X \in M$, un habitante de M identificará perfectamente cualquier conjunto de la forma

$$\{a \in X \mid X \vDash \phi[a, a_1, \ldots, a_n]\}, \qquad \text{con } a_1, \ldots, a_n \in X$$

sin necesidad de ver nada que esté fuera de M y, como además en M "se ven" todas las fórmulas ϕ del lenguaje de la teoría de conjuntos, al formar el conjunto $\mathcal{D}X$ de todos los conjuntos definibles de este modo, un habitante de M incluirá en él justamente los elementos del auténtico $\mathcal{D}X$.

A su vez esto se traduce en que la fórmula $Y = L_\alpha$ se absoluta para modelos transitivos, es decir, que si un habitante de M ve un ordinal α, entonces el conjunto que tomará por L_α será el auténtico L_α, sin perjuicio de que no vea algunos conjuntos L_α porque el ordinal α correspondiente esté fuera de M.

Ahora tenemos que distinguir dos casos:

1. Si M es una clase propia, como L, entonces todos los ordinales están en M, luego M ve todos los conjuntos L_α y, por lo tanto, todos los conjuntos constructibles, de modo que $L \subset M$. Así pues:

   La clase L es el menor modelo transitivo de ZF que es una clase propia, y si M es cualquier otro, "ser constructible" es absoluto para M.

   En otras palabras, alguien "que viva en M" verá todos los conjuntos constructibles y distinguirá correctamente si un conjunto dado es constructible o no. En particular:

   L es el único modelo transitivo numerable de ZFC + $V = L$ que es una clase propia.

   Pues si M es un modelo en esas condiciones, un habitante de M sólo verá conjuntos constructibles y no se equivocará en su apreciación, luego estará viendo los elementos de $M = L$.

2. Si M es un conjunto, entonces los ordinales de M son los de $\lambda = M \cap \Omega$, que es un ordinal límite.

   Para alguien que "viva en M", los conjuntos constructibles son los que están en uno de los conjuntos L_α que él puede ver, es decir, los conjuntos que están en $L_\lambda \subset M$. Por lo tanto, "ser constructible" no es necesariamente absoluto para M, sino que:

   $$x \text{ es coonstructible}^M \leftrightarrow x \in L_\lambda,$$

   y puede ocurrir que $M \subset L$, pero que haya conjuntos en $M \setminus L_\lambda$, es decir, conjuntos que se pueden construir, pero que para ello se necesitan más ordinales de los que se ven en M, y por ello en M parecen no constructibles.

   Ahora bien, si M es un modelo (de suficientes axiomas de) ZFC + $V = L$, entonces M tiene que ver construtibles todos los conjuntos que ve, luego tiene que ser $M = L_\lambda$. Por lo tanto:

   Los únicos modelos transitivos numerables de (suficientes axiomas de) ZFC + $V = L$ que son conjuntos son de la forma L_λ, para cierto ordinal límite λ.

   Pero no sirve todo λ. Un conjunto L_λ cualquiera no tiene por qué cumplir todos los axiomas de ZFC en los que podamos pensar.

Con esto tenemos suficiente para entender por qué $\mathcal{P}L_\kappa \subset L_{\kappa^+}$:

Demostración: Tomemos $x \subset L_\kappa$ y sea $X = L_\kappa \cup \{x\}$, que es un conjunto transitivo. Por el teorema de reflexión, existe un conjunto V_η que cumple cualquier conjunto finito de axiomas de ZFC que queramos y tal que

$$V_\eta \vDash \ulcorner \text{Todo conjunto es constructible} \urcorner \leftrightarrow \text{todo conjunto es constructible}.$$

Además, la demostración del teorema de reflexiónmuestra que η se puede tomar tan grande como se quiera (pues es el supremo de una sucesión de ordinales cuyo primer elemento lo podemos elegir arbitrariamente), luego podemos elegirlo de modo que $X \subset V_\eta$. Como estamos suponiendo que $V = L$, de hecho tenemos que V_η cumple un conjunto arbitrariamente grande de axiomas de ZFC + $V = L$.

Ahora tomamos el núcleo de Skolem $N(X) \prec V_\eta$, que será también un modelo natural del mismo conjunto de axiomas de ZFC+$V = L$ y además $|N(X)| = |X| = |L_\kappa| = \kappa$. Puesto que $N(X)$ cumple el axioma de extensionalidad, la relación de pertenencia en X es extensional, y necesariamente bien fundada, luego podemos considerar el colapso de Mostowski $\pi : N(X) \longrightarrow M$, que será un modelo transitivo del mismo conjunto de axiomas de ZFC + $V = L$ y $|M| = \kappa$.

Más aún, $L_\kappa \subset X \subset N(X)$ y la identidad $L_\kappa \longrightarrow L_\kappa$ cumple trivialmente todas las condiciones para ser la función colapsante, por lo que podemos concluir que, para todo $a \in L_\kappa$, se cumple $\pi(a) = a$. Más aún, como $x \subset L_\kappa$, tenemos que

$$\pi(x) = \{\pi(a) \mid a \in x\} = \{a \mid a \in x\} = x.$$

Por lo tanto, $x = \pi(x) \in M$.

Por otro lado, hemos visto que todo modelo del suficiente ZFC + $V = L$ tiene que ser de la forma L_λ, para cierto ordinal límite λ luego tenemos que $x \in M = L_\lambda$. Pero $\kappa = |L_\lambda| = |\lambda|$, luego $\lambda < \kappa^+$ (pues si se diera la desigualdad opuesta λ tendría al menos κ^+ elementos). Y así $x \in L_\lambda \subset L_{\kappa^+}$. ∎

87 El décimo problema de Hilbert Entre los problemas que Hilbert había planteado en su conferencia en el Segundo Congreso Internacional de Matemáticos de 1900, el décimo consistía en encontrar un procedimiento para resolver cualquier ecuación diofántica, es decir, para encontrar las soluciones enteras de cualquier ecuación de la forma

$$P(x_1, \ldots, x_n) = 0,$$

donde P es un polinomio con coeficientes enteros. Un poco más en general, podemos decir que una relación R sobre números naturales es *diofántica* si puede expresarse en la forma

$$R(x_1, \ldots, x_n) \leftrightarrow \bigvee y_1 \cdots y_m \in \mathbb{N}\ P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0,$$

donde P es un polinomio con coeficientes enteros.

Gödel había demostrado (véase la sección 50) que toda relación recursiva se puede expresar mediante una fórmula en la aritmética de Peano, o incluso en la aritmética de Robinson (véase la sección 79). En realidad, las fórmulas del lenguaje de la aritmética necesarias para expresar relaciones recursivas tenían una forma especialmente simple, pero, a partir de los resultados de Gödel, no se podía asegurar que sean equivalentes a fórmulas de tipo[189] $\bigvee y_1 \cdots y_m \in \mathbb{N}\, P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$.

En 1952 Julia Robinson (doctorada en 1948 bajo la dirección de Tarski) obtuvo varios resultados sobre relaciones diofánticas, pero no logró demostrar que la relación de exponenciación $a = b^c$ fuera diofántica. Por ello definió las relaciones exponencial-diofánticas, que son las de la forma

$$R(x_1, \ldots, x_n) \leftrightarrow \bigvee y_1 \cdots y_m z_1 \cdots z_m w_1 \cdots w_m \in \mathbb{N}\, (P(x_1, \ldots, x_n, y_1, \ldots, y_m, z_1, \ldots, z_m, w_1, \ldots, w_m) = 0$$
$$\wedge\, y_1 = z_1^{w_1} \wedge \cdots \wedge y_m = z_m^{w_m}),$$

es decir, relaciones expresables en términos de una ecuación diofántica, salvo que se permite calcular aparte potencias de números naturales. A partir de las propiedades elementales de las relaciones diofánticas es fácil demostrar que, si la exponenciación es diofántica, las relaciones exponencial-diofánticas coinciden con las relaciones diofánticas.

Robinson obtuvo algunos resultados destacados sobre este tipo de relaciones, y en **1961**, Martin Davis (doctorado en 1950 bajo la dirección de Church), Hilary Putnam y Robinson demostraron que toda relación recursiva es exponencial-diofántica. De hecho, esto implica automáticamente algo un poco más general: una relación se dice *semirecursiva* si es de la forma

$$R(x_1, \ldots, x_n) \leftrightarrow \bigvee y \in \mathbb{N}\, S(x_1, \ldots, x_n, y),$$

donde S es una relación recursiva. Si toda relación recursiva es exponencial-diofántica, de hecho lo es toda relación semirrecursiva, pues una relación exponencial-diofántica sigue siéndolo si se le añade delante un $\bigvee y \in \mathbb{N}$.

Esto hacía que cobrara una gran importancia la conjetura de Robinson según la cual la exponenciación es diofántica, pues, en caso de ser cierta, se podía concluir que el décimo problema de Hilbert no tiene solución. En efecto, si admitimos que la exponenciación es diofántica, tenemos que toda relación semirrecursiva es diofántica. Pero existen relaciones semirrecursivas que no son recursivas. Por ejemplo, la relación

$$R(n) \leftrightarrow \bigvee d \underset{T}{\overset{d}{\vdash}} n$$

que se cumple si n codifica una fórmula α del lenguaje de una teoría aritmética recursiva y consistente T y existe otro número natural d que codifica una demostración de α en la T. En efecto, la relación $\underset{T}{\overset{d}{\vdash}} n$ es recursiva, pues siempre podemos determinar si un número dado d codifica o no una demostración de una fórmula codificada por n, pero no existe un algoritmo finito para determinar si existe o no una demostración de una fórmula dada (véase la página 138).

Si la conjetura de Robinson es cierta, la relación R se puede expresar como

$$R(n) \leftrightarrow \bigvee y_1 \cdots y_m \in \mathbb{N}\, P(n, y_1, \ldots, y_m) = 0,$$

donde P es un polinomio con coeficientes enteros. De hecho, una pequeña manipulación permite expresar R en la forma[190]

$$R(n) \leftrightarrow \bigvee z_1 \cdots z_k \in \mathbb{Z}\, Q(n, z_1, \ldots, z_k) = 0.$$

De este modo resulta que comprobar si se cumple o no $R(n)$ equivale a resolver una ecuación diofántica, es decir, a determinar si una ecuación polinómica con coeficientes enteros tiene o no soluciones enteras.

Si la relación R no es recursiva, esto significa que, para cada número natural n, tenemos una ecuación diofántica $Q(n, z_1, \ldots, z_k) = 0$ que tiene una solución $(z_1, \ldots, z_n)$ si y sólo si se cumple $R(n)$, pero, como no existe ningún algoritmo que determine para qué valores de n se cumple $R(n)$, no hay ningún algoritmo que determine cuáles de dichas ecuaciones diofánticas tienen solución y cuáles no.

Más concretamente, si tomamos como T la teoría de conjuntos ZFC y como n el número natural que codifica la sentencia $0 \neq 0$, entonces $R(n)$ es $\neg\mathrm{Consis}(\ulcorner \mathrm{ZFC} \urcorner)$, luego concluimos:

[189] En la aritmética de Peano se pueden definir los números enteros, aunque no es necesario para tratar con relaciones diofánticas, pues basta sustituir las ecuaciones de la forma $P = 0$, donde P es un polinomio con coeficientes enteros, por ecuaciones $P_1 = P_2$, donde P_1 y P_2 son polinomios con coeficientes naturales.

[190] Basta usar que todo número natural es suma de cuatro cuadrados, y sustituir cada $y_i = z_{i1}^2 + z_{i2}^2 + z_{i3}^2 + z_{i4}^2$.

La consistencia de ZFC equivale a que cierta ecuación diofántica no tenga solución.

Por lo tanto, si ZFC es consistente, tenemos una ecuación diofántica que no tiene solución, pero que es imposible demostrar que no la tiene.

Sin embargo, los especialistas consideraban poco probable que la conjetura de Robinson fuera correcta. Por ejemplo, se podía probar que, de ser cierta, toda relación diofántica puede expresarse en términos de un polinomio de grado ≤ 4 o con un número máximo m de variables, el mismo para todas las relaciones diofánticas. Posteriormente se probó que es suficiente con 9 variables, y esto no parecía plausible. Sin embargo, en 1970, leería su tesis doctoral un joven soviético de 23 años llamado Yuri Vladímirovich Matiyasévich, en la que demostró que la conjetura de Robinson era cierta y, por lo tanto, que el décimo problema de Hilbert es insoluble.

88 Ultraproductos Los últimos años, Tarski había estado interesado en una operación que estaba esbozada en el artículo de Skolem de 1934, en el que mostró ejemplos de modelos no estándar de la aritmética, y casi explícito en un artículo de 1955 del polaco Jerzy Łoś titulado *Algunas observaciones, teoremas y problemas sobre las clases definibles de álgebras,* pero que sólo ahora empezaba a ser formulado explícitamente, por ejemplo en el artículo de Kochen (publicado ese año de **1961**), pero también en otros, como *Ultraproductos y clases elementales,* de Howard Jerome Keisler, también de **1961**, año en el que se doctoró bajo la dirección de Tarski.

Consideremos una familia $\{M_i\}_{i\in I}$ de modelos de un mismo lenguaje formal. Por ejemplo, podemos pensar en una familia de cuerpos ordenados, pero serviría cualquier otra estructura algebraica, o también una familia de modelos del lenguaje de la teoría de conjuntos, etc. Llamamos $M = \prod_{i\in I} M_i$ al producto cartesiano de la familia. Un elemento $f \in M$ es una función definida sobre el conjunto de índices I, de modo que, para cada índice i, se cumple que $f(i) \in M_i$. Es fácil dotar a M de estructura de modelo sobre el mismo lenguaje formal, definiendo todo lo necesario componente a componente.

Por ejemplo, si hablamos de una familia de cuerpos ordenados, podemos definir $\mathbf{0} \in M$ como la función dada por $\mathbf{0}(i) = \mathbf{0}_i$, donde $\mathbf{0}_i$ es el cero del cuerpo M_i. Similarmente se define $\mathbf{1}(i) = \mathbf{1}_i$. La relación de orden se define mediante

$$f \leq g \quad \text{si y sólo si} \quad \text{para todo } i \in I \quad f(i) \leq_i g(i).$$

Similarmente, $-f(i) = -_i f(i)$, $\quad (f+g)(i) = f(i) +_i g(i)$, e igualmente con el producto.

Por ejemplo, para un producto de dos cuerpos $M_1 \times M_2$ lo que estamos diciendo es que

$$-(a,b) = (-_1 a, -_2 b), \qquad (a,b) + (c,d) = (a +_1 c, b +_2 d),$$

etc. Ahora bien, este modelo no es un cuerpo ordenado. Por ejemplo,

$$(\mathbf{1}_1, \mathbf{0}_2) \cdot (\mathbf{0}_1, \mathbf{1}_2) = (\mathbf{0}_1, \mathbf{0}_2),$$

cosa que no puede ocurrir en un cuerpo, y los dos factores no son comparables (ninguno es menor o igual que el otro). Sin embargo, vamos a ver que un pequeño retoque en el producto nos dará un modelo que cumplirá todas las sentencias que cumplan todos los factores.

Para ello consideramos el álgebra de Boole $\mathcal{P}I$, y en ella tomamos un ultrafiltro U. Es costumbre llamar ultrafiltros en I a los ultrafiltros del álgebra $\mathcal{P}I$. Recordemos la definición (página 174) particularizada a álgebras de tipo $\mathcal{P}I$:

Definición Un *ultrafiltro* en un conjunto I es un conjunto $U \subset \mathcal{P}I$ que cumple:

1. $I \in U$, $\varnothing \notin U$
2. Si $A \in U$, y $B \subset A \subset I$, entonces $A \in U$.
3. Si $A, B \in U$, entonces $A \cap B \in U$.
4. Si $A \subset I$, o bien $A \in U$, o bien $I \setminus A \in U$.

Recordemos que esto puede verse como una partición de $\mathcal{P}I$ en conjuntos grandes (los del ultrafiltro) y pequeños (los que no están en el ultrafiltro, que forman un ideal primo).[191]

[191] Łoś expresaba la construcción que vamos a ver en términos de un ideal primo, pero es equivalente.

En todo conjunto I se pueden definir unos ultrafiltros muy simples. Basta tomar $i_0 \in I$ y definir

$$U_{i_0} = \{A \in \mathcal{P}I \mid i_0 \in A\}.$$

Los ultrafiltros de este tipo se llaman *principales* (o *fijos*), y veremos que no son nada interesantes en nuestro contexto. Eso se debe a que, respecto a U_{i_0}. el conjunto $\{i_0\}$ es grande, lo cual no es muy razonable.

La existencia de ultrafiltros no principales no puede probarse sin el axioma de elección. En 1930 Tarski había demostrado que todo filtro está contenido en un ultrafiltro (*Una contribución a la teoría de la medida*), aunque hoy en día eso es una consecuencia inmediata del lema de Zorn, o del hecho de que todo ideal propio en un anillo unitario está contenido en un ideal maximal. Si I es un conjunto infinito, la familia F de sus subconjuntos cofinitos (de complementario finito) es un filtro, y cualquier ultrafiltro U que lo contenga es un ejemplo de ultrafiltro respecto al que los todos conjuntos cofinitos son grandes, luego sus complementarios, todos los conjuntos finitos, son pequeños. Por lo tanto, se trata de un ultrafiltro no principal (o *libre*).

Ahora volvamos a nuestro producto $M = \prod_{i\in I} M_i$ y fijemos un ultrafiltro U en I. De momento no importa si es principal o no.

Con él podemos definir una relación en M dada por

$$f =_U g \quad \text{si y sólo si} \quad \{i \in I \mid f(i) = g(i)\} \in U.$$

Esto significa que consideramos que f y g son "iguales respecto de U" si el conjunto de índices donde son iguales es grande. Es muy fácil ver que se trata de una relación de equivalencia, es decir que 1) $f =_U f$, 2) si $f =_U g$, entonces $g =_U f$ y 3) si $f =_U g$ y $g =_U h$, entonces $f =_U h$.

Llamamos $[f]_U$, o simplemente $[f]$, cuando podamos sobrentender U, a la clase de equivalencia formada por todas las funciones relacionadas con f, de modo que $[f]_U = [g_U]$ si y sólo si $f =_U g$. Esto nos permite definir el *ultraproducto*

$$M^* = \prod_{i\in I} M_i/U$$

como el conjunto cociente, formado por todas las clases de equivalencia $[f]$, que también admite una estructura natural de modelo del mismo lenguaje formal que los factores.

Por ejemplo, para el caso de la teoría de cuerpos ordenados, definimos

$$[f] \leq [g] \quad \text{si y sólo si} \quad \{i \in I \mid f(i) \leq g(i)\} \in U,$$

de modo que, para que se dé la desigualdad $[f] \leq [g]$, no pedimos que $f(i) \leq g(i)$ se cumpla para todos los índices, sino sólo que se cumpla para un conjunto grande de índices. Por otro lado, definimos:

$$\mathbf{0} = [\mathbf{0}], \quad \mathbf{1} = [\mathbf{1}], \quad [f] + [g] = [f + g], \quad [f] \cdot [g] = [f \cdot g].$$

Para modelos de un lenguaje arbitrario, las relaciones se interpretan como las relaciones que se cumplen si y sólo si se cumplen para un conjunto grande de factores, y las constantes y funtores se interpretan como hemos hecho en el ejemplo de los cuerpos ordenados (la función que interpreta a un funtor en el ultraproducto es la que hace actuar en cada componente la función que interpreta a dicho funtor en el modelo correspondiente). El resultado es que todo ultraproducto de una familia de modelos de un lenguaje formal es un modelo del mismo lenguaje formal y cumple el teorema siguiente:

Teorema fundamental de los ultraproductos (Łoś) Si $\{M_i\}_{i\in I}$ es una familia de modelos de un mismo lenguaje formal y U es un ultrafiltro en I, entonces el ultraproducto $M^* = \prod_{i\in I} M_i/U$ es un modelo de dicho lenguaje tal que, para cada fórmula $\alpha(x_1, \ldots, x_n)$, se cumple

$$M^* \vDash \alpha[[f_1], \ldots, [f_n]] \quad \text{si y sólo si} \quad \{i \in I \mid M_i \vDash \alpha[f_1(i), \ldots, f_n(i)]\} \in U.$$

Es decir, que M^* cumple una fórmula si ésta se cumple en un conjunto grande de factores. En particular, M^* satisface todas las sentencias que son satisfechas a la vez por todos sus factores. Así, si todos los factores son cuerpos ordenados, M^* también lo es.

Si el ultrafiltro es principal, es decir, si $U = U_{i_0}$, el ultraproducto es trivial, pues no es difícil probar que la aplicación $M^* \longrightarrow M_{i_0}$ dada por $[f] \mapsto f(i_0)$ es un isomorfismo de modelos, por lo que M^* es lo mismo que M_{i_0}, sin que los demás factores influyan en nada. En cambio, si el ultrafiltro no es principal, el ultraproducto es un modelo "esencialmente nuevo".

Como aplicación (y muestra de las técnicas que permite la teoría de modelos) vamos a demostrar el teorema de compacidad de Gödel:

Teorema de compacidad (Gödel) Si un conjunto de sentencias Γ de un lenguaje formal tiene la propiedad de que todos sus subconjuntos finitos admiten un modelo, entonces Γ admite un modelo.

Gödel probó este hecho como paso intermedio para demostrar el teorema de completitud, pero hoy en día puede probarse directamente (por ejemplo, con la demostración de Henkin) y el teorema de compacidad es una consecuencia inmediata del de completitud: si todos los subconjuntos finitos de Γ tienen un modelo, es que son consistentes, pero si son consistente, Γ también es consistente (porque una demostración de una contradicción a partir de las sentencias de Γ usaría sólo una cantidad finita de ellas, luego ese subconjunto finito no sería consistente), y si Γ es consistente, por el teorema de completitud tiene un modelo.

El interés de Tarski por los ultraproductos surgió cuando en 1958 dos alumnos suyos, Chen Chung Chang (doctorado en 1955) y Anne C. Morel (doctorada en 1953) usaron productos reducidos con filtros (sin suponer que eran ultrafiltros) y Tarski lo relacionó con el trabajo de Łoś, sugiriendo que se podrían unificar las técnicas, y que de ello podría surgir una demostración del teorema de compacidad que mostrara explícitamente como construir un modelo de Γ a partir de la familia de los modelos de sus subconjuntos finitos. Otro alumno de Tarski, Thomas Frayne (doctorado en 1957), formuló una definición general de producto reducido, mientras que Dana Scott (doctorado en 1958 bajo la dirección de Church) obtuvo resultados similares de forma independiente. En 1962, Frayne, Morel y Scott publicarían un artículo conjunto (*Productos directos reducidos*) en el que demostraban, entre otras cosas, el teorema de compacidad mediante ultraproductos. La prueba es muy simple:

Demostración: Sea $\gamma_0, \gamma_1, \gamma_2, \ldots$ un conjunto de sentencias con la propiedad de que cada subconjunto finito tiene un modelo, y sea M_n un modelo de las n primeras. Fijemos un ultrafiltro no principal U en $\mathbb{N}$ y consideremos el ultraproducto $M^* = \prod_{n\in\mathbb{N}} M_n/U$.

Entonces, cada sentencia γ_n es verdadera en todos los modelos M_n salvo a lo sumo en los n primeros, luego el conjunto $\{i \in \mathbb{N} \mid M_i \vDash \gamma_n\} \in U$, puesto que es un conjunto cofinito y el ultrafiltro U no es principal. Por el teorema fundamental, $M^* \vDash \gamma_n$, para todo n, luego M^* es un modelo de todas las sentencias dadas. ∎

Si partimos de un único modelo M y de un ultrafiltro U en un conjunto infinito cualquiera I, podemos formar la *ultrapotencia* $M^* = \mathrm{Ult}_U(M) = \prod_{i\in I} M/U$. En este caso tenemos también una aplicación

$$j_U : M \longrightarrow \mathrm{Ult}_U(M)$$

dada por $j_U(m)(i) = m$, es decir, la que hace corresponder a cada $m \in M$ la función constante igual a m. Del teorema fundamental se sigue que j_U es una inmersión elemental, llamada la *inmersión elemental canónica* en la ultrapotencia. En efecto, se cumple

$$M \vDash \alpha[j(a_1), \ldots, j(a_n)] \quad \text{si y sólo si} \quad \{i \in I \mid M \vDash \alpha(j(a_1)(i), \ldots j(a_n)(i))\} \in U \quad \text{si y sólo si}$$

$$\{i \in I \mid M \vDash \alpha(a_1, \ldots a_n)\} \in U \quad \text{si y sólo si} \quad M \vDash \alpha(a_1, \ldots a_n),$$

pues el último conjunto es I o $\varnothing$, según si M cumple o no α.

Si el ultrafiltro es principal, se trata de un isomorfismo, pero en caso contrario proporciona una extensión no trivial de M.

Por ejemplo, podemos partir de $\mathbb{R}$, visto como cuerpo ordenado, y de un ultrafiltro no principal U en $\mathbb{N}$. Así formamos la ultrapotencia $\mathbb{R}^* = \mathrm{Ult}_U(\mathbb{R})$. Los elementos de $\mathbb{R}^*$ son clases de equivalencia de sucesiones $(a_0, a_1, a_2, \ldots)$, de modo que dos sucesiones determinan la misma clase si y sólo si coinciden en un conjunto grande de índices.

Entonces $\mathbb{R}^*$ es un cuerpo ordenado, y tenemos una inmersión elemental $j : \mathbb{R} \longrightarrow \mathbb{R}^*$, que en particular es un monomorfismo de cuerpos, por lo que podemos identificar a $\mathbb{R}$ con su imagen y considerar que $\mathbb{R}$ es un subcuerpo de $\mathbb{R}^*$.

Pero en realidad tenemos mucho más. Sabemos que $\mathbb{R}$ y $\mathbb{R}^*$ son elementalmente equivalentes, es decir, que $\mathbb{R}^*$ cumple todas las propiedades elementales que cumple $\mathbb{R}$ (todas las que pueden expresarse en el lenguaje de la teoría de cuerpos ordenados). Y, más aún, unos números reales $a_1, \ldots, a_n$ cumplen una propiedad elemental si y sólo si la cumplen $j(a_1), \ldots, j(a_n)$ (esto es lo que significa que j sea una inmersión elemental).

Abraham Robinsohn fue un judío alemán que emigró a Israel con su familia a los 14 años en cuanto los nazis llegaron al poder, pero, con 22 años, estaba en Francia cuando los nazis la ocuparon, y le tocó huir de nuevo como para salir del país. Se instaló en los Estados Unidos, y allí cambió su nombre al de Abraham Robinson. En **1961** publicó su artículo *Análisis no estándar,* en el que mostraba cómo $\mathbb{R}^*$ podía usarse para formular con rigor el cálculo diferencial con infinitesimales que los matemáticos (serios) habían desterrado hacía ya tanto tiempo.

Por ejemplo, si llamamos números reales estándar a los números reales (de $\mathbb{R}$) y números reales no estándar a los elementos de $\mathbb{R}^* \setminus \mathbb{R}$, lo primero que podemos probar es que hay números reales no estándar, para lo cual basta considerar el determinado por la sucesión

$$N = (0, 1, 2, 3, \ldots).$$

El número natural $0 \in \mathbb{R}$ se identifica con $j(0) = (0, 0, 0, \ldots)$, luego $0 \leq N$, ya que la desigualdad se da en todas las componentes. Pero $1 \leq N$, porque la desigualdad se da en todas las componentes menos la primera, y en general tenemos que $n \leq N$ para todo número natural (estándar). Pero todo número real estándar está por debajo de un número natural estándar, así que, para todo número real estándar r, tenemos que $r \leq n < n + 1 \leq N$, y así, N es mayor que todo número real estándar.

A su vez, si llamamos $\delta = 1/N$, tenemos que $\delta > 0$ (recordemos que $\mathbb{R}^*$ es un cuerpo ordenado que cumple las mismas propiedades elementales que $\mathbb{R}$ y, en particular, el inverso de un número positivo es positivo). Pero si $r > 0$ es un número real estándar, también lo es $1/r$, luego $1/r < N$, luego $\delta = 1/N < r$. Así pues, δ es un número positivo menor que todo número real estándar positivo.

Para expresar adecuadamente estos hechos definimos

$$\mathcal{O} = \{x \in \mathbb{R}^* \mid \bigvee r \in \mathbb{R}\ |x| \leq r\}, \qquad o = \{x \in \mathbb{R}^* \mid \bigwedge r \in \mathbb{R}^+\ |x| \leq r\}.$$

Así, $\mathcal{O}$ es el conjunto de los números reales finitos (los que son menores en valor absoluto que algún número real estándar) y o es el conjunto de los infinitésimos (los que son menores o iguales en valor absoluto que todo número real positivo). Hemos probado que N es un número real infinito (es decir, que no está en $\mathcal{O}$) y que δ es un infinitésimo no nulo.

Diremos que dos números reales están *infinitamente próximos,* y lo representaremos por $r \approx s$, si $r - r'$ es infinitesimal.

Teorema

1. La suma y el producto de números finitos (infinitesimales) es un número finito (infinitesimal).
2. Si $|x| \leq \delta$ y δ es infinitesimal, entonces x también lo es.
3. El producto de un número finito por un infinitésimo es infinitesimal.
4. Todo número finito x está infinitamente cerca de un único número estándar x^*, al que llamaremos su *parte estándar.*

Demostración: Dejamos 1 y 2 como ejercicio. Para probar 3) tomamos x finito y η infinitesimal, y observamos que $x\eta$ es infinitesimal, pues si $|x| \leq r$ estándar, entonces, para todo $r' > 0$ estándar, se cumple que $|\eta| \leq r'/r$, por definición de infinitésimo, luego $|x\eta| \leq r|\eta| \leq r'$.

4) Supongamos que $x > 0$ (el caso contrario es análogo, o se reduce a éste considerando $-x$). Sea r un número estándar tal que $x = |x| \leq r$. El conjunto $A = \{s \in \mathbb{R} \mid s \leq x\}$ es no vacío, pues contiene a 0, y está acotado por r, luego el principio de existencia de supremo (que cumple $\mathbb{R}$, aunque no necesariamente $\mathbb{R}^*$, ya que no es una propiedad elemental) nos da que existe el supremo x^* de A, que es un número real estándar. Vamos a ver que $x^* \approx x$. Fijamos $t > 0$ estándar.

Supongamos en primer lugar que $x^* \leq x$. Si fuera $x - x^* > t$, entonces $x^* + t < x$, luego $x^* + t \in A$, luego $x^* + t \leq x^*$, lo cual es absurdo. Por lo tanto $|x - x^*| = x - x^* \leq t$ para todo t, y concluimos que $x - x^*$ es infinitesimal.

Si es $x < x^*$, entonces $x^* - t < x^*$, luego no es cota superior de A, luego existe $s \in A$ tal que $x^* - t < s \leq x$, luego $|x - x^*| = x^* - x < t$, y también concluimos que $x - x^*$ es infinitesimal.

La unicidad se debe a que la diferencia entre dos números reales estándar distintos es estándar, luego no puede ser infinitesimal (no es menor que sí misma). ∎

Así pues, todo número real estándar está rodeado de un *halo* de números infinitamente próximos de modo que cada número finito está en uno de estos halos, y sólo en uno, porque si un mismo número x estuviera en los halos de dos números estándar a y b, sería $a \approx x \approx b$, pero dos números estándar distintos no pueden estar infinitamente próximos, porque $|a-b|$ no es infinitesimal (ya que para ello tendría que ser menor que todo número estándar positivo, pero no es menor que sí mismo).

Ejemplo Consideremos la función $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ dada por $f(x) = x^2$.

Una forma de probar que es derivable usando técnicas no estándar de usar esta caracterización de la derivabilidad:

f es derivable en un punto x si y sólo si, para todo infinitésimo δ no nulo, el cociente

$$\frac{f(x+\delta)-f(x)}{\delta}$$

es finito y su parte estándar no depende de δ. En tal caso, dicha parte estándar es la derivada $f'(x)$.

En este caso tenemos:

$$\frac{f(x+\delta)-f(x)}{\delta} = \frac{x^2+2x\delta+\delta^2-x^2}{\delta} = 2x+\delta \approx 2x,$$

y esto prueba que $f'(x) = 2x$.

Otras caracterizaciones no estándar son:

f es continua en un punto estándar a si y sólo si cuando $a \approx x$, entonces $f(a) \approx f(x)$.

f es uniformemente continua si y sólo si cuando $x \approx y$, entonces $f(x) \approx f(y)$.

En nuestro ejemplo, si $\delta = y - x \approx 0$, tenemos que

$$f(y) = (x+\delta)^2 = x^2 + 2x\delta + \delta^2 \approx x^2 = f(x),$$

donde hemos usado que el producto de un infinitésimo por un número finito es infinitesimal, y así tenemos que f es continua en todo punto estándar. En cambio, no es uniformemente continua, pues si tomamos un infinitésimo δ arbitrario y consideramos los puntos $x = 1/\delta$, $y = x + \delta$, sucede que $x \approx y$, pero

$$f(y) = (1/\delta+\delta)^2 = \frac{1}{\delta^2} + 2 + \delta^2 = f(x) + 2 + \delta^2 \approx f(x) + 2,$$

luego $f(x), f(y)$ no están infinitamente próximos. ∎

No vamos a demostrar aquí estas caracterizaciones de la derivabilidad y la continuidad porque trabajar exclusivamente con $\mathbb{R}^*$ es complicado y el análisis no estándar se iba a desarrollar mucho más hasta hacerse bastante más manejable que lo que podríamos hacer aquí sin más herramientas. Robinson desarrollaría un poco más su idea en su libre *Introducción a la teoría de modelos y a la metamatemática del álgebra,* de 1963, que es el primer libro dedicado a la teoría de modelos como disciplina matemática.

89 Cardinales medibles En **1961** Scott publicó un artículo revolucionario, si no en cuanto a los resultados obtenidos, sí en cuanto a la técnica que usó, pues construyó una ultrapotencia de la clase universal. El artículo se titulaba *Cardinales medibles y conjuntos constructibles.*

Recordemos (página 90) que Ulam había estudiado las consecuencias de que exista una medida no trivial $\mu : \mathcal{P}X \longrightarrow [0,1]$ definida sobre todos los subconjuntos de un conjunto X. En tal caso, el menor cardinal κ sobre el que puede definirse una medida así es $\mathbb{R}$-medible, y Ulam demostró que puede haber dos tipos de cardinales $\mathbb{R}$-medibles:

- o bien existe una medida no trivial en κ que es bivaluada (es decir, que sólo toma los valores $0, 1$), y en tal caso κ es fuertemente inaccesible,
- o bien $\kappa \leq 2^{\aleph_0}$ es débilmente inaccesible y existe una medida no trivial definida sobre todos los subconjuntos del intervalo $[0,1]$.

Scott se propuso estudiar la primera posibilidad. En primer lugar observamos que una medida bivaluada no trivial $\mu : \mathcal{P}X \longrightarrow \{0,1\}$ está completamente determinada por el conjunto U de los subconjuntos de X de medida 1 o, alternativamente, por su complementario, el conjunto P de los subconjuntos de X de medida 0. Y es inmediato que U es un filtro en X y que P es un ideal primo. En este punto necesitamos unas definiciones:

Definición Si μ es un cardinal infinito: Un ideal I en un conjunto X es *μ-completo* si la unión de menos de μ conjuntos de I está en I.

Un filtro F en un conjunto X es *μ-completo* si la intersección de menos de μ conjuntos de F está en F.

Los ideales / filtros $\aleph_1$-completos (es decir, cerrados para uniones / intersecciones numerables) se llaman *σ-completos.*

Una *medida de Ulam* en un conjunto X es un ultrafiltro no principal σ-completo en X.

Es inmediato que cada medida bivaluada $\mu : \mathcal{P}X \longrightarrow \{0,1\}$ no idénticamente nula se corresponde con un ideal primo σ-completo P en X o, equivalentemente, con un ultrafiltro σ-completo U. Que la medida sea no trivial (es decir, que los puntos tengan medida nula) equivale a que P (o U) no sea principal. Por lo tanto, la existencia de una medida bivaluada no trivial en $\mathcal{P}X$ equivale a la existencia de una medida de Ulam en X.

Notemos además que lo único que importa del conjunto X es su cardinal, pues si dos conjuntos X e Y tienen el mismo cardinal, a través de una biyección entre ellos podemos convertir cualquier medida en uno en una medida en el otro, con las mismas características, luego no perdemos generalidad si consideramos únicamente medidas sobre cardinales infinitos κ.

Definición Un cardinal κ es *medible Ulam* si existe una medida de Ulam U en κ.

Un cardinal κ es *medible*[192] si existe un ultrafiltro κ-completo no principal U en $\mathcal{P}\kappa$. En tal caso se dice que U es una *medida* en κ.

En la página 90 hemos demostrado que si existe una medida no trivial en un conjunto X y κ es el menor cardinal posible para X, entonces cualquier medida no trivial en X es κ-aditiva, luego, si la medida es bivaluada, el ultrafiltro correspondiente será κ-completo,[193] luego será una medida en κ. Por lo tanto:

Teorema Si κ es el menor cardinal medible Ulam, entonces es medible.

Scott no tiene en cuenta este hecho, pero nos permitirá entender mejor la situación. Notemos que si U es una medida en un cardinal κ, todos los puntos tienen medida nula, luego todos los conjuntos de cardinal $< \kappa$ son nulos (porque son unión de menos de κ conjuntos de cardinal 1). Equivalentemente, todos los conjuntos de medida 1 tienen cardinal κ.

Ulam había probado que el menor cardinal medible Ulam es fuertemente inaccesible, pero no cuesta nada demostrar algo más general:

Teorema Todo cardinal medible es fuertemente inaccesible.

Demostración: Si κ es un cardinal medible, es regular, es decir, no puede expresarse como unión de menos de κ conjuntos de cardinal $< \kappa$, pues sería una unión de menos de κ conjuntos nulos, luego la unión sería nula. Ciertamente, no puede ser numerable, pues entonces sería nulo. Sólo falta probar que para todo cardinal $\xi < \kappa$, se cumple que $2^\xi < \kappa$. Supongamos, por el contrario, que $2^\xi \geq \kappa$. Esto significa que el conjunto de todas las funciones $\xi \longrightarrow 2$ tiene cardinal mayor que κ, luego podemos tomar un conjunto X formado por funciones de este tipo con $|X| = \kappa$. Entonces podemos tomar una medida U en X. Para cada $\alpha < \xi$, tenemos que $X = \{f \in X \mid f(\alpha) = 0\} \cup \{f \in X \mid f(\alpha) = 1\}$. Sea $\epsilon_\alpha = 0, 1$ de modo que $X_\alpha = \{f \in X \mid f(\alpha) = \epsilon_\alpha\} \in U$. Entonces $X^* = \bigcap_{\alpha<\xi} X_\alpha \in U$, pero entonces debería ser un conjunto de cardinal κ, cuando en realidad tiene un único elemento, la función dada por $f(\alpha) = \epsilon_\alpha$. ∎

Volviendo al trabajo de Scott, éste considera también el menor cardinal medible Ulam, aunque no demuestra que es medible. Lo que vamos a ver ahora —siguiendo a Scott— vale para todo cardinal medible κ en el que hemos fijado una medida U.

[192] Scott llama cardinales medibles a los cardinales tales que existe una medida $\mu : \mathcal{P}\kappa \longrightarrow [0,1]$ no trivial, lo cual no coincide con las definiciones habituales hoy en día, que son las que estamos dando.

[193] La prueba muestra que si la medida (bivaluada) no es κ-aditiva, existe una medida en un cardinal menor que también es bivaluada, luego el teorema es válido para el menor cardinal con una medida bivaluada no trivial, es decir, para el menor cardinal medible Ulam.

Scott trabaja en NBG y considera la clase V^κ formada por todas las aplicaciones $f : \kappa \longrightarrow V$. En general, una aplicación es un conjunto si su dominio lo es, por lo que estas aplicaciones son conjuntos y está definida la clase V^κ formada por todas ellas, que puede verse como el producto cartesiano de V por sí misma κ veces.

Como decíamos, Scott construyó una ultrapotencia de V. Para ello sólo hace falta definir en V^κ las relaciones dadas por

$$f =_U g \leftrightarrow \{\alpha < \kappa \mid f(\alpha) = g(\kappa)\} \in U, \qquad f\, R_U\, g \leftrightarrow \{\alpha < \kappa \mid f(\alpha) \in g(\kappa)\} \in U.$$

La primera relación es de equivalencia, pero no podemos definir la clase de equivalencia $[f]_U$ de una función como la clase de todas las funciones relacionadas con ella porque sería una clase propia (mejor dicho, sí que podríamos definirla así, pero no nos interesa que sea una clase propia). Scott muestra cómo definir unas clases de equivalencia que cumplan el mismo papel siendo conjuntos, pero un camino más simple es usar el mismo truco que usaron Montague y Vaught (página 227) para definir los cardinales sin el axioma de elección: basta definir $[f]_U$ como el conjunto de todas las funciones relacionadas con f por $=_U$ de rango mínimo en la jerarquía de von Neumann. De este modo, si se cumple $f =_U g$, para cierta $g \subset V_\alpha$ y α es el mínimo posible, entonces $[f]_U \subset V_{\alpha+1}$ es un conjunto y, para $f, g \in V^\kappa$, se cumple que

$$[f]_U = [g]_U \leftrightarrow f =_U g \leftrightarrow \{\alpha < \kappa \mid f(\alpha) = g(\alpha)\} \in U.$$

Esto nos permite definir la clase de todas las clases de equivalencia. Scott no le da ningún nombre en concreto, pero podemos llamarla

$$\mathrm{Ult}^*_U(V) = \{[f]_U \mid f \in V^\kappa\}.$$

En esta clase tenemos definida la relación de pertenencia dada por

$$[f]_U\, R\, [g]_U \leftrightarrow \{\alpha < \kappa \mid f(\alpha) \in g(\alpha)\} \in U,$$

y también tenemos la aplicación $j^*_U : V \longrightarrow \mathrm{Ult}^*_U(V)$ dada por $j^*_U(x) = [c_x]$, donde $c_x : \kappa \longrightarrow V$ es la función constante $c_x(\alpha) = x$.

La demostración del teorema fundamental de los ultraproductos se adapta sin más que cambios obvios a este contexto, y nos da que, para cada fórmula metamatemática $\phi(x_1, \ldots, x_n)$, la fórmula siguiente es un teorema de NBG:

$$\bigwedge f_1 \cdots f_n \in V^\kappa(\phi^{\mathrm{Ult}^*_U(V),R}([f_1]^*_U, \ldots [f_n]^*_U) \leftrightarrow \{\alpha < \kappa \mid \phi(f_1(\alpha), \ldots, f_n(\alpha))\} \in U),$$

donde $\phi^{\mathrm{Ult}^*_U(V),R}$ es la fórmula que resulta de sustituir en ϕ cada $\in$ por R y cada $\bigwedge x, \bigvee x$ por $\bigwedge x \in \mathrm{Ult}^*_U(V)$, $\bigvee x \in \mathrm{Ult}^*_U(V)$, es decir, lo que entendería por ϕ alguien que tomara por conjuntos los elementos de $\mathrm{Ult}^*_U(V)$ y por "pertenencia" la relación R. En otras palabras:

> Para que unos conjuntos $[f_1]^*_U, \ldots, [f_n]^*_U$ de $\mathrm{Ult}^*_U(V)$ cumplan una propiedad (a ojos de alguien que llame conjuntos a los elementos de $\mathrm{Ult}^*_U(V)$ y tome por pertenencia la relación R) es necesario y suficiente que el conjunto de índices $\alpha < \kappa$ tales que $(f_1(\alpha), \ldots, f_n(\alpha))$ cumplen la propiedad tenga medida 1.

En particular:

$$\bigwedge a_1 \cdots a_n(\phi^{\mathrm{Ult}^*_U(V),R}(j^*_U(a_1), \ldots, j^*_U(a_n)) \leftrightarrow \phi(a_1, \ldots, a_n)).$$

Esto indica que j^*_U es una inmersión elemental, de modo que $a_1, \ldots, a_n$ tiene una propiedad si y sólo si sus imágenes la tienen en $\mathrm{Ult}^*_U(V)$.

Por lo tanto, $\mathrm{Ult}^*_U(V)$, con la relación R, cumple todos los axiomas de ZFC, pero Scott no se quedó ahí y demostró que este modelo puede colapsarse a un modelo transitivo.

Para eso Scott observa que el teorema del colapso de Mostowski vale también para clases propias (M, R) con tal de que la relación R cumpla una condición adicional obviamente necesaria, y es que la extensión de cada $a \in M$ sea un conjunto (pues si una función colapsante tiene que transformar un $a \in M$ en un conjunto cuyos elementos se correspondan con la extensión $E(a)$, es necesario que ésta sea un conjunto). Scott demostró que la relación R de la ultrapotencia cumple esta propiedad, así como que es extensional y bien fundada,[194] y eso asegura la existencia de una clase transitiva, que llamaremos $\mathrm{Ult}_U(V)$, y de una función colapsante biyectiva

$$\pi : \mathrm{Ult}^*_U(V) \longrightarrow \mathrm{Ult}_U(V)$$

[194] Para que esté bien fundada es esencial que la medida U sea σ-aditiva.

que transforma la relación R en la pertenencia usual. Esto hace que π sea un isomorfismo de modelos, por lo que, si llamamos $[f]_U = \pi([f]^*_U)$, tenemos que unos conjuntos $[f_1]^*_U, \dots, [f_n]^*_U$ de $\mathrm{Ult}^*_U(V)$ cumplen una propiedad en $\mathrm{Ult}^*_U(V)$ si y sólo si sus colapsos $[f_1]_U, \dots, [f_n]_U$ la cumplen en $\mathrm{Ult}_U(V)$. Si, por último, llamamos j_U a la composición de j^*_U con la función colapsante, llegamos a la situación siguiente:

> Para cada medida U en un cardinal medible κ, hemos definido una aplicación $j_U : V \longrightarrow \mathrm{Ult}_U(V)$ en una clase transitiva $\mathrm{Ult}_U(V)$ de modo que, para cada fórmula metamatemática $\phi(x_1, \dots, x_n)$, las fórmulas siguientes son teoremas de NBG:
>
> $$\bigwedge f_1 \cdots f_n \in V^\kappa(\phi^{\mathrm{Ult}_U(V)}([f_1]_U, \dots [f_n]_U) \leftrightarrow \{\alpha < \kappa \mid \phi(f_1(\alpha), \dots, f_n(\alpha))\} \in U),$$
>
> $$\bigwedge a_1 \cdots a_n(\phi^{\mathrm{Ult}_U(V)}(j_U(a_1), \dots, j_U(a_n)) \leftrightarrow \phi(a_1, \dots, a_n)),$$
>
> donde $\phi^{\mathrm{Ult}_U(V)}$ es la fórmula que resulta de cambiar todos los $\bigwedge x, \bigvee x$ de ϕ por $\bigwedge x \in \mathrm{Ult}_U(V)$, $\bigvee x \in \mathrm{Ult}_U(V)$.

La primera fórmula afirma que, si tomamos por conjuntos los conjuntos de $\mathrm{Ult}_U(V)$ (con la pertenencia usual), unos objetos $[f_1]_U, \dots, [f_n]_U$ cumplen una propiedad ϕ si y sólo si el conjunto de los $\alpha < \kappa$ tales que $(f_1(\alpha), \dots, f_n(\alpha))$ cumplen ϕ (considerando ahora todos los conjuntos) tiene medida 1.

La segunda fórmula afirma que j_U es una inmersión elemental, de modo que unos conjuntos $a_1, \dots, a_n$ cumplen una propiedad ϕ si y sólo si sus imágenes la cumplen a ojos de alguien que sólo vea los conjuntos de $\mathrm{Ult}_U(V)$.

Aplicando a sentencias el hecho de que j_U es elemental, tenemos que $\mathrm{Ult}_U(V)$ cumple todas las sentencias que cumple V, luego en particular $\mathrm{Ult}_U(V)$ es un modelo transitivo de ZFC.

Igualmente, teniendo en cuenta que "ser un ordinal" es absoluto para modelos transitivos de ZFC, tenemos que

$$\alpha \text{ es un ordinal} \leftrightarrow j_U(\alpha) \text{ es un ordinal}^{\mathrm{Ult}_U(V)} \leftrightarrow j_U(\alpha) \text{ es un ordinal.}$$

Por lo tanto, j_U se restringe a una aplicación $j_U : \Omega \longrightarrow \Omega$. Además, como j_U es elemental, si $\alpha \in \beta$, se cumple que $j_U(\alpha) \in j_U(\beta)$, es decir, que j_U es estrictamente creciente en Ω.

Esto implica que $\bigwedge \alpha \in \Omega\, \alpha \le j_U(\alpha)$, pues si existiera un α tal que $j_U(\alpha) < \alpha$, aplicando j_U tendríamos que $j_U(j_U(\alpha)) < j_U(\alpha))$, luego $j_U(\alpha)$ contradiría la minimalidad de α.

Ahora vamos a aprovechar que estamos suponiendo que U es κ-completa para demostrar algo que Scott no demuestra:

$$\bigwedge \alpha < \kappa\, j_U(\alpha) = \alpha.$$

En efecto, razonamos por inducción sobre α. Si es cierto para todo $\beta < \alpha$, tomemos un $[f]_U \in j_U(\alpha)$. Esto significa que

$$X = \{\delta < \kappa \mid f(\delta) \in c_\alpha(\delta) = \alpha\} \in U.$$

Para cada $\eta < \alpha$, sea $X_\eta = \{\delta < \kappa \mid f(\delta) = \eta\}$. Entonces $X = \bigcup_{\eta<\alpha} X_\eta$. Como U es κ-completa, si todos los conjuntos X_η fueran nulos, también lo sería X, que no lo es, luego existe un $\eta < \alpha$ tal que $X_\eta \in U$, lo cual significa que $[f]_U = [c_\eta]_U = j_U(\eta) = \eta < \alpha$ por hipótesis de inducción.

Con esto hemos probado que todo elemento de $j_U(\alpha)$ está en α, es decir, que $j_U(\alpha) \le \alpha$, y la otra inclusión se da siempre, luego $j_U(\alpha) = \alpha$.

Todo lo que hemos dicho hasta aquí valdría aunque el ultrafiltro U fuera principal, pero entonces podríamos probar que $\mathrm{Ult}_U(V) = V$ y que j_U es la identidad. En cambio, el hecho de que U no sea principal implica que j_U no es suprayectiva. En efecto, Scott toma la función $d \in V^\kappa$ dada por $d(\alpha) = \alpha$, y considera $\mu = [d]_U \in \mathrm{Ult}_U(V)$. Como

$$\{\alpha < \kappa \mid d(\alpha) \text{ es un ordinal}\} = \kappa \in U,$$

tenemos que $[d]_U$ es un ordinal en $\mathrm{Ult}_U(V)$, pero ser un ordinal es absoluto para modelos transitivos, así que $\mu = [d]_U$ es un ordinal. Además:

$$\{\alpha < \kappa \mid d(\alpha) < c_\kappa(\alpha)\} = \kappa \in U,$$

luego $\mu = [d]_U < [c_\kappa] = j_U(\kappa)$. Y, por último, si $\delta < \kappa$,

$$\{\alpha < \kappa \mid c_\delta(\alpha) < d(\alpha)\} = \kappa \setminus \delta \in U,$$

pues su complementario, δ es unión de menos de κ puntos de medida nula (aquí se usa que U no es principal), luego tiene medida nula gracias a la κ-aditividad de U. Por lo tanto, $\delta = j_U(\delta) = [c_\delta]_U < [d]_U = \mu$. Como esto vale para todo $\delta < \kappa$, hemos probado que:

$$\kappa \leq \mu < j_U(\kappa),$$

luego κ es el menor ordinal no fijado por j_U. Todos los ordinales $\kappa \leq \alpha < j_U(\kappa)$ no tienen antiimagen por j_U.

En resumen:

Teorema Si U es una medida en un cardinal medible κ, existe una inmersión elemental no trivial (es decir, distinta de la identidad) $j_U : V \longrightarrow \mathrm{Ult}_U(V)$ en un modelo transitivo de ZFC tal que κ es el menor cardinal que cumple $\kappa < j_U(\kappa)$.

Observemos que, en términos conjuntistas, por supuesto, $\mathrm{Ult}_U(V) \subset V$, pero la inmersión j_U nos permite ver a V como un submodelo de la ultrapotencia. En principio no tiene nada de especial que tengamos una aplicación $f : V \longrightarrow V$ inyectiva y no suprayectiva. Sirve, por ejemplo, $f(x) = x \times \{0\}$, pero en este caso hemos "expandido el universo", hemos sumergido la clase universal V en un modelo de ZFC mayor. Es cierto que, como clase, está contenida en V, pero hemos usado esta inclusión para mostrar que V puede verse como una parte de un modelo mayor de la teoría de conjuntos. Hemos "creado nuevos conjuntos".

Es fácil imaginar que esto abre muchas posibilidades de investigación, pero Scott se limitó a sacar una consecuencia rápida. Él supone desde el primer momento que $V = L$, y entonces concluye que

$$L \subset \mathrm{Ult}_U(V) \subset V = L$$

(porque, como hemos visto en la sección 86, la clase L está contenida en todos los modelos transitivos de ZFC que son clases propias), de modo que $\mathrm{Ult}_U(V) = V$ y lo que tenemos es una inmersión elemental no trivial:

$$j_U : V \longrightarrow V.$$

Ahora bien, esto es imposible, porque, si tomamos, concretamente, como κ el menor cardinal medible, como j_U es elemental, tendría que ser cierto también que $j_U(\kappa)$ es el menor cardinal medible,[195] es decir, que $j_U(\kappa) = \kappa$, cuando hemos probado que no se da la igualdad. Por lo tanto:

Teorema (Scott) Si existe una medida $\mu : \mathcal{P}X \longrightarrow [0,1]$ definida en todos los subconjuntos de un conjunto X, entonces $V \neq L$.

Demostración: Según el resultado de Ulam, pueden darse dos casos. En uno $2^{\aleph_0} \neq \aleph_1$ (pues tiene por debajo un cardinal débilmente inaccesible), luego $V \neq L$, ya que $V = L$ implica la hipótesis del continuo generalizada. El segundo caso es el que hemos analizado aquí y que nos ha llevado igualmente a que $V \neq L$. ∎

En un congreso celebrado en 1960, Tarski había anunciado algunos resultados sobre cardinales medibles, que finalmente publicaría en 1964 en un artículo conjunto con Keisler titulado *De los cardinales accesibles a los inaccesibles,* donde se aplican sistemáticamente las ultrapotencias de V para el estudio de los cardinales medibles. A raíz de estos hechos, Scott dice:

> *Aunque el menor cardinal medible, si es que existe, ahora se sabe que tiene que ser increíblemente grande, puesto que los resultados de Tarski se aplican a un número aparentemente inagotable de cardinales inaccesibles, todavía parece plausible a mucha gente, incluido el autor, suponer que estos cardinales existen.*

Los resultados a los que se refiere pueden deducirse fácilmente del hecho de que, eligiendo adecuadamente una medida D en κ, se puede exigir[196] que $\kappa = [d]_D$. Una medida D que cumpla esto es lo que se llama una *medida normal* en κ, y se caracteriza por que

$$X \in D \leftrightarrow \{\alpha < \kappa \mid \alpha \in X\} \in D \leftrightarrow \{\alpha < \kappa \mid d(\alpha) \in c_X(\alpha)\} \in D \leftrightarrow \kappa \in j_D(X).$$

[195] Si no suponemos $V = L$, lo único que concluimos de aquí es que $j_U(\kappa)$ es el menor cardinal medible a ojos de alguien que sólo vea $\mathrm{Ult}_U(V)$, pero esta propiedad no es absoluta y esto sólo implica que κ no es medible en $\mathrm{Ult}_U(V)$, y no da lugar a ninguna contradicción.

[196] Como $\kappa \in \mathrm{Ult}_U(V)$, existe $f : \kappa \longrightarrow V$ tal que $\kappa = [f]_U$. Es inmediato comprobar que $D = \{X \in \mathcal{P}\kappa \mid f^{-1}[X] \in U\}$ es una medida en κ. Sea $\kappa = [h]_D$. Sabemos que $[h]_D \leq [d]_D$. Si fuera $[h]_D < [d]_D$, entonces $\{\alpha < \kappa \mid h(\alpha) < \alpha\} \in D$, luego $\{\alpha < \kappa \mid h(f(\alpha)) < f(\alpha)\} \in U$. Si llamamos $g(\alpha) = h(f(\alpha))$, esto significa que $[g]_U < [f]_U = \kappa$, luego $[g]_U = \delta = j_U(\delta) < \kappa$, luego $\{\alpha < \kappa \mid g(\alpha) = \delta\} \in U$, luego $\{\alpha < \kappa \mid h(\alpha) = \delta\} \in D$, luego $\kappa = [h]_D = [c_\delta]_D = j_D(\delta) = \delta < \kappa$. Por lo tanto, tiene que ser $\kappa = [h]_D = [d]_D$.

Por ejemplo, sabemos que κ es fuertemente inaccesible, pero si "nos ponemos en el lugar de alguien que viva en $\mathrm{Ult}_D(\kappa)$", seguiremos viendo que κ es fuertemente inaccesible.

DEMOSTRACIÓN: Ante todo κ sigue siendo un cardinal en $\mathrm{Ult}_D(\kappa)$. Si no lo fuera, significaría que alguien que viva en la ultrapotencia vería una biyección $f : \xi \longrightarrow \kappa$, para cierto ordinal $\xi < \kappa$, pero no puede ver tal biyección porque no existe. (Al revés sí que puede pasar, que un ordinal no sea un cardinal, pero que alguien que viva en un modelo crea que sí que lo es.) Como $\omega \in \kappa$, esto lo ve también un habitante de la ultrapotencia, luego ve que κ no es numerable.

Tampoco puede ser que un habitante de la ultrapotencia crea que κ es singular, pues eso significa que vería $\kappa = \bigcup_{\alpha<\xi} A_\alpha$, donde $\xi < \kappa$ y cada A_ξ tiene cardinal $< \kappa$. Pero esto significa que ve biyecciones $f_\alpha : \xi_\alpha \longrightarrow A_\alpha$ con $\xi_\alpha < \kappa$, y si ve esas biyecciones, es que realmente $|A_\alpha| < \kappa$, con lo que realmente κ sería singular, cuando no lo es.

Por último, si alguien que vive en la ultrapotencia viera un cardinal $\xi < \kappa$ tal que $2^\xi \geq \kappa$, ese ξ no tendría por qué ser realmente un cardinal, pero sería sin duda un ordinal menor que κ, y vería una aplicación inyectiva $\kappa \longrightarrow \mathcal{P}^{\mathrm{Ult}_D(V)}\xi \subset \mathcal{P}(\xi)$, pero no puede ver tal aplicación porque no existe, ya que κ es fuertemente inaccesible, luego $|\mathcal{P}\xi| = 2^{|\xi|} < \kappa$. ∎

Entonces, como $[d]$ es fuertemente inaccesible$^{\mathrm{Ult}_D(V)}$, se cumple que

$$\{\alpha < \kappa \mid \alpha \text{ es fuertemente inaccesible}\} \in D.$$

Por lo tanto, hay κ cardinales fuertemente inaccesibles por debajo de κ. En particular, el menor cardinal fuertemente inaccesible no puede ser medible, sino que tiene que haber infinitos cardinales fuertemente inaccesibles por debajo de un cardinal medible.

Pero aún hay más. Si decimos que un cardinal κ tiene la propiedad[197] M si hay κ cardinales fuertemente inaccesibles bajo él, hemos probado que todo cardinal medible κ tiene la propiedad M, pero se comprueba como antes que alguien que viva en la ultrapotencia también ve que κ tiene la propiedad M. Y a su vez, esto implica que

$$\{\alpha < \kappa \mid \alpha \text{ tiene la propiedad M}\} \in D,$$

luego κ no sólo tiene infinitos cardinales fuertemente inaccesibles bajo κ, sino que tiene por debajo κ cardinales ξ con la propiedad de que cada uno de ellos tiene ξ cardinales fuertemente inaccesibles por debajo. En particular, el menor cardinal κ que tiene κ cardinales inaccesibles por debajo no puede ser medible, sino que un cardinal medible debe tener infinitos cardinales de este tipo por debajo. Y análogamente podríamos definir una propiedad M^2 consistente en tener por debajo κ cardinales M, etc. Con esto podemos formarnos una idea de lo grandes que son los cardinales medibles.

90 El castor laborioso Tibor Radó era un matemático húngaro que en 1929 emigró a los Estados Unidos y en **1962** cumplió 67 años. Ese año publicó su artículo *Sobre las funciones no computables,* en el que describió *"el juego del castor laborioso",*[198] cuyas reglas son las siguientes:

> *i. El concursante selecciona un entero positivo n y construye su propia máquina de Turing binaria de n cartas* [estados] [...]
>
> *ii. Inicia su máquina (con la Carta 1* [estado 1]*) en una cinta en blanco y se asegura de que se detenga después de un cierto número s de pasos.*
>
> *iii. Entrega su entrada* [el programa de su máquina], *así como el número de pasos s, a cualquier miembro (en regla) del Club Internacional del Castor Laborioso.*
>
> *iv. El árbitro verifica primero que la entrada se detenga exactamente después de s pasos. Cabe destacar que éste es un asunto decidible; el árbitro simplemente hace actuar la entrada, manteniéndola durante no más del número especificado de s turnos. Si la entrada no se detiene después de s turnos, se rechaza; si se detiene antes de s turnos, se devuelve al concursante para su corrección. Tras la verificación de la entrada, su puntuación es el número de unos que aparecen en la cinta al detenerse.*
>
> *Naturalmente, el campeón de* CL-*n es el concursante que ha conseguido la puntuación más alta (hasta el momento) en la clasificación de* CL-*n.*

[197] Los cardinales de Mahlo son cardinales que cumplen una propiedad ligeramente más fuerte, y todo lo que vamos a decir vale para cardinales de Mahlo.

[198] *Beaver* (castor) en inglés tiene un sentido aproximado al de "hormiguita" en castellano, que se emplea para describir a una persona laboriosa.

Más precisamente, considerando siempre máquinas de Turing con un alfabeto de dos signos (0, 1, entendiendo que una casilla con un 0 está en blanco) y en la que es obligatorio moverse a la izquierda o a la derecha en cada paso, Radó definió dos funciones: $\Sigma(n)$ es el máximo número de unos que puede escribir partiendo de una cinta en blanco una máquina de Turing con n estados activos que termine deteniéndose, y $S(n)$ es el máximo número de pasos que puede dar una máquina de Turing con n estados activos que termine deteniéndose. Se conocen los valores siguientes de estas funciones:

	1	2	3	4	5
$\Sigma(n)$	1	4	6	13	4 098
$S(n)$	1	6	21	107	47 176 870

Por ejemplo, la máquina de Turing descrita en la página 136 es la ganadora absoluta del concurso 3-CL, pues imprime el valor máximo posible de 6 unos, pero se detiene tras 14 pasos, cuando el récord está en 21. Una de las máquinas que consigue este récord (pero imprimiendo sólo 5 unos) es ésta:

	q_1	q_2	q_3
0	$1Dq_2$	$1Iq_2$	$1Iq_3$
1	$1Dq_0$	$0Dq_3$	$1Iq_1$

La tabla siguiente muestra el estado de la máquina y de la cinta en cada paso:

0	q_1	0	[0]	0	0	0	11	q_3	1	0	[1]	1	0
1	q_2	0	1	[0]	0	0	12	q_1	1	[0]	1	1	0
2	q_2	0	[1]	1	0	0	13	q_2	1	1	[1]	1	0
3	q_3	0	0	[1]	0	0	14	q_3	1	1	0	[1]	0
4	q_1	0	[0]	1	0	0	15	q_1	1	1	[0]	1	0
5	q_2	0	1	[1]	0	0	16	q_2	1	1	1	[1]	0
6	q_3	0	1	0	[0]	0	17	q_3	1	1	1	0	[1]
7	q_3	0	1	[0]	1	0	18	q_3	1	1	1	[0]	1
8	q_3	0	[1]	1	1	0	19	q_3	1	1	[1]	1	1
9	q_1	[0]	1	1	1	0	20	q_1	1	[1]	1	1	1
10	q_2	1	[1]	1	1	0	21	q_0	1	1	[1]	1	1

Lo que Radó demuestra en su artículo es:

Las funciones $\Sigma(n)$ y $S(n)$ no son recursivas.

Con ello proporciona ejemplos de funciones no recursivas construidas de una forma sencilla, sin recurrir a enumeraciones de las funciones recursivas y a argumentos de diagonalización.

Hay una razón obvia por la que la función $S(n)$ no puede ser recursiva, y es que si lo fuera resolvería el problema de la detención de las máquinas de Turing. Para saber si una máquina de Turing con n estados activos se detiene o no sólo habría que calcular $S(n)$ y dejarla funcionar hasta un máximo de $S(n)$ pasos. Si para entonces no se ha detenido, ya sabemos que nunca se detendrá. Esto si la máquina empieza con la cinta en blanco. Si queremos que una máquina T empiece con otra situación de la cinta, sólo tendríamos que encadenarla a otra máquina que, al empezar con la cinta en blanco, escriba en ella la situación inicial con que queremos que empiece T. No obstante, es fácil dar argumentos directos que justifiquen que dichas funciones no son recursivas:

Demostración: Supongamos que la función $S(n)$ fuera recursiva. Entonces existirá una máquina de Turing M que la calcula. A partir de ella podemos calcular otra máquina N que, cuando empieza con la cinta con el número n escrito en ella (es decir, con una sucesión de $n+1$ unos seguidos de modo que la casilla escrutada sea el último de ellos), haga lo siguiente:

1. Duplica el número de unos, con lo que el número escrito pasa a ser $2n + 1$.
2. Hace actuar M, de modo que en la cinta quedará escrito $2n + 1, S(2n + 1)$.

Llamemos n_0 al número de estados de la máquina N. Sea finalmente P la máquina de Turing que, al empezar con la cinta en blanco, hace lo siguiente:

1. Imprime n_0 (es decir, $n_0 + 1$ unos), para lo cual necesitará $n_0 + 1$ estados.
2. Hace actuar N, con lo que la cinta terminará con $2n_0 + 1, S(2n_0 + 1)$, y el programa completo tendrá $2n_0 + 1$ estados.

Pero, para dejar escrito $2n_0+1, S(2n_0+1)$ es necesario dar al menos $2n_0+2+S(2n_0+1)+1$ pasos (al menos un paso por cada uno que hay que escribir), luego tenemos una máquina con $2n_0+1$ estados que se detiene tras haber dado más de $S(2n_0+1)$ pasos, lo cual es una contradicción.

La prueba para $\Sigma(n)$ es idéntica: construimos una máquina con $2n_0+1$ estados que, cuando empieza con la cinta en blanco, acaba escribiendo $2n_0+2+\Sigma(2n_0+1)+1$ unos. ∎

91 La independencia de la hipótesis del continuo En **1963** murió Skolem, a los 75 años. Gödel tenía entonces 57 años, y unos días después de su cumpleaños recibió como regalo una carta de un profesor de 29 años de la universidad de Stanford llamado Paul Cohen, en la que le anunciaba que había demostrado que el axioma de elección y la hipótesis del continuo no podían demostrarse a partir de los axiomas de ZF y ZFC, respectivamente. Una semana más tarde Cohen le escribía otra carta en la que, por una parte, le confesaba su temor a que hubiera un fallo oculto en su argumento, y por otra su disgusto con los lógicos que la ponían en cuestión, lo que le resultaba especialmente molesto teniendo en cuenta la expectación que había suscitado entre los matemáticos no especialistas en lógica. Gödel le respondió con una carta muy amable en la que lo invitó a visitarlo. A pesar de que lo que le envió Cohen debía de ser una versión muy provisional y sin detallar, Gödel le dijo:

> *Permítame repetir que es un verdadero placer leer su demostración de la independencia de la hipótesis del continuo. Creo que, en todos los aspectos esenciales, ha presentado la mejor demostración posible, y esto no sucede a menudo. Leer su demostración tuvo en mí un efecto tan placentero como ver una obra de teatro realmente buena.*

Tras su encuentro, Gödel estudió la prueba de Cohen y la dio por válida. Tras la muerte de Gödel, Cohen recordaría así esos meses:

> *Volví a Princeton durante varios meses y tuve muchas reuniones con él. Planteé la cuestión de si, como se rumoreaba, había demostrado la independencia del axioma de elección. Respondió que sí, evidentemente mediante un método similar al mío, pero no me dio una idea precisa ni me explicó por qué su método fracasaba con la hipótesis del continuo. Su principal interés parecía residir en discutir la "verdad" o "falsedad" de estas cuestiones, no sólo en su indecidibilidad. Me pareció tener una creencia casi inquebrantable en esta postura "realista", que me resultó difícil compartir. Sus ideas se basaban en una profunda convicción filosófica sobre lo que la mente humana podía lograr. Admiraba profundamente esta fe en el poder y la belleza de la cultura occidental, como él la expresaba, y me habría gustado comprender mejor las fuentes de sus firmes convicciones. A través de nuestras conversaciones, me acerqué a su punto de vista, aunque nunca compartí del todo su perspectiva "realista", según la cual todas las cuestiones de la teoría de conjuntos eran, en última instancia, verdaderas o falsas.*

Constructibilidad relativa Antes de que Cohen anunciara sus resultados, los lógicos estaban convencidos de que no había forma de construir más modelos de la teoría de conjuntos esencialmente nuevos, más allá de la construcción de la clase L de Gödel y algunas ligeras variantes. Por ejemplo, en 1960 Lévy había publicado su trabajo *Una generalización de la noción de constructibilidad de Gödel* y en 1961 el húngaro András Hajnal había publicado *Sobre un teorema de consistencia conectado con el problema del continuo generalizado.*

- Lévy había definido una clase $L(A)$, que es el modelo de ZF que se obtiene por el mismo procedimiento que la clase L, pero, en vez de partir de $L_0=\varnothing$, se parte de $L_0(A)=A$ (supuesto que A sea transitivo), y luego se van tomando partes definibles $L_{\alpha+1}(A)=\mathcal{D}L_\alpha(A)$. Así, $L(A)$ resulta ser la menor clase propia que es un modelo de ZF (no necesariamente de ZFC) y que cumple $A\in L(A)$.

- Por su parte, Hajnal había definido una clase $L[A]$, que se define partiendo de $L_0[A]=\varnothing$, pero en la que $L_{\alpha+1}[A]=\mathcal{D}_A L_\alpha[A]$ se calcula "haciendo un poco de trampa" y admitiendo a los subconjuntos de $L_\alpha[A]$ que pueden definirse haciendo referencia a la pertenencia a A, aunque el conjunto A no esté en $L_\alpha[A]$. Más precisamente, los elementos de $\mathcal{D}_A X$ son los de la forma

$$\{x\in X \mid (X,A)\vDash \phi[x,x_1,\dots,x_n]\},$$

  donde $x_1,\dots,x_n\in X$ y ϕ es una fórmula del lenguaje de la teoría de conjuntos extendido con un relator monádico R de modo que, (X,A) es el modelo de este lenguaje cuyo universo es X, en el que la pertenencia

se interpreta como la pertenencia y en el que el relator R se interpreta como la relación $x \in A$. El modelo $L[A]$ siempre cumple el axioma de elección, pero no siempre[199] $A \in L[A]$. ∎

Pero ningún modelo de este tipo podía servir para demostrar la independencia de la hipótesis del continuo o del axioma de elección. En efecto, consideremos cualquier modelo M de ZF que sea una clase propia. Entonces, según vimos en la sección 86, automáticamente $L \subset M$. Si pudiéramos demostrar que en M falla el axioma de elección o la hipótesis del continuo, estaríamos demostrando que M contiene estrictamente a L, luego estaríamos demostrando que existen conjuntos no constructibles. ¡Pero Gödel había demostrado que no se puede demostrar que hay conjuntos no constructibles! Por lo tanto, por ahí no hay nada que hacer.

Cohen se había dado cuenta de esto, y por ello siguió otro camino. Su punto de partida era suponer la existencia de un modelo transitivo numerable M de ZFC + $V = L$. Entonces, según lo visto en la sección 86, tiene que ser $M = L_\lambda$, para cierto ordinal límite, y nada impide, *a priori,* construir otro modelo transitivo numerable N que contenga estrictamente a M. Si pudiéramos asegurar que M y N tienen los mismos ordinales, es decir que $N \cap \Omega = M \cap \Omega = \lambda$, entonces, sin contradecir que todo conjunto es constructible, los conjuntos constructibles "a ojos de alguien que viva en N" serían únicamente los de $M = L_\lambda$, es decir, que todos los conjuntos "nuevos" que estuvieran en $N \setminus M$, aun siendo constructibles, no serían constructibles en N (por falta de ordinales para construirlos), con lo que no hay inconveniente, en principio, a que se pueda demostrar que en un modelo de estas características no se cumpla el axioma de elección o la hipótesis del continuo.

Cohen construía un modelo N a partir de uno dado $M = L_\lambda$ imitando el proceso que Gödel había seguido para definir la clase L en su monografía de 1940, que no es la que hemos explicado aquí. Dicho trabajo se basaba en que Gödel sabía que, para que una clase L fuera un modelo de ZFC (que a su vez se pudiera convertir en un modelo de NBG definiendo adecuadamente las clases constructibles), era necesario y suficiente que estuviera cerrada para 8 operaciones conjuntistas elementales. Por ejemplo, la primera operación es $x, y \mapsto \{x, y\}$, de modo que se debe cumplir que si $x, y \in L$, entonces $\{x, y\} \in L$. La segunda es $x \mapsto \{(u, v) \mid u \in x \wedge v \in x \wedge u \in v\}$, de modo que si $x \in L$, se tiene que cumplir que $\{(u, v) \mid u \in x \wedge v \in x \wedge u \in v\} \in L$, etc.

Por ello, Gödel definía una biyección $H : \Omega \longrightarrow 9 \times \Omega \times \Omega$ y, a partir de ella, una función $F : \Omega \longrightarrow V$ de modo que si $H(\alpha) = (i, \beta, \gamma)$ (lo que, para $i > 0$, necesariamente implicaba que $\beta, \gamma < \alpha$), entonces:

- Si $i = 0$, $F(\alpha) = \{F(\delta) \mid \delta < \alpha\}$,
- Si $i = 1$, entonces $F(\alpha) = \{F(\beta), F(\gamma)\}$,
- Si $i = 2$, entonces $F(\alpha) = \{(F(\delta), F(\epsilon)) \mid \delta < \beta \wedge \epsilon < \beta \wedge F(\delta) \in F(\epsilon)\}$,
- Si $i = 3$, entonces $F(\alpha) = F(\beta) \setminus F(\gamma)$,
- Si $i = 4$, entonces $F(\alpha) = F(\beta) \cap (V \times F(\gamma))$, etc.

y luego definía $L = \{F(\alpha) \mid \alpha \in \Omega\}$. Por ejemplo, sabiendo que

$$H(0) = (0, 0, 0), \quad H(1) = (0, 1, 0), \quad H(2) = (1, 1, 0), \quad H(3) = (2, 1, 0), \quad H(4) = (3, 1, 0), \quad H(5) = (4, 1, 0),$$

podemos calcular

$$F(0) = \varnothing, \quad F(1) = \{\varnothing\} = 1, \quad F(2) = \{\varnothing, \{\varnothing\}\} = 2, \quad F(3) = \varnothing, \quad F(4) = \{\varnothing\} = 1, \quad F(5) = \varnothing.$$

Así, Gödel introducía los conjuntos constructibles uno a uno (con repeticiones): $F(0) = 0$ era el primer conjunto constructible, $F(1) = 1$ era el segundo conjunto constructible, etc. De este modo, si $x, y \in L$, existen ordinales tales que $x = F(\beta)$, $y = F(\gamma)$, luego, tomando α el ordinal correspondiente a $(1, \beta, \gamma)$, se cumple que $\{x, y\} = F(\alpha) \in L$, mientras que con el correspondiente a $(3, \beta, \gamma)$ se tiene que $x \setminus y = F(\alpha) \in L$, etc., y así L está cerrado para las ocho operaciones requeridas (el caso $i = 0$ sirve para ir acumulando los conjuntos ya construidos).

Igualmente, Cohen definía una función $F : \lambda \longrightarrow V$ y a su vez $N = F[\lambda]$, pero la definición de F era más compleja, porque, además de incluir las nueve operaciones de Gödel, necesitaba asegurarse de que N acabara conteniendo conjuntos "nuevos" que no están en M y que cumplieran condiciones deseadas. En realidad, Cohen no estaba imitando la construcción de L, sino la de $L(A)$. Primero introducía los elementos de un A adecuado, para asegurarse de que estuvieran en N y tener así el equivalente a $L_0(A) = A$, y luego ya pasaba a imitar la construcción de Gödel.

[199] Si llamamos $\bar{A} = A \cap L[A]$, entonces $L[A] = L[\bar{A}]$ y $\bar{A} \in L[\bar{A}]$.

Por ejemplo, pongamos que $\tau \in M$ es un cardinal no numerable en M (es decir, que alguien que "viva" en M piense que τ es un cardinal no numerable, cuando en realidad $\tau < \lambda$ es un ordinal numerable). Vamos a ver qué hace Cohen para construir un modelo N en el que se cumpla $2^{\aleph_0} \geq \tau$.

Para ello se propone elegir una familia (numerable) $\{a_\delta\}_{\delta<\tau}$ de subconjuntos de ω que, de momento, deja indeterminada (en el sentido de que en principio es una familia arbitraria y más adelante precisará cuál toma en concreto). El objetivo es que dicha familia esté en el modelo N de manera que "para alguien que viva en N", sea una familia de τ subconjuntos de ω. Esto requiere en particular que los "habitantes de N no vean la trampa" y sigan creyendo que τ (que no es más que un ordinal numerable) es un cardinal no numerable tan grande como creen "los habitantes de M".

Para ello, define la función F que enumerará los elementos de N de modo que:

- Si $\alpha \leq \omega$, entonces $F(\alpha) = \alpha$, con lo que ya tenemos en N los números naturales y ω.
- Si $\delta < \tau$, entonces $F(\omega + 1 + \delta) = a_\delta$, con lo que ya tenemos en N los conjuntos a_δ.
- Si $\tau \leq \alpha < \tau \cdot 3$ (producto de ordinales), $F(\alpha)$ recorre todos los pares $\{a_\delta, a_{\delta'}\}$ y todos los pares $(a_\delta, a_{\delta'})$, con lo que aseguramos que todos éstos estarán en N.
- $F(\tau \cdot 3) = W = \{(a_\delta, a_{\delta'}) \mid \delta < \delta' < \tau\}$, que es un buen orden en el conjunto $X = \{a_\delta \mid \delta < \tau\}$ con el que éste es similar a τ. Así, "alguien que viva en N" verá en particular que X se puede biyectar con τ.
- Para $\tau \cdot 3 < \alpha < \lambda$, la función F se define imitando la construción de Gödel, para que N resulte cerrado para las ocho operaciones conjuntistas básicas y una más que añade Cohen por razones técnicas.

Así, Cohen puede definir $N = \{F(\alpha) \mid \alpha < \lambda\}$, que es un conjunto numerable, pero que depende de la elección que se haga de los conjuntos a_δ, y no sirve cualquier elección, sino que hay que elegirlos adecuadamente para que pueda probarse que N es un modelo transitivo numerable de ZFC que viola la hipótesis del continuo.

Para ello Cohen define el *"lenguaje del forcing"* que es un lenguaje como el de la teoría de conjuntos, pero más complejo, porque, además de todos los signos del lenguaje de la teoría de conjuntos, incluye:

- Constantes F_α, con $\alpha < \lambda$, para nombrar[200] a cada elemento $F(\alpha)$ de N.
- Unos "cuantificadores limitados", de la forma $\bigwedge_\alpha$ y $\bigvee_\alpha$, para cada $\alpha < \lambda$, que se interpretarán como "para todo $F(\beta)$ con $\beta < \alpha$" y "existe un $F(\beta)$ con $\beta < \alpha$".

Cohen llama *fórmulas limitadas* a las que sólo tienen cuantificadores limitados, mientras que las fórmulas ilimitadas tienen también cuantificadores "normales". Cada fórmula limitada tiene asignado un rango, que es un par (α, r), donde $\alpha < \lambda$ es el mínimo ordinal tal que todos los cuantificadores están acotados por α y r es el número de cuantificadores.

Teniendo en cuenta que cada número natural n es $n = F(n)$ y cada a_δ es $a_\delta = F(\omega + 1 + \delta)$, entre las constantes del *lenguaje del forcing* tenemos las de la forma $\mathbf{n} = F_n$, que nombran a los números naturales, y las de la forma $\mathbf{a}_\delta = F_{\omega+1+\delta}$, que nombran a los conjuntos a_δ, que de momento son arbitrarios.

Con estas constantes podemos formar las sentencias de la forma $\mathbf{n} \in \mathbf{a}_\delta$ y $\mathbf{n} \notin \mathbf{a}_\delta$. Cohen llama *condiciones* a los conjuntos finitos P formados por sentencias de estos dos tipos que no sean contradictorios, es decir, que no contengan una sentencia y su negación. Por ejemplo, una condición es

$$P = \{\mathbf{5} \in \mathbf{a}_{\omega+7}, \mathbf{3} \notin \mathbf{a}_{89}\}.$$

Así, con cada elección posible de unos conjuntos $\{a_\delta\}_{\delta<\tau}$, cada condición se vuelve verdadera o falsa respecto a dicha elección. Por ejemplo, la condición P anterior será verdadera si el número natural 5 pertenece al conjunto $a_{\omega+7}$ y el número natural 3 no pertenece al conjunto a_{89}.

Recíprocamente, Cohen se propone definir adecuadamente una sucesión de condiciones

$$P_0 \subset P_1 \subset P_2 \subset \cdots$$

de manera que, para cada $n < \omega$ y cada $\delta < \tau$, alguna de ellas contenga una de las sentencias $\mathbf{n} \in \mathbf{a}_\delta$ o $\mathbf{n} \notin \mathbf{a}_\delta$, y así serán estas condiciones las que definirán los conjuntos $\{a_\delta\}_{\delta<\tau}$.

[200] Pero notemos que F_α no se define a partir de la función F. "Alguien que viva en M" nunca conocerá la función F, pero podemos definir, por ejemplo, $F_\alpha = (\alpha, 0)$, y así las constantes F_α están todas en M, y "alguien que viva en M" sabe cuál es la constante correspondiente a cada ordinal α.

Pero antes de entrar en ello, Cohen define, por inducción sobre el rango de una fórmula limitada ϕ, una propiedad que llama "P fuerza ϕ". La definición es puramente técnica, con el objeto de que pueda calcularla mecánicamente "alguien que viva en M", es decir, alguien que tome por "conjuntos" únicamente los conjuntos de M y que, en particular, aunque vea las fórmulas del *lenguaje del forcing,* no sepa atribuir un significado a las constantes $\mathbf{a}_\delta$ (porque los conjuntos a_δ los vamos a elegir fuera de M). Por ejemplo, "alguien que viva en M" puede considerar la afirmación:

$$\{\mathbf{5} \in \mathbf{a}_{\omega+7}, \mathbf{3} \notin \mathbf{a}_{89}\} \text{ fuerza } F_{\tau\cdot 8+\omega+7} \in \mathbb{R}$$

y, aunque no sepa quiénes son $a_{\omega+7}$, a_{89} ni quién es $F(\tau\cdot 8+\omega+7)$, sin más que analizar la condición P (que sí que ve) y la fórmula ϕ (que sí que ve), aplicando la definición de "forzar", puede comprobar si la afirmación es cierta o no. Y el resultado clave es que, aunque "alguien que viva en M" no lo sepa, si determina que una afirmación del tipo "P fuerza ϕ" es verdadera, eso implica que si la condición P es verdadera (para una elección de los conjuntos a_δ), entonces la fórmula ϕ es verdadera en el modelo N construido con dichos conjuntos a_δ.

Dicho de otro modo: alguien que "vive en M" puede decir: *yo no sé si es cierto o no que* 5 *está en* $a_{\omega+7}$ *o si* 3 *no está en* a_{89}*, ni tampoco sé qué conjunto es* $F(\tau\cdot 8+\omega+7)$*, pero lo que sí que sé es que, si se cumple que* 5 *está en* $a_{\omega+7}$ *y que* 3 *no está en* a_{89}*, teniendo en cuenta cómo se construye* $F(\tau\cdot 8+\omega+7)$ *a partir de los* a_δ *desconocidos para mí, puedo afirmar (o, por el contrario, sólo con esos datos no se puede asegurar) que alguien que considere como conjuntos los objetos (desconocidos para mí) que nombran los términos* F_α*, juzgará que* $F(\tau\cdot 8+\omega+7)$ *es un número real.*

Una vez ha definido "P fuerza ϕ" para fórmulas limitadas, Cohen extiende la definición a fórmulas arbitrarias por inducción sobre el número de cuantificadores de ϕ, de modo que lo dicho anteriormente sigue siendo cierto: aunque "alguien que viva en M" no conoce los conjuntos a_δ, ni mucho menos los conjuntos que nombra cada término F_α, pero sí que tiene información suficiente para determinar si una condición dada fuerza o no una fórmula dada, y con ello está comprobando que, en el supuesto de que los a_δ hagan verdadera la condición, la fórmula ϕ será verdadera para "alguien que viva en la extensión N del modelo M".

Podemos pensar entonces que cada condición P contiene información parcial sobre el modelo N (que será verídica si la condición es verdadera), y cuanto mayor es la condición, más información contiene. Esto se plasma en dos hechos básicos:

1. Si $P \subset P'$ son condiciones y P fuerza una fórmula ϕ, entonces P' también fuerza ϕ.
2. Si P es una condición y ϕ es una fórmula, entonces existe una condición P' que extiende a P tal que P' fuerza ϕ o P' fuerza $\neg\phi$.

El primer hecho expresa que, cuantos más datos tenemos, más podemos concluir, y el segundo expresa que si una condición P no contiene información suficiente para responder a una pregunta sobre si N cumple o no una determinada fórmula ϕ, siempre es posible responderla añadiendo algunos datos más a los disponibles (pero sin contradecir los que ya tenemos).

Y éste es el punto crucial en el que usamos que el modelo M de partida es numerable. El *lenguaje del forcing* tiene una constante para cada $\alpha < \lambda$ y un cuantificador limitado para cada $\alpha < \lambda$. Como λ es un ordinal numerable, el *lenguaje del forcing* tiene una cantidad numerable de signos, como cualquier lenguaje formal usual, y, por consiguiente, tiene una cantidad numerable de fórmulas, luego podemos considerar una enumeración $\{\phi_k\}_{k<\omega}$ de todas ellas.[201] A partir de esta enumeración y, teniendo en cuenta las propiedades precedentes, podemos construir una sucesión de condiciones

$$P_0 \subset P_1 \subset P_2 \subset \cdots$$

de modo que cada P_k fuerce ϕ_k o su negación.[202] En particular, para cada $n < \omega$ y cada $\delta < \tau$, una de estas condiciones fuerza si $\mathbf{n} \in \mathbf{a}_\delta$ o $\mathbf{n} \notin \mathbf{a}_\delta$, lo que permite definir el conjunto a_δ precisamente como el conjunto de los n tales que alguna condición de la sucesión elegida fuerza que $\mathbf{n} \in \mathbf{a}_\delta$. Así tenemos definida una sucesión $\{a_\delta\}_{\delta<\tau}$ que hace verdaderas todas las condiciones P_n. A partir de aquí consideramos concretamente el conjunto N construido a partir de estos conjuntos.

[201] Notemos que, desde el punto de vista de "alguien que viva en M", la situación es muy diferente, pues para él λ es la clase de todos los ordinales, luego, aunque puede ver, ciertamente, todas las fórmulas del *lenguaje del forcing,* para él no son un conjunto numerable, sino una clase propia.

[202] En realidad Cohen hace que P_{2k} decida ϕ_k o su negación, y usa las condiciones P_{2k+1} para garantizar que se cumpla otra condición técnica.

En **1963** Cohen publicó la primera parte de *La independencia de la hipótesis del continuo,* donde anunciaba:

> TEOREMA 1. *Existen modelos de* ZF *en los que se cumple lo siguiente:*
>
> *(1) Existe un conjunto a, $a \subset \omega$, tal que a no es constructible en el sentido de la referencia 3, pero que cumple tanto el axioma de elección como la hipótesis del continuo generalizada.*
>
> *(2) El continuo (es decir, $\mathcal{P}\omega$, donde $\mathcal{P}$ significa conjunto-potencia) no admite un buen orden.*
>
> *(3) El axioma de elección se cumple, pero $\aleph_1 \neq 2^{\aleph_0}$.*
>
> *(4) El axioma de elección falla para una familia numerable*[203] *de pares de $\mathcal{P}(\mathcal{P}\omega)$.*
>
> *Sólo se analizará la parte 3 en este artículo. En las partes 1 y 3, el universo está bien ordenado por una relación definible. Nótese que 4 implica que $\mathcal{P}(\mathcal{P}\omega)$ no puede ser totalmente ordenado.*

y presentaba la construcción que acabamos de describir, mientras que en **1964** se publicó la segunda parte, en la que probaba (laboriosamente) los hechos siguientes:

1. N es un modelo transitivo numerable de ZFC.
2. Los ordinales de N son los mismos que los de M, es decir, que $N \cap \Omega = M \cap \Omega = \lambda$.
3. Los cardinales de N son los mismos que los de M, es decir, que "alguien que viva en N" creerá que un ordinal de los que ve es un cardinal (es decir, que no puede biyectarse con un ordinal menor) si y sólo si "alguien que viva en M" cree lo mismo. Por ejemplo, si $\tau = \aleph_2^M$, entonces también[204] $\tau = \aleph_2^N$.
4. $X = \{a_\delta\}_{\delta<\tau} \in N$ es un subconjunto de $\mathcal{P}^N\omega$ de cardinal^N τ. Por lo tanto, "a ojos de alguien que viva en N", se cumple que[205] $2^{\aleph_0} \geq \tau$.
5. Más aún, si en M se cumple que $\tau^{\aleph_1} = \tau$ (lo cual pasa, por ejemplo, si $\tau = 2^{\aleph_1} = \aleph_2$) entonces en N se cumple que $2^{\aleph_0} = 2^{\aleph_1} = \tau$, tal y como a Lusin le hubiera gustado[206] (véase la nota de la página 161).

En definitiva, Cohen había demostrado una amplia variedad de resultados del estilo de:

> Si ZFC es consistente,[207] también lo es ZFC más $2^{\aleph_0} = 2^{\aleph_1} = \aleph_2$, o $2^{\aleph_0} = \aleph_{\omega+5}$, etc.

La idea básica subyacente a la prueba es muy simple: partimos de un modelo transitivo numerable M de ZFC + $V = L$. En dicho modelo, $\mathcal{P}\omega$ es un conjunto numerable. Alguien "que vive en M" sólo ve una cantidad numerable de subconjuntos de ω, pero él cree que son $\aleph_1$, pero eso sólo significa que ve una biyección entre "su" $\mathcal{P}\omega$, es decir, el conjunto $\mathcal{P}^M\omega = \mathcal{P}\omega \cap M$ y "su" $\aleph_1$, es decir, el ordinal $\aleph_1^M$, que es un ordinal numerable, el menor para el que no existe en M una biyección con ω (aunque sí que la haya fuera de M). Tomamos entonces un cardinal τ no numerable en M, por ejemplo, $\tau = \aleph_2^M$, que es un ordinal numerable, pero alguien que vive en M cree que no se puede biyectar, no ya con ω, sino tampoco con $\aleph_1^M$. Elegimos (muy astutamente) una familia $\{a_\delta\}_{\delta<\tau}$ de subconjuntos de ω que no están en M. Esto no tiene nada de paradójico: $\mathcal{P}\omega$ es no numerable, y sólo una cantidad numerable de sus elementos está en M, nada nos impide tomar otra cantidad numerable fuera de M. Pero, con la elección astuta de Cohen, esta cantidad numerable de subconjuntos de ω se integra como parte de un nuevo modelo N de ZFC donde parece tener cardinal $\tau = \aleph_2^M = \aleph_2^N$, y así obtenemos un modelo en el que $2^{\aleph_0} = \aleph_2$. En realidad no "nos hemos sacado de la manga" $\aleph_2$ subconjuntos de ω, sino que

[203] Esto significa que existe una familia $\{P_n\}_{n=0}^{\infty}$ de conjuntos tales que cada $P_n \subset \mathcal{P}(\mathcal{P}\omega))$ tiene dos elementos la cual no tiene una función de elección. Si $\mathcal{P}(\mathcal{P}\omega))$ admitiera un orden total, siempre se podría elegir el menor elemento de cada par. Notemos que $\mathcal{P}\omega$ sí que admite un orden total, porque se puede biyectar con $\mathbb{R}$ sin necesidad del axioma de elección, y $\mathbb{R}$ admite un orden total.

[204] Esto, en principio, no tendría por qué pasar. Por ejemplo, en la construcción de N se podría "haber colado" una biyección entre $\aleph_1^M$ y ω, con lo que, "a ojos de alguien que viva en N", $\aleph_1^M$ ya no sería un cardinal y, para él, $\aleph_2^M = \aleph_1^N$, supuesto que no se "hubiera colado también" una biyección que le hiciera ver que $\aleph_2^M$ es numerable. Pero nada de esto sucede realmente.

[205] Más precisamente, se cumple $2^{\aleph_0} = \tau$ salvo que τ pueda expresarse como unión numerable de cardinales menores que τ, en cuyo caso $2^{\aleph_0} = \tau^+$.

[206] Lusin había muerto en 1950, a los 66 años.

[207] En realidad, Cohen supone la consistencia de ZFC más la existencia de un modelo transitivo de ZFC, que es algo un poco más fuerte. En la parte final de su segundo artículo explica que esta hipótesis se puede eliminar: si, por ejemplo, ZFC + $2^{\aleph_0} = \aleph_7$ fuera contradictorio, se podría probar una contradicción, digamos $0 \neq 0$, a partir de un conjunto finito Δ de sus axiomas, pero para garantizar que N cumple los axiomas Δ (más $2^{\aleph_0} = \aleph_7$) es suficiente con que M cumpla una cantidad finita Γ de axiomas de ZFC + $V = L$, y la existencia de un modelo transitivo numerable de cualquier conjunto finito de axiomas de ZFC es demostrable en ZFC (es el teorema de reflexión). Entonces en ZFC se puede demostrar que existe un modelo transitivo numerable N de ZFC + Δ en el cual se tiene que cumplir $0 \neq 0$, lo cual es absoluto, luego habríamos demostrado $0 \neq 0$ en ZFC, que sería, por consiguiente, contradictorio.

meramente hemos hecho que una cantidad numerable de subconjuntos de ω parezcan ser $\aleph_2$. El truco no es añadir a N muchos subconjuntos de ω (sólo añadimos una cantidad numerable) sino asegurarnos de que en N no entra ninguna biyección entre los subconjuntos añadidos y ω (o $\aleph_1^M$).

Sin embargo, cuando esta segunda parte fue publicada, a Cohen ya "le habían quitado de las manos" el *forcing*. La primera versión de su artículo había circulado en abril de 1963 en copias *offset,* y en mayo Cohen había impartido una conferencia sobre su técnica en el Instituto de Estudios Avanzados de Princeton. En junio Scott ya había observado que la definición de "forzar" se podía simplificar. En efecto, la definición de Cohen requería expresar cada fórmula del *lenguaje del forcing* en forma prenexa, es decir, con todos los cuantificadores al principio, mientras que Scott mostró cómo podía trabajarse con fórmulas arbitrarias modificando la definición de "P fuerza $\neg\phi$", a saber:

$P \Vdash \neg\phi$ si y sólo si no existe ninguna extensión $P' \supset P$ tal que $P' \Vdash \phi$,

donde usamos la notación $P \Vdash \phi$ que introdujo Scott y que ahora es estándar para expresar que P fuerza ϕ.

Solomon Feferman (que se había doctorado en 1957 bajo la dirección de Tarski) observó que $\Vdash$ tenía tendencias intuicionistas, pues podía darse el caso de que $P \Vdash \neg\neg\phi$ sin que fuera cierto $P \Vdash \phi$. Esto sucede si una condición P no permite determinar si ϕ tiene que ser cierta o no en N, pero todas las extensiones que permiten determinarlo lo hacen en el sentido de que sí que es cierta. Sin embargo, Feferman definió $P \Vdash_d \phi$ (P *fuerza débilmente* ϕ) como $P \Vdash_f \neg\neg\phi$, donde $P \Vdash_f \phi$ (P *fuerza fuertemente* ϕ) es la relación definida por Cohen, y probó que una condición fuerza una fórmula en sentido débil si y sólo si fuerza cualquier fórmula equivalente en ZF. Más aún $P \Vdash_d \phi$ se cumple si y sólo si ϕ es cierta en todo modelo N obtenido a partir de una sucesión de condiciones que haga verdadera a P (la novedad es el "sólo si").

En verano, Stanley Tennenbaum, uno de los matemáticos más allegados a Gödel, ya había usado el *forcing* para construir un modelo de ZFC en el que existe un árbol de Suslin.

Mientras tanto, Cohen también hizo algunos avances. En su prueba de la independencia de la hipótesis del continuo, había tenido que asegurar que todos los cardinales de M seguían siendo cardinales en N, lo cual, como hemos señalado, no es obvio en absoluto. Él mismo obtuvo una variante en la que en el modelo N había una biyección entre $\aleph_1^M$ y ω, y entonces se dice que el cardinal $\aleph_1^M$ se ha *colapsado,* ha dejado de ser un cardinal en N. Pero, "a ojos de alguien que viva en N" el modelo $M = L_\lambda$ es la clase de los conjuntos constructibles (porque en N no hay más ordinales, luego "alguien que viva en N" no reconoce más conjuntos constructibles que los de M), luego si en N hay una biyección entre $\aleph_1^M$ y ω, lo que está viendo "alguien que viva en N" es una biyección entre $\aleph_1^L$ y ω. Por lo tanto:

Si ZFC es consistente, también lo es ZFC + $\aleph_1^L$ es numerable.

Esto significa que es ingenuo interpretar el hecho de que L cumple $2^{\aleph_0} = \aleph_1$ como que hay $\aleph_1$ números reales constructibles, por lo que, si nos quedamos sólo con los conjuntos constructibles, entonces vemos $\aleph_1$ números reales. Esto es posible, pero también puede ocurrir que sólo haya $\aleph_0$ números reales constructibles, y que si nos quedamos sólo con los conjuntos constructibles, también estamos descartando todas las biyecciones entre $\mathbb{R}^L = \mathbb{R} \cap L$ y ω, con lo que, aunque sólo nos quede una cantidad numerable de números reales, nos parece que son $\aleph_1$, porque todas las biyecciones que prueban su numerabilidad son no constructibles y nos hemos deshecho de ellas.

Antes de septiembre, Lévy había llevado esto mucho más lejos y, partiendo de un modelo transitivo numerable de ZFC + $V = L$ que contuviera un cardinal inaccesible κ, mostró cómo construir N de forma que incluyera biyecciones entre ω y todos los cardinales menores que κ en M (que en realidad son todos ordinales numerables), pero no entre ω y κ, de modo que κ, "a ojos de alguien que viva en N", pasa a ser el primer cardinal no numerable, es decir, $\aleph_1$. Con esto había demostrado:

Teorema (Lévy) Si ZFC más la existencia de un cardinal inaccesible es consistente, también lo es ZFC más "$\aleph_1$ es inaccesible en L".

Observemos que suponer "$\aleph_1$ es inaccesible en L" implica que hay muchos ordinales numerables que, "a ojos de alguien que viva en L", son cardinales, es decir, que no hay biyecciones (constructibles) entre ellos y ordinales menores. En particular, $\aleph_1^L$ es un ordinal numerable.

Por su parte, Feferman construyó un modelo de ZF en el que un subconjunto no numerable de $\mathbb{R}$ es unión numerable de conjuntos numerables, y Lévy modificó el argumento hasta lograr que el propio $\mathbb{R}$ fuera una unión

numerable de conjuntos numerables. Feferman y Lévy publicaron una nota titulada *Resultados de independencia en la teoría de conjuntos por el método de Cohen,* en la que se anunciaba el resultado siguiente:

> Si ZF es consistente, también lo es ZF más el supuesto de que tanto $\aleph_1$ como $\mathbb{R}$ pueden expresarse como uniones numerables de conjuntos numerables.

Robert Solovay, que estaba elaborando su tesis sobre geometría diferencial bajo la dirección de Mac Lane (y la leyó en **1964**) había asistido a la conferencia de Cohen, y fue él quien calculó el valor exacto de $2^{\aleph_0}$ en el modelo en el que Cohen adjuntaba τ conjuntos genéricos (Cohen no sabía si era $2^{\aleph_0}=\tau$ o $2^{\aleph_0}=\tau^+$). También le escribió a Cohen para indicarle cómo se podía evitar la hipótesis de la existencia de un modelo transitivo numerable de ZFC como punto de partida. En una conferencia que Cohen dio unos días más tarde, éste planteó el problema de si podía construirse un modelo de ZF en el que todo subconjunto de $\mathbb{R}$ fuera medible Lebesgue, a finales de **1964** ya lo había resuelto. A partir de ese momento se dedicó, junto con Tennenbaum, a tratar de construir un modelo en el que no hubiera árboles de Suslin. Tenían claro cómo hacer que un árbol de Suslin en un modelo M dejara de serlo en una extensión N obtenida por *forcing,* pero el problema era que no bastaba con "destruir un árbol de Suslin", sino que había que acabar, no sólo con todos los que hubiera en M, sino también con los que aparecieran nuevos en N, para lo cual estaban tratando de construir una sucesión de extensiones de modo que en cada una se "destruyera un árbol de Suslin" y de modo que al final del proceso no quedara ninguno.

Sin embargo, durante varios años estos resultados permanecieron inéditos, porque, al tiempo que se obtenían nuevos resultados, se obtenían cada vez versiones más generales de la teoría de Cohen, para no tener que estar repitiendo todas las comprobaciones en cada variante del argumento. Pero no había una forma única de hacerlo y se barajaban constantemente nuevas propuestas y variantes. La apreciación de Gödel de que Cohen "había presentado la mejor demostración posible" estaba siendo desmentida a marchas forzadas.

La primera publicación sobre *forcing,* aparte del artículo de Cohen, fue una tesis doctoral, pues obviamente el doctorando no tenía ningún interés en posponer la lectura de su tesis. Se trataba de William Bielow Easton, que en **1964** leyó su tesis titulada *Potencias de cardinales regulares,* realizada bajo la dirección de Church.

En ella generalizaba al máximo la idea inicial de Cohen para obtener un resultado muy general sobre las posibilidades de la "función del continuo" (la función $\kappa \mapsto 2^\kappa$). Para enunciar su resultado necesitamos el concepto de cofinalidad de un cardinal infinito:

> Si κ es un cardinal infinito, su *cofinalidad* es el menor cardinal μ necesario para obtener un conjunto de cardinal κ uniendo μ conjuntos de cardinal menor que κ o, equivalentemente, el menor cardinal μ que permite expresar $\kappa=\sum_{\alpha<\mu}\mu_\alpha$, con $\mu_\alpha<\kappa$. Se representa por $\mu=\operatorname{cf}\kappa$.

En estos términos, un cardinal κ es regular si y sólo si $\operatorname{cf}\kappa=\kappa$. En cambio, $\operatorname{cf}\aleph_\omega=\aleph_0$, pues podemos obtener un conjunto de cardinal $\aleph_\omega$ sin más que unir un conjunto de cardinal $\aleph_0$ con otro de cardinal $\aleph_1$, con otro de cardinal $\aleph_2$, etc., luego $\aleph_\omega$ se puede poner como suma de una cantidad numerable de cardinales menores.

El teorema de Kőnig (página 36) tiene varias consecuencias sobre la exponenciación de cardinales:

> **Teorema de Kőnig (3)** Si κ es un cardinal infinito, entonces:
>
> $$\kappa^{\operatorname{cf}\kappa}>\kappa, \qquad \operatorname{cf}2^\kappa>\kappa.$$

Demostración: Por definición de cofinalidad, $\kappa=\sum_{\alpha<\operatorname{cf}\kappa}\mu_\alpha$, con $\mu_\alpha<\kappa$, luego el teorema de Kőnig de la página 36 nos da que

$$\kappa=\sum_{\alpha<\operatorname{cf}\kappa}\mu_\alpha<\prod_{\alpha<\operatorname{cf}\kappa}\kappa=\kappa^{\operatorname{cf}\kappa}.$$

Si fuera $\operatorname{cf}2^\kappa\le\kappa$, entonces $(2^\kappa)^{\operatorname{cf}2^\kappa}\le(2^\kappa)^\kappa=2^\kappa$, en contradicción con la desigualdad precedente. ∎

Así pues, en principio, nada impide que $2^{\aleph_0}=\aleph_7$ o que $2^{\aleph_0}=\aleph_{\omega+1}$, pero es imposible que $2^{\aleph_0}=\aleph_\omega$, pues $2^{\aleph_0}$ tiene que tener cofinalidad no numerable.

Ahora ya podemos enunciar el teorema que obtuvo Easton:

Teorema de Easton Si M es un modelo transitivo numerable de ZFC[208] en el que se cumple la hipótesis del continuo generalizada y sea G una función definida sobre el conjunto de los cardinales regulares de M definible en M mediante una fórmula y que cumpla las condiciones siguientes:

1) $G(\kappa)$ es un cardinal en M tal que $\operatorname{cf} G(\kappa) > \kappa$.

2) Si $\kappa \leq \mu$, entonces $G(\kappa) \leq G(\mu)$.

Entonces existe un modelo transitivo numerable N de ZFC que contiene a M, cuyos cardinales son los mismos que los de M y, para todo cardinal regular κ de N (o de M), en N se cumple que $2^\kappa = G(\kappa)$.

En particular, si ZFC es consistente también lo es al añadir como axioma, por ejemplo,

$$2^{\aleph_0} = \aleph_5, \quad 2^{\aleph_1} = 2^{\aleph_2} = \aleph_7, \quad 2^{\aleph_3} = \aleph_{\omega^2+5}, \quad 2^{\aleph_4} = \aleph_{\omega_5}.$$

En cambio, la técnica de Easton no permitía decidir el valor de ninguna potencia 2^κ cuando κ es un cardinal singular. En el modelo N, el valor de 2^κ para κ singular era el supremo μ de los cardinales 2^ν, con $\nu < \kappa$, salvo que $\operatorname{cf}\mu \leq \kappa$, en cuyo caso $2^\kappa = \mu^+$. En otras palabras, era el menor valor posible consistente con los valores fijados para las potencias 2^ν con ν regular y el teorema de Kőnig.

92 La Introducción a la lógica matemática de Mendelson En 1955 se había doctorado bajo la dirección de Rosser Elliott Mendelson, que en **1964** publicó su *Introducción a la lógica matemática,* que no tardaría en convertirse en un texto de referencia en el área. En la introducción, tras explicar brevemente de qué trata la lógica, dice:

> *Aunque la lógica es fundamental para todos los demás estudios, su carácter fundamental y aparentemente evidente desalentó cualquier investigación lógica profunda hasta finales del siglo XIX. Posteriormente, impulsado por el descubrimiento de las geometrías no euclídeas y el deseo de proporcionar una base rigurosa para el análisis, resurgió el interés por la lógica. Sin embargo, este nuevo interés seguía siendo bastante escaso hasta que, a principios de siglo, el mundo matemático se vio conmocionado por el descubrimiento de las paradojas, es decir, argumentos que conducen a contradicciones.*

Luego expone las paradojas más famosas y explica el planteamiento logicista de Russell y el método axiomático de Zermelo como formas de neutralizarlas. Sobre el intuicionismo dice:

> *Brouwer y su escuela intuicionista han defendido una interpretación más radical de las paradojas. Se niegan a aceptar la universalidad de ciertas leyes lógicas básicas, como la ley del tercio excluso: P o no-P. Dicha ley, afirman, es cierta para conjuntos finitos, pero no es válido extenderla de forma generalizada a todos los conjuntos. Asimismo, afirman que no es válido concluir que "existe un objeto x tal que no-$P(x)$" se sigue de "no-(para todo $x, P(x)$)"; estamos justificados al afirmar la existencia de un objeto con una propiedad determinada sólo si conocemos un método eficaz para construir (o encontrar) dicho objeto. Las paradojas, por supuesto, no son derivables (ni siquiera significativas) si obedecemos las restricciones intuicionistas, pero, por desgracia, también lo son muchos teoremas apreciados de las matemáticas cotidianas y, por esta razón, el intuicionismo ha encontrado pocos adeptos entre los matemáticos.*

La introducción termina de un modo sorprendente:

> *Para el principiante absoluto, se presentará aquí un resumen de algunas de las ideas y resultados básicos utilizados en el texto. Se recomienda al lector omitir estas explicaciones ahora y, si es necesario, consultarlas más adelante. Un conjunto es una colección de objetos.*(∗) *Los objetos de la colección se denominan elementos del conjunto, y escribiremos "$x \in y$" para la afirmación de que x es un elemento de y.*
>
> (∗)*No se especificará aquí qué colecciones de objetos forman conjuntos. Se procurará evitar el uso de ideas o procedimientos que puedan conducir a paradojas; todos los resultados pueden formalizarse en la teoría axiomática de conjuntos del Capítulo 4. El término "clase" se utiliza a veces como sinónimo de "conjunto", pero se evitará aquí porque tiene un significado diferente en el Capítulo 4. Si la propiedad $P(x)$ determina un conjunto, éste suele denotarse como $\{x \mid P(x)\}$.*

[208] En realidad Easton trabaja con NBG, que entonces era la teoría de conjuntos habitual.

A continuación introduce rápidamente todos los conceptos conjuntistas básicos, empezando con uniones e intersecciones y terminando con álgebras de Boole, pasando por productos cartesianos, relaciones, funciones, inducción, etc. En suma, establece una teoría ingenua de conjuntos como base para su exposición del cálculo proposicional (Capítulo 1), el cálculo de predicados (Capítulo 2), la aritmética de Peano (Capítulo 3) y sólo en el Capítulo 4 presenta la teoría axiomática de NBG. El quinto y último capítulo está dedicado a la computabilidad, y el libro termina con un apéndice con una variante de la prueba de Gentzen de la consistencia de la aritmética (en la que el finitismo de la argumentación queda desdibujado).

Dirk van Dalen (que se había doctorado el año anterior bajo la dirección de Heyting) señalaría este hecho en una recensión del libro:

> *Al tratar estos temas, el autor no impone restricciones sobre las metamatemáticas que se pueden utilizar; es decir, se emplean métodos de teoría de conjuntos siempre que sea conveniente, según la opinión del autor de que a los principiantes se les debe proporcionar las demostraciones más naturales y sencillas; una visión razonable si no fuera porque la cuestión de qué nociones son naturales y sencillas puede dar lugar a desacuerdos.*

Van Dalen se refiere a un pasaje del prólogo de libro, en el que Mendelson dice:

> *Con la convicción de que a los principiantes hay que presentarles las demostraciones más naturales y sencillas, se han utilizado libremente los métodos de la teoría de conjuntos. La importancia de la demanda de demostraciones constructivas sólo puede evaluarse tras cierta experiencia con la lógica matemática. Al fin y al cabo, si vamos a ser expulsados del "paraíso de Cantor" (como Hilbert denominó a la teoría de conjuntos no constructiva), al menos deberíamos saber qué nos estamos perdiendo.*

El resultado es que —deliberadamente— Mendelson no hace distinción alguna entre la metamatemática basada en la capacidad de razonar intuitivamente bajo ciertas restricciones y la metamatemática fundada en su formalización en una teoría de conjuntos. Por ejemplo, en un momento dado dice:

> *La palabra "prueba" se usa en dos sentidos distintos. Primero, tiene un significado preciso, definido anteriormente, como cierto tipo de secuencia finita de fórmulas de L. Sin embargo, en otro sentido, también designa ciertas secuencias de oraciones del idioma inglés (complementadas con diversos términos técnicos) que se supone sirven como argumento para justificar alguna afirmación sobre el lenguaje L (u otras teorías formales). En general, el lenguaje que estudiamos (en este caso L) se denomina lenguaje objeto, mientras que el lenguaje en el que formulamos y demostramos resultados sobre el lenguaje objeto se denomina metalenguaje. El metalenguaje también podría formalizarse y convertirse en objeto de estudio, lo cual llevaríamos a cabo en un metametalenguaje, etc. Sin embargo, utilizaremos el idioma inglés como nuestro metalenguaje (no formalizado), aunque, en gran parte de este libro, empleamos sólo una parte matemáticamente débil del idioma inglés.* [...] *La distinción entre "prueba" y "metaprueba" (es decir, una prueba en el metalenguaje) lleva a una distinción entre teoremas del lenguaje objeto y metateoremas del metalenguaje. Para evitar confusiones, generalmente usamos "proposición" en lugar de "metateorema". El término "metamatemática" se refiere al estudio de los lenguajes objeto lógicos y matemáticos; a veces, el término se limita a aquellas investigaciones que utilizan lo que al metamatemático le parecen métodos constructivos (o los llamados finitistas).*

La última frase parece sugerir que tal limitación le parece gratuita. Naturalmente, la mayor parte de su exposición es concebible en términos intuitivos, aunque no duda en insertar pasajes donde esto ya no es sostenible. Por ejemplo, al introducir la definición de Tarski de satisfacción de una fórmula dice:

> *Por ejemplo, si el dominio de la interpretación es el conjunto de números reales, la interpretación de A_1^2 es la relación $\leq$ y la interpretación de $f_1^1(x)$ es e^x, entonces una sucesión $s = (b_1, b_2, \ldots)$ de números reales satisface $A_1^2(f_1^1(x_2), x_5)$ si y sólo si $e^{b_2} \leq b_5$.* [...]

Así, o bien Mendelson considera que no hay inconveniente en hablar intuitivamente de los números reales y de la función exponencial sin aclaración alguna al respecto, o no tiene inconveniente en mezclar metamatemática intuitiva con metamatemática formalizada, o considera que no hace falta marear de momento a un principiante con estas sutilezas. Otro ejemplo en el que parece plantear como melindres ajenos las preocupaciones sobre fundamentos es esta nota:

> *Existe otra razón más para un enfoque axiomático formal. Los conceptos y proposiciones que implican la noción de interpretación e ideas relacionadas, como verdad, modelo, etc., a menudo se denominan semánticos para distinguirlos de los conceptos sintácticos, que se refieren a relaciones simples entre signos y expresiones de lenguajes formales precisos. Dado que las nociones semánticas son de carácter conjuntista, y dado que la teoría de conjuntos, debido a las paradojas, se considera una base bastante inestable para el estudio de la lógica matemática, muchos lógicos consideran que un enfoque sintáctico, consistente en un estudio de teorías axiomáticas formales utilizando únicamente métodos aritméticos bastante débiles, es mucho más seguro. Para más información, véase el estudio pionero sobre semántica de Tarski* [1936], *Kleene* [1952], *Church* [1956] *y Hilbert-Bernays* [1934].

Lo que parece leerse entre líneas de estos pasajes es que, para Mendelson, no hay ningún problema en tomar como base del razonamiento matemático una teoría ingenua de conjuntos, lo cual es razonable para un Bourbaki interesado en hacer matemáticas (pues puede decir con razón que todas las sutilezas sobre fundamentos se resuelven formalizando la teoría, aunque en la práctica no hace falta hacerlo) pero resulta chocante en un libro que presenta en su capítulo cuarto una teoría axiomática de conjuntos, con lo que no puede referirse a ella como un presupuesto implícito. Se diría que Mendelson compartía con muchos matemáticos la opinión de que las paradojas de la teoría de conjuntos no eran realmente un problema una vez se sabía cómo mantenerlas a raya, y que cualquier limitación en el razonamiento metamatemático "para mayor seguridad" era una incomodidad prescindible. Sin entrar a valorar la confusión que esto puede ocasionar a esos principiantes por los que dice preocuparse, lo indudable es que tal enfoque justificaba que cualquier lector receloso de los rumores de circularidad de la fundamentación de las matemáticas viera confirmados todos sus recelos.

En cuanto al Capítulo 4, contenía una introducción muy profunda y detallada de la teoría de conjuntos de NBG, que va mucho más allá que, por ejemplo, el libro de Suppes. Es perfectamente vigente hoy en día, como introducción, salvo a lo sumo por su envoltorio de jerga "peaniana" de la que uno puede librarse leyendo libros más modernos.

93 El axioma de determinación En 1962 Steinhaus había publicado con Jan Mycielski una nota breve titulada *Un axioma matemático que contradice al axioma de elección,* cuyo contenido desarrolló Mycielski en un artículo de **1964** titulado *Sobre el axioma de determinación,* que fue seguido poco después por *Sobre la medibilidad Lebesgue y el axioma de determinación,* publicado conjuntamente con Stanisław Świerczkowski, un amigo suyo que se había doctorado en 1960 bajo la dirección de Steinhaus.

Steinhaus y Mycielski habían propuesto un axioma que, con la notación que hemos empleado en la sección 78, afirma lo siguiente:

Axioma de determinación (AD) Para todo conjunto $A \subset \mathbb{N}^\omega$, el juego $J_{\mathbb{N}}(A)$ está determinado.

Recordemos que $\mathbb{N}^\omega$, el conjunto de las sucesiones de números naturales, no es sino el espacio de Baire $\mathcal{N}$. En esta sección escribiremos $J(A)$ en lugar de $J_{\mathbb{N}}(A)$. Es costumbre decir que un conjunto $A \subset \mathbb{N}^\omega$ está *determinado* si lo está el juego $J(A)$.

En estos términos, el axioma de determinación afirma que todos los subconjuntos de $\mathcal{N}$ están determinados. Gale y Stewart habían demostrado que existen conjuntos A no determinados, pero la prueba requiere el axioma de elección, así que AD no es compatible con el axioma de elección, pero aún cabía la posibilidad de que la teoría ZF + AD fuera consistente.

Mycielski se había propuesto estudiar las consecuencias de AD. En su primer artículo demostró, por ejemplo, que todo subconjunto de $\mathbb{R}$ no numerable contiene un subconjunto perfecto,[209] y en colaboración con Świerczkowski probó que todo subconjunto de $\mathbb{R}^n$ es medible Lebesgue.[210] Sobre todo esto Mycielski dice:

> *El incumplimiento del axioma de elección en esta nueva teoría es considerado por el autor como un "hecho lamentable". Éste cree que los modelos naturales de* ZF *son suficientemente reales como para demostrar la consistencia de* ZF. *La nueva teoría no muestra ninguna evidencia similar de consistencia. Sólo podemos esperar que algunos submodelos de los modelos naturales de* ZF *sean modelos de la nueva teoría.* En tal caso* AD *podría considerarse como una limitación en el concepto*

[209] Más en general, probó que todo espacio métrico separable no numerable contiene un subconjunto perfecto.

[210] Más aún, que si μ es una medida definida sobre los conjuntos de Borel de un espacio métrico separable X y $Y \subset X$ es un conjunto arbitrario, entonces existen conjuntos de Borel $B_1 \subset Y \subset B_2$ tales que $\mu(B_1) = \mu(B_2)$, lo cual permite extender μ a $\mathcal{P}X$.

de conjunto que excluye algunos conjuntos "patológicos" de ZF. *Desde este punto de vista,* AD *resulta muy fructífero.*

(*) En la literatura se han considerado muy pocas alternativas al axioma de elección. Algunas proposiciones de ese tipo han sido propuestas por Church y Specker. Tarski ha considerado la proposición "El conjunto de los números reales es una unión numerable de conjuntos numerables" (que por los resultados que veremos más abajo es incompatible con AD*). Pero ninguna de ellas parece tener consecuencias tan interesantes como* AD.

Observemos que, para construir la medida de Lebesgue hace falta usar el axioma de elección, al menos en una versión débil, pero Mycielski demuestra que AD implica una versión débil del axioma de elección que es suficiente para este fin:

Teorema (AD) Toda familia $\{X_n\}_{n\in\omega}$ de conjuntos no vacíos tales que $\bigcup_{n<\omega} X_n$ tenga cardinal $\leq \mathfrak{c}$ admite una función de elección.

Demostración: No perdemos generalidad si suponemos que $\bigcup_{n<\omega} X_n \subset \mathbb{N}^\omega$. Consideramos el juego $J_{\mathbb{N}}(A)$ determinado por el conjunto A formado por las partidas $(x_0, y_0, x_1, y_1, x_2, y_2, \ldots)$ tales que $(y_0, y_1, \ldots) \notin X_{x_0}$. Si suponemos AD, uno de los jugadores tiene que tener una estrategia ganadora, pero es imposible que la tenga el jugador I, ya que, si juega x_0, nada impide a II elegir un $y \in X_{x_0}$ e ir jugando sus componentes y ganar así la partida. Por lo tanto, tiene que ser II quien tenga una estrategia ganadora τ, la cual nos permite definir una función de elección: para cada $n \in \omega$, formamos la sucesión $x = (n, 0, 0, \ldots)$, calculamos $x*\tau = (x_0, y_0, x_1, y_1, \ldots)$ y extraemos $f(n) = (y_0, y_1, \ldots) \in A_n$. ∎

Esto es suficiente para construir la medida de Lebesgue. Ahora conviene observar que AD implica la determinación de los juegos con reglas:

Teorema (AD) Si $R \subset \mathbb{N}^{<\omega}$ es un árbol de reglas y $A \subset \mathbb{N}^\omega$, el juego $J(\mathbb{N}, R, A)$ está determinado.

Demostración: Recordemos que $J(\mathbb{N}, R, A)$ es el juego en el que se exige que cada situación $s \in \mathbb{N}^{<\omega}$ del juego en una partida cumpla $s \in R$, pero, por simplicidad, sólo consideramos reglas R en las que toda situación sea prolongable, de modo que no haya partidas que terminen tras un número finito de jugadas.

Para cada $s \in \mathbb{N}^{<\omega}$, llamamos $B_s = \{x \in \mathbb{N}^\omega \mid s \subset x\}$, es decir, al conjunto de todas las sucesiones que empiezan por s. Llamamos

$$[R] = \{x \in \mathbb{N}^\omega \mid \bigwedge n \in \omega\, x|_n \in R\}$$

al conjunto de todas las partidas legales. Si $x \in \mathbb{N}^\omega$ no es legal, eso significa que existe un (mínimo) n tal que $x|_n \notin R$. Como $\varnothing \in R$, no puede ser $n = 0$, luego será $n = k + 1$, con $x|_k \in R$. Esto significa que, si una sucesión x es ilegal, ello se debe a que era legal hasta un cierto punto $x|_k$ (tal vez con $k = 0$), pero que la jugada k-ísima ha sido ilegal y así $x|_{k+1} \notin R$. Por lo tanto

$$\mathbb{N}^\omega \setminus [R] = \bigcup_{s\in I} B_s,$$

donde I es el conjunto de todas las sucesiones $s \in \mathbb{N}^{<\omega}$ de longitud $k + 1$ tales que $s|_k \in R$, pero $s \notin R$. Ahora bien, podemos dividir las partidas ilegales en las que lo son por culpa del jugador I y las que lo son por culpa del jugador II: $X \setminus [R] = U_1 \cup U_2$, con

$$U_1 = \bigcup_{s\in I_1} B_s, \qquad U_2 = \bigcup_{s\in I_2} B_s,$$

donde I_1 está formado por los elementos de I de longitud impar e I_2 con los de longitud par.

Notemos que $\mathbb{N}^\omega = [R] \cup U_1 \cup U_2$ y los tres conjuntos son disjuntos dos a dos. Ahora basta tomar $A' = A \cup U_2$ y se cumple que, si $J(A')$ está determinado, lo mismo le sucede a $J(\mathbb{N}, R, A)$.

En efecto, supongamos que el jugador I tiene una estrategia ganadora para $J(A')$ y la aplica a $J(\mathbb{N}, R, A)$.

Su estrategia nunca lo llevará a una jugada ilegal respecto a R, porque si hiciera una jugada ilegal, independientemente de lo que hiciera a partir de ese momento el jugador II, la partida resultante x cumpliría $x \in U_1$, con lo que I perdería el juego $J(A')$. Por lo tanto, si el jugador II también respeta las reglas de este juego, la partida final estará en $[R]$, pero también en A', luego estará en A, y así I gana siempre al juego $J(\mathbb{N}, R, A)$.

Si es el jugador II el que tiene una estrategia ganadora en $J(A')$, se razona análogamente. Así pues, como AD implica que $J(A')$ está determinado, también lo está $J(\mathbb{N}, R, A)$. ∎

Como ilustración "del funcionamiento" de AD, vamos a demostrar que AD implica que todo subconjunto de $\mathbb{R}$ es medible Lebesgue. El argumento que dan Mycielski y Świerczkowski es algo más técnico que el que vamos a dar, porque nosotros nos apoyaremos en el hecho siguiente:

Si $f : C \longrightarrow [0,1]$ es una aplicación continua definida en un subconjunto cerrado C del espacio de Baire, entonces su imagen $f[C]$ es un conjunto analítico y, por consiguiente, medible Lebesgue.

Si en lugar de C hubiéramos puesto $\mathcal{N}$, tendríamos esencialmente la definición de conjunto analítico dada por Lusin (salvo que él usaba el espacio homeomorfo $\mathcal{I}$ de los números irracionales), por lo que la única "novedad" respecto de lo visto hasta aquí es que el resultado sigue siendo cierto si consideramos un cerrado arbitrario C. Esto se debe simplemente a que todo cerrado en $\mathcal{N}$ es imagen continua de $\mathcal{N}$, por lo que toda imagen continua de C lo es también de $\mathcal{N}$. Admitiendo esto, tenemos todo lo necesario para demostrar el teorema:

Teorema (AD) Todo subconjunto de $\mathbb{R}$ es medible Lebesgue.

Demostración: No perdemos generalidad[211] si consideramos subconjuntos del intervalo $I = [0,1]$. Llamamos N al conjunto de los números reales en I cuyo desarrollo binario es finalmente constante. Se trata de un conjunto numerable que podremos despreciar. Sea $\{B_n\}_{n=0}^{\infty}$ una enumeración de todos los intervalos abiertos $B_n =]a_n, b_n[$ tales que $a_n, b_n \in N$ se diferencian sólo en su última cifra binaria, como $]0.011000, 0.011001[$. Esto hace que dos cualesquiera de ellos estén uno contenido en el otro o sean disjuntos. Sea $\{s_n\}_{n\in\omega}$ una enumeración de $\omega^{<n}$.

Para cada $A \subset I$ y cada $\epsilon > 0$, definimos el juego $J'(A,\epsilon)$ con las reglas siguientes:

- Las jugadas de I deben ser $0, 1$.
- Si $y_n \in \mathbb{N}$ es la n-sima jugada de II, consideramos la sucesión $s_{y_n} = (k_0, \ldots, k_{l-1})$, y a su vez el abierto $U_n = \bigcup_{i<l} B_{k_i} \subset I$. Se tiene que cumplir que $m(U_n) < \epsilon/2^{2n+2}$.

Equivalentemente, podemos pensar que el jugador I va jugando las cifras binarias x_i de un número $x \in I$, mientras que II va jugando abiertos U_n que al final de la partida determinan un abierto $U = \bigcup_{n\in\omega} U_n$.

El jugador I gana la partida si $x \in A \setminus (N \cup U)$. Claramente es un juego de la forma $J(\mathbb{N}, R, A^*)$, luego AD implica que está determinado. Vamos a probar lo siguiente:

1. Si I tiene una estrategia ganadora, entonces A contiene un conjunto medible Lebesgue de medida positiva.
2. Si II tiene una estrategia ganadora, entonces existe un abierto U en I tal que $A \setminus N \subset U$ y $m(U) < \epsilon$.

Supongamos que I tiene una estrategia ganadora σ. Sea $C \subset \mathcal{N}$ el conjunto de todas las sucesiones $y \in \mathbb{N}^\omega$ tales que las jugadas y_n son legales para II, es decir, que los abiertos U_n correspondientes tienen medida suficientemente pequeña para cumplir las reglas del juego.

Ahora observamos que C es cerrado en $\mathcal{N}$, pues si $y \in \mathcal{N} \setminus C$, es que alguna jugada y_i es ilegal, luego todas las sucesiones que coincidan con y hasta y_i, estarán igualmente en $\mathcal{N} \setminus C$, luego éste es abierto.

Por otro lado, para cada $y \in C$, podemos calcular la partida $\sigma * y$ que resulta cuando I aplica su estrategia y II juega y, de la cual podemos extraer la sucesión x de jugadas de 1, que son las cifras binarias de un número real $f(y)$ que tiene que estar en $A \setminus (N \cup U)$, porque, con su estrategia, I gana todas las partidas.

Tenemos así una aplicación $f : C \longrightarrow A \setminus (N \cup U)$, y vamos a ver que se trata de una aplicación continua.

En efecto, para ver que es continua en un punto $y \in C$, tenemos que probar que, para todo $\eta > 0$, podemos conseguir que $|f(y) - f(y')| < \eta$ sin más que exigir que y' esté suficientemente cerca de y. Pero, para que dos números reales estén suficientemente próximos, basta con que sus cifras binarias sean iguales hasta un N suficientemente grande, y para que esto suceda basta con que las cifras binarias de y' coincidan con las de y hasta N, pues en tal caso, si II juega una partida jugando y o jugando y' y el jugador I aplica su estrategia σ, las N primeras jugadas de I serán las mismas, porque las de II también lo serán. Por lo tanto $f(y)$ y $f(y')$ tendrán las mismas N primeras cifras binarias. Pero que y, y' tengan las mismas N primeras cifras binarias es lo que significa precisamente que y' esté suficientemente próximo a y.

[211] Si $A \subset \mathbb{R}$ y llamamos $A_n = A \cap [n, n+1]$, se cumple que $A = \bigcup_{n\in\mathbb{Z}} A_n$, luego si todos los A_n son medibles Lebesgue, lo mismo le sucede a A, y el argumento que vamos a dar vale tomando como I cualquier intervalo $[n, n+1]$.

Por lo tanto, por el teorema que hemos comentado previamente, podemos concluir que $B_0 = f[C] \subset A$ es un conjunto medible Lebesgue. Como N es numerable, también lo será $B = B_0 \setminus N \subset A$. Tenemos que probar que tiene medida positiva. La idea es que si tuviera medida nula, entonces II podría burlar la estrategia de I.

En efecto, supongamos que $m(B) = 0$. Según vimos en la sección 19, esto implica que B tiene medida exterior 0, es decir, que puede cubrirse con una unión numerable de intervalos abiertos cuyas medidas sumen menos que cualquier valor prefijado. Concretamente, podemos tomar una unión numerable $G^* \subset \mathbb{R}$ de intervalos abiertos de modo que $B \subset G^*$ y $m(G^*) < \epsilon/2^2$.

Cada $x \in B$ es un número real cuya expresión binaria no es finalmente constante, luego podemos tomar un intervalo B_n suficientemente pequeño como para que $x \in B_n \subset G^*$. Aunque B no tiene por qué ser numerable, sólo hay una cantidad numerable de intervalos B_n que elegir, luego al final habremos elegido únicamente una familia numerable $\{B_{n_i}\}_{i<\omega}$ de intervalos B_n tales que

$$B \subset G = \bigcup_{i<\omega} B_{n_i} \subset G^*.$$

Como dos abiertos B_{n_i} son disjuntos o están contenidos uno en otro, eliminando abiertos redundantes podemos suponer que los B_{n_i} son disjuntos dos a dos. Además, como $G \subset G^*$, tenemos también que $m(G) < \epsilon/2^2$. Vamos a ver que los abiertos B_{n_i} permiten a II ganar la partida. Como son disjuntos dos a dos, se cumple que

$$m(G) = \sum_{i<\omega} m(B_{n_i}) < \epsilon/2^2.$$

Si tomamos un número finito de sumandos, cuantos más tomemos más nos acercaremos a $\epsilon/2^2$, luego podemos definir $U_0 = B_{n_0} \cup \cdots \cup B_{n_{k_0}}$, donde k_0 es suficientemente grande como para que $B_{n_0} \subset U_0$ y $m(G \setminus U_0) < \epsilon/2^4$. Además tenemos que $m(U_0) \le m(G) < \epsilon/2^2$.

Similarmente, definimos $U_1 = B_{n_{k_0+1}} \cup \cdots \cup B_{n_{k_1}}$ de modo que $m(G \setminus (U_0 \cup U_1)) < \epsilon/2^6$ y asegurando que $B_{n_1} \subset U_0 \cup U_1$. Además, como $U_1 \subset G \setminus U_0$, tenemos que $m(U_1) < \epsilon/2^4$.

Procediendo de este modo, vamos construyendo abiertos $U_n \subset G$, cada uno de los cuales es unión de un número finito de abiertos B_{n_i}, disjuntos dos a dos, con $m(U_n) < \epsilon/2^{2n+2}$ y $B_{n_r} \subset U_0 \cup \cdots \cup U_n$, luego resulta que $G = \bigcup_{n<\omega} U_n$.

Si $U_n = \bigcup_{i<l} B_{k_i}$, consideramos el número natural y_n que cumple $s_{y_n} = (k_0, \ldots, k_{l-1})$, de modo que, si II juega y_n en su n-simo turno, está jugando precisamente el abierto U_n, que es legal, y la partida termina con el abierto $U = G$. Pero si I juega con su estrategia σ, terminará con $x = f(y) \in B_0$. Si $x \in N$, entonces pierde la partida, y si $x \notin N$, entonces $x \in B_0 \setminus N = B \subset G = U$, con lo que también pierde la partida. Esta contradicción muestra que B tiene medida positiva.

Ahora supongamos que es II quien tiene una estrategia ganadora τ. Para cada sucesión finita $s = (x_0, \ldots, x_n)$ de ceros y unos, llamemos U_s al abierto que jugará II con su estrategia si I ha ido jugando $(x_0, \ldots, x_n)$. Como será una jugada legal, cumplirá que $m(U_s) \le \epsilon/2^{2n+2}$. Sea $U = \bigcup_{s\in 2^{<\omega}} U_s$.

Entonces U es abierto en I (por ser unión de abiertos), y $A \setminus N \subset U$, pues si $x \in A \setminus N$, el jugador I puede jugar x, con lo que II irá jugando los abiertos $U_{x|_n}$ hasta formar el abierto $U^* = \bigcup_{n<\omega} U_{x|_n} \subset U$ y ganará la partida, luego $x \in U^* \subset U$. Por otra parte

$$m(U) \le \sum_{n=0}^{\infty} m\Big(\bigcup_{s\in 2^{n+1}} U_s\Big) \le \sum_{n=0}^{\infty} \big(2^{n+1}\frac{\epsilon}{2^{2n+2}}\big) = \epsilon.$$

Con esto ya podemos concluir la prueba. Tomamos un conjunto $X \subset I$ arbitrario y vamos a ver que es medible Lebesgue. De acuerdo con la sección 19, está definida la medida exterior $m_e(X)$, que es el ínfimo de las sumas $S = \sum_{i=0}^{\infty} l(I_n)$, donde $X \subset \bigcup_{n=0}^{\infty} I_n$ y cada I_n es un intervalo abierto. Por definición de ínfimo, para cada número natural $n \ge 1$, podemos tomar[212] una unión numerable de abiertos $U_n = \bigcup_{n=0}^{\infty} I_n$ tal que $X \subset U_n$ y

$$m(U_n) \le \sum_{n=0}^{\infty} m(I_n) \le m_e(X) + 1/n.$$

[212] Aquí usamos el axioma de elección para elegir un abierto U_n de un conjunto de abiertos de I, pero el conjunto de todos los abiertos en I tiene la potencia del continuo, por lo que podemos aplicar el caso particular del axioma de elección que hemos demostrado a partir de AD.

Sea $G = \bigcap_{n=0}^{\infty} U_n$, que es un conjunto de Borel tal que $X \subset G$ y $m(G) \leq m(U_n) \leq m_e(X)+1/n$ para todo n, luego $m(G) \leq m_e(X)$. La inclusión $X \subset G$ hace que, de hecho, $m(G) = m_e(X)$. Sea $A = G \setminus X$. Este conjunto no puede tener subconjuntos medibles de medida positiva, pues si $Y \subset G \setminus X$ es medible, tenemos que $X \subset G \setminus Y$, luego $m(G) = m^*(X) \leq m(G \setminus Y) = m(G) - m(Y)$, luego $m(Y) = 0$.

Entonces, para todo $\epsilon > 0$, el jugador I no puede tener una estrategia ganadora en el juego $J'(A, \epsilon)$, luego es II quien la tiene, lo que se traduce en que existe un abierto U en I tal que $A \setminus N \subset U$ y $m(U) < \epsilon$. Esto implica que $m^*(A \setminus N) = 0$, por lo que $A \setminus N$ es medible Lebesgue y tiene medida nula. Como N es numerable, lo mismo vale para A, y entonces $X = G \setminus A$ también es medible Lebesgue. ∎

Como consecuencia:

Teorema (AD) $\mathbb{R}$ no puede ser bien ordenado.

Esto se debe a que un buen orden en $\mathbb{R}$ permite construir el ejemplo de Vitali de subconjunto de $\mathbb{R}$ no medible Lebesgue, mientras que AD implica que todo subconjunto de $\mathbb{R}$ es medible Lebesgue. Por lo tanto, el cardinal del continuo $\mathfrak{c}$ no es un álef. Pero podemos decir más:

Teorema (AD) Los cardinales $\aleph_1$ y $\mathfrak{c}$ no son comparables.

Demostración: Si fuera $\mathfrak{c} \leq \aleph_1$, tendríamos una aplicación inyectiva $f : \mathbb{R} \longrightarrow \omega_1$, con lo que $\mathbb{R}$ admitiría un buen orden. Por el contrario, si $\aleph_1 \leq \mathfrak{c}$, entonces $\mathbb{R}$ contendría un subconjunto X de cardinal ω_1. Pero AD implica que todo subconjunto de $\mathbb{R}$ no numerable contiene un subconjunto perfecto $P \subset X$, pero todo conjunto perfecto tiene cardinal $\mathfrak{c}$, y así existe una aplicación $\mathbb{R} \longrightarrow P$ biyecctiva y, componiéndola con una aplicación $X \longrightarrow \omega_1$ inyectiva, obtenemos una aplicación $\mathbb{R} \longrightarrow \omega_1$ inyectiva, con lo que $\mathfrak{c} \leq \aleph_1$, caso que ya hemos descartado. ∎

Una consecuencia sencilla es la siguiente:

Teorema (ZF) Existe un juego $J_{\omega_1}(A)$ no determinado.

Demostración: Si todos los juegos $J_{\omega_1}(A)$ estuvieran determinados, también lo estarían todos los juegos $J_\omega(A)$, es decir, se cumpliría AD. En efecto, si $A \subset \omega^\omega \subset \omega_1^\omega$, una estrategia ganadora para un jugador en $J_{\omega_1}(A)$ lo es también para $J_\omega(A)$, pues la estrategia nunca recomendará jugar fuera de ω, ya que eso supone perder la partida.

Fijemos una biyección $f : \omega \times \omega \longrightarrow \omega$ y consideremos ahora el conjunto $A \subset \omega_1^\omega$ formado por las sucesiones $(\alpha, y_0, x_1, y_1, x_2, y_2, \ldots)$ tales que $y_i \in \{0, 1\}$ y el conjunto $R_y = \{(m, n) \in \omega^2 \mid y(f(m, n)) = 1\}$ es un buen orden en ω de ordinal α.

Es inmediato que ninguna estrategia σ para I en el juego $J_{\omega_1}(A)$ puede ser ganadora, pues si $\sigma(\varnothing) = \alpha$, basta tomar un buen orden R en ω de ordinal α, tomar $y(n) = 1$ si y sólo si $f^{-1}(n) \in R$, y entonces II gana la partida $\sigma * y$.

Por lo tanto, tiene que ser II quien tenga una estrategia ganadora τ. Para cada $\alpha < \omega_1$, consideramos el elemento $y^\alpha \in \mathbb{N}^\omega$ que cumple $(\alpha, 0, 0, \ldots) * \tau = (\alpha, y_0^\alpha, 0, y\alpha_1, 0, y\alpha_2, \ldots)$. Como la partida la gana II, eso significa que R_{y^α} es un buen orden en ω de tipo α, lo que en particular nos da que si $\alpha \neq \beta$, entonces $y^\alpha \neq y^\beta$, por lo que tenemos una aplicación $\omega_1 \longrightarrow \mathbb{N}^\omega$ inyectiva. Esto implica a su vez que $\aleph_1 \leq \mathfrak{c}$, en contra del teorema anterior. ∎

94 La teoría de conjuntos de Morse En **1965** Morse publicó *Una teoría de conjuntos,* en la que exponía su versión de la teoría de conjuntos de Morse-Kelley. El prólogo estaba escrito por Trevor James McMinn, que en 1955 se había doctorado bajo la dirección de Morse. En él se lee:

> *El libro es el resultado de sucesivos refinamientos de las conferencias impartidas por el autor a lo largo de los años en la Universidad de California en Berkeley. En este proceso, el sistema ha evolucionado desde uno de escasa formalidad y separación tradicional de la lógica y la teoría de conjuntos hasta el actual de completa formalidad y lógica unificada y teoría de conjuntos. Los axiomas para la teoría de conjuntos han experimentado una metamorfosis, desde los que aparecen en el Apéndice de la Topología General de J. L. Kelley hasta los actuales, más primitivos. En los últimos años, el lenguaje formal ha sido utilizado activamente por el autor y sus estudiantes en cursos de teoría de conjuntos y análisis, y el sistema axiomático ha sido probado con la experiencia.*

Los lectores de diversos niveles de educación matemática pueden beneficiarse de esta iniciativa, elegantemente gestionada y audaz. Un académico que ya comprenda en gran medida los objetivos del autor aún puede descubrir mucha originalidad e ingenio en su forma de alcanzarlos. Un estudiante perplejo por preguntas fundamentales tiene buenas posibilidades de encontrar respuesta. Aquel que esté menos interesado en los fundamentos de la teoría de conjuntos que en su superestructura debería verse ampliamente recompensado, tras el esfuerzo invertido en aprender los preliminares necesarios, por el impulso dado a su comprensión del hermoso edificio subsiguiente.

Sin embargo, lo que vemos a la derecha es el contenido de una página elegida al azar. En cuanto uno pasa el prólogo, se encuentra con un texto que hace parecer al "peaniano" más abstruso un cuento para niños. Joseph Robert Shoenfield publicó una reseña del libro en la que se leía:

Por otro lado, no se explica la noción de conjunto ni se justifican los axiomas seleccionados. La identificación de clases y valores de verdad se esboza en media página; no se proporciona ninguna explicación adicional para ayudar al lector a comprender axiomas tan inusuales como $x \leftrightarrow 0 \in x$. No se discuten las propiedades sintácticas o semánticas generales del sistema. Estas deficiencias hacen que la lectura del volumen sea muy difícil, incluso para un experto en teoría de conjuntos.

2.48 THE THEOREM OF UNIONS.

$$(a \in \mathbf{U} \wedge b \in \mathbf{U} \leftrightarrow a \cup b \in \mathbf{U})$$

This follows from the Theorem of Heredity and:

Lemma. $(a \in \mathbf{U} \wedge b \in \mathbf{U} \to a \cup b \in \mathbf{U})$

Proof. Using 2.47.5 we see

$$\begin{aligned}(\forall x\ 2\mathrm{B}\ abx &= \forall x(x \in \mathrm{sb}\ \mathrm{sng}\ 0 \wedge 2\mathrm{B}\ abx)\\ &= \forall x(\mathrm{sb}\ \mathrm{sng}\ 0 \in \mathbf{U} \wedge x \in \mathrm{sb}\ \mathrm{sng}\ 0 \wedge\\ &\qquad 2\mathrm{B}\ abx \in \mathbf{U} \wedge 2\mathrm{B}\ abx) \in \mathbf{U}).\end{aligned}$$

But 2.47.1 and 2.47.2 tell us

$$(a \cup b = 2\mathrm{B}\ ab0 \cup 2\mathrm{B}\ ab\ \mathrm{sng}\ 0 \subset \forall x\ 2\mathrm{B}\ abx \in \mathbf{U}).$$

2.49 THEOREM. $\sim(\mathbf{U} \in \mathbf{U})$

Proof. From the Theorem of Heredity we have

$$(\mathbf{U} \in \mathbf{U} \to x \subset \mathbf{U} \in \mathbf{U} \to x \in \mathbf{U}).$$

Hence

$$(x \backsim\!\in \mathbf{U} \to \mathbf{U} \backsim\!\in \mathbf{U}).$$

Accordingly, because of 2.38,

$$(\alpha = \mathsf{E}x \sim(x \in x) \to \alpha \backsim\!\in \mathbf{U} \to \mathbf{U} \backsim\!\in \mathbf{U}),$$

and the desired conclusion is at hand.

Y ésta era la crítica cortés. Una más espontánea era la del canadiense Joachim Lambek, en la que decía entre otras cosas:

¡Ay del pobre estudiante de posgrado, a quien, entre otros, va dirigido este libro! Podría haber sido peor; el libro podría haberse impreso en código Morse. [...] *En cuanto al formalismo matemático, el autor cree que las fórmulas no se leen, sino que se descifran (véase la página 15).*[213][...] *Este lector sólo llegó hasta la página 42, donde $\{x\}$ se define como la intersección de todos los y tales que $y \to (x \in y)$. En otro lugar se nos dice que $y \leftrightarrow (0 \in y)$, donde 0 es el conjunto vacío. Parecería deducirse que $\{x\} = 0$, lo cual seguramente no es una consecuencia pretendida.* [...] *Sin duda, un lector dispuesto y perseverante puede aprender mucho de este libro, pero este recensor faltaría a su deber si lo recomendara como lectura general antes de dormir.*

Las consecuencias que los hados parecen propiciar tras este tipo de publicaciones no se hicieron esperar: ese año de **1965** murió Fraenkel a sus 74 años, y en 1966 murió Brouwer, a los 85, atropellado enfrente de su casa.

95 El desarrollo del forcing Mientras tanto, la concepción del *forcing* seguía evolucionando y se publicaban versiones que incluían paulatinamente simplificaciones y clarificaciones conceptuales. Veamos algunas de ellas:

Feferman En **1965** Feferman publicó *Algunas aplicaciones de las nociones de forcing y conjuntos genéricos,* donde generaliza el concepto de *forcing* para construir modelos de teorías sobre otros lenguajes distintos del lenguaje de la teoría de conjuntos, como la aritmética de Peano. No vamos a entrar en estas variantes y nos centramos en la última parte del artículo, dedicada al *forcing* "usual" para la teoría de conjuntos. Feferman sigue bastante de cerca el planteamiento de Cohen (de hecho, remite a él, sin dar muchos detalles de las partes más técnicas).

Cohen había usado el *forcing* para, partiendo de un modelo transitivo numerable M de ZFC, construir otro N que contuviera una familia $\{a_\delta\}_{\delta<\tau}$ de subconjuntos de ω, donde τ era un cardinal en M. Feferman, en cambio, se propone estudiar el resultado de añadir únicamente una cantidad finita o numerable de conjuntos, pensando en violar el axioma de elección en lugar de la hipótesis del continuo.

[213] En la página 15 se lee: *Aunque la mayoría de las fórmulas que utilizamos pueden descifrarse intuitivamente, sugerimos una lectura algo superficial y una referencia ocasional a esta sección.*

Una primera variante que propone es, en lugar de imitar la construcción de L que había usado Gödel en su monografía de 1940, usar la construcción que había esbozado en su artículo de 1939, que es la que hemos explicado aquí, de modo que no es necesario ir definiendo los elementos del modelo N uno a uno, sino que pueden introducirse "por estratos" de modo que si $M = L_\lambda$, entonces $N = \bigcup_{\alpha<\lambda} N_\alpha$, donde N_0 es, en principio, arbitrario (a falta de determinarlo en su momento), y cada

$$N_\alpha = \mathcal{D}\big(\bigcup_{\beta<\alpha} N_\beta\big)$$

está formado[214] por los subconjuntos definibles de $\bigcup_{\beta<\alpha} N_\beta$. Concretamente, Feferman pretende tomar como N_0 un conjunto $\{S_n \mid n < \delta\}$ de subconjuntos de ω, donde $\delta \le \omega$.

Aunque no da detalles, Feferman considera un *lenguaje del forcing,* que contendrá, entre otras, unas constantes $\mathbf{S}_n$ (equivalentes a las $\mathbf{a}_\delta$ que hemos considerado al discutir la construcción de Cohen) que, cuando definamos los conjuntos S_n, harán referencia a ellos, pero que de momento se manejan formalmente.

En lugar de introducir cuantificadores limitados, Feferman expresa la limitación asignando un rango $\alpha < \lambda$ a cada variable, de modo que su lenguaje tiene una cantidad numerable de variables de cada rango α. Así, una expresión de la forma[215] $\bigwedge X$ o $\bigvee X$, donde X es una variable de rango α, se interpretará como "para todo $x \in N_\alpha$" o "existe un $x \in N_\alpha$".

Al igual que Cohen, Feferman considera *condiciones* Q, que son conjuntos finitos de fórmulas de tipo $\mathbf{m} \in \mathbf{S}_n$ o $\mathbf{m} \notin \mathbf{S}_n$. Alguien que "viva en M", puede ver todas las condiciones y operar formalmente con ellas, aunque no vea los conjuntos S_n de los que pretenden hablar. Feferman remite a Cohen sin dar detalles sobre cómo se define la relación "$Q \Vdash \phi$".

Otra novedad importante es que Feferman da un significado preciso a un concepto que Cohen había usado sólo informalmente para referirse a los conjuntos a_δ que quería construir. En la introducción de su artículo se refería a ellos como "conjuntos genéricos":

> *Sólo aquellas propiedades que son verdaderas de manera "uniforme" para subconjuntos "genéricos" de ω en M serán verdaderas para los a_δ en N. Por ejemplo, cada a_δ contiene infinitos primos, no tiene densidad asintótica, etc.*

aunque luego, en el cuerpo del artículo, no vuelve a aparecer el término. Por el contrario, Feferman define una *sucesión genérica de condiciones* $\{Q_k\}_{k<\omega}$ como una sucesión que cumple dos condiciones:

1. $\bigcup_{k<\omega} Q_k$ es consistente, es decir, que no contiene ninguna fórmula $\mathbf{m} \in \mathbf{S}_n$ y su negación $\mathbf{m} \notin \mathbf{S}_n$.
2. Para toda fórmula ϕ del *lenguaje de forcing,* existe un k tal que $Q_k \Vdash \phi$ o $Q_k \Vdash \sim\phi$.

Cohen escogía de forma similar la sucesión de condiciones, pero imponía algunos requisitos técnicos adicionales que Feferman puede eliminar. Como ya hemos señalado, la clave para la existencia de sucesiones genéricas está en que el modelo M es numerable, por lo que también lo es el conjunto de las fórmulas del *lenguaje del forcing* y esto permite elegir una condición Q_k para dedicir cada fórmula.

A su vez, una sucesión de conjuntos $\{S_n\}_{n<\delta}$ es *genérica* si cada S_n viene dado por

$$S_n = \{m < \omega \mid \bigvee k < \omega\ Q_k \Vdash \mathbf{m} \in \mathbf{S}_n\}.$$

Cada sucesión genérica determina un conjunto transitivo numerable N, que, de hecho, se puede ver que es el menor modelo transitivo de ZF que contiene a M y a la sucesión genérica.

Sucede que, en general, no se puede asegurar que el modelo N vaya a cumplir el axioma de elección. Esto depende esencialmente de la elección del conjunto N_0 con el que empezamos a imitar la construcción de los conjuntos constructibles. La idea es que N cumplirá el axioma de elección si N_0 puede ser bien ordenado[216]

[214] Si imitamos la definición de L dada en la página 154 deberíamos tomar $N_{\alpha+1} = \mathcal{D}N_\alpha$ y sólo cuando η es un ordinal límite $N_\eta = \bigcup_{\delta<\eta} N_\delta$. La variante de Feferman es equivalente, pues sólo cambia la numeración de los niveles. Lo que sería $N_{\eta+1}$ pasa a llamarse N_η, mientras que lo que sería N_η no tiene nombre en esta forma de llevar a cabo la construcción.

[215] Feferman usa los signos $\sim, \wedge, \vee, \bigwedge, \bigvee$ en el "lenguaje del forcing", mientras que usa $\neg, \&,$ o $,\forall, \exists$ para el lenguaje usual de ZFC.

[216] En el modelo con el que Cohen violaba la hipótesis del continuo el axioma de elección se cumplía porque la base de su construcción (el equivalente a N_0) era el conjunto que contenía a los conjuntos $F(\alpha)$ con $\alpha \le \tau \cdot 3$, entre los cuales se encuentra $F(\tau \cdot 3) = W$, que es un buen orden que permite definir un buen orden sobre los a_δ, los pares $\{a_\delta, a_{\delta'}\}$ y $(a_\delta, a_{\delta'})$ e incluso sobre el propio W.

en N. Feferman toma $N_0 = \{S_n \mid n < \delta\}$. Si $\delta < \omega$, se trata de un conjunto finito, luego admite un buen orden, pero si $\delta = \omega$, Feferman no se asegura de incluir en N la biyección $n \mapsto S_n$ o cualquier otra que permita a "alguien que viva en N" reconocer que N_0 es numerable o, al menos, bien ordenable. Y de hecho sucederá que N_0 no admitirá un buen orden en N.

Feferman describe brevemente la prueba de Cohen de la independencia del axioma de elección (que por aquel entonces sólo circulaba en unas notas mimeografiadas) y presenta una variante con la que, entre otras cosas, considerando el caso $\delta = 1$ en que se añade un único conjunto genérico S_0, muestra que, en el modelo N correspondiente, se cumple el axioma de elección y, en particular, el conjunto $\mathcal{P}\omega$ (o, equivalentemente, el conjunto de los números reales), puede ser bien ordenado, pero no por una fórmula explícita $\alpha(x, y)$ del lenguaje de la teoría de conjuntos. Por lo tanto:

> En ZFC se puede demostrar que $\mathbb{R}$ admite un buen orden, pero no se puede definir ninguno. Se puede demostrar que existe un conjunto que es un buen orden en $\mathbb{R}$, pero no es posible definir ninguno en concreto.

En cambio, en un modelo en el que se cumple $V = L$ la fórmula $x \trianglelefteq y$ determina un buen orden, no ya en $\mathcal{P}\omega$ o en $\mathbb{R}$, sino en la clase de todos los conjuntos.

Por otro lado, para $\delta = \omega$ obtiene un modelo de ZF en el que no existen ultrafiltros no principales en ω. Por lo tanto:

> La existencia de ultrafiltros no principales en ω no se puede demostrar sin usar el axioma de elección.

Lévy Ese mismo año de **1965** Lévy publicó *Definibilidad en la teoría axiomática de conjuntos,* en el que presentaba su versión del *forcing* para añadir subconjuntos genéricos de ω a un modelo, donde incorporaba algunas de las ideas de Feferman y añadía otras nuevas. Una era que, hasta ese momento, las condiciones se definían como conjuntos finitos de fórmulas del *lenguaje del forcing,* mientras que es posible —y preferible— definirlas de forma independiente. Por ejemplo, a la hora de definir una sucesión $\{a_\delta\}_{\delta<\tau}$ de conjuntos genéricos, en lugar de considerar una condición como

$$P = \{\mathbf{100} \in \mathbf{a}_{16}, \quad \mathbf{0} \in \mathbf{a}_{\omega+4}, \quad \mathbf{19} \notin \mathbf{a}_{\omega^2}\}.$$

Lévy considera el conjunto

$$p = \{(16, 100, 1), (\omega + 4, 0, 1), (\omega^2, 19, 0)\}.$$

En general, Lévy define las *condiciones* como funciones definidas de un subconjunto finito de $\tau \times \omega$ en el conjunto $2 = \{0, 1\}$. Las condiciones definidas de este modo contienen la misma información que las de Cohen. Por ejemplo, $p(16, 100) = 1$ se interpreta como que $100 \in a_{16}$, mientras que $p(\omega^2, 19) = 0$ se interpreta como que $19 \notin a_{\omega^2}$.

Así, si $p_0 \subset p_1 \subset p_2 \subset \cdots$ es una sucesión genérica de condiciones, la unión de todas ellas es una función $P : \tau \times \omega \longrightarrow 2$, pues, para cada par $(\alpha, n) \in \tau \times \omega$, tiene que haber una condición p_k que fuerce $\mathbf{n} \in \mathbf{a}_\alpha$ o bien $\mathbf{n} \notin \mathbf{a}_\alpha$, lo cual equivale a que p_k esté definida en (α, n) (ya sea con el valor $p_k(\alpha, n) = 1$ o $p_k(\alpha, n) = 0$), y entonces P está definida en todos los pares (α, n).

Recíprocamente, una función $P : \tau \times \omega \longrightarrow 2$ se dice *genérica* si es la unión de una sucesión genérica de condiciones. De este modo, cada sucesión genérica determina una función genérica y cada función genérica determina los conjuntos genéricos.

$$a_\delta = \{n \in \omega \mid P(\delta, n) = 1\}.$$

Esto es lo mismo que hacían Cohen o Feferman, pero expresado en términos conceptualmente más simples. De esta forma las condiciones pueden verse como aproximaciones parciales de un objeto que se desea incorporar al nuevo modelo, como piezas de un puzzle de las que hay que seleccionar juiciosamente una "sucesión genérica" adecuada para que éstas encajen y determinen el objeto deseado. En este caso, τ subconjuntos de ω son lo mismo que una función $P : \tau \times \omega \longrightarrow 2$, y las condiciones son piezas finitas que pueden combinarse para montar una función P que no sea cualquiera, sino que sea *genérica*, en el sentido de que con sus piezas se pueda forzar cualquier fórmula o su negación.

Como Feferman, Lévy basa su construcción de N en la construcción de L esbozada por Gödel en 1939, pero no exactamente igual que Feferman. Éste construye N mediante una jerarquía acumulativa que empieza con un N_0 indeterminado, que contendrá los conjuntos genéricos que interpreten las constantes $\mathbf{S}_n$, y luego va tomando partes definibles $N_\alpha = \mathcal{D}\big(\bigcup_{\beta<\alpha} N_\beta\big)$.

Lévy, en cambio, parte de $N_0 = \varnothing$, y toma $N_\alpha = \mathcal{D}_P\big(\bigcup_{\beta<\alpha} N_\beta\big)$, que contiene todos los subconjuntos de $X = \bigcup_{\beta<\alpha} N_\beta$ que se pueden definir mediante fórmulas que sólo hacen referencia a conjuntos de X salvo que también pueden "hacer una pequeña trampa" y tener en cuenta los valores de la función genérica P, aunque no esté en X. En otras palabras, mientras Cohen y Feferman imitaban la construcción de $L(A)$, Lévy imita la construcción de $L[A]$. En realidad este enfoque sigue la tesis de Easton, pero lo detallamos aquí porque Easton trabajaba con NBG en lugar de ZFC, y eso complica un tanto las cosas.[217] La diferencia es que, al imitar la construcción de $L[A]$ en lugar de la de $L(A)$, Lévy demostrará que el modelo N cumple siempre el axioma de elección (supuesto que lo cumpla M), mientras que en los modelos de Feferman (como en los de Cohen) N cumple el axioma de elección si y sólo si N_0 admite un buen orden en N, y por eso le falla a Feferman cuando toma $\delta = \omega$, porque, como ya hemos señalado, al tomar $N_0 = \{S_n \mid n \in \omega\}$, no está introduciendo ningún conjunto que ordene a los S_n (o que los biyecte con ω) y al final N_0 no admite un buen orden en N.

Otra diferencia notable es que esta construcción no requiere que el modelo M satisfaga el axioma de constructibilidad, sino que, en lugar de usar que $M = L_\lambda$, para cierto ordinal λ, estratifica los elementos de M mediante la jerarquía de von Neumann. Esto es importante porque así es posible encadenar aplicaciones del *forcing:* de un modelo M podemos pasar a otro M_1 (que normalmente no cumplirá $V = L$) y de éste podemos pasar a su vez a otro M_2, y así tantas veces como sea oportuno.

Solovay Más en general, Solovay había constatado que es posible aplicar la técnica del *forcing* tomando cualquier conjunto parcialmente ordenado como conjunto de condiciones de partida. En su construcción de un modelo en el que todo subconjunto de $\mathbb{R}$ es medible Lebesgue, Solovay había combinado varios conjuntos de condiciones para construir varias extensiones sucesivas de modelos. Uno era el que había usado Lévy para convertir en $\aleph_1$ a un cardinal inaccesible, que era una variante de los conjuntos de condiciones de Cohen, pero otro era especialmente novedoso.

La idea básica era que Solovay quería partir de un modelo transitivo numerable M para construir otro modelo N en el que hubiera un número real "aleatorio" $x \in [0,1]$. Esto significa que, "alguien que viva en M" no podrá ver el número x, pero podrá manejarlo como una variable aleatoria. Si llamamos $\mathcal{B}$ al álgebra de los subconjuntos de Borel del intervalo $[0,1]$ (o, mejor dicho, lo que toma como tal alguien que "viva en M"), para cada $B \in \mathcal{B}$, la medida $m(B)$ expresa la probabilidad de que el número x esté[218] en B. Por ejemplo, la probabilidad de que $x \in [0,1/2]$ es $1/2$. ¿Probabilidad en qué sentido? Podemos pensar que elegir una sucesión genérica es como tirar una moneda al aire. Si sale cara, $x \in [0,1/2]$ y si sale cruz, $x \in]1/2,1]$. Cada conjunto de Borel expresa la probabilidad de que, al elegir una sucesión genérica al azar, el número aleatorio determinado por ella cumpla $x \in B$.

Pero esto era sólo una idea vaga. Para precisarla, tomamos como conjunto de condiciones el conjunto P formado por los conjuntos de Borel $B \in \mathcal{B}$ de medida no nula. De este modo, cada condición B nos da

[217] Concretamente, si $\lambda = M \cap \Omega$ es el conjunto de los ordinales de M, Lévy define un *lenguaje del forcing* que consta de los signos $\neg, \vee, \exists, \in$, además de variables v_n (para $n < \omega$), constantes $\mathbf{s}$ para cada $s \in M$ (cada una de las cuales tiene asociado un rango $\alpha < \lambda$, que no es sino el rango de s en la jerarquía de von Neumann), un relator diádico A, de modo que $A(x,y)$ se interpreta como $P(x,y) = 0$, los particularizadores limitados $\bigvee_\alpha$, para $\alpha < \lambda$ (en lugar considerar variables de rangos distintos, Lévy considera un único juego de variables, pero, como Cohen, usa un cuantificador distinto para cada rango para limitar las cuantificaciones), y unos signos $\aleph_\alpha$, para $\alpha < \lambda$, de modo que, si ϕ es una fórmula con x como única variable libre (en la que sólo aparezcan términos y cuantificadores de rango menor que α), el término $\hat{x}_\alpha\phi \equiv \aleph_\alpha x\phi$ (de rango α) pretende nombrar al conjunto de los x en N_α que cumplen $N_\alpha \vDash \phi$ (donde ϕ puede contener el relator A y así hacer referencia a P).

Ahora, fijada una función $P : \tau \times \omega \longrightarrow 2$ que interprete a A, podemos definir recurrentemente una aplicación val_P que asigne un conjunto a cada término t, de modo que, si llamamos N_α al conjunto de los valores de los términos de rango α, entonces $N_\alpha = \mathcal{D}_P(\bigcup_{\beta<\alpha} N_\beta)$ es el conjunto de todos los subconjuntos de $\bigcup_{\beta<\alpha} N_\beta$ definibles mediante fórmulas $\phi(x, t_1, \ldots, t_n)$ en las que sólo aparecen cuantificadores y términos de rango $< \alpha$, es decir, el conjunto de todos los conjuntos de la forma $\{x \in \bigcup_{\beta<\alpha} N_\beta \mid \bigcup_{\beta<\alpha} N_\beta \vDash \phi[x, \mathrm{val}_P(t_1), \ldots, \mathrm{val}_P(t_n)]\}$, donde en $\vDash$ se interpreta el relator A mediante la función P. Finalmente, $N = \bigcup_{\alpha<\lambda} N_\alpha$ es el conjunto de los valores de todos los términos.

[218] Literalmente, esto no tiene sentido, porque $B \subset M$, luego, si $x \notin M$, es imposible que x esté en B. Ahora, bien, cada conjunto de Borel de M se puede extender a un "análogo" en N de la misma medida. Por ejemplo, el "análogo" en N de un intervalo $]a,b[^M =]a,b[\cap M$ de M es el intervalo $]a,b[^N =]a,b[\cap N$. El segundo tendrá más elementos que el primero, pero, en cierto sentido, ambos son "el mismo conjunto de Borel" y, desde luego, ambos tienen medida $b-a$. Similarmente, si un conjunto de M es unión numerable de intervalos, su "análogo" en N es la unión de los intervalos análogos y, en general, a cada $B \in \mathcal{B}^M$ del álgebra de Borel en M, se le puede asociar un conjunto "análogo" $B^N \in \mathcal{B}^N$, de modo que la idea de Solovay era que $m(B)$ expresara la probabilidad de que el número aleatorio x cumpla $x \in B^N$.

información parcial sobre dónde está el número aleatorio x. Nos dice que x estará en B con probabilidad $m(B)$. Por eso hemos descartado los conjuntos de medida nula, porque es seguro que x no estará en ninguno de ellos, luego no nos sirven como localizadores de x.

Ahora observamos que tenemos que definir que una condición B *extiende* a otra C (en el sentido de que nos aporta más información sobre dónde está x) si $B \subset C$. Al contrario de lo que sucede con las condiciones de Cohen, que cuanto mayores son más información aportan, aquí es al revés: cuanto menor es un conjunto de Borel, mejor está ubicando a x.

De hecho, debemos hacer un matiz, y es que, en realidad, debemos considerar que B extiende a C si $B \setminus C$ es nulo, pues $B = (B \cap C) \cup (B \setminus C)$ y si $B \setminus C$ es nulo, B aporta exactamente la misma información que $B \cap C$ (porque sabemos que x no va a estar en $B \setminus C$ y, como $B \cap C \subset C$, resulta que B aporta más información que C.

Pero esto no es un orden parcial. Si $(B \setminus C) \cup (C \setminus B)$ es nulo, se cumple que B extiende a C y C extiende a B sin que B y C sean necesariamente iguales.

Esto se arregla considerando el álgebra cociente $\mathcal{B}_m = \mathcal{B}/I_m$, donde I_m es el ideal formado por los conjuntos de Borel de medida nula. Cada elemento de $\mathcal{B}_m$ es una clase de equivalencia $[B]$, donde $[B] = [C]$ precisamente si $(B \setminus C) \cup (C \setminus B)$ es nulo, lo que se traduce en que B y C aportan exactamente la misma información sobre el número aleatorio x. Nos dicen que x está en $B \cap C$ con probabilidad $m(B) = m(B \cap C) = m(C)$.

La clase $0 \in \mathcal{B}_m$ está formada por los conjuntos de Borel de medida nula, que son justo los que no nos sirven, luego el conjunto de condiciones que necesitamos es en realidad $\mathbb{P} = \mathcal{B}_m \setminus \{0\}$. Una condición $[B]$ extiende a otra $[C]$ si $[B] \leq [C]$ en el sentido del álgebra de Boole, que equivale precisamente a que $B \setminus C$ sea nulo.

La condición $1 \in \mathcal{B}_m$ es la clase de todos los conjuntos de Borel de medida 1, que no aporta ninguna información sobre la situación de x, pues es seguro que x estará en todos ellos. Ahora, si

$$[B_0] \geq [B_1] \geq [B_2] \geq \cdots$$

es una sucesión genérica, sucede que los conjuntos de Borel

$$B_0^N \supset B_1^N \supset B_2^N \supset \cdots$$

determinan un único número real x tal que $\bigcap\limits_{n<\omega} B_n^N = \{x\}$.

Con esto ya podemos concretar la idea vaga inicial: Solovay llamó *reales aleatorios* a los reales "genéricos" obtenidos de este modo, porque tienen la propiedad de que pertenecen a (las extensiones de) todos los conjuntos de Borel de M de medida 1, y no pertenecen a ninguno de medida 0. (Por ejemplo, x pertenece a $\{x\}$, que es un conjunto de Borel de medida 0, pero no es la extensión de ningún conjunto de Borel de M.)

Así, al igual que en el modelo de Cohen podemos pensar en las condiciones como determinaciones parciales de los conjuntos genéricos a_δ, de modo que una condición es verdadera si las afirmaciones que contiene de tipo $\mathbf{m} \in \mathbf{a}_\delta$ o $\mathbf{m} \notin \mathbf{a}_\delta$ son todas verdaderas, también podemos considerar que los conjuntos de Borel B de M son determinaciones (ubicaciones) parciales del real aleatorio x, de modo que un conjunto de Borel B de M es "verdadero" o "falso" según si $x \in B^N$ o $x \notin B^N$, y $m(B)$ es la probabilidad de que $x \in B^N$, que en general depende de la elección de la sucesión genérica.

Por otra parte, el álgebra $\mathcal{B}_m$ tiene una propiedad sorprendente: es completa, en el sentido de que todo subconjunto $X \subset \mathcal{B}_m$ tiene supremo $\bigvee X$ e ínfimo $\bigwedge X$. En general, si $X \subset \mathcal{B}$, no es cierto que X tenga que tener supremo o ínfimo. En principio, el supremo debería ser $\bigcup X$, pero una unión arbitraria de conjuntos de Borel no tiene por qué ser de Borel. Ni siquiera tendría por qué ser medible Lebesgue, y si no lo es, no hay ningún conjunto de Borel Y por encima de $\bigcup X$ que sea el menor que contiene a todos los conjuntos de X (pues siempre habría un punto $p \in Y \setminus \bigcup X$, con lo que $Y \setminus \{p\}$ sería un conjunto menor que seguiría conteniendo a todos los elementos de X. En cambio, al tomar el cociente, estos problemas desaparecen.[219]

[219]La idea es esta: dado $X \subset \mathcal{B}_m$, el conjunto $Y = \{p \in \mathcal{B} \setminus \{0\} \mid \bigvee q \in X\, p \leq q\}$ debería tener el mismo supremo. El lema de Zorn nos permite tomar una anticadena maximal $A \subset Y$, es decir, una familia de elementos de Y incompatibles dos a dos (cumplen $p \wedge q = 0$) y tal que no se puede extender a una anticadena mayor. Pero sucede que una familia de conjuntos de Borel con intersecciones nulas dos a dos tiene que ser a lo sumo numerable (si fuera no numerable, existiría un n tal que una cantidad no numerable de elementos de A cumplirían $m(a) > 1/n$, pero, tomando la unión de n de ellos, obtendríamos un elemento con medida > 1, lo cual es absurdo). Por lo tanto, A es numerable, y eso garantiza que existe $\bigvee A$ (se toma un conjunto de Borel en cada elemento de A y se forma la unión de todos ellos, que es un conjunto de Borel y su clase es el supremo de A). Por último se demuestra que $\bigvee A$ es también el supremo de X.

Solovay observó que esto simplificaba enormemente el trabajo con $\mathcal{B}_m$. Por ejemplo, a cada fórmula ϕ del *lenguaje del forcing* se le puede asociar el supremo

$$[\![\phi]\!] = \bigvee\{p \in \mathcal{B}_m \mid p \Vdash \phi\},$$

y entonces sucede que $p \Vdash \phi$ es equivalente a $p \leq [\![\phi]\!]$. Pero resulta que es mucho más fácil definir directamente la aplicación $\phi \mapsto [\![\phi]\!]$ y definir $\Vdash$ a partir de ella que no definir $\Vdash$ directamente. Por ejemplo, se puede definir $[\![\neg\phi]\!] = [\![\phi]\!]'$, $[\![\phi \vee \psi]\!] = [\![\phi]\!] \vee [\![\psi]\!]$, etc.).

Solovay había planteado a Scott una idea según la cual toda construcción de un modelo por *forcing* podría simplificarse usando un álgebra de Boole completa, y entre ambos habían elaborado un manuscrito titulado *Modelos booleanos de la teoría de conjuntos,* del que estaban circulando copias y actualizaciones.

Al mismo tiempo, Solovay y Tennenbaum habían completado su construcción de un modelo de ZFC en el que no hay árboles de Suslin, para lo cual habían desarrollado la técnica conocida como *"forcing iterado"*, que permite reducir una sucesión transfinita de extensiones de un modelo mediante *forcing* a una única extensión del modelo de partida.

Cohen En **1966** Cohen publicó su libro *La teoría de conjuntos y la hipótesis del continuo,* en cuyo capítulo IV presenta su demostración de la independencia del axioma de elección (inédita hasta entonces) y de la hipótesis del continuo, pero en los tres capítulos previos incluye los preliminares necesarios sobre lógica (capítulo I) y teoría de conjuntos (capítulo II), así como la prueba de Gödel de la consistencia del axioma de elección y de la hipótesis del continuo generalizada (capítulo III). A modo de introducción dice:

> *Ahora se sabe que la verdad o falsedad de la hipótesis del continuo y otras conjeturas relacionadas no puede determinarse mediante la teoría de conjuntos tal como la conocemos hoy. Esta situación, con respecto a un problema clásico y presumiblemente bien planteado, sin duda debe parecer bastante insatisfactoria para el matemático típico. Uno se siente tentado a examinar con mayor detenimiento, y quizás con mayor espíritu crítico, los fundamentos de las matemáticas. Aunque nuestra matemática "cantoriana" actual es muy exitosa en el tratamiento de las abstracciones, no debe pasarse por alto que, desde el principio, el uso de procesos infinitos fue visto con recelo por muchos. En el siglo XIX, las objeciones al uso de series convergentes y números reales fueron respondidas por Cauchy, Dedekind, Cantor y otros, a las que siguieron críticas más profundas por parte de matemáticos posteriores como Brouwer, Poincaré y Weyl. La controversia subsiguiente dio lugar a la formación de diversas escuelas de pensamiento sobre sus fundamentos. Cabe afirmar que ninguna postura ha sido completamente exitosa en la respuesta a las preguntas fundamentales, sino que las dificultades parecen ser inherentes a la naturaleza misma de las matemáticas. A pesar de que la hipótesis del continuo es un ejemplo muy claro de lo que podría llamarse una afirmación absolutamente indecidible (en nuestro esquema actual), el teorema de incompletitud de Gödel sigue representando el mayor obstáculo a una filosofía satisfactoria de las matemáticas. Estas dificultades fundamentales, que los matemáticos pasan por alto a menudo, hacen que la independencia de la hipótesis del continuo sea menos sorprendente.*

En el capítulo I, sobre lógica, define lo que es un lenguaje formal, y el cálculo deductivo, demuestra el teorema de completitud, introduce las funciones recursivas y demuestra los teoremas de incompletitud. Cohen admite lenguajes con una cantidad no numerable de signos (constantes, relatores, etc.) y observa, por ejemplo, que su demostración del teorema de completitud usa el axioma de elección, y demuestra que si una teoría tiene un modelo, tiene modelos de cardinal arbitrariamente grande, con lo que hay que entender que está razonando en el seno de una teoría de conjuntos, aunque sólo en el capítulo II introduce la teoría de conjuntos ZF, y dedica una sección a presentar también NBG.

La sección 7 de este segundo capítulo se titula *Axiomas superiores y modelos de la teoría de conjuntos,* donde plantea axiomas con los que se puede extender ZF, como el axioma M, que afirma la existencia de un modelo de ZF, o el axioma SM, que afirma la existencia de un "modelo estándar" (lo que hemos llamado un modelo natural, un modelo en el que la relación de pertenencia se interpreta como ella misma). Sobre ellos dice:

> *Estos axiomas son ejemplos de cómo podemos extender los axiomas de* ZF *añadiendo sentencias intuitivamente verdaderas.*

lo que supone una concepción muy generosa de lo que es "intuitivamente verdadero". Luego plantea también el axioma que postula la existencia de un cardinal fuertemente inaccesible, y luego el axioma que postula la existencia de un cardinal medible. Por último considera la posibilidad de extender NBG admitiendo que fórmulas arbitrarias definan clases, es decir, la teoría de Morse-Kelley, aunque no la llama por este nombre. En la última sección del capítulo II demuestra el teorema de reflexión, concluye que ZF no es finitamente axiomatizable y demuestra el teorema del colapso de Mostowski. En el capítulo III construye la clase de los conjuntos constructibles, pero trabajando en ZF y no en NBG, y usando la construcción esbozada por Gödel en 1939 y no la que expuso en su monografía de 1940, que era la más conocida.

> *Si la hipótesis del continuo es verdadera, entonces los números reales pueden ponerse en correspondencia biunívoca con $\aleph_1$, el conjunto de todos los ordinales numerables. Si pensamos en un ordinal como la representación de un "proceso", tendremos un método para asignar a cada "proceso" numerable un número real único. Por lo tanto, no es irrazonable imaginar un proceso transfinito de construcción de números reales, o incluso conjuntos en general, que sea lo suficientemente general como para incluir posiblemente todos los conjuntos. Ahora bien, se han presentado varios puntos de vista filosóficos que sólo aceptarían aquellos objetos matemáticos que han sido efectivamente construidos. El más estricto de estos sólo aceptaría conjuntos finitos y, por lo tanto, claramente no tiene relevancia para la teoría de conjuntos. La noción correcta, para este propósito, es la de definiciones predicativas. Adoptemos el punto de vista de que un conjunto no es un objeto dado* a priori, *sino que debe definirse por una propiedad. Dado que* ZF *permite argumentos tan poco constructivos, seremos liberales y permitiremos cualquier propiedad razonable $P(x)$, incluso si no puede verificarse empíricamente en modo alguno para un x dado. Sin embargo, parece razonable exigir que, sea cual sea $P(x)$, sólo se refiera a objetos previamente admitidos. Por ejemplo, supongamos que aceptamos los números naturales como dados, así como las operaciones aritméticas. Entonces podríamos considerar un conjunto de números naturales definido por la propiedad $P(n)$, cuyas variables ligadas abarcan únicamente los números naturales. Se dice que dicho conjunto de números naturales está definido* predicativamente *en términos de los números naturales. Consideremos, sin embargo, la propiedad siguiente. Un número natural n satisface $P(n)$ si existe una partición del conjunto ω de números naturales en n conjuntos disjuntos, ninguno de los cuales contiene progresiones aritméticas de longitud arbitraria. Sea $S = \{n \mid P(n)\}$. Para determinar si, por ejemplo, $5 \in S$, debemos considerar todas las particiones de ω en 5 conjuntos, incluyendo posiblemente particiones en las que aparece el propio conjunto S. Por lo tanto, para definir el conjunto S, debemos aceptar que tiene sentido como totalidad el conjunto de todos los conjuntos de números naturales. Éste es un ejemplo de una definición impredicativa. Desde el punto de vista de* ZF, *esta definición es perfectamente aceptable. Sin embargo, desde un punto de vista más constructivo, la definición deja mucho que desear. Lo importante aquí no es que la definición no pueda llevarse a cabo eficazmente, sino que ni siquiera el dominio del discurso no se ha especificado suficientemente. Ciertamente, este es el tipo de situación (aunque presumiblemente aquí en forma inocua) que se da en las paradojas. Por lo tanto, se intentó desarrollar la teoría de conjuntos sobre una base predicativa. En los* Principia Mathematica, *Russell y Whitehead desarrollaron la "teoría de tipos" que evitaba ciertos aspectos de la impredicatividad. También H. Weyl, en su libro "El Continuo", mostró cómo se podía desarrollar la mayor parte, pero no todo, del análisis clásico a lo largo de líneas predicativas. Por supuesto, el carácter impredicativo del axioma de reemplazo es una característica esencial de* ZF, *y ningún desarrollo estrictamente predicativo puede ser verdaderamente relevante para ella. Sin embargo, buscamos una correspondencia entre ordinales y conjuntos, y la idea de Gödel fue que si iteramos construcciones predicativas hasta cualquier ordinal, los conjuntos resultantes podrían proporcionar un modelo adecuado de* ZF. *Filosóficamente, no habremos ganado nada, ya que no explicamos cómo se obtienen nuestros ordinales ni distinguimos entre ordinales "predicativos" e "impredicativos". Dado que aquí, en cambio, nos ocupa un problema de consistencia relativa, esta noción es extremadamente útil. A un conjunto que puede obtenerse como resultado de una secuencia transfinita de definiciones predicativas, Gödel, lo denominó "constructible". Su resultado, entonces, es que los conjuntos constructibles son un modelo de* ZF *y que, en este modelo, se cumplen el axioma de elección y la hipótesis del continuo generalizada.*
>
> *La noción de construcción predicativa debe precisarse, por supuesto, pero esencialmente sólo hay una manera de proceder. Otra forma de explicar la constructibilidad es señalar que los conjuntos constructibles son aquellos conjuntos que deben aparecer en cualquier modelo en el que se admitan todos los ordinales.*

Después de definir los conjuntos constructibles de forma parecida[220] a como hemos explicado en la sección 68 y de enunciar los resultados principales (que la clase L es un modelo de ZF, que en él se cumple $V = L$ y que $V = L$ implica el axioma de elección y la hipótesis del continuo generalizada), Cohen dice:

> *Antes de continuar, nos gustaría aclarar la relación entre la exposición de* [Gödel 1939] *y la de* [Gödel 1954].[221] *El enfoque de* [Gödel 1939] *que acabamos de describir es probablemente más fácil de entender que el de* [Gödel 1954]*. Por supuesto, ambos enfoques son idénticos en la práctica. Sin embargo, debido a la amplia influencia de* [Gödel 1954]*, más adelante también presentaremos dicho enfoque y demostraremos la equivalencia de ambos métodos.*

Cuando luego presenta NBG, lo califica de *sistema menos intuitivo* que ZF. Al inicio del capítulo IV, donde va a demostrar la independencia del axioma de elección y de la hipótesis del continuo, Cohen dice:

> *El método general que presentamos es aplicable a una amplia gama de cuestiones de independencia y, dado que el tema se está desarrollando rápidamente, sólo podremos ofrecer un resumen incompleto de los resultados conocidos.*

El resumen es bastante incompleto, pues apenas alude de pasada a una nota de Solovay y la tesis de Easton como ejemplos de determinaciones de la función del continuo que pueden conseguirse mediante *forcing* y, por otro lado, reproduce la prueba de Feferman de que $\mathbb{R}$ no puede ser bien ordenado por una fórmula en el modelo que construye. Por lo demás, Cohen incluye únicamente sus propios resultados, que estaban muy por detrás de los que estaban obteniendo Solovay, Tennenbaum, Lévy, Scott y otros.

Cohen hace un gran esfuerzo por explicar las motivaciones[222] que conducen al concepto de "*forcing*" que va a exponer, tanto previamente como durante la exposición. Ésta presenta algunas mejoras técnicas frente a la de su primer artículo. Para empezar, sigue el criterio de Feferman y define N mediante el procedimiento análogo a la construcción de L de Gödel de 1939 y no la de 1940. Cohen explica que si siguió el otro enfoque fue porque la única construcción de L que había sido publicada con detalle era la de 1940, pero ahora que él mismo había incluido con detalle la de 1939 en el capítulo III, era preferible adoptar este enfoque.

Pero es importante que la nueva construcción de N de Cohen es como la de Feferman y no como la de Lévy (o Easton): parte de un N_0 que sólo se determinará cuando se fije una sucesión genérica de condiciones, y luego toma $N_\alpha = \mathcal{D}(\bigcup_{\beta<\alpha} N_\beta)$. El modelo completo es $N = \bigcup_{\alpha<\lambda} N_\alpha$, donde λ es el conjunto de todos los ordinales del modelo de partida M.

En principio, Cohen se propone construir un modelo que incluya un único subconjunto "genérico" $a \subset \omega$ (aunque Cohen emplea muy pocas veces la palabra "genérico", y lo hace más bien cuando considera que está hablando "informalmente"). Para ello define la relación "P fuerza ϕ" (sin usar el signo $\Vdash$), primero para fórmulas limitadas y luego para fórmulas arbitrarias, con algunas simplificaciones que agradece a Scott. A continuación define las "sucesiones genéricas" de condiciones igual que Feferman, pero no las llama "genéricas" sino "completas".

Cuando termina la construcción, prueba que, en el modelo N de ZFC que obtiene, se cumple la hipótesis del continuo generalizada, pero el conjunto a no es constructible, con lo que ha demostrado que

> (Si ZFC es consistente) el axioma de constructibilidad no puede demostrarse ni siquiera suponiendo el axioma de elección y la hipótesis del continuo generalizada.

[220] Una diferencia es que, como Feferman y Lévy, Cohen define $M_0 = \varnothing, M_\alpha = \mathcal{D}(\bigcup_{\beta<\alpha} M_\beta)$, y esto hace que, por ejemplo, $M_\omega = L_{\omega+1}$, mientras que L_ω y, en general, los niveles L_λ de la jerarquía constructible (donde λ es un ordinal límite), no tienen nombre en la jerarquía que construye Cohen. Esto es en general más incómodo, pero así se ajusta mejor a lo que necesitará para el *forcing* en el capítulo siguiente.

[221] 1954 es la fecha de una segunda edición de la monografía de Gödel. La primera apareció en 1940.

[222] Cohen titula una sección *Motivación intuitiva.* Éste y otros usos que hemos señalado que hace de la palabra "intuitivo" ponen en evidencia que usa la palabra en un sentido habitual en los matemáticos, pero muy distinto al sentido que le daban Hilbert y los interesados en clarificar la fundamentación de las matemáticas y que hemos explicado en estas páginas. En efecto, para una gran parte de los matemáticos, "intuitivo" significa, "informal", "sin rigor", "idea vaga, pero sugerente", etc., nada que ver con el sentido de "dotado de pleno sentido intuitivo", que es todo lo contrario de una idea deficientemente precisada y sin rigor. No se puede decir que ese sentido de la palabra "intuitivo" sea contrario a la etimología y la tradición de uso de la palabra, pero lo que sí que es contraproducente es no ser consciente de que estamos ante dos significados radicalmente opuestos de una misma palabra y que confundirlos sólo puede dar lugar a malentendidos graves. Por ejemplo, algunos llaman *teoría intuitiva de conjuntos* a lo que aquí hemos llamado siempre *teoría ingenua de conjuntos.* No hay dada de intuitivo, en el sentido riguroso de la palabra, en la teoría de conjuntos abstractos no numerables.

Luego dedica una sección a explicar que todo lo que ha hecho se puede hacer más en general partiendo de un conjunto parcialmente ordenado U de condiciones, y plantea el caso de un conjunto de condiciones que adjunta a M una sucesión $\{a_\delta\}_{\delta<\omega}$ de subconjuntos de ω, donde τ es un cardinal infinito en M, pero, como en su artículo original, tiene que asegurarse de que en N_0 no sólo introduce los conjuntos $\{a_\delta\}_{\delta<\tau}$, sino también un buen orden W. Finalmente obtiene un modelo de ZFC con los mismos cardinales que M en el que $2^{\aleph_0}=\tau^+$ o $2^{\aleph_0}=\tau$ según si τ tiene cofinalidad numerable o no. (Notemos que el segundo caso no puede darse si τ tiene cofinalidad numerable, por el teorema de Kőnig.) No entramos en más detalles sobre esto porque ya lo hemos comentado al tratar de sus primeros artículos.

A continuación Cohen explica cómo construir modelos en los que falle el axioma de elección. Esta parte de sus resultados permanecía inédita hasta el momento. Vamos a explicar la idea comentando la demostración de este teorema:

> Si ZF es consistente, también lo es ZF más la existencia de un conjunto $C\subset\mathcal{P}\omega$ que es infinito, pero no tiene ningún subconjunto numerable.

Equivalentemente, esto significa que A es infinito (en el sentido de que no se puede biyectar con ningún número natural), pero no es infinito en el sentido de Dedekind (no es biyectable con un subconjunto propio, pues si lo fuera, contendría una copia de $\mathbb{N}$). Esto implica que $\mathcal{P}\omega$ no admite un buen orden, pues si lo tuviera, también A se podría ordenar bien, y se podría biyectar con un ordinal infinito, luego tendría un subconjunto numerable.

Demostración: Cohen construye el modelo N que resulta de adjuntar a M una cantidad numerable de conjuntos genéricos $C=\{a_n\mid n<\omega\}\subset\mathcal{P}\omega$. Recordemos cómo se hace esto. Consideramos condiciones P, que son conjuntos finitos de fórmulas del *lenguaje del forcing*[223] de la forma $\mathbf{m}\in\mathbf{a}_n$ o $\mathbf{m}\notin\mathbf{a}_n$, de modo que P no contenga a una fórmula y a su negación, donde $\mathbf{m}$ es un nombre para el número natural m y los $\mathbf{a}_n$ son términos del *lenguaje del forcing* que nombrarán a los conjuntos a_n que queremos construir. Se cumplen las dos propiedades básicas siguientes:

1. Si $P\subset P'$ son condiciones y $P\Vdash\phi$, entonces $P'\Vdash\phi$.
2. Si P es una condición y ϕ es una fórmula, entonces existe una condición P' que extiende a P tal que $P'\Vdash\phi$ o $P'\Vdash\neg\phi$.

Fijando una enumeración $\{\phi_n\}_{n<\omega}$ de todas las fórmulas del *lenguaje del forcing,* fijada cualquier condición P, podemos ir construyendo una cadena de condiciones

$$P\subset P_0\subset P_1\subset P_2\subset\cdots$$

de modo que $P_k\Vdash\phi_k$ o $P_k\Vdash\neg\phi_k$. La sucesión $\{P_k\}_{k<\omega}$ es un ejemplo de sucesión genérica (o completa, como la llama Cohen), es decir, que tiene la propiedad de que, dada cualquier fórmula ϕ, siempre hay una condición P_k tal que $P_k\Vdash\phi$ o $P_k\Vdash\neg\phi$. Fijada una sucesión genérica, podemos definir los conjuntos genéricos

$$a_n=\{m\in\omega\mid \bigvee k\in\omega\, P_k\Vdash\mathbf{m}\in\mathbf{a}_n\},$$

con los que a su vez podemos definir el modelo N, tomando $N_0=\omega\cup C$, pero sin añadir nada más que permita definir un buen orden sobre C. Así $C\in N$. Entonces:

3. Para cada fórmula ϕ, se cumple
$$N\vDash\phi \qquad \text{si y sólo si} \qquad \bigvee k\in\omega\, P_k\Vdash\phi.$$

Conviene destacar un par de hechos más:

4. Para cualquier condición P, se cumple:
$$P\Vdash\mathbf{m}\in\mathbf{a}_n \qquad \text{si y sólo si} \qquad (\mathbf{m}\in\mathbf{a}_n)\in P.$$
5. Hemos probado que si P es una condición, siempre existe una sucesión genérica tal que $P\subset P_0$, por lo que la condición P es verdadera en el modelo correspondiente N.

[223] Aunque Cohen no define el *lenguaje del forcing* exactamente igual que Lévy, para no discutir variantes no esenciales, podemos suponer que la definición es la misma que hemos explicado en la nota al pie de la página 264, salvo que no incluimos el relator A y añadimos las constantes $\mathbf{a}_n$ para nombrar los conjuntos genéricos. En particular tenemos una constante $\mathbf{s}$ para cada $s\in M$, lo que incluye a los números naturales.

Por ejemplo, vamos a usar estos hechos para demostrar que C es infinito, para lo cual basta ver que los conjuntos genéricos a_n son distintos dos a dos (y en tal caso será infinito en N, pues "alguien que viva en N" no puede ver una biyección entre C y un número natural porque no existe tal cosa, ni dentro, ni fuera de N).

Fijemos dos números naturales $n \neq n'$ y supongamos que $a_n = a_{n'}$. Entonces existe una condición P_k tal que $P_k \Vdash \mathbf{a}_n = \mathbf{a}_{n'}$ (por la propiedad 3). Sea r un número natural que no se mencione en ninguna de las fórmulas que contiene P_k. Entonces $P^* = P_k \cup \{\mathbf{r} \in \mathbf{a}_n, \mathbf{r} \notin \mathbf{a}_{n'}\}$ es una condición (porque las fórmulas que hemos añadido a P_k no pueden contradecir ninguna de sus fórmulas, pues no hablan de r).

Por 5) sabemos que existe una sucesión genérica cuyas condiciones extienden a P^* (luego a P_k, por lo que $P^* \Vdash \mathbf{a}_n = \mathbf{a}_{n'}$), luego en el modelo N^* que definen, se cumplirá que $a_n = a_{n'}$, pero también tenemos que $P^* \Vdash \mathbf{r} \in \mathbf{a}_n$ y $P^* \Vdash \mathbf{r} \notin \mathbf{a}_{n'}$, luego en N^* se cumple $r \in a_n$ y $r \notin a_{n'}$, y tenemos una contradicción.

Así pues, $C \in N$ es un conjunto infinito, en el sentido de que no se puede biyectar con ningún número natural.

Llamemos G al grupo de todas las aplicaciones $\pi : \omega \longrightarrow \omega$ biyectivas que dejan fijos a todos los números naturales salvo a lo sumo un número finito. Sea G_n el subgrupo formado por las biyecciones que fijan a los n primeros números naturales.

Cada conjunto $x \in N$ es el objeto denotado por un término t del *lenguaje del forcing,* de modo que t describe cómo construir x en función de cómo se interprete cada una de las constantes $\mathbf{a}_n$ que nombran a los conjuntos genéricos a_n. Para cada $\pi \in G$, podemos definir $\pi(t)$ como el término que resulta de intercambiar cada aparición de $\mathbf{a}_n$ por $\mathbf{a}_{\sigma n}$ en t, de modo que $\pi(t)$ nombra el conjunto que nombraría t si la sucesión genérica fuera la dada por $a'_n = a_{\pi n}$. En particular $\pi(\mathbf{a}_n) = \mathbf{a}_{\pi n}$.

Para cada fórmula ϕ del lenguaje del forcing, llamamos $\pi(\phi)$ a la fórmula que resulta de cambiar cada término t que aparezca en ϕ por $\pi(t)$. A su vez, para cada condición P, podemos definir $\pi(P)$ como la condición que consta de las fórmulas $\mathbf{n} \in \mathbf{a}_{\sigma n}$ o $\mathbf{n} \notin \mathbf{a}_{\sigma n}$ según si $\mathbf{n} \in \mathbf{a}_n$ o $\mathbf{n} \notin \mathbf{a}_n$ está en P. Entonces, Cohen demuestra:

$$P \Vdash \phi \qquad \text{si y sólo si} \qquad \pi(P) \Vdash \pi(\phi).$$

Para probar que C no contiene subconjuntos numerables (en N), suponemos que "alguien que viva en N" ve una aplicación $f : \omega \longrightarrow C$ inyectiva. Sea $\mathbf{f}$ un nombre para f en el *lenguaje del forcing.* Entonces, por la propiedad 3), tiene que haber una condición P_k de la sucesión genérica tal que

$$P_k \Vdash \mathbf{f} : \omega \longrightarrow V.$$

Cohen demuestra que podemos tomar un n suficientemente grande tal que toda permutación $\pi \in G_n$, es decir, que fije a los números naturales menores que n, cumple $\pi(\mathbf{f}) = \mathbf{f}$, $\pi(P_k) = P_k$. (La idea es que en cada término $\mathbf{f}$ sólo puede aparecer un número finito de términos $\mathbf{a}_n$ luego si π fija a suficientes números naturales, fija a todos los términos de $\mathbf{f}$.)

Para cada número natural k, se cumple que $f(k) = a_l$, para cierto $l < \omega$. Como f es inyectiva, de entre los números $k > N$, habrá a lo sumo un número finito de valores para los que el l correspondiente sea $l < N$, luego podemos tomar un $k > N$ suficientemente grande como para que $f(k) = a_l$, con $l \geq N$.

A su vez, tiene que haber una condición de la sucesión genérica, digamos $P_{k'}$, con $k' \geq k$, tal que

$$P_{k'} \Vdash \mathbf{f}(\mathbf{k}) = \mathbf{a}_l.$$

Tomemos $l' > l$ suficientemente grande como para que $\mathbf{a}_{l'}$ no aparezca en $P_{k'}$ y sea π la permutación que únicamente intercambia l con l'. Entonces $\pi \in G_n$, luego $P_k = \pi(P_k) \subset \pi(P_{k'})$ y $\pi(P_{k'}) \Vdash \bar{f}(\mathbf{k}) = \mathbf{a}_{l'}$, donde hemos usado que $\pi(\mathbf{k}) = \mathbf{k}$, porque, en general, π deja fijos a todos los nombres de los elementos de M, que se definen sin hacer referencia a la función genérica.

Ahora bien, $Q = P_{k'} \cup \pi(P_{k'})$ es una condición válida, es decir, no contiene fórmulas contradictorias. Esto se debe a que $\pi(P_{k'})$ se calcula cambiando cada fórmula $\mathbf{m} \in \mathbf{a}_l$ o $\mathbf{m} \notin \mathbf{a}_l$ que haya en $P_{k'}$ por $\mathbf{m} \in \mathbf{a}_{l'}$ o $\mathbf{m} \notin \mathbf{a}_{l'}$ y estas fórmulas no van a contradecir a ninguna fórmula de P_k porque, por la elección de l', no hay ninguna fórmula en P_k que mencione a $\mathbf{a}_{l'}$.

De este modo, la condición Q extiende a $P_{k'}$ (luego a P_k) y a $\pi(P_{k'})$, por lo que

$$Q \Vdash \mathbf{f} : \omega \longrightarrow V \wedge \mathbf{f}(\mathbf{k}) = \mathbf{a}_l \wedge \mathbf{f}(\mathbf{k}) = \mathbf{a}_{l'}.$$

Ahora bien, por 5) existe una sucesión genérica cuyas condiciones extienden a Q. Si consideramos un modelo N' definido a partir de una de ellas y llamamos f' al conjunto nombrado por $\mathbf{f}$ en dicho modelo N', debería cumplirse

$$f' : \omega \longrightarrow V \wedge f(k) = a_l \wedge f(k) = a_{l'},$$

luego sería $a_l = a_{l'}$, cuando hemos demostrado que los conjuntos genéricos son siempre distintos dos a dos. ∎

Como consecuencia:

Las dos definiciones siguientes no son equivalentes si no se supone el axioma de elección:

- Un conjunto es finito si se puede biyectar con un número natural (y es infinito en caso contrario).
- Un conjunto es infinito si se puede biyectar con un subconjunto propio (y es finito en caso contrario).

Por último, Cohen incluye la demostración (inédita) de Feferman y Lévy de la consistencia con ZF de que $\aleph_1$ y $\mathbb{R}$ sean uniones numerables de conjuntos numerables.

Tras explicar cómo se puede sustituir el supuesto (indemostrable) de la existencia de un modelo transitivo numerable de ZFC por la existencia (demostrable) de modelos transitivos numerables de cualquier conjunto finito de axiomas de ZFC y de incluir la prueba de Sierpiński de que la hipótesis del continuo generalizada implica el axioma de elección, el libro termina con una sección de conclusiones, en la que se lee:

> *Nos enfrentamos ahora al problema de cómo considerar cuestiones como la hipótesis del continuo a la luz de estos resultados de independencia. Repasemos algunas posibles posturas. El punto de vista finitista, por supuesto, rechaza categóricamente la teoría de conjuntos por referirse a ficciones inexistentes y, por lo tanto, no consideraría que la hipótesis del continuo sea ni "verdadera" ni "falsa". Esta actitud probablemente sería compartida por otros lógicos de convicciones algo más liberales, como los intuicionistas. Aunque pueda parecer extremo, este punto de vista puede presentarse de forma bastante contundente y persuasiva. En esencia, uno puede tener la sensación de que la teoría de conjuntos es simplemente una envoltura muy exitosa que no tiene nada que ver con los conjuntos "reales", sino que, en el mejor de los casos, describe algún tipo de proceso mental utilizado para describir objetos reales como los números enteros. El gran defecto de esta perspectiva es que deja sin explicar*[224] *por qué esta ficción tiene éxito y cómo una intuición presuntamente incorrecta nos ha llevado a un sistema tan notable. Porque, como implica el teorema de Incompletitud de Gödel, podemos generar enunciados aritméticos demostrables en la teoría de conjuntos, pero no en sistemas inferiores. Rechazar simplemente estos enunciados y renunciar para siempre a cualquier posibilidad de decidirlos es tan insatisfactorio como no saber qué hacer con la hipótesis del continuo. Dado que la mayoría de los matemáticos son más o menos idealistas en su opinión de que los conjuntos realmente existen y que preguntas como la hipótesis del continuo tienen un significado, ahora analizaremos el problema desde este punto de vista. Uno puede tener la sensación de que nuestra intuición sobre los conjuntos es inagotable y que, eventualmente, se presentará un axioma intuitivamente claro que decida la hipótesis del continuo. Una posibilidad es $V = L$, pero ésta se rechaza casi universalmente. Introducir cualquiera de los axiomas superiores de infinito no altera la situación, ya que el lector puede convencerse de que si el modelo M tiene un cardinal muy grande, la introducción de los conjuntos genéricos utilizados para demostrar la consistencia de la hipótesis del continuo no afectará el tamaño (independientemente del sentido del término) del cardinal en N. Parece que sólo los axiomas que restringen el carácter de los conjuntos, como $V = L$, tienen alguna esperanza de demostrar la hipótesis del continuo, y éstos no son muy aceptables.*
>
> *Un punto de vista que el autor cree que podría eventualmente aceptarse es que la hipótesis del continuo es obviamente falsa. La razón principal por la que se acepta el axioma de infinito es probablemente que nos parece absurdo pensar que el proceso de añadir sólo un conjunto a la vez pueda agotar todo el universo. Lo mismo ocurre con los axiomas de infinitud superiores. Ahora bien, $\aleph_1$ es el conjunto de ordinales numerables, y éste es simplemente una forma especial y la más simple de generar un cardinal mayor. El conjunto $C = \mathcal{P}\omega$, en cambio, se genera mediante un principio totalmente nuevo y más poderoso: el axioma del conjunto de partes. Es irrazonable esperar que cualquier descripción de un cardinal mayor que intente construirlo a partir de ideas derivadas*

[224] Hilbert lo explica, y nadie habla de "intuiciones incorrectas". A lo sumo, los intuicionistas hablarían de "supuestos contrarios a la intuición", que no es lo mismo, pero aquí hay que tener en cuenta que Cohen usa "intuición" en un sentido completamente distinto al que le daban al término Hilbert o Brouwer, y que es posible que ni él mismo fuera consciente de ello.

del axioma de reemplazo pueda llegar a C. Por lo tanto, C es mayor que $\aleph_n$, $\aleph_\omega$, $\aleph_\alpha$ donde $\alpha = \aleph_\omega$, etc. Este punto de vista considera a C como un conjunto increíblemente rico, proporcionado por un nuevo y audaz axioma, que nunca podrá abordarse mediante un proceso de construcción fragmentado. Quizá las generaciones posteriores vean el problema con mayor claridad y se expresen con mayor elocuencia.

96 La Lógica matemática de Kleene y la de Shoenfield En **1966** Kleene publicó su *Lógica matemática,* un tratado de lógica dirigido a estudiantes universitarios (con la intención de ser más accesible que su *Introducción a la metamatemática.* La diferencia respecto al libro de Mendelson es radical. Kleene opta por posponer la distinción sutil entre matemática y metamatemática hasta el capítulo IV. Así, en el capítulo I (dedicado al cálculo proposicional) pasa por encima sobre el asunto:

Ahora nos proponemos estudiar la lógica, y de hecho mediante métodos matemáticos. Aquí nos enfrentamos a una paradoja. ¿Cómo podemos tratar la lógica matemáticamente (o de forma sistemática) sin usar la lógica en su tratamiento?

La solución de esta paradoja es sencilla, aunque nos llevará algún tiempo comprender plenamente su funcionamiento. Simplemente, colocamos la lógica que estudiamos en un compartimento y la lógica que utilizamos para estudiarla en otro. En lugar de "compartimentos", podemos hablar de "lenguajes". Cuando estudiamos lógica, la lógica que estudiamos pertenecerá a un lenguaje, al que llamamos lenguaje objeto, porque este lenguaje (incluida su lógica) es objeto de nuestro estudio. Consideramos que nuestro estudio de este lenguaje y su lógica, incluido nuestro uso de la lógica para llevarlo a cabo, tiene lugar en otro lenguaje, al que llamamos lenguaje del observador. O podemos hablar de la lógica objeto y la lógica del observador. Será muy importante, a medida que avancemos, tener presente esta distinción entre la lógica que estudiamos (la lógica del objeto) y nuestro uso de la lógica al estudiarla (la lógica del observador). A cualquier estudiante que no esté dispuesto a hacerlo, le sugerimos que cierre el libro ahora y elija otro tema, como acrósticos o apicultura.

Un poco más adelante incide un poco más en la diferencia entre el razonamiento formal y el razonamiento en "el lenguaje del observador":

Dijimos "demostración formal" y "deducción formal" en las definiciones anteriores (aunque usualmente omitiremos la palabra "formal") para enfatizar que estas demostraciones y deducciones están en el lenguaje objeto, que estamos estudiando en el lenguaje del observador (§1). [...] *En nuestro estudio (en el lenguaje del observador), también probaremos teoremas, deduciremos consecuencias de premisas, etc. Esto será tan cierto aquí en la teoría de la demostración como lo fue en la teoría de modelos. En estas demostraciones y deducciones informales podemos operar con flexibilidad, basándonos en el significado de nuestros enunciados, utilizando cualquier inferencia convincente. (Es posible que algunas de estas inferencias sean la contrapartida informal de las operaciones disponibles en las demostraciones formales, pero no están limitadas a serlo).*

Esto no significa que nuestras demostraciones y deducciones informales en el lenguaje del observador no deban ajustarse a ningún estándar lógico. Pero ahora no intentamos regularlas ni estudiarlas como ejemplos de lógica.

En los capítulos II y III presenta el cálculo de predicados[225] y el cálculo de predicados con igualdad, y sólo en el capítulo IV, el primero de la segunda parte del libro, entra abiertamente en la distinción entre el razonamiento formal y el razonamiento intuitivo. En una exposición similar al inicio de su *Introducción a la metamatemática,* Kleene introduce algo de teoría ingenua de conjuntos, explica las paradojas de la teoría de conjuntos, y luego viene la sección §36 *Pensamiento axiomático frente a pensamiento intuitivo en matemáticas,* donde plantea la cuestión en términos como éstos:

Uno de los problemas de la axiomática formal es demostrar que los sistemas axiomáticos no son vacíos. Sin embargo, un sistema de objetos utilizado como interpretación a menudo se deriva de otra teoría axiomática; entonces tenemos una regresión, que simplemente nos lleva a la cuestión de la importancia de dicha teoría axiomática. Si en ninguna etapa se realiza una aplicación fuera de

[225] Del capítulo II citamos sólo esa nota al pie: *El cálculo de predicados (o lo que añade al cálculo proposicional) a veces se denomina "teoría de la cuantificación". En la literatura, "$(\forall x)$", "(x)", "$\bigwedge x$", "Πx" se utilizan a menudo para nuestro "$\forall x$"; "$(\exists x)$", "(Ex)", "$\bigvee x$", "Σx" para "$\exists x$".*

la axiomática formal, toda la actividad parecerá fútil. Por lo tanto, concluimos que, si no vamos a adoptar un nihilismo matemático, las matemáticas formalmente axiomatizadas no deben ser la totalidad de las matemáticas. En algún punto debe haber significado, verdad y falsedad. Como mínimo, cuando decimos que en una teoría axiomática formal dada una determinada proposición es un teorema, debemos creer que esto es verdad, es decir, que la proposición se sigue de los axiomas, aunque no se tiene en cuenta si la proposición en sí es verdadera, ya que en la axiomática formal las deducciones se llevan a cabo antes de asignar significados a los términos primitivos (o de descartar dicha asignación).

Luego discute los puntos de vista de Hilbert y Brouwer. En §37 *Sistemas formales, metamatemáticas,* establece ya definitivamente la necesidad de que el razonamiento metamatemático sea finitista, o al menos, intuitivamente significativo:

Ahora relacionamos la terminología actual con la utilizada en la Parte I. No consideramos que un lenguaje, tomado como objeto de estudio, sea un "sistema formal" a menos que sea un lenguaje simbólico (no parte de un lenguaje verbal, como el inglés) y a menos que se especifiquen para él axiomas y reglas de inferencia (no simplemente conceptos de teoría de modelos, como "válido" y "consecuencia válida"). No nos referimos a un lenguaje utilizado en el estudio de un lenguaje objeto como "metalenguaje" o "lenguaje sintáctico" a menos que en él se utilicen únicamente métodos finitistas (aunque algunos autores lo hagan). Por lo tanto, "lenguaje objeto" y "lenguaje del observador", tal como se utilizan en la Parte I, son términos más amplios que "sistema formal" y "metalenguaje".

En la Parte I, utilizamos el término "teoría de la demostración" de forma un tanto imprecisa en comparación con el sentido que Hilbert pretendía, al que nos ceñiremos ahora. Porque, en realidad, allí no habíamos especificado un lenguaje simbólico.

En nuestra "teoría de la demostración" de la Parte I utilizamos únicamente métodos finitistas, aunque no lo mencionamos. En la "teoría de modelos", los métodos no se limitan a ser finitistas. En la "teoría de modelos" moderna, también trabajaríamos con un lenguaje completamente simbólico.

Y a partir de aquí pasa a exponer ya la teoría de las funciones computables, los teoremas de incompletitud, etc. Especialmente interesante es su minucioso análisis de los teoremas de completitud y de Löwenheim-Skolem, en los que sigue aproximadamente la prueba que dio en 1955 el neerlandés Evert Willem Beth en su trabajo *Inferencia semántica y derivabilidad formal,* aunque expresada en términos del cálculo secuencial de Gentzen, pero considerando secuentes que admiten una cantidad numerable de fórmulas, en lugar de una cantidad finita. Sobre ella dice:

Dado que el teorema de completitud de Gödel y el teorema de Löwenheim-Skolem implican las nociones no constructivas de validez y satisfacibilidad, no pertenecen a la metamatemática. Por lo tanto, sus demostraciones no pueden ser completamente finitistas. Demostraciones como las que hemos visto reducen esta no constructividad al mínimo. De hecho, los únicos pasos no constructivos en las demostraciones del teorema 34 y del teorema 37 con "$\aleph_0 \vDash$" son aplicaciones de la ley clásica del tercio excluso a proposiciones sobre conjuntos infinitos numerables.

Pero esta preocupación por mostrar que las teorías axiomáticas para tratar con conceptos no finitistas pueden construirse por medios finitistas era cada vez menos frecuente. Así, en **1967** Joseph Robert Shoenfield publicó un libro con el mismo título que el de Kleene: *Lógica matemática,* aunque no iba dirigido a estudiantes universitarios, sino a graduados. Su primer capítulo se titula *La naturaleza de la lógica matemática,* y sobre los métodos finitistas dice lo siguiente:

La segunda razón [para estudiar la lógica de las teorías matemáticas] *es que los conceptos matemáticos suelen ser muy abstractos y, por lo tanto, difíciles de comprender. Una sentencia, por otro lado, es un objeto concreto; así que, al estudiar los axiomas como sentencias, nos acercamos a lo abstracto a través de lo concreto.*

Un punto es evidente: no tiene sentido estudiar objetos concretos (en lugar de abstractos) a menos que los abordemos de manera concreta o constructiva. Por ejemplo, cuando queremos demostrar que un objeto concreto con una propiedad determinada existe, deberíamos construir dicho objeto, no simplemente demostrar que su inexistencia llevaría a una contradicción.

Las demostraciones que abordan objetos concretos de manera constructiva se denominan finitistas. Otra descripción, sugerida por Kreisel, es la siguiente: una demostración es finitista si podemos

visualizarla. Por supuesto, ninguna de las dos descripciones es muy precisa; pero podemos aplicarlas en muchos casos para decidir si una demostración en particular es finitista o no. Una vez apreciada la diferencia fundamental entre objetos concretos y abstractos, se plantean diversas preguntas que sólo pueden responderse mediante el estudio de las demostraciones finitistas. Por ejemplo, Hilbert, quien inició este estudio, consideraba que sólo las matemáticas finitistas están justificadas de forma inmediata por nuestra intuición. Se introducen las matemáticas abstractas para obtener resultados finitistas de una manera más fácil o elegante. Por lo tanto, propuso como programa demostrar que toda (o una parte considerable) de las matemáticas abstractas comúnmente aceptadas puede considerarse de esta manera. La cuestión de hasta qué punto puede llevarse a cabo tal programa es de evidente interés, incluso para quienes no suscriben la visión de Hilbert de las matemáticas abstractas.

El estudio de axiomas y teoremas como sentencias se denomina estudio sintáctico de los sistemas axiomáticos; el estudio del significado de estas sentencias se denomina estudio semántico de los sistemas axiomáticos. Por las razones expuestas, a menudo separaremos las partes sintáctica y semántica de nuestras investigaciones. Cuando sea posible y razonablemente conveniente, realizaremos nuestras investigaciones sintácticas de manera finitista. Siempre consideraremos los axiomas y teoremas como sentencias y, por lo tanto, objetos sintácticos; cuando deseemos estudiarlos semánticamente, hablaremos del significado del axioma o teorema.

Así pues, Shoenfield simplemente se compromete a usar métodos finitistas "cuando sea posible", pero no tiene inconveniente en enunciar y usar una afirmación equivalente al axioma de elección en el capítulo 4, en la sección dedicada al teorema de completitud, o de hablar de cardinales infinitos en el capítulo 5, dedicado a la teoría de modelos, antes de introducir una teoría axiomática de conjuntos en el capítulo 9. Naturalmente, esto no significa que Shoenfield esté haciendo nada mal. Simplemente, está exponiendo la lógica matemática tomando como metamatemática la teoría de conjuntos, y el capítulo 9 es simplemente el capítulo dedicado a estudiar la propia teoría de conjuntos. A lo sumo, se le podría pedir que dedicara unas líneas en la introducción a aclarar que su libro no pretende fundamentar el razonamiento matemático, sino que lo da por hecho para estudiar la lógica matemática. De este modo, un lector que tomara el libro esperando encontrar una fundamentación del razonamiento matemático y creyera que ése es uno de los propósitos del libro, no se sentiría engañado o, peor aún, no empezaría a sospechar que la fundamentación de la matemática es una estafa. Lo que ponen en evidencia las últimas publicaciones en lógica es que en esa época ya nadie consideraba un problema serio, delicado y peliagudo la fundamentación de la matemática —porque ciertamente no lo es— y por eso lo que interesa a un lógico de primera línea como Shoenfield no es entrar en disquisiciones filosóficas sobre cuán finitista es un argumento, sino exponer los hechos que considera interesantes de la forma más cómoda, y la forma más cómoda es, sin duda, trabajando en el marco de la teoría axiomática de conjuntos. Probablemente, para Shoenfield, fundamentar la matemática, era simplemente un ejercicio que dejaba a cargo del lector, y no era un ejercicio complicado para un lector que hubiera asimilado su libro (salvo que el lector tuviera muchas objeciones filosóficas a las que Shoenfield, sin duda, no tenía ningunas ganas de pararse a replicar).

El libro de Shoenfield es hoy en día un clásico muy completo, de mucho más nivel que los de Kleene, que cubre con gran profundidad, para el espacio disponible, el cálculo deductivo, la teoría de modelos, la teoría de la recursión, la teoría de la demostración, incluyendo los teoremas de incompletitud (y resultados afines) y la prueba de la consistencia de la aritmética en una versión que había formulado Gödel en 1958 de la prueba de Gentzen.

En cuanto al último capítulo, dedicado a la teoría de conjuntos, describe la teoría de conjuntos de Zermelo-Fraenkel (y es uno de los primeros textos en los que se llama ZFC a ZF con el axioma de elección), y sus cuatro últimas secciones están dedicadas, respectivamente,

1. A demostrar la consistencia del axioma de elección y de la hipótesis del continuo generalizada (mediante la construcción que dio Gödel de L en 1940 para NBG, pero adaptada a ZF).

2. A exponer una presentación axiomática del *forcing* muy peculiar.

3. A demostrar la independencia del axioma de elección y de la hipótesis del continuo.

4. A estudiar los cardinales inaccesibles y medibles, incluyendo el teorema de Scott, por el que la existencia de un cardinal medible contradice al axioma de constructibilidad.

Shoenfield dice que su presentación del *forcing* es básicamente la de Cohen, pero haciendo uso "de ciertas simplificaciones descubiertas por Feferman, Scott y Solovay". Para entenderla conviene prestar atención antes a un artículo que Scott publicó ese mismo año de **1967**, titulado *Una demostración de la independencia de la hipótesis del continuo,* donde esbozaba una forma de demostrar la independencia de la hipótesis del continuo usando álgebras de Boole. Scott explica en el propio artículo cómo surgió la idea:

> *A aquellos lectores familiarizados con la demostración original de Cohen, nuestro enfoque les puede parecer al principio muy diferente. En realidad, no lo es. Fue R. M. Solovay quien primero señaló al autor [comunicación privada, septiembre de 1965] que la definición de Cohen de* forcing *podía verse como una forma de asignar valores booleanos a fórmulas. (Había descubierto esta idea en un caso particular al usar conjuntos de Borel de medida positiva como condiciones de* forcing*). De hecho, al asociar a cada fórmula el par de conjuntos que consisten, primero, en aquellas condiciones que fuerzan (débilmente) la fórmula y, segundo, en aquellas que fuerzan (débilmente) la negación de fórmula, Solovay observó que, en general, estos pares formaban un álgebra de Boole completa. Más importante aún, se podía demostrar que las propiedades bien conocidas de las álgebras de Boole, como las leyes distributivas y la condición de cadena numerable, eran responsables de las propiedades deseables de los modelos que se construían.*
>
> *El autor* [Scott] *sugirió entonces invertir la situación y utilizar las condiciones simples en la asignación de los valores booleanos como una forma de evitar la definición de la relación "forzar". Desde este punto de vista, quedó muy claro cómo se podía utilizar un álgebra de Boole completa arbitraria para asignar valores a las fórmulas. Esto ya lo sabía Solovay, porque una construcción abstracta de condiciones de* forcing *podía llevar a convertir cualquier álgebra de Boole que se quisiera en el álgebra de pares de conjuntos de condiciones. Por supuesto, en definitiva, esto no es más que una reformulación del método original de Cohen. Sin embargo, tenía la ventaja de que permitiía evitar el uso de los modelos numerables de la teoría de conjuntos si se estaba dispuesto a trabajar con valores booleanos de fórmulas. Esta misma ventaja también la había observado Vopěnka en su reformulación del método de Cohen. (La idea de Vopěnka no funcionaba tan bien como la de Solovay porque utilizaba el* forcing *fuerte, que requiere que los valores de las fórmulas se encuentren en un retículo completo determinado que no es un álgebra de Boole. El álgebra de Boole, más útil, es simplemente un subretículo del retículo de Vopěnka).*
>
> *Luego, el 1 de enero de 1966, al autor* [Scott] *se le ocurrió que, una vez que uno acepta la idea de los valores booleanos, realmente no hay necesidad de hacer el esfuerzo de construir un modelo para la teoría completa de conjuntos transfinitos. En particular, el uso del método de Gödel de conjuntos constructibles, que parecía tan necesario para la definición recursiva transfinita del* forcing*, podría evitarse por completo. En otras palabras, el método original de Cohen, tal como lo reinterpretó Solovay, podría verse como la construcción de algunas extensiones muy especiales con valores booleanos de nociones ordinarias. Pero luego, cuando reconocimos sus propiedades más simples, pudimos tomar todos los objetos con esas propiedades para formar un modelo tan bueno como el de Cohen (como lo hemos hecho al definir funciones aleatorias). Parece que, para noviembre de 1965, el propio Solovay había notado que una versión con valores booleanos de la construcción de conjuntos de potencias* [de la jerarquía de von Neumann] *conduciría a modelos para la teoría de tipos y la teoría de conjuntos; y, como señaló más tarde, cuando se utiliza la versión de Easton del método de Cohen, los objetos construidos por recursión transfinita darán esencialmente todos los objetos del modelo booleano.*

Modelos booleanos Vamos a explicar todo esto, en gran parte siguiendo los detalles que da el propio Scott en su artículo. Según ya hemos señalado, en la construcción del modelo en que todo subconjunto de $\mathbb{R}$ es medible Lebesgue, Solovay había aplicado el *forcing* tomando como condiciones los elementos del "álgebra de la medida" $\mathcal{B}_m = \mathcal{B}/I_m$ que resulta de dividir el álgebra de los conjuntos de Borel del intervalo $[0,1]$ entre el ideal formado por los conjuntos de Borel de medida de Lebesgue 0, que resulta ser un álgebra de Boole completa (donde todo subconjunto tiene supremo e ínfimo), y había observado que esto le permitía simplificar bastante la definición de $\Vdash$.

Pero, más en general, Solovay se había planteado que, en cualquier construcción mediante *forcing,* un "habitante del modelo base M" podía pensar en la extensión N en términos probabilísticos, es decir, puede pensar en la probabilidad de que en N se cumpla una propiedad, cosa que en general dependerá de la elección de la sucesión genérica con la que se ha construido N, desconocida para él.

Para concretar esa idea, según cuenta Scott, Solovay se dio cuenta de que, cualquiera que sea el conjunto P de condiciones empleado, el conjunto de los pares

$$(\{p \in P \mid p \Vdash \phi\}, \{p \in P \mid p \Vdash \neg\phi\})$$

(para la versión débil de "forzar") podía dotarse de estructura de álgebra de Boole completa $\mathbb{B}$, de modo que era equivalente usar como condiciones los elementos de P o los de $\mathbb{B} \setminus \{0\}$. Recíprocamente, fijada un álgebra de Boole completa $\mathbb{B}$, "alguien que viva en M" puede pensar en N en términos probabilísticos, asignando a cada fórmula ϕ del *lenguaje del forcing* el supremo

$$[\![\phi]\!] = \bigvee\{p \in \mathbb{B} \mid p \Vdash \phi\},$$

(que será 0 si ninguna condición fuerza ϕ) con lo que $p \Vdash \phi$ si y sólo si $p \leq [\![\phi]\!]$.

Así, si $[\![\phi]\!] = 1$, esto significa que todas las condiciones fuerzan ϕ, por lo que ϕ será verdadera en todos los modelos N, independientemente de qué sucesión genérica se tome. En cambio, si $[\![\phi]\!] = 0$, eso significa que ninguna condición fuerza ϕ, luego ϕ será falsa en todos los modelos N, mientras que si $[\![\phi]\!]$ toma un valor distinto de $0, 1$, eso significa que hay condiciones que fuerzan ϕ y otras que fuerzan $\neg\phi$, por lo que ϕ será verdadera en unos modelos N y falsa en otros, según la elección de la sucesión genérica.

En particular, dados dos nombres (términos) del *lenguaje del forcing,* tenemos definidos $[\![s = t]\!]$ y $[\![s \in t]\!]$ en el álgebra $\mathbb{B}$, que "miden" la probabilidad de que hagan referencia o no al mismo conjunto de N, o a que los conjuntos que nombran en N se pertenezcan o no el uno al otro.

La idea revolucionaria que, al parecer, tuvieron independientemente Solovay y Scott, era que es posible empezar de cero definiendo una sucesión de "nombres" imitando la construcción de la jerarquía de von Neumann:

$$V_0^{\mathbb{B}} = \varnothing, \qquad V_{\alpha+1}^{\mathbb{B}} = \mathbb{B}^{V_\alpha^{\mathbb{B}}}, \qquad V_\lambda^{\mathbb{B}} = \bigcup_{\delta<\lambda} V_\delta^{\mathbb{B}}, \qquad V^{\mathbb{B}} = \bigcup_{\alpha\in\Omega} V_\alpha^{\mathbb{B}},$$

donde $\mathbb{B}^{V_\alpha^{\mathbb{B}}}$ es el conjunto de todas las aplicaciones $\sigma : V_\alpha^{\mathbb{B}} \longrightarrow \mathbb{B}$. Sobre estos nombres se puede definir de forma relativamente sencilla y natural unas aplicaciones $[\![\sigma = \tau]\!]$ y $[\![\sigma \in \tau]\!]$ que tomen valores en $\mathbb{B}$. Por ejemplo, si $\sigma \in V_\alpha^{\mathbb{B}}$ y $\tau \in V_{\alpha+1}^{\mathbb{B}}$, entonces[226] $\|\sigma \in \tau\| = \tau(\sigma)$. Así pues, cada "nombre" τ es una función que asigna a los nombres previos σ una "probabilidad" $\tau(\sigma) = [\![\sigma \in \tau]\!]$ de que el objeto nombrado por σ pertenezca al objeto nombrado por τ.

A partir de estas asignaciones de valores booleanos a las fórmulas atómicas, es fácil[227] asignar un valor booleano a cada fórmula ϕ del lenguaje usual de la teoría de conjuntos (no de ningún *lenguaje del forcing* con cuantificaciones limitadas) extendido simplemente con los elementos de $V^{\mathbb{B}}$ como constantes. Concretamente:

$$[\![\neg\phi]\!] = [\![\phi]\!]', \qquad [\![\phi \vee \psi]\!] = [\![\phi]\!] \vee [\![\psi]\!], \qquad [\![\bigwedge x\, \phi(x)]\!] = \bigwedge_{\sigma\in V^{\mathbb{B}}} [\![\phi(\sigma)]\!],$$

y se puede definir $p \Vdash \phi$ como $p \leq [\![\phi]\!]$, aunque en realidad no es necesario hacerlo, sino que se puede trabajar siempre con los valores booleanos en lugar de con $\Vdash$. (Notemos que, en este contexto, una condición p extiende a otra q, es decir, contiene más información, si $p \leq q$, pues entonces q fuerza todas las fórmulas que fuerza p.)

En realidad, todo lo que hemos definido hasta aquí puede definirse en ZFC a partir de un álgebra de Boole completa $\mathbb{B}$, y la clase $V^{\mathbb{B}}$ de todos los nombres resulta ser una clase propia, pero si fijamos un modelo transitivo numerable M de ZFC, todo esto puede hacerse en M, donde $\mathbb{B} \in M$ es un álgebra de Boole completa en M, y así obtenemos $M^{\mathbb{B}}$, que es una clase propia para "alguien que viva en M", pero en realidad es un conjunto numerable.

Usando la numerabilidad de M (que a su vez implica la numerabilidad de conjunto de fórmulas $\phi(\sigma_1, \ldots, \sigma_n)$ del lenguaje de ZFC extendido con los nombres de $M^{\mathbb{B}}$ como constantes), podemos construir una sucesión genérica

$$p_0 \geq p_1 \geq p_2 \geq \cdots,$$

[226] En realidad esto no es exacto, sino que para que se cumpla es necesario tomar como $V_{\alpha+1}^{\mathbb{B}}$ un cierto subconjunto de $\mathbb{B}^{V_\alpha^{\mathbb{B}}}$. Si no, hay que tener en cuenta que puede ocurrir, por ejemplo, que $\sigma_1, \sigma_2 \in V_\alpha^{\mathbb{B}}$ cumplan $[\![\sigma_1 = \sigma_2]\!] = 1$ mientras que $\tau(\sigma_1) \neq \tau(\sigma_2)$, y ambos valores deben ser tenidos en cuenta para definir $[\![\sigma_i \in \tau]\!]$, pues debe cumplirse que $[\![\sigma_1 \in \tau]\!] = [\![\sigma_2 \in \tau]\!]$.

[227] Daremos los detalles en la sección 98

y cada sucesión genérica determina un *ultrafiltro genérico* $G = \{p \in \mathbb{B} \mid \bigvee k \in \omega\ p_k \leq p\}$, formado por todas las condiciones verdaderas.[228] A su vez, a partir de un ultrafiltro genérico G se puede construir el modelo N a partir de $M^{\mathbb{B}}$, como el conjunto de todos los valores σ_G de todos los nombres $\tau \in M^{\mathbb{B}}$, definidos recurrentemente como sigue:

$$\tau_G = \{\sigma_G \mid \sigma \in \mathcal{D}\tau \wedge [\![\sigma \in \tau]\!] \in G\}.$$

Es decir, cada nombre τ es una función $\tau : V_\alpha^{\mathbb{B}} \longrightarrow \mathbb{B}$. Supuesto que ya estén definidos los conjuntos σ_G nombrados por cada elemento $\sigma \in V_\alpha^{\mathbb{B}}$, para determinar el conjunto τ_G nos quedamos únicamente con los nombres σ tales que la condición $[\![\sigma \in \tau]\!]$ es verdadera (es decir, que está en el filtro genérico) y τ_G está formado por los σ_G correspondientes.

Así, definimos $N = M[G] = \{\tau_G \mid \tau \in M^{\mathbb{B}}\}$, y resulta ser el mismo modelo construido con el *forcing* usual,[229] y el resultado fundamental es que

$$M[G] \vDash \phi((\sigma_1)_G, \ldots, (\sigma_n)_G) \qquad \text{si y sólo si} \qquad [\![\phi(\sigma_1, \ldots, \sigma_n)]\!] \in G.$$

Esta relación plasma que $[\![\phi]\!]$ expresa la probabilidad de que ϕ sea cierta. Lo será si y sólo si $[\![\phi]\!] \in G$. El valor $[\![\phi]\!]$ puede calcularlo "alguien que viva en M", de modo que, si obtiene el valor 1, sabe que ϕ va a ser cierta en $N = M[G]$ con toda seguridad, si obtiene el valor 0 será falsa con toda seguridad, y si obtiene otro valor es que la verdad o falsedad de ϕ depende del ultrafiltro genérico considerado.

Lo que señala Scott es que, llegados a este punto, en realidad no es necesario considerar para nada los modelos M y N. Simplemente, razonando en ZFC, sin considerar modelos, partiendo de un álgebra de Boole completa $\mathbb{B}$, podemos construir la clase $V^{\mathbb{B}}$, definir $[\![\phi]\!]$ y demostrar directamente que todos los teoremas de ZFC cumplen $[\![\phi]\!] = 1$ (como tiene que ser, porque son verdaderos en todos los modelos N). Entonces, si, eligiendo el álgebra adecuada, podemos demostrar, por ejemplo, que $[\![2^{\aleph_0} = \aleph_1]\!] < 1$, podemos concluir que la hipótesis del continuo no es demostrable en ZFC, y tenemos una prueba de consistencia que no requiere ni modelos numerables, ni el lenguaje sofisticado del *forcing,* ni, puestos tomar un M y construir N, hacerlo imitando la construcción de L.

Scott menciona al matemático checo Petr Vopěnka, que en 1965 había publicado un artículo titulado *Sobre el modelo* ∇ *de la teoría de conjuntos,* y ese mismo año de **1967** publicó *Teoría general de modelos* ∇*,* donde desarrollaba una teoría similar a la de Scott y Solovay. ∎

Los *lenguajes del forcing* habituales, se llamaban *lenguajes ramificados.* Esto hace referencia al hecho de que permiten construir fórmulas limitadas, bien usando cuantificadores limitados, bien usando juegos de variables con un rango asociado que restringe los valores que pueden tomar en las cuantificaciones. Así, cada fórmula tiene un rango y éste es esencial, por ejemplo, para definir términos $\hat{x}_\alpha\phi(x)$ o para determinar recurrentemente las constantes F_α sin hacer referencia a constantes "posteriores" (en la formulación original de Cohen).

Sin embargo, el enfoque de Solovay y Scott en términos de álgebras de Boole no necesitaba construir un lenguaje ramificado, ni considerar modelos M o N. Para demostrar que una fórmula ϕ no es demostrable en ZFC, bastaba elegir el álgebra de Boole adecuada y demostrar que $[\![\phi]\!] \neq 1$.

Shoenfield se propuso conseguir lo mismo sin álgebras de Boole, es decir, partir de un conjunto parcialmente ordenado P de condiciones cualesquiera y definir un análogo a $[\![\phi]\!] = 1$ sin definir un lenguaje ramificado y sin construir ningúna álgebra de Boole, de modo que, eligiendo el conjunto P adecuado, bastara demostrar $[\![\phi]\!] \neq 1$ para justificar que ϕ no es demostrable en ZFC.

Conjuntos genéricos Para entender el planteamiento de Shoenfield necesitamos incorporar todavía un ingrediente más, y es que, al igual que Lévy había observado que es posible definir el conjunto de condiciones independientemente del *lenguaje del forcing,* Solovay observó también que es posible definir la genericidad a partir del conjunto de condiciones, sin necesidad de hacer referencia a $\Vdash$.

Para entender cómo, consideremos un conjunto de condiciones P, parcialmente ordenado por la inclusión. Diremos que un conjunto $D \subset P$ es *denso* en P si, para toda condición $p \in P$ existe una condición $q \in P$ tal que $p \subset q$ y $q \in D$, es decir, que toda condición se extiende a una que está en D.

[228] Las condiciones verdaderas respecto de una sucesión genérica forman un ultrafiltro del álgebra $\mathbb{B}$, pero no todo ultrafiltro es genérico. Un ultrafiltro genérico se define como un ultrafiltro generado por una sucesión genérica.

[229] Como señala Scott, esto es cierto si consideramos la versión de Easton (o de Lévy), que garantiza que N cumple el axioma de elección si lo cumple M, pero no la construcción de Cohen de su libro de 1966, donde N no cumple necesariamente el axioma de elección.

En estos términos, hemos visto que, para toda fórmula ϕ del *lenguaje del forcing,* el conjunto

$$D_\phi = \{p \in P \mid p \Vdash \phi \vee p \Vdash \neg\phi\}$$

es denso en P. Con esto ya podemos dar una definición general de "genericidad":

Diremos que un conjunto $G \subset P$ es *P-genérico* sobre un conjunto M si cumple las propiedades siguientes:

1. $\varnothing \in G$.
2. Si $p \in G$ y $q \in D$ cumple $q \subset p$, entonces $q \in G$.
3. Si $p, q \in G$, entonces $p \cup q \in G$.
4. Si $D \in M$ es un conjunto denso en P, entonces $P \cap D \neq \varnothing$.

Y podemos demostrar que siempre hay conjuntos genéricos sobre conjuntos numerables:

Teorema Si M es un conjunto numerable y $p \in P$, existe un conjunto G tal que $p \in G$ y G es P-genérico sobre M.

Demostración: Si M es un conjunto numerable, siempre existe un conjunto P-genérico sobre M. Basta considerar una enumeración $\{D_k\}_{k<\omega}$ de todos los subconjuntos densos en P que están en M. Dada cualquier condición $p \in P$, podemos tomar $p_0 \supset p$ tal que $p_0 \in D_0$, y a su vez $p_1 \supset p_0$ tal que $p_1 \in D_1$, etc. Obtenemos así una sucesión de condiciones

$$p \subset p_0 \subset p_1 \subset p_2 \subset \cdots$$

tales que $p_k \in D_k$. El conjunto

$$G = \{q \in P \mid \bigvee k < \omega\ p \leq p_k\}$$

contiene a p y a todos los p_k y es claramente P-genérico sobre M. ∎

Ahora, si ϕ es una fórmula del *lenguaje del forcing* y M es un modelo transitivo numerable de ZFC, el conjunto $D_\phi \in M$, luego, si G es P-genérico sobre M, existe una condición $p \in G \cap D_\phi$, es decir, una condición tal que $p \Vdash \phi$ o bien $p \Vdash \neg\phi$, que era justo lo que requiere la teoría del *forcing.* El conjunto genérico G es simplemente el conjunto de todas las condiciones verdaderas respecto de cualquier sucesión que lo genera.

Con esta definición de "conjunto genérico" se ve claramente en qué consiste la "genericidad" (también puede verse en términos de la definición de Cohen, pero es más técnico). Pensemos en el caso más simple, del conjunto P de las condiciones que determinan un único subconjunto genérico de ω. Podemos verlas como funciones $p : A \longrightarrow 2$, donde A es un subconjunto finito de ω.

Si G es un conjunto genérico (sobre un modelo M) para estas condiciones, entonces G define una *función genérica* $f_G = \bigcup_{p\in G} p : \omega \longrightarrow 2$.

En efecto, para cada $n \in \omega$, el conjunto de condiciones p que están definidas en n es denso (porque toda condición se puede extender a una definida en n), luego existe al menos una condición $p \in G$ definida en n, luego f_G está definida en n, para todo número natural n.

¿Y cómo es esta función genérica? ¿Puede ser constante? No, porque, para todo $n \in \omega$, el conjunto de las condiciones que toman el valor 0 en un número $m > n$ es denso (toda condición se puede extender a otra que tome el valor 0 en un número $m > n$), luego existe $p \in G$ que está definida en un $m > n$ y $p(m) = 0$, luego $f_G(m) = 0$ en números arbitrariamente grandes, e igualmente $f_G(m) = 1$ en números arbitrariamente grandes.

En general, f_G cumple *todas* las propiedades que una condición no puede desmentir que vaya a cumplir. Por ejemplo, no podemos asegurar que $f_G(5) = 1$, porque si una condición que cumpla $p(5) = 0$ fuera verdadera, f_G no podría cumplir esto. En cambio, sí que podemos asegurar que f_G toma el valor 1 sobre números primos arbitrariamente grandes, porque, dado n, toda condición se puede extender a otra que tome el valor 1 sobre un primo mayor que n. Esto se traduce en que el conjunto genérico $a_G = \{n \in \omega \mid f_G(a) = 1\}$ contiene infinitos primos (y también infinitos compuestos, o infinitos cuadrados, etc.).

Por la misma razón, viendo a f_G como una sucesión de ceros y unos, en algún tramo tiene una codificación en binario de *La divina comedia,* porque toda condición se puede extender a otra que contenga una codificación en binario de *La divina comedia.* Así, una función genérica, en sus distintos tramos, contiene toda la literatura universal, y cualquier porción finita de información en la que podamos pensar. Eso es la "genericidad". ∎

Veamos finalmente cómo plantea Shoenfield el *forcing* en su libro. Como indicábamos, su planteamiento era muy "peculiar" y muy distinto de lo que hoy en día es habitual, y eso oculta las ideas importantes. Vamos a explicarlo un poco, pero la construcción se entenderá mejor en la página 280, donde comentaremos otro artículo de Shoenfield cuyo enfoque es mucho más moderno.

Consideremos un modelo transitivo numerable M de ZFC + $V = L$ en el que hemos fijado un conjunto P de condiciones. Entonces existe un conjunto genérico G que determina un modelo $M \subset M[G]$. "Alguien que viva en M" no puede ver el conjunto G, pero ¿qué pasaría si pudiera consultar un oráculo que le respondiera a cualquier pregunta sobre si una condición dada está o no en G?

Para concretar esta idea, le añadimos al lenguaje formal de ZFC un relator monádico C, de modo que $C(p)$ significa "la condición p es correcta" (es decir, es verdadera, está en G). Entonces "el habitante de M" podría constatar que se cumplen los axiomas siguientes:

1. $\bigwedge p(C(p) \to p \in P)$.
2. $C(\varnothing)$.
3. $\bigwedge pq(C(p) \wedge C(q) \to C(p \cup q))$.
4. $\bigwedge X \bigvee p(C(p) \wedge (p \in X \vee \bigwedge q(p \subset q \wedge q \in P \to q \notin X)))$.

El significado de los tres primeros es obvio, y el último afirma que todo conjunto X, o bien contiene un elemento de G, o bien hay un elemento de G que no tiene extensiones en X. No es inmediato, pero esto es una propiedad de los conjuntos genéricos. Esto se traduce, y Shoenfield así lo demuestra, en que si ZF es consistente, también lo es ZFC + $V = L$ más estos cuatro axiomas.[230] Y es en este contexto "peculiar" y atípico en el que Shoenfield expone el *forcing.*

Shoenfield empieza por aquí porque tiene que dejar claro cuáles son sus axiomas, pero de momento no los necesita y define (sin hacer referencia a C) la relación

$$p \Vdash \phi(x_1, \ldots, x_n)$$

para toda fórmula ϕ del lenguaje de ZFC, donde $x_1, \ldots, x_n$ son conjuntos cualesquiera.

Aquí hay una sutileza importante que no podemos dejar que pase inadvertida, y que se entiende mejor si consideramos un modelo transitivo numerable M de los axiomas de Shoenfield y pensamos en usar esto para construir un modelo $M[G]$. La sutileza es que Shoenfield había encontrado una forma de usar a todos los conjuntos de M como nombres posibles para los conjuntos de $M[G]$. En otras palabras, el análogo en Shoenfield del conjunto de nombres $M^{\mathbb{B}}$ de Solovay y Scott es simplemente M. Por lo tanto, cuando escribimos $p \Vdash \phi(x_1, \ldots, x_n)$, no tenemos que pensar en $x_i \in M$ como el conjunto x_i, sino como el nombre de un conjunto $(x_i)_G$ de $M[G]$, que será un conjunto u otro en función de quién sea G.

Pero volvamos al caso general, sin tomar ningún modelo. Ahora Shoenfield aprovecha su oráculo y define:

$$\Vdash \phi \quad \text{si y sólo si} \quad \bigvee p(C(p) \wedge p \Vdash \phi).$$

Si esto lo hiciéramos en un modelo M, entonces, cuando un "habitante de M" comprobara $\Vdash \phi(x_1, \ldots, x_n)$ (para lo cual necesitaría consultar el oráculo) estaría comprobando que en $M[G]$ se cumple, no $\phi(x_1, \ldots, x_n)$, sino $\phi((x_1)_G, \ldots, (x_n)_G)$, para ciertos conjuntos $(x_i)_G$ que no hemos definido. Lo único que queremos resaltar aquí es que no debemos pensar que los conjuntos x_i "se representan a sí mismos".

En realidad, desde un punto de vista teórico, Shoenfield no necesitaría ir más allá, pues $\Vdash \phi$ le sirve como análogo a $[\![\phi]\!] = 1$, y se puede demostrar que todo teorema de ZFC cumple $\Vdash \phi$, pero para depender menos de la definición de $\Vdash$, que puede ser farragoso manejarla, Sheonfield define las relaciones

$$x =^* y \;\leftrightarrow \Vdash x = y, \qquad x \in^* y \;\leftrightarrow \Vdash x \in y.$$

[230] Aquí es fundamental que no estamos considerando como axiomas los casos particulares del axioma del reemplazo (o del esquema de especificación) para fórmulas que incluyan el relator nuevo. En otras palabras, que "el habitante de M" puede consultar el oráculo, pero no puede definir conjuntos usando sus predicciones. Sin esta restricción, la teoría sería contradictoria. Por ejemplo, el conjunto $X = \{p \in P \mid \neg C(p)\}$ contradiría el axioma 4 con casi cualquier conjunto P de condiciones que tomemos.

Así ha definido una igualdad y una pertenencia alternativas sobre conjuntos cualesquiera. Si $\phi(x_1,\dots,x_n)$ es cualquier fórmula del lenguaje de ZFC, podemos llamar $\vDash \phi(x_1,\dots,x_n)$ a la fórmula que resulta de sustituir cada $=$ por $=^*$ y cada $\in$ por $\in^*$. En estos términos, se cumple que, para todos los conjuntos $x_1,\dots,x_n$,

$$\vDash \phi(x_1,\dots,x_n) \qquad \leftrightarrow \qquad \Vdash \phi(x_1,\dots,x_n).$$

Y Shoenfield demuestra que si ϕ es un axioma de ZFC, entonces se cumple $\vDash \phi$, es decir, que la clase de todos los conjuntos es un modelo de ZFC cuando se reinterpretan la igualdad y la pertenencia como acabamos de indicar. Luego, en la sección siguiente, Shoenfield muestra cómo se puede usar esto para demostrar la independencia de la hipótesis del continuo y del axioma de elección. Habría muchas cosas que se podrían aclarar sobre este planteamiento, pero no merece la pena, porque, como decíamos, a continuación, en la sección siguiente, vamos a analizar otro artículo de Shoenfield "casi totalmente moderno" donde las ideas que aquí quedan escondidas quedan completamente expuestas.

97 Los Ángeles 1967 Del 10 de julio al 5 de agosto de **1967** tuvo lugar un congreso en la Universidad de California (en Los Ángeles) dedicado a la teoría axiomática de conjuntos. El comité organizador lo formaban Cohen, Abraham Robinson y Scott. Hubo más de 125 participantes. Scott fue el responsable de la edición de las contribuciones al congreso, que se retrasaría hasta 1971, y aún quedó una segunda parte pendiente que no vería la luz hasta 1974. En esta sección vamos a comentar las contribuciones más destacadas, que dan una buena panorámica del estado de la teoría de conjuntos tras casi un siglo de historia.

1. Forcing no ramificado (Shoenfield) Para conectar con la sección anterior, empezamos con la contribución de Shoenfield, que presenta una forma más convencional de eliminar el *lenguaje del forcing* ramificado, que es casi idéntica a una de las formas alternativas en que hoy en día se plantea el *forcing.* Copiamos su planteamiento:

> *Una noción de* forcing *es un conjunto parcialmente ordenado C que tiene un máximo elemento. Escribimos $\le_C$ o $\le$ para la relación de orden y 1_C o 1 para el máximo. Los elementos de C se llaman* condiciones. *Las condiciones se designan generalmente por p, q y r. Si $p \le q$, decimos que p es una* extensión *de q. Un subconjunto D de C es C-*denso *(o simplemente* denso*) si cada condición en C tiene una extensión en D. Sea C una noción de* forcing *y sea M un conjunto. Un subconjunto G de C es C-*genérico *sobre M (o simplemente* genérico*) si se cumplen las condiciones siguientes:*
>
> *(G1)* $1 \in G$.
>
> *(G2) Para todo $p \in G$ y $q \ge p$, $q \in G$.*
>
> *(G3) Para todo $p, q \in G$, p y q tienen una extensión común en G.*
>
> *(G4) Para todo conjunto denso D en M, $G \cap D \ne 0$.*

Notemos que estos convenios están motivados por la presentación en términos de álgebras de Boole, o por la concepción probabilística del *forcing.* Por ejemplo, si pensamos en las condiciones que adjuntan un subconjunto genérico de ω, el conjunto C está formado en ese caso por las funciones p definidas de un subconjunto finito de ω en 2, vistas como "piezas" para construir una función genérica $f : \omega \longrightarrow 2$.

Según la notación de Shoenfield, una condición p extiende a otra q (es decir, $p \le q$) si $q \subset p$. Notemos que esto significa que p tiene más información que q, pero escribimos $p \le q$ porque eso significa que p es menos probable que q (cuanta más información, menos probabilidad). La condición máxima es $1 = \varnothing$, que no contiene ninguna información, y por ello se cumple con "probabilidad 1" (todo esto no son más que ideas vagas para explicar la notación empleada).

Actualmente a los conjuntos genéricos en este sentido se les llama más bien *filtros genéricos.* A continuación Shoenfield demuestra que siempre existen filtros (o conjuntos) genéricos sobre un conjunto numerable, por el argumento que hemos dado en la página 278.

En este punto es donde empieza la parte original. Shoenfield quiere definir un modelo $M[G]$ que extienda a M, para lo cual va a definir en M una clase de nombres para los conjuntos de $M[G]$, pero para ello no introduce un lenguaje ramificado, con términos que describan cómo se ha construido el conjunto que representan, sino que toma como conjunto de nombres al propio conjunto M, ni más ni menos, y en él define una relación de pertenencia:

$$a \in_G b \leftrightarrow \bigvee p \in G\, (a, p) \in b.$$

Es fácil ver que esta relación está bien fundada, lo que permite definir una aplicación $K_G : M \longrightarrow N$ mediante[231]

$$K_G(b) = \{K_G(a) \mid a \in_G b\}.$$

Ésta es la notación de Shoenfield, pero a partir de aquí usaremos la notación usual hoy en día, y escribiremos b_G en lugar de $K_G(b)$. Así, la igualdad anterior es[232]

$$b_G = \{a_G \mid \bigvee p \in G\,(a,p) \in b\}$$

y la imagen de la aplicación K_G es el conjunto $M[G] = \{a_G \mid a \in M\}$.

Analicemos esto: pensemos en los elementos de M como nombres de los elementos de $M[G]$. De cada $b \in M$, al considerarlo como nombre, sólo importa realmente qué pares contiene de la forma (a,p), con $p \in C$. Si b contiene este par, eso se interpreta como que "el conjunto nombrado por b podría contener al conjunto nombrado por a, y eso sucederá si la condición p es verdadera, es decir, si $p \in G$". Alternativamente, podemos pensar en p como un dato "probabilístico" sobre la posibilidad de que el conjunto nombrado por a pertenezca o no al conjunto nombrado por b. Por ejemplo, si $(a,1) \in b$, entonces es seguro que el conjunto nombrado por a pertenece al conjunto nombrado por b.

Al construir b_G, miramos todos los pares $(a,p) \in b$ (cualquier otro elemento que no sea de esta forma no influye en nada). Siempre que encontramos una condición p verdadera ($p \in G$), calculamos a_G y lo tomamos como un elemento de b_G. Por ejemplo, $\varnothing_G = \varnothing$. Si $b = \{(\varnothing, p)\}$, con $p \in C$, entonces

$$b_G = \begin{cases} \{\varnothing\} & \text{si } p \in G, \\ \varnothing & \text{si } p \notin G, \end{cases}$$

y de este modo se puede calcular el conjunto nombrado por cualquier nombre.

La única diferencia con el enfoque actual es que, como sólo importan los elementos de cada conjunto de la forma (a,p), en la práctica se define recurrentemente un *C-nombre* b como un conjunto formado por elementos de la forma (a,p), donde a es un C-nombre[233] y $p \in C$. Llamamos V^C a la clase de todos los C-nombres y $M^C = V^C \cap M$ es la clase de los C-nombres que ve "alguien que viva en M".

Con esto simplemente se eliminan todos los conjuntos que tienen elementos superfluos, pero el conjunto

$$M[G] = \{b_G \mid b \in M^C\}$$

es exactamente el mismo.

Observación 1 La relación con los modelos booleanos es que, si partimos de un álgebra de Boole completa, podemos exigir que cada nombre sea una función definida sobre otros nombres, de modo que un nombre $b \in M^{\mathbb{B}}$ asigna una única "probabilidad" $b(a) \in \mathbb{B}$ a cada nombre de su dominio, mientras que si partimos de un conjunto de condiciones arbitrario C, tenemos que dejar a cada nombre a que "juegue con varias papeletas" para pertenecer a b, de modo que b puede contener varios pares (tal vez infinitos) de la forma $(a,p_1),(a,p_2),(a,p_3)$, etc., y basta con que alguna condición p_i cumpla $p_i \in G$ para que tengamos $a_G \in b_G$. Si C fuera un álgebra de Boole completa, podríamos sustituir todos esos pares por un único par (a,p), tomando como p el supremo de las condiciones que acompañan a a en los elementos de b y así podríamos hacer que b fuera una función, pero no hay ninguna necesidad de que b sea una función. ∎

Por ejemplo, para probar que $M \subset M[G]$ basta definir, para cada $x \in M$, el nombre $\check{x} = \{(\check{y}, 1) \mid y \in x\}$. Por ejemplo:

$$\check{\varnothing} = \varnothing, \quad \check{1} = \{(\check{\varnothing}, 1)\}, \quad \check{2} = \{(\check{0}, 1), (\check{1}, 1)\}, \quad \check{3} = \{(\check{0}, 1), (\check{1}, 1), (\check{2}, 1)\}, \quad \ldots$$

Es claro entonces que $x = (\check{x})_G \in M[G]$

[231] Se trata del colapso de Mostowski (página 232), que está definido siempre que la relación está bien fundada y su imagen es siempre un conjunto transitivo. El hecho de que en este caso no sea una relación extensional se traduce en que la función colapsante K_G no es inyectiva.

[232] No necesitamos recurrir al colapso de Mostowski para justificar que esta definición es correcta. podemos verla como una definición por recursión transfinita sobre el rango de un conjunto en la jerarquía de von Neumann. Si $(a,p) \in b$, necesariamente a tiene rango menor que b, por lo que, si suponemos que a_G está definido para todos los conjuntos a de rango menor que b, podemos definir b_G de este modo, ya que los conjuntos a_G necesarios están ya definidos.

[233] Igual que se explica en la nota precedente, esto es una definición por recursión transfinita sobre el rango de un conjunto en la jerarquía de von Neumann: si está definido "ser un C-nombre para todo conjunto de rango menor que el de b, entonces definimos así que b sea un C-nombre.

Para probar que $G \in M[G]$ consideramos el nombre $\Gamma = \{(\check{p}, p) \mid p \in C\}$. Así, $G = \Gamma_G \in M[G]$, porque al calcular Γ_G sólo consideramos los pares $(\check{p}, p)$ con $p \in G$, y así nos quedamos sólo con los p tales que $p \in G$.

A continuación Shoenfield define el *lenguaje del forcing,* que no es más que el lenguaje de ZFC admitiendo a los elementos de M (hoy diríamos los de M^C) como constantes. En realidad, no hace falta definir lenguaje alguno, pues podemos trabajar sin más con fórmulas del lenguaje de ZFC. Ahora define (para $x_1, \ldots, x_n \in M$, aunque podríamos tomarlos en M^C):

$$p \Vdash \phi(x_1, \ldots, x_n)$$

si y sólo si cuando G es un filtro C-genérico sobre M tal que $p \in G$, se cumple $M[G] \vDash \phi[(x_1)_G, \ldots, (x_n)_G]$.

En definitiva: p fuerza una fórmula ϕ si ϕ se cumple en todo modelo $M[G]$ calculado con un filtro G respecto al cual p es verdadera (sustituyendo cada conjunto x_i por el conjunto que nombra).

"Alguien que viva en M" no puede calcular esta relación $p \Vdash \phi$, porque requiere usar el filtro genérico G, que no está a su alcance, pero a continuación Shoenfield define una relación

$$p \Vdash^* \phi(x_1, \ldots, x_n)$$

para conjuntos cualesquiera $x_1, \ldots, x_n$ (aunque podemos exigir que $x_1, \ldots, x_n \in V^{\mathbb{C}}$), sin mencionar filtros genéricos, simplemente en términos de condiciones y nombres, y se demuestra que si $x_1, \ldots, x_n \in M$ (o $\in M^C$), la relación $p \Vdash \phi(x_1, \ldots, x_n)$ es equivalente[234] a que "alguien que viva en M" vea que se cumple $p \Vdash^* \phi(x_1, \ldots, x_n)$. Esto significa que la relación $p \Vdash \phi$, pese a las apariencias, sí que se puede calcular desde M. Aunque G no esté accesible en M, "alguien que viva en M" puede hacer razonamientos del tipo: si me aseguran que p es verdadera, puedo asegurar que los objetos nombrados por $x_1, \ldots, x_n$ cumplirán ϕ en $M[G]$.

Por ejemplo, si $b = \{(\varnothing, p)\}$, podemos asegurar que $p \Vdash \varnothing \in b$. No necesitamos conocer G para asegurar que, si $p \in G$, entonces $\varnothing_G = \varnothing \in b_G = \{\varnothing\}$, sino que basta analizar los nombres involucrados. El hecho es que esto es posible, al menos en teoría, en cualquier caso, y no sólo en casos tan simples como éste.

A continuación Shoenfield demuestra que $M[G]$ es un modelo transitivo numerable de ZFC.

Observación 2 Ahora pueden verse las ideas que quedan ocultas en el planteamiento "axiomático" del *forcing* que presentaba Shoenfield en su libro de lógica. La relación $p \Vdash \phi(x_1, \ldots, x_n)$ que definía allí es la misma que la relación $p \Vdash^* \neg\neg\phi(x_1, \ldots, x_n)$ que define aquí, considerando conjuntos cualesquiera como nombres en el mismo sentido que aquí, es decir, teniendo en cuenta únicamente los pares que contiene un conjunto b de la forma (a, p), donde $p \in C$ para decidir qué elementos debe tener b_G, sólo que allí nunca se llega a definir b_G. ∎

Luego Shoenfield muestra varias aplicaciones conocidas del *forcing,* pero formuladas según su planteamiento. Por ejemplo, si C_1 y C_2 son conjuntos parcialmente ordenados, considera en el producto $C_1 \times C_2$ la relación de orden dada por

$$(p_1, p_2) \leq (q_1, q_2) \quad \text{si y sólo si} \quad p_1 \leq q_1 \wedge p_2 \leq q_2,$$

y demuestra que una extensión genérica $M[G]$ respecto a $C_1 \times C_2$ se descompone como $M[G] = M[G_1][G_2]$, donde G_1 es C_1-genérico sobre M y G_2 es C_2-genérico sobre $M[G_1]$ (y, recíprocamente, una cadena de extensiones se puede expresar como una única extensión respecto del producto).

Shoenfield construye modelos en los que no se cumple el axioma de elección por un procedimiento similar al empleado por Cohen, pero con algunas ideas esencialmente distintas. A título ilustrativo vamos a ver cómo se traduce al planteamiento de Shoenfield el argumento de Cohen que hemos analizado en la página 269.

La independencia del axioma de elección Consideramos el conjunto de condiciones P formado por las funciones $p : D \longrightarrow 2$ definidas en un subconjunto finito $E \subset \omega \times \omega$. Si partimos de un modelo transitivo numerable M y G es un filtro P-genérico sobre M, en $M[G]$ tenemos la función genérica $f_G = \bigcup G : \omega \times \omega \longrightarrow 2$, que a su vez define los conjuntos genéricos $a_n = \{m \in \omega \mid f(n, m) = 1\}$.

Como $G \in M[G]$, también f_G, así como cada a_n, está en $M[G]$. De hecho, un P-nombre para a_n es

$$\tau_n = \{(\check{m}, p) \mid p \in P \wedge p(n, m) = 1\},$$

y un nombre para $A = \{a_n \mid n \in \omega\}$ es

$$\rho = \{(\tau_n, 1) \mid n \in \omega\}.$$

[234] En realidad $p \Vdash^* \phi$ es la relación fuerte, de modo que Shoenfield demuestra que $p \Vdash \phi$ equivale a la versión débil $p \Vdash^* \neg\neg\phi$. Hoy en día se sabe cómo definir directamente la versión débil.

Sea H el grupo de todas las permutaciones de ω, es decir, de todas las biyecciones $\pi : \omega \longrightarrow \omega$ (podríamos tomar, como Cohen, el subgrupo de las biyecciones que fijan a todos los números naturales salvo un número finito de ellos, pero esto no afecta a la construcción que vamos a hacer).

Para cada $\pi \in H$ y cada condición $p \in P$, consideramos la condición $\bar{\pi}(p)$ que cumple

$$\bar{\pi}(p)(n,m) = p(\pi^{-1}(n), m),$$

es decir, que $\bar{\pi}(p)$ está definida sobre un par (n,m) si y sólo si p está definida en $(\pi^{-1}(n), m)$, y entonces se cumple la igualdad anterior, que equivale a

$$\bar{\pi}(p)(\pi(n), m) = p(n,m),$$

Es fácil ver que así $\bar{\pi} : P \longrightarrow P$ es un *automorfismo* de P, es decir, una biyección que conserva la relación de orden.

A su vez, π induce, por recurrencia, una biyección $\pi^* : M^P \longrightarrow M^P$ en el conjunto de los P-nombres, dada por

$$\pi^*(\tau) = \{(\pi^*(\sigma), \bar{\pi}(p)) \mid (\sigma, p) \in \tau\}.$$

(Cada P-nombre τ es un conjunto de pares (σ, p), donde σ es un P-nombre y $p \in P$, y lo que hace π^* es transformar cada uno de estos pares aplicando el propio π^* a la primera componente y $\bar{\pi}$ a la segunda, con lo que obtenemos otro P-nombre.)

Por ejemplo, es fácil ver que si $x \in M$, entonces $\pi^*(\check{x}) = x$, mientras que:

$$\pi^*(\tau_n) = \{(\check{m}, \bar{\pi}(p)) \mid p \in P \wedge p(n,m) = 1\} = \{(\check{m}, \bar{\pi}(p)) \mid p \in P \wedge \bar{\pi}(p)(\pi(n), m) = 1\}$$

$$= \{(\check{m}, q) \mid q \in P \wedge q(\pi(n), m) = 1\} = \tau_{\pi(n)}.$$

A su vez:

$$\pi(\rho) = \{(\pi^*(\tau_n), 1) \mid n \in \omega\} = \{(\tau_{\pi(n)}, 1) \mid n \in \omega\} = \rho.$$

Un P-nombre τ es *simétrico* si existe un subconjunto finito $A \subset \omega$ tal que toda permutación π que fija a cada elemento de A cumple también $\pi^*(\tau) = \tau$. Por recurrencia se puede definir el conjunto HSM^P de los P-nombres *hereditariamente simétricos,* que son los P-nombres τ simétricos tales que, para todo par $(\sigma, p) \in \tau$, se cumple que σ es hereditariamente simétrico.

Por ejemplo, para cada $x \in M$, el nombre $\check{x}$ es simétrico, pues lo fija cualquier permutación, y esto hace que, de hecho, sea hereditariamente simétrico. A su vez, el nombre τ_n es simétricos, porque lo fijan todas las permutaciones que cumplen $\pi(n) = n$, y, como sus elementos son de la forma $(\check{m}, p)$, y los nombres $\check{m}$ son hereditariamente simétricos, resulta que cada τ_n es hereditariamente simétrico. Y esto, a su vez, implica que ρ es hereditariamente simétrico, pues es simétrico (lo fijan todas las permutaciones) y sus elementos contienen nombres τ_n hereditariamente simétricos.

Definimos $SM[G] = \{K_G(\tau) \mid \tau \in HSM^P\}$, es decir $SM[G]$ es el subconjunto de $M[G]$ formado por los conjuntos que admiten un nombre hereditariamente simétrico. Según hemos visto, $M \subset SM[G] \subset M[G]$ y todos los conjuntos genéricos a_n están en $SM[G]$, al igual que el conjunto $A = K_G(\rho)$ formado por todos ellos.

El caso es que se puede demostrar que $SM[G]$ es un modelo transitivo numerable de ZF, pero no cumple necesariamente el axioma de elección, y también se puede definir un "*forcin simétrico*" que cumpla las mismas propiedades que el usual, pero con $SM[G]$ en lugar de $M[G]$. Además,

$$p \Vdash \phi(\sigma_1, \ldots, \sigma_n) \leftrightarrow \bar{\pi}(p) \Vdash \phi(\pi^*(\sigma_1), \ldots, \pi^*(\sigma_n)).$$

Y ahora ya podemos demostrar que en $SM[G]$ el conjunto A es infinito, pero no tiene subconjuntos numerables. En efecto, si suponemos que existe en $SM[G]$ una aplicación $f : \omega \longrightarrow A$ inyectiva, podemos expresar $f = \tau_G$, para cierto nombre τ *hereditariamente simétrico,* y existirá una condición $p \in G$ tal que

$$p \Vdash \tau : \omega \longrightarrow V.$$

El hecho de que τ sea hereditariamente simétrico se traduce en que existe un número natural n suficientemente grande tal que toda permutación que fije a los números menores que n cumple $\pi^*(\tau) = \tau$. A partir de este punto ya podemos seguir casi literalmente (la parte final de) el argumento de Cohen que hemos visto en la página 269.

∎

En la observación de la página 157 señalábamos que la consistencia del axioma de elección no se demuestra construyendo modelos con conjuntos "raros" que sólo pueden ser obtenidos con el axioma, sino eliminando todos los conjuntos "raros" para que siempre haya un criterio de elección. Recíprocamente, un modelo en el que no se cumpla el axioma de elección no se construye eliminando conjuntos "raros" cuya existencia depende de dicho axioma, sino introduciendo unos conjuntos genéricos "raros" a_n no constructibles (luego no definibles ni siquiera mediante un proceso bastante "generoso", pues involucra ordinales arbitrarios) y eliminando los conjuntos poco simétricos, que podrían distinguir unos a_n de otros, lo cual es necesario, por ejemplo, para construir una función de elección en $\mathcal{P}A$.

En conclusión, este trabajo de Shoenfield contiene ya, salvo detalles mínimos, el concepto de *forcing* como se entiende hoy en día: el *forcing* consiste en partir de un modelo transitivo numerable M de ZFC, fijar en él un conjunto parcialmente ordenado C, fijar un filtro C-genérico sobre M y con él construir una extensión genérica $M[G]$. La relación $\Vdash$, drásticamente simplificada por Shoenfield, es esencial para el estudio de $M[G]$. De hecho, un nombre alternativo a *forcing* mucho más descriptivo para hacer referencia a la teoría podría ser el de *teoría de extensiones genéricas.* ∎

2. Problemas no resueltos en la teoría de conjuntos (Erdős, Hajnal) El húngaro Pál Erdős, más conocido como Paul Erdős, era uno de los matemáticos más excéntricos y más prolíficos de todos los tiempos. Llegó a publicar unos 1 500 artículos a lo largo de su vida, una cifra nunca igualada. Entre otros muchos temas, se ocupó de lo que se conoce como *cálculo de particiones.* La teoría se remonta a un artículo de Frank Plumpton Ramsey titulado *Sobre un problema de la lógica formal*, que fue publicado[235] en 1930. El artículo estaba dedicado a demostrar que cierta clase de sentencias es decidible (es decir, que existe un procedimiento para determinar si una sentencia de ese tipo es verdadera o falsa), pero para ello establecía antes unos teoremas que consideró que tenían interés en sí mismos y, en efecto, son lo que hoy se conoce como *teorema de Ramsey* en la teoría de grafos finitos, junto con una versión para conjuntos infinitos. La versión finita dice así:

> **Teorema de Ramsey** Para cada natural m existe un número natural n de modo que todo grafo con al menos n vértices posee m vértices conectados dos a dos, o bien m vértices desconectados dos a dos.

Por ejemplo, de entre 6 personas elegidas al azar, siempre hay 3 que se conocen dos a dos o bien 3 que no se conocen dos a dos. La versión infinita afirma que, de entre $\aleph_0$ personas elegidas al azar, siempre hay $\aleph_0$ que se conocen dos a dos, o bien $\aleph_0$ que no se conocen dos a dos.

Estos resultados admiten generalizaciones (de hecho, Ramsey formuló versiones más generales que las que hemos dado), y también hay resultados negativos que muestran que ciertas variantes no pueden darse. Por ejemplo, en 1933 Sierpiński demostro que, de entre $\aleph_1$ personas elegidas al azar, no tiene por qué haber $\aleph_1$ que se conozcan dos a dos ni $\aleph_1$ que no se conozcan dos a dos.[236]

El estudio de este tipo de problemas fue sistematizado en un artículo de 1956 titulado *Un cálculo de particiones en la teoría de conjuntos,* escrito por Erdős junto con Richard Rado (otro de los muchos judíos que huyeron de Alemania en cuanto Hitler llegó al poder). La ponencia de Erdős y Hajnal discutía 82 problemas abiertos del cálculo de particiones.

Aprovechamos para comentar que algunas relaciones del cálculo de particiones definen cardinales grandes. Por ejemplo, en 1961 Erdős y Tarski publicaron *Sobre ciertos problemas que involucran cardinales inaccesibles,* donde estudiaron los cardinales κ que cumplen el teorema de Ramsey, es decir, que de entre κ personas elegidas al azar, siempre hay κ que se conocen dos a dos o κ que no se conocen dos a dos. Los cardinales no numerables con esta propiedad se llamarían más adelante *débilmente compactos,* porque Tarski los caracterizó como los que hacen que ciertos lenguajes con fórmulas infinitas satisfacen el teorema de compacidad de Gödel. El caso es que si κ es débilmente compacto, entonces es fuertemente inaccesible[237] y hay κ cardinales fuertemente inaccesibles menores que él.

En 1962 Erdős y Hajnal introdujeron los que hoy se conocen como *cardinales de Ramsey.* Sucede que si κ es un cardinal medible, es de Ramsey y tiene por debajo κ cardinales de Ramsey, y a su vez todo cardinal de Ramsey de débilmente compacto.

[235] Póstumamente, pues Ramsey murió de ictericia a principios de año antes de cumplir los 27 años.

[236] Más en general, de entre 2^κ personas elegidas al azar, no tiene por qué haber κ^+ que se conozcan dos a dos ni κ^+ que no se conozcan dos a dos.

[237] Erdős y Tarski demostraron que un cardinal fuertemente inaccesible es débilmente compacto si y sólo si cumple el teorema de Kőnig para árboles: todo árbol de altura κ con niveles de cardinal $< \kappa$ tiene al menos una rama de cardinal κ.

En 1966 se había doctorado Jack Howard Silver bajo la dirección de Vaught, con la tesis titulada *Algunas aplicaciones de la teoría de modelos a la teoría de conjuntos.* En ella mostraba el impacto que la existencia de un cardinal de Ramsey tenía sobre la clase L de los conjuntos constructibles (Haim Gaifman, que se había doctorado en 1962 bajo la dirección de Tarski, había obtenido parte de estos resultados a partir de la existencia de un cardinal medible).

Entre otras cosas, Gaifman y Silver habían demostrado que todo conjunto que pueda definir "alguien que viva en L" es necesariamente finito o numerable. Por ejemplo, lo que "alguien que viva en L" llama $\aleph_{25}$ es un ordinal numerable, lo que "alguien que viva en L" llama "el primer cardinal inaccesible" (si es que existe, o el quinto, si existe) es un ordinal numerable, etc.

Recíprocamente, cualquier conjunto no numerable que esté en L, como $\aleph_1$ es "a ojos de alguien que viva en L" un cardinal, pero uno entre muchos, sin ninguna característica que permita distinguirlo de cualquier otro: no es ni el menor cardinal no numerable, ni $2^{\aleph_0}$, ni nada que lo identifique.

Más aún, es posible definir una fórmula $L \vDash \alpha[v]$ que determine si una fórmula α del lenguaje de la teoría de conjuntos es satisfecha o no en L (lo que el teorema de Tarski dice que es imposible hacer con V). ∎

3. La consistencia de la HCG con la existencia de un cardinal medible (Silver) Si κ es un cardinal inaccesible, sigue siendo inaccesible "a ojos de alguien que viva en L", lo que implica que, si es consistente que existan tales cardinales, también lo es que existan y se cumpla la hipótesis del continuo generalizada. Lo mismo vale para otros cardinales grandes, como los cardinales débilmente compactos. En cambio, Scott había demostrado que si κ es un cardinal medible, entonces $V \neq L$, por lo que ya no es posible asegurar que la existencia de un cardinal medible sea consistente con la hipótesis del continuo generalizada. Esto es precisamente lo que demostraba Silver:

> **Teorema (Silver)** Si κ es un cardinal medible y D es una medida normal[238] en κ, entonces κ sigue siendo un cardinal medible en el modelo[239] $L[D]$, y en éste se cumple la hipótesis del continuo generalizada.

Así pues, si es consistente que existan cardinales medibles, es consistente suponer además la hipótesis del continuo generalizada. En particular, la existencia de cardinales medibles implica la existencia de conjuntos no constructibles, pero implica que tenga que fallar la hipótesis del continuo.

Silver hace referencia a otra prueba del mismo resultado, pero obtenida mediante *forcing,* que Ronald Björnr Jensen presentó también en el congreso con el título de *Cardinales medibles y la* HCG.

Ese año de **1967** Silver dio un curso titulado *Forcing a la Solovay,* en el que mostraba cómo construir extensiones genéricas $M[G]$ a partir de cualquier conjunto parcialmente ordenado como conjunto de condiciones, aunque seguía basándose en un lenguaje ramificado para construir la extensión. Los apuntes del curso circularon ampliamente, a la par que las notas de Solovay y Scott sobre *forcing* con álgebras de Boole. Silver dice:

> *El marco general más simple para construir modelos de Cohen de* ZF *se obtiene considerando estructuras parcialmente ordenadas. Este enfoque, una generalización directa del trabajo original de Cohen, se debe a Solovay. Es más simple para fines elementales que el enfoque mediante álgebras de Boole completas de Solovay y Scott y proporcionará una transición hacia este enfoque más profundo.* ∎

4. Cardinales $\mathbb{R}$-medibles (Solovay) Recordemos (página 90) que Ulam había demostrado que puede haber dos tipos sustancialmente distintos de cardinales $\mathbb{R}$-medibles κ. Por una parte puede ocurrir que κ sea medible (página 241), en cuyo caso es fuertemente inaccesible, y por otra parte puede ser $\kappa \leq 2^{\aleph_0}$, y entonces es débilmente inaccesible y la medida de Lebesgue se extiende a una medida κ-aditiva en $\mathcal{P}[0,1]$. En esta ponencia, Solovay demuestra que las dos posibilidades son equiconsistentes, es decir:

> **Teorema (Solovay)** Si una de las dos teorías siguientes es consistente, también lo es la otra:[240]
>
> 1. ZFC + "existe un cardinal medible".
> 2. ZFC + "la medida de Lebesgue se extiende a $\mathcal{P}[0,1]$".

[238] Véase la página 244.
[239] Véase la página 247.
[240] Como Shoenfield, Solovay llama ZFC a ZF más el axioma de elección, pero tiene que aclarar en una nota al pie el significado de estas siglas.

Si suponemos que la medida de Lebesgue se extiende a $\mathcal{P}[0,1]$, tomamos el mínimo cardinal $\kappa \leq 2^{\aleph_0}$ tal que existe una medida no trivial en $\mathcal{P}\kappa$ (que es un cardinal débilmente inaccesible, según probó Ulam[241]). Llamamos J al ideal de κ formado por los conjuntos de medida 0. Solovay, aprovechando el trabajo de Silver que acabamos de comentar, demuestra que en el modelo $L[J]$, el cardinal κ deja de ser $\leq 2^{\aleph_0}$ y pasa a ser medible.

Recíprocamente, partiendo de un modelo M en el que hay un cardinal medible κ, Solovay construye una extensión genérica[242] $M[G]$ donde sigue habiendo una medida no trivial en $\mathcal{P}\kappa$, pero ahora $2^{\aleph_0} = \kappa$, lo cual descarta el primero de los dos casos del teorema de Ulam (porque κ debería tener por debajo un cardinal fuertemente inaccesible μ, y entonces $2^{\aleph_0} < \mu \leq \kappa$), por lo que tiene que darse el segundo. Más aún, con esto Solovay demostraba que, si es consistente que existan cardinales $\mathbb{R}$-medibles, es consistente que $2^{\aleph_0}$ sea $\mathbb{R}$-medible.

Scott había demostrado que los cardinales medibles son increíblemente grandes (véase el final de la sección 89), mientras que los cardinales $\mathbb{R}$-medibles $\leq 2^{\aleph_0}$ son, en comparación, relativamente pequeños. Sin embargo, Solovay había demostrado que, en cuanto a consistencia son equivalentes, y que un cardinal $\mathbb{R}$-medible $\kappa \leq 2^{\aleph_0}$ será visto como medible sin más que restringir adecuadamente la noción de "conjunto". ∎

5. Sobre modelos de la teoría de conjuntos sin AE (Jech) Tomáš Jech se había doctorado en 1966 bajo la dirección de Vopěnka con una tesis titulada *El axioma de elección.* Su ponencia muestra cómo construir modelos ∇ (el análogo desarrollado por Vopěnka de los modelos booleanos de Solovay) en los que falla el axioma de elección.

Ese mismo año de **1967** Jech había publicado el artículo *La indemostrabilidad de la hipótesis de Suslin,* en el que demostraba, precisamente con un modelo ∇, la consistencia de que exista un árbol de Suslin (Tennenbaum publicaría su demostración en **1968**, en un artículo breve titulado *El problema de Suslin.*) Ese mismo año Jech publicó el artículo ω_1 *puede ser medible,* donde, partiendo de un modelo M en el que existe un cardinal medible κ, pasaba a una extensión genérica $M[G]$ en el que κ pasaba a ser $\aleph_1$ (porque todos los cardinales anteriores se vuelven numerables), y luego construye una extensión simétrica $SM[G]$ en la que $\aleph_1$ sigue siendo medible. (En realidad Jech no construye ninguna extensión, porque trabaja con modelos booleanos, pero lo que hace es equivalente a lo dicho.) Esto prueba la mitad del teorema siguiente:

> **Teorema** La consistencia de ZFC + "existe un cardinal medible" es equivalente a la consistencia de ZF + "$\aleph_1$ es un cardinal medible".

La otra mitad se debe a que si U es un ultrafiltro no principal $\aleph_1$-completo en ω_1, entonces $L[U]$ es un modelo de ZFC en el que $\kappa = \aleph_1$ ya no es $\aleph_1$, sino que es un cardinal medible.

Más aún, también en **1968**, Solovay demostró que el axioma de determinación implica que $\aleph_1$ es un cardinal medible. Esto implica que es imposible demostrar la consistencia del axioma de determinación sin suponer, al menos, la consistencia de que exista un cardinal medible, que es algo mucho más fuerte que la mera consistencia de ZFC. ∎

Destacamos brevemente algunos resultados adicionales presentados en el congreso:

- Scott y John Myhill (que se había doctorado en 1949 bajo la dirección de Quine) desarrollaron una teoría que Gödel había esbozado en 1964 sobre la clase de los conjuntos *hereditariamente definibles con ordinales,* que es un modelo más sencillo que L y que permite demostrar igualmente la consistencia del axioma de elección (pero no la de la hipótesis del continuo).

- Mycielski presentó una ponencia breve sobre el Axioma de Determinación.

[241] Este cardinal, aun siendo débilmente inaccesible, es relativamente pequeño, en cuanto que es $\leq 2^{\aleph_0}$, pero Solovay demuestra que la consistencia de que exista un cardinal así es equivalente a la de que exista un cardinal medible, que sí que es un cardinal increíblemente grande.

[242] En realidad Solovay no considera ningún modelo M ni ninguna extensión, sino que, remitiendo a sus notas inéditas con Scott sobre *forcing* con modelos booleanos (véase la página 275), considera una cierta álgebra de Boole completa $\mathcal{B}$ y razona que, en $V^{\mathcal{B}}$, se cumple $[\![2^{\aleph_0} = \check{\kappa} \wedge$ hay una medida en $\mathcal{P}\check{\kappa}]\!] = 1$, pero esto significa que, si tomamos dicha álgebra en un modelo M, este hecho se cumplirá en cualquier extensión genérica $M[G]$.

- Mac Lane discute los problemas de formalización en la teoría de conjuntos de la teoría de categorías. Entre otras cosas, comenta una propuesta de Grothendieck de suponer la existencia de infinitos "universos", cada uno incluido en el siguiente, de modo que las categorías de un universo (o que relacionan dos universos) pueden ser estudiadas desde un universo superior. La forma más sencilla de llevar esto a la práctica es suponer la existencia de infinitos cardinales fuertemente inaccesibles y tomar como universos los conjuntos V_κ correspondientes.

6. Observaciones sobre las discusiones populares sobre fundamentos (Kreisel) Georg Kreisel, de familia judía, fue enviado a Gran Bretaña por sus padres a los 15 años, cuando la anexión de Austria a la Alemania nazi. Nunca se doctoró, pero, a sus 44 años, era ya una autoridad en la teoría de la demostración. La introducción de su ponencia empieza así:

> *Los lógicos matemáticos suelen afirmar que prefieren demostrar teoremas complejos en lugar de formular cuidadosamente distinciones y puntos de vista filosóficos. Naturalmente, no se puede esperar demasiado de ellos cuando publican sobre cuestiones filosóficas, sobre fundamentos. Igualmente natural es que, al no estar acostumbrados a la disciplina del análisis de los fundamentos, al ver una discusión detallada sobre fundamentos como* [dos referencias a artículos "filosóficos" de Gödel]*, la leen con menos atención que los argumentos matemáticos (lo que corresponde,* mutatis mutandis*, a los filósofos anticuados, que están convencidos de comprender los resultados de la lógica matemática sin prestar mucha atención a las formulaciones ni a las demostraciones). El objetivo de esta nota es seleccionar algunas observaciones y distinciones sencillas sobre los fundamentos que proporcionen cierta orientación sobre el progreso en los fundamentos sin, espero, agotar la paciencia del lector.* [...]
>
> *Un componente central del pensamiento popular actual es la concepción formalista de las matemáticas en diversas formas. En su forma más extrema, rechaza todos los problemas de fundamentos (y, por lo tanto, la distinción entre fundamentación y organización). Otra versión, quizás más común, no rechaza estos problemas, sino que simplemente asume que una fundamentación debe consistir en una reducción formalista; por lo tanto, el fracaso de dicha reducción se interpreta como una dificultad para los fundamentos, sin más.*

Así pues, Kreisel se dispone a analizar lo que podríamos llamar el "formalismo mal entendido" o "formalismo radical" que adoptan muchos matemáticos y que llega incluso a incapacitarlos para entender la fundamentación de la matemática. Tras recordar los grandes progresos que se han logrado en los últimos cincuenta años, dice:

> *Insistir en el hecho objetivo del progreso en las fundaciones no es sólo una cuestión de honor tribal. Al contrario, las discusiones fundacionales que no tienen en cuenta este progreso son inútiles; objetivamente, cuando retoman cuestiones obsoletas* (como nuevas propuestas para la cuadratura del círculo) y subjetivamente, por una de las dos reacciones comunes siguientes: una es sentirse apesadumbrado porque se siente que no hay nada sobre lo que construir; la otra es sentirse mareado, porque se siente que "todo vale", ya que, proponga uno lo que proponga, no puede ser peor que nada. De hecho, la impresión de que no ha habido progreso puede llevar a inventar doctrinas negativas como el positivismo para explicarla.***
>
> (*) *Por ejemplo, el artículo "Formalismo-64" de A. Robinson o el artículo de Cohen (en este volumen), que, como señala Cohen, fue influido por el de Robinson. Se supone que el número "64" se refiere a 1964, pero el artículo bien podría haber sido escrito en 1864, ya que presenta simplemente una versión rudimentaria del formalismo. No tiene en cuenta la crítica clásica de Frege a ese tipo de formalismo, ni, peor aún, los estudios masivos del único intento genuino de desarrollar el formalismo, a saber, el programa de Hilbert, ni siquiera su análisis de las condiciones de adecuación. Por lo tanto, no sólo no aporta nada a nuestro conocimiento, sino que no tiene en cuenta los resultados existentes. Presumiblemente, tanto el artículo de Robinson como el de Cohen reflejan bastante bien la opinión de mucha gente. (Como señala Cohen, las opiniones de estos artículos no son consistentes en detalle).*
>
> (**) *Existen, por supuesto, algunas razones secundarias para esta impresión.* [...] *Otra es que hay quienes simplemente buscan una razón para no preocuparse por los fundamentos. ¿Para qué molestarse en encontrar una razón? ¿Acaso es para convencerse a uno mismo (o a los demás) de que no se pierde nada concentrándose en el propio trabajo? Esto parece demasiado suponer. ¿Acaso es para seguir —inconscientemente, por supuesto— al Dr. Jowett de Oxford? (No es conocimiento si yo no lo conozco).*[243]

[243] Alude a un poema satírico compuesto por alumnos de Oxford sobre la arrogancia del profesor Benjamin Jowett: First come I, my name is Jowett. / There's no knowledge but I know it. / I am Master of this College; / What I don't know isn't knowledge.

Por ejemplo —a propósito de la nota (∗)— muchos matemáticos que se declaran formalistas y ven a Hilbert como un ideal, parecen ignorar que lo primero que tenía claro Hilbert es que no toda la matemática puede reducirse a puro formalismo, sino que el formalismo debe sustentarse en una matemática intuitiva informal, más amplia incluso que lo que Hilbert había previsto en un principio, pero que no dudó en admitir en cuanto los teoremas de incompletitud mostraron la necesidad de hacerlo. En palabras de Kreisel:

> **Formalismo: un obstáculo para reconocer el progreso cuando se observa.** *En primer lugar, no olvidemos el aspecto positivo de los fundamentos formalistas, a saber, el notable descubrimiento de que gran parte de las matemáticas que no se presentan como un "juego formal con símbolos" permiten, sin embargo, una base formalista adecuada en el sentido del programa de Hilbert.*

Y lo peor es que el formalismo mal entendido impide —como decíamos— entender la fundamentación de la matemática:

> *El lado negativo del formalismo, ya mencionado en la introducción, es el requisito de que unos fundamentos, para merecer tal nombre, deben ser una reducción formalista. Si se acepta este requisito, la impresión popular de que ha habido poco progreso en fundamentos es sin duda correcta, ya que toda la evidencia demuestra que ¡no es posible una fundamentación formalista!*
>
> *Pero un efecto mucho más trascendental de aceptar este requisito es el siguiente: se vuelve realmente difícil apreciar el trabajo en los fundamentos, ya que la restricción formalista afecta a la idea misma de precisión. Una noción será rechazada por ser "imprecisa" no sólo cuando sea realmente vaga (y, por lo tanto, deba ser rechazada o al menos analizada), sino simplemente porque no encaja en el proyecto formalista.*

Como diría unos años más tarde Raymond Smullyan: *Un formalista es alguien que no es capaz de entender algo a menos que carezca de significado,* y eso es un lastre muy difícil de arrastrar. Un formalista radical considera que cualquier razonamiento que no sea un caso particular de reglas dadas de antemano, o aplicación de unos principios generales establecidos de antemano no es riguroso, sin entender que la fundamentación de la matemática trata de llegar a principios fundamentales y reglas de razonamiento para las matemáticas, no partir de ellas. Eso es imposible:

> *Pero dado que este proyecto ha fracasado, el progreso posterior utilizará nociones y métodos ajenos a él; de hecho, las principales preguntas fructíferas ni siquiera tienen por qué ser formulables en términos aceptados en este proyecto. Por lo tanto, al aceptar el proyecto formalista, uno no sólo no está dispuesto a apreciar (¡o estudiar!) trabajos más avanzados sobre fundamentos, sino que simplemente no puede hacerlo sin reexaminar sus propias ideas.*

Reexaminarlas hasta entender que existe un conocimiento intuitivo informal que puede proporcionar un conocimiento sólido, no sobre cardinales infinitos ni ultrafiltros ni cosas así, pero sí sobre una parte de las matemáticas mucho más extensa que los razonamientos elementales sobre marcas en un papel, como Hilbert pretendía en un principio. Por ejemplo, una teoría de modelos metamatemática requiere convencerse de que es posible hablar intuitivamente con seguridad de conjuntos siempre y cuando se satisfagan ciertas restricciones de naturaleza muy diferente de las que determinan cuándo un razonamiento formal es riguroso:[244]

> *El atractivo del formalismo, en particular para los matemáticos, no es casual. En cierto sentido, pretende proporcionar una razón teórica para no preocuparse por los fundamentos.* [...] *En particular, si bien Hilbert creía que eliminaría las nociones y métodos que resultan problemáticos, la investigación ha demostrado la necesidad de estas nociones. Es necesario analizarlas y estudiarlas. Cabe destacar que, en teoría, este cambio constituye un avance muy real: uno podría haber sospechado la conclusión, pero, antes del teorema de incompletitud de Gödel, no existía un análisis preciso de su propósito.*

[244] Por ejemplo, en una teoría axiomática formal del estilo de ZFC, uno puede usar "para todo" y "existe" con total libertad, siempre que respete las leyes lógicas correspondientes, mientras que, en un razonamiento intuitivo sobre conjuntos, no podemos decir "para todo subconjunto de $\mathbb{N}$" sin más precaución (pues así pretendemos recorrer una clase de objetos que escapa a nuestra intuición), salvo que lo que venga después del "para todo" pueda concebirse como un esquema argumento que proporcione un argumento concreto cada vez que se aplica a cualquier conjunto que nos podamos encontrar. Sin embargo, las sutilezas de este tipo suelen pasar desapercibidas a los formalistas que pretenden examinar críticamente el razonamiento metamatemático y, en cambio, cuestionan otros argumentos que nadie juzgaría dudosos si no fuera por comparación irreflexiva con unos criterios de trabajo formalistas que están fuera de lugar.

Se refiere a las nociones intuitivas y a las formas de razonamiento intuitivo, que en un principio nadie se había molestado en analizar porque se consideraba que el razonamiento intuitivo era sólo una forma "de andar por casa" de entenderse uno consigo mismo, pero que al final, cualquier razonamiento serio, tenía que exponerse formalmente. Pero el matemático convencido de que apoyarse oficialmente en la matemática intuitiva es prostituir el razonamiento matemático dirigirá todos sus esfuerzos a tratar de prescindir totalmente de la intuición o, cuanto menos, si se resigna a que algo de intuición va a necesitar, a reducir su uso al mínimo, sin entender que el camino exitoso no es ése, sino el de estudiar y analizar el razonamiento intuitivo para determinar cuál es el máximo uso, no el mínimo, que puede hacerse de él de forma rigurosa y confiable.

Estos párrafos pueden verse como un análisis psicológico de por qué el matemático formalista se siente incómodo con el razonamiento metamatemático, aunque hay razones de peso mucho más profundas:

> **Organización y fundamentos: una distinción.** *Obviamente, la diferencia más notable es la siguiente: Los fundamentos se ocupan de la validez, constructiva o no constructiva, de los principios matemáticos; en la práctica matemática, rara vez se examinan los principios a menos que se esté convencido de su validez, y el principal interés es hacerlos eficientes. Dicho de otro modo, los fundamentos proporcionan razones para los axiomas, la práctica matemática se ocupa de las deducciones a partir de los axiomas, y la organización de la práctica matemática pretende que estas deducciones sean tan inteligibles como sea posible. Algunas consecuencias prácticas saltan a la vista.*
>
> *Para los fundamentos, es importante saber de qué estamos hablando; hacemos que el tema sea lo más específico posible. De esta manera, tenemos la oportunidad de hacer afirmaciones sólidas. En la práctica matemática, para que una demostración sea inteligible, queremos eliminar todas las propiedades que no sean relevantes para el resultado demostrado; en otras palabras, hacemos que el tema sea menos específico.*
>
> *Los fundamentos proporcionan un análisis de la práctica matemática. Para merecer este nombre, se espera que los fundamentos introduzcan nociones que no se dan en la práctica matemática. Así, en los fundamentos de la teoría de conjuntos, los tipos de conjuntos se tratan explícitamente, mientras que en la práctica matemática generalmente están ausentes; y en los fundamentos de las matemáticas constructivas, el análisis de las operaciones lógicas requiere demostraciones (intuitivas), mientras que en la práctica matemática las demostraciones no se mencionan explícitamente.*

El problema psicológico de fondo no es tanto la diferencia de objetivos entre la práctica matemática y la metamatemática como el hecho de que varias generaciones de matemáticos fueron educadas irreflexivamente en que los criterios de rigor matemático son los que son, y eran concretamente los que garantizan que el discurso es lo suficientemente preciso como para que su formalización sea una mera cuestión rutinaria de la que uno puede despreocuparse, para lo cual hay que cuidar mucho unos aspectos que en el razonamiento intuitivo son secundarios, mientras que se pueden descuidar todos los aspectos que no van a dar problemas gracias a la protección de la axiomática formal (que, hasta donde sabemos, nos evita cualquier paradoja), pero que en el marco de un razonamiento intuitivo son cuestionables, porque no está claro lo que significan, que es justo lo que en el contexto formal, no supone ningún inconveniente.

Dejamos aquí el artículo de Kreisel, porque luego entra en cuestiones más técnicas y, en cualquier caso, no es más que una descripción superficial de los problemas del "formalismo radical" que tampoco aporta ninguna orientación concreta que pueda ayudar a un formalista radical a salir de su formalismo radical.

7. Comentarios sobre la fundamentación de la teoría de conjuntos (Cohen) Hemos dejado para el final la aportación de Cohen, que no tiene ningún contenido matemático, sino puramente filosófico. La situación de Cohen era peculiar. Tenía entonces 33 años. Había estudiado matemáticas junto con Tennenbaum y luego coincidió con Feferman en el Instituto de Estudios Avanzados de Princeton. Se había doctorado en 1958 con una tesis sobre el problema de la unicidad de los desarrollos en serie trigonométrica, bajo la dirección de Antoni Zygmund, que a su vez se había doctorado en 1923 bajo la dirección de Mazurkiewicz y Rajchman. Era un matemático brillante, pero la lógica no era su especialidad. Estaba al tanto de los avances en gran parte por sus amigos lógicos. Sin embargo, a los 29 años, había tenido una idea revolucionaria cuando nadie pensaba que podría tener éxito, pero los lógicos se la habían quitado de las manos y la habían desarrollado hasta tal punto que todo lo que él estaba en condiciones de añadir se consideraba ya "trivial". Más adelante Cohen declararía que había sentido con cierta amargura el tratamiento que le habían dado algunos lógicos, y que creía que los matemáticos en general no se habrían comportado de una manera tan mezquina como consideraba que lo habían

hecho los lógicos con él. Dijo que a los ojos de varios lógicos sus resultados sobre forcing habían pasado de ser incorrectos a ser extremadamente difíciles de entender, a ser fáciles y, finalmente, a estar ya presentes en la literatura precedente.[245]

Como hemos visto que señalaba Kreisel en el dardo que le lanzaba a Cohen, la posición que Cohen defendió en su ponencia estaba "obsoleta". Vamos a comentar algunos de sus pasajes incidiendo principalmente en esto. Un año antes, en 1966, Cohen se había declarado realista (con reservas) y se decantaba por considerar que la hipótesis del continuo es falsa (véase la página 271). En cambio, ahora, se declaraba formalista, aunque más bien formalista por resignación:

> *A estas alturas, puede que ya sea obvio que he elegido la postura formalista. Esta no es una decisión audaz, ya que probablemente la mayoría de los matemáticos famosos que se han expresado sobre la cuestión han rechazado, de una u otra forma, la postura realista. En mi caso, puedo decir que fue la charla de Abraham Robinson en Jerusalén en 1964 lo que me impulsó a hacer explícita mi elección. Es una elección que conlleva ciertas cargas. Sin duda, una de las más pesadas es la admisión de que la hipótesis del continuo, quizás la primera pregunta significativa sobre conjuntos no numerables que se puede plantear, carece de significado intrínseco. Si el programa de Hilbert no hubiera sido destrozado por Gödel, la vida sería mucho más cómoda. Creo firmemente que el programa de Hilbert no puede ser resucitado en ningún sentido. Siempre existe una gran frustración con las demostraciones de consistencia, y parecen conservar un carácter circular que las hace sumamente insatisfactorias.*

Pensar que Gödel había destrozado el programa de Hilbert y que, con ello, había hecho la vida más difícil a los matemáticos era ya entonces un punto de vista "obsoleto".

Puede decirse que Gödel había destrozado el programa de Hilbert en cuanto a dicho programa aspiraba a demostrar la consistencia de la teoría de conjuntos y, ciertamente, Gödel había demostrado que eso es imposible, pero no es menos cierto que eso puede verse como que Hilbert había sobreestimado la importancia de esa hipotética demostración de consistencia dentro de su programa formalista. Nada impide concebir la matemática exactamente como Hilbert la concebía: como una teoría formal que permite formular tanto afirmaciones que no tienen un significado objetivo definido, como de otras que sí que lo tienen[246] y que la consistencia de dicha teoría formal no necesita demostrarse, sino que es posible desarrollar las matemáticas sin tal prueba de consistencia igual que los físicos teóricos pueden desarrollar la física sin tener una demostración de que sus presupuestos son correctos y que nunca se encontrarán con una experiencia que les obligue a modificarlos.[247] Además, esa parte de la matemática formal que sí que tiene un significado objetivo resulta ser mucho más amplia que lo que Hilbert había imaginado o lo que había juzgado necesario reconocer, y nada impide desarrollar teorías auxiliares que axiomaticen sólo partes significativas de la matemática formal y demuestren su consistencia. La "frustración" de la que habla Cohen es típica del matemático que no acaba de entender esta naturaleza mixta de la teoría matemática. Lo que puso de manifiesto la facilidad con la que ahora podían construirse modelos de ZFC con las propiedades más diversas y contradictorias entre sí es que ZFC no era como una axiomática para la geometría euclídea (que aspira a describir un único modelo), sino una axiomática en el sentido bourbakista de una estructura, como pueda ser la teoría de grupos, o la teoría de anillos. Considerar frustrante que haya muchas estructuras esencialmente distintas que satisfacen los axiomas de la teoría de conjuntos es como si un algebrista considerara frustrante que todos los grupos no fueran isomorfos entre sí. Y buscar unos axiomas para "la teoría de conjuntos verdadera" tiene tan poco sentido como si un algebrista buscara "el grupo verdadero", de modo que cualquier otro grupo no isomorfo a él fuera un "grupo indeseable".

Cohen explica cómo se había convencido de mala gana de la necesidad de abandonar una postura realista:

> *En la filosofía realista se aceptan incondicionalmente las matemáticas tradicionales al pie de la letra. Todas las cuestiones, como la hipótesis del continuo, son verdaderas o falsas en el mundo real, a pesar de su independencia de varios sistemas axiomáticos. La postura realista es probablemente la que la mayoría de los matemáticos preferiría adoptar. No es hasta que se percatan de algunas de las dificultades de la teoría de conjuntos que empiezan a cuestionarla. Si estas dificultades les molestan especialmente, se refugian en el formalismo, mientras que su postura habitual se sitúa en un punto intermedio, intentando disfrutar de lo mejor de ambos mundos.*

[245] Por ejemplo Gerald Enoch Sacks, que se había doctorado en 1961 bajo la dirección de Rosser, en su ponencia dice que el tipo de *forcing* del que iba a hablar (lo que hoy se conoce como *forcing de Sacks*), tenía su origen en el trabajo de Cohen y en un artículo de 1958 de Clifford Spector (doctorado en 1955 bajo la dirección de Kleene y que había muerto de leucemia en 1961, a los 30 años).

[246] Una analogía sería pensar en una novela que mezcla personajes históricos con personajes ficticios.

[247] Esto lo señalaba, por ejemplo, Curry en su *Logica matemática,* de 1963, de donde está tomada la frase con la que empieza este libro.

Ese punto intermedio no tiene nada de incoherente. Es como si un novelista que está escribiendo una novela en la que mezcla personajes históricos con personajes ficticios, a la hora de diseñar su novela, piensa en todos sus personajes como si fueran reales. No sólo es legítimo, sino que es lo natural y lo conveniente. Recordar en cada momento que "Napoleón existió realmente, pero su criado *François* es un invento tuyo" no aporta nada a la elaboración de una trama interesante. Al contrario, para crear una trama "realista" lo que procede es pensar en todos los personajes como si fueran reales, para asegurarse de que todos se comportan como se comportarían si fueran reales. Esto no tiene nada que ver con que, si al novelista le preguntan si *François* existió realmente, no tenga ninguna duda en bajar de sus fantasías y reconocer que no, sin frustración alguna.

> *La principal ventaja del realismo es que no es necesario justificar los axiomas de la teoría de conjuntos. No es necesario demostrar su consistencia y, lo que es igualmente importante para mí, no es necesario explicar por qué estos axiomas en particular son tan exitosos y merecen una atención especial. En consecuencia, la mayor debilidad de la postura formalista reside en explicar por qué los axiomas de la teoría de conjuntos, presumiblemente sin reflejar ninguna realidad subyacente, son capaces de demostrar enunciados aritméticos indemostrables por medios más finitistas.*

Como hemos señalado, tampoco un formalista necesita demostrar la consistencia de los axiomas de la teoría de conjuntos. Simplemente, un formalista trabaja bajo la hipótesis de que esos axiomas descartan cualquier razonamiento contradictorio y, si no fuera así, habría que buscar otros axiomas, pero eso no afectaría a la práctica totalidad de los teoremas conocidos. El trabajo de un matemático es, en este sentido, análogo al de un físico, que supone un marco teórico para explicar la naturaleza, sin descartar que en algún momento necesite cambiarlo por otro.

En cuanto a la segunda parte, los axiomas de la teoría de conjuntos no reflejan ninguna realidad subyacente en su totalidad, pero eso no impide que incluyan afirmaciones que sí que son verdaderas en una realidad subyacente. Los axiomas de ZFC no son intuitivos porque son mucho más amplios que lo que la intuición abarca, pero precisamente por ello incluyen afirmaciones intuitivamente verdaderas. Por ejemplo, es intuitivamente verdadero que existen conjuntos infinitos, por lo que el axioma de infinitud es intuitivamente verdadero. Lo que ocurre es que, en cuanto se acepta este axioma, el axioma de partes deja de ser intuitivamente verdadero, porque ahora afirma que existe un conjunto que incluye a la totalidad de los subconjuntos de $\mathbb{N}$, cosa que no tiene ningún fundamento intuitivo, pero, a la vez, no contradice a ningún hecho intuitivamente verdadero. No podemos decir que es intuitivamente falso que exista un conjunto no numerable, sino más bien que nuestra intuición no nos proporciona ningún ejemplo de tal cosa, y por ello no podemos permitirnos el lujo de hablar intuitivamente de conjuntos no numerables, porque no podemos hablar intuitivamente de algo de lo que no tenemos ninguna representación intuitiva precisa, a riesgo de caer en contradicciones. Pero el hecho de que ZFC suponga la existencia de conjuntos no numerables no afecta en nada a que nos permite hablar de conjuntos infinitos cuya existencia sí que está intuitivamente justificada. ZFC habla de conjuntos intuitivamente existentes y de más cosas. Y así, la demostración en ZF de la sentencia aritmética Consis(AP) que expresa la consistencia de la aritmética de Peano (basada en que tiene como modelo a los números naturales) es un argumento intuitivamente verdadero, que no se ve afectado en nada por el hecho de que, además, ZFC permita demostrar afirmaciones sin un significado intuitivo objetivo.

> *Una debilidad que, en mi opinión, cualquier realista debería aceptar es su incapacidad para explicar el origen de la secuencia interminable de axiomas superiores, como los axiomas de infinitud superiores. Ciertamente, incluso el realista más acérrimo se estremece al contemplar cardinales de un tipo suficientemente inaccesible. También existen axiomas, como el de la existencia de un cardinal medible, que son más poderosos que el axioma de infinitud más general considerado hasta ahora, pero para los cuales no parece haber evidencia intuitivamente convincente que los justifique.*

El realista más acérrimo debería estremecerse al "contemplar" (si es que puede decirse que es contemplable) el cardinal $\aleph_1$. Cohen —como muchos matemáticos— tiene un concepto muy elástico de lo que puede llamarse "evidencia intuitiva". Confunde "intuitivo" con "plausible", "análogo a cosas que me resultan familiares", etc.

> *Los recientes resultados de independencia constituyen otro desafío a la postura realista. Respecto a esto último, algunos creen que algún axioma intuitivamente aceptable podría eventualmente resolver la hipótesis del continuo y problemas similares. Por otro lado, el axioma de existencia de cardinales medibles no ofrece la más remota posibilidad de tal resolución y parece destinado a ser adoptado como axioma por los especialistas en teoría de conjuntos más entusiastas. Sin embargo, incluso en este aspecto, la postura realista es más envidiable que la formalista, ya que para ésta última existen*

> *proposiciones en la propia teoría de números, como* Consis(ZF)*, que son insolubles. Una postura realista optimista parecería ser que, de alguna manera,* Consis(ZF + Existe un cardinal medible) *se reducirá a la consistencia de enunciados adecuadamente contundentes que se considerarán como axiomas de infinitud. La postura más optimista sería que toda cuestión de teoría de números pueda resolverse mediante un axioma de infinitud adecuado.*

Esos problemas son tan insolubles para un realista como para un formalista. Afirmar que "tienen una solución desconocida", que es lo que, según Cohen, hace el realista, es lo mismo que no decir nada. Que un axioma se considerara "adecuado" en el sentido en que aquí considera Cohen —y aquí hay que señalar que está expresando la posición de Gödel— sería algo puramente subjetivo (acepto este axioma porque me parece "intuitivo" es decir, "plausible", "familiar", etc.)

> *Nuestra familiaridad con el Teorema de Incompletitud no debería hacernos perder de vista la gran deficiencia de todos los sistemas formales, un hecho de mayor alcance que la independencia de enunciados particulares como la hipótesis del continuo. Subyace a mi pesimismo fundamental de que ningún logro puramente técnico arrojará jamás mucha luz sobre los problemas filosóficos básicos.*

Esto es un ejemplo de lo que decía Kreisel: sus propios prejuicios le impiden ver a Cohen que esos "resultados técnicos" a los que se refiere están arrojando luz más que suficiente sobre lo que hay detrás de la matemática formal: Cohen no es consciente de que existe una amplia parte de las matemáticas que no necesita de ninguna teoría axiomática formal para justificarse con rigor, porque sus conceptos tienen un contenido intuitivo preciso, no en el sentido vago y subjetivo con el que él emplea la palabra "intuición". Pero los límites del territorio que abarca la matemática intuitiva son muy técnicos. Y, en lugar de dedicar páginas y más páginas a justificar que una determinada definición sofisticada tiene un contenido intuitivo preciso, es mucho más fácil adoptar unos axiomas que admitan conceptos generales sin pedirles ninguna justificación más allá de lo imprescindible para evitar paradojas. Lo que ocurre es que no hay una única forma de completar la matemática intuitiva con conceptos abstractos sin caer en contradicciones y, según se haga de un modo u otro, podemos tener que se cumple o no la hipótesis del continuo, que existe o no un árbol de Suslin, etc. Y no hay nada de raro ni de frustrante en eso.

> *Para el matemático medio que simplemente desea asegurar la solidez de su trabajo, la opción más atractiva es evitar dificultades mediante el programa de Hilbert. En este caso, las matemáticas se consideran como un juego formal y uno sólo se preocupa por la cuestión de la consistencia. Este punto de vista quizás se ha vuelto aún más atractivo con el paso del tiempo, a medida que el enfoque operacional se ha extendido a otros campos, como la física. Es decir, uno sólo se preocupa por los objetos con los que tiene contacto directo, que en matemáticas es el lenguaje formal, en lugar de los conjuntos infinitos. De hecho, este programa formalista de Hilbert sigue siendo el único punto de vista totalmente preciso (que no es lo mismo que correcto) en estos asuntos. Este es, sin duda, un ejemplo de cómo el tiempo ha contribuido poco a presentar puntos de vista nuevos y originales sobre los fundamentos.*

La comparación con la física es acertada, como ya habíamos señalado, pero no es cierto que el formalismo suponga renunciar a "preocuparse" de los conjuntos infinitos. Por una parte, es posible desarrollar teorías formales más restrictivas que hablen de conjuntos infinitos, pero que tengan un contenido intuitivo que justifique sus axiomas, cuya consistencia se puede estudiar con éxito, y en las que se puede formalizar una parte sustancial de la matemática. No es algo que necesite hacer "el matemático medio" pero es algo que puede ser estudiado como cualquier otro ámbito de las matemáticas que no tiene por qué interesar tampoco al "matemático medio". Por otra parte, el formalismo matemático sólo crea un muro de contención entre la matemática y la filosofía de las matemáticas, lo cual no significa que fulmine a la segunda: uno puede filosofar todo lo que quiera sobre qué son los conjuntos, si existen, si no existen, etc., pero con la garantía de que todo lo que filosofe será irrelevante para la práctica del "matemático medio" que seguirá siendo demostrar teoremas en ZFC (o con axiomas adicionales debidamente explicitados).

> *Históricamente, los matemáticas no parecen tolerar proposiciones indecidibles. Pueden elevar dicha proposición a la categoría de axioma y, tras una exposición repetida, llegar a ser ampliamente aceptada. Este es, en mayor o menor medida, el caso del axioma de elección. Yo caracterizaría esta tendencia simplemente como una forma de oportunismo. Es, por supuesto, un oportunismo impersonal y bastante constructivo. Sin embargo, la sensación de que las matemáticas son una actividad*

> *valiosa y relevante no debería borrar por completo de nuestra mente una apreciación honesta de los problemas que nos aquejan. En el caso de la Hipótesis del Continuo, esta tendencia podría, aunque improbable, conducir a una división de la teoría de conjuntos en ramas, dependiendo de cómo se evalúe la potencia del continuo.*

He aquí otra muestra de lo que decía Kreisel: Cohen está anticuado, tiene toda una serie de descubrimientos ante su vista y considera que no aportan nada. La realidad hoy en día es justo la contraria de la que describe: las matemáticas toleran perfectamente las proposiciones indecidibles (salvo que entendamos por "matemáticas" la opinión de los matemáticos no familiarizados con la fundamentación de las matemáticas). Pese a que le pareciera improbable, es justo lo que ha sucedido. La "división en ramas" está completamente asumida hoy en día: hay teoremas interesantes que suponen la hipótesis del continuo y teoremas interesantes que suponen su negación, y lo mismo con mil variantes asociadas a otras tantas afirmaciones indecidibles. Y prácticamente nadie se plantea adoptar religiosamente unas como axiomas y desterrar las contrarias. No hay ninguna clase de "problemas que nos aquejan" en el sentido en que lo plantea.

> *Desde una perspectiva cínica, se podría decir que el oportunismo juzgará las cuestiones filosóficas desde la perspectiva de que las matemáticas deberían desarrollarse para dar empleo al mayor número posible de matemáticos.*

Es una forma pintoresca de expresarlo, pero es cierto si lo traducimos a que una teoría matemática podrá ser (subjetivamente) interesante o no en función de lo que sea en sí misma, como ha sucedido siempre, pero no será más o menos interesante por el hecho de que suponga unos axiomas u otros.

> *Sería realmente triste que esta ola de éxito* [en cuanto a pruebas de consistencia] *lograra descartar por completo toda preocupación filosófica sobre la hipótesis del continuo y cuestiones similares por considerarla intrascendente.*

Eso es justo lo que ha sucedido, y no tiene nada de triste. Es la consecuencia natural de tener en cuenta lo que aportan los hechos que, a juicio de Cohen, no aportan nada a la fundamentación de las matemáticas.

La crisis de los fundamentos En conclusión: tras casi un siglo de debates, *la crisis de los fundamentos* de la matemática estaba prácticamente resuelta. La solución no correspondió a ningún descubrimiento de nadie en particular, sino a la constatación de que llevaba muchos años resuelta. La solución era ZFC (durante unos años, NBG había sido mucho más popular, pero las pruebas de consistencia eran más sencillas en ZFC, así que por estas fechas ya estaba imponiéndose, aunque en realidad es algo intrascendente, pues ambas teorías son equivalentes).

Desde un punto de vista práctico, ZFC define el trabajo del matemático: hacer matemáticas es demostrar teoremas de ZFC (más algún axioma adicional, si se estima oportuno, aunque este caso puede verse como la demostración de una implicación en ZFC). Y el "matemático medio" puede incluso olvidar esto. Le basta asimilar un libro de teoría ingenua de conjuntos que exponga los principios conjuntistas básicos, sin necesidad de presentar explícitamente ninguna axiomática (pero sin decir nada que "no quepa" en ZFC), interiorizar las reglas de "rigor formal" y ya tiene el bagaje necesario para hacer matemáticas en su área predilecta. Todo lo que demuestre rigurosamente serán teoremas de ZFC, sea consciente de ello o no.

Desde un punto de vista teórico ZFC justifica el trabajo del matemático bajo la hipótesis de que es una teoría consistente. No caben dudas filosóficas sobre si algo es o no una demostración. Puesto que nunca se presenta una demostración totalmente formalizada, podrá haber dudas sobre determinados pasajes sobre los que se requiera una aclaración, pero, o bien tal aclaración puede darse, o bien hay un "agujero" en la demostración. Lo que es inconcebible es que un punto sea puesto en duda y se sostenga que es correcto a la vez que no se sepa dar una explicación de por qué (otra cosa es que se conjeture que es correcto, pero no que se dé por correcto en ausencia de una justificación adecuada). No hay lugar a debates filosóficos sobre si un argumento es correcto o no. Si lo es, se puede detallar hasta que su corrección sea incuestionable, tomando como referencia la posibilidad de formalizarlo en ZFC.

De este modo, ZFC aísla el trabajo del matemático de las discusiones filosóficas sobre el contenido de la matemática. Se puede filosofar, pero eso no afecta a la teoría ni a la práctica de la matemática. Cada cual puede pensar lo que quiera sobre la filosofía de la matemática, pero eso no puede llevar a ninguna discrepancia efectiva. Naturalmente, alguien puede negarse a trabajar en ZFC por objeciones filosóficas, pero eso es como el

vegetariano que no quiere comer carne: la carne es un alimento disponible, independientemente de que alguien quiera comerlo o no. Del mismo modo, los teoremas de ZFC están ahí y son matemáticas relevantes, tanto si alguien quiere interesarse por ellos como si no.

Todas las variantes de ZFC que resultan de poner o quitar axiomas adicionales son interesantes con el mismo grado de subjetividad con que los matemáticos evalúan el interés de una teoría, pero está fuera de lugar descartar un axioma sólo porque sea "raro". Será interesante o no, a uno le podrá interesar o no, pero da igual si es "raro" o no. No hay ningún criterio para decir que unas matemáticas son "mejores" que otras sólo por que usen unos axiomas u otros.

Esto incluye la posibilidad de estudiar igualmente otras teorías axiomáticas independientes, o incluso contradictorias con ZFC (como puedan ser los Nuevos Fundamentos de Quine). Cualquier teoría axiomática que, por un motivo u otro, se pueda considerar interesante es matemática. Que el estándar se fije en ZFC es una mera cuestión de conveniencia. No hay ninguna razón teórica por la que no pudiera sustituirse por otra teoría suficientemente potente. La ventaja principal de ZFC es que permite a los matemáticos razonar en ZFC sin necesidad de conocer siquiera ZFC, sin más que respetar unas reglas de rigor formal que les resultan naturales. Eso no valdría, por ejemplo, para NF, pero cualquier teoría alternativa que cumpliera este requisito valdría igualmente. Adoptar concretamente ZFC no es esencial, sino que es, más o menos, como la adopción del Sistema Internacional de Unidades por parte de los físicos: un mero convenio intrascendente para unificar criterios.

No hay que concluir de aquí que haya un consenso universal por el que todos los matemáticos suscriban el punto de vista que acabamos de describir, pero, salvo pequeños matices, sí que es un hecho que el resumen precedente describe la situación de la matemática actual. Un matemático podrá tener sus opiniones filosóficas realistas, constructivistas o las que sean, pero un matemático constructivista no debería considerarse legitimado a rechazar la publicación de un trabajo correctamente demostrado en ZFC porque sus conclusiones no sean constructivistamente aceptables, y en eso hay consenso de la comunidad matemática. Igualmente, un matemático platonista que esté convencido de que "de verdad de verdad de la buena" $2^{\aleph_0} = \aleph_2$ no se debería considerar legitimado a rechazar la publicación de un artículo por el hecho de que suponga la hipótesis del continuo, y en eso hay consenso de la comunidad matemática, y alguien que considere que ZFC no es la teoría correcta para formalizar las matemáticas, sino que la buena es YEB[248], no tendrá ninguna legitimidad para rechazar la publicación de un artículo que se base en ZFC, del mismo modo que nadie podrá rechazar el valor matemático de un teorema demostrado en YEB por el mero hecho de que YEB no sea ZFC, en la medida en que satisfaga criterios razonables de lo que es matemáticamente interesante. Kronecker murió y sigue muerto y enterrado.

98 Las Pruebas de independencia simplificadas, de Rosser En **1969** Rosser publicó su libro *Pruebas de independencia simplificadas,* donde se expuso por primera vez de forma detallada y sistemática el *forcing* desde el punto de vista de las álgebras de Boole completas. Aprovechamos para explicar con cierto detalle en qué consiste este método que ya hemos esbozado anteriormente.

Partimos de un álgebra de Boole completa $\mathbb{B}$ y vamos a definir, por recursión transfinita, una sucesión de conjuntos $\{V_\alpha^{\mathbb{B}}\}_{\alpha\in\Omega}$ juntamente con dos aplicaciones

$$\| \ = \ \|_\alpha : V_\alpha^{\mathbb{B}} \times V_\alpha^{\mathbb{B}} \longrightarrow \mathbb{B}, \qquad \| \ \in \ \|_\alpha : V_\alpha^{\mathbb{B}} \times V_\alpha^{\mathbb{B}} \longrightarrow \mathbb{B},$$

es decir, que para cada par de elementos $a, b \in V_\alpha^{\mathbb{B}}$, definiremos $\|a = b\|_\alpha$ y $\|a \in b\|_\alpha$. Se cumplirá que si $\alpha \le \beta$, entonces $V_\alpha \subset V_\beta$, y las aplicaciones en $V_\beta \times V_\beta$ extenderán a las correspondientes a α.

Partimos de $V_0 = \varnothing$, con lo que las aplicaciones $\| \ = \ \|_0$ y $\| \ \in \ \|_0$ son vacías y no hay nada que definir. Para un ordinal límite λ definimos simplemente $V_\lambda^{\mathbb{B}} = \bigcup_{\delta<\lambda} V_\delta^{\mathbb{B}}$, con lo que $\| \ = \ \|_\lambda$ y $\| \ \in \ \|_\lambda$ son las únicas aplicaciones que extienden a las precedentes.

El único caso delicado consiste en suponer definido $V_\alpha^{\mathbb{B}}$ con sus aplicaciones correspondientes y definir $V_{\alpha+1}^{\mathbb{B}}$ con las suyas. Para ello, si $b : V_\alpha^{\mathbb{B}} \longrightarrow \mathbb{B}$, decimos que b es *extensional* si, para cada $x, y \in V_\alpha^{\mathbb{B}}$, se cumple

$$b(x) \wedge \|x = y\|_\alpha \le b(y).$$

Definimos $V_{\alpha+1}^{\mathbb{B}}$ como la unión de $V_\alpha^{\mathbb{B}}$ y el conjunto de todas las aplicaciones $b : V_\alpha^{\mathbb{B}} \longrightarrow \mathbb{B}$ extensionales.

Ahora consideramos $a, b \in V_{\alpha+1}^{\mathbb{B}}$ y distinguimos varios casos:

[248] YEB es la teoría que resulta de sustituir cada letra de ZFC por su predecesora en el alfabeto.

1. Si $a, b \in V_\alpha^{\mathbb{B}}$, entonces definimos $\|a = b\|_{\alpha+1} = \|a = b\|_\alpha$, $\|a \in b\|_{\alpha+1} = \|a \in b\|_\alpha$. Con esto tenemos garantizado que las nuevas aplicaciones extienden a las precedentes.

2. Si $a \in V_\alpha^{\mathbb{B}}$ y $b \notin V_\alpha^{\mathbb{B}}$, definimos $\|a \in b\|_{\alpha+1} = b(a)$. Así, si pensamos en los elementos de los $V_\alpha^{\mathbb{B}}$ como "nombres", cada uno de ellos, como b, es una función que asigna a cada nombre a previamente definido un valor en $\mathbb{B}$ que indica la "probabilidad" de que el conjunto nombrado por a pertenezca al conjunto nombrado por b. Observemos que, en estos términos, la definición de extensionalidad puede escribirse así:

$$\|x \in b\|_{\alpha+1} \wedge \|x = y\|_{\alpha+1} \le \|y \in b\|_{\alpha+1}.$$

   Por lo tanto, si G es un ultrafiltro en $\mathbb{B}$ y se cumple que $\|x \in b\|_{\alpha+1}$, $\|x = y\|_{\alpha+1} \in G$, también se cumple que $\|y \in b\|_{\alpha+1} \in G$. Por otro lado, definimos

$$\|a = b\|_{\alpha+1} = \bigwedge_{x \in V_\alpha^{\mathbb{B}}} (\|x \in a\|_{\alpha+1} \to \|x \in b\|_{\alpha+1}) \wedge \bigwedge_{x \in V_\alpha^{\mathbb{B}}} (\|x \in b\|_{\alpha+1} \to \|x \in a\|_{\alpha+1}),$$

   donde $\bigwedge$ indica el ínfimo en $\mathbb{B}$ y, para $p, q \in \mathbb{B}$, definimos $p \to q = p' \vee q$. Notemos que todas las funciones del miembro derecho están ya definidas.

3. Si $a \notin V_\alpha^{\mathbb{B}}$ y $b \in V_\alpha^{\mathbb{B}}$, definimos $\|a = b\|_{\alpha+1}$ con la misma expresión que en el caso anterior, mientras que

$$\|a \in b\|_{\alpha+1} = \bigvee_{x \in V_\alpha^{\mathbb{B}}} (\|x = a\|_\alpha \wedge \|x \in b\|_\alpha).$$

4. Si $a \notin V_\alpha^{\mathbb{B}}$ y $b \notin V_\alpha^{\mathbb{B}}$, usamos las mismas expresiones que en el caso precedente, cuyos miembros derechos también están ya definidos en este caso.

Con esto podemos definir $V^{\mathbb{B}} = \bigcup_{\alpha \in \Omega} V_\alpha^{\mathbb{B}}$, así como las aplicaciones

$$\| \ = \ \| : V^{\mathbb{B}} \times V^{\mathbb{B}} \longrightarrow \mathbb{B}, \qquad \| \ \in \ \| : V^{\mathbb{B}} \times V^{\mathbb{B}} \longrightarrow \mathbb{B}$$

que son las únicas que extienden a todas las que hemos definido. Así, cada $a \in V^{\mathbb{B}}$ es una función definida sobre $\mathcal{D}a = V_\alpha^{\mathbb{B}}$, para cierto ordinal α, y un cálculo rutinario muestra que, en todos los casos,

$$\|a = b\| = \bigwedge_{x \in \mathcal{D}a} (\|x \in a\| \to \|x \in b\|) \wedge \bigwedge_{x \in \mathcal{D}b} (\|x \in b\| \to \|x \in a\|), \qquad \|a \in b\| = \bigvee_{x \in \mathcal{D}b} (\|x = a\| \wedge \|x \in b\|).$$

También conviene recordar que, si $a \in \mathcal{D}b$, entonces $\|a \in b\| = b(a)$.

A partir de aquí podemos definir $\|\phi(a_1, \ldots, a_n))\| \in \mathbb{B}$ para cada fórmula $\phi(x_1, \ldots, x_n)$ del lenguaje de la teoría de conjuntos y elementos $a_1, \ldots, a_n \in V^{\mathbb{B}}$ en términos de las operaciones del álgebra de Boole:

1. $\|a = b\|$ y $\|a \in b\|$ son los valores que ya tenemos definidos.
2. $\|\neg\phi\| = \|\phi\|'$.
3. $\|\phi \vee \psi\| = \|\phi\| \vee \|\psi\|$, $\|\phi \wedge \psi\| = \|\phi\| \wedge \|\psi\|$, $\|\phi \to \psi\| = \|\phi\| \to \|\psi\|$, $\|\phi \leftrightarrow \psi\| = \|\phi\| \leftrightarrow \|\psi\|$, donde, para $p, q \in \mathbb{B}$, definimos $p \leftrightarrow q = (p \to q) \wedge (q \to p)$.
4. $\|\bigwedge x\, \phi(x)\| = \bigwedge_{a \in V^{\mathbb{B}}} \|\phi(a)\|$, $\|\bigvee x\, \phi(x)\| = \bigvee_{a \in V^{\mathbb{B}}} \|\phi(a)\|$.

A partir de aquí es una tarea rutinaria comprobar que 1) todos los teoremas lógicos cumplen $\|\phi\| = 1$, y que 2) todos los axiomas de ZFC cumplen $\|\phi\| = 1$. Descartando explicaciones, a Rosser lo primero le ocupa unas 9 páginas lo primero y otras 23 lo segundo.

Esto es el contenido principal del tercer capítulo del libro de Rosser, junto con algunos hechos más sobre valores booleanos de fórmulas sobre cardinales y ordinales, y sobre el axioma de elección. (El primer capítulo habla de pruebas de consistencia y el segundo contiene preliminares sobre álgebras de Boole.)

En el capítulo 4, Rosser da un primer ejemplo de cómo se puede usar esto para obtener pruebas de consistencia. Concretamente, construye un álgebra de Boole para la que demuestra que $\|V \neq L\| = 1$ o, equivalentemente,

que $\|V = L\| = 0$. Esto implica que, si ZFC es consistente, en ZFC no se puede demostrar que $V = L$, porque si $V = L$ fuera un teorema de ZFC, Rosser ha demostrado que a partir de una demostración de $V = L$ en ZFC se podría construir otra demostración en ZFC de $\|V = L\| = 1$, pero en ZFC se puede demostrar que $\|V = L\| = 0$, luego tendríamos una contradicción en ZFC.

El método es general. Por ejemplo, en el capítulo 7 Rosser elegirá un álgebra de Boole adecuada con la que demostrar que $\|2^{\aleph_0} = \aleph_2\| = 1$. Esto prueba que si ZFC es consistente, es imposible demostrar que $2^{\aleph_0} \neq \aleph_2$, por el mismo argumento anterior.

El capítulo 5 está dedicado, en teoría, a explicar la relación de esta construcción con el *forcing,* pero Rosser deja claro que no entiende lo que está haciendo. Antes de comentar lo que dice, vamos a explicar lo que debería haber dicho.

Modelos booleanos y *forcing* ¿Qué relación tiene la teoría que acabamos de exponer con el *forcing* tal y como lo describe, por ejemplo, Shoenfield en su artículo *Forcing no ramificado*?

Para responder a esta pregunta consideremos un modelo transitivo numerable M de ZFC y consideremos un álgebra de Boole completa[249] $\mathbb{B}$ en M. Entonces, "alguien que viva en M", puede definir la clase $V^{\mathbb{B}}$ que define Rosser, pero que no será la auténtica clase $V^{\mathbb{B}}$, sino el conjunto $M^{\mathbb{B}} \subset M$ que tomará por $V^{\mathbb{B}}$ alguien que sólo vea los conjuntos de M. Para cada fórmula $\phi(x_1, \ldots, x_n)$ del lenguaje de la teoría de conjuntos y todos los $a_1, \ldots, a_n \in M^{\mathbb{B}}$, está definido $\|\phi(a_1, \ldots, a_n)\| \in \mathbb{B}$, de modo que, si ϕ es un teorema de ZFC, entonces $\|\phi\| = 1$.

Por otra parte, podemos considerar el conjunto de condiciones $\mathbb{P} = \mathbb{B} \setminus \{0\}$, con el orden dado por la estructura de álgebra de Boole. Siguiendo a Shoenfield, podemos proponernos construir con él una extensión genérica de M. Para ello tenemos que fijar un filtro genérico. Puesto que $\mathbb{P}$ y $\mathbb{B}$ son "casi lo mismo", es conveniente llamar filtros $\mathbb{B}$-genéricos sobre M a los filtros $\mathbb{P}$-genéricos sobre M. Sucede que, en este contexto, tienen la caracterización siguiente:

> **Teorema** Si M es un modelo transitivo numerable de ZFC, $\mathbb{B}$ es un álgebra de Boole completa en M, entonces G es un filtro $\mathbb{B}$-genérico sobre M si y sólo si es un ultrafiltro de $\mathbb{B}$ y para todo $X \in M$ tal que $X \subset G$, se cumple que $\bigwedge X \in G$.

El paso siguiente para construir la extensión genérica $M[G]$ es considerar un conjunto de $\mathbb{P}$-nombres (que, desde el punto de vista de M es, de hecho, una clase propia). Por no tener que hacer distinciones, Shoenfield toma como nombres todos los conjuntos de M, y define

$$M[G] = \{b_G \mid b \in M\}.$$

Pero, al calcular b_G, no se tienen en cuenta para nada los elementos de b que no sean de la forma (a, p), con $p \in \mathbb{P}$. Por eso hemos visto que, si definimos $M^{\mathbb{P}}$ como el conjunto de los nombres b cuyos elementos son todos de la forma (a, p), donde $a \in M^{\mathbb{P}}$ y $p \in \mathbb{P}$, no perdemos nada realmente, y sucede que

$$M[G] = \{b_G \mid b \in M\} = \{b_G \mid b \in M^{\mathbb{P}}\}.$$

Y el caso es que tampoco perdemos nada si tomamos como nombres únicamente los elementos de la clase de nombres $M^{\mathbb{B}}$ definida por Rosser:

$$M[G] = \{b_G \mid b \in M\} = \{b_G \mid b \in M^{\mathbb{P}}\} = \{b_G \mid b \in M^{\mathbb{B}}\}.$$

Al usar nombres de $M^{\mathbb{B}}$ nos encontraremos de tanto en tanto con nombres b que contienen pares $(a, 0)$ que son inútiles, porque 0 nunca va a estar en G, luego es como si no estuvieran, pero no molestan igual que tampoco molestan todos los conjuntos de más que hay cuando Shoenfield toma como nombres todos los elementos de M.

Así pues, concluimos que el la clase $M^{\mathbb{B}}$ que define Rosser es simplemente una clase de nombres "más eficiente" en el sentido de que permite construir los mismos conjuntos que forman $M[G]$ con menos redundancias.

El paso siguiente, siguiendo el camino de Shoenfield, sería definir la relación[250]

$$p \Vdash^* \phi(x_1, \ldots, x_n),$$

[249] Con esto queremos decir que B es un álgebra de Boole que"alguien que viva en M" considera que es completa. Para ello basta con que todo subconjunto de $\mathbb{B}$ *que esté en* M tenga supremo e ínfimo.

[250] Por simplicidad, vamos a llamar $p \Vdash^* \phi$ a la relación débil que, con la notación de Shoenfield, sería $p \Vdash^* \neg\neg\phi$. Actualmente se sabe definir la relación débil sin pasar antes por la fuerte.

que Shoenfield define para conjuntos arbitrarios (aunque podríamos restringir a la clase de C-nombres V^C), pero sucede que, en realidad, si nos limitamos a definirla para nombres en $V^{\mathbb{B}}$, podemos ahorrarnos toda la definición técnica de Shoenfield, porque, con su definición, para todos los $a_1, \ldots, a_n \in V^{\mathbb{B}}$, se cumple que[251]

$$p \Vdash^* \phi(a_1, \ldots, a_n) \qquad \leftrightarrow \qquad p \leq \|\phi(a_1, \ldots, a_n)\|.$$

Así pues: la definición de $\|\phi\|$ es una simplificación de la definición de $p \Vdash^* \phi$ que aprovecha que $\mathbb{B}$ es un álgebra de Boole completa y no un conjunto ordenado arbitrario. Es más sencillo definir $\|\phi\|$ como Rosser y tomar la equivalencia precedente como definición de $p \Vdash^* \phi$, y el resultado será el mismo que si usamos la definición de Shoenfield.

Luego tenemos que demostrar que, para $a_1, \ldots, a_n \in M^{\mathbb{B}}$, el hecho de que "alguien que viva en M" vea que se cumple $p \Vdash^* \phi(a_1, \ldots, a_n)$ equivale a que si G es un filtro $\mathbb{B}$-genérico sobre M, y $p \in G$, entonces $M[G] \vDash \phi((a_1)_G, \ldots, (a_n)_G)$. Pero, en lugar de demostrarlo como lo hace Shoenfield, en este contexto es mucho más fácil demostrar este teorema equivalente:

> **Teorema** Si M es un modelo transitivo numerable de ZFC, $\mathbb{B}$ es un álgebra de Boole completa en M, $a_1, \ldots, a_n \in M^{\mathbb{B}}$ y G es un ultrafiltro $\mathbb{B}$-genérico sobre M, entonces
>
> $$M[G] \vDash \phi((a_1)_G, \ldots, (a_n)_G) \quad \leftrightarrow \quad \|\phi(a_1, \ldots, a_n)\| \in G.$$

No obstante, si adoptamos la definición de $p \Vdash^* \phi(x_1, \ldots, x_n)$ de Shoenfield, que vale para conjuntos $x_1, \ldots, x_n$ arbitrarios, no necesariamente en $V^{\mathbb{B}}$, podemos demostrar lo siguiente:

> Si $\mathbb{B}$ es un álgebra de Boole completa y x es cualquier conjunto (considerado como nombre), existe un nombre $b \in V^{\mathbb{B}}$ tal que $1 \Vdash^* x = b$.

Esto significa que, si construimos $M[G]$ como Shoenfield y tomamos un elemento arbitrario en $M[G]$, éste será de la forma x_G, para cierto $x \in M$, pero entonces, "alguien que viva en M", usando el resultado anterior, encontrará un $b \in M^{\mathbb{B}}$ tal que $1 \Vdash^* x = b$, que equivale a $1 \Vdash x = b$ y, como $1 \in G$, esto equivale a que $x_G = b_G$, lo que demuestra que, como habíamos afirmado $M[G] = \{x_G \mid x \in M\} = \{b_G \mid b \in M^{\mathbb{B}}\}$.

Así pues, $\|\phi\|$ es simplemente la condición que tiene que ser verdadera para que ϕ se cumpla en $M[G]$ y, en conclusión, podemos decir lo siguiente:

> La definición de $\|\phi\|$ es simplemente una simplificación de la definición de $p \Vdash^* \phi$ que puede hacerse cuando el conjunto de condiciones no es cualquiera, sino un álgebra de Boole completa (menos el 0). Los nombres de $V^{\mathbb{B}}$ son simplemente un tipo particular de nombres que son suficientes para nombrar a todos los objetos de $M[G]$.

En definitiva, queda claro que los modelos booleanos son un caso particular de una parte de la teoría del *forcing,* que simplifica drásticamente la definición de la relación $p \Vdash^* \phi$ hasta el punto de que hace viable trabajar exclusivamente con ella, sin considerar modelos numerables y extensiones genéricas, pero nada impide hacerlo igualmente.

Recíprocamente, sucede que, si partimos de un conjunto de condiciones arbitrario C, es posible construir un álgebra de Boole completa $\mathbb{B}$ de modo que las extensiones genéricas construidas con C son las mismas que las construidas con $\mathbb{B}$, pero antes de entrar en detalles sobre esto veamos ya lo que dice Rosser en su capítulo 5, donde se supone que va a explicar la relación entre el *forcing* y los modelos booleanos. Como decíamos, pone en evidencia que la desconoce por completo. Después de explicar que existe un método para traducir demostraciones con *forcing* a demostraciones con álgebras de Boole, dice:

> *Este método de traducir argumentos de* forcing *a argumentos con álgebras de Boole se atribuye a Solovay y se dice que inspiró el enfoque con álgebras de Boole, notablemente diferente, que utilizamos.*
>
> *De hecho, este método de traducir argumentos de* forcing *a argumentos de álgebras de Boole probablemente sea un formalismo vacío en la mayoría de los casos, ya que la definición del álgebra de Boole está tan estrechamente ligada al argumento de* forcing *que el único medio aparente para demostrar cualquier enunciado relativo al álgebra de Boole es traducirlo de nuevo a un enunciado*

[251] Y esto no es casual, sino que Shoenfield llegó a su definición de $p \Vdash^* \phi$ tomando la definición de $\|\phi\|$ y viendo cómo podía eliminar de ella las operaciones booleanas, dejando únicamente la relación de orden.

> *relativo al* forcing *y luego demostrarlo mediante un argumento de* forcing. *Aun así, en cierto sentido, esta traducción nos permite reemplazar un tratamiento mediante* forcing *por un tratamiento mediante álgebras de Boole.*
>
> *¿Podemos decir, a la inversa, que cada tratamiento mediante álgebras de Boole puede transformarse en el tipo familiar de tratamiento de forcing?*
>
> *No parece haber argumentos claros para esto. De hecho, cabe señalar que, para los desarrollos del capítulo anterior, el universo $V^{\mathbb{B}}$ del modelo no es numerable. De hecho, es una clase, no un conjunto. Por lo tanto, no puede identificarse fácilmente con uno de los lenguajes ramificados utilizados en los argumentos de* forcing, *ya que éstos lenguajes se consideran habitualmente numerables.*
>
> *Sin embargo, podemos extraer un subconjunto de $V^{\mathbb{B}}$ que se corresponderá muy bien con el universo de un lenguaje ramificado de un argumento de* forcing. *Específicamente,* [...]

Este pasaje está lleno de errores o malentendidos. Acabamos de ver que el quinto párrafo de la cita anterior es un completo despropósito. Ciertamente $V^{\mathbb{B}}$ es una clase propia, pero si fijamos un modelo transitivo numerable M de ZFC y consideramos en él lo que "un habitante de M" llama $V^{\mathbb{B}}$, obtenemos el conjunto numerable $M^{\mathbb{B}}$, cuyos elementos pueden usarse como nombres, no para un *lenguaje del forcing* ramificado —porque precisamente el interés de estos nombres es que permiten construir las mismas extensiones genéricas sin necesidad de definir un lenguaje ramificado— sino para el *lenguaje del forcing* no ramificado según la presentación del *forcing* de Shoenfield, que a su vez da lugar a las mismas extensiones genéricas que las construidas con lenguajes ramificados.

Hemos cortado el sexto párrafo porque Rosser simplemente pone un ejemplo muy particular que no aporta nada. La relación entre los modelos booleanos y el *forcing* usual no consiste en encontrar un subconjunto de $V^{\mathbb{B}}$ que se corresponda con nada, sino en que $V^{\mathbb{B}}$ puede relativizarse a cualquier modelo transitivo numerable de ZFC, como hemos visto.

En definitiva: la respuesta a la pregunta del tercer párrafo (en contra de lo que cree Rosser) es un rotundo "sí", tal y como hemos explicado. Por ejemplo, considerando que Rosser ha demostrado en su capítulo 4 que, tomando un álgebra adecuada, se cumple $\|V \neq L\| = 1$, automáticamente tenemos que, si en un modelo numerable M consideramos lo que "sus habitantes" entiendan por dicha álgebra, en el modelo $M[G]$ construido a partir de cualquier ultrafiltro genérico se tiene $V \neq L$; como, en el capítulo 7, Rosser demuestra que, con cierta álgebra de Boole, se cumple $\|2^{\aleph_0} = \aleph_2\| = 1$, automáticamente tenemos que, usando lo que entiende por dicha álgebra "alguien que vive en un modelo numerable M" y tomando un ultrafiltro genérico cualquiera G, en la extensión genérica $M[G]$ se cumple $2^{\aleph_0} = \aleph_2$, etc.

Pasemos ahora a la relación opuesta, a la que se refiere Rosser en los dos primeros párrafos de la cita: ¿se puede transformar un argumento de *forcing* en un argumento con álgebras de Boole? Rosser dice que en teoría sí, pero que en la práctica no, porque Solovay había mostrado que a partir de cualquier conjunto de condiciones se puede construir un álgebra de Boole completa con la que se puede hacer lo mismo, pero ésta se define a partir de la relación $\Vdash$, por lo que no se puede razonar con ella sin estar, en definitiva, razonando con el *forcing* usual.

Eso es cierto, pero Rosser ignora que, en realidad, todo conjunto parcialmente ordenado $\mathbb{P}$ puede sumergirse densamente en un álgebra de Boole completa $\mathbb{B}$ con una construcción muy sencilla,[252] y que sin más que saber que $\mathbb{B}$ contiene una imagen densa de $\mathbb{P}$ (sin necesidad de conocer los detalles de la inmersión, aunque no son complicados) es suficiente para hacer con $\mathbb{B}$ todo lo que se puede hacer con $\mathbb{P}$.

Pero, aunque no estuviera al tanto de esto, cuesta disculpar que no fuera consciente de que Solovay, Scott y muchos otros sabían traducir, al menos en casos concretos, conjuntos $\mathbb{P}$ de condiciones a las álgebras de Boole completas adecuadas para construir con ellas modelos booleanos. Él mismo está usando álgebras de Boole que representan el mismo papel que los conjuntos parcialmente ordenados que usaron Cohen y Easton para sus pruebas de consistencia, por lo que sí que debía ser consciente de que, en la práctica, sí que era viable traducir argumentos de *forcing* generales a argumentos con álgebras de Boole, aunque no supiera dar un criterio general viable en la práctica para llevar a cabo la traducción. Así pues, lo de que el método que presenta es "notablemente diferente" es puro desconocimiento.

Para no ser injustos con Rosser, hay que citar este pasaje anterior al que hemos citado, aunque tampoco es que arregle mucho las cosas:

[252] Este resultado fue demostrado en su tesis doctoral por Holbrook Mann MacNeille en 1935, leída en Harvard bajo la dirección de Stone, y fue publicado en 1937 en el artículo *Conjuntos parcialmente ordenados*.

> *No hay nada en el tratamiento mediante álgebras de Boole que corresponda exactamente a la sucesión completa* [= genérica] $\{P_n\}$ *de condiciones de* forcing *definida por Cohen. Se puede lograr un resultado similar eligiendo un ultrafiltro* Δ *del álgebra de Boole y luego diciendo que* X *es verdadera si* $\|X\| \in \Delta$ *y que* X *es falso en caso contrario. De esta manera, se obtiene un modelo bivaluado. Este enfoque es adoptado por Sochor* [9] *y Vopěnka* [11,12]. *Este refinamiento produce algunos modelos interesantes, pero no es necesario para las demostraciones de independencia. Esto plantea la cuestión de si se puede obtener una demostración de independencia por métodos de* forcing *sin introducir una sucesión completa* $\{P_n\}$ *de condiciones de* forcing.

Lo de que "no hay nada" es cierto desde un punto de vista muy miope. Es equivalente al hecho de que, si fijamos un conjunto de condiciones $\mathbb{P}$ en un modelo transitivo numerable M de ZFC, en M no hay nada que se corresponda con una sucesión o filtro $\mathbb{P}$-genérico sobre M. Pero es que los filtros genéricos están fuera de M. Igualmente, en cuanto se relativiza su tratamiento mediante álgebras de Boole a un modelo numerable, ya podemos tomar filtros genéricos. Por otro lado, tomar un ultrafiltro de $\mathbb{B}$ sin relativizar a un modelo es como considerar un modelo M y tomar un ultrafiltro de $\mathbb{B}$ que esté en M. Un ultrafiltro que esté en M nunca puede ser genérico sobre M. Lo máximo que se consigue con él es dividir las sentencias (metamatemáticas) en verdaderas y falsas, pero con eso no se puede construir un modelo. Vopěnka habla de "modelos sintácticos", que son esencialmente lo mismo que los modelos booleanos, no modelos en el sentido de la teoría de modelos.

En cuanto a la última pregunta, una primera respuesta obvia es que, cuando el conjunto de condiciones es un álgebra de Boole completa, la respuesta es afirmativa, pues eso es justamente lo que hace Rosser, aunque no es consciente de estar haciéndolo y, en general, la respuesta es que el teoría sí, y en la práctica, a veces. Por ejemplo, lo hace Shoenfield en su libro *Lógica matemática.* Al margen de la peculiaridad de su "método axiomático", la demostración que muestra de la independencia de la hipótesis del continuo podría reformularse en términos de su *forcing no ramificado* sin necesidad de trabajar en ningún momento con $M[G]$ (pues en su exposición no hay ningún M[G]), razonando (sin filtros y sin álgebras de Boole) que $1 \Vdash^* 2^{\aleph_0} = \aleph_2$, que es equivalente a lo que hace Rosser cuando demuestra que $\|2^{\aleph_0} = \aleph_2\| = 1$.

Ahora bien, en la práctica, en demostraciones más complejas, el camino de trabajar exclusivamente con $\Vdash^*$ puede volverse inviable. Sería como tratar de calcular $\int_1^7 e^x \cos e^x\, dx$ aplicando la definición de integral en lugar de aplicar la regla de Barrow. En teoría es posible, en la práctica, en el mejor de los casos, sería un suplicio. Pero, igual que uno podría preguntarse qué interés tiene calcular una integral complicada mediante la definición de integral, sin usar resultados disponibles que simplifican drásticamente el cálculo, también puede uno preguntarse qué interés tiene no usar filtros genéricos cuando se pueden usar. De hecho, las cuatro alternativas:

1. Dar una prueba de consistencia usando sólo la definición de $p \Vdash^* \phi$ para conjuntos de condiciones parcialmente ordenados, sin usar filtros genéricos ni álgebras de Boole.

2. Dar una prueba de consistencia usando sólo la definición de $\|\phi\|$, usando álgebras de Boole completas como condiciones, pero no filtros genéricos.

3. Dar una prueba de consistencia usando modelos numerables y filtros genéricos, sin álgebras de Boole.

4. Dar una prueba de consistencia usando modelos numerables y ultrafiltros genéricos sobre álgebras de Boole completas.

Permiten, en teoría, hacer las mismas cosas, pero están ordenadas desde la más complicada hasta el punto de que puede resultar inviable en la práctica hasta la más cómoda. Y no hay ninguna razón para quedarse en un nivel y no pasar al siguiente si ello simplifica las cosas.

No parece que la lectura de estos pasajes de Rosser que hemos comentado tuvieran nada que ver con la muerte de Sierpiński, que falleció en Varsovia en **1969,** a los 87 años.

Que Rosser no tuviera estas cosas claras cuando escribió su libro, puede ser disculpable, pero en 1975 publicó una reseña del *Forcing no ramificado* de Shoenfield (que se publicó en 1971 en las actas del congreso de Los Ángeles) y del artículo *Potencias de cardinales regulares,* que Easton publicó en **1969** con el contenido de su tesis, en la que Rosser muestra que sigue sin entender nada:

> *Shoenfield introduce una versión del* forcing *que no requiere la jerarquía ramificada. Como resultado, se pueden dar demostraciones más breves, con muchos menos detalles. Aunque Shoenfield justifica su tratamiento para que se pueda comprender la relación entre éste y los tratamientos anteriores del* forcing*, la formulación resultante no es en absoluto intuitiva.* [...]

> *Para cada C y G, se define $M[G]$, que es un modelo numerable de* ZFC *que incluye a M y contiene a G, y es el menor de éstos. Es posible que $M[G]$ sea uno de los modelos que podrían generarse mediante* forcing *ramificado, pero Shoenfield no aclara mucho este punto.*

Lo que Rosser considera "no intuitivo en absoluto" es lo que hoy se ha convertido en la formulación estándar del forcing, mientras que la suya (que no era suya, sino de Solovay y Scott) tiene ahora un uso muy minoritario. Y Rosser seguía creyendo que el método de las álgebras de Boole eliminaba las hipótesis de numerabilidad del *forcing* y que, por lo tanto, era más general:

> *Easton y Shoenfield se basan en gran medida en la numerabilidad, por lo que sus tratamientos parecen, a primera vista, no aplicables. En cambio, el tratamiento mediante álgebras de Boole en el capítulo 8 de* [el libro de Rosser] *del revisor es directamente aplicable.*

Como ya hemos señalado, "el tratamiento mediante álgebras de Boole" es aplicable exactamente en los mismos casos que el *forcing* en general, pues no es más que el caso particular del *forcing* que se da cuando el conjunto de condiciones es un álgebra de Boole completa (sin el 0).

Que en 1975 Rosser "siguiera sin caer del burro" ya no tiene disculpa, pues en 1971 Jech[253] había publicado su libro *Lecciones sobre teoría de conjuntos con especial énfasis en el método del forcing,* donde dejaba bien claro todo lo que Rosser ignoraba, y la forma más habitual de presentar el *forcing* hoy en día es esencialmente la misma que se adopta en él.

En las nueve primeras secciones Jech presenta los resultados básicos sobre ZFC, hasta la aritmética cardinal, en la sección 10 introduce los modelos transitivos, en la sección 11 estudia la clase L de los conjuntos constructibles y en la sección 12 la usa para probar la consistencia del axioma de elección y de la hipótesis del continuo generalizada. Tras algunos resultados adicionales (sobre constructibilidad relativa, ultrapotencias, etc.) en la sección 16 demuestra el resultado de MacNeille según el cual:

> **Teorema** Si $\mathbb{P}$ es un conjunto parcialmente ordenado, existe un álgebra de Boole completa $\mathbb{B}$ (única salvo isomorfismo) y una inmersión $i : \mathbb{P} \longrightarrow \mathbb{B}$ cuya imagen es densa en $\mathbb{B}$.

donde una inmersión conserva el orden y también la incompatibilidad (dos condiciones p, q son incompatibles si no admiten una extensión común $r \le p, r \le q$). El álgebra $\mathbb{B}$ se llama la *compleción* de $\mathbb{P}$.

En la sección 17 empieza a presentar el *forcing.* Jech fija un modelo transitivo M de ZFC (no necesariamente numerable, sino que podría ser incluso $M = V$) y procede como sigue:

1. Para cada álgebra de Boole completa $\mathbb{B}$ en M, define el concepto de *ultrafiltro $\mathbb{B}$-genérico* sobre M, como un ultrafiltro en $\mathbb{B}$ con la propiedad de que si $X \in M$ cumple $X \subset G$, entonces $\bigwedge X \in G$.

2. Para cada conjunto parcialmente ordenado $\mathbb{P} \in M$, define el concepto de *filtro $\mathbb{P}$-genérico* sobre M, y demuestra que si $\mathbb{B}$ es la compleción de $\mathbb{P}$, existe una correspondencia biunívoca entre los filtros $\mathbb{P}$-genéricos sobre M y los ultrafiltros $\mathbb{B}$-genéricos sobre M.

3. Luego define la clase $M^{\mathbb{B}}$ más o menos igual que como hacía Rosser, define las funciones $[\![x = y]\!]$, $[\![x \in y]\!]$, con $x, y \in M^{\mathbb{B}}$, extiende la definición a fórmulas arbitrarias y demuestra que todos los teoremas de ZFC cumplen $[\![\phi]\!] = 1$.

4. Luego define el valor x_G de un nombre $x \in M^{\mathbb{B}}$ respecto de un ultrafiltro genérico (aunque lo llama $i_G(x)$) y define la *extensión genérica* $M[G] = \{x_G \mid x \in M^{\mathbb{B}}\}$.

5. Luego demuestra el teorema fundamental: $M[G] \vDash \phi((x_1)_G, \ldots, (x_n)_G) \leftrightarrow [\![\phi(x_1, \ldots, x_n)]\!] \in G$.

6. De ahí deduce que $M[G]$ es un modelo transitivo de ZFC, de hecho, el menor modelo transitivo N tal que $M \subset N$ y $G \in N$.

7. Tras discutir algunos ejemplos, considera un conjunto parcialmente ordenado $\mathbb{P}$, así como su compleción $i : \mathbb{P} \longrightarrow \mathbb{B}$ y, para cada $p \in \mathbb{P}$, define

$$p \Vdash \phi(x_1, \ldots, x_n) \quad \leftrightarrow \quad i(p) \le [\![\phi(x_1, \ldots, x_n))]\!].$$

[253] Para entonces Jech ya se había escapado de la Checoslovaquia comunista y no regresaría a Praga hasta la caída del régimen.

8. Para cada filtro $\mathbb{P}$-genérico G_1 sobre M, llama G al ultrafiltro genérico en $\mathbb{B}$ asociado a $\mathbb{P}$, define la extensión genérica $M[G_1] = M[G]$ y demuestra que

$$M[G_1] \vDash \phi((x_1)_G, \dots, (x_n)_G) \leftrightarrow \bigvee p \in G_1\, p \Vdash \phi(x_1, \dots, x_n).$$

Lo único que podría haber hecho y no hace es definir directamente la clase de nombres $M^{\mathbb{P}}$ y demostrar que cada elemento de $M[G_1]$ admite un nombre en $M^{\mathbb{P}}$.

De este modo Jech define $p \Vdash \phi$ y demuestra los teoremas fundamentales aprovechando la potencia de las álgebras de Boole completas, lo que le permite simplificar sustancialmente las definiciones y las demostraciones, pero al final está en condiciones de trabajar con un conjunto de condiciones arbitrario $\mathbb{P}$ sin necesidad de considerar para nada su compleción $\mathbb{B}$, salvo que sea conveniente por algún motivo.

A partir de aquí Jech aplica la técnica expuesta para presentar un gran número de pruebas de consistencia. Las últimas secciones están dedicadas a construir modelos de ZF en los que falla el axioma de elección mediante una teoría general para construir submodelos de extensiones genéricas formados por los conjuntos con nombres herditariamente simétricos, como hemos visto en la página 282 en un caso particular.

99 Aplicaciones de la teoría de extensiones genéricas Entre las pruebas de consistencia que Jech incluyó en su libro estaba la de la consistencia de que todo subconjunto de $\mathbb{R}$ sea medible Lebesgue, que finalmente Solovay había publicado el año anterior, en **1970** en un artículo titulado *Un modelo de la teoría de conjuntos en el que todo conjunto de reales es medible Lebesgue.* En él enuncia sin demostración los resultados básicos de la teoría de extensiones simétricas. Para las demostraciones, Solovay plantea dos alternativas: o usar un lenguaje ramificado, y cita el artículo de Lévy de 1965 como referencia, o usar álgebras de Boole, para lo que da como referencia sus notas con Scott, que seguían pendientes de publicación y nunca llegarían a publicarse.

Hemos señalado que Gödel había definido en 1964 la clase $\mathrm{HD}(\Omega)$ de los conjuntos hereditariamente definibles por ordinales, aunque sus ideas no aparecieron publicadas hasta que las desarrollaron Scott y Myhill en el congreso de 1966. Se trata de un modelo de ZFC, pero Solovay definió otro más amplio: la clase $\mathrm{HD}(\Omega^\omega)$ de los conjuntos *hereditariamente definibles por sucesiones de ordinales,* que es un modelo de ZF que no cumple necesariamente el axioma de elección. Solovay partía de un modelo transitivo numerable M de ZFC más la existencia de un cardinal inaccesible y construía extensiones genéricas en las que se cumplían las variantes que se indican en el teorema siguiente:

> **Teorema (Solovay)** Si ZFC más la existencia de un cardinal inaccesible es consistente, también lo es ZFC más la hipótesis del continuo generalizada más la afirmación siguiente:
>
> > Si $A \subset \mathbb{R}$ y $A \in \mathrm{HD}(\Omega^\omega)$, entonces A es medible Lebesgue y, si es no numerable, contiene un subconjunto perfecto.
>
> Alternativamente, en lugar de la hipótesis del continuo generalizada, se puede suponer que $2^{\aleph_0}$ es $\aleph_2$ o, más en general, cualquier otro cardinal de cofinalidad no numerable.

Lusin no había logrado determinar si los conjuntos $\mathbf{\Sigma}^1_2$ eran medibles Lebesgue, pero todos los conjuntos proyectivos son hereditariamente definibles mediante sucesiones de ordinales, por lo que Solovay había demostrado la consistencia de que todos los conjuntos proyectivos sean medibles Lebesgue (así como que, si son no numerables, contienen un subconjunto perfecto, luego ninguno de ellos puede desmentir la hipótesis del continuo, a pesar de que $2^{\aleph_0}$ puede ser $\aleph_2$ o $\aleph_{\omega+11}$).

Por otro lado, Solovay demostró que, en sus modelos, la clase $\mathrm{HD}(\Omega^\omega)$ cumple el principio de elecciones dependientes (ED), y esto basta y sobra para que "alguien que viva en esta clase" pueda construir la medida de Lebesgue. De este modo, Solovay había demostrado lo siguiente:

> Si ZFC más la existencia de un cardinal inaccesible es consistente, también lo es ZFC más "$\mathrm{HD}(\Omega^\omega)$ es un modelo de ZF + ED + todo subconjunto de $\mathbb{R}$ es medible Lebesgue y, si es no numerable, contiene un subconjunto perfecto", luego, en particular, también es consistente esta teoría.

La clase $\mathrm{HD}(\Omega^\omega)$ contiene un modelo que es "más natural", a saber, la clase $L(\mathbb{R}) = L(\mathcal{P}\omega)$ de los conjuntos constructibles respecto de $\mathbb{R}$ (o equivalentemente, respecto de $\mathcal{P}\omega$), que es la menor clase propia que es un modelo de ZF y contiene a todos los números reales, o a todos los subconjuntos de ω. Como decimos, se cumple que $L \subset L(\mathbb{R}) \subset \mathrm{HD}(\Omega^\omega)$, y de los resultados de Solovay se sigue inmediatamente esta variante:

Si ZFC más la existencia de un cardinal inaccesible es consistente, también lo es ZFC más "$L(\mathbb{R})$ es un modelo de ZF + ED + todo subconjunto de $\mathbb{R}$ es medible Lebesgue y, si es no numerable, contiene un subconjunto perfecto".

Otro resultado que Jech incluía en su libro se había publicado ese mismo año de 1971 en el artículo *Extensiones de Cohen iteradas y el problema de Suslin,* donde Solovay y Tennenbaum demostraban la consistencia de la hipótesis de Suslin, es decir, de que no existan árboles (luego tampoco rectas) de Suslin.

Recordemos (página 163) que un árbol de Suslin se define como un árbol de cardinal $\aleph_1$ cuyas cadenas y anticadenas son todas numerables. Esto implica en particular que sus niveles (los conjuntos de elementos de una misma altura) son numerables, luego tiene que tener elementos de cualquier altura numerable (o, de lo contrario, el árbol sería una unión numerable de niveles numerables), así como que no tiene elementos de altura no numerable (pues por debajo de un elemento de altura no numerable hay una cadena no numerable).

Un árbol de Suslin A está *bien podado* si tiene un único elemento de altura 0 y, por encima de cada nodo, hay nodos de cualquier altura numerable. Es fácil ver que todo árbol de Suslin tiene un subárbol bien podado que también es un árbol de Suslin.[254] Por lo tanto, la hipótesis de Suslin (es decir, la no existencia de rectas de Suslin) equivale a que no existan árboles de Suslin bien podados.

Un hecho básico es que un árbol de Suslin bien podado "se destruye a sí mismo" cuando se usa como conjunto de condiciones para construir una extensión genérica. En efecto:

Teorema Sea M un modelo transitivo numerable de ZFC y supongamos que A es un árbol de Suslin bien podado en M. Entonces, existe una extensión genérica de M en la cual A tiene una cadena de altura $\aleph_1$, luego ya no es un árbol de Suslin.

Demostración: Tomamos como conjunto de condiciones $\mathbb{P} = A$ con la relación de orden inversa, de modo que una condición p extiende[255] a otra q si $p \geq q$. Si G es un filtro $\mathbb{P}$-genérico sobre M, entonces G es una cadena en A de altura $\aleph_1$. Basta tener en cuenta que, para cada ordinal $\alpha < \omega_1$, el conjunto D_α de los nodos de A de altura $\geq \alpha$ es denso en $\mathbb{P}$ (porque A está bien podado), luego G tiene elementos de todas las alturas y por ser un filtro, dos cualesquiera de sus elementos tienen una extensión común, luego son comparables, y así G es una cadena. Por lo tanto, A tiene una cadena de altura $\aleph_1$ en $M[G]$ y así ha dejado de ser un árbol de Suslin. ∎

En realidad el argumento anterior tiene una laguna, y es que presupone que $\aleph_1$ en $M[G]$ es el mismo que en M. La alternativa sería que $\aleph_1^M$ pasara a ser numerable en $M[G]$, lo cual no sería grave, pues entonces A pasaría a ser numerable en $M[G]$ y con mayor razón dejaría de ser un árbol de Suslin.

Sin embargo, lo cierto es que esto no sucede y conviene entender por qué.

En general, en un conjunto parcialmente ordenado $\mathbb{P}$, se dice que dos elementos p, q son *incompatibles* si no tienen una extensión común, es decir, si no existe un $r \in \mathbb{P}$ tal que $r \leq p$ y $r \leq q$, y se representa por $p \perp q$.

Por ejemplo, en el conjunto $\mathbb{P}$ de condiciones de Cohen que añaden un subconjunto genérico de ω, es decir, las funciones de un subconjunto finito de ω en 2, dos condiciones son incompatibles cuando se contradicen. Por ejemplo, si una cumple $p(5) = 0$ y otra $q(5) = 1$, es imposible que una condición extienda a ambas, y viceversa, si dos condiciones p y q no se contradicen, entonces $p \cup q$ es una extensión común.

Definición Si $\mathbb{P}$ es un conjunto parcialmente ordenado, una *anticadena* en $\mathbb{P}$ es un conjunto $A \subset \mathbb{P}$ de condiciones incompatibles dos a dos.

[254] Si A es un árbol de Suslin, su nivel 0 es numerable, luego tiene que haber un nodo altura 0 que tenga por encima nodos de cualquier altura numerable. En caso contrario, para cada nodo p de altura 0, los nodos por encima de p no superarían una altura numerable α_p, y el supremo $\alpha < \omega_1$ de la familia numerable de ordinales α_p sería una cota de las alturas de los nodos del árbol. FIjamos un nodo de altura 0 con esta propiedad y llamamos A' al conjunto de los nodos que tiene por encima, que sigue siendo un árbol de Suslin, pero con un único nodo de altura 0. Luego llamamos A'' al conjunto de los nodos de A' que tienen por encima elementos de cualquier altura numerable, y es fácil ver que se trata también de un árbol de Suslin, que además está bien podado.

[255] Durante un tiempo, los textos sobre extensiones genéricas se dividirían en dos clases: los que (como Shoenfield o Jech), para expresar que una condición p extiende a otra q (en el sentido de que aporta más información), escriben $p \leq q$ y los que (como Solovay y Tennenbaum) escriben $q \leq p$. El convenio más habitual actualmente (porque es el que encaja mejor con el uso de álgebras de Boole) consiste en escribir $p \leq q$, de modo que la condición trivial 1, que se cumple siempre, es la máxima. Si queremos usar esta notación, al considerar un árbol de Suslin bien podado A como conjunto de condiciones, tenemos que considerar la relación inversa a la del orden, es decir, que $p \leq q$ (en el sentido de que p extiende a q) si y sólo si $q \leq p$ en el sentido del orden del árbol. En suma: una extensión tiene más información cuanto mayor es su altura en el árbol.

Se dice que $\mathbb{P}$ cumple la *condición de cadena numerable*[256] si toda anticadena en $\mathbb{P}$ es a lo sumo numerable.

Notemos que si A es un árbol y lo consideramos como conjunto parcialmente ordenado con la relación inversa, es decir, de modo que p extiende a q si $q \leq p$, entonces dos condiciones en A cumplen $p \perp q$ si no existe ninguna condición $r \in A$ que cumpla $p \leq r$ y $q \leq r$ (con la relación de orden del árbol), y esto equivale a que p y q no sean comparables (por definición de árbol).

Por lo tanto, las anticadenas de A en el sentido que acabamos de definir (considerando en A la relación de orden opuesta a la que tiene como árbol) coinciden con las anticadenas de A como árbol, luego si A es un árbol de Suslin, visto como conjunto de condiciones, cumple la condición de cadena numerable.

Esto es importante por el teorema siguiente:

Toda extensión genérica construida a partir de un conjunto de condiciones que cumple la condición de cadena numerable tiene los mismos cardinales que el modelo base.

Así pues, cuando destruimos un árbol de Suslin, poniéndolo "copa abajo" los cardinales en la extensión genérica son los mismos que en el modelo base, y lo que era un árbol de Suslin sigue siendo un árbol de altura $\aleph_1$, pero ahora con una cadena no numerable.

El caso es que destruir un árbol de Suslin no basta para probar la consistencia de la hipótesis de Suslin, sino que hay que destruir todos los árboles de Suslin. Solovay y Tennenbaum habían encontrado el modo de reducir una sucesión transfinita de extensiones genéricas a partir de un modelo de partida M a una única extensión, incluyendo el caso de que el conjunto de condiciones $\mathbb{P}_\alpha$ del paso α-ésimo se encuentre en la extensión α-ésima, pero no necesariamente en el modelo de partida. Esto lo aplicaban para partir de un modelo M e ir construyendo una sucesión de extensiones genéricas en cada una de las cuales se destruyera un árbol de Suslin (haciendo que dejara de ser un árbol de Suslin en la extensión) y de modo que, al terminar el proceso, a cualquier árbol de Suslin que hubiera aparecido en su transcurso le hubiera llegado más tarde el turno de ser destruido. El hecho de que todos los conjuntos de condiciones empleados cumplían la condición de cadena numerable (porque eran árboles de Suslin puestos del revés) permitía probar que el conjunto de condiciones que daba el modelo final también la cumplía, por lo que los cardinales de la extensión última eran los mismos que los del modelo de partida.

Al parecer, una vez encontraron la prueba, Solovay se empeñó en publicarla en términos de álgebras de Boole. Tennenbaum, aunque reticente, acabó accediendo, pero más adelante declararía que él no entendía su artículo.

Pero Donald Anthony Martin había visto la demostración antes de su publicación y había observado que, en lugar de recorrer todos los árboles de Suslin para destruirlos, el argumento valía igualmente para recorrer todos los posibles conjuntos de condiciones con la condición de cadena numerable, y que con ello se demostraba la consistencia de una afirmación más fuerte que la hipótesis de Suslin. Kenneth Kunen, que se había doctorado en 1968 bajo la dirección de Scott, llamó *Axioma de Martin* en su tesis a una versión equivalente formulada en términos de álgebras de Boole, así se refirieron a ella en su artículo Solovay y Tennenbaum y así se la conoce hoy en día.

Así pues, Solovay y Tennembaum modificaron su iteración de extensiones para demostrar la consistencia del axioma de Martin y luego observaron que de él se deduce fácilmente la hipótesis de Suslin.

El axioma de Martin Con la notación actual, que es distinta a la que usaban Martin y Solovay, el axioma de Martin se enuncia así:

Si κ es un cardinal infinito, $\mathsf{AM}(\kappa)$ es la afirmación: Si $\mathbb{P}$ es un conjunto parcialmente ordenado que cumple la condición de cadena numerable y $\mathcal{D}$ es una familia de subconjuntos densos de $\mathbb{P}$ con cardinal $|\mathcal{D}| \leq \kappa$, existe un filtro $\mathbb{P}$-genérico sobre $\mathcal{D}$ (es decir, que corta a todos los conjuntos $D \in \mathcal{D}$).

El *axioma de Martin* (AM) afirma que se cumple $\mathsf{AM}(\kappa)$ para todo cardinal infinito $\kappa < 2^{\aleph_0}$.

[256] Solovay y Tennenbaum la llaman *condición de anticadena numerable,* que es un nombre mucho más razonable, pero para entonces ya existía cierta tradición en topología de referirse a ella como "condición de cadena numerable" y ése es el nombre con que se conoce hoy en día.

Así el método de iteración de extensiones de Solovay y Tennenbaum permitía añadir un filtro genérico a un conjunto parcialmente ordenado con la condición de cadena numerable en cada paso, de modo que, al final del proceso, a cualquier conjunto parcialmente ordenado que hubiera aparecido en un paso intermedio (junto con cualquier familia $\mathcal{D}$ en las condiciones del axioma) se le habrá añadido un filtro genérico en un paso posterior, de modo que se cumpla AM. En definitiva, el resultado que obtuvieron fue el siguiente:

> **Teorema** Sea M un modelo transitivo numerable de ZFC. Sea κ un cardinal regular no numerable en M tal que, si $\mu < \kappa$, entonces $2^\mu \leq \kappa$. Entonces existe una extensión genérica de M en la que $2^{\aleph_0} = \kappa$ y se cumple AM.

Notemos que la condición $2^\mu \leq \kappa$ la cumple todo cardinal regular si suponemos que M cumple la hipótesis del continuo generalizada. Esto significa que si ZFC es consistente, también lo es añadir como axiomas, por ejemplo, $2^{\aleph_0} = \aleph_{17}$ y AM.

Lo primero que hay que tener claro sobre el axioma de Martin es que no pretende expresar una "verdad" razonable, o plausible, sobre los conjuntos, sino que es una mera forma de "encapsular" la teoría de las extensiones genéricas. Si alguien demuestra que AM implica cierta afirmación ϕ, para ello no necesitará saber nada de extensiones genéricas, y con ello habrá demostrado que, partiendo de un modelo M, es posible construir una extensión genérica en la que se cumple ϕ, por lo que, si ZFC es consistente, también lo es añadir ϕ como axioma. En resumen: el interés de AM es que toda consecuencia de AM es necesariamente consistente con ZFC (supuesto que ZFC sea consistente), y que no se necesita saber nada de modelos ni de extensiones genéricas para extraer consecuencias de AM.

Martin y Solovay publicaron un artículo titulado *Extensiones de Cohen internas* en el que demostraban muchas consecuencias del axioma de Martin, pero que apareció publicado antes, en **1970.** Veamos algunas de ellas:

1. AM($\aleph_0$) es un teorema de ZF, luego la hipótesis del continuo implica el axioma de Martin.

   En efecto, AM($\aleph_0$) afirma simplemente que siempre existe un filtro genérico sobre un conjunto numerable, que es el resultado que venimos usando para justificar la existencia de filtros genéricos sobre modelos numerables.

2. AM(κ) implica que $2^\kappa = 2^{\aleph_0}$. En particular, $\kappa < 2^{\aleph_0}$.

   Por lo tanto, no podemos extender AM pidiendo que AM(κ) se cumpla para cardinales mayores, porque sería contradictorio.

3. AM implica que $2^{\aleph_0}$ es un cardinal regular.

   En efecto, si la cofinalidad de $2^{\aleph_0}$ fuera $\mu < 2^{\aleph_0}$, como se cumple AM(μ), tendría que ser $2^\mu = 2^{\aleph_0}$, y entonces 2^μ tendría cofinalidad μ, lo que contradice al teorema de Kőnig. ∎

4. AM($\aleph_1$) implica la hipótesis de Suslin.

   La demostración es esencialmente la misma que la prueba de que un árbol de Suslin fuerza su propia destrucción: Supongamos que A es un árbol de Suslin bien podado. Entonces, visto como conjunto de condiciones (con la relación de orden inversa) tiene la condición de cadena numerable, luego se le puede aplicar AM($\aleph_1$). Para cada ordinal $\alpha < \omega_1$, el conjunto D_α de los elementos de A de altura $\geq \alpha$ es denso, luego por AM($\aleph_1$) existe un filtro G que corta a todos ellos, con lo que es una cadena en A de altura $\aleph_1$, en contradicción con que A sea un árbol de Suslin. ∎

5. AM(κ) implica que la unión de κ conjuntos nulos para la medida de Lebesgue es nula. En particular, todo subconjunto de $\mathbb{R}$ de cardinal $\leq \kappa$ es nulo.[257]

   Sea $\{A_\alpha\}_{\alpha<\kappa}$ una familia de conjuntos nulos para la medida de Lebesgue y sea A su unión. Para cada $\epsilon > 0$, llamamos $\mathbb{P}_\epsilon$ al conjunto de los subconjuntos abiertos de $\mathbb{R}$ de medida $< \epsilon$, con el orden dado por $p \leq q$ si $p \subset q$. Para cada $\alpha < \kappa$, sea $D_\alpha = \{p \in \mathbb{P}_\epsilon \mid A_\alpha \subset p\}$ y vamos a ver que es denso. Dado $p \in \mathbb{P}_\epsilon$, como A_α es nulo, existe una unión numerable de intervalos abiertos q tal que $A_\alpha \subset q$ y $m(q) < \epsilon - m(p)$. Entonces $d = p \cup q$ cumple $m(d) \leq m(p) + m(q) < \epsilon$, luego $d \in \mathbb{P}_\epsilon$, $d \in D_\alpha$, $d \leq p$.

[257] Esto responde negativamente al problema 6 de la página 55. Por otra parte, Solovay demuestra en el trabajo que es consistente que $\mathbb{R} \cap L$ sea un ejemplo de conjunto de cardinal $\aleph_1$ que no es medible Lebesgue, por lo que tampoco se puede demostrar lo contrario. Este $\mathbb{R} \cap L$ es $\mathbf{\Sigma}^1_2$ y responde también al problema 8.

Puede probarse que $\mathbb{P}_\epsilon$ cumple la condición de cadena numerable. Admitiendo esto, podemos aplicar $\mathrm{AM}(\aleph_1)$ y concluir que existe un filtro G en $\mathbb{P}_\epsilon$ que corta a todos los conjuntos D_α. Esto significa que $H = \bigcup G$ es un abierto en $\mathbb{R}$ tal que $A \subset H$. Vamos a probar que $m(H) \leq \epsilon$. Así, tendremos que A puede cubrirse por abiertos de medida $\leq \epsilon$ para todo $\epsilon > 0$, y eso implica que A es nulo.

Si $m(H) > \epsilon$, puede probarse que existen[258] $\{p_i\}_{i<n}$ en G tales que $m(p_0 \cup \cdots \cup p_{n-1}) > \epsilon$. Pero, como G es un filtro, dos condiciones cualquiera de G se extienden a otra en G, y lo mismo vale para un número finito, es decir, tendría que existir $p \in G$ tal que $p_0 \cup \cdots \cup p_{n-1} \subset p$, pero entonces la medida de la unión sería menor o igual que $m(p) < \epsilon$. ∎

6. $\mathrm{AM}(\kappa)$ implica que la unión de κ conjuntos medibles Lebesgue es medible Lebesgue y, si son disjuntos dos a dos, la medida de la unión es la suma de las medidas.

   Esto es una consecuencia de (5) que se prueba sin necesidad de AM. En efecto, sea $\{A_\alpha\}_{\alpha<\kappa}$ una familia de conjuntos medibles Lebesgue, y sea A su unión. No perdemos generalidad si suponemos que $A \subset I = [0,1]$. Sea $A' = I \setminus A$. Por definición de medida exterior (véase la sección 19 en la página 33) existe una unión numerable de intervalos abiertos, G_n, tal que $A' \subset G_n$ y $m(G_n) \leq m_e(A') + 1/n$, luego, llamando G a la intersección de los G_n, resulta que $A' \subset G$ y $m_e(A') = m(G)$. Llamando $C = I \setminus G$, tenemos que $C \subset A$ y $m(C) = m_i(A)$.

   Entonces $m(A_\alpha \setminus C) = 0$, luego, por (5), la unión de todos estos conjuntos, que es $A \setminus C$, es nula, luego $A = C \cup (A \setminus C)$ es medible Lebesgue.

   Si los A_α son disjuntos dos a dos, sólo una cantidad numerable de ellos puede tener medida positiva (o de lo contrario, habría una cantidad no numerable con medida $> 1/n$, y tomando n de ellos tendríamos que la unión tiene medida > 1, lo cual es absurdo. Si llamamos $I \subset \kappa$ al conjunto numerable de los índices α tales que A_α no es nulo, tenemos que

$$m(A) = m\Big(\bigcup_{\alpha\in I} A_\alpha\Big) + m\Big(\bigcup_{\alpha\in\kappa\setminus I} A_\alpha\Big) = \sum_{\alpha\in I} m(A_\alpha) = \sum_{\alpha<\kappa} m(A_\alpha),$$

   donde hemos usado que, (5), la unión de κ conjuntos nulos es nula. ∎

7. $\mathrm{AM}(\aleph_1)$ implica que todo conjunto $\mathbf{\Sigma}^1_2$ es medible Lebesgue.

   Esto es consecuencia de (6) y de un resultado de la teoría descriptiva de conjuntos según el cual todo conjunto $\mathbf{\Sigma}^1_2$ es unión de $\aleph_1$ conjuntos de Borel. ∎

8. AM implica que no existen cardinales medibles $\kappa \leq 2^{\aleph_0}$.

En los usos que hemos mostrado del axioma de Martin, la condición de cadena numerable no se usa para nada, salvo que hay que comprobar que la cumple el conjunto de condiciones al que queremos aplicarle el axioma. Esto será más o menos molesto, pero necesario:

$\mathrm{AM}(\aleph_1)$ sería falso si elimin——ramos la exigencia de la condición de cadena numerable.

Demostración: Por ejemplo, basta tomar como $\mathbb{P}$ el conjunto de las aplicaciones de un subconjunto finito de ω en ω_1 con el orden dado por $p \leq q$ si y sólo si $q \subset p$. Para cada $n \in \omega$, el conjunto D_n de las condiciones definidas en d es denso (toda condición se puede extender a otra definida en n) y, para cada $\alpha < \omega_1$, el conjunto E_α de las condiciones que toman el valor α también lo es. Si pudiéramos aplicarle $\mathrm{AM}(\omega_1)$, concluiríamos que existe un filtro G que corta a todos estos conjuntos densos, lo que implica que $f_G = \bigcup G : \omega \longrightarrow \omega_1$ suprayectiva, lo cual es imposible. Pero es fácil ver que $\mathbb{P}$ no cumple la condición de cadena numerable. ∎

En particular, Solovay y Tennembaum (junto con la construcción previa de Tennenbaum de un modelo con un árbol de Suslin) habían demostrado la independencia de la hipótesis de Suslin:

La hipótesis de Suslin no es demostrable ni refutable en ZFC.

Más adelante Jensen demostraría que la existencia de un árbol de Suslin también se deduce del axioma de constructibilidad.

[258] Esto se debe a que la medida de Lebesgue es regular, lo que implica que existe un compacto $K \subset H$ con $m(K) > \epsilon$, y los elementos de G forman un cubrimiento abierto de K.

100 El formalismo moderno En **1970** se cumplían 100 años de la publicación del primer artículo de Cantor sobre series trigonométricas, que llevó al descubrimiento de los ordinales y los cardinales infinitos. El desarrollo de la teoría abstracta de conjuntos había provocado "la gran crisis de los fundamentos," pero para entonces ya estaba ampliamente superada. La matemática moderna "oficial" es formalista, pero no exactamente en el sentido formulado por Hilbert, sino en el sentido que describe muy bien Curry en la introducción de su *Lógica matemática,* de 1963, que hemos pospuesto hasta esta última sección porque nos sirve muy bien para recapitular buena parte de lo que hemos venido analizando hasta aquí:

> *Pero, ¿las matemáticas necesitan certeza absoluta para su justificación? En particular, ¿por qué necesitamos estar seguros de que una teoría sea consistente o de que pueda derivarse de una intuición absolutamente cierta del tiempo puro, antes de usarla? En ninguna otra ciencia hacemos tales exigencias. En física, todos los teoremas son hipotéticos; adoptamos una teoría mientras haga predicciones útiles y la modificamos o la descartamos en cuanto deja de hacerlo. Esto es lo que les pasó a las teorías matemáticas en el pasado, donde el descubrimiento de contradicciones ha llevado a la modificación en las doctrinas matemáticas aceptadas hasta el momento de ese descubrimiento. ¿Por qué no deberíamos hacer lo mismo en el futuro? Al usar las concepciones formalistas para explicar lo que es una teoría, aceptamos una teoría mientras es útil, satisface las condiciones de naturalidad y simplicidad que resultan razonables en ese momento y no se sabe que nos lleven a error alguno. Debemos mantener nuestras teorías bajo vigilancia para comprobar que se cumplen esas condiciones y obtener todas las presuntas evidencias de adecuación que podamos. El teorema de Gödel sugiere que eso es todo lo que podemos hacer y una filosofía empírica de la ciencia sugiere que eso es todo lo que deberíamos hacer. Más aún, como la utilidad es relativa a un propósito, teorías constituidas diferentemente pueden ser aceptadas para propósitos diferentes, de modo que una matemática intuicionista y otra clásica pueden coexistir una al lado de la otra.*

Pero, a la vez que Curry expresa perfectamente la concepción formalista moderna de las matemáticas, también pone en evidencia las inconsistencias a las que frecuentemente lleva el formalismo mal entendido. Por ejemplo, Curry explica que el formalismo es la única posición que puede dotar a las matemáticas de un concepto objetivo de rigor y, en esta línea, analiza así la filosofía intuicionista:

> *La metafísica intuicionista, por otra parte, es muy oscura. En la tesis de Brouwer la intuición primordial se vincula a una intuición del tiempo* a priori *(quizá similar a la intuición kantiana a priori del espacio y el tiempo, aunque la geometría no euclídea acabó con la concepción* a priori *del espacio), pero no sé hasta que punto los intuicionistas actuales consideran esencial esta idea. Sin embargo, parecen seguir postulando las características siguientes de su intuición básica: (1) Es una actividad intelectual de la mente humana. (2) Es independiente del lenguaje; la construcción intuicionista no necesita vincularse a ninguna expresión lingüística y, aunque el lenguaje es necesario para comunicar las conclusiones, el lenguaje puede proporcionar únicamente una reproducción imperfecta del pensamiento puro, que es exacto por sí mismo. (3) No puede ser descrita por ningunas reglas preestablecidas: una demostración es válida cuando es una construcción cuyos pasos individuales son evidentes de forma inmediata; no importa qué reglas se hayan dado, que siempre podría encontrarse una prueba válida que no se adecúe a ellas. (4) Tiene un carácter* a priori, *en el sentido de que es independiente de la experiencia. (5) Es una realidad objetiva, en el sentido de que es la misma en todos los seres pensantes.* [...]
>
> *De acuerdo con la tercera de estas propiedades, es imposible dar una descripción exacta de lo que es una demostración rigurosa. Una construcción es válida cuando es una serie finita de pasos cada uno de los cuales es directamente evidente a la mente. Si dos mentes discrepan sobre lo que es directamente evidente, no hay un criterio objetivo por el que esa discrepancia pueda ser resuelta. Esto muestra que el criterio de "demostración rigurosa" es vago. Sobre su carácter metafísico, basta señalar que, desde ciertos puntos de vista filosóficos, las cinco características son inaceptables, al menos conjuntamente. Un empirista, por ejemplo, mantendría que no hay conocimiento* a priori, *luego no hay ninguna intuición* a priori *que pueda usarse como criterio de verdad. Similarmente, algunos pensadores han defendido la tesis de que no hay pensamiento sin lenguaje. Finalmente, incluso si pudiéramos asegurar la existencia de una intuición que tuviera las cuatro primeras características, parece muy dudoso que fuera a tener la quinta, y sin la quinta característica, la matemática intuicionista no es una ciencia en absoluto. Por lo tanto el intuicionista requiere la existencia de una intuición* a priori *que es objetiva y prelingüística y, aunque este supuesto ontológico es aceptable*

> *para ciertos tipos de filosofía, aún así es un supuesto para todas ellas, que para otros puntos de vista filosóficos es altamente dudoso y metafísico.*

Así, Curry no distingue entre lo que supondría la pretensión de fundamentar todas las matemáticas en la intuición (lo que daría lugar a polémicas insolubles sobre si el tercio excluso es intuitivamente válido o no, o si hacer infinitas elecciones simultáneas o sucesivas tiene un significado intuitivo o no), de lo que es admitir que sí que existe un conocimiento intuitivo preciso que reúne esas cinco características (aunque la segunda sería secundaria), basada en esa intuición temporal pura y *a priori* kantiana que ha mencionado en Brouwer (en incluso en la intuición espacial, cuyo carácter *a priori* no se ve afectado en absoluto por la existencia de geometrías no euclídeas) y que permite justificar lo que el formalismo necesita, que es un fundamento objetivo para la construcción y valoración de los sistemas formales. El propio Curry, desde el primer capítulo de su libro, va a hablar de "lenguajes", "procesos", "clases", "cuestiones bien definidas", etc. Incluso llega a decir:

> *A menudo tendremos que formular, mediante el metalenguaje, propiedades (o relaciones) que definen en un sentido estrictamente intuitivo (o material) una totalidad de elementos o nociones. Para distinguir esas totalidades intuitivas de los conjuntos o clases que se forman más adelante* (y que se conciben más bien como objetos de cierto estudio teórico y no como nociones intuitivas), las llamaremos* clases conceptuales *(o relaciones). Los elementos elegibles para ser considerados miembros de tales clases se llamarán elementos admisibles.*
>
> *En partes más elevadas de la lógica, como la teoría de conjuntos, pero no en este libro.*

Y sigue teorizando sobre estas clases intuitivas, sin especificar ningunas reglas prefijadas para razonar sobre ellas. Simplemente incide en el carácter constructivo de los razonamientos. El capítulo tercero de su libro lo dedica a lo que llama *epiteoría,* que no es sino lo que normalmente se llama *metateoría* o *metamatemática,* así que usaremos estas denominaciones más habituales. La primera sección se titula, precisamente, *La naturaleza de la metamatemática.* Como ejemplos de metateoremas cita los teoremas de incompletitud de Gödel, y también el teorema de Löwenheim-Skolem, o el teorema de completitud de Gödel, de los que dice que "son de naturaleza no constructiva", en los que hay involucrados supuestos intuitivos no finitistas, pero a continuación aclara que en su libro sólo tratará de metateoremas constructivos. A continuación se detiene a discutir en qué sentido se puede decir que tales metateoremas son verdaderos, y trata de vincular todo a la naturaleza constructiva de las afirmaciones involucradas. Sólo al final de su libro, cuando ya no tiene más remedio, se acerca a los aspectos constructivos del teorema de completitud de Gödel, como lo presenta Kleene en su *Lógica para matemáticos,* pero sin llegar a enunciar el teorema en sí. Curry presenta el concepto de "modelo" diciendo: *Las nociones que hemos usado aquí están relacionadas con el concepto ordinario de "modelo",* y luego lo introduce "con pinzas", le dedica apenas un párrafo y termina diciendo: *En el estudio de los modelos se adopta un punto de vista platonista y no se incide en el carácter constructivo.* Es su forma de decir que no va a ocuparse más del concepto.

En resumen, aunque Curry trata en todo momento de explicitar de qué habla y en qué sentido dice lo que dice, con ello no hace sino poner en evidencia que está apelando, a veces implícitamente, y a veces incluso explícitamente, a esa intuición cuya existencia ha tachado de metafísica, sólo que no para abordar cuestiones en las que podría haber polémicas (que pueden zanjarse dejando claro que si es polémico si algo es intuitivamente cierto, es que NO es intuitivamente cierto), sino para abordar lo que es inexcusable abordar, y es la fundamentación de la matemática formal.

Sus intentos de negar que se apoya en la intuición son equiparables a los intentos de los logicistas de negar que se apoyaban en la aritmética intuitiva, ante los que Poincaré no necesitó más que señalar las evidencias de lo contrario:

> *El Sr. Couturat repite a menudo que esta nueva lógica es completamente independiente de la idea de número. No me divertiré contando cuántas veces su exposición contiene adjetivos numerales, tanto cardinales como ordinales, o adjetivos indefinidos, como "varios". Citemos, no obstante, algunos ejemplos:*
>
> *El producto lógico de* dos *o* más *proposiciones es...*
>
> *Todas las proposiciones son susceptibles de tomar únicamente* dos *valores: verdadero y falso.*
>
> *El producto relativo de* dos *relaciones es una relación.*
>
> *Una relación se da entre* dos *términos ..., etc., etc.*

> *A veces este inconveniente no será imposible de evitar, pero otras veces es esencial. Una relación no se entiende sin dos términos. Es imposible tener una intuición de la relación sin tener al mismo tiempo la de estos dos términos y sin recalcar que son dos, pues para que la relación sea concebible hace falta que sean dos y sólo dos.*

De hecho, la aversión que Curry muestra por admitir que toda su metamatemática se sustenta en un uso riguroso de la intuición, hace que destierre de su libro aquellos metateoremas en los que ya no podría disimular que esto es así, los que tienen componentes con sentido intuitivo, pero no constructivos, como son el teorema de completitud y el teorema de Löwenheim-Skolem, teoremas que es artificial desterrar cuando lo que procedería es justificar que el cálculo deductivo adoptado cumple la función que se pretende que cumpla, que es lo que garantiza el teorema de completitud.

> *En cuanto al platonismo, no haría falta decir que atribuir realidad a todas las nociones no finitistas de las matemáticas es un supuesto metafísico que resulta altamente repulsivo para algunos tipos de mentes, entre ellas las de los intuicionistas. Por lo tanto, la situación en lo que respecta al carácter metafísico es bastante peor para el platonismo que para el intuicionismo. En lo tocante al criterio de rigor, en cambio, la situación es bastante mejor, porque muchos platonistas admiten la posibilidad de formalización (en un sentido que explicaremos ahora). De hecho, la mayoría de las teorías platonistas no tienen más criterio de rigor que el derivado de la formalización, y el criterio es preciso en la medida en que la formalización es estricta y minuciosa.*

Aquí Curry vuelve a describir acertadamente lo que es la concepción moderna de las matemáticas: uno puede ser platonista, o intuicionista, o lo que quiera, pero al final, las cuentas que debe rendir como matemático consisten en presentar formalmente sus demostraciones (o en un contexto que deje claro que cuanto dice es formalizable en una teoría axiomatica especificada o especificable). Todo lo que no sea eso sólo tiene cabida en el caso de la metamatemática informal destinada a fundamentar la matemática formal. Más allá de este caso, estaremos hablando de filosofía de las matemáticas, pero no de matemáticas. La metamatemática intuitiva informal construye la matemática formal que sirve de línea divisoria clara y precisa entre la matemática (distinta de la metamatemática) y la filosofía de las matemáticas (un filósofo puede hablar de lo que quiera, en los términos que quiera).

> *En el próximo capítulo nos ocuparemos de estudiar detalladamente ciertos tipos de formalismo. Veremos que el formalismo puede proporcionar un concepto de demostración rigurosa que es objetivo y preciso, y que este concepto está libre de supuestos metafísicos del tipo que acabamos de discutir para el platonismo y el intuicionismo. Puesto que es deseable concebir las matemáticas como una ciencia objetiva libre de supuestos metafísicos, en este libro adoptamos un punto de vista formalista.*

Este pasaje es delicado de analizar, porque, ciertamente, el formalismo está libre de supuestos metafísicos, pero no lo estaría si la existencia de una intuición que nos permite atribuir un significado objetivo a ciertas afirmaciones se considera un supuesto metafísico. Aquí es inevitable darle la razón a lo que ya explicaba Kleene en su *Introducción a la metamatemática:*

> *La metateoría pertenece a la matemática intuitiva e informal (a menos que la metateoría se formalice en una metametateoría, cosa que aquí no consideramos). La metateoría se expresará en lenguaje ordinario, con signos matemáticos, como variables metamatemáticas, introducidos según sea necesario. Las afirmaciones de la metateoría deben tener un significado. Las deducciones deben ser convincentes. Deben proceder mediante inferencias intuitivas y no, como las deducciones en la teoría formal, mediante la aplicación de reglas establecidas. Se han establecido reglas para formalizar la teoría objeto, pero ahora debemos comprender, sin reglas, cómo funcionan esas reglas. Una matemática intuitiva es necesaria para definir la matemática formal.*

o en su *Lógica matemática:*

> *Uno de los problemas de la axiomática formal es demostrar que los sistemas axiomáticos no son vacíos. Sin embargo, un sistema de objetos utilizado como interpretación a menudo se deriva de otra teoría axiomática; entonces tenemos una regresión, que simplemente nos lleva a la cuestión de la importancia de dicha teoría axiomática. Si en ninguna etapa se realiza una aplicación fuera de la axiomática formal, toda la actividad parecerá fútil. Por lo tanto, concluimos que, si no vamos a adoptar un nihilismo matemático, las matemáticas formalmente axiomatizadas no deben ser la*

> *totalidad de las matemáticas. En algún punto debe haber significado, verdad y falsedad. Como mínimo, cuando decimos que en una teoría axiomática formal dada una determinada proposición es un teorema, debemos creer que esto es verdad, es decir, que la proposición se sigue de los axiomas, aunque no se tiene en cuenta si la proposición en sí es verdadera, ya que en la axiomática formal las deducciones se llevan a cabo antes de asignar significados a los términos primitivos (o de descartar dicha asignación).*

Y, naturalmente, Curry no desmiente a Kleene, por más que parezca pretenderlo. En su libro no adopta en modo alguno un punto de vista formalista, sino todo lo contrario: su objetivo es fundamentar el formalismo, y para ello se esfuerza por explicar en qué sentido se puede decir que todo lo que dice es verdad, y no en explicar cómo se deduce de unos axiomas inexistentes. Pese a esto, Curry sigue describiendo muy acertadamente el formalismo bien entendido (aunque no parezca entender bien sus fundamentos):

> *No obstante, es necesario hacer algunas observaciones adicionales para clarificar la postura. Naturalmente, estas observaciones requerirán luego de más aclaraciones.*
>
> *En primer lugar, los teoremas de incompletitud de Gödel muestran que ninguna teoría formal puede, por sí sola, agotar las matemáticas. Consecuentemente, el formalismo no tiene que identificarse con el punto de vista de que exista tal teoría. En su lugar, el tipo de formalismo que adoptamos aquí sostiene que la esencia de las matemáticas consiste en el método formal en sí, y que admite toda clase de teorías formales, así como discusiones generales comparativas sobre relaciones entre unas teorías formales y otras y con otras doctrinas. En este sentido las matemáticas son la ciencia de los métodos formales.*

Aquí tenemos una idea importante y novedosa respecto al formalismo de Hilbert: que en realidad no se trata de encontrar una teoría formal "oficial" que excluya cualquier otra, sino que cualquier teoría formal es una teoría matemática (más o menos interesante, que eso ya es otro asunto). Pero luego la enturbia mezclando la matemática como sistema de teorías formales con la metamatemática que estudia las relaciones entre ellas. Ciertamente, la metamatemática se puede formalizar, pero entonces sobraría el "así como", mientras que si Curry se refiere al estudio de esas relaciones entre teorías formales como algo diferente a una teoría formal, entonces está hablando de metamatemática informal, con lo que no tiene sentido que la considere "formalismo", sino más bien, "fundamentación informal del formalismo", que no puede ser formalismo, como Kleene señala irrefutablemente.

> *Una teoría formal contiene por definición ciertos elementos no especificados o parámetros, o, como ya hemos dicho, elementos que se pueden cambiar. Si esos elementos se determinan de una forma material en particular, entonces la teoría así interpretada se convierte en una teoría material.*[259] *Llamemos a una teoría así una teoría material formalizada. Más aún, si las afirmaciones verdaderas de esta teoría formalizada son aceptables desde cierto punto de vista material, diremos que la teoría formal es compatible con dicho punto de vista. Así podemos tener teorías formales compatibles con el platonismo y otras que sean compatibles con el intuicionismo. Pero hay una diferencia fundamental entre una tal teoría material formalizada y una teoría material que es primaria, pues una demostración u otro argumento al que se llega en la teoría formal sigue siendo válido independientemente de la interpretación. Si el rigor se define por la teoría formal —como sucede en muchas formas de platonismo— ese rigor se mantiene como un hecho objetivo tanto si uno acepta como si no los presupuestos de la teoría material. Más aún, formalismos que difieren a este respecto pueden considerarse simultáneamente. Por lo tanto, el formalismo no es una doctrina que excluya o niegue las doctrinas de este o aquel tipo de materialismo; es igualmente independiente de, y compatible con, cualquier forma razonable de materialismo.*

Esto sería del todo exacto salvo por un detalle, y es que el formalismo depende necesariamente de una teoría material primaria, la necesaria para precisar y estudiar, como mínimo, los conceptos de "lenguaje formal", "fórmula", "teorema", etc., pero también de demostrar los hechos que Curry parece dar por evidentes, como que si unos axiomas son verdaderos en una determinada interpretación, entonces todos los teoremas lógicos que se deduzcan de dichos axiomas también lo serán, cosa que Curry no demuestra en su libro porque eso le obligaría a hablar excesivamente de esas clases intuitivas de las que ha confesado que necesita hablar (pero sin pasarse), pues tendría que hablar de modelos, de conjuntos (intuitivos), de relaciones, etc.

[259] Estamos traduciendo por "material" la palabra *contensive,* que a su vez Curry explica que usa para traducir el alemán *inhaltlich* (con contenido).

Curry aún no había cumplido los 12 años cuando murió Poincaré, pero bien podría añadirse su nombre junto a los de Russell y Hilbert en este pasaje:

> *En resumen: los Sres. Russell y Hilbert han realizado un vigoroso esfuerzo, y han escrito uno y otro un libro lleno de puntos de vista originales, profundos, y a menudo muy ciertos. Estos dos libros nos darán mucho material para pensar, y para aprender de ellos. Algunos de sus resultados, muchos, de hecho, son sustanciales y están destinados a perdurar.*
>
> *Pero decir que han resuelto la controversia entre Kant y Leibniz de manera definitiva y que han destruido la teoría kantiana de las matemáticas es evidentemente falso. No sé si en realidad creen haberlo logrado, pero si es así, se han equivocado.*

Sólo una mínima parte del libro de Curry es matemática formal. La mayor parte es matemática intuitiva informal, como no puede ser de otro modo, ya que su intento es fundamentar el formalismo, tal y como Poincaré señaló certeramente.

La situación es peculiar, pero es realmente la situación en la que se encuentran muchos matemáticos desde la época en que Curry escribió su libro hasta nuestros días: cualquier matemático que suscriba sus tesis formalistas será un perfecto profesional de las matemáticas, concebirá las matemáticas justo como hay que concebirlas para que hoy en día sean consideradas como matemáticas rigurosas y aceptables. Sin embargo, en cuanto se le pregunte por la fundamentación de las matemáticas, sus esquemas se romperán, y nos encontraremos con la situación que cuatro años más tarde señalaría Kreisel:

> *Pero dado que este proyecto* [el programa formalista de Hilbert] *ha fracasado, el progreso posterior utilizará nociones y métodos ajenos a él; de hecho, las principales preguntas fructíferas ni siquiera tienen por qué ser formulables en términos aceptados en este proyecto. Por lo tanto, al aceptar el proyecto formalista, uno no sólo no está dispuesto a apreciar (¡o estudiar!) trabajos más avanzados sobre fundamentos, sino que simplemente no puede hacerlo sin reexaminar sus propias ideas.*

En efecto, no es posible entender la fundamentación formalista de las matemáticas si se piensa que la intuición es un supuesto metafísico, y mucho menos si se piensa que es una forma burda, primitiva y poco fiable de razonamiento. Esto no supone ningún problema en la práctica porque "el matemático medio" no necesita fundamentar las matemáticas. Se las encuentra "ya fundamentadas". Sabe que si se limita a proceder según los criterios de rigor formal que tiene plenamente interiorizados, "lo está haciendo bien" y no va a tener ningún problema (y si apareciera algún problema, supondría el desencadenamiento de una nueva crisis de fundamentos, pero, hoy por hoy, eso se ve como la posibilidad de una invasión alienígena). Pero cuando un matemático que tenga la visión formalista de Curry (que —insistimos— es la "oficial" hoy en día) decide abrir un libro de lógica, aunque sea el propio libro de Curry, no va a entender nada. Es decir, entenderá todos los argumentos, por supuesto, pero no entenderá cómo debe entender esos argumentos en ausencia de un marco axiomático de referencia.

El formalismo que tan sensata y acertadamente describe Curry como forma de concebir la matemática moderna, tiende a degenerar a un "formalismo radical" insostenible, consistente en que uno se acostumbra a concebir el significado de las afirmaciones matemáticas como "algo de andar por casa", como algo de lo que no hay que preocuparse, porque nunca hay que dar cuenta de ello, porque lo que importa es la corrección formal, que cuando se vuelve necesario evaluar un razonamiento en términos de su contenido material y no de su forma, el matemático se encuentra como un urbanita abandonado en medio de la selva: ve peligros donde no los hay, y no los ve donde los hay realmente.

Por ejemplo, un formalista está acostumbrado a usar "para todo" y "existe" sin más restricciones que las que impone la lógica, y, en efecto, eso es legítimo en la matemática formal, pues ésta es en última instancia eso mismo: una estructura que fundamente cuantificar arbitrariamente, igual que un espacio topológico es una estructura que fundamente hablar de continuidad, y le cuesta concebir, por ejemplo, las objeciones que Poincaré ponía al uso y abuso de la palabra "todos":

> *Es la creencia en la existencia del infinito actual lo que da origen a las definiciones impredicativas. Me explico: en estas definiciones aparece la palabra "todos", como hemos visto en los ejemplos citados más arriba. La palabra "todos" tiene un sentido bien claro cuando se aplica a un número finito de objetos. Para que siga teniéndolo cuando los objetos son infinitos, haría falta que hubiera un infinito actual. En caso contrario "todos" los objetos no podrían concebirse como dados anteriormente a*

> *la definición, y entonces, si la definición de una noción N depende de "todos" los objetos A, esta puede caer en un círculo vicioso si entre los objetos A los hay que no pueden definirse sin hacer que intervenga la propia noción N.*
>
> *No existe el infinito actual, los cantorianos lo han olvidado y han caído en la contradicción. Es cierto que el cantorismo ha prestado servicios, pero esto ha sucedido cuando ha sido aplicado a un problema verdadero, cuyos términos estaban claramente definidos y por ello podían avanzar sin preocupaciones.*

En realidad, este predicativismo de Poincaré está ligeramente "anticuado" en la medida en que los lógicos modernos que se declaran predicativistas (o que estudian el predicativismo) admiten las definiciones impredicativas de números naturales. Por ejemplo, en sentido estricto, tal y como lo concibe Poincaré, definir un número natural n como "el mínimo que cumple tal propiedad" es una definición impredicativa, porque define n como el único número natural que tiene la "propiedad tal" y *para todo* número natural m que también la tenga se cumple $n \leq m$. Por lo tanto, supone definir un número natural en función de la totalidad de los números naturales, uno de los cuales es el propio número que se está definiendo. Sin embargo, esto no se considera problemático, porque los números naturales "son los que son", no hay problema, pese a las reticencias de Poincaré, en concebirlos intuitivamente como un infinito actual existente. En palabras de Weyl (en *El continuo*): *La intuición de* [el concepto de] *iteración nos asegura que el concepto de "numero natural" está extensionalmente determinado* (que es una forma técnica de decir que "los números naturales son los que son", que podemos hablar de todos ellos como un todo, exactamente igual que hacemos con los conjuntos finitos). Dicho de otro modo: cuando definimos un número natural, aunque hagamos referencia a la totalidad de los números naturales, acabaremos seleccionando uno de ellos, uno de los que "ya estaban ahí" antes de que decidiéramos fijarnos en él concretamente.

Sin embargo, esto ya no se aplica necesariamente cuando pretendemos definir, por ejemplo, un subconjunto de $\mathbb{N}$ (o una sucesión de números naturales, etc.) haciendo referencia a la totalidad de los subconjuntos de $\mathbb{N}$ (o de las sucesiones, etc.), porque en ese contexto ya no podemos decir que tenemos "extensionalmente determinada" por la intuición una totalidad bien definida, de la cual, con cada definición, simplemente estamos destacando uno de sus elementos, sino que, si una definición es impredicativa, no deja claro en absoluto, al menos *a priori,* qué es lo que está definiendo, porque la afirmación "todos los subconjuntos de $\mathbb{N}$" no tiene ningún significado intuitivo preciso *a priori.* En este punto es razonable recordar a Skolem:

> *Presumiblemente, aún no se ha demostrado que el sistema axiomático de Zermelo sea consistente, y sin duda será muy difícil hacerlo. En particular, las estipulaciones no predicativas que rigen la formación de conjuntos causarán dificultades. No es descabellado pensar en los axiomas como principios generadores de algún tipo; generamos nuevos conjuntos según ciertas reglas a partir de conjuntos ya conocidos. Si, ahora, la formación de conjuntos fuera una mera cuestión de construir cada nuevo conjunto únicamente a partir de un número finito de conjuntos anteriores, podríamos fácilmente verificar, a través de un proceso infinito, si los axiomas son consistentes. Pero la dificultad es que tenemos que formar algunos conjuntos cuya existencia depende de* todos *los conjuntos. Entonces tenemos lo que se llama una definición no predicativa. Poincaré criticó este tipo de definición y la consideró la verdadera debilidad lógica de la teoría de conjuntos.*

Sin necesidad de entrar en el problema de la teoría de conjuntos en general, pensemos simplemente en lo que supone aceptar una aritmética de segundo orden que permita hablar de subconjuntos de números naturales. Nos referimos a una teoría sobre un lenguaje formal con dos tipos de variables: variables de primer orden, que se interpretan como números naturales, y variables de segundo orden, que se interpretan como subconjuntos de $\mathbb{N}$. En ella podemos tomar como axiomas todos los axiomas de Peano y, si además, queremos tomar como esquema axiomático que

$$\bigvee A \bigwedge x(x \in A \leftrightarrow \phi(x)),$$

donde A es una variable de segundo orden y ϕ es una fórmula de primer orden, en el sentido de que puede tener parámetros de primer y segundo orden, pero en la que todas las variables cuantificadas son de primer orden, esto no supone ningún problema, pues, para que se cumplan estos axiomas, basta considerar como "subconjuntos de $\mathbb{N}$" a los *subconjuntos aritméticos,* es decir, los subconjuntos de $\mathbb{N}$ definibles mediante una fórmula aritmética que tenga sólo variables de primer orden.

La clase de los subconjuntos aritméticos de $\mathbb{N}$ es una clase numerable que se puede considerar bien definida intuitivamente. Desde el momento en que sabemos enumerar todas las fórmulas aritméticas y también todas las n-tuplas de números naturales que pueden tomar como parámetros, podemos enumerar explícitamente todos

los conjuntos aritméticos, por lo que podemos decir que sabemos de lo que hablamos cuando hablamos de la totalidad de los subconjuntos aritméticos, por lo que tiene sentido decir "para todo conjunto aritmético". Y estos conjuntos bastan como interpretación de las variables de segundo orden para que se cumpla el esquema axiomático anterior. Si la fórmula ϕ tiene parámetros de segundo orden, cuando evaluamos cada uno de ellos en un conjunto aritmético, podemos sustituir en $\phi(x)$ cada parámetro de segundo orden por la fórmula que lo define, y así obtenemos una fórmula equivalente $\psi(x)$ sin parámetros de segundo orden, por lo que el conjunto definido por ϕ no es sino el conjunto aritmético definido por ψ.

En cambio, si queremos extender el esquema axiomático anterior de modo que $\phi(x)$ pueda tener cuantificaciones de segundo orden (que tengan que interpretarse como "para todo subconjunto de $\mathbb{N}$" o "existe un subconjunto de $\mathbb{N}$"), entonces ya no sabemos qué subconjuntos de $\mathbb{N}$ tendríamos que tomar para que se cumpla este axioma. Como dice Skolem, no podemos ir añadiendo subconjuntos de $\mathbb{N}$ a un modelo mediante un proceso iterativo análogo al que nos permite construir todos los números naturales, porque necesitamos asegurar la presencia de conjuntos que satisfagan definiciones que dependen de la totalidad de los subconjuntos de $\mathbb{N}$ del modelo que pretendemos construir, de los ya construidos, y también de los pendientes de construir. Ésta es la frontera entre el predicativismo moderno y el impredicativismo moderno. Las definiciones mediante fórmulas aritméticas con cuantificadores de primer orden son impredicativas en el sentido estricto que rechazaba Poincaré, pero hoy en día se consideran predicativas (o, al menos, no son rechazadas por el predicativismo aunque sean impredicativas) porque se considera que cada una de ellas determina intuitivamente un subconjunto de $\mathbb{N}$ bien definido. En cambio, una definición mediante una fórmula que incluya una cuantificación de segundo orden, es "esencialmente impredicativa", y es rechazada por el predicativismo (o, al menos, no es aceptada *a priori*) porque si tratamos de concebir qué clase de objetos son necesarios para que tengan sentido tales definiciones nos encontramos con que necesitaríamos conocerlos todos de antemano, es decir, que nos resulta imposible, no ya construirlos, sino meramente formarnos una imagen intuitiva de en qué consiste "la totalidad de ellos" sin presuponer que, de algún modo, previo a toda intuición, ya está determinada "la totalidad de ellos".

Pero para un matemático formalista descendido al mundo de la matemática significativa (o material, no formal) estas distinciones cruciales entre unos *paratodos* y otros le resultan tan artificiales e irrelevantes como para el urbanita abandonado en la selva lo es la distinción entre frutas comestibles y frutas venenosas, ya que él está acostumbrado a que todas las frutas de la frutería tengan su certificado de sanidad.

Por el contrario, el formalista "desubicado" se mostrará receloso de hechos que no tienen nada de particular, como manejar conceptos del estilo de "propiedad bien definida" que no admiten una definición, ni buena ni mala, sino que es en cada uso concreto de este concepto cuando hemos de valorar si realmente estamos o no ante una propiedad bien definida, o que un concepto pueda no estar bien definido hasta que no se demuestra una propiedad sobre él. Es el caso del teorema de completitud. Pensemos, por ponernos en el caso más simple:

> Una fórmula α es un teorema lógico si y sólo si es verdadera en todo modelo de su lenguaje formal.

El formalista "desubicado" tenderá a aceptar "ingenuamente" el buen sentido de "todo modelo", porque tiene tendencia a confiar irreflexivamente en todos los "paratodos", ya que en la matemática formal (o por lo menos, en las teorías formales con las que suele trabajar, ya que hay muchas teorías formales que restringen la cuantificación) todos ellos son legítimos. Pero, si llega a convencerse de que ese "todo modelo" no tiene en principio ningún significado intuitivo, ya que no tenemos ninguna representación intuitiva de lo que es la totalidad de los modelos que pueden definirse para un lenguaje formal dado, le resultará desconcertante que se le diga que, después de todo, el enunciado anterior sí que tiene un significado intuitivo preciso, pero sólo gracias a su demostración. En efecto, en ella se ve que si α no es un teorema lógico, podemos construir, no de forma efectiva, pero sí de forma intuitivamente precisa, un modelo concreto en el que α no es verdadera. Así, el enunciado anterior tiene un sentido intuitivo preciso porque puede reformularse como:

> Dada una fórmula α de un lenguaje formal, o bien es un teorema lógico (lo cual tiene una interpretación intuitiva precisa), o bien sabemos determinar intuitivamente un modelo de dicho lenguaje en el que no es verdadera.

Y este desconcierto se agrava cuando el formalista radical se encuentra con que muchos libros de lógica que teóricamente deberían resolver sus dudas, lo cierto es que no lo hacen, porque, para los lógicos, la fundamentación de la matemática ya no es un problema, y por ello, cuando escriben libros de lógica, su interés es hablar de lógica, no de fundamentar las matemáticas, y la forma más cómoda de hablar de lógica, como de cualquier otro contenido matemático, es hacerlo en el marco de la teoría de conjuntos, y así lo hacen. Ya hemos visto

que es el caso del libro de Mendelson, o el de *Una introducción matemática a la lógica,* publicada por Herbert Bruce Enderton en 1972, que es otra referencia clásica de la lógica moderna, cuyo capítulo 0 presenta la teoría de conjuntos como base para los capítulos posteriores. Este enfoque —que es totalmente legítimo— genera en muchos "formalistas desubicados" la creencia de que hay un tremendo círculo vicioso en la fundamentación de la matemática, pues ésta en última instancia se apoya en la teoría de conjuntos que teóricamente debería ser justificada sin recurrir a ella misma, aunque algunos libros traten de ocultarlo o disimularlo hablando de "la intuición", y otras entelequias similares.

En resumen, el formalismo tiene una doble vertiente. Por una parte proporciona el fundamento preciso y riguroso que la matemática necesita, tal y como Curry describe muy lúcidamente y, por otra, cuando los matemáticos se acomodan a él y olvidan (o sin llegar a haber conocido nunca) su fundamento intuitivo, en su versión radical, se convierte en lo que decía Kreisel:

> *Formalismo: un obstáculo para reconocer el progreso cuando se observa.*

Capítulo II

Epílogo al capítulo I

Es prácticamente imposible resumir en un espacio razonable y con el nivel de detalle que hemos dado en el capítulo I los avances en el terreno de la teoría de conjuntos en el último medio siglo, desde 1970 hasta la actualidad, y mucho menos presentarlo en orden cronológico como hemos hecho en dicho capítulo, pues ello llevaría a continuos saltos de un tema a otro. No obstante, dedicamos este capítulo a describir brevemente cómo han evolucionado algunos de los temas tratados allí.

2.1 Cardinales grandes

En el capítulo I hemos hablado de cardinales inaccesibles, $\mathbb{R}$-medibles, medibles, débilmente compactos y de Ramsey. Todos ellos son ejemplos de lo que se conoce como *cardinales grandes*. Son cardinales cuya existencia no se puede demostrar en ZFC porque implican la consistencia de ZFC. Más aún, unos implican la consistencia de que existan otros, por lo que los cardinales grandes se ordenan en una compleja jerarquía según varios criterios que no coinciden exactamente. En las dos páginas siguientes podemos ver dos esquemas con algunos de los cardinales grandes conocidos hoy en día (y la relación dista mucho de ser exhaustiva). Así, por ejemplo, el cardinal de Erdős $\kappa(\omega)$ (si existe) tiene por debajo $\kappa(\omega)$ cardinales inefables, y si κ es inefable, tiene por debajo κ cardinales casi inefables, y si κ es casi inefable, tiene por debajo κ cardinales sutiles, etc.

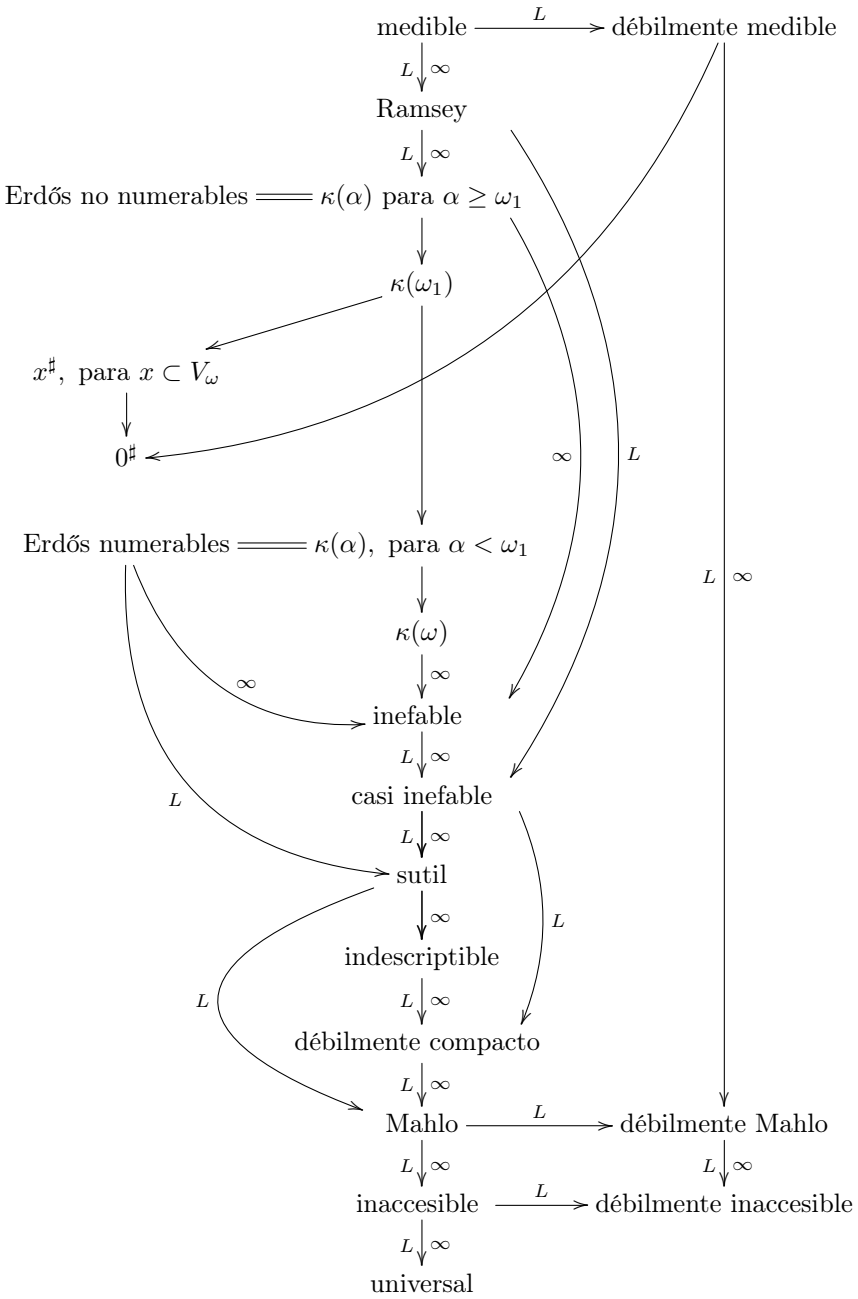
Una de las razones por las que los cardinales grandes son interesantes es porque son ingredientes necesarios en muchas pruebas de consistencia. Por ejemplo, Solovay había demostrado la consistencia de que todo subconjunto de $\mathbb{R}$ es medible Lebesgue suponiendo la consistencia de ZFC más la existencia de un cardinal inaccesible. Durante mucho tiempo se pensó que dicha hipótesis debía de ser prescindible, pero en 1984 Saharon Shelah (que se había doctorado en 1969 bajo la dirección de Michael Oser Rabin, que a su vez se había doctorado en 1956 bajo la dirección de Church) demostró que si todo subconjunto de $\mathbb{R}$ de tipo de $\mathbf{\Sigma}^1_3$ es medible Lebesgue, entonces $\aleph_1$ es un cardinal inaccesible "a ojos de alguien que viva en L". Por lo tanto, es imposible demostrar la consistencia de que todo subconjunto de $\mathbb{R}$ es medible Lebesgue (o meramente la de que lo es todo conjunto $\mathbf{\Sigma}^1_3$) sin suponer la consistencia de que existe un cardinal inaccesible.[1]

Otro ejemplo: Solovay demostró (página 285) que la consistencia de que la medida de Lebesgue se pueda extender a $\mathcal{P}\mathbb{R}$ es equivalente a la consistencia de que exista un cardinal medible. La diferencia es que la existencia de una extensión de la medida de Lebesgue es algo que no es trivial en absoluto, y nada nos dice que no pueda ser imposible. En cambio, que para que un cardinal medible κ basta con que exista un cardinal medible Ulam, es decir, un cardinal κ con un ultrafiltro σ-completo en κ (página 241). Esta afirmación es mucho más elemental y su consistencia se puede considerar mucho más plausible. Con esto hemos reducido la consistencia de una afirmación dudosa a la de otra cuya consistencia se puede considerar plausible, sobre todo

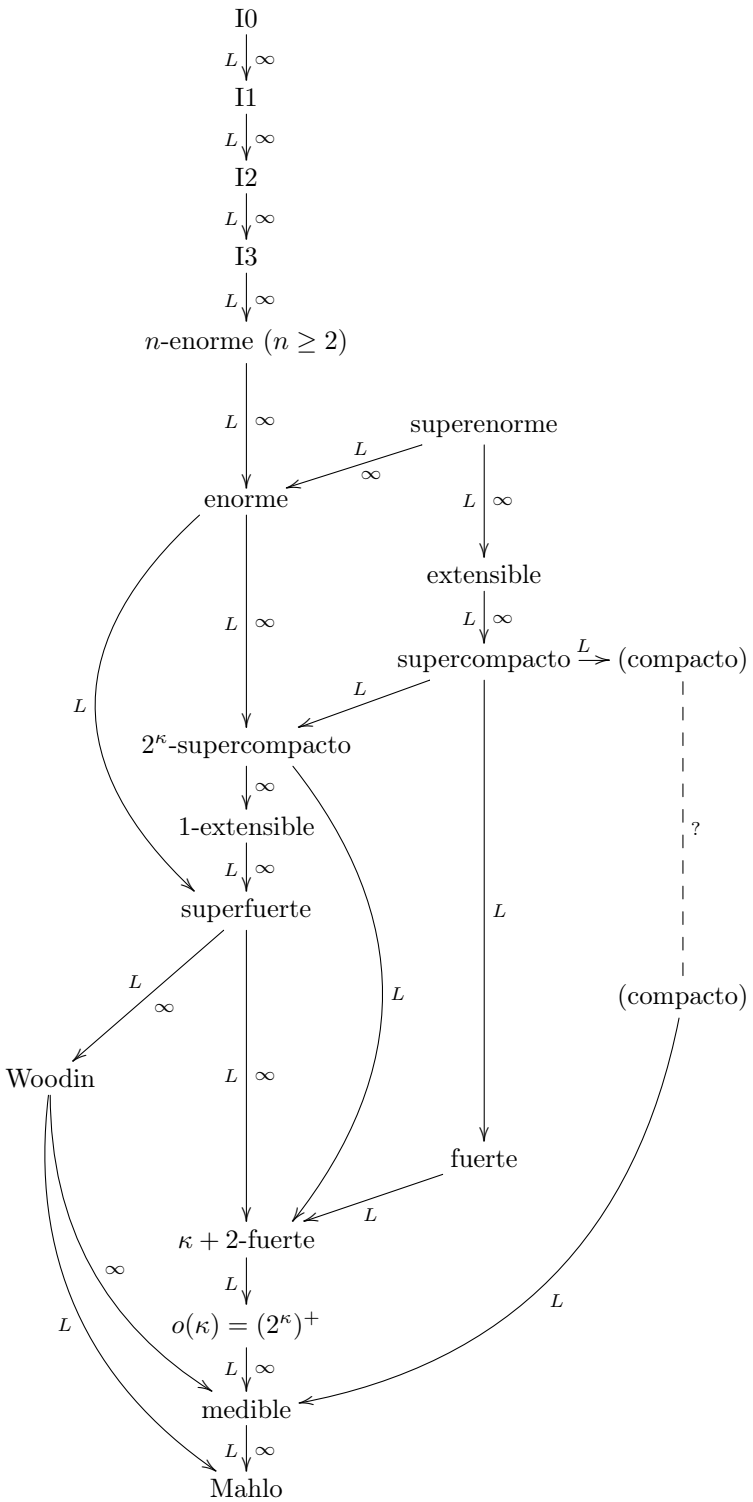
[1] Esto es una aplicación típica del segundo teorema de incompletitud de Gödel. Llamemos FI a la sentencia que afirma la existencia de un cardinal inaccesible y M a la sentencia que afirma que todo conjunto $\mathbf{\Sigma}^1_3$ es medible Lebesgue. Por el teorema de Shelah, si ZFC + FI fuera contradictorio, en dicha teoría podríamos demostrar, por ejemplo, que $0 \neq 0$, luego ZFC + M sería contradictorio, ya que en esta teoría $\aleph_1$ es inaccesible en L, luego podríamos demostrar que $0 \neq 0$ en L, pero eso es lo mismo que $0 \neq 0$. Así pues, Shelah demostró que $\mathrm{Consis}(\ulcorner \mathrm{ZFC} + \mathrm{M} \urcorner) \to \mathrm{Consis}(\ulcorner \mathrm{ZFC} + \mathrm{FI} \urcorner)$. Si se pudiera demostrar que ZFC + M es consistente sin suponer la consistencia de ZFC + FI, es decir, si se pudiera demostrar $\mathrm{Consis}(\ulcorner \mathrm{ZFC} \urcorner) \to \mathrm{Consis}(\ulcorner \mathrm{ZFC} + \mathrm{M} \urcorner)$, tendríamos que $\mathrm{Consis}(\ulcorner \mathrm{ZFC} \urcorner) \to \mathrm{Consis}(\ulcorner \mathrm{ZFC} + \mathrm{I} \urcorner)$, pero sabemos que en ZFC + FI se puede demostrar $\mathrm{Consis}(\ulcorner \mathrm{ZFC} \urcorner)$ (véase la página 105), luego tendríamos que en ZFC + FI se podría demostrar $\mathrm{Consis}(\ulcorner \mathrm{ZFC} + \mathrm{FI} \urcorner)$, en contra del segundo teorema de incompletitud.

porque los cardinales medibles se han estudiado a fondo, y dan lugar a una teoría que tiene todo el aspecto de ser coherente, y no podemos ver el hecho de que su consistencia no sea demostrable como un indicio de que vaya a ser contradictoria, sino que es una mera consecuencia del teorema de incompletitud de Gödel, que impide demostrar la consistencia de la existencia de cardinales grandes.

Cardinales grandes hasta los cardinales medibles Cada axioma de existencia implica la consistencia de los axiomas situados por debajo. Una flecha $A \longrightarrow B$ indica que la existencia de A implica la existencia de B. Una flecha $A \xrightarrow{L} B$ indica una implicación lógica, es decir, que todo A es B. Una flecha $A \xrightarrow{\infty} B$ indica que la existencia de A implica la existencia de infinitos cardinales B menores. Una doble raya = conecta conceptos equivalentes.



Cardinales grandes por encima de los cardinales medibles



El axioma de determinación Más interesante es el caso del axioma de determinación. En 1953 Gale y Stewart habían demostrado que los cerrados (conjuntos $\mathbf{\Pi}^0_1$) están determinados, y en 1954 Wolfe había probado que también lo están los conjuntos $\mathbf{\Pi}^0_2$. Desde entonces no se había hecho ningún progreso a este respecto, pero en 1975 Martin demostró que todos los conjuntos de Borel (es decir, los conjuntos $\mathbf{\Delta}^1_1$) están determinados.

No podía aspirarse a llegar demasiado lejos en esa línea, pues en 1968 Solovay había demostrado que el axioma de determinación implica que $\aleph_1$ es un cardinal medible (lo que a su vez llevaba a un modelo de ZFC + "existe un cardinal medible"), por lo que la consistencia del axioma de determinación no podía demostrarse sin suponer, al menos, la consistencia de que existe un cardinal medible. En esa línea, en 1970 Martin había demostrado el teorema siguiente:

Si existe un cardinal medible, todo conjunto $\mathbf{\Pi}^1_1$ está determinado.[2]

Este resultado era notable, porque no es un resultado de tipo "si existe un modelo con un cardinal medible, entonces existe otro en el que se cumple tal cosa", sino que muestra una consecuencia directa de la existencia de un cardinal medible. Uno podría pensar que la existencia o no de un cardinal increíblemente grande no tendría que afectar a las matemáticas "terrenales", más allá de que se pueda usar para construir modelos y obtener pruebas de consistencia, pero no. La existencia de un cardinal medible tiene como consecuencia la determinación de una amplia familia de subconjuntos de $\mathbb{R}$.

En 1974 Haim Gaifman (que se había doctorado en 1958 bajo la dirección de Tarski) introdujo unos de los mayores cardinales grandes que se conocen, los cardinales de tipo I1, I2, I3 y en 1980 Martin demostró que si existe un cardinal de tipo I2, entonces los conjuntos $\mathbf{\Pi}^1_2$ están determinados. En este caso, la hipótesis estaba en la cúpula de la jerarquía de los cardinales grandes. Si algunos cardinales eran sospechosos de ser contradictorios, ésos eran los I1, I2, I3 (aunque nadie ha demostrado que lo sean).

En 1984 se doctoró William Hugh Woodin bajo la dirección de Solovay, y demostró que si existe un cardinal aún mayor, que llamó I0, entonces el axioma de determinación se cumple en $L(\mathbb{R})$. En su demostración aisló una clase de cardinales que luego se llamarían *cardinales de Woodin* y demostró que, por ejemplo, la determinación de los conjuntos $\mathbf{\Pi}^1_2$ implica la consistencia de que exista un cardinal de Woodin.

En 1989 Martin y John Robert Steel (doctorado en 1977 bajo la dirección de John West Addison y de Steve George Simpson, que a su vez se habían doctorado en 1955 y 1971 bajo la dirección de Kleene y Sacks, respectivamente) demostraron que si existen infinitos cardinales de Woodin con un cardinal medible por encima, entonces el axioma de determinación se cumple en $L(\mathbb{R})$. En 1999 Woodin demostró que la consistencia del axioma de determinación es equivalente a la consistencia de que existan infinitos cardinales de Woodin.

Notemos que esto no supone renunciar al axioma de elección. Lo que tenemos es (supuesta la consistencia de que existan ciertos cardinales grandes) la consistencia de ZFC más $L(\mathbb{R})$ cumple AD (más el principio ED de elecciones dependientes, de hecho), de modo que "si nos quedamos sólo con los conjuntos de $L(\mathbb{R})$, sólo vemos subconjuntos de $\mathbb{R}$ determinados" (y deja de cumplirse el axioma de elección, naturalmente). En particular, sucede que todo conjunto proyectivo está en $L(\mathbb{R})$, por lo que tenemos la consistencia de ZFC más el *axioma de determinación proyectiva* (ADP), que afirma que todo conjunto proyectivo está determinado.

Nuevamente, no estamos ante una mera prueba de consistencia, sino que la existencia de cardinales grandes implica que una amplia familia de subconjuntos de $\mathbb{R}$ está determinada.

El problema de los cardinales singulares Otro contexto en el que son necesarios cardinales grandes como hipótesis necesarias en pruebas de consistencia es el de lo que se conoce como el *problema de los cardinales singulares.* La función $\kappa \mapsto 2^\kappa$ se conoce como *función del continuo,* y Easton demostró que, sobre los cardinales regulares, podemos suponer que se comporta como queramos, sin más restricción que la monotonía y el teorema de Kőnig. Por ejemplo, si suponemos que

$$2^{\aleph_0} = \aleph_7, \qquad 2^{\aleph_1} = 2^{\aleph_2} = \aleph_{\omega+9}, \qquad 2^{\aleph_3} = \aleph_{\omega_5},$$

cualquier valor que queramos fijar para $2^{\aleph_4} = \aleph_\alpha$ será consistente siempre y cuando $\alpha \geq \omega_5$ y la cofinalidad de $\aleph_\alpha$ sea mayor que $\aleph_4$. En cambio, si κ es un cardinal singular, las posibilidades para 2^κ están sujetas a más restricciones en función de los valores que la función del continuo toma bajo κ. Por ejemplo, llamando $2^{<\kappa}$ al supremo del conjunto $\{2^\mu \mid \mu < \kappa\}$, se cumple:

[2]Esto implica que todo conjunto $\mathbf{\Pi}^1_1$ no numerable contiene un subconjunto perfecto, luego tiene cardinal $\mathfrak{c}$, y es una respuesta posible al problema 30 de la página 55. Por otro lado, el axioma de Martin es compatible con $2^{\aleph_0} > \aleph_1$ y $|\mathbb{R} \cap L| = \aleph_1$, y esto implica que todo subconjunto de $\mathbb{R}$ de cardinal $\aleph_1$ es $\mathbf{\Pi}^1_1$, lo que proporciona una respuesta alternativa. Recordemos (página 93) que todo conjunto $\mathbf{\Pi}^1_1$ tiene cardinal $\leq \aleph_1$ o $\mathfrak{c}$.

Teorema Si κ es un cardinal límite, entonces $2^\kappa = (2^{<\kappa})^{\operatorname{cf}\kappa}$.

DEMOSTRACIÓN: Recordemos que la cofinalidad de κ es el menor cardinal tal que existe una familia $\{\mu_\alpha\}_{\alpha<\kappa}$ de cardinales $\mu_\alpha < \kappa$ tales que $\kappa = \sum_{\alpha<\operatorname{cf}\kappa} \mu_\alpha$. Entonces

$$2^\kappa = 2^{\sum_{\alpha<\operatorname{cf}\kappa}\mu_\alpha} = \prod_{\alpha<\kappa} 2^{\mu_\alpha} \le \prod_{\alpha<\kappa} 2^{<\kappa} = (2^{<\kappa})^{\operatorname{cf}\kappa} \le (2^\kappa)^{\operatorname{cf}\kappa} = 2^{\kappa\operatorname{cf}\kappa} = 2^\kappa,$$

luego todas las desigualdades son igualdades. ∎

Y de aquí se sigue, por ejemplo, que si, para todo $n < \omega$, se cumple $2^{\aleph_n} = \aleph_{\omega+9}$, entonces no queda ningún margen para $2^{\aleph_\omega}$, que tiene que ser necesariamente $2^{\aleph_\omega} = \aleph_{\omega+9}$, pues tenemos que $2^{<\aleph_\omega} = \aleph_{\omega+9} = 2^{\aleph_0}$, luego

$$2^{\aleph_\omega} = (2^{<\aleph_\omega})^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0} = \aleph_{\omega+9}.$$

En general, Lev Bukovský (doctorado en 1966 bajo la dirección de Vopěnka) y Stephen Herman Hechler (doctorado en 1967 bajo la dirección de Solovay) demostraron:

Teorema Si κ es un cardinal singular y la función del continuo es finalmente constante por debajo de κ, entonces $2^\kappa = 2^{<\kappa}$.

DEMOSTRACIÓN: La hipótesis es que, para todo $\nu < \kappa$ suficientemente grande, se cumple que $2^\nu = \mu$. Entonces $2^{<\kappa} = \mu$ y, tomando un $\nu > \operatorname{cf}\kappa$ tal que $2^\nu = \mu$, tenemos que

$$2^\kappa = (2^{<\kappa})^{\operatorname{cf}\kappa} = \mu^{\operatorname{cf}\kappa} = (2^\nu)^{\operatorname{cf}\kappa} = 2^{\nu\operatorname{cf}\kappa} = 2^\nu = \mu = 2^{<\kappa}.$$

∎

Vemos así que el valor de 2^κ, cuando κ es un cardinal singular, está sujeto a más condiciones, aparte de la monotonía y el teorema de Kőnig, y determinar qué posibilidades son consistentes con ZFC es lo que se conoce como *el problema de los cardinales singulares,* del cual se conocen muchos resultados parciales, pero no una respuesta general. Por ejemplo, todos los modelos de Easton cumplían lo siguiente:

Hipótesis de los Cardinales Singulares Si κ es un cardinal singular, entonces $\kappa^{\operatorname{cf}\kappa} = \kappa^+ \cdot 2^{\operatorname{cf}\kappa}$.

Notemos, por una parte, que los cardinales regulares cumplen esto y, por otra, que por el teorema de Kőnig siempre se cumple que $\kappa^{\operatorname{cf}\kappa} \ge \kappa^+$ y, trivialmente, $\kappa^{\operatorname{cf}\kappa} \ge 2^{\operatorname{cf}\kappa}$, luego la HCS afirma que $\kappa^{\operatorname{cf}\kappa}$ toma el menor valor posible compatible con la monotonía de la función del continuo y el teorema de Kőnig:. A su vez, implica que lo mismo le sucede a 2^κ:

Teorema (HCS) Si κ es un cardinal singular, entonces

$$2^\kappa = \begin{cases} 2^{<\kappa} & \text{si existe un } \mu<\kappa \text{ tal que } 2^\mu = 2^{<\kappa},\\ (2^{<\kappa})^+ & \text{en caso contrario.}\end{cases}$$

En efecto, el primer caso es el teorema anterior, y en el segundo se demuestra que $\mu = 2^{<\kappa}$ cumple $\operatorname{cf}\mu = \operatorname{cf}\kappa$, y hemos visto que $2^\kappa = \mu^{\operatorname{cf}\kappa} = \mu^{\operatorname{cf}\mu}$, que no puede ser μ por el teorema de Kőnig, luego al menos tiene que ser μ^+.

La Hipótesis del Continuo Generalizada implica la HCS, pues, para todo cardinal infinito κ:

$$\kappa^+ \le \kappa^{\operatorname{cf}\kappa} \le \kappa^\kappa = 2^\kappa = 2^\kappa \cdot 2^{\operatorname{cf}\kappa} \le \kappa^+ \cdot 2^{\operatorname{cf}\kappa} \le \kappa^+(\operatorname{cf}\kappa)^+ = \kappa^+.$$

Sucede que no es posible violar la HCS sin usar cardinales grandes. El primero que lo consiguió fue Silver, que partió de un modelo con un cardinal supercompacto κ y obtuvo una extensión genérica en la que κ era un cardinal medible (en particular fuertemente inaccesible) y $2^\kappa = \kappa^{++}$. Esto podía unirse a un resultado de Karel Libor Prikry de 1970 (que se había doctorado bajo su dirección en 1968), que permitía construir una nueva extensión genérica en la que el cardinal medible κ pasa a tener cofinalidad numerable. En esta extensión κ es un cardinal singular que cumple $2^{<\kappa} = \kappa$, luego según la HCS debería cumplir $2^\kappa = \kappa^+$, pero cumplía $2^\kappa = \kappa^{++}$.

Podría pensarse entonces que, aunque en el caso en que la función del continuo es finalmente constante bajo un cardinal singular κ, el teorema de Bukovský-Hechler determina el valor de 2^κ, en el caso contrario 2^κ puede tomar cualquier valor razonable, aunque cueste probar la consistencia de que así sea, debido a que hacen falta cardinales grandes. Sin embargo, no es así. En 1975 Silver demostró que si κ es un cardinal singular de cofinalidad no numerable y, para todo cardinal infinito $\mu < \kappa$, se cumple $2^\mu = \mu^+$ (con lo que la función del continuo no es finalmente constante), entonces no hay ningún margen para 2^κ, sino que tiene que ser necesariamente $2^\kappa = \kappa^+$.

En cambio, esto no es cierto para cardinales de cofinalidad numerable, pero, inevitablemente, la construcción de modelos que lo muestren requiere cardinales grandes. Así, por ejemplo, en 1983 Shelah demostró que, si es consistente la existencia de un cardinal supercompacto, también lo es que, para cualquier $\alpha < \omega_1$ prefijado, se cumpla $2^{\aleph_n} = \aleph_{n+1}$ para todo $n < \omega$ y $2^{\aleph_\omega} = \aleph_{\alpha+1}$ (mientras que la HCS requeriría que $2^{\aleph_\omega} = \aleph_{\omega+1}$).

Pero tampoco podemos deducir de aquí que, en este caso (el de los cardinales límite de cofinalidad numerable), tengamos la misma libertad que el teorema de Easton nos da para los cardinales regulares, porque en 1982, haciendo uso de una teoría novedosa desarrollada por él y conocida como *teoría de las cofinalidades posibles,* Shelah había demostrado —entre otras cosas— que si, para todo $n < \omega$, se cumple $2^{\aleph_n} < \aleph_\omega$, entonces necesariamente $2^{\aleph_\omega} < \aleph_{\omega_4}$. No se sabe si la cota se puede rebajar a $\aleph_{\omega_1}$.

Axiomas de forcing Otro contexto en el que son necesarios los cardinales grandes es el de las pruebas de consistencia de los llamados *axiomas de forcing.* El más sencillo de todos es el axioma de Martin (véase la página 303), que es equiconsistente con ZFC. Los *axiomas de forcing* son los axiomas que, como AM, afirman la existencia de filtros genéricos bajo ciertas hipótesis, con lo que permiten evitar el uso del forcing en algunas pruebas de consistencia. Ya vimos que en el axioma de Martin no es posible eliminar sin más el requisito de que los conjuntos parcialmente ordenados a los que se aplica cumplan la condición de cadena numerable, pero ésta se puede sustituir por una condición más débil. Así, en 1984 James Earl Baumgartner (que se había doctorado en 1970 bajo la dirección de Vaught) suponiendo la consistencia de que exista un cardinal supercompacto, demostró la consistencia del llamado *Axioma del Forcing Propio,* en el que es como $\mathrm{AM}(\aleph_1)$, pero extendido a conjuntos parcialmente ordenados "propios", que es una propiedad técnica que Shelah había introducido en 1980.

En 1989 Stevo Todorčević (que se había doctorado en 1979 bajo la dirección de Kurepa) demostró que el axioma del forcing propio implica que $2^{\aleph_0} = \aleph_2$ (lo que muestra que la generalización correspondiente de $\mathrm{AM}(\aleph_2)$ sería contradictoria). En 2005 Steel demostró que también implica que el axioma de determinación se cumple en $L(\mathbb{R})$.

En 1988 Matthew Foreman (que se había doctorado en 1980 bajo la dirección de Solovay), Menájem Magidor (doctorado en 1973 bajo la dirección de Lévy), y Shelah, suponiendo también la consistencia de que existe un cardinal supercompacto, demostraron la consistencia de lo que llamaron *Máximo de Martin,* una versión aún más general del axioma del forcing propio y que es la versión más general posible, puesto que se puede demostrar que si un conjunto parcialmente ordenado $\mathbb{P}$ no cumple la condición que impone MM, entonces existen familias de $\aleph_1$ conjuntos densos en $\mathbb{P}$ para las que no hay filtros genéricos. Foreman, Magidor y Shelah demostraron que MM implica la Hipótesis de los Cardinales Singulares.

Cardinales de Mahlo Terminamos explicando qué son exactamente los cardinales de Mahlo (los más bajos en la escala de cardinales grandes por encima de los inaccesibles), porque para ello tenemos que introducir un concepto muy importante en diversas áreas de la teoría de conjuntos. Los cardinales de Mahlo fueron introducidos y estudiados por Paul Mahlo en tres artículos fechados en 1911–1913, aunque en términos muy distintos a como se presentan actualmente.

Definición Si κ es un ordinal límite, un conjunto $C \subset \kappa$ es *cerrado* si para todo ordinal límite $\lambda < \kappa$, si $C \cap \lambda$ no está acotado en λ, entonces $\lambda \in C$.

La idea tras esta definición es muy simple: si C contiene ordinales menores que λ arbitrariamente altos, entonces $\lambda \in C$. Los conjuntos cerrados no acotados en un cardinal regular no numerable tienen un comportamiento especialmente bueno. Por ejemplo, la intersección de menos de κ cerrados no acotados es cerrada y no acotada.

Esto se traduce en que el conjunto $\mathcal{F}_\kappa$ de los subconjuntos de κ que contienen un cerrado no acotado es un filtro κ-completo en κ.

Podemos pensar en los elementos de $\mathcal{F}_\kappa$ como en los subconjuntos "muy grandes" de κ (o "de medida 1", en analogía con los subconjuntos del intervalo $[0,1]$). A su vez, los elementos del ideal dual $\mathcal{I}_\kappa$, formado por los complementarios de los conjuntos de $\mathcal{F}_\kappa$ o, equivalentemente, los conjuntos que no cortan a un cerrado no acotado, son los subconjuntos "muy pequeños" de κ (o "de medida 0"). A su vez, los conjuntos que no están en $\mathcal{I}_\kappa$, es decir, los que cortan a todo cerrado no acotado, son los conjuntos "no muy pequeños" (o "de medida positiva"). Dichos conjuntos se llaman estacionarios:

Definición Si κ es cardinal regular no numerable, un conjunto $E \subset \kappa$ es *estacionario* si corta a todos los subconjuntos cerrados no acotados de κ.

Notemos que, en particular, todo conjunto estacionario en κ es no acotado en κ, y esto a su vez (por la regularidad de κ) implica que tiene cardinal κ. Basta tener en cuenta que si E está acotado por $\alpha < \kappa$, entonces $C = \kappa \setminus \alpha$ es un cerrado no acotado que no corta a E, luego E no es estacionario.

Con esto ya podemos definir los cardinales de Mahlo:

Definición *Un cardinal κ es fuertemente/débilmente de Mahlo si es fuertemente/débilmente inaccesible y el conjunto de los cardinales $\mu < \kappa$ fuertemente/débilmente inaccesibles es estacionario en κ.*

En realidad, en los diagramas de las páginas 316 y 317, las flechas marcadas con ∞ indican que el conjunto de los cardinales inferiores es estacionario en cada cardinal superior. Por ejemplo, si κ es un cardinal débilmente compacto, entonces el conjunto de los cardinales (fuertemente) de Mahlo menores que κ es estacionario en κ.

Los cardinales de Mahlo son el primer peldaño de toda una jerarquía de cardinales infinitos. Por ejemplo, podemos definir un cardinal *hiper-Mahlo* (o 2-Mahlo) como un cardinal de Mahlo κ tal que el conjunto de los cardinales de Mahlo menores que κ sea estacionario en κ, y del mismo modo podemos definir los cardinales 3-Mahlo, 4-Mahlo, etc. Incluso podemos definir un cardinal ω-Mahlo como un cardinal que es n-Mahlo para todo $n < \omega$, lo que a su vez nos permite definir los cardinales $\omega + 1$-Mahlo, etc. Sucede que todo cardinal débilmente compacto κ es κ-Mahlo (y más es imposible).

2.2 Constructibilidad

El estudio de la clase L de los conjuntos constructibles, y de los modelos relacionados $L(A)$ y $L[A]$ distaba mucho de estar agotado. En 1972 Jensen publicó un artículo titulado *La estructura fina de la jerarquía constructible,* en el que hacía un profundo análisis de la estructura de L del que derivó muchas consecuencias. Entre ellas estaban algunos "principios combinatorios", que es el nombre que dio a ciertos hechos que se cumplen en L y que son fáciles de enunciar, y que permiten obtener pruebas de consistencia sin saber nada de L, del mismo modo que el axioma de Martin permite obtener pruebas de consistencia que requerirían construir extensiones genéricas sin necesidad de saber nada de extensiones genéricas.

Concretamente, Jensen definió dos familias de principios combinatorios, que son sólo las primeras de otros muchos principios similares que se descubrirían más adelante. Una es la de los diamantes $\diamondsuit_\kappa(E)$:

Si κ es un cardinal regular no numerable y $E \subset \kappa$ es estacionario, se llama $\diamondsuit_\kappa(E)$ a la afirmación siguiente:

($\diamondsuit_\kappa(E)$) Existe una sucesión $\{A_\alpha\}_{\alpha\in E}$ tal que $\bigwedge\alpha \in E\ A_\alpha \subset \alpha$ y que verifica

$$\bigwedge A \subset \kappa\ \{\alpha \in E \mid A \cap \alpha = A_\alpha\} \text{ es estacionario en } \kappa.$$

Y la otra es la de los *cuadrados* $\square_\kappa$:

Si κ es un cardinal infinito, se llama $\square_\kappa$ a la afirmación siguiente:

($\square_\kappa$) Existe una sucesión $\{C_\lambda\}_{\lambda<\kappa^+}$ (donde λ recorre los ordinales límite menores que κ^+) tal que:

1. C_λ es cerrado no acotado en λ.
2. Si $\operatorname{cf}\lambda < \kappa$, entonces $|C_\lambda| < \kappa$.
3. Si $\lambda' < \lambda$ cumple que $C_\lambda \cap \lambda'$ no está acotado en λ', entonces $C_{\lambda'} = C_\lambda \cap \lambda'$.

Como en el caso del axioma de Martin, nadie pretende que un platonista vea estas afirmaciones como propiedades que es razonable suponer que cumplen los conjuntos, sino que son meras consecuencias del axioma de constructibilidad, de modo que cualquier consecuencia que se deriva de cualquiera de ellas es automáticamente consistente con ZFC. La demostración de estos principios combinatorios es muy técnica. La de los cuadrados requiere buena parte de la compleja maquinaria de la "estructura fina" de L desarrollada por Jensen, mientras que la prueba de los diamantes es más elemental, aunque requiere igualmente hablar de submodelos e inmersiones elementales. En cambio, estos principios pueden usarse sin saber nada de modelos ni de lógica, en argumentos puramente conjuntistas.

Por concretar, vamos a centrarnos en el caso más sencillo, el conocido simplemente como *diamante de Jensen* $\diamondsuit$ que es $\diamondsuit_{\omega_1}(\omega_1)$:

($\diamondsuit$): Existe una sucesión $\{A_\alpha\}_{\alpha<\omega_1}$ tal que $\bigwedge\alpha<\omega_1\ A_\alpha\subset\alpha$ y que verifica

$$\bigwedge A\subset\omega_1\ \{\alpha<\omega_1\mid A\cap\alpha=A_\alpha\}\ \textit{es estacionario en}\ \omega_1.$$

A una sucesión en estas condiciones se la llama *sucesión diamante.* Puede verse como una contrapartida de $\mathrm{AM}(\aleph_1)$. Por ejemplo, $\mathrm{AM}(\aleph_1)$ implica que no existen árboles de Suslin, mientras que a partir de una sucesión $\diamondsuit$ se puede construir uno. Similarmente, $\mathrm{AM}(\aleph_1)$ implica que $2^{\aleph_0}>\aleph_1$, mientras que $\diamondsuit$ implica que $2^{\aleph_0}=\aleph_1$.

Demostración: Como los conjuntos estacionarios no están acotados, si $A\subset\omega\subset\omega_1$, tiene que existir un $\alpha\geq\omega$ tal que $A=A\cap\alpha=A_\alpha$, por lo que una sucesión diamante contiene a todos los subconjuntos de ω. ∎

Por ejemplo, para demostrar $\diamondsuit$ a partir de $V=L$ se realiza la construcción siguiente:

Definimos recurrentemente dos sucesiones $\{A_\alpha\}_{\alpha<\omega_1}$ y $\{C_\alpha\}_{\alpha<\omega_1}$ mediante $A_0=C_0=\varnothing$, $A_{\alpha+1}=C_{\alpha+1}=\alpha+1$ y, para cada ordinal límite λ, tomamos como (A_λ,C_λ) el mínimo par (A,C), respecto al buen orden constructible $\trianglelefteq$, tal que $A,C\subset\lambda$, C es cerrado no acotado en λ y $\bigwedge\alpha\in C\,A\cap\alpha\neq A_\alpha$ si existe tal par, o bien $A=C=\lambda$ en caso contrario.

No es trivial en absoluto demostrar que la sucesión $\{A_\alpha\}_{\alpha<\omega}$ es una sucesión diamante.

Actualmente se trabaja también con variantes de estos principios, y con otros similares, como el *trébol* ♣, que es más débil que $\diamondsuit$ y fue introducido por Adam Ostaszewski en su artículo *Sobre los espacios numerablemente compactos perfectamente normales,* o el palo ♠, más débil aún, introducido en 1978 en el artículo *Topologías determinadas por σ-ideales en ω_1,* de Broverman, Ginsburg, Kunen y Tall. Los títulos muestran el uso de estos principios en topología.

Más en general, el estudio de los modelos transitivos de ZF que son clases propias ha dado lugar a la *teoría de modelos internos* como rama de la teoría de conjuntos.

2.3 Afirmaciones indecidibles en matemáticas

Tanto la teoría de extensiones genéricas como la teoría sobre los cardinales grandes pusieron pronto de manifiesto que la hipótesis del continuo no era, ni mucho menos, un caso aislado, sino que las afirmaciones indecidibles en ZFC son muy numerosas y, aunque son especialmente frecuentes las que tienen un contenido puramente conjuntista o sobre topología conjuntista, es posible encontrarlas en muchas otras áreas de la matemática.

Entre las sentencias indecidibles[3] en ZFC se encuentran, para empezar, todas las que postulan la existencia de uno o varios cardinales grandes (inaccesibles, de Mahlo, débilmente compactos, etc.) y todos los axiomas y principios adicionales de los que hemos hablado (los principios combinatorios, el axioma de Martin, el axioma de determinación proyectiva, etc.), así como casi cualquier afirmación razonable que pretenda determinar, total o parcialmente, la función del continuo.

Afirmaciones indecidibles en topología Un ejemplo sencillo de problema indecidible en topología es el siguiente:

Un espacio topológico tiene la condición de cadena numerable si en él toda familia de abiertos disjuntos dos a dos es a lo sumo numerable. ¿El producto de dos espacios con la condición de cadena numerable tiene la condición de cadena numerable?

La hipótesis del continuo implica que no necesariamente, mientras que el axioma de Martin implica que sí.

En 1929 Alexandroff y Urysohn preguntaron si existe un espacio topológico compacto infinito que no contenga ninguna sucesión convergente no trivial (es decir, no finalmente constante). La respuesta la proporcionó en 1935

[3]No incidimos aquí los supuestos técnicos de consistencia por no ser repetitivos. Por ejemplo, cuando decimos que la existencia de un cardinal inaccesible es indecidible en ZFC hay que entender que lo es supuesto que ZFC sea consistente (hipótesis necesaria para que no se pueda demostrar que existen cardinales inaccesibles) y que también lo es que ZFC + existe un cardinal inaccesible (hipótesis necesaria para que no se pueda demostrar que no existen).

uno de sus alumnos de doctorado, Andréi Nikoláyevich Tychonoff (doctorado en 1927) e independientemente, en 1937, Eduard Čech. Ambos encontraron el mismo compacto sin sucesiones convergentes, aunque su presentación fue muy diferente. Čech desarrolló en general el concepto que hoy se conoce como la compactificación de Stone-Čech de un espacio completamente regular, y demostró que $\beta\omega$ (la compactificación de un espacio discreto numerable) no contiene sucesiones convergentes no triviales.

Desde entonces $\beta\omega$ ha sido una fuente de afirmaciones indecidibles en ZFC. Por ejemplo, $\beta\omega$ puede construirse dotando de una topología al conjunto de todos los ultrafiltros en ω, de modo que los ultrafiltros principales se corresponden con los elementos de ω, mientras que $\omega^* = \beta\omega \setminus \omega$ está formado por los ultrafiltros libres.

Es obvio que un ultrafiltro principal es muy diferente de un ultrafiltro libre, y eso se traduce, desde un punto de vista topológico, en que los puntos de ω son aislados en $\beta\omega$, mientras que los de ω^* no lo son. En particular, todo homeomorfismo de $\beta\omega$ transforma puntos de ω en puntos de ω (y puntos de ω^* en puntos de ω^*).

Pero resulta natural plantearse si ω^* es homogéneo, es decir, si, dados dos puntos $p, q \in \omega^*$, existe un homeomorfismo de ω^* en sí mismo que transforma uno en otro. Esto es tanto como decir que todos los ultrafiltros no principales "son iguales". La cuestión se planteó en un seminario en 1955 y en 1956 Walter Rudin, suponiendo la hipótesis del continuo, demostró que no. Para ello demostró que la hipótesis del continuo implica que ω^* contiene *P-puntos,* es decir, puntos p tales que la interesección de una cantidad numerable de entornos de p sigue siendo un entorno de p. Es fácil ver que no todos los puntos de ω^* pueden ser P-puntos, por lo que ω^* no es homogéneo: no puede haber homeomorfismos que transformen un P-punto en un no P-punto. Sin embargo, en 1982 Shelah demostró mediante una extensión genérica que es consistente que no haya P-puntos en ω^*.

No obstante, en 1967 Zdeněk Frolík (que se había doctorado en 1964 bajo la dirección de Čech y Miroslav Katě tov) había demostrado en ZFC que ω^* no es homogéneo y en 1978 Kunen demostró en ZFC que ω^* contiene lo que llamó *P-puntos débiles,* que prueban igualmente que no es homogéneo.

Por otro lado, en 1969 B.A. Efimov planteó el problema de si todos los espacios topológicos compactos infinitos sin sucesiones convergentes no triviales contienen necesariamente un subespacio homeomorfo a $\beta\omega$ (es decir, si $\beta\omega$ es esencialmente la única solución al problema que habían planteado Alexandroff y Urysohn. Los espacios compactos infinitos que no contienen sucesiones convergentes no triviales ni subespacios homeomorfos a $\beta\omega$ se llaman *espacios de Efimov.* En 1975 Vitaly Fedorchuk (doctorado en 1967 bajo la dirección de Alexandroff) construyó un ejemplo de espacio de Efimov usando la hipótesis del continuo. Hoy en día no se sabe si es posible construir un espacio de Efimov en ZFC, por lo que no podemos asegurar que la existencia de tales espacios sea independiente de ZFC.

En principio, podría ocurrir con ellos como con los espacios de Dowker. En la página 207 vimos que en 1955 Mary Ellen Rudin mostró que una recta de Suslin es un ejemplo de espacio de Dowker, pero en 1971 la propia Rudin encontró un ejemplo en ZFC, luego existencia de espacios de Dowker no es independiente de ZFC.

Afirmaciones indecidibles en análisis Ya hemos tratado algunos ejemplos de problemas en el contexto del análisis matemático que son indecidibles en ZFC, como si la medida de Lebesgue se puede extender a todos los subconjuntos de $\mathbb{R}$, o si una unión de $\aleph_1$ conuntos nulos para la medida de Lebesgue tiene que ser nula. No obstante, se puede decir que, en cierto modo, se trata de problemas conjuntistas "disfrazados". Veamos algunos ejemplos más "genuinamente" analíticos.

Recordemos (un caso particular de) el bien conocido teorema de Fubini:

Teorema Sea $f : [0,1] \times [0,1] \longrightarrow \mathbb{R}$ una función integrable. Entonces:

1. Las funciones $x \mapsto f(x,y)$, $y \mapsto f(x,y)$ son integrables para casi todo y, $x \in [0,1]$, respectivamente.
2. Las funciones
$$\int_0^1 f(x,y)\,dy, \qquad \int_0^1 f(x,y)\,dx$$
están definidas y son integrables para casi todo x, $y \in [0,1]$, respectivamente, y se cumple
$$\int_{[0,1]\times[0,1]} f(x,y)\,dxdy = \int_0^1 \left(\int_0^1 f(x,y)\,dy\right) dx = \int_0^1 \left(\int_0^1 f(x,y)\,dx\right) dy.$$

Ahora vamos a plantear una variante:

Sea $f : [0,1] \times [0,1] \longrightarrow \mathbb{R}$ una función que cumpla:

1. Las funciones $x \mapsto f(x,y)$, $y \mapsto f(x,y)$ son integrables para casi todo y, $x \in [0,1]$, respectivamente.
2. Las funciones
$$x \mapsto \int_0^1 f(x,y)\,dy, \qquad y \mapsto \int_0^1 f(x,y)\,dx$$
son integrables en $[0,1]$.

Entonces
$$\int_0^1 \left(\int_0^1 f(x,y)\,dy\right) dx = \int_0^1 \left(\int_0^1 f(x,y)\,dx\right) dy.$$

Sucede que esta variante es falsa. El lector puede comprobar que un contraejemplo lo proporciona la función $f : [0,1] \times [0,1] \longrightarrow [0,1]$ dada por:

$$f(x,y) = \begin{cases} 1/y^2 & \text{si } 0 < x < y < 1, \\ -1/x^2 & \text{si } 0 < y < x < 1, \\ 0 & \text{en otro caso.} \end{cases}$$

Sin embargo, se podría pensar que jugar con términos positivos y negativos que se cancelan es "jugar sucio" y, puestos a ser cautos, podemos exigir, no sólo que f sea ≥ 0, sino que esté acotada. En tal caso no perdemos generalidad si suponemos que la cota es 1, con lo que podemos replantear así el problema:

Problema Sea $f : [0,1] \times [0,1] \longrightarrow [0,1]$ una función que cumpla:

1. Las funciones $x \mapsto f(x,y)$, $y \mapsto f(x,y)$ son medibles para casi todo y, $x \in [0,1]$, respectivamente.
2. Las funciones
$$x \mapsto \int_0^1 f(x,y)\,dy, \qquad y \mapsto \int_0^1 f(x,y)\,dx$$
son medibles en $[0,1]$.

¿Se da entonces la igualdad siguiente?:
$$\int_0^1 \left(\int_0^1 f(x,y)\,dy\right) dx = \int_0^1 \left(\int_0^1 f(x,y)\,dx\right) dy.$$

Hemos cambiado los requisitos de integrabilidad por medibilidad porque, para una función $0 \leq f \leq 1$, ser integrable es lo mismo que ser medible. Sucede que esta pregunta no puede responderse en ZFC. Es consistente que la respuesta sea afirmativa y también negativa. Puede probarse que la existencia de una función f que no cumpla la igualdad es equivalente a la existencia de un *conjunto de Steinhaus:*

Definición Un *conjunto de Steinhaus* es un subconjunto $A \subset [0,1] \times [0,1]$ tal que, para casi todo $x, y \in [0,1]$ (es decir, salvo en un conjunto de medida nula), los conjuntos

$$A_x = \{y \in [0,1] \mid (x,y) \in A\}, \qquad A^y = \{x \in [0,1] \mid (x,y) \in A\}$$

son medibles Lebesgue, con $m(A_x) = 1$, $m(A^y) = 0$.

Ciertamente, si A es un conjunto de Steinhaus y f es su función característica, entonces f cumple las hipótesis del problema anterior pero las integrales finales dan 1 y 0, respectivamente. Puede probarse que, de hecho, la existencia de una función que sea un contraejemplo para el problema anterior equivale a la existencia de un conjunto de Steinhaus.

Teorema El axioma de Martin (en particular, la hipótesis del continuo) implica que existe un conjunto de Steinhaus.

DEMOSTRACIÓN: En la página 304 hemos visto que el axioma de Martin implica que todo subconjunto de $\mathbb{R}$ de cardinal menor que $\mathfrak{c}$ es nulo (lo cual es trivial si se cumple la hipótesis del continuo). Sea $\{x_\alpha\}_{\alpha<\mathfrak{c}}$ una enumeración del intervalo $[0,1]$. Basta tomar

$$A = \{(x_\alpha, x_\beta) \mid \alpha < \beta < \mathfrak{c}\}.$$

Entonces, si $y = x_\beta$, tenemos que $A^y = \{x_\alpha \mid \alpha < \beta\}$, luego $|A^y| < \mathfrak{c}$, luego $m(A^y) = 0$. En cambio, si $x = x_\alpha$, entonces $A_x = \{x_\beta \mid \alpha < \beta\}$, luego $|[0,1] \setminus A_x| < \mathfrak{c}$, luego $m([0,1] \setminus A_x) = 0$, luego $m(A_x) = 1$. ∎

Así pues, el axioma de Martin implica que el problema que hemos planteado tiene respuesta negativa. Por otra parte:

Teorema Si existe un conjunto de Steinhaus y κ es el menor cardinal de un conjunto no nulo en $[0,1]$ para la medida de Lebesgue, entonces $[0,1]$ puede expresarse como unión de κ conjuntos nulos.

DEMOSTRACIÓN: Sea $A \subset [0,1] \times [0,1]$ un conjunto de Steinhaus y sea $B \subset [0,1]$ un conjunto no nulo de cardinal κ. Sea $N \subset [0,1]$ un conjunto nulo tal que si $x \in [0,1] \setminus N$, entonces $m(A_x) = 1$.

Basta probar que $[0,1] = N \cup \bigcup_{y\in B} A^y$. En efecto, si $x \in [0,1] \setminus N$, tenemos que $m(A_x) = 1$, luego $A_x \cap B \neq 0$ (o, de lo contrario, la unión tendría medida mayor que 1), luego existe un $y \in B$ tal que $(x,y) \in A$, es decir, tal que $x \in A^y$. ∎

Sucede que es posible construir un modelo de ZFC en el que, por ejemplo, haya conjuntos no nulos de cardinal $\aleph_1$, pero en el que $[0,1]$ no pueda expresarse como unión de $\aleph_1$ conjuntos nulos. El teorema anterior implica que en dicho modelo no hay conjuntos de Steinhaus, luego el problema que hemos planteado tiene respuesta positiva.[4]

Veamos ahora un ejemplo correspondiente al análisis funcional. Si K es un espacio topológico compacto, llamamos $C(K)$ al espacio de todas las funciones continuas $f : K \longrightarrow \mathbb{C}$, que es un espacio vectorial sobre $\mathbb{C}$ y un *álgebra de Banach* con la *norma uniforme,* que es la dada por $\|f\| = \sup f[K]$. Una *norma de álgebra* en $C(K)$ es una aplicación que, además de cumplir con la definición usual de norma, cumple la desigualdad $\|fg\| \leq \|f\|\|g\|$.

Conjetura de Kaplansky Si K es un espacio topológico compacto, toda norma de álgebra en $C(K)$ es equivalente a la norma uniforme (es decir, que induce la misma topología).

Esta conjetura fue planteada en 1948 por Irving Kaplansky (doctorado en 1941 bajo la dirección de Mac Lane), que previamente había demostrado que toda norma de álgebra completa en $C(K)$ es equivalente a la norma uniforme. En 1976 Garth Dales y Jean Sterle demostraron independientemente que si se cumple la hipótesis del continuo la conjetura de Kaplansky es falsa, mientras que ese mismo año Solovay construyó un modelo de ZFC en el que la conjetura de Kaplansky es verdadera.

Afirmaciones indecidibles en álgebra En 1956 Cartan y Eilenberg introdujeron el concepto de *módulo proyectivo.* Un *módulo* es lo mismo que un espacio vectorial, salvo que los escalares varían en un anillo que no es necesariamente un cuerpo. Así como todo espacio vectorial tiene una base, en general un módulo sobre un anillo A no tiene por qué tener base. Los módulos con base se llaman *módulos libres.* Los módulos proyectivos son una familia un poco más amplia que la de los módulos libres y que es más cómoda de manejar en el contexto de la teoría de categorías. Una de sus propiedades es que, si M es un A-módulo arbitrario, siempre existe un epimorfismo $P_0 \longrightarrow M$, donde P_0 es un A-módulo proyectivo. Si no es inyectivo, podemos aplicar la misma propiedad a su núcleo, y obtenemos un homomorfismo

$$P_1 \longrightarrow P_0 \longrightarrow M,$$

donde P_1 es proyectivo y la imagen del primer homomorfismo es el núcleo del segundo. Si este segundo homomorfismo tampoco es inyectivo, podemos prolongar el proceso. Si es posible, tras un número finito de pasos, llegar a una sucesión

$$P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M,$$

donde la imagen de cada homomorfismo es el núcleo del siguiente, el primero es inyectivo y el último suprayectivo, entonces, el mínimo n para el que existe una sucesión así se llama *dimensión proyectiva* del módulo M. En 1968 Barbara Osofsky demostró lo siguiente:

[4]Esto lo probó en 1980 Havery Friedman, doctorado en 1967 (a los 19 años), bajo la dirección de Sacks. Esto da una respuesta negativa al problema 7 de la página 55, mientras que el conjunto de Steinhaus construido a partir del axioma de Martin da una respuesta positiva.

Teorema (Osofsky) Sea $M = \mathbb{R}(x, y, z)$ el cuerpo de funciones racionales (cocientes de polinomios) con tres indeterminadas y coeficientes reales, considerado como A-módulo, donde $A = \mathbb{R}[x, y, z]$. La dimensión proyectiva de M es 2 si se cumple la hipótesis del continuo y 3 en caso contrario.

Los $\mathbb{Z}$-módulos son simplemente los grupos abelianos, y no todos ellos son libres. Si unos grupos abelianos cumplen $G/H \cong L$, se dice que G es una *extensión* de H por L. Dados H y L, siempre es posible construir una extensión de H por L, la *extensión trivial* dada por $G = H \times L$. Los grupos abelianos libres se caracterizan por que las únicas extensiones por grupos libres son las triviales:

Teorema Un grupo abeliano L es libre si y sólo si cuando un grupo cociente es isomorfo a L, es decir, $G/H \cong L$, necesariamente existe un subgrupo K de G tal que $G \cong L \times K$.

En términos del álgebra homológica, esto equivale a que L es libre si y sólo si $\mathrm{Ext}(L, H) = 0$, para todo grupo abeliano H. Sin embargo, John Henry Constantine Whitehead se planteó si bastaba considerar extensiones de $H \cong \mathbb{Z}$, es decir:

Problema de Whitehead ¿Si un grupo abeliano L cumple $\mathrm{Ext}(L, \mathbb{Z}) = 0$, es necesariamente libre?

Un grupo que cumpla $\mathrm{Ext}(L, \mathbb{Z}) = 0$ se llama un *grupo de Whitehead,* con lo que el problema de Whitehead plantea si todo grupo de Whitehead es libre. Sin embargo, en 1974 Shelah demostró que si $V = L$ entonces la respuesta es afirmativa, mientras que el axioma de Martin $\mathrm{AM}(\aleph_1)$ implica que existe un grupo de Whitehead que no es libre.

Ecuaciones diofánticas indecidibles Entre los ejemplos de sentencias indecidibles no podemos omitir los correspondientes a enunciados aritméticos de la teoría de números elemental que, en virtud del segundo teorema de incompletitud de Gödel, expresan la consistencia de teorías axiomáticas suficientemente potentes, como ZFC o teorías con axiomas adicionales. Según hemos visto en la sección 87 (página 234), pueden expresarse, más concretamente, como ecuaciones diofánticas, lo que pone en evidencia que el décimo problema de Hilbert (encontrar un método para resolver cualquier ecuación diofántica) no tiene solución.

2.4 La teoría descriptiva de conjuntos

En el capítulo I no hemos dado muchos detalles sobre los avances en la teoría descriptiva de conjuntos porque ello habría requerido introducir muchos conceptos específicos que habrían requerido demasiado espacio. No obstante, señalaremos aquí que, aunque los primeros trabajos en esta área trataban con subconjuntos de $\mathbb{R}^n$, ya desde la publicación en 1951 de la *Topología* de Kuratowski estaba claro que era posible y más conveniente trabajar en el contexto más general de los espacios topológicos completamente metrizables y separables. Más adelante, estos espacios recibirían el nombre de *espacios polacos,* en honor a la escuela de matemáticos polacos —entre los que se encontraba Kuratowski— que los estudiaron con detalle.

La teoría descriptiva experimentó una revolución cuando se fusionó con una teoría general sobre funciones recursivas que había desarrollado Kleene. En 1939 Turing había introducido el concepto de "función f computable computable a partir de unas funciones dadas $f_1, \ldots, f_n$", en el sentido de que f se puede calcular por un algoritmo explícito que puede "consultar un oráculo" para conocer los valores que necesite en cada momento de las funciones $f_1, \ldots, f_n$, sin exigir que este cálculo tenga que ser efectivo. Kleene recogió esta idea, que ya aparece expuesta en su *Introducción a la metamatemática,* donde define las *funciones recursivas en* $f_1, \ldots, f_n$ como las funciones que pueden calcularse mediante sucesivas aplicaciones de los procedimientos de composición, recursión o minimización a partir de las funciones elementales "cero", "siguiente" y las proyecciones, pero también de las funciones $f_1, \ldots, f_n$. Posteriormente, esto lo llevó a trabajar con funciones de la forma

$$f : \omega^r \times \mathcal{N}^s \longrightarrow \omega,$$

donde $\mathcal{N} = \omega^\omega$ es el conjunto de todas las funciones de ω en sí mismo. Kleene definió las funciones *recursivas* de este tipo, de modo que f es recursiva si existe un algoritmo para calcular $f(n_1, \ldots, n_r, x_1, \ldots, x_s)$ a partir de $n_1, \ldots, n_r$ y de las restricciones $x_1|_m, \ldots, x_s|_m$, para un m suficientemente grande (que dependerá de $n_1, \ldots, n_r$). Pero sucede que, si consideramos a ω como espacio topológico discreto y a $\mathcal{N}$ como el espacio de Baire, el espacio $X^{r,s} = \omega^r \times \mathcal{N}^s$ es un espacio polaco, y resultaba que Kleene estaba elaborando una teoría descriptiva sobre los subconjuntos de $X^{r,s}$ que se parecía bastante a la teoría descriptiva "clásica".

Kleene no sabía gran cosa de teoría descriptiva de conjuntos (que entonces se consideraba una parte de la topología), y el primero en notar la analogía fue Addison, en su tesis doctoral de 1955 (dirigida por Kleene). En 1959 Addison publicó un artículo titulado *Principios de separación en las jerarquías de la teoría descriptiva de conjuntos clásica y efectiva,* escrito durante una estancia en Varsovia, invitado por Mostowski, en el que la "analogía" empezaba a dar paso a un tratamiento unificado. Addison dice que *Tras largas discusiones aquí en Varsovia, se ha decidido proponer...* y a continuación introduce la notación $\Sigma_n^{0,C}, \Pi_n^{0,C}, \Sigma_n^{1,C}, \Pi_n^{1,C}$ para ciertas clases de subconjuntos de $X^{r,s}$ definidas por Kleene, donde $C \subset \mathcal{N}$, con el convenio de que si $C = \varnothing$ se escribe simplemente $\Sigma_n^0, \Pi_n^0, \Sigma_n^1, \Pi_n^1$, mientras que para $C = \mathcal{N}$ las clases correspondientes se representarán por $\mathbf{\Sigma}_n^0, \mathbf{\Pi}_n^0, \mathbf{\Sigma}_n^1, \mathbf{\Pi}_n^1$. Estas últimas clases son precisamente las que desde un principio venimos llamando así: los niveles finitos de la jerarquía de Borel y los niveles de la jerarquía proyectiva, pero para los espacios $X^{r,s}$.

En principio, las clases $\mathbf{\Sigma}_n^{0,C}$, etc. estaban definidas para $n < \omega$, pero Kleene había definido y estudiado los ordinales recursivos, y su teoría podía extenderse para definir los *ordinales recursivos en x,* para cierta función $x \in \mathbb{N}$ (es decir, los ordinales correspondientes a buenos órdenes en ω recursivos en x), de modo que todo ordinal numerable es recursivo respecto de un $x \in \mathcal{N}$ adecuado que codifique una relación con su tipo de orden. Por ello, si llamamos $\omega_1^{CK}(x)$ al menor ordinal no recursivo en x, sucede que el supremo de estos ordinales es ω_1, y el trabajo de Kleene permitía definir clases $\Sigma_\alpha^0(x), \Pi_\alpha^0(x)$, para $\alpha < \omega_1^{CK}(x)$ y, para cada $\alpha < \omega_1$, al unir todas las clases $\sigma_\alpha^0(x)$, donde x recorre los elementos de $\mathcal{N}$ tales que $\alpha < \omega_1^{CK}(x)$, se obtiene la clase de Borel $\mathbf{\Sigma}_\alpha^0$, e igualmente con $\mathbf{\Pi}_\alpha^0$.

No vamos a dar más detalles porque, como decíamos, esto requeriría introducir muchos conceptos técnicos que quedarían descontextualizados. Nos quedamos simplemente con que muchos resultados sobre cada clase "clásica" $\mathbf{\Gamma}$ podían deducirse trivialmente de los resultados correspondientes para las clases "efectivas" $\Gamma(x)$, aunque éstos en muchos casos eran más difíciles de demostrar (pero a la vez eran más profundos), así como que, a partir de la década de los 70, la teoría tenía esencialmente dos aspectos muy diferentes entre sí, según se supusiera el axioma de constructibilidad (o alguna versión débil $V = L[A]$) o bien algún fragmento del axioma de determinación proyectiva (o el axioma de determinación completo).

Capítulo III

Nuevas alternativas a la matemática clásica

3.1 El constructivismo de Bishop

En 1966 se celebró en Moscú el decimoquinto Congreso Internacional de Matemáticos, en el que Erret Albert Bishop (doctorado en 1954 bajo la dirección de Halmos) dio una conferencia titulada *La constructivización del análisis matemático abstracto,* en la que presentó su concepto de lo que eran las *matemáticas constructivas.*

> *El punto de vista constructivo sostiene que todas las matemáticas deberían tener un significado numérico. En otras palabras, todo teorema matemático debería admitir una interpretación última según la cual ciertos cálculos finitos dentro del conjunto de los números naturales darán unos resultados determinados. En contraste, la matemática clásica (es decir, la contemporánea) es idealista: no se exige que los teoremas y sus demostraciones tengan un significado numérico ni ningún contenido predictivo. Por ejemplo, el teorema de que los números reales pueden estar bien ordenados es evocador (o idealista), más que descriptivo (o constructivo). También lo es el teorema de que toda sucesión monótona y acotada de números reales converge.*
>
> *Brouwer ha demostrado que las idealizaciones presentes en la matemática clásica pueden, en la mayoría de los casos, atribuirse al uso de un principio lógico: el principio del tercio excluso. Quizás sea más natural atribuirlas a un principio estrechamente relacionado: el principio de omnisciencia, que establece que un conjunto arbitrario A tiene o no un elemento con una propiedad dada P. En el caso de que A sea un conjunto infinito, este principio no es constructivamente válido, ya que examinar cada elemento de A para determinar si alguno posee la propiedad P no es algo que pueda realizarse necesariamente mediante un proceso finito y rutinario.* [...]
>
> *Brouwer se propuso desarrollar las matemáticas siguiendo líneas constructivas. Su desarrollo, que no fue sistemático, se vio obstaculizado por una teoría revolucionaria y semimística del continuo. Esta teoría, que en retrospectiva parece tan innecesaria, resultaba repulsiva para la mayoría de los matemáticos.*
>
> *Además de Brouwer, otros han adoptado puntos de vista más o menos constructivos, generalmente menos. Están los formalizadores de la constructividad, cuyos sistemas formales tienen poca relevancia para la constructivización de las matemáticas existentes; están los especialistas en la teoría de las funciones recursivas, que basan la constructividad en un supuesto* ad hoc[1] *que es más un impedimento que una herramienta; está Hilbert, que creía que el precio de una matemática constructiva era demasiado alto; y varios otros grupos, ninguno de los cuales se conforma con dejar que la matemática constructiva siga su curso natural de desarrollo. Este artículo describe un intento de volver a desarrollar el análisis abstracto a lo largo de líneas constructivas directas, dejando que el material hable por sí mismo, en lugar de forzarlo a soportar una carga de filosofía preconcebida.*

El resto de la conferencia estaba dedicada a esbozar que teorías y resultados matemáticos podían ser "constructivizados". Estas ideas las desarrolló en el libro *Fundamentos del análisis constructivo,* publicado en 1967, en cuyo prefacio se lee:

[1] Bishop no acepta que todas las funciones definibles de forma constructiva tengan que ser recursivas.

A la mayoría de los matemáticos les resultaría difícil creer que pudiera existir una controversia seria sobre los fundamentos de las matemáticas, una controversia cuyo resultado pudiera afectar significativamente su propia actividad matemática. Su actitud representa bien la situación actual: durante medio siglo de espléndido progreso matemático no ha habido ninguna desviación de la norma. Las voces disidentes, nunca muy escuchadas, han permanecido en silencio por mucho tiempo. [...]

Por otro lado, muchos enunciados matemáticos tienen un contenido pragmático bastante peculiar. Consideremos el teorema de que o bien todo entero par mayor que 2 *es la suma de dos primos, o bien existe un entero par mayor que* 2 *que no es la suma de dos primos. El contenido pragmático de este teorema no consiste en que si observamos los números enteros, veremos que suceden ciertas cosas. Más bien, el contenido pragmático de dicho teorema, si existe, reside en que lo utilizaremos para derivar otros teoremas, que a su vez tienen un contenido pragmático peculiar y que, a su vez, servirán de base para futuros desarrollos.*

Parece entonces que existen ciertas afirmaciones matemáticas meramente evocativas, que formulan afirmaciones sin validez empírica. También existen afirmaciones matemáticas de validez empírica inmediata, que afirman que ciertas operaciones realizables producirán ciertos resultados observables, por ejemplo, el teorema de que todo número natural es la suma de cuatro cuadrados. Las matemáticas son una mezcla de lo real y lo ideal, a veces uno, a veces el otro, a menudo presentados de tal manera que es difícil distinguir cuál es cuál. El componente realista de las matemáticas —el deseo de interpretación pragmática— proporciona el control que determina el curso del desarrollo y evita que las matemáticas caigan en un formalismo sin sentido. El componente idealista permite simplificaciones y abre posibilidades que de otro modo estarían cerradas. Los métodos de prueba y los objetos de investigación se han idealizado para formar un juego, pero el desarrollo real del juego está motivado en última instancia por consideraciones pragmáticas.

Durante 50 años no ha habido cambios significativos en las reglas de este juego. Los matemáticos coinciden unánimemente en cómo deben jugarse las matemáticas. Los estándares de conducta aceptados bastan para regular el curso de la actividad matemática, y no hay perspectivas de que estos estándares se modifiquen significativamente mediante una revisión del código idealista. De hecho, no hay ningún intento de imponer tal revisión.

Sin embargo, ha habido intentos de constructivizar las matemáticas, depurándolas por completo de su contenido idealista. El intento más sostenido fue el de L.E.J. Brouwer, a partir de 1907. El movimiento que fundó lleva mucho tiempo muerto, aniquilado en parte por las concesiones de los discípulos de Brouwer a la perspectiva idealista, en parte por peculiaridades ajenas al sistema de Brouwer que lo hicieron vago e incluso ridículo para los matemáticos en activo, pero principalmente por el fracaso de Brouwer y sus seguidores en convencer al público matemático de que abandonar la perspectiva idealista no esterilizaría ni paralizaría el desarrollo de las matemáticas. Brouwer y otros constructivistas tuvieron mucho más éxito en sus críticas a las matemáticas clásicas que en sus esfuerzos por sustituirlas por algo mejor. Muchos matemáticos familiarizados con las objeciones de Brouwer a las matemáticas clásicas admiten su validez, pero siguen sin estar convencidos de que exista una alternativa satisfactoria.

Este libro es una pieza de propaganda constructivista, diseñada para demostrar que existe una alternativa satisfactoria. Para ello, desarrollamos gran parte del análisis abstracto dentro de un marco constructivo. Este desarrollo se lleva a cabo con un mínimo absoluto de prejuicios filosóficos sobre la naturaleza de las matemáticas constructivas. No hay dogmas a los que debamos adherirnos. Nuestro programa es simple: dar significado numérico al máximo posible del análisis abstracto clásico. Nuestra motivación es el conocido escándalo, expuesto detalladamente por Brouwer (y otros), de que las matemáticas clásicas carecen de significado numérico. [...]

El libro tiene un triple propósito: primero, presentar el punto de vista constructivo; segundo, demostrar que el programa constructivo puede tener éxito; tercero, sentar las bases para trabajos futuros. Estos fines inmediatos tienden a un objetivo final: acelerar el inevitable día en que las matemáticas constructivas se conviertan en la norma aceptada. No afirmamos que las matemáticas idealistas sean inútiles desde el punto de vista constructivo. Esto sería tan absurdo como afirmar que las matemáticas poco rigurosas son inútiles desde el punto de vista clásico. Todo teorema demostrado con métodos idealistas presenta un desafío: encontrar una versión constructiva y darle una prueba constructiva.

El capítulo 1 tiene un título que evoca a Marx: *Un manifiesto constructivista* (lo cual tiene sentido si pensamos en que, cada uno en lo suyo, Marx y Bishop eran ambos materialistas). En primer lugar, Bishop señala su convicción en la objetividad de las matemáticas:

> *Las matemáticas son esa parte de nuestra actividad intelectual que trasciende nuestra biología y nuestro entorno. Los principios de la biología, tal como los conocemos, pueden aplicarse a formas de vida en otros mundos, pero no es necesario que así sea. Los principios de la física deberían ser más universales, pero es fácil imaginar otro universo gobernado por leyes físicas diferentes. Las matemáticas, creación de la mente, son menos arbitrarias que la biología o la física, creaciones de la naturaleza; las criaturas que imaginamos habitando otro mundo en otro universo, con otra biología y otra física, desarrollarán una matemática que, en esencia, será la misma que la nuestra.*

A continuación Bishop se declara —más o menos— kantiano:

> *El objeto de estudio principal de las matemáticas son los números, es decir, los números naturales. Consideramos los números como Kant consideraba el espacio*[2]*. Los números naturales y su aritmética se presuponen por la naturaleza misma de nuestra inteligencia y —nos sentimos tentados a creer— por la naturaleza misma de la inteligencia en general. El desarrollo de la teoría de los números naturales a partir del concepto primitivo de unidad, el concepto de unidad adyacente y el proceso de inducción matemática conlleva una convicción absoluta. En palabras de Kronecker, los números naturales fueron creados por Dios. Kronecker lo habría expresado aún mejor si hubiera dicho que los números naturales fueron creados por Dios para beneficio del hombre (y de otros seres finitos). Las matemáticas pertenecen al hombre, no a Dios. No nos interesan las propiedades de los números enteros positivos que no tienen un significado descriptivo para el hombre finito. Cuando alguien prueba la existencia de un número natural, debería mostrar cómo encontrarlo. Si Dios tiene sus propias matemáticas que necesita desarrollar, que lo haga Él mismo.*

Todas las matemáticas pueden construirse a partir de los números naturales:

> *Casi igual de importantes que los números son las construcciones mediante las cuales ascendemos de los números a los niveles superiores de la existencia matemática. Estas construcciones implican el descubrimiento de relaciones entre entidades matemáticas ya construidas, en cuyo proceso se crean nuevas entidades matemáticas. Las relaciones que forman el punto de partida son el orden y las relaciones aritméticas de los números naturales. A partir de estas, construimos diversas reglas para emparejar números, separar ciertos números del resto y asociar un número con otro. Reglas de este tipo dan lugar a las nociones de conjunto y función.*
>
> *Un conjunto no es una entidad con una existencia ideal. Un conjunto existe sólo cuando ha sido definido. Para definir un conjunto, prescribimos, al menos implícitamente, lo que nosotros (la inteligencia constructora) debemos hacer para construir un elemento del conjunto y lo que debemos hacer para demostrar que dos elementos del conjunto son iguales. Una observación similar se aplica a la definición de una función: para definir una función de un conjunto A a un conjunto B, prescribimos un proceso finito que lleva de un elemento de A a un elemento de B, y demostramos que elementos iguales de A dan lugar a elementos iguales de B.*
>
> *A partir de los enteros positivos, tejiendo una red de cada vez más conjuntos y funciones, obtenemos las estructuras básicas de las matemáticas: el sistema de los números racionales, el sistema de los números reales, los espacios euclídeos, el sistema de los números complejos, los cuerpos de números algebraicos, los espacios de Hilbert, los grupos clásicos, etc. En el marco de estas estructuras se desarrolla la mayor parte de las matemáticas. Todo se relaciona con los números, y cada enunciado matemático expresa, en última instancia, el hecho de que si realizamos ciertos cálculos dentro del conjunto de los números naturales, obtendremos ciertos resultados.*

Sin embargo, Bishop es sólo *semikantiano,* pues sólo atribuye auténtico significado a la intuición temporal, mientras que la intuición espacial (geométrica) es ideal, salvo a partir del momento en que los puntos del espacio se identifican con ternas de números:

> *La geometría fue altamente idealista desde la época de Euclides y los antiguos hasta la época de Descartes, desarrollándose a partir de axiomas considerados evidentes o reflejando propiedades del*

[2] Y los números.

mundo real. Descartes redujo la geometría a la teoría de los números reales, y en el siglo XIX, Dedekind, Weierstrass y otros, mediante la aritmetización del sistema de números reales, incorporaron el espacio al ámbito concreto de los objetos construidos por el pensamiento puro. Desafortunadamente, la promesa que la aritmetización del espacio ofrecía a las matemáticas no se cumplió, en gran medida debido a la intervención, a finales de siglo, del programa formalista. La exitosa formalización de las matemáticas contribuyó a mantenerlas en un rumbo equivocado. El hecho de que el espacio haya sido aritmetizado pierde gran parte de su significado si el espacio, los números y todo lo demás se encajan en una matriz de idealismo donde incluso los números naturales tienen una existencia computacional ambigua. Las matemáticas se convierten en el juego de los conjuntos, un juego excelente dentro de sus posibilidades, con reglas admirablemente precisas. El juego se convierte en su propia justificación, y el hecho de que represente una versión altamente idealizada de la existencia matemática no se tiene en cuenta en ningún momento.

Por supuesto, las tendencias idealistas han estado presentes, si no han sido dominantes, en las matemáticas desde los griegos, pero fue necesario el pleno florecimiento del formalismo para acabar con la comprensión de la naturaleza de las matemáticas que su aritmetización podría haber proporcionado.

A continuación, Bishop razona que no es posible justificar constructivamente que toda sucesión acotada de números reales tiene supremo, o que toda función continua f en $[0,1]$ que cumple $f(0) < 0$ y $f(1) > 0$ se anula en algún punto. Luego insiste en desmarcarse de Brouwer y los intuicionistas:

Brouwer luchó contra el avance del formalismo y emprendió la separación de las matemáticas de la lógica. Quería fortalecer las matemáticas asociando a cada teorema y a cada demostración una interpretación pragmáticamente significativa. Su programa no logró apoyo. Fue un expositor poco entusiasta y un abogado inflexible en su lucha contra el gran prestigio de Hilbert y el hecho innegable de que las matemáticas idealistas producían los resultados más generales con el mínimo esfuerzo. Más importante aún, el propio sistema de Brouwer tenía rastros de idealismo y, peor aún, de especulación metafísica. Existía una preocupación por los aspectos filosóficos del constructivismo a expensas de la actividad matemática concreta. Se desarrolló un cálculo de la negación que se convirtió en una muleta para evitar la necesidad de obtener resultados constructivos precisos. No es sorprendente que algunos de los preceptos de Brouwer se formalizaran posteriormente, dando lugar a la llamada teoría de números intuicionista, y que el sistema formal así obtenido resultara no tener ningún valor constructivo. Para ser justos con Brouwer, cabe decir que no se identificó con estos esfuerzos por formalizar la realidad; por culpa de los lógicos, muchos matemáticos que creen conocer algo del punto de vista constructivo tienen en mente un sistema formal insignificante o, lo que es igual de malo, confunden el constructivismo con la teoría de las funciones recursivas.

En suma, Bishop considera que Heyting traicionó al intuicionismo al formalizarlo. El propio Brouwer había calificado tal formalización como un *ejercicio estéril.*

Brouwer se involucró en la especulación metafísica por su deseo de mejorar la teoría del continuo. Una obsesión tanto de Brouwer como de los lógicos ha sido la especulación compulsiva sobre la naturaleza del continuo. En el caso de los lógicos, esto conduce a contorsiones en las que varios sistemas formales, todos ellos desvinculados de la realidad, se interpretan entre sí con la esperanza de que la naturaleza del continuo emerja de alguna manera. En el caso de Brouwer, parecía existir la persistente sospecha de que, a menos que él interviniera personalmente para evitarlo, el continuo resultaría discreto. Por lo tanto, introdujo el método de sucesiones de libre elección para construir el continuo, por lo que éste no puede ser discreto porque no está suficientemente bien definido. Esto hace que las matemáticas sean tan extrañas que resultan desagradables para los matemáticos y condena al fracaso todo el programa de Brouwer. Es una lástima, ya que Brouwer poseía una notable comprensión de los defectos de las matemáticas clásicas e hizo un intento heroico por corregirlos.

A continuación Bishop describe las técnicas de razonamiento constructivamente aceptables, y luego se ocupa de las que no lo son:

La existencia constructiva es mucho más restrictiva que la existencia ideal de las matemáticas clásicas. La única manera de demostrar la existencia de un objeto es proporcionar un proceso finito para encontrarlo, mientras que en las matemáticas clásicas se pueden utilizar otros métodos. De hecho, el siguiente principio es válido en las matemáticas clásicas: o bien todos los elementos de A

> *tienen la propiedad P, o bien existe un elemento de A con la propiedad no P. Este principio, al que llamaremos principio de omnisciencia, se encuentra en la raíz de la mayoría de los argumentos no constructivos de las matemáticas clásicas. Esto es cierto incluso para el principio de omnisciencia en su forma más simple: si $\{n_k\}$ es una secuencia de números naturales, entonces $n_k = 0$ para algún k o $n_k \neq 0$ para todo k. Llamaremos a esto el principio limitado de omnisciencia. Un teorema tras otro de las matemáticas clásicas depende esencialmente del principio limitado de omnisciencia y, por lo tanto, no es constructivamente válido. Algunos ejemplos de esto son el teorema que afirma que una función continua con valores reales en un intervalo cerrado y acotado alcanza su máximo, el teorema del punto fijo para una función continua de una bola cerrada en sí misma, el teorema ergódico y el teorema de Hahn-Banach. Sin embargo, estos teoremas no se pierden en la matemática constructiva. Cada uno de estos teoremas P tiene un sustituto constructivo Q, que es un teorema constructivamente válido que implica P en el sistema clásico mediante un argumento más o menos simple basado en el principio limitado de omnisciencia. Por ejemplo, la afirmación de que toda función continua de una bola cerrada en el espacio euclídeo en sí misma admite un punto fijo encuentra un sustituto constructivo en la afirmación de que dicha función admite un punto arbitrariamente cercano a su imagen.*
>
> *El grado en que existen buenos sustitutos constructivos para los teoremas de las matemáticas clásicas puede considerarse una demostración de que estas matemáticas tienen una base sustancial de verdad constructiva.*

Curiosamente, Bishop acepta como constructivo al axioma de elección (aunque se refiere al axioma de elección numerable):

> *Cuando un matemático clásico se proclama constructivista, probablemente quiere decir que evita el axioma de elección. Este axioma es único en su capacidad de inquietar al matemático clásico, pero en realidad no es una fuente real de los aspectos no constructivos de las matemáticas clásicas. Existe una función de elección en las matemáticas constructivas, porque la elección está implícita en el significado mismo de la existencia. Las aplicaciones del axioma de elección en las matemáticas clásicas, o bien son irrelevantes o bien están asociadas a una apelación generalizada al principio de omnisciencia. El axioma de elección se utiliza para extraer elementos de clases de equivalencia donde nunca deberían haberse incluido. Por ejemplo, un número real no debería definirse como una clase de equivalencia de sucesiones de Cauchy de números racionales; no hay necesidad de arrastrar las clases de equivalencia. La prueba de que los números reales pueden estar bien ordenados es un ejemplo de prueba en la que se combina un uso generalizado del principio de omnisciencia con una apelación al axioma de elección. Tales pruebas ofrecen pocas esperanzas de constructivización. No es probable que el teorema "los números reales pueden estar bien ordenados" admita una versión constructiva consonante con la interpretación intuitiva del resultado clásico.*
>
> *Se han presentado casi toda forma imaginable de resistencia a un tratamiento realista y directo de las matemáticas, incluso por parte de los constructivistas. Brouwer, quien ha hecho más por las matemáticas constructivas que nadie, consideró necesario introducir una teoría revolucionaria y semimística del continuo. Weyl, un gran matemático que en la práctica reprimió sus convicciones constructivistas, expresó la opinión de que las matemáticas idealistas encuentran su justificación en sus aplicaciones a la física. Hilbert, quien insistía en la constructividad en las metamatemáticas, pero creía que el precio de una matemática constructiva era demasiado alto, estaba dispuesto a conformarse con la consistencia. Los discípulos de Brouwer unieron fuerzas con los lógicos en un intento por formalizar la matemática constructiva. Otros buscan la verdad constructiva en el marco de la teoría de funciones recursivas. Otros buscan un atajo hacia la realidad, un punto de vista que revele repentinamente la matemática clásica bajo una luz constructiva. Ninguno de estos sustitutos de un enfoque realista directo ha funcionado. No es exagerado decir que aún no se ha intentado un enfoque realista directo de las matemáticas. Es hora de intentarlo.*

En los capítulos siguientes Bishop expone —de acuerdo con su criterio de constructividad— los resultados básicos sobre el cálculo diferencial e integral en $\mathbb{R}$, la teoría de conjuntos, los espacios métricos, el análisis complejo, la teoría de la medida, la teoría general sobre integración, los espacios normados, los grupos abelianos localmente compactos y las álgebras de Banach conmutativas. No vamos a entrar en detalles, pero mostramos algunos ejemplos que ilustren el carácter de este constructivismo. El capítulo 2, dedicado al cálculo diferencias

e integral, empieza con algunas consideraciones conjuntistas elementales, en las que Bishop no se ciñe a ninguna teoría axiomática formal, sino que define los conceptos que necesita en términos materiales. Por ejemplo:

> *Una sucesión es una regla que asocia a cada entero positivo n un objeto matemático a_n. El objeto a_n se denomina término n-simo de la sucesión. La regla puede darse explícitamente o dejarse indefinida, por ejemplo, escribiendo los elementos de la sucesión en orden:*
>
> $$\{a_1, a_2, a_3, \ldots\}$$
>
> *hasta que la regla de formación quede clara.* [...]
>
> *La totalidad de los objetos matemáticos construidos de acuerdo con ciertos requisitos se denomina conjunto. Los requisitos de la construcción, que varían según el conjunto considerado, determinan el conjunto.* [...] *Cada conjunto A estará dotado de una relación $=$ de igualdad. Esta relación es una cuestión de convención, salvo que debe ser una relación de equivalencia.*

Esto se entiende considerando cómo define Bishop los números reales:

> **Definición 1:** *Una sucesión $\{x_n\}$ de números racionales es regular si*
>
> $$|x_m - x_n| \leq m^{-1} + n^{-1} \qquad (n \in \mathbb{Z}^+).$$
>
> *Un número real es una sucesión regular de números racionales. Dos números reales $x \equiv \{x_n\}$ e $y \equiv \{y_n\}$ son iguales si*
>
> $$|x_n - y_n| < 2n^{-1}$$
>
> *El conjunto de números reales se denota por $\mathbb{R}$.*

Así, tal y como había anunciado, Bishop no define los números reales como clases de equivalencia de sucesiones de números racionales, sino como las sucesiones mismas:

> *Obsérvese que un número real es una sucesión regular de números racionales, no una clase de equivalencia de sucesiones regulares de números racionales. Definir un número real como una clase de equivalencia sería incorrecto o inútil; inútil (pero correcto) si se requiere especificar la clase de equivalencia mediante una secuencia regular particular de números racionales que le pertenezca, e incorrecto en caso contrario.*

Y en el conjunto de tales sucesiones se establece arbitrariamente una relación de igualdad, que no es la igualdad propiamente dicha (es la igualdad de números reales). En el capítulo 3, dedicado a la teoría de conjuntos, precisa esta idea:

> *La noción de igualdad, a diferencia del uso clásico, es una convención. Definimos lo que significa que los elementos de un conjunto dado sean iguales, pero la noción de igualdad de elementos de conjuntos diferentes no está definida. La única manera de considerar iguales los elementos de conjuntos diferentes A y B es considerar A y B como subconjuntos de un tercer conjunto C. Por esta razón, definimos las operaciones de unión e intersección sólo para conjuntos que vienen dados como subconjuntos de un conjunto dado.*

Entre los preliminares conjuntistas del capítulo 2 se encuentran éstos:

> *Un conjunto A es numerable si existe una aplicación $f : \mathbb{Z}^+ \longrightarrow A$ suprayectiva. Intuitivamente, esto significa que los elementos de A pueden ordenarse en una sucesión con posibles duplicaciones.*
>
> *Para cada entero positivo n, sea $\mathbb{Z}_n$ el conjunto $\{0, 1, \ldots, n-1\}$. Se dice que un conjunto A que es equipotente con $\mathbb{Z}_n$ tiene n elementos. Estos conjuntos se denominan finitos. Todo conjunto finito es numerable. Contrariamente al uso habitual, todo conjunto finito o numerable tiene al menos un elemento.*
>
> *Si existe una aplicación de $\mathbb{Z}_n$ a un conjunto A, decimos que A tiene como máximo n elementos. Estos conjuntos A se denominan subfinitos.*
>
> *No es cierto que todo conjunto numerable sea infinito numerable o subfinito. Por ejemplo, supongamos que A está formado por todos los enteros positivos n tales que tanto n como $n+2$ son primos. Entonces A es numerable, pero no es ni infinito numerable ni subfinito. Esto no significa que en*

algún momento futuro A no se vuelva numerablemente infinito o subfinito. Es posible que mañana alguien demuestre que A es subfinito.

Este conjunto A tiene la propiedad de que si es subfinito, entonces es finito. No todos los conjuntos tienen esta propiedad.

Con estas "salvedades", Bishop acaba demostrando teoremas como que la derivada de x^n es nx^{n-1}, y versiones débiles de algunos otros, como esta versión del teorema del valor medio:

Teorema 7 *Sea f diferenciable en el intervalo $[a, b]$. Entonces, para cada $\epsilon > 0$ existe un x en $[a, b]$ tal que*

$$|f(b) - f(a) - f'(x)(b - a)| \leq \epsilon.$$

Bishop presenta incluso una versión constructiva de la no numerabilidad de $\mathbb{R}$:

Teorema 1 *Sea $\{a_n\}$ una sucesión de números reales. Sean x_0 e y_0 números reales $x_0 < y_0$. Entonces existe un número real x con $x_0 \leq x \leq y_0$ y $x \neq a_n$ $(n \in \mathbb{Z}^+)$.*

En el capítulo 3 dice:

El conjunto de todas las funciones de un conjunto A a un conjunto B se escribirá $F(A, B)$. Cuando A no es numerable, el conjunto $F(A, B)$ parece tener poco interés práctico, ya que comprender su estructura es demasiado difícil. Por ejemplo, Brouwer ha afirmado que todas las funciones en $F(\mathbb{R}, \mathbb{R})$ son continuas, pero no se conoce ninguna prueba aceptable.

En 1972 Bishop publicó otro libro titulado *Teoría de la medida constructiva,* junto con Henry Cheng, que se había doctorado bajo su dirección el año anterior. En 1973 la *American Mathematical Society* invitó a Bishop a dar una serie de cuatro charlas de una hora, a la que dio el título de *Esquizofrenia en las matemáticas contemporáneas.* Empieza con una crítica a las matemáticas contemporáneas:

El sentido común es una cualidad constantemente atacada. Tiende a ser reemplazado por la metodología, transformándose en dogma. La codificación de la comprensión sólo es loable en la medida en que la metodología resultante no se eleve a la categoría de dogma y, por lo tanto, impida la formación de nuevas ideas.

Las matemáticas contemporáneas han presenciado el triunfo del dogma formalista, que tuvo su origen en la importante idea de que la mayoría de los argumentos de las matemáticas modernas pueden descomponerse y presentarse como aplicaciones sucesivas de unos pocos esquemas básicos. Los expertos ahora equiparan sistemáticamente el panorama de las matemáticas con las producciones de tal o cual sistema formal. Las demostraciones se consideran manipulaciones de cadenas de símbolos. La filosofía matemática consiste en la creación, comparación e investigación de sistemas formales.

El objetivo es la consistencia. En consecuencia, el significado se degrada e incluso deja de existir en un nivel primario. La degradación del significado tiene otra fuente: la negativa deliberada del matemático contemporáneo a examinar el contenido de algunos de sus términos, como la frase "existe". Se niega a distinguir entre los diferentes significados que podrían atribuirse a esta frase. Además, es impreciso respecto a su significado. Cuando se le presiona, tiende a refugiarse en formalismos, declarando que el significado de la frase y los enunciados de los que forma parte sólo pueden entenderse en el contexto de todo el conjunto de suposiciones y técnicas a su disposición. De este modo, invierte el orden natural, que sería desarrollar primero el significado y luego basar sus suposiciones y técnicas en la roca del significado. La preocupación por esta degradación del significado es una fuerza principal detrás del constructivismo. Dado que el significado se degrada y se rechaza el sentido común, no es sorprendente descubrir que los medios son inadecuados para los fines. Las matemáticas aplicadas dan mucha importancia al concepto de modelo como herramienta para abordar la realidad por medios matemáticos. Cuando el modelo no es una representación adecuada de la realidad, como sucede con demasiada frecuencia, los medios resultan inadecuados. Da la impresión de que algunos constructores de modelos ya no se interesan por la realidad. Sus modelos se han vuelto autónomos. Esto ha sucedido claramente en la filosofía matemática: los modelos (sistemas formales) se aceptan como las herramientas preferidas para la investigación de la naturaleza de las matemáticas, e incluso como la fuente de significado.

> *Cualquiera que haya enseñado matemáticas a nivel universitario debe haber quedado impresionado por la naturaleza esotérica de la comunicación. No es natural que "A implica B" signifique "no A o B", y los estudiantes te lo dirán si les das la oportunidad.*[3] *Por supuesto, esta no es una objeción fatal. La cuestión es si la definición estándar de implicación es útil, no si es natural. El constructivista, siguiendo a Brouwer, sostiene que una definición más natural de implicación sería más útil. Este punto se desarrollará más adelante. Uno de los conceptos más difíciles de comunicar al estudiante universitario es el concepto de demostración. Con razón: el concepto es esotérico. La mayoría de los matemáticos, cuando se les presiona para que digan qué entienden por demostración, recurrirán a criterios formales. La noción constructiva de demostración, en cambio, es muy simple, como veremos a su debido tiempo.*

La noción constructiva tan simple de "demostración" es, como veremos, que *una demostración es cualquier argumento completamente convincente.* Y nadie niega —o nadie debería negar— que ésa es la noción material (no formal) de demostración, pero Bishop debería darse cuenta de que no es apropiada para tratar asuntos que exceden nuestra capacidad de intuición (que Bishop sobreestima), donde pueden surgir discrepancias irreconciliables. Si Bishop juzga un argumento no convincente porque usa el tercio excluso y otro matemático lo encuentra absolutamente convincente y todas las objeciones que le pueda plantear Bishop le resultan irrelevantes, ¿qué convicción debemos dar por válida? El mismo Bishop admite que algunos constructivistas no aceptan algunos de sus puntos de vista.

Por otro lado, Bishop mezcla confusamente el concepto material de demostración con el concepto formal. Decir que el concepto formal de demostración es esotérico es como preguntarle a alguien sin formación matemática por el concepto de movimiento continuo y deducir de que no sepa precisar qué entiende por "continuidad" que el concepto de "continuidad" es esotérico. Si un estudiante (o un matemático) no es capaz de precisar lo que entiende por demostración formal, lo que necesita es un curso de lógica matemática, pues ésa es una de las funciones principales de dicha disciplina.

> *Igualmente esotérico, y quizás más problemático, es el concepto de existencia. Algunos de los problemas asociados con este concepto ya se han mencionado, y volveremos a tratarlo. Finalmente, deseo señalar la naturaleza esotérica del concepto clásico de verdad. Como veremos más adelante, la verdad no es una fuente de problemas para el constructivista, debido a su énfasis en el significado.*

Esto es una obviedad: está claro que es posible razonar formalmente, y entonces el concepto de "verdad" deja de ser relevante, porque el formalismo está diseñado precisamente para que la "verdad" sea irrelevante sin que ello suponga ningún problema, y, en determinadas circunstancias, es posible razonar materialmente, y esto requiere tener claro el significado de cualquier afirmación que se discuta. Sólo el razonamiento material puede tener problemas con el concepto de "verdad", pues se ve en la obligación de justificar que cada afirmación que se hace tenga un significado concreto y sea verdadera, lo cual, en cuanto el objeto de estudio se complica, puede dar lugar a disensiones irreconciliables, como ya hemos señalado, sobre lo que es verdad y lo que no lo es. Y es por esto que el razonamiento material no es adecuado para el desarrollo de la matemática abstracta (incluso para el desarrollo de la matemática intuitiva si uno se encuentra con alguien que decide negar cosas como el principio del tercio excluso sin más base que sus propios prejuicios).

> *La fragmentación de las matemáticas se debe en parte a la vastedad de la materia, pero se ve agravada por nuestro sistema educativo. A un estudiante de posgrado en matemáticas puras se le puede exigir o no que amplíe sus conocimientos aprobando exámenes en diversas ramas de la matemática pura, pero casi con seguridad no se le exigirá, ni siquiera se le animará, a familiarizarse con la filosofía de las matemáticas, su historia ni sus aplicaciones. Nos hemos orientado a formar investigadores matemáticos que comiencen a escribir artículos académicos lo antes posible. Este proceso antisocial y antiintelectual frustra incluso sus propios límites. Es improbable que la situación cambie hasta que modifiquemos nuestra concepción de las matemáticas. Antes de que se produzcan cambios importantes en nuestros métodos educativos y nuestros valores profesionales, tendremos que descubrir la importancia del teorema y la demostración. Si continuamos centrando la atención en el proceso de producción de teoremas y seguimos devaluando su contenido, la fragmentación es inevitable.*

[3] Bishop declaró en cierta ocasión que fue a raíz de que unos estudiantes le preguntaran por esto por lo que empezó a elaborar su filosofía constructivista.

Esto es irrelevante para el asunto que se trata aquí. De hecho, que el formalismo marque una línea divisoria clara y estricta entre las matemáticas y la filosofía matemática, que a su vez vuelve a las primeras inmunes a cualquier consideración de la segunda es, sin duda, la mayor bendición que han podido recibir las matemáticas. Un poco más adelante, Bishop presenta el punto de vista constructivista:

> *Al analizar los principios del constructivismo, intentaré separar los aspectos fundamentales de la filosofía de aquellos que son meramente convenientes (o inconvenientes, según el caso). Cuatro principios se destacan como base:*
>
> *(A) Las matemáticas son sentido común.*
>
> *(B) No preguntes si una afirmación es verdadera hasta que entiendas lo que significa.*
>
> *(C) Una demostración es cualquier argumento completamente convincente.*
>
> *(D) Es importante mantener las distinciones significativas.*

El principio (A) es muy burdo, porque requiere ser precisado y al final la precisión siempre acaba siendo: *Las matemáticas son lo que dice MI sentido común, frente a lo que diga el sentido común de los demás.*

> *Sorprendentemente, muchas personas brillantes se niegan a aplicar el sentido común a las matemáticas. Una actitud frecuente es que la formalización de las matemáticas ha sido de gran valor, ya que el formalismo constituye un tribunal de última instancia para resolver cualquier disputa que pueda surgir sobre la corrección de una demostración.*

Efectivamente.

> *El sentido común nos dice, por el contrario, que si una demostración es tan compleja que no podemos determinar su corrección mediante métodos informales, tampoco podremos comprobarla por medios formales.*

Y aquí tenemos una muestra clara de por qué no es buena idea fiarse de "el sentido común", que al final no tiene nada de "común", sino que siempre acaba siendo "mi sentido mío y sólo mío".

> *Además, el formalismo no puede utilizarse para resolver disputas filosóficas, ya que simplemente refleja la filosofía básica y, en consecuencia, los desacuerdos filosóficos inevitablemente resultarán en desacuerdos sobre la validez del formalismo.*

Efectivamente, el formalismo no se usa para resolver disputas filosóficas, sino para dejar que los filósofos traten de resolver sus disputas filosóficas sin que ello afecte al trabajo formal del matemático.

> *El principio (B) resuelve el problema de la verdad constructiva. De hecho, resolvería el problema de la verdad clásica si los matemáticos clásicos lo aceptaran.*

De donde se deduce una vez más que el sentido común de Bishop tiene poco en común con el sentido común de los matemáticos clásicos, con lo que podría ocurrir perfectamente que, al fin y al cabo, las matemáticas no fueran el sentido común de Bishop, sino el sentido común de los matemáticos clásicos que consideran razonable el punto de vista formalista.

> *Podríamos decir que la verdad es una cuestión de convenio. Esto simplemente significa que todos los argumentos relativos a la verdad o falsedad de cualquier enunciado dado, sobre el cual ambas partes poseen los mismos hechos relevantes, surgen porque no han llegado a un acuerdo claro sobre el significado del enunciado. Por ejemplo, en respuesta a la pregunta "¿Es cierto que los constructivistas creen que no toda sucesión monótona acotada de números reales converge?", si estoy cansado, respondo "sí". Pero si no, le digo a quien pregunta que mi respuesta dependerá del significado que quiera asignar al enunciado $(*)$ de que toda sucesión monótona acotada de números reales converge. Además, le digo que una vez que haya asignado un significado preciso al enunciado $(*)$, probablemente le quedará clara mi respuesta a su pregunta antes de dársela. Los dos significados que se suelen asignar a $(*)$ son el clásico y el constructivo. Me parece que el matemático clásico no es tan preciso como podría serlo en cuanto al significado que asigna a tal enunciado.*

Lo que Bishop parece no entender es que cuando los matemáticos "clásicos" hablan de verdad o falsedad de un enunciado, en realidad es una forma coloquial de plantearse si se puede demostrar o no. Lo cual no

hace referencia a ningún concepto de "verdad" que pueda ser acordado. Al contrario, cuando un matemático "clásico" dice que es verdad que toda sucesión monótona acotada de números reales converge, no está diciendo nada realmente sobre su "verdad", sino únicamente que tiene un argumento que así lo demuestra, y que ese argumento es formalmente válido como teorema de ZF o de cualquier otra teoría formal razonable para tratar el asunto. Decir que el matemático clásico no es preciso asignando un significado al enunciado es no entender —o, probablemente, no querer entender— lo que es el formalismo, porque la esencia del formalismo es entender que no hay que asignar ningún significado al enunciado para demostrarlo.

> *Siempre que un estudiante me pregunta si una demostración que ha presentado es correcta, antes de responder a su pregunta intento descubrir su concepto de qué constituye una demostración. Luego le comento mi propio concepto (C) mencionado anteriormente y le pregunto si considera su argumento completamente convincente y si cree haberse expresado con la suficiente claridad como para que otras personas informadas e inteligentes también queden completamente convencidas. Claramente, es imposible aceptar (C) sin aceptar (B), porque no tiene sentido estar convencido de que algo es cierto a menos que se sepa su significado.*
>
> *A menudo surge la pregunta de si un constructivista aceptaría una demostración no constructiva de un resultado numérico que no implica cuantificadores existenciales, como la conjetura de Goldbach o el último teorema de Fermat. Mi respuesta es (C): Quisiera examinar la demostración para ver si la encuentro completamente convincente. Quizás deberíamos mantener la mente abierta, pero me cuesta creer que cualquier prueba basada en el principio del tercio excluso, por ejemplo, me resulte completamente convincente. Afortunadamente, el problema es hipotético, porque tales pruebas no parecen surgir. Sin embargo, plantea la interesante cuestión de que una prueba clásicamente aceptable de la conjetura de Goldbach podría no ser constructivamente aceptable y, por lo tanto, las interpretaciones clásica y constructiva de la conjetura de Goldbach deben diferir en algún aspecto fundamental. Más adelante veremos que, efectivamente, éste es el caso.*

Todo el argumento de Bishop se desmorona sin más que insertar un pronombre que, naturalmente, la gramática inglesa obliga a que esté en la frase original, pero que haberlo dejado en la traducción habría sido tramposo: *Quisiera examinar la demostración para ver si* YO *la encuentro completamente convincente.*

Terminamos comentando un pasaje en el que Bishop plantea lo que dice SU sentido común sobre las funciones recursivas:

> *Si bien es cierto que los intuicionistas consideran el concepto constructivo de una secuencia generada por un algoritmo demasiado preciso para describir adecuadamente el sistema de números reales, los especialistas en la teoría de funciones recursivas, en cambio, lo consideran demasiado vago.*

Se refiere a que lo consideran demasiado vago para tratar con él sin precisarlo debidamente a través del concepto de función recursiva.

> *Quieren especificar con mayor precisión qué se entiende por algoritmo, y encuentran un candidato en la noción de función recursiva. Solo admiten secuencias de números enteros o racionales que sean recursivas (un concepto que no definiremos aquí: véase* [La Introducción a la metamatemática, de Kleene] *para más detalles). Sus razones son que el concepto es más preciso que el concepto ingenuo de algoritmo, que todo algoritmo definido ingenuamente ha resultado ser recursivo, y parece improbable que alguna vez descubramos un algoritmo que no lo sea.*

Cuestionar la tesis de Church-Turing en 1973 no era muy serio.

> *Este requisito de que toda secuencia de números enteros debe ser recursiva es erróneo por tres razones fundamentales. En primer lugar, y lo más importante, no cabe duda de que el concepto ingenuo es básico, y la importancia del concepto recursivo se deriva de la presunción de que todo algoritmo resultará ser recursivo.*

Cuestionar la tesis de Church-Turing en 1973 no era muy serio.

> *En segundo lugar, las matemáticas se complican en lugar de simplificarse debido a la restricción a sucesiones recursivas. Si existe alguna duda al respecto, se puede resolver comparando algunos de los desarrollos recursivistas del análisis elemental con el tratamiento constructivista del mismo material.*

> *Incluso si uno se orienta a ejecutar material en una computadora, la formulación recursivista constituiría un obstáculo, ya que es muy probable que la presentación recursiva se traduzca al lenguaje informático traduciéndola primero a la terminología constructiva común (al menos mentalmente) y luego al lenguaje de la computadora que se esté utilizando.*

Eso es como decir que la caracterización algebraica de la constructibilidad con regla y compás es una complicación innecesaria, porque a la hora de construir un pentágono con regla y compás es inútil pensar en extensiones de cuerpos. Por si esto no deja claro del todo que Bishop no entiende la teoría de las funciones recursivas, su "tercera razón" elimina todo margen de duda:

> *En tercer lugar, no se consigue ninguna mejora en la precisión. Uno de los procedimientos para definir el valor de una función recursiva consiste en buscar una secuencia de enteros uno por uno y elegir el primero distinto de cero, tras haber demostrado previamente que uno de ellos es distinto de cero. Por lo tanto, la noción de función recursiva es al menos tan imprecisa como la de una demostración correcta.*

Para Bishop el concepto de "función recursiva parcial" y el análisis del problema de la detención que la teoría de funciones computables (en cualquiera de sus formas equivalentes) permite analizar con completa precisión, son, sin duda, algo completamente desconocido.

> *Esta última noción, sin duda, no es más precisa que la ingenua noción de una sucesión (constructiva) de enteros. El deseo de lograr una precisión completa, sea cual sea, está condenado al fracaso.*

Vemos así que, complementando la frase de Kreisel con la que termina el capítulo I, el formalismo (radical) no es la única forma de pensamiento radical que incapacita para reconocer el progreso cuando se observa.

> *Lo que realmente se busca es garantizar que no surjan desacuerdos. Las matemáticas son una actividad tan compleja que es inevitable que surjan desacuerdos.*

Es inevitable cuando se rechaza la forma de evitar desacuerdos y se confía todo al "sentido común sólo mío".

> *Además, los matemáticos siempre se verán tentados a probar nuevas ideas tan complejas o innovadoras que su significado sea cuestionable. Lo importante no es desarrollar un marco, como la teoría de funciones recursivas, con la vana esperanza de prevenir innovaciones cuestionables, sino someter cada desarrollo a un escrutinio intenso (en términos de significado, no desde el punto de vista formal).*

Este pasaje ya roza la teoría de la conspiración.

Bishop murió de cáncer a los 54 años en 1983, tras una breve convalecencia. Unos meses después se organizó un congreso en su honor en la Universidad de California. Entre los participantes, Halsey Lawrence Royden fue el encargado de comentar su labor sobre el constructivismo:

> *Así pues, con gran entusiasmo y placer leí el libro de Errett tras su publicación. Se trataba de un tratamiento sistemático del análisis desde una perspectiva completamente constructiva, eliminando el misticismo del intuicionismo anterior y demostrando que gran parte del material importante del análisis moderno podía abordarse en un sistema de este tipo mediante métodos no muy alejados del tratamiento clásico. El libro ofrece una explicación clara de los teoremas constructivos de Brouwer, pero simplemente elude cuestiones tan arcanas e irrelevantes como la existencia de una función definida en todas partes que no sea continua.*
>
> *Además de demostrar que el análisis constructivo no tiene por qué ser una truncación drástica del análisis clásico, Bishop demuestra que, en muchos casos, la reformulación de un teorema clásico para obtener uno constructivamente válido no sólo aporta una nueva perspectiva del teorema, sino que a menudo también resulta en un teorema con mayor contenido (clásico) que el original.*
>
> *Me sorprendió y me decepcionó que el libro de Errett haya tenido tan poco impacto en el pensamiento de la mayoría de los matemáticos actuales. Sé que Errett llegó a sentir que la mayoría de los matemáticos eran indiferentes y ajenos a todas las cuestiones filosóficas sobre el significado de las matemáticas. El viejo mito de que las matemáticas constructivas eran demasiado complicadas, demasiado extravagantes y sacrificaban demasiado de las matemáticas clásicas ha prevalecido durante demasiado tiempo. Demasiadas generaciones de matemáticos se han acostumbrado a un realismo*

ingenuo basado en la teoría de conjuntos. Por lo tanto, una obra como la de Errett, que demuestra cuánto se puede lograr, y que debería marcar el inicio de un vigoroso intento de reconstruir el análisis en un contexto constructivo, llega demasiado tarde cuando ya no se cree en el objetivo de una base sólida para las matemáticas, o si se cree, sólo se cree en la memoria.

Aunque mis propias opiniones sobre los fundamentos de las matemáticas se inclinan hacia la postura formalista con un toque de pragmatismo, no soy inmune al atractivo de la postura constructivista. Inspirado por el libro de Errett, a menudo me he entregado a las matemáticas constructivas, quizás con una tendencia formalista a considerarlas como otro sistema formal (pero con un considerable atractivo filosófico).

En otras palabras, el formalismo cumplió su función como se esperaba de él y las matemáticas permanecieron inmunes a la filosofía de Bishop. Esto no significa que el constructivismo desapareciera con su creador, pero, como decía Royden (probablemente sin ser consciente de que Bishop habría recibido su afirmación como un puñetazo en el estómago), convertido en un sistema formal adicional. Por ejemplo, en 1988 se publicó *Constructivismo en matemáticas: una introducción,* de Anne Sjerp Troelstra y Dirk van Dalen (doctorados en 1966 y 1963, respectivamente, bajo la dirección de Heyting, que había fallecido en 1980). El libro no tiene nada que ver con los planteamientos de Brouwer o de Bishop. Tras un capítulo introductorio, que explica que hay posturas constructivistas para todos los gustos, desde el finitismo de Kronecker al intuicionismo de Brouwer, pasando por el predicativismo, el constructivismo de Bishop y las *mátemáticas recursivas constructivas* desarrolladas por Andréi Márkov hijo y su escuela (que esencialmente son teoría de la recursión combinada con la lógica intuicionista), el libro de Troelstra y van Dalen se ajusta a los estándares modernos: discute varias teorías axiomáticas y sus modelos, unas con la lógica clásica y otras con la lógica intuicionista. En palabras de los propios autores:

En este libro tendremos frecuentes ocasiones para referirnos al intuicionismo, las Matemáticas Recursivas Constructivas y las Matemáticas Constructivas de Bishop en particular. Sin embargo, este libro no está escrito desde la perspectiva de ninguna escuela o tendencia en particular mencionada anteriormente, ya que no aceptaremos ninguna de estas perspectivas como normativa para las matemáticas.

Presentamos las matemáticas constructivas (en sentido amplio) como una parte legítima de las matemáticas, que contiene material matemáticamente interesante, independientemente de cualquier sesgo filosófico.

Las matemáticas constructivas, y especialmente su lógica y sus metamatemáticas, son de considerable interés para la filosofía de las matemáticas. Existen algunos indicios de que la lógica intuicionista también puede ser útil en otras áreas de las matemáticas, como la teoría de topos o la informática teórica.

En suma, Troelstra y van Dalen hicieron con el constructivismo de Bishop justo lo contrario de lo que Bishop consideraba que había que hacer (que era justo lo que cualquier matemático actual consideraba que había que hacer).

Cuando Bishop murió, llevaba tres años trabajando con Douglas Bridges en una segunda edición revisada de su libro *Fundamentos del análisis constructivo,* que finalmente fue publicada en 1985.

Posiblemente Bishop fue "el último rebelde" que trató de convencer a los matemáticos de que lo que hacían estaba mal y había que cambiarlo. Ha habido más matemáticos que han propuesto fundaciones alternativas para la matemática constructiva, pero lo han hecho siguiendo todos los estándares modernos, a través de sistemas deductivos formales que, a ojos de un formalista, son meros sistemas axiomáticos adicionales que se pueden usar o estudiar, o no, como una alternativa más, de modo que se puede prescindir de toda la filosofía más o menos radical que ensalce unos en detrimento de otros.

Es el caso de la *Teoría de Tipos Intuicionista* o *Teoría de Tipos Constructiva,* del sueco Per Erik Rutger Martin-Löf (doctorado en 1970 bajo la dirección de Kolmogórov), publicada en 1972, o de la *Lógica lineal,* del francés Jean-Yves Girard (publicada en 1987). Ambas tienen aplicaciones a los lenguajes de programación y a los sistemas de demostración asistida por ordenador.

Así, al margen de las concepciones filosóficas de cada cual, que el formalismo vuelve irrelevantes, estudiar la matemática constructiva es equivalente a lo que hace, por ejemplo, un algebrista cuando decide estudiar únicamente los grupos finitos, sin interesarse por los infinitos. Es sólo una acotación arbitraria y legítima del campo de trabajo de cada uno.

3.2 El análisis no estándar

En 1966 Abraham Robinson publicó su libro *Análisis no estándar,* en el que presentó sistemáticamente su teoría que le permitía reformular rigurosamente el análisis matemático en términos de cantidades infinitesimales,[4] y dedicaba sus distintos capítulos a mostrar cómo podía aplicarse en diversas áreas: el cálculo diferencial e integral, la teoría de funciones de variable compleja, el análisis funcional, e incluso aplicaciones a la física (a la teoría del potencial, la hidrodinámica, etc.) De hecho, sus métodos permitían un tratamiento no estándar incluso de espacios topológicos arbitrarios, no necesariamente metrizables. La idea básica es que a cada punto x de un espacio topológico se le puede asociar (imitando el lenguaje de la filosofía Leibniziana) una *mónada* $\mu(x)$, que representa el conjunto de los puntos infinitamente próximos a x (pero sin relación con ninguna noción de distancia). En la introducción dice:

> *Es natural preguntarse si un método no estándar (en el sentido técnico en que se utiliza aquí el término no estándar, es decir, un método de análisis no estándar) siempre puede sustituirse por una demostración matemática estándar. Esta pregunta presupone que los métodos de la lógica matemática se distinguen de las matemáticas ordinarias, y, para nuestros propósitos actuales, podemos concordar en que la distinción tiene sentido en la práctica. La respuesta, entonces, es que el método de las ultrapotencias proporciona un medio fácil para traducir una demostración no estándar en una demostración matemática estándar en cada caso particular. Sin embargo, al hacerlo, podemos complicar considerablemente la demostración, por lo que con frecuencia el procedimiento resultante será menos deseable desde un punto de vista heurístico. Al mismo tiempo, bien podría existir una demostración matemática más breve que pueda obtenerse de forma independiente.*
>
> *El desarrollo de la teoría de los infinitesimales ha permanecido estancado prácticamente durante los últimos ciento cincuenta años. Durante el mismo período, se ha invertido una enorme cantidad de esfuerzo e ingenio en los métodos clásicos. Sin embargo, creemos haber demostrado que, incluso en esta etapa avanzada, los métodos no estándar pueden complementar eficazmente a los métodos estándar, tanto para arrojar nueva luz sobre teorías antiguas como para obtener nuevos resultados. Esperamos que algunos expertos, tanto en los temas abordados en este libro como en los que no, consideren la aplicación de métodos no estándar a su campo. Es posible que descubran que, en algunos casos, la interpretación no estándar adecuada de una teoría clásica no se descubre sin esfuerzo. Sin embargo, una vez encontrada, la reformulación y el desarrollo posterior de la teoría pueden ser una experiencia gratificante.*

Ese mismo año de 1966, Robinson publicó junto con Allen Richard Bernstein (que se había doctorado el año anterior bajo su dirección) un artículo titulado *Solución de un problema de subespacios invariantes de K.T. Smith y P.R. Halmos,* en el que, usando de forma esencial técnicas del análisis no estándar, demostraban una conjetura de análisis funcional que Halmos y Kennan Taylor Smith habían formulado hacía una década. El trabajo formaba parte de la tesis de Bernstein, y Robinson había enviado un borrador a Halmos en 1964. Durante ese tiempo, Halmos había estudiado la prueba y la había traducido para eliminar el análisis no estándar del argumento. La versión de Halmos fue publicada justo a continuación de la de Robinson y Bernstein, bajo el título de *Subespacios invariantes de operadores polinómicamente compactos.* Años más tarde, Halmos recordaría el caso de este modo:

> *Las pruebas mediante lógica de teoremas matemáticos, todas ellas hasta donde yo sé, son innecesarias. Pueden ser —y han sido— sustituidas por pruebas que usan el lenguaje y las técnicas de las matemáticas ordinarias. La prueba de Bernstein-Robinson usa modelos no estándar de lenguajes del cálculo de predicados de orden superior, y cuando Abby (como conocíamos a Abraham Robinson) me envió su* preprint, *tuve que sudar lo mío para localizar y traducir el contenido matemático. El artículo no me convenció (¿convenció a alguien?) de que los modelos no estándar deberían ponerse inmediatamente en la caja de herramientas de todo matemático: sólo demostraba que Bernstein y Robinson eran matemáticos inteligentes que habían resuelto un problema difícil usando un lenguaje que hablaban con fluidez. Si lo hubieran hecho en Telugu, habría encontrado el artículo mucho más difícil de decodificar, pero la dificultad extra hubiera sido de grado, no de naturaleza.*

Los expertos en análisis funcional acogieron con frialdad la demostración de Bernstein-Robinson, lo cual era predecible, pues si tenían que elegir entre una demostración que resultaba críptica para ellos o pasar unas

[4] Aunque su técnica era algo más complicada de lo necesario, pues usaba la lógica de tipos para relacionar las estructuras de partida con las estructuras no estándar. Existen formas más simples de llegar a los mismos resultados.

páginas para leer en la misma revista otra perfectamente comprensible, sin negarle a Bernstein y Robinson el mérito del descubrimiento, preferían la demostración de Halmos. Parece ser que, en privado, Robinson declaró:

> *En cuanto a la traducción estándar de Halmos, era muy agradable, pero la prueba con análisis no estándar era muy natural, mientras que la prueba estándar requería un argumento que no habría sido fácil de divisar sin haber visto antes la prueba no estándar.*

Halmos se convirtió en acérrimo detractor del análisis no estándar en particular y de las técnicas de la lógica matemática en general. Robinson murió de cáncer en 1974, a los 55 años, pero también dejó sus seguidores, como Howard Jerome Keisler, que se había doctorado en 1966 bajo la dirección de Tarski, y que en 1976 publicó su libro *Cálculo infinitesimal, un enfoque infinitesimal,* con los contenidos propios de un manual universitario de cálculo infinitesimal de una y varias variables, pero expuesto en términos del análisis no estándar. En el prefacio leemos:

> *El cálculo se desarrolló originalmente utilizando el concepto intuitivo de infinitésimo, o de número infinitamente pequeño. Sin embargo, durante los últimos cien años, los infinitésimos han sido desterrados de los cursos de cálculo por razones de rigor matemático. Los estudiantes han tenido que aprender la materia sin la intuición original. Este libro de cálculo se basa en el trabajo de Abraham Robinson, quien en 1960 encontró una manera de hacer que los infinitésimos fueran rigurosos. Mientras que un curso tradicional comienza con el difícil concepto de límite, este curso comienza con los infinitésimos, más fáciles de entender. Está dirigido al alumno principiante promedio de cálculo y cubre la secuencia habitual de tres o cuatro semestres.*
>
> *El enfoque infinitesimal ofrece tres ventajas importantes para el estudiante. Primero, se acerca más a la intuición que originariamente condujo al cálculo. Segundo, los conceptos centrales de derivada e integral se vuelven más fáciles de comprender y utilizar para el estudiante. Tercero, enseña tanto el enfoque infinitesimal como el tradicional, lo que proporciona al estudiante una herramienta adicional que podría adquirir mayor importancia en el futuro.*
>
> *Antes de describir este libro, quisiera situar la obra de Robinson en una perspectiva histórica. En la década de 1670, Leibniz y Newton desarrollaron el cálculo basándose en la noción intuitiva de los infinitésimos. Los infinitésimos se utilizaron durante doscientos años más, hasta que Weierstrass perfeccionó el primer tratamiento riguroso del cálculo en la década de 1870. Un curso de cálculo estándar actual todavía se basa en la definición de límite dada por Weierstrass. En 1960, Robinson resolvió un problema de trescientos años de antigüedad al ofrecer un tratamiento preciso del cálculo utilizando infinitésimos. El logro de Robinson probablemente se considerará uno de los mayores avances matemáticos del siglo XX.* [...]
>
> *Originalmente, me decidí a escribir este libro cuando se hizo evidente que el cálculo infinitesimal de Robinson podría hacerse accesible a los estudiantes universitarios de primer curso. La teoría se presenta de forma sencilla; por ejemplo, el trabajo de Robinson utilizaba lógica matemática, pero este libro no.*

El truco está en que Keisler presenta como axiomas todos los resultados que requerirían técnicas de la lógica matemática. Por ejemplo, presenta como axioma I* que existen "hiperreales" que extienden a los números reales, y (axioma III*) que contienen "infinitésimos" (hiperreales no nulos, pero menores en valor absoluto que cualquier número real positivo), etc., sin justificar de ningún modo cómo se construyen tales hiperreales ni como se justifica que contienen infinitésimos. El punto 4 del teorema de la página 239 es el axioma IV*. El resultado es un texto que, a primera vista, podría parecer escrito por el marqués de L'Hôpital, pero en el que Keisler se asegura de no decir nada que no sea justificable rigurosamente mediante el aparato lógico subyacente del análisis no estándar.

Halmos tenía entonces 50 años, y estaba lo suficientemente bien de salud como para resistir la lectura del libro de Keisler. Por aquel entonces era el encargado de la sección de reseñas del *Bulletin of the American Mathematical Society* y encargó una reseña justamente a Erret Bishop. El resultado se puede imaginar. Copiamos únicamente el final:

> *No es hasta la página 298 que Keisler relaciona su desarrollo del cálculo con el habitual y coloca cada cosa en lo que para él es su debido lugar. La definición convencional de límite la da a regañadientes. Le dice al estudiante: "De hecho, la idea de nuestro enfoque infinitesimal del cálculo es que es más fácil definir y explicar los límites utilizando infinitesimales". Esta afirmación merece ser examinada.*
> [...]

> *En el sentido de que Keisler ha desarrollado los límites a partir de un sistema de axiomas supuestamente consistente, éstos han sido explicados. Pero no ha explicado los axiomas. Son meras conveniencias para generar demostraciones, cuyo contenido intuitivo sin duda escapará a los estudiantes. Si no lo creen, léanlos, en particular los axiomas*[5] V* *y* VI*. *Por supuesto, todas las nociones habituales se definen, tarde o temprano, de la forma habitual, porque el cálculo trata sobre los números reales. El libro no ofrece ninguna evidencia de que los números hiperreales sean algo más que un mecanismo para demostrar teoremas sobre los números reales. Ni siquiera son un mecanismo eficiente, ya que dependen, entre otros factores, de los axiomas* V* *y* VI*.
>
> *Las complicaciones técnicas introducidas por el enfoque de Keisler son de menor importancia. El verdadero daño reside en su ofuscación y desvitalización de esas maravillosas ideas. Ninguna invocación de Newton y Leibniz justificará el desarrollo del cálculo utilizando los axiomas* V* *y* VI* *¡con el argumento de que la definición habitual de límite es demasiado complicada!*
>
> *Aunque parece que es inútil, siempre les digo a mis estudiantes de cálculo que las matemáticas no son esotéricas: son de sentido común. (Incluso la famosa definición de límite* $\epsilon - \delta$ *es de sentido común y, además, fundamental para los importantes problemas prácticos de aproximación y estimación). No me creen. De hecho, la idea los incomoda porque contradice su experiencia previa. Ahora tenemos un texto de cálculo que puede usarse para confirmar su experiencia de que las matemáticas son un ejercicio técnico esotérico y sin sentido.*

Ese mismo año (1977) Keisler publicó una breve nota en la sección de cartas al director de las *Notices of the American Mathematical Society,* en la que decía:

> *Varias personas me han instado a comentar sobre el tratamiento de mi libro "Elementary Calculus" en el Boletín de la AMS de marzo de 1977. El Boletín rara vez reseña libros de cálculo. Presumiblemente, mi libro fue reseñado porque es controvertido al reintroducir los infinitesimales en el curso de cálculo. El revisor, Errett Bishop, no ha impartido clases a partir del libro y no puede saber cómo se desarrolla en el aula. Sin embargo, Bishop es el exponente más conocido del constructivismo, una postura extrema que rechaza todas las demostraciones indirectas y gran parte de las matemáticas modernas. Un constructivista no tiene más remedio que oponerse a un libro que añade un nuevo método no constructivo al curso de cálculo.*
>
> *La pregunta principal es: ¿por qué Paul Halmos, editor de reseñas de libros del Boletín, eligió a un constructivista como revisor? Es como elegir a un abstemio para catar vino.*[6]

La teoría de Nelson También en 1977, Edward Nelson publicó *Internal Set Theory, un nuevo enfoque del análisis no estándar,* un artículo en el que presenta una teoría axiomática que simplifica radicalmente el uso del análisis no estándar. Ésta tiene tres conceptos no definidos: "conjunto", la "pertenencia" y "ser estándar". Por ello, su lenguaje formal es el de ZFC al que se le ha añadido un relator monádico st, de modo que $\mathrm{st}(x)$ se lee "x es estandar". Los axiomas de la teoría son los mismos que los de ZFC más tres esquemas axiomáticos. Nelson le dio a su teoría el ingenioso nombre de IST, donde las siglas pueden verse como las iniciales de *Internal Set Theory* (Teoría de Conjuntos Internos), o también como las iniciales de los tres esquemas axiomáticos adicionales: *Idealisation, Standarization* y *Tranfer* (Idealización, Estandarización y Transferencia).

El hecho de que todos los axiomas de ZFC son también axiomas de IST nos da inmediatamente:

Todo teorema de ZFC es un teorema de IST.

Pero aquí hay una sutileza. Las fórmulas ϕ del lenguaje de ZFC, es decir, las que no contienen el relator st, se llaman *fórmulas internas.* En ZFC se demuestra que si $\phi(x, x_1, \ldots, x_n)$ es una fórmula (interna) se cumple

$$\bigwedge y \bigvee z \bigwedge x(x \in z \leftrightarrow x \in y \wedge \phi(x)),$$

es decir, que existe un conjunto cuyos elementos son los conjuntos $x \in y$ que cumplen $\phi(x)$, que es el que representamos por $\{x \in y \mid \phi(x)\}$. El punto está en que, al trabajar en ZFC decimos que esto vale "para toda fórmula ϕ", pero, en el contexto de IST, esto mismo hay que expresarlo diciendo "para toda fórmula interna ϕ".

[5] AXIOMA V*: *Para cada función real f de una o más variables, existe una función hiperreal correspondiente f^* del mismo número de variables, llamada extensión natural de f. La extensión natural de las funciones suma, resta, producto y recíproca son las funciones hiperreales dadas en el Axioma* I*.

AXIOMA VI* *Si dos sistemas de fórmulas tienen exactamente las mismas soluciones reales, entonces tienen exactamente las mismas soluciones hiperreales. (Un sistema de fórmulas es un conjunto finito de ecuaciones e inecuaciones).*

[6] En 1986 Ian Stewart lo comparó con elegir a Margaret Tatcher para hacer una reseña de *El capital.*

Con ello no es que estemos restringiendo el teorema de especificación, sino meramente estamos señalando que no lo estamos extendiendo, que el teorema de especificación en IST es el mismo que en ZFC, en cuanto a que es válido exactamente para las mismas fórmulas, que en ZFC son todas, pero en IST esas mismas fórmulas son sólo las fórmulas internas.

En particular, en IST no podemos considerar, por ejemplo $\{x \in \mathbb{R} \mid \mathrm{st}(x)\}$. Este conjunto no está bien definido porque no podemos aplicar el teorema de especificación a la fórmula $\mathrm{st}(x)$, ya que no es interna. Enseguida veremos que el principio de estandarización nos da la forma de definir conjuntos en IST mediante fórmulas no necesariamente internas.

Pasamos ya a describir brevemente los tres principios I, S, T que hay que añadir a los axiomas de ZFC para tener los de IST:

Transferencia Si $\phi(x, x_1, \ldots, x_n)$ es una fórmula interna (es decir, una fórmula del lenguaje de ZFC, en la que no aparece el relator st), la fórmula siguiente es un axioma:

$$\bigwedge{}^{\mathrm{st}} x_1 \cdots x_n (\bigwedge{}^{\mathrm{st}} x\, \phi(x, x_1, \ldots, x_n) \to \bigwedge x\, \phi(x, x_1, \ldots, x_n)),$$

(donde $\bigwedge^{\mathrm{st}} x\, \alpha$ es una abreviatura por $\bigwedge x(\mathrm{st}(x) \to \alpha)$.

En otras palabras: para demostrar que todo conjunto x cumple una propiedad interna con parámetros estándar (en este caso la propiedad $\phi(x, x_1, \ldots, x_n)$, donde "interna" quiere decir que es definible en ZFC, sin usar el relator st) basta probar que todo conjunto estándar la cumple.

Equivalentemente, negando la implicación:

$$\bigwedge{}^{\mathrm{st}} x_1 \cdots x_n (\bigvee x\, \phi(x, x_1, \ldots, x_n) \to \bigvee{}^{\mathrm{st}}\, \phi(x, x_1, \ldots, x_n)),$$

donde $\bigvee^{\mathrm{st}} x\, \alpha$ es una abreviatura por $\bigvee x(\mathrm{st}(x) \wedge \alpha)$.

Esto implica que todo conjunto definible en ZFC es estándar. Por ejemplo, $x = \mathbb{R}$ es una fórmula interna (porque puede definirse en ZFC) sin parámetros, luego, por el principio de transferencia:

$$\bigvee x(x = \mathbb{R}) \to \bigvee{}^{\mathrm{st}} x(x = \mathbb{R}),$$

es decir, que existe un conjunto estándar que es igual a $\mathbb{R}$, luego $\mathbb{R}$ es estándar, y lo mismo vale para $\mathbb{N}$, para 8, para $\varnothing$ o para cualquier conjunto definible en ZFC. Más aún, toda operación definible en ZFC da conjuntos estándar cuando se aplica a conjuntos estándar. Por ejemplo, para probar que la unión de conjuntos estándar es estándar, basta aplicar el principio de transferencia a la fórmula interna: $x = y \cup z$:

$$\bigwedge{}^{\mathrm{st}} yx(\bigvee x\, x = y \cup z \to \bigvee{}^{\mathrm{st}} x\, x = y \cup z).$$

Como, ciertamente, en ZFC se demuestra que existe un conjunto x que cumple $x = y \cup z$, tenemos que dicho x tiene que ser estándar.

Otro caso particular del principio de transferencia es:

$$\bigwedge{}^{\mathrm{st}} xy(\bigwedge{}^{\mathrm{st}} u(u \in x \leftrightarrow u \in y) \to \bigwedge u(u \in x \leftrightarrow u \in y)).$$

Esto significa que si dos conjuntos estándar x e y tienen los mismos elementos estándar u, entonces tienen los mismos elementos, luego son iguales. Así pues:

> **Teorema** Para que dos conjuntos estándar sean iguales basta con que tengan los mismos elementos estándar.

Idealización Para toda fórmula interna $\phi(x, y, x_1, \ldots, x_n)$, la fórmula siguiente es un axioma:

$$\bigwedge{}^{\mathrm{st}} z(z \text{ finito} \to \bigvee x \bigwedge y \in z\, \phi(x, y)) \leftrightarrow \bigvee x \bigwedge{}^{\mathrm{st}} y\, \phi(x, y).$$

Para entender este axioma conviene considerar primero una de sus consecuencias:

> **Teorema** Un conjunto es estándar y finito si y sólo si todos sus elementos son estándar.

DEMOSTRACIÓN: Dado un conjunto A, aplicamos el principio de idealización a la fórmula $x \in A \wedge x \neq y$ (que es interna). El resultado es:

$$\bigwedge^{\mathrm{st}} z(z \text{ finito} \to \bigvee x \bigwedge y \in z\,(x \in A \wedge x \neq y)) \leftrightarrow \bigvee x \bigwedge^{\mathrm{st}} y\,(x \in A \wedge x \neq y),$$

que equivale a

$$\bigwedge^{\mathrm{st}} z(z \text{ finito} \to \neg A \subset z) \leftrightarrow \bigvee x(x \in A \wedge \neg \mathrm{st}(x)).$$

Negando los dos miembros obtenemos que A está contenido en un conjunto estándar y finito si y sólo si todos sus elementos son estándar. Esto ya muestra que si A es estándar y finito, entonces todos sus elementos son estándar. Para probar el recíproco, suponemos que todos los elementos de A son estándar, y tenemos probado que $A \subset z$, para cierto conjunto z estándar y finito. Pero entonces $A \in \mathcal{P}z$, donde $\mathcal{P}z$ es estándar (por transferencia) y finito, luego por la parte ya probada, sus elementos son estándar, y en particular A es estándar (y finito, por estar contenido en un conjunto finito). ∎

Teniendo esto en cuenta, el miembro izquierdo del principio de idealización afirma que, para cualquier conjunto finito z de conjuntos estándar, existe un x que cumple $\phi(x, y)$ para cada $y \in z$, y el principio dice que esto equivale a que exista un mismo x que cumple $\phi(x, y)$ simultáneamente para todos los conjuntos estándar y.

Por ejemplo, puesto que, para cada conjunto finito de números naturales estándar $y_1, \ldots, y_n$, existe un número natural x tal que $x > y_i$, podemos concluir que existe un número natural x que es mayor que todos los números naturales estándar. Concretamente, aplicamos el principio de idealización a la fórmula $x \in \mathbb{N} \wedge (y \in \mathbb{N} \to x > y)$.

Estandarización Si $\phi(x, x_1, \ldots, x_n)$ es cualquier fórmula (interna o no), la fórmula siguiente es un axioma:

$$\bigwedge^{\mathrm{st}} y \bigvee^{\mathrm{st}} z \bigwedge^{\mathrm{st}} x(x \in z \leftrightarrow x \in y \wedge \phi(x)).$$

Equivalentemente: para cada conjunto estándar y, existe un conjunto estándar z cuyos elementos estándar son los conjuntos estándar $x \in y$ que cumplen $\phi(x)$. Ahora observamos que el conjunto estándar z es único, porque ya hemos visto que si dos conjuntos estándar tienen los mismos elementos estándar, entonces son iguales. A este único conjunto lo podemos llamar

$$^S\{x \in y \mid \phi(x, x_1, \ldots, x_n)\},$$

pero hay que tener claro que si $x \in$ cumple $\phi(x)$, no podemos asegurar que x esté en este conjunto, pues no es necesariamente cierto si x no es estándar y, recíprocamente, si x está en este conjunto, no podemos asegurar que cumpla $\phi(x)$, pues no es necesariamente cierto si x no es estándar.

Esta teoría axiomática podría parecer similar a la que utilzaba Keisler en su libro de texto, pero en el fondo es radicalmente distinta. En el contexto de Keiser, los axiomas son meramente teoremas no demostrados. Keisler trabaja en ZFC y está afirmando que en ZFC es posible construir unos objetos que cumplen sus axiomas. En particular, Keisler, como Robinson, trabaja con el conjunto $\mathbb{R}$ de los números reales (los números "normales") y afirma que está contenido en otro cuerpo "raro" $\mathbb{R}^*$ de números hiperreales que construye ingeniosamente mediante técnicas de la teoría de modelos y que se parece a $\mathbb{R}$, pero contiene infinitésimos.

El planteamiento de Nelson es el opuesto: en IST no hay reales e hiperreales, sino que el conjunto $\mathbb{R}$, que no es ni mas ni menos que el definido en ZFC, sin cambiarle una coma a la definición, como es estándar e infinito, *contiene* números no estándar, y enseguida veremos que algunos de ellos son infinitésimos no nulos, pero la diferencia es que ya están en $\mathbb{R}$, en el $\mathbb{R}$ "de toda la vida", si necesidad de extenderlo de ningún modo. Los "reales de toda la vida" se corresponden en IST con los números reales estándar.

En otros términos, el planteamiento de IST es el siguiente:

Cuando uno trabaja en ZFC y define conjuntos como $\mathbb{N}$ o $\mathbb{R}$, etc., no puede asegurar de ningún modo que estos conjuntos (con sus definiciones usuales) no contengan elementos "extraños", como números naturales mayores que $0, 1, 2, 3, \ldots$ (es decir, números naturales infinitamente grandes) o números reales positivos menores que $1/2, 1/3, 1/4, \ldots$ (números reales infinitamente pequeños). Los axiomas de ZFC describen lo que pasa en cualquier modelo de ZFC, y nada nos asegura que, si elegimos un modelo

cualquiera, en él no haya números así, que pasan completamente inadvertidos porque son innombrables. Lo que hace IST es introducir un relator st que distinga a los conjuntos estándar (los que queremos que estén) de los no estándar (los que no pretendíamos que estuvieran, pero que pueden estar queramos o no). De este modo, un modelo de IST es simplemente un modelo de ZFC en el que sabemos seguro que hay conjuntos no estándar, mientras que en un modelo arbitrario de ZFC puede haberlos o no haberlos, sin que podamos hacer nada para asegurarnos de que no hay.

Veamos algunos teoremas elementales que ilustren el funcionamiento de IST:

1. Si $m \leq n$ son números naturales y n es estándar, entonces m también lo es.

   DEMOSTRACIÓN: El conjunto $I_n = \{x \in \mathbb{N} \mid x \leq n\}$ es estándar (porque puede definirse en ZFC y el parámetro n es estándar) y es finito (se demuestra en ZFC). Por lo tanto, todos sus elementos son estándar y eso se aplica a m. ∎

2. Existen números naturales no estándar, y cada número natural no estándar es mayor que todos los números naturales estándar.

   DEMOSTRACIÓN: Existen números naturales no estándar porque $\mathbb{N}$ es un conjunto infinito, y la segunda parte es consecuencia del teorema anterior. ∎

3. Un número real δ es *infinitesimal* si, para todo número real estándar $x > 0$, se cumple $|\delta| < x$. Existen infinitesimales no nulos.

   DEMOSTRACIÓN: Si n es un número natural no estándar, entonces $\delta = 1/n$ es un infinitésimo no nulo. En efecto, si $x > 0$ es un número real estándar entonces la parte entera $E[1/x]$ es estándar (por transferencia, porque toda operación definible en ZFC da conjuntos estándar cuando se aplica a conjuntos estándar) y, por el mismo motivo $E[1/x] + 1$ es estándar, luego tenemos que $1/x \leq E[1/x] + 1 < n$, por el teorema anterior, luego $|\delta| = \delta = 1/n < x$. ∎

4. Un número real x es *finito* si existe un número real estándar y tal que $|x| \leq y$. En caso contrario se dice *infinito*. La suma y el producto de números finitos (infinitesimales) es un número finito (infinitesimal). Más aún, el producto de un número finito por un infinitésimo es infinitesimal.

   DEMOSTRACIÓN: Si x_1 y x_2 son números finitos, existen números estándar y_1, y_2 tales que $|x_i| \leq y_i$. Entonces $|x_1 + x_2| \leq |x_1| + |x_2| \leq y_1 + y_2 = y$, donde y es estándar por transferencia, porque cualquier operación definida en ZFC da conjuntos estándar cuando se aplica a conjuntos estándar. Esto prueba que $x_1 + x_2$ es finito, y análogamente se razona con el producto.

   Si x_1 y x_2 son infinitesimales, para cada número real estándar $x > 0$, se cumple que $|x_1| < x/2$ y $|x_2| < x/2$, pues $x/2$ también es estándar. Por lo tanto, $|x_1 + x_2| \leq |x_1| + |x_2| < x/2 + x/2 = x$, y esto prueba que $x_1 + x_2$ es infinitesimal.

   Si x_1 es finito y x_2 es infinitesimal, existe un número estándar $y > 0$ tal que $|x| \leq y$. Para cada número real estándar $x > 0$, el número $x/y > 0$ es estándar, luego $|x_2| < x/y$, luego $|x_1 x_2| = |x_1||x_2| < y(x/y) = x$, luego $x_1 x_2$ es infinitesimal. ∎

5. La parte entera de un número finito es estándar.

   DEMOSTRACIÓN: Sea x un número finito y sea $n = E[x]$ su parte entera. Si x es entero, entonces $n = x$, luego es finito y es claro que $|n|$ también cumple la definición de finitud. Por lo tanto, $|n|$ es un número natural finito, luego es estándar por 2.

   Supongamos que x no es entero, con lo que $n < x < n + 1$. Si $x > 0$, entonces n es un número natural y claramente cumple la definición de finitud, luego es estándar. Si $x < 0$, entonces $-n-1 < -x < -n$, luego $-n - 1 = E[-x]$ es estándar por la parte ya probada, luego $-n$ es estándar (porque, por transferencia, la suma de números estándar es estándar) y n es estándar (porque el producto de números estándar es estándar). ∎

6. Dos números reales x, y están infinitamente próximos, y lo representamos $x \approx y$, si $x - y$ es infinitesimal. Todo número finito x está infinitamente próximo a un único número estándar ${}^*x$.

   DEMOSTRACIÓN: Consideramos el conjunto estándar $A = {}^S\{y \in \mathbb{R} \mid y \le x\}$. Por el teorema anterior, $E[x] \le x$ es un número estándar, luego $E[x] \in A$, que es, por lo tanto, no vacío. Como x es finito, existe un número estándar z tal que $x \le |x| \le z$. Se cumple que $\bigwedge y(y \in A \to y \le z)$. En efecto, por el principio de transferencia, para probar esto (teniendo en cuenta que los parámetros A y z son estándar) basta probar que $\bigwedge^{\text{st}} y(y \in A \to y \le z)$, pero si $y \in A$ es estándar, eso implica que $y \le x \le z$.

   Así pues, A es un subconjunto de $\mathbb{R}$ no vacío y acotado superiormente. Por lo tanto, podemos considerar su supremo ${}^*x$, que es un número estándar, por transferencia, pues el supremo de un conjunto estándar es estándar. Vamos a probar que ${}^*x \approx x$. Para ello fijamos $t > 0$ estándar.

   Supongamos en primer lugar que ${}^*x \le x$. Si fuera $x - {}^*x > t$, entonces ${}^*x + t < x$, luego, como es un número estándar, ${}^*x + t \in A$, luego ${}^*x + t \le {}^*x$ (porque ${}^*x$ es el supremo de A), lo cual es absurdo. Por lo tanto $|x - {}^*x| = x - {}^*x \le t$ para todo t, y concluimos que $x - {}^*x$ es infinitesimal.

   Si es $x < {}^*x$, entonces ${}^*x - t < {}^*x$, luego no es cota superior de A, luego existe $s \in A$ tal que ${}^*x - t < s$. Es decir, tenemos que $\bigvee s(s \in A \wedge {}^*x - t < s)$, y todos los parámetros son estándar, luego por transferencia podemos tomar s estándar. Así ${}^*x - t < s \le x$, luego $|x - {}^*x| = {}^*x - x < t$, y también concluimos que $x - {}^*x$ es infinitesimal.

   La unicidad se debe a que si dos números estándar cumplen $x \approx y$, entonces $x - y$ es un infinitésimo estándar, pero eso sólo puede ser si $x - y = 0$, pues, de lo contrario tendría que ser $0 < |x - y| < \frac{1}{2}|x - y|$, pues el último término es un número real estándar, lo cual es absurdo. Así pues, $x = y$. ∎

El principio de estandarización permite dar definiciones generales particularizadas a conjuntos estándar. Veamos un ejemplo de lo que queremos decir. Consideremos esta definición:

Definición Una función estándar $f : I \longrightarrow \mathbb{R}$, donde I es un intervalo estándar en $\mathbb{R}$ es *continua* en un punto estándar $x \in I$ si para todo $y \in I$ tal que $y \approx x$, se cumple que $f(y) \approx f(x)$.

Se puede objetar que esto no define cuándo es continua una función arbitraria $f : I \longrightarrow \mathbb{R}$ en un punto $x \in I$ arbitrario, pero no es así. La definición anterior determina un concepto general de continuidad válido para cualquier función $f : I \longrightarrow \mathbb{R}$ en cualquier punto, pero dicha definición no es la que resulta de eliminar los requisitos de que los conjuntos considerados sean estándar. La definición general se obtiene considerando el conjunto

$$\mathcal{C} = {}^S\{(f, I, x) \in \mathcal{P}(\mathbb{R} \times \mathbb{R}) \times \mathcal{I} \times \mathbb{R} \mid f : I \longrightarrow \mathbb{R} \wedge x \in I \wedge \bigwedge y(y \in I \wedge y \approx x \to f(y) \approx f(x))\},$$

donde $\mathcal{I}$ es el conjunto (estándar) de todos los intervalos en $\mathbb{R}$. Decimos que una función $f : I \longrightarrow \mathbb{R}$ es continua en un punto $x \in I$ si $(f, I, x) \in \mathcal{C}$. De este modo, si f, I, x son estándar, esto equivale a la definición que hemos dado, pero esta definición vale en general. En la práctica no es necesario escribir el conjunto $\mathcal{C}$, sino que toda definición como la que hemos dado (sólo para conjuntos estándar) se extiende así a conjuntos arbitrarios.

Ejemplo Para todo $a \in \mathbb{R}$, la función $f : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(x) = ax$ es continua en $\mathbb{R}$.

DEMOSTRACIÓN: Queremos probar que para todo $a \in \mathbb{R}$ y para todo $x_0 \in \mathbb{R}$, la función $f(x) = ax$ es continua en x_0. Por el principio de transferencia,[7] podemos suponer que a y x_0 son estándar. En tal caso, la función f también es estándar (pues es una función que puede definirse en ZFC y la definimos a partir de un conjunto estándar), luego podemos aplicar directamente la definición para el caso estándar. Y la conclusión es trivial: si $y \approx x_0$, entonces $f(y) - f(x_0) = ay - ax_0 = a(y - x_0) \approx 0$, porque el producto de un número finito y uno infinitesimal es infinitesimal. ∎

En particular, si $a > 0$ es un número real infinito, la función $f(x) = ax$ es continua, pero no cumple la definición que hemos dado para funciones estándar. Por ejemplo, tomando $x_0 = 1$, tenemos que $1 \approx 1 + 1/a$, pero no es cierto que $a = f(1) \approx f(1 + 1/a) = a + 1$.

Una sutileza que hay que tener en cuenta es la siguiente: en ZFC se demuestra que si n es un número natural, entonces el conjunto $I_n = \{m \in \mathbb{N} \mid m \le n\}$ es finito. Por lo tanto, esto mismo es válido en IST, incluso si n es un número natural infinito. En tal caso, el conjunto I_n es finito, aunque contiene a todos los números estándar $0, 1, 2, 3, \ldots$

[7] Lo aplicamos a la fórmula $\bigwedge f(f : \mathbb{R} \longrightarrow \mathbb{R} \wedge \bigwedge x \in \mathbb{R}(f(x) = ax) \to (f, \mathbb{R}, x_0) \in \mathcal{C})$, que tiene únicamente el parámetro estándar $\mathcal{C}$, luego el principio de transferencia es aplicable.

En realidad, el principio de idealización implica un hecho mucho más fuerte:

Teorema Existe un conjunto finito que contiene a todos los conjuntos estándar.

DEMOSTRACIÓN: Basta aplicar el principio de idealización a la fórmula $y \in x \wedge x$ es finito. El resultado es

$$\bigwedge^{\mathrm{st}} z(z \text{ finito} \to \bigvee x \bigwedge y \in z\,(y \in x \wedge x \text{ es finito})) \leftrightarrow \bigvee x \bigwedge^{\mathrm{st}} y(y \in x \wedge x \text{ es finito}).$$

El miembro izquierdo se cumple tomando $x = z$, luego se cumple el miembro derecho, que afirma precisamente que existe un conjunto finito x que contiene a todos los conjuntos estándar. ∎

Nelson presenta en su artículo ejemplos variados del uso de su teoría. Veamos algunos de ellos. El primero es un ejercicio para que el lector juzgue si es más cómodo trabajar con las definiciones estándar o con las no estándar. Para ello presenta un concepto similar al de función continua y su equivalente en términos ϵ–δ, y propone demostrar una propiedad sencilla partiendo de una definición o de su equivalente:

1. Una función $f : \mathbb{R} \longrightarrow \mathbb{R}$ es *aunitnoc* en un punto x si para todo $\epsilon > 0$ existe un $\delta > 0$ tal que si $|y - x| \le \epsilon$, entonces $|f(y) - f(x)| \le \delta$.

   Equivalentemente:[8]

   Una función estándar $f : \mathbb{R} \longrightarrow \mathbb{R}$ es *aunitnoc* en un punto estándar x si cuando $y - x$ es finito, entonces $f(y) - f(x)$ es finito.

   Demostrar (a partir de una de las dos definiciones) que si f es *aunitnoc* en un punto x, entonces es *aunitnoc* en todos los puntos de $\mathbb{R}$.

   DEMOSTRACIÓN: Queremos probar que esto vale para toda f y todo x, luego por transferencia podemos suponer que f y x son estándar. Ahora queremos probar que, para todo punto x', se cumple que f es *aunitnoc* en x', luego, de nuevo por transferencia, podemos suponer que x' es estándar.

   Tomamos $y \in \mathbb{R}$ tal que $y - x'$ es finito. Entonces $y - x = (y - x') + (x' - x)$ es finito, pues el segundo sumando es estándar, luego es finito, y la suma de números finitos es finita. Por hipótesis $f(y) - f(x)$ es finito. Como también es finito $x' - x$, tenemos también que $f(x') - f(x)$ es finito. Como la resta de números finitos es finita, $f(y) - f(x') = f(y) - f(x) - (f(x') - f(x))$ es finito. ∎

2. Si $f : [a, b] \longrightarrow \mathbb{R}$ es una función continua tal que $f(a) < 0$ y $f(b) > 0$, existe un $c \in [a, b]$ tal que $f(c) = 0$.

   DEMOSTRACIÓN: Por transferencia, podemos suponer que f, a, b son estándar. Sea n un número natural infinito y sea $x_i = a + i(b - a)/n$. De este modo $a = x_0 < x_1 < \cdots < x_n = b$ y $x_i - x_{i-1} = (b - a)/n \approx 0$.

   Como $f(x_0) < 0$ y $f(x_n) > 0$, tiene que haber un índice i tal que $f(x_{i-1}) < 0 \le f(x_i)$. Pero $x_{i-1} \approx x_i$, luego ambos tienen la misma parte estándar $c = {}^*x_{i-1} = {}^*x_i$. Como f es continua en c, se cumple que $f(c) \approx f(x_{i-1}) \approx f(x_i) \approx 0$, pues $0 \le f(x_i) \le f(x_i) - f(x_{i-1}) \approx 0$, de donde se sigue que $f(x_i)$ es infinitesimal. Como $f(c) \approx 0$ y ambos son estándar, tiene que ser $f(c) = 0$. ∎

3. Un *grafo* es un conjunto G (a cuyos elementos llamamos *vértices*) y un conjunto R formado por subconjuntos de G de dos vértices (a cuyos elementos llamamos *aristas*). Un grafo es *k-coloreable* si existe una aplicación $f : G \longrightarrow \{1, \ldots, k\}$ tal que si $\{i, j\}$ es una de sus aristas, entonces $f(i) \ne f(j)$. Probar que si todos los subgrafos finitos de un grafo son k-coloreables, entonces el grafo completo es k-coloreable.[9]

   DEMOSTRACIÓN: Por transferencia podemos suponer que el grafo es estándar (lo que incluye a su conjunto de aristas), al igual que el número natural k. Sea F un conjunto finito que contenga a todos los conjuntos estándar, y sea $G_0 = G \cap F$, que es un conjunto finito de vértices de G que contiene a todos los vértices estándar. Por hipótesis, existe $f : G_0 \longrightarrow \{1, \ldots, k\}$ que cumple la definición de grafo k-coloreable. Entonces consideramos el conjunto

   $${}^S f = {}^S\{z \in G \times \{1, \ldots, k\} \mid z \in f\}.$$

[8] Para probar la equivalencia podemos suponer que f y x son estándar. Si se cumple la definición no estándar, para probar que cumple la definición clásica, podemos suponer que ϵ es estándar, en cuyo caso sirve cualquier $\delta > 0$ infinito. En efecto, si $|y - x| < \epsilon$, entonces $y - x$ es finito, luego $f(y) - f(x)$ es finito, luego $|f(y) - f(x)| < \delta$. Recíprocamente, si f y x cumplen la definición clásica y se cumple que $y - x$ es finito, entonces existe un $\epsilon > 0$ estándar tal que $|y - x| \le \epsilon$. Sabemos que $\bigvee \delta > 0 \bigwedge y \in \mathbb{R}(|y - x| \le \epsilon \to |f(y) - f(x)| \le \delta)$. Como los parámetros f, x, ϵ son estándar, el principio de transferencia nos permite tomar δ estándar. Así $|f(y) - f(x)| \le \delta$, lo que implica que $f(y) - f(x)$ es finito.

[9] Esto se conoce como teorema de De Bruijn-Erdős.

Así, ${}^Sf$ es un conjunto estándar cuyos elementos estándar son los pares $z = (x, i)$ estándar que están en f. Vamos a ver que ${}^Sf : G \longrightarrow \{1, \dots, k\}$ y cumple lo requerido. Se trata de una comprobación rutinaria:

(a) $\bigwedge z(z \in {}^Sf \to \bigvee x \in G \bigvee i \in \{1, \dots, k\}\, z = (x, i))$.
En efecto, puesto que los parámetros ${}^Sf$ y k son estándar, basta probarlo cuando z es estándar, pero entonces $z \in f$, luego, ciertamente, existen $x \in G_0$ y $i \in \{1, \dots, k\}$ tales que $z = (x, i)$. Así pues ${}^Sf \subset G \times \{1, \dots, k\}$.

(b) $\bigwedge x \in G \overset{1}{\bigvee} i\, (x, i) \in {}^Sf$.
Por transferencia basta probarlo cuando x es estándar, pero entonces $x \in G_0$, luego $i = f(x)$ cumple $(x, i) \in f$, luego también $(x, i) \in {}^Sf$. Si $(x, j) \in {}^Sf$, como $j \in \{1, \dots, k\}$, tiene que ser estándar, luego $(x, j) \in f$, luego $j = f(x) = i$. Por lo tanto, $f : G \longrightarrow \{1, \dots, k\}$.

(c) Si R es el conjunto de aristas de G, entonces $\bigwedge xy(\{x, y\} \in R \to {}^Sf(x) \neq {}^Sf(y))$.
Como R y ${}^Sf$ son estándar, basta probarlo si x, y son estándar. Sean $f(x) = i$, $f(y) = j$. Tenemos que $(x, i), (y, j) \in {}^Sf$, luego $(x, i), (x, j) \in f$, luego $i = f(x)$, $j = f(y)$ y, como f cumple la definición de grafo k-coloreable, $i \neq j$. ∎

El artículo de Nelson termina con un apéndice en el que demuestra un teorema fundamental:

Teorema de conservación Todo teorema interno demostrable en IST es demostrable en ZFC.

Esto significa que IST es lo que se llama una *extensión conservativa* de ZFC. En IST se pueden demostrar más teoremas que en ZFC, porque hay teoremas que incluyen en su enunciado el relator st, que no pueden demostrarse en ZFC porque carece de este relator, pero si hablamos de fórmulas internas, es decir, de fórmulas del lenguaje de ZFC, éstas son demostrables en ZFC si y sólo si lo son en IST. En otras palabras, que al demostrar una fórmula interna en IST no estamos demostrándola en una teoría rara, donde se puede esperar cualquier cosa rara, sino que una demostración en IST equivale a una demostración en ZFC. O, dicho de otro modo, IST no es más que una herramienta para demostrar teoremas de ZFC. ∎

La teoría de Hrbáček En la teoría de Nelson no es posible definir el conjunto de todos los infinitésimos. No sólo es que no podemos definir

$$o = \{x \in \mathbb{R} \mid x \approx 0\},$$

porque la fórmula $x \approx 0$ no es interna, sino que podemos demostrar que no existe ningún conjunto cuyos elementos sean los números reales infinitesimales.

Demostración: Si existiera tal conjunto o, sería un subconjunto de $\mathbb{R}$ no vacío y acotado superiormente, luego tendría que tener un supremo $\delta > 0$. Ahora bien, si $\delta \approx 0$, entonces $\delta < 2\delta$, pero $2\delta \approx 0$, con lo que δ no es una cota superior de o. Pero si δ no es infinitesimal, tampoco lo será $\delta/2 < \delta$, luego existe un infinitésimo $\delta/2 < \epsilon \leq \delta$, pero esto implica que $\delta/2 \approx 0$, luego también $\delta \approx 0$, y tenemos una contradicción. ∎

Sin embargo, nada nos impide considerar la definición anterior de o en el mismo sentido en que podemos considerar clases propias en ZFC, es decir, como una forma de decir que cuando escribimos $x \in o$ queremos decir que $x \approx 0$.

Se dice entonces que o es un *conjunto externo,* que es tanto como decir un conjunto que no existe, pero que podemos hablar de él con limitaciones (como una mera notación, pero sin que sea legítimo aplicarle teoremas válidos para *conjuntos internos,* es decir, conjuntos "reales", como el principio de existencia de supremo. En estos términos podemos distinguir entre conjuntos estándar, conjuntos internos y conjuntos externos. Los últimos no existen oficialmente. Nelson esbozaba en su artículo cómo pueden ser formalizados, pero la primera teoría de conjuntos no estándar que axiomatizó los conjuntos externos fue propuesta por Karel Hrbáček (que se había doctorado bajo la dirección de Vopěnka) en su artículo de 1978 titulado *Fundamentos axiomáticos del análisis no estándar* (fue publicado un año después que el artículo de Nelson, pero había sido enviado un año antes).

En realidad, Hrbáček presenta tres variantes distintas, cada una de las cuales se puede construir sobre cualquier teoría de conjuntos T de partida que cumpla unos requisitos mínimos. Por simplicidad aquí describiremos sólo una de ellas, a la que llamaremos H, partiendo de $T =$ ZFC.

La teoría de Hrbáček se construye sobre el lenguaje formal de ZFC ampliado con dos relatores monádicos st e in, de modo que $\mathrm{st}(x)$ se lee "x es estándar" e $\mathrm{in}(x)$ se lee "x es interno". Esto nos lleva a definir $\bigwedge^{\mathrm{in}}$ y $\bigvee^{\mathrm{in}}$ análogamente a como hemos definido $\bigwedge^{\mathrm{st}}$ y $\bigvee^{\mathrm{st}}$ en la teoría de Nelson. Si α es una fórmula interna, es decir una fórmula del lenguaje de ZFC, en la que no aparecen los relatores "nuevos", llamaremos α^{in} y α^{st} a las fórmulas que resulta de sustituir todos sus cuantificadores $\bigwedge$ y $\bigvee$ por $\bigwedge^{\mathrm{in}}$ y $\bigvee^{\mathrm{in}}$ (o por $\bigwedge^{\mathrm{st}}$ y $\bigvee^{\mathrm{st}}$, respectivamente), es decir, las fórmulas que expresan lo que entendería por α alguien que no viera más que los conjuntos internos (o estándar). Los axiomas de la teoría H son los siguientes:

Z Los axiomas de la teoría de Zermelo (Extensionalidad, par, unión, especificación (para fórmulas externas), partes y elección).

Notemos que el esquema axiomático de especificación, es decir:

$$\bigwedge y \bigvee z \bigwedge x(x \in z \leftrightarrow x \in y \wedge \phi(x, x_1, \dots x_n))$$

se admite para todas las fórmulas del lenguaje de H, no sólo para las internas. No podemos incluir ni el axioma del reemplazo ni el de regularidad, o la teoría se volvería contradictoria.

Inclusión $\bigwedge^{\mathrm{st}} x\, \mathrm{in}(x)$ (todo conjunto estándar es interno).

Transitividad $\bigwedge^{\mathrm{in}} x(\bigwedge u(u \in x \to \mathrm{in}(u)))$ (la clase de los conjuntos internos es transitiva).

ZFC$^{\mathrm{st}}$ Si α es un axioma de ZFC (formulado sin variables libres), entonces α^{st} es un axioma de H.

Inmersión Si $\alpha(x_1, \dots, x_n)$ es una fórmula interna, la fórmula siguiente es un axioma:

$$\bigwedge^{\mathrm{st}} x_1 \cdots x_n(\alpha^{\mathrm{st}}(x_1, \dots, x_n) \leftrightarrow \alpha^{\mathrm{in}}(x_1, \dots, x_n)).$$

Esto significa que la clase de los conjuntos internos es una extensión elemental de la clase de los conjuntos estándar. En particular, los dos últimos axiomas implican que, para todo axioma α de ZFC (formulado sin variables libres), α^{in} es un teorema de H. En particular:

Si dos conjuntos estándar tienen los mismos elementos estándar, entonces son iguales.

Basta aplicar el esquema de inmersión a $\alpha(A, B) \equiv \bigwedge x(x \in A \leftrightarrow x \in B)$, lo que nos da

$$\bigwedge^{\mathrm{st}} AB(\bigwedge^{\mathrm{st}} x(x \in A \leftrightarrow x \in B) \leftrightarrow \bigwedge^{\mathrm{in}} x(x \in A \leftrightarrow x \in B))$$

Así, si dos conjuntos estándar A y B tienen los mismos elementos estándar, de hecho tienen los mismos elementos internos. Pero como A y B son internos (por el axioma de inclusión) y todos sus elementos son internos (por el axioma de transitividad), concluimos que A y B tienen los mismos elementos, luego $A = B$ (por el axioma de extensionalidad).

Transferencia $\bigwedge A \bigvee^{\mathrm{in}} B \bigwedge^{\mathrm{st}} x(x \in B \leftrightarrow x \in A)$. Para cada conjunto externo A, existe un conjunto estándar B que tiene los mismos elementos estándar que A.

Por la observación precedente, el conjunto B es único, luego podemos llamar *estandarización* de A al único conjunto estándar ${}^S A$ que tiene los mismos elementos estándar que A.

Saturación Diremos que un conjunto A tiene *tamaño estándar* si existe un conjunto estándar B y una aplicación $f : B \longrightarrow A$ suprayectiva. Para cada fórmula $\phi(x, y, x_1, \dots, x_n)$, la fórmula siguiente es un axioma:

$$\bigwedge^{\mathrm{in}} x_1 \cdots x_n \bigwedge A(A\text{tiene tamaño estándar} \wedge \bigwedge z(z \subset A \wedge a \text{ es finito} \to \bigvee^{\mathrm{in}} x \bigwedge^{\mathrm{in}} y \in z\, \alpha^{\mathrm{in}}(x, y)) \to$$

$$\bigvee^{\mathrm{in}} x \bigwedge^{\mathrm{in}} y \in A\, \alpha^{\mathrm{in}}(x, y)).$$

No vamos a dar los detalles, pero de estos axiomas de deduce que la clase de los conjuntos internos cumple los axiomas de IST. La diferencia es que en H podemos definir, por ejemplo,

$$o = \{x \in \mathbb{R} \mid x \approx 0\},$$

y esto es una aplicación legítima del axioma de especificación, por lo que o es un conjunto. La demostración que hemos visto en el apartado precedente según la cual o no existe en IST se adapta para demostrar en H que o es un conjunto estrictamente externo, es decir, que no es interno.

Hrbáček demuestra un teorema de conservación análogo al de Nelson, que en este caso se enuncia así:

Teorema de conservación Si α es una sentencia interna, entonces α es un teorema de ZFC si y sólo si α^{in} es un teorema de H.

Posteriormente se han propuesto otras teorías axiomáticas para el análisis no estándar, pero no vamos a entrar en ello. ∎

Balance Halmos siguió combatiendo el análisis no estándar casi hasta el final de sus días. Por ejemplo, en 1985 (a sus 69 años) publicó una autobiografía titulada *Quiero ser matemático: una automatografía*[10] *en tres partes,* en la que, de tanto en tanto, lanzaba algún dardo, tanto al análisis no estándar, como a la teoría de categorías, que tampoco era de su gusto. De ella procede, por ejemplo, la cita de la página 341, o también esta otra:

> [...] *para algunos conversos, (como Pete Loeb y Ed. Nelson) es una religión* [...] *Para algunos otros, que están en contra (por ejemplo Errett Bishop), es igualmente algo emocional. La ven como un culto diabólico.*

(Los conversos Albert Emerson Hurd y Peter Albert Loeb, doctorados en 1962 y 1965 bajo la dirección de Royden, habían publicado ese mismo año *Una introducción al análisis no estándar.*)

Sin embargo, el balance del análisis no estándar que puede hacerse medio siglo después de su apogeo en la década de los setenta es que, desde el punto de vista de la investigación, actualmente es una modesta rama más de la matemática, tan digna como cualquier otra, pero que de ningún modo ha cumplido las expectativas de que iba a revolucionar la concepción del análisis matemático. Y desde un punto de vista didáctico, es decir, como medio para introducir el cálculo diferencial en los primeros cursos universitarios, ha sido un rotundo fracaso. En palabras de Philip J. Davis:

> *Existió el movimiento de análisis no estándar para la enseñanza del cálculo elemental. Su popularidad aumentó ligeramente antes de que el movimiento colapsara debido a su complejidad interna y escasa necesidad.*

Todavía se puede encontrar opiniones aisladas de quienes afirman que es mucho más intuitivo y fácil de entender, pero son simplemente las opiniones de quienes desconocen los detalles de la historia de su fracaso:

> ZFC tiene una virtud que hace que nunca será sustituido por otra teoría que carezca de ella: y es que se puede razonar sin salirse de los límites que impone ZFC sin saber nada de lógica.

Toda teoría formal tiene límites técnicos que le impiden caer en contradicciones, por ejemplo, violando el segundo teorema de incompletitud. Así, por ejemplo, no es difícil "colar" a un matemático que no conozca los detalles técnicos de ZFC una demostración de la consistencia de ZFC basada en la definición de una relación $V \vDash \alpha$ que no es correcta porque aplica indebidamente un teorema de recursión a una clase propia (algo que es formalizable en MK, pero no en NBG, ni mucho menos en ZFC), pero estos tecnicismos están tan alejados del trabajo cotidiano del matemático que en la práctica no le afectan en nada. Un matemático sabe que no caerá en ningún desliz lógico en ZFC sin más que mantenerse prudentemente alejado de las clases propias, cosa que no le supone ninguna restricción práctica.

Los razonamientos que se emplean en cualquier aula universitaria (salvo en asignaturas técnicas de lógica o de teoría de conjuntos) son razonamientos informales formalizables en ZFC. Pero, al mantenerse tan lejos de los límites técnicos que impone ZFC para garantizar su propia consistencia, sucede que cualquier error de razonamiento que un alumno (o incluso un matemático profesional) pueda cometer en su trabajo habitual no será un error técnico debido a no haber respetado un tecnicismo lógico, sino un error conceptual que podrá ser fácilmente detectado, señalado y entendido.

En cambio, para trabajar en IST, o en cualquier presentación alternativa del análisis no estándar, se está constantemente en el borde entre lo permitido y lo prohibido por los tecnicismos lógicos. Hay que cuidar de no definir nunca un conjunto con una fórmula no estándar, o de no aplicar el principio de transferencia a una fórmula con algún parámetro no estándar, o de no dejar de cambiar ningún $\bigwedge$ por $\bigwedge^{\text{st}}$ cuando es necesario cambiarlos todos en una fórmula, etc., y el más sutil error de cualquiera de estos tipos o de muchos otros igualmente delicados puede descarriar completamente un argumento y conducir a un absurdo sin que el "perpetrador" pueda adivinar qué ha hecho mal. Esta dependencia de los tecnicismos lógicos no la compensa ninguna de las ventajas que

[10] Mezcla de "autobiografía" y "matemática", algo así como una autobiografía matemática.

pueda aportar el análisis no estándar. Dicho de otro modo, uno puede razonar más o menos eficientemente con el análisis clásico con unas nociones rudimentarias de lógica (aunque pueda requerir que un profesor le corrija errores de tanto en tanto), pero es imposible dar correctamente cinco pasos seguidos en análisis no estándar sin tener una profunda comprensión de la lógica formal y de la estructura de las fórmulas que formalizan las distintas nociones matemáticas. Alguien con una buena base en lógica matemática puede permitirse el lujo de juzgar si el análisis no estándar le resulta más natural o más práctico que el análisis convencional, pero, si se decide por el análisis no estándar, se equivocará si cree que puede compartir eficientemente su punto de vista con alguien que carezca de su misma base lógica.

3.3 Otras teorías alternativas

Terminamos este capítulo comentando brevemente —sin ánimo de ser exhaustivos— algunas teorías formales que, de un modo u otro, podrían considerarse alteriativas a ZFC, aparte de NBG y otras de las que ya hemos hablado con detalle.

La teoría de Kripke-Platek En 1964 Saul Aaron Kripke (doctorado en 1962 bajo la dirección de Quine) publicó una nota titulada *Recursión transfinita en ordinales,* en la que introducía una axiomática que fue desarrollada por Richard Alan Platek en su tesis doctoral, titulada *Fundamentos de la teoría de la recursión,* realizada bajo la dirección de Kreisel y leída en 1966. Hoy se conoce como la *teoría de Kripke-Platek* (KP).

Se trata de una versión débil de ZF que surgió como parte de un estudio sobre la posibilidad de extender la teoría de la recursión a ciertos conjuntos, pero pronto cobró interés por varios motivos. Kripke y Platek llamaron *ordinales admisibles* a los ordinales α tales que L_α es un modelo de la teoría KP. Más en general, se llama *conjuntos admisibles* a los modelos transitivos de KP. Por ejemplo, éstos surgen de forma natural en el estudio de la estructura fina de L. Otro contexto que los vuelve interesantes se da cuando se consideran modelos (M, R) de ZF en los que la pertenencia se interpreta mediante una relación arbitraria R, que no es necesariamente la pertenencia. Estos modelos no tienen por qué estar bien fundados, por lo que no es posible calcular su colapso transitivo. No obstante, siempre es posible tomar lo que se llama su *parte bien fundada* M_0, formada por los elementos $x \in M$ a partir de los cuales no se pueden formar sucesiones decrecientes

$$\ldots \quad x_3\, R\, x_2\, R\, x_1\, R\, x_0 = x.$$

M_0 sí que está bien fundada, por lo que se puede calcular su colapso transitivo, pero éste (o el propio M_0) no es necesariamente un modelo de ZF, pero sí que cumple al menos los axiomas (y los teoremas) de KP. Por lo tanto, saber qué teoremas de ZF son demostrables en KP nos aporta información aplicable a estos modelos.

Los Nuevos Fundamentos La teoría de los Nuevos Fundamentos de Quine recibió un ligero impulso cuando en 1968 Jensen publicó *Sobre la consistencia de una ¿ligera? modificación de los Nuevos Fundamentos de Quine,* donde demostraba que si ZFC es consistente, también lo es una variante NFU de NF que admite la existencia de elementos primitivos o "átomos", es decir, objetos que no son conjuntos, pero pueden ser elementos de los conjuntos (la U es de *urelement*). Al contrario que NF, esta variante es consistente con el axioma de elección. En realidad, basta suponer la consistencia de una teoría más débil, como la teoría de Mac Lane, de la que hablamos más abajo. Sin embargo, el trabajo de Jensen no implica la consistencia de NF, aun sin el axioma de elección, que quedó como problema abierto.

En la práctica, NF o NFU no pueden rivalizar con ZFC como fundamentos para las matemáticas por el mismo motivo que explicábamos al final de la sección anterior para las teorías de análisis no estándar, porque obligan a tener presentes en todo momento tecnicismos lógicos cuyos equivalentes en ZFC quedan relegados a regiones remotas, apartadas de la práctica matemática habitual. Sin embargo, es una curiosidad lógica que ha interesado ocasionalmente a algunos matemáticos de prestigio, como Jensen, o Solovay, aunque su principal promotor ha sido durante décadas Randall Holmes, que en 2010 presentó una prueba de la consistencia de NF, aunque durante muchos años nadie confirmó que la prueba era correcta. En 2024 Holmes y un estudiante de doctorado llamado Sky Wilshaw anunciaron que habían comprobado la corrección del argumento mediante Lean, un *asistente de demostración,* es decir, una aplicación informática que verifica la corrección de las demostraciones. Sobre la relevancia de esto, copiamos del artículo:

> *Por lo tanto, no creemos que este artículo sea un hito filosófico. Si lo hubo, fue en 1969, cuando Jensen demostró que* NFU *es consistente, y nadie lo advirtió.*

La teoría de Mac Lane En 1986 Mac Lane publicó el libro *Matemáticas: forma y función,* una especie de vista panorámica de las matemáticas dirigida a filósofos que no tuvo respuesta alguna por parte de la comunidad matemática, excepto por una charla que impartió en un congreso en 1989 Adrian Mathias (doctorado en 1970 bajo la dirección de Jensen y de John Horton Conway), titulada *¿Qué pasa por alto Mac Lane?* a la que Mac Lane respondió con otra titulada *¿Es Mathias un ontólogo?* (Mac Lane tenía entonces 80 años.)

En su libro, de pasada, Mac Lane había afirmado que, para formalizar la mayor parte de las matemáticas, sólo era necesario usar el esquema de especificación para fórmulas con cuantificadores acotados, es decir, de la forma $\bigwedge x \in y$ o $\bigvee x \in y$. Concretamente:

> *Al utilizar el axioma de especificación para las partes comunes de las matemáticas, suele bastar con considerar únicamente fórmulas con cuantificadores acotados. Esto puede enunciarse de la siguiente manera:*
>
> *Especificación Acotada (BQ). Para cualquier conjunto u y cualquier fórmula $F(x)$ del lenguaje de la teoría de conjuntos en la que todos los cuantificadores están acotados, existe un conjunto s tal que $x \in s \leftrightarrow x \in u \wedge F(x)$.*
>
> *Para la mayoría de las matemáticas, los axiomas apropiados para la teoría de conjuntos parecen ser* ZBQC: *los axiomas de Zermelo con el de especificación reemplazado por el de especificación acotada y añadiendo el axioma de elección. Este enfoque (que no se ha desarrollado en detalle en ninguna parte) es una elección pragmática de axiomas: son suficientes.*
>
> *Algunos especialistas en teoría de conjuntos afirman que pueden "ver" que los axiomas de* ZFC *son "verdaderos" para los conjuntos descritos en la jerarquía acumulativa. Nótese que en esta jerarquía, en la etapa $\alpha + 1$, cada nuevo conjunto $s \in \mathcal{P}(V_\alpha)$ es un subconjunto de V_α, por lo que consta de elementos ya presentes en V_α. Pero en la descripción de la jerarquía no hay una explicación real de qué se entiende por "subconjunto". Si cada subconjunto de V_α se describe dando una propiedad de sus elementos, parece plausible que la fórmula de primer orden que expresa esta propiedad se refiera sólo a los conjuntos ya disponibles y, por lo tanto, sólo involucre cuantificadores sobre V_α. Sobre esta base, la especificación acotada es mucho más fácil de "ver" en la jerarquía que la especificación ilimitada. (El mismo argumento se aplicaría para el Reemplazo "acotado".) Esto ilustra nuevamente la observación de que una idea intuitiva (en este caso, la jerarquía acumulativa) tiene más de una realización formal.*
>
> *Dentro de la teoría de conjuntos ZFC, la jerarquía acumulativa puede construirse formalmente. Antes de que existan los axiomas, la jerarquía es un mito platónico, claramente visible sólo para quienes tienen un sexto sentido para los conjuntos.*

Mathias deduce de aquí que la "ontología" de Mac Lane, es decir, la realidad que describe matemática según Mac Lane es la que describe la teoría ZBQC (a la que más tarde bautizaría como teoría de Mac Lane), pero ésta admite como modelo $V_{\omega+\omega}$, y es insuficiente para demostrar resultados importantes. Por ello reprochó a Mac Lane de erigirse en juez de qué matemáticas son dignas de estudio y cuáles no. Entre las partes más interesantes de su respuesta figura esta defensa del platonismo, que hoy en día tiene seguidores:

> *Este podría ser un buen momento para cuestionar una de las opiniones de Mac Lane, que creo que se basa en un error. En la página 359 de su libro, escribe, tras reflexionar sobre la plétora de resultados de independencia, que "por estas razones, el término "conjunto" resulta tener múltiples significados, de modo que el supuesto fundamento de todas las matemáticas sobre la teoría de conjuntos se tambalea" . En otra parte, en la página 385, señala que "la noción platónica de que existe en algún lugar el reino ideal de los conjuntos, aún no completamente descrito, es una gloriosa ilusión".*
>
> *Yo sugeriría una visión contraria: los resultados de independencia dentro de la teoría de conjuntos se logran generalmente examinando un modelo interno del universo (siendo un modelo interno una clase transitiva que contiene todos los ordinales) o utilizando el* forcing *para construir un universo más amplio del cual el original es un modelo interno. La concepción que empieza a parecer cada vez más razonable con el avance del programa de modelos internos, por un lado, y una comprensión más profunda del* forcing iterado, *por otro, es que dentro de un universo enorme existen numerosos modelos internos, y que los diversos "argumentos de independencia" pueden reelaborarse para brindar información positiva sobre cómo se relacionan entre sí. Lejos de socavar la unidad de la perspectiva de la teoría de conjuntos, las diversas técnicas disponibles para construir modelos promueven dicha unidad.*

La respuesta de Mac Lane fue un tanto esquiva:

> *ZFC tiene diferentes modelos. Mathias observa que un modelo de los conjuntos a menudo es interno con respecto a otro. No estoy convencido de que esta circunstancia sugiera la existencia de "un universo enorme". Evidentemente, lo que uno tiene son diferentes universos, quizá con diferentes axiomas, y conectados entre sí. Estas diferencias coinciden con los diferentes propósitos de la teoría de conjuntos.* [...]
>
> *Mathias pregunta: "¿Cuál es, entonces, la ontología de Mac Lane?" Dado que las matemáticas son proteicas, puedo responder fácilmente: la ontología tiene que ver con la naturaleza de la realidad en cuestión. Cada noción matemática es proteica, por lo tanto, trata con diferentes realidades, por lo que no tiene una ontología.* [...] *La teoría de conjuntos, como el resto de las matemáticas, es proteica, cambia y funciona de diferentes maneras según sus diferentes usos. Está subordinada a las matemáticas y no a su fundamento. La unidad de las matemáticas es real y depende de nuevas y maravillosas conexiones que surgen a nuestro alrededor. Insto a mis amigos en lógica a que miren a su alrededor.*

En 1986, el mismo año de publicación del libro de Mac Lane, en una sociedad de estudiantes de Cambridge, Mathias había dado una charla titulada *La ignorancia de Burbaki,* en la que criticaba la falta de conocimientos de lógica de Bourbaki, al (o a los) que acusaba de tener una visión pregödeliana de la lógica. El contenido fue publicado en la revista de dicha sociedad, pero tuvo bastante difusión y en 1991 Mathias publicó una versión revisada que fue reproducida en varias revistas, en 1992 y en 1998, en la que respondía a las críticas recibidas por parte de varios matemáticos, entre ellos Mac Lane.

> *La actitud adoptada por Bourbaki sobre la cuestión de la geometría* versus *el análisis aún es relevante hoy en día, pues recientemente el distinguido matemático estadounidense Saunders Mac Lane a instado a revivir la discusión de la filosofía de las matemáticas y ha criticado lo que llama la Gran Fundamentación Conjuntista de las Matemáticas en frases como*
>
> > *La Gran Fundamentación Conjuntista de las Matemáticas es una visión erróneamente sesgada de las matemáticas: la teoría de conjuntos es en gran medida irrelevante para la práctica de la mayoría de los matemáticos.*
> > *El logicismo, el formalismo y el platonismo han estado demasiado dominados por por las nociones de la teoría de conjuntos y el rigor deductivo.*
>
> *También ha habido críticas como la de Thom:*
>
> > *La teoría de conjuntos parece suprimir la geometría.*
>
> *y, ante todo, la deliciosa schlussbemerkung* [observación final] *del artículo de 1922 de Skolem, que, traducida aproximadamente, dice:*
>
> > *El resultado más importante entre lo que hemos visto es el carácter relativo de los conceptos de la teoría de conjuntos. Mencioné esto de palabra al profesor F. Bernstein en Gotinga en el invierno de 1915/16. Hay dos razones por las que no he publicado antes nada al respecto. Primero, que este tiempo he estado ocupado con otros problemas y, segundo, que yo creía que era tan claro que la axiomatización en términos de conjuntos no era una fundamentación última satisfactoria de las matemáticas que los matemáticos, en su mayor parte, no se interesarían por ella. Pero en los últimos tiempos he visto, para mi sorpresa, que muchos matemáticos piensan que esos axiomas de la teoría de conjuntos proporcionan la fundamentación ideal de las matemáticas. Por ello, me pareció que había llegado el momento de hacer pública una crítica.*
>
> *Imagino que es a causa de que Bourbaki ha fosilizado el conocimiento sobre lógica de los matemáticos a su nivel de 1929* que este ataque está siendo renovado. Mac Lane, que, habiendo sido alumno de Bernays en Gotinga de 1930 a 1933, conoce mucho mejor la lógica que los burbakistas, está, con otras palabras, atacando una posición de la que los lógicos se han estado alejando durante los últimos 60 años, pero en la que todavía permanecen los matemáticos.*
>
> (*) *De hecho, se dice que un miembro del grupo Bourbaki dijo en una conferencia dada en Princeton ante una audiencia que incluía a Gödel que nada había sucedido en la lógica desde Aristóteles. ¿Algún lector podría decirme quién fue?*

No es éste el lugar para iniciar una discusión sobre las fortalezas y debilidades de los puntos de vista sobre los fundamentos que Mac Lane sostiene en su libro Matemáticas: forma y función, pero algunos comentarios serán oportunos:

A Skolem le diría que no hay una fundamentación final de las matemáticas, pero que la teoría de conjuntos captura una parte sustancial de las matemáticas. Estoy de acuerdo con el primer comentario de Mac Lane y con el de Thom, y los relaciono con mi idea de que la teoría de conjuntos está en el lado aritmético y no en el geométrico de las matemáticas. Pero matizaría el segundo comentario de Mac Lane diciendo que la teoría de conjuntos no es particularmente relevante para la práctica de la geometría, pero que es muy relevante para la aritmética en su sentido más amplio.

Aunque coincido con buena parte de la tercera crítica de Mac Lane, cuestiono su uso de las expresiones "teoría de conjuntos" y "rigor deductivo". Piensa que ambas cosas van de la mano y se opone a que se hagan pasar por la solución final para las matemáticas. Quisiera separar las dos cosas: la lógica es el estudio de nuestro uso del lenguaje; la teoría de conjuntos es el estudio de las relaciones bien fundadas, y no, como cree Mac Lane, el estudio del proceso de formación de conjuntos.

Ésa es la gran diferencia entre Zermelo-Fraenkel y Zermelo. Zermelo —y más particularmente el subsistema que podemos llamar la teoría de Mac Lane, en vista de su predilección por esta teoría en sus libros y artículos— es un sistema para sostener la formación de conjuntos y es adecuado para las consideraciones geométricas. Zermelo-Fraenkel es un sistema que contiene además soporte para las definiciones por recursión, es decir, para construir estructuras hacia lo desconocido. Este elemento, que es el punto crucial de la teoría de conjuntos de Kriple-Platek, está pensado para el lado aritmético de las matemáticas.

En la teoría de Zermelo no se puede demostrar que todo conjunto bien ordenado es isomorfo a un ordinal de von Neumann; no se puede probar la existencia del ordinal de von Neumann $\omega+\omega$, aunque uno puede probar la existencia y la buena fundación de conjuntos ordenados con ese tipo de orden. No se puede justificar la recursión sobre ordinales o sobre relaciones bien ordenadas arbitrarias. Así, la inducción, que es el corazón de la aritmética, está ausente en (grandes partes de) la geometría. Por otra parte, la intuición espacial está ausente en la aritmética, así que necesitamos a ambas.

La concepción geométrica de los enteros como puntos igualmente espaciados en una recta sugiere que todos los números naturales están en pie de igualdad. En términos russelianos, son todos del mismo tipo. En la concepción aritmética, el 0 *es el número natural más simple, a partir del cual se generan números mayores y, por lo tanto, más complejos que los anteriores, así que no todos los números naturales son del mismo tipo.* Se ejerce la violencia contra cada una de estas intuiciones cuando se trata de subordinar la una a la otra, así que tal vez deberíamos buscar una filosofía de las matemáticas que permita a ambas progresar en una interacción saludable.*

(∗) *Esta sucesión de enteros aritméticos es capturada hermosamente por la definición de ordinal de von Neumann. Por eso no puedo aceptar el punto de vista del profesor Mac Lane según el cual la definición de von Neumann es un mero "artilugio".*

En 2001 Mathias publicó *La potencia de la teoría de Mac Lane* dedicado *"A Saunders Mac Lane con ocasión de su nonagésimo cumpleaños"* (Mac Lane había cumplido 90 años en 1999), donde demuestra que si la teoría de Mac Lane es consistente, también lo es la que resulta de añadirle los axiomas de KP y el axioma de constructibilidad. De paso discute minuciosamente la capacidad y las relaciones mutuas de hasta 24 variantes de teorías de conjuntos. El artículo es estrictamente técnico, excepto su parte final, donde podemos leer:

Durante algunos años ha existido una rivalidad, no siempre amistosa, entre dos bandos, a los que llamaré CAT *y* SET. *Ambos bandos, al menos los miembros más extremos de cada facción, afirman tener la única visión verdadera de las matemáticas puras.*

Esta rivalidad se deriva de las dos reacciones a la crisis fundacional de principios del siglo XX: el enfoque de la teoría de tipos —que comenzó con Russell, Whitehead, Ramsey, Chwistek y Quine— y el de la teoría de conjuntos, que comenzó con Zermelo, Fraenkel y Skolem (quien, a pesar de sus importantes contribuciones a su desarrollo, no habría considerado la teoría de conjuntos como una solución) y muchos otros desde entonces.

He escrito en [L5] *sobre las deficiencias fundacionales de Bourbaki. Un estudio mucho más profundo es el de Leo Corry* [L4], [L7], *a partir de cuyos escritos me he formado la opinión de que Mac Lane y*

su escuela han logrado con éxito lo que los bourbakistas habían intentado en algunas ocasiones: dar una organización conveniente a la parte de las matemáticas relacionada con la teoría de tipos. Lo que no creo es que Mac Lane haya encontrado una organización para la totalidad de las matemáticas.

De hecho, vería con recelo cualquier pretensión de alguien de tener una explicación de la totalidad de las matemáticas, porque creo que las matemáticas surgen de al menos dos intuiciones distintas, [la espacial y la temporal, o la geométrica y la aritmética] *y que el equilibrio entre estas intuiciones será diferente en distintos matemáticos. Deseo la unidad de las matemáticas —es decir, su comunicabilidad—, aunque creo que debe resistirse la presión de grupos particulares que buscan imponer una uniformidad perjudicial sofocando enfoques alternativos.*

El bando CAT *puede, con razón, afirmar que la teoría de categorías revela sutilezas de la geometría a las que la teoría de conjuntos es ciega. Pero eso dista mucho de afirmar cosas como "Las matemáticas no necesitan la teoría de conjuntos" o "La teoría de conjuntos ha sido relegada por la marea de la historia".*

Es totalmente razonable que la gente afirme que considera que su tipo de matemáticas se beneficia más adoptando el estilo de la teoría de categorías. Pero quienes hacen esa afirmación deben conceder la misma libertad a quienes consideran ajeno el estilo de la teoría de categorías.

El bando SET *puede, con igual justicia, afirmar que el análisis de la teoría de conjuntos revela sutilezas que el bando* CAT *ignora: para ejemplos, véase mi artículo expositivo* Afirmaciones fuertes del análisis [F4], *donde se argumenta que las hipótesis sobre cardinales grandes estudiadas por los especialistas en teoría de conjuntos están inextricablemente involucradas en ciertos conceptos, problemas y teoremas del análisis. Ese artículo surgió de conversaciones con matemáticos de diversos orígenes que habían hecho pronunciamientos precipitados sobre una supuesta irrelevancia de la lógica para su trabajo. Su propósito no era decir que no se debería estudiar la teoría de topos, sino mostrar que se perdería mucha comprensión al negarse a contemplar la teoría de conjuntos.* [...]

No es mi propósito criticar a Mac Lane alegando que su sistema es débil. No hay nada de malo en estudiar sistemas débiles; en estos sistemas se requiere mucha matemática compleja; se puede obtener mucha información cuando algo tiene una demostración en un sistema débil; pero a veces un sistema no puede resolver un problema y es necesario saber cuándo ocurre esto. [...]

Hay partes del razonamiento matemático en las que el lenguaje de categorías ofrece una presentación muy fluida (por ejemplo, el tratamiento de las estructuras algebraicas que surgen en geometría, que se limitan esencialmente a tipos ω en el espacio considerado); hay partes en las que resulta torpe (por ejemplo, las construcciones recursivas); hay partes que no puede manejar en absoluto (por ejemplo, la determinación). Por lo tanto, creo que las matemáticas se enriquecerían si los miembros de los diferentes campos fundacionales aprendieran algo del lenguaje y las percepciones fundamentales de los demás.

El Cálculo de Construcciones Entre las propuestas para fundamentar las matemáticas en términos "estructurados", unas de las más provechosas son las que conectan con lenguajes de programación. Entre ellas destaca, por ejemplo, el llamado *Cálculo de Construcciones,* una forma de cálculo lambda cuyas siglas (CoC) recuerdan sospechosamente a su creador, Thierry Coquand, que lo presentó en 1988 en un artículo conjunto con Gérard Huet. En 1989, junto con varios colaboradores, presentaron Coq, un asistente de demostración basado en una variante de CoC llamada *Cálculo de Construcciones Inductivas.* Otra variante es la que usa Lean, el asistente de demostración que hemos mencionado más arriba.

Una versión posterior de Coq llamada Rocq se ha usó, por ejemplo, en 2002 para generar una prueba "legible" del teorema de los cuatro colores, y en 2012 para comprobar la demostración del teorema de Feit-Thompson (cuya prueba simplificada ocupa dos libros enteros) y en 2024 para demostrar que una máquina de Turing descubierta en 1989 por Heiner Marxen y Jürgen Buntrock (que imprime 4 098 unos en 47 176 870 pasos) es la ganadora absoluta del concurso del castor laborioso de 5 estados.

Capítulo IV

La formalización de la metamatemática

Como el lector debería haber sacado en claro de la lectura de este libro, la matemática formal necesita sustentarse inevitablemente en una serie de resultados metamatemáticos que, por pura necesidad, no pueden considerarse demostrados formalmente, ya que tienen que ser lógicamente anteriores a la matemática formal que se pretende definir y estudiar. Estos resultados incluyen, como mínimo, los resultados sintácticos estrictamente finitistas necesarios para definir los lenguajes formales y demostrar lo necesario para que sea viable trabajar con ellos (lo que incluye metateoremas que nos eviten tener que dar demostraciones explícitas y detalladas de cada resultado, lo cual sería imposible en la práctica). Pero la metamatemática incluye también una parte semántica, una teoría de modelos informal, cuyos requisitos trascienden el finitismo, pero sin salir del ámbito conceptual para el que nuestra intuición proporciona interpretaciones precisas que nos permiten afirmar que cuanto decimos es objetivamente verdadero.

Ahora bien, que la matemática formal se sustente en una metamatemática informal no está reñido con que, una vez construida aquélla, ésta pueda formalizarse en ella. Toda la metamatemática puede formalizarse trivialmente en cualquier teoría de conjuntos potente, como ZFC, y es frecuente que muchos libros de lógica matemática (que no aspiren a justificar la matemática formal) trabajen directamente en ZFC, lo que permite desarrollar la lógica mucho más allá de lo que tendría sentido si tuviéramos la necesidad de atribuir a cada resultado un contenido intuitivo preciso (y eso permite hablar de lenguajes formales con una cantidad no numerable de signos, o con fórmulas infinitamente largas, o de ultrapotencias, etc.)

Pero también es posible formalizar la metamatemática en teorías mucho más débiles que ZFC, tan débiles que podemos justificar intuitivamente su consistencia. Al hacerlo así, respondemos a una pregunta muy natural y pertinente a la hora de entender la metamatemática en general y la fundamentación de la matemática en particular: ¿qué supuestos intuitivos son necesarios para demostrar los resultados metamatemáticos?

En la página 306, Curry describe muy bien las características principales de lo que él llama despectivamente "la metafísica intuicionista", que no es sino la intuición en el sentido kantiano (no en el sentido peyorativo que le dan muchos formalistas "desubicados"), y está en lo cierto cuando dice que no es posible describirla mediante reglas preestablecidas. Esto no se debe a que sea caótica o azarosa, sino a que es imposible darle a una regla el grado de generalidad justo. Uno puede encontrarse en una situación en la que sea intuitivamente evidente que es posible extraer una cierta conclusión, pero que cualquier intento de formular un principio general del cual esa inferencia pueda verse como un caso particular puede llevarnos a un principio demasiado general, en cuanto que no podamos asegurar que cualquier aplicación que se haga de él vaya a estar intuitivamente justificada.

Pero una cosa es determinar formalmente *a priori* el alcance de nuestro conocimiento intuitivo (algo que no tiene visos de ser posible, porque los límites de nuestra intuición son muy difusos, y precisamente por eso no es fiable apoyarse en la intuición cuando uno se acerca a dichos límites) y otra muy distinta definir teorías formales cuyos axiomas (y reglas de inferencia) sean intuitivamente válidos sin lugar a dudas, con lo que delimitan formalmente una porción parcial, pero precisa, de nuestro conocimiento intuitivo suficiente para demostrar los resultados metamatemáticos o, mejor aún, podemos utilizar teorías distintas, con axiomas más o menos potentes según lo necesario para demostrar unos teoremas u otros. Esto nos lleva a lo que se conoce como *matemáticas inversas.*

El origen de las matemáticas inversas se remonta a los *Fundamentos de las matemáticas,* de Hilbert y Bernays, donde pusieron de manifiesto que, para formarlizar una buena parte de las matemáticas, no es necesario ZFC, ni siquiera una teoría de conjuntos como la que proponía MacLane, sino que en realidad basta con lo que se conoce como *aritmética de Peano de segundo orden* (AP^2), una teoría axiomática que formaliza los números

naturales y los subconjuntos del conjunto de los números naturales. Por otro lado, aunque con argumentos y técnicas demasiado "personales", Bishop había difundido la idea de que, en realidad, hay una gran parte de la matemática que puede formalizarse en términos "constructivos". La teoría AP^2 dista mucho de ser "constructiva" en ningún sentido razonable de la palabra, pero es posible definir teorías más débiles a cuyos axiomas se les puede dar una interpretación que va desde el constructivismo más estricto (o casi más estricto, porque estas teorías no cuestionan la lógica clásica) a un contenido no constructivo, pero intuitivamente bien definido, en las que es posible demostrar una porción mayor o menor de la matemática clásica.

Varias teorías de estas características habían sido introducidas y estudiadas por diversos motivos, pero en el decimoséptimo Congreso Internacional de Matemáticos, celebrado en Vancouver en 1974, Friedman presentó cinco subteorías de AP^2 que hoy se conocen como *las cinco grandes,* y mostró que algunos teoremas clásicos eran equivalentes, sobre la base de la más débil de ellas, a los axiomas de alguna de las otras cuatro (cada una se obtiene de añadir un axioma a la primera). Esta idea fue desarrollada en 1976 en la tesis doctoral de Steel, y durante la década de los ochenta se fueron configurando las *matemáticas inversas* bajo el impulso principal de Simpson. Su objetivo es encontrar la teoría más débil en la cual es posible demostrar cada teorema de un área lo más amplia posible de las matemáticas clásicas (álgebra, análisis, etc.) y también de la lógica matemática. Cuando hablamos de un teorema que no es demostrable en la teoría más débil, la matemática inversa trata de encontrar una equivalencia demostrable en ésta entre el teorema y el axioma que determina una de las teorías usadas como referencia (que no tiene por qué ser necesariamente una de las cinco grandes, aunque suele serlo en la práctica).

En este capítulo presentaremos los resultados principales de las matemáticas inversas en relación con los teoremas principales de la metamatemática, para obtener así una idea precisa de los principios intuitivos que son necesarios para su justificación.

El estudio de las relaciones mutuas entre las cinco grandes (que son fragmentos de la aritmética de segundo orden), así como entre ellas y "sus partes de primer orden" (en el sentido que explicaremos más adelante) forma parte de la teoría de la demostración, que ha desarrollado espectacularmente las ideas de Gentzen. Algunas referencias históricas son tres libros titulados igualmente *Teoría de la demostración,* el de 1960 de Kurt Schütte (doctorado en 1934 bajo la dirección de Hilbert), el de 1975 de Gaisi Takeuti y el de 1989 de Wolfram Pohlers (doctorado en 1973 bajo la dirección de Schütte).

4.1 La aritmética recursiva primitiva

Nuestro punto de partida es la Aritmética Recursiva Primitiva (ARP), que hemos presentado con cierto nivel de detalle en la sección 80 del capítulo I, en la página 197. De hecho, todo este capítulo cuarto puede verse como una prolongación de dicha sección. Allí seguimos aproximadamente la formulación de Goodstein de la ARP. Vimos que el lenguaje formal de ARP es peculiar porque carece de signos lógicos. Tiene una constante para nombrar al cero y funtores que nombran a todas las funciones recursivas primitivas y sus fórmulas se reducen a ecuaciones $t_1 = t_2$ entre términos. Los axiomas de ARP (página 201) son simplemente las definiciones de las funciones recursivas primitivas y las cuatro reglas de inferencia (página 202) expresan hechos completamente elementales (salvo, a lo sumo, la que expresa un caso particular del principio de inducción, que puede parecer sofisticada, pero al analizarla se pone de manifiesto que no es más que un caso muy particular de este principio).

Las fórmulas del lenguaje de ARP tienen una interpretación natural y resulta difícil concebir que alguien pueda poner objeción alguna a la validez de sus axiomas y reglas de inferencia, por muy intuicionista, constructivista, finitista o loqueseaísta que sea. Ni siquiera se puede objetar el uso de la lógica clásica porque las fórmulas de ARP no presuponen ninguna lógica. No tienen negadores ni disyuntores susceptibles de suponer el tercio excluso o la doble negación.

Ahora bien, hemos visto que en ARP es posible *definir* los conectores lógicos y los cuantificadores acotados $\bigwedge u \leq x$, $\bigvee u \leq x$ y *demostrar* las leyes de la lógica clásica a partir de sus modestos axiomas. Es difícil no ver en esto una refutación de cualquier reticencia al uso de la lógica clásica, al menos en el marco finitista delimitado por ARP.

En efecto, ARP garantiza el carácter estrictamente finitista de sus teoremas por el hecho de que su lenguaje formal está mutilado, carece de cuantificadores (no acotados), de modo que la única forma de expresar que una afirmación es válida para todos los números naturales es a través del convenio de que una variable libre representa a un número natural arbitrario. Así, por ejemplo,

$$x + y = y + x$$

es un teorema de ARP, que se demuestra por inducción, y que afirma que la conmutatividad de la suma es válida *para todos* los números naturales x, y.

El lector podría pensar que esto es una trampa, porque muestra que en realidad ARP sí que tiene un cuantificador universal, aunque sea "invisible", pero no es cierto. El hecho de que no haya un cuantificador universal "tangible" tiene consecuencias drásticas. Por ejemplo, es cierto que una fórmula $\alpha(x)$ equivale a lo que podríamos escribir como $\bigwedge x\,\alpha(x)$ si dispusiéramos de un cuantificador universal "tangible", pero en el lenguaje de ARP no se puede escribir algo equivalente a $\bigvee x\,\alpha(x)$. El intento de reducir una afirmación como ésta al cuantificador universal mediante $\neg\bigwedge x\neg\alpha(x)$ no es expresable en ARP, porque no tenemos un cuantificador que intercalar entre los dos negadores.

La única forma de expresar en el lenguaje de ARP una afirmación que en un lenguaje "no mutilado" expresaríamos como $\bigvee x\,\alpha(x)$ es encontrar un x concreto que cumpla $\alpha(x)$ y escribir $\alpha(0)$, o $\alpha(1)$, o $\alpha(2)$, etc., según quién sea x. Y lo mismo vale si no sólo se trata de enunciar, sino de demostrar:

> La única forma de demostrar en ARP que existe un número natural que cumple una propiedad es encontrar uno en concreto que la tenga y demostrar que así sucede.

Así pues, ARP no admite demostraciones de existencia no constructivas, sencillamente porque su lenguaje no tiene capacidad para expresarlas. Similarmente, el lenguaje de ARP no permite expresar ninguna afirmación que, en un lenguaje "no mutilado", se expresaría en la forma $\bigwedge x\bigvee y\,\alpha(x,y)$ salvo que encontremos una función recursiva primitiva (que admitirá un nombre f en el lenguaje de ARP) que cumpla $\alpha(x, f(x))$. Así pues:

> La única forma de demostrar en ARP para cada número natural x existe un número natural y que cumple una propiedad $P(x,y)$ es (supuesto que dicha propiedad sea definible en ARP) encontrar un funtor monádico f que permita demostrar $\alpha(x, f(x))$, donde α es una fórmula que expresa la propiedad P.

Esto significa que todas las pruebas de existencia en ARP son necesariamente constructivas. Sólo se puede demostrar (o meramente enunciar) que existe un número natural que cumple algo en función de unos parámetros demostrando cómo se puede construir efectivamente un número tal a partir de dichos parámetros.

A los matemáticos les desagrada que les impidan enunciar afirmaciones por restricciones sintácticas, pero en este caso se ve que las restricciones que impone ARP no son gratuitas ni arbitrarias, sino que tienen la finalidad clara de evitar que ARP pueda formalizar ninguna clase de argumento no constructivo. Ahora bien, sucede que podemos mantener estas garantías sin necesidad de mutilar el lenguaje formal. Pero antes de entrar en ello conviene que recordemos una característica de ARP que ya hemos señalado en la sección 80 del capítulo I:

> En ARP se pueden formalizar los conceptos de "lenguaje formal", "fórmula", "demostración", etc., para lenguajes formales arbitrarios y también para el lenguaje formal "peculiar" de ARP, y demostrar formalmente todos los resultados básicos sobre estos conceptos (todos los que no hacen referencia a modelos o a "verdad" o "falsedad" de fórmulas), incluyendo los resultados sobre la lógica de ARP que en principio necesitan ser formulados como metateoremas y demostrados en términos intuitivos finitistas para que podamos estar en condiciones de usar ARP.

En particular, esto significa que ARP "se justifica a sí misma", en el sentido de que, si nos preguntamos qué presupuestos intuitivos hemos aceptado para construir ARP, la respuesta es que no más que los que expresan los axiomas y reglas de inferencia de ARP, porque bastan estos axiomas y reglas de inferencia para definir y demostrar formalmente (las formalizaciones de) todos los metateoremas sobre ARP que se usan para definirla y volverla "operativa" en la práctica (lo que incluye, por ejemplo, la definición de los signos lógicos y la demostración de que en ARP se pueden demostrar las propiedades que éstos deben cumplir, etc.)

Pero, más aún, en ARP podemos definir, por ejemplo, el lenguaje formal (usual) de la aritmética, que, además de las variables y los signos lógicos, incluye la constante 0 y los funtores $S, +, \cdot$, y definir los axiomas de Peano que hemos enunciado en la página 60, y definir lo que es un teorema de la aritmética de Peano, etc.

Similarmente, podemos considerar que la definición siguiente es una definición formal en ARP (enunciada en el lenguaje natural, como habitualmente hacen todos los libros de matemáticas, aunque técnicamente estén enunciando y demostrando teoremas de ZFC):

Definición 4.1 Llamamos ARP^+ a la teoría axiomática sobre el lenguaje de la aritmética extendido[1] con los funtores de ARP y cuyos axiomas son los de ARP (es decir, las definiciones de los funtores) más los siguientes:

[1]Notemos que los funtores S, $+$ y $\cdot$ del lenguaje de la aritmética se corresponden con tres de los funtores de ARP, por lo que hay que entender que extendemos el lenguaje de la aritmética añadiéndole todos los funtores del lenguaje ARP distintos de los tres que ya tiene.

1. $Sx \neq 0$.
2. $Sx = Sy \to x = y$
3. $\alpha(0) \wedge \bigwedge u(\alpha(u) \to \alpha(Su)) \to \bigwedge u\, \alpha(u)$,
   para toda fórmula $\alpha(u)$ sin cuantificadores (tal vez con más variables libres).

Si el lector compara estos axiomas con los de la aritmética de Peano debe tener en cuenta que los axiomas 3, 4, 5 y 6 (en la numeración de la página 60) que definen la suma y el producto son parte de los axiomas de ARP (los que definen los funtores + y ·), por lo que los axiomas de ARP$^+$ incluyen a todos los axiomas de la aritmética de Peano salvo que el principio de inducción está restringido a fórmulas sin cuantificadores (pero, a cambio, son fórmulas que pueden contener todos los funtores del lenguaje de ARP y no sólo los del lenguaje de la aritmética).

Y el teorema siguiente, que no es trivial, es demostrable en ARP (es decir, mediante un argumento indiscutiblemente finitista), usando técnicas de la teoría de la demostración:

Teorema 4.2 *Una fórmula del lenguaje de* ARP *es demostrable en* ARP *si y sólo si lo es en* ARP$^+$.

La demostración (como no podía ser de otra manera, siendo formalizable en ARP) es constructiva, de modo que existe un algoritmo para transformar cada demostración en ARP$^+$ (de una fórmula del lenguaje de ARP) en una demostración en ARP.

Teniendo esto en cuenta, a partir de aquí sería absurdo trabajar en ARP, pues resulta mucho más cómodo trabajar en ARP$^+$, teniendo a nuestra disposición todos los signos lógicos y todas las reglas de inferencia de la lógica clásica, sabiendo que las conclusiones a las que lleguemos (bajo el supuesto obviamente necesario de que sean expresables en el lenguaje de ARP) son, de hecho, demostrables en ARP. En realidad ARP$^+$ se parece mucho más a la formulación original de Skolem que lo que hemos llamado ARP, que es una variante de la presentación posterior debida a Goodstein. El interés teórico de ARP reside en que, en principio, uno puede pensar que aceptar la validez de ARP$^+$ supone aceptar *a priori* la validez intuitiva de toda la lógica clásica, mientras que ahora sabemos que en realidad basta con aceptar la existencia de las funciones recursivas primitivas (un concepto indiscutiblemente finitista), así como unas reglas de inferencia elementales que no presuponen la lógica clásica.

4.2 La aritmética de Peano con inducción restringida

En ARP$^+$, el principio de inducción está restringido a fórmulas sin cuantificadores. Alguien que simplemente lea la definición de ARP$^+$ considerará esta restricción arbitraria y caprichosa. De ahí la importancia del estudio metamatemático[2] de las teorías axiomáticas para justificar lo que en principio puede presentarse como arbitrario. En efecto, según hemos visto en la sección anterior, esta restricción garantiza que ARP$^+$ es equivalente a ARP, lo que a su vez garantiza que todos los razonamientos formalizables en ella son de carácter estrictamente constructivo.[3] Ahora bien, esta extensión de ARP se puede mejorar. Para ello conviene introducir las definiciones siguientes:

Definición 4.3 Una fórmula del lenguaje de ARP$^+$ es de tipo Δ_0^* si todos sus cuantificadores están acotados en la forma $\bigwedge x \leq t$ o $\bigvee x \leq t$, donde t es un término que no tiene a x como variable libre.[4]

Una fórmula del lenguaje de ARP$^+$ es de tipo Σ_1^* (resp. Π_1^*) si es de la forma

$$\bigvee x_1 \cdots x_n\, \alpha(x_1, \ldots, x_n) \qquad (\text{resp. } \bigwedge x_1 \cdots x_n\, \alpha(x_1, \ldots, x_n)),$$

donde α es una fórmula de tipo Δ_0^*. Las fórmulas de tipo Π_2^* son las de la forma

$$\bigwedge x_1 \cdots x_n \bigvee y_1 \cdots y_m\, \alpha(x_1, \ldots, x_n, y_1, \ldots, y_m),$$

de nuevo con α de tipo Δ_0^* (entendiendo que esto incluye a las de tipo Σ_1^* y a las de tipo Π_1^*).

[2] Aquí metamatemático no significa necesariamente que tenga que hacerse en un marco de razonamiento intuitivo. Insistimos en que toda la metateoría sobre ARP, ARP$^+$ y otras teorías axiomáticas puede desarrollarse formalmente en ARP, o equivalentemente, en ARP$^+$ (siempre entendiendo que nos referimos a los aspectos puramente sintácticos que estamos considerando aquí, sin hablar de interpretaciones de fórmulas en modelos).

[3] Más precisamente, todos los razonamientos que demuestran fórmulas expresables en el lenguaje de ARP.

[4] Aquí hay que entender que, en ARP$^+$, se define $x \leq y \equiv \bigvee u\, u + x = y$.

Las fórmulas del lenguaje de ARP son las de la forma $t_1 = t_2$, donde t_1 y t_2 son términos del lenguaje de ARP, pero, como hemos visto que en ARP es posible definir los conectores lógicos y los cuantificadores acotados, una comprobación rutinaria muestra que toda fórmula de tipo Δ_0^* es equivalente en ARP^+ a una fórmula de tipo $t_1 = t_2$. Pero, más aún, teniendo en cuenta que en ARP las variables libres equivalen a variables cuantificadas universalmente, concluimos que las fórmulas de tipo Π_1^* son, ni más ni menos, las que expresan afirmaciones enunciables en el lenguaje de ARP.

Más precisamente, una fórmula $\bigwedge x_1 \cdots x_n\, \alpha(x_1, \ldots, x_n)$ de tipo Π_1^*, será demostrable en ARP^+ si y sólo si lo es la fórmula $\alpha(x_1, \ldots, x_n)$, de tipo Δ_0^*, la cual es equivalente en ARP^* a una fórmula $t_1 = t_2$, que será demostrable en ARP^+ si y sólo si lo es en ARP. En resumen:

> Para cada fórmula del lenguaje de ARP, podemos calcular explícitamente una sentencia de tipo Π_1^* del lenguaje de ARP^+, de modo que demostrar una en ARP es equivalente a demostrar la otra en ARP^+, y viceversa.

Recordemos que en ARP^+ el principio de inducción sólo se admite como axioma para fórmulas sin cuantificadores. Ahora lo extendemos un poco:

Definición 4.4 Llamaremos $\mathrm{I}\Sigma_1^+$ a la teoría axiomática que resulta de extender ARP^+ admitiendo el principio de inducción para fórmulas de tipo Σ_1^* (y se puede demostrar que esto equivale a admitirlo para fórmulas de tipo Π_1^*).

El teorema siguiente es otro ejemplo de teorema no trivial, demostrable en ARP (o, más cómodamente, en ARP^+) mediante técnicas de la teoría de la demostración:

Teorema 4.5 *Una fórmula de tipo Π_2^* es demostrable en $\mathrm{I}\Sigma_1^+$ si y sólo si lo es en* ARP^+.

En particular:

> Para cada fórmula del lenguaje de ARP, podemos calcular explícitamente una sentencia de tipo Π_1^* del lenguaje de ARP^+, de modo que demostrar una en ARP es equivalente a demostrar la otra en ARP^+ o en $\mathrm{I}\Sigma_1^+$, y viceversa.

Así pues, a efectos prácticos, es equivalente trabajar en ARP, o en ARP^+ o en $\mathrm{I}\Sigma_1^+$, pues cualquier teorema que demostremos en las dos últimas y que sea expresable en el lenguaje de la primera será, de hecho, demostrable en la primera, pero en $\mathrm{I}\Sigma_1^+$ disponemos de medios más potentes para llevar a cabo las demostraciones más cómodamente. No obstante, esto todavía se puede mejorar:

Definición 4.6 Una fórmula del lenguaje de la aritmética es de tipo Δ_0 si todos sus cuantificadores están acotados en la forma $\bigwedge x \le y$ o $\bigvee x \le y$ (donde la variable y es distinta de x).

Las fórmulas de tipo Σ_1, Π_1 o Π_2 son las de la forma $\bigvee x\, \alpha(x)$, $\bigwedge x\, \alpha(x)$, $\bigwedge x \bigvee y\, \alpha(x, y)$, donde la fórmula α es de tipo Δ_0.

Una fórmula del lenguaje de la aritmética es de tipo Δ_1 en una teoría T si en ella es equivalente a una de tipo Σ_1 y a la vez a otra de tipo Π_1. Por ejemplo, toda fórmula de tipo Δ_0 es trivialmente de tipo Δ_1, pues ella misma es Σ_1 y Π_1. Cuando hablemos de fórmulas de tipo Δ_1 sin especificar ninguna teoría T, nos referiremos a fórmulas de tipo Δ_1 en $\mathrm{I}\Sigma_1$.

La teoría $\mathrm{I}\Sigma_1$ es la teoría axiomática que resulta de restringir el principio de inducción en la aritmética de Peano a fórmulas de tipo Σ_1 (y se puede demostrar que esto equivale a admitirlo para fórmulas de tipo Π_1).

La diferencia fundamental entre las fórmulas de tipo Δ_0^* y Δ_0 es que las primeras pueden contener cualquier funtor del lenguaje de ARP, mientras que las segundas sólo pueden tener los funtores del lenguaje de la aritmética, es decir, $S, +, \cdot$.

Es claro entonces que los axiomas de $\mathrm{I}\Sigma_1^+$ incluyen a los de $\mathrm{I}\Sigma_1$, por lo que todo teorema de $\mathrm{I}\Sigma_1$ lo es de $\mathrm{I}\Sigma_1^+$. Pero la relación entre ambas teorías es mucho más estrecha debido al hecho siguiente:

> En $\mathrm{I}\Sigma_1$ es posible definir todas las funciones recursivas primitivas mediante fórmulas de tipo Δ_1.

Ejemplo Una función recursiva primitiva es $f(x,y) = x^y$, que en principio no está definida en $\mathrm{I}\Sigma_1$, pero es posible construir una fórmula de tipo Δ_1 (es decir, dos fórmulas equivalentes, una de tipo Σ_1 y otra de tipo Π_1), digamos $\phi(x,y,z)$, de modo que en $\mathrm{I}\Sigma_1$ se demuestra:

$$\bigwedge xz(\phi(x,0,z) \to z = 1), \qquad \bigwedge xyzz'(\phi(x,y,z) \wedge \phi(x,y+1,z') \to z' = z \cdot x),$$

de modo que, si definimos $x^y \equiv z \mid \phi(x,y,z)$, en $\mathrm{I}\Sigma_1$ se demuestra que

$$x^0 = 1, \qquad x^{y+1} = x^y \cdot x.$$

Así, en $\mathrm{I}\Sigma_1$ podemos trabajar con la exponenciación de números naturales sin necesidad de tener un funtor diádico f y unos axiomas que afirmen que

$$f(x,0) = 1, \qquad f(x,y+1) = f(x,y) \cdot x,$$

que sí que son necesarios en ARP^+. Lo mismo sucede con todas las funciones recursivas primitivas. ∎

Por lo tanto, los funtores del lenguaje de ARP (sin contar los tres del lenguaje de la aritmética) son redundantes en $\mathrm{I}\Sigma_1^+$. Más precisamente:

Teorema 4.7 *Para toda fórmula α del lenguaje de ARP^+, existe una fórmula α^* de lenguaje de la aritmética que es equivalente a α en $\mathrm{I}\Sigma_1^+$. Más aún, si α es de tipo Δ_0^*, Σ_1^*, Π_1^* o Π_2^*, entonces α^* puede tomarse de tipo Δ_1, Σ_1, Π_1 o Π_2.*

Como siempre, este teorema puede demostrarse en ARP, luego la demostración es constructiva: a partir de α se puede calcular α^* explícitamente. La idea es sustituir cada funtor que aparezca en α por su definición en $\mathrm{I}\Sigma_1$. Una demostración rutinaria nos da el teorema siguiente:

Teorema 4.8 *Una fórmula α del lenguaje de la aritmética es demostrable en $\mathrm{I}\Sigma_1$ si y sólo si lo es en $\mathrm{I}\Sigma_1^+$.*

Como decimos, esto no es un teorema profundo, sino un teorema técnico, pues sólo expresa que $\mathrm{I}\Sigma_1^+$ no aporta nada a $\mathrm{I}\Sigma_1$ en realidad, pues sólo aporta los funtores que representan las funciones recursivas primitivas junto con los axiomas que los definen, pero esto no sirve de ninguna ayuda para demostrar nada en $\mathrm{I}\Sigma_1$, ya que tales funciones son definibles en $\mathrm{I}\Sigma_1$, luego podemos contar ya con ellas sin necesidad de pasar a $\mathrm{I}\Sigma_1^+$. En particular, los teoremas que hemos enunciado hasta aquí nos dan:

> Para cada fórmula del lenguaje de ARP, podemos calcular explícitamente una sentencia de tipo Π_1 del lenguaje de la aritmética, de modo que demostrar una en ARP es equivalente a demostrar la otra en $\mathrm{I}\Sigma_1$, y viceversa.

Lo mismo vale para fórmulas de tipo Π_2 entre ARP^+ e $\mathrm{I}\Sigma_1$.

En conclusión, para obtener resultados constructivos en el sentido más estricto de la palabra no es necesario trabajar en ARP, o ARP^+, sino que podemos trabajar perfectamente en $\mathrm{I}\Sigma_1$, con la garantía de que todo teorema de tipo Π_1 que demostremos admite una demostración constructiva, aunque esto no sea evidente viendo la demostración que demos. Y la equivalencia es constructiva, es decir, que es posible transformar mecánicamente toda demostración de un teorema Π_1 en $\mathrm{I}\Sigma_1$ en una demostración de la fórmula equivalente en ARP, con lo que su carácter constructivo quedará patente.

Insistimos en que este hecho no es evidente en absoluto a partir de la mera definición de $\mathrm{I}\Sigma_1$. Si a alguien le dicen simplemente que $\mathrm{I}\Sigma_1$ es, por definición, la aritmética de Peano con el principio de inducción restringido a fórmulas de tipo Σ_1 (o Π_1, que es equivalente), lo natural es que se plantee qué razón puede haber para restringir arbitrariamente el principio de inducción de esa manera. Y la respuesta la proporciona la teoría de la demostración al probar esta relación entre $\mathrm{I}\Sigma_1$ y la Aritmética Recursiva Primitiva. El hecho de que la prueba de dicha relación sea formalizable en ARP demuestra que se trata de un hecho que tiene que aceptar como verdadero cualquiera que acepte la validez intuitiva de los axiomas y las reglas de inferencia de ARP.

En particular, tenemos que $0 = 1$ es un teorema de ARP si y sólo si lo es de ARP^+, si y sólo si lo es de $\mathrm{I}\Sigma_1^+$, si y sólo si lo es de $\mathrm{I}\Sigma_1$, luego la consistencia de cualquiera de estas teorías es equivalente a la de los demás, y si aceptamos que todos los axiomas y reglas de inferencia de ARP son válidos en la interpretación natural intuitiva de sus fórmulas, entonces concluimos que todas ellas son consistentes.

Una vez justificados estos hechos, ya no hay necesidad de considerar para nada ARP, con su lógica peculiar sin conectores ni cuantificadores:

A partir de este momento llamaremos ARP a la teoría que hasta ahora hemos llamado ARP^+, y el lenguaje de ARP será el que hasta ahora hemos llamado lenguaje de ARP^+.

De este modo, ARP es una teoría basada en la lógica clásica y podemos considerar[5] a $\mathrm{I}\Sigma_1$ como una *extensión conservativa* de ARP, en el sentido de que ambas teorías demuestran los mismos teoremas de tipo Π_2. Ahora sabemos que cualquier demostración de una sentencia Π_1 en $\mathrm{I}\Sigma_1$ puede considerarse finitista en el sentido más estricto.

Por encima de $\mathrm{I}\Sigma_1$ tenemos la aritmética de Peano AP, que resulta de extender el principio de inducción de $\mathrm{I}\Sigma_1$ a fórmulas arbitrarias, pero aquí es importante darse cuenta de que las "fórmulas arbitrarias" de las que hablamos no son totalmente arbitrarias, sino que son "fórmulas arbitrarias del lenguaje de la aritmética". Por ejemplo, en ZFC podemos demostrar el principio de inducción para fórmulas que no son equivalentes a ninguna fórmula aritmética, pues hacen referencia a conjuntos que no tienen nada que ver con los números naturales.

Es natural preguntarse entonces qué puede demostrarse en AP que no pueda demostrarse en $\mathrm{I}\Sigma_1$. Un ejemplo es la sentencia $\mathrm{Consis}(\ulcorner \mathrm{I}\Sigma_1 \urcorner)$, que afirma que $\mathrm{I}\Sigma_1$ es consistente o, más concretamente, la fórmula $\phi - \mathrm{IND}(\omega^\omega)$, que expresa el principio de inducción transfinita hasta el ordinal ω^ω para una cierta[6] fórmula ϕ (véase la sección 60 del capítulo I, en la página 125). En ARP (luego en $\mathrm{I}\Sigma_1$) se puede demostrar que

$$\phi - \mathrm{IND}(\omega^\omega) \to \mathrm{Consis}(\ulcorner \mathrm{I}\Sigma_1 \urcorner),$$

luego, en virtud del segundo teorema de incompletitud de Gödel, ninguna de las dos fórmulas es demostrable en $\mathrm{I}\Sigma_1$. Para probar cualquiera de ellas hace falta usar el principio de inducción para fórmulas de tipo Π_2, es decir, de la forma $\phi(x) \equiv \bigwedge u \bigvee v \psi(x,u,v)$, donde la fórmula ψ es de tipo Δ_0. ¿Y qué hay de cuestionable en aplicarle el principio de inducción a una fórmula así? Simplemente, que, fijado un número natural n, hay que suponer que se cumple $\bigwedge u \bigvee v \psi(n,u,v)$ para tratar de demostrar $\bigwedge u \bigvee v \psi(n+1,u,v)$, y esto significa suponer que *todos* los números naturales u cumplen la propiedad $\bigvee v \psi(n,u,v)$ como hipótesis de inducción, y eso no es una afirmación finitista en sentido estricto, pues requiere considerar a la vez todos los números naturales, sin que la afirmación pueda reducirse a una afirmación sobre una cantidad finita de ellos.[7] Por el contrario, cualquiera que admita que cada fórmula aritmética $\phi(x)$ expresa una propiedad bien definida (con un significado intuitivo preciso) que puede, o no, poseer un número natural, no tendrá nada que objetar al principio de inducción para fórmulas aritméticas arbitrarias en general, o a la demostración de la consistencia de $\mathrm{I}\Sigma_1$ en particular.

4.3 La lógica de segundo orden

Toda la parte sintáctica de la metamatemática necesaria para definir y estudiar los lenguajes formales en los que basar la matemática formal puede formalizarse en la Aritmética Recursiva Primitiva o, equivalentemente, en $\mathrm{I}\Sigma_1$. Las secciones siguientes las dedicaremos a presentar teorías con una interpretación intuitiva precisa en las que podemos formalizar la teoría de modelos, pero para ello necesitamos dedicar esta sección a discutir la lógica de segundo orden, porque dichas teorías serán subteorías de la aritmética de Peano de segundo orden.

Para presentar las ideas principales sin tener que preocuparnos sobre su posible significado intuitivo, de momento vamos a tomar como metateoría ZF, es decir, las definiciones y teoremas que vamos a discutir a continuación hay que entenderlas como definiciones y teoremas de ZF, enunciados en el lenguaje natural como es habitual en cualquier libro de matemáticas. Llamaremos *lenguajes formales de primer orden* a lo que hasta ahora hemos llamado simplemente lenguajes formales.

[5] Decimos "podemos considerar" porque, técnicamente, la extensión conservativa de ARP es $\mathrm{I}\Sigma_1^+$, pero esta teoría es "esencialmente la misma" que $\mathrm{I}\Sigma_1$.

[6] Se trata de la fórmula $\phi(\alpha)$ que expresa que α no es el ordinal asociado a una demostración de una contradicción en $\mathrm{I}\Sigma_1$ que es expresable en ARP, por lo que se corresponde con una fórmula de tipo Π_1 en $\mathrm{I}\Sigma_1$.

[7] Podría objetarse que lo mismo podría decirse si aplicamos el principio de inducción a una fórmula de tipo Π_1, es decir, de la forma $\phi(x) \equiv \bigwedge u\, \psi(x,u)$ y, en efecto, así es, pero dicho principio de inducción es un teorema de $\mathrm{I}\Sigma_1$, que no es finitista en sentido estricto, pero, por la observación tras el teorema 4.8, sabemos que aceptarlo facilita la demostración de enunciados finitistas, con la garantía de que todos los teoremas admitirán demostraciones finitistas. Esto es lo que justifica que un finitista estricto pueda aceptar las demostraciones en $\mathrm{I}\Sigma_1$, aunque no sean estrictamente finitistas. No puede decirse lo mismo de la inducción para fórmulas de tipo Π_2, pues, con ella puede demostrarse, por ejemplo, $\mathrm{Consis}(\ulcorner \mathrm{I}\Sigma_1 \urcorner)$, que es una afirmación estrictamente finitista (afirma meramente que no existe ningún número natural que codifique una demostración de $0 \neq 0$ en $\mathrm{I}\Sigma_1$) que no es demostrable en $\mathrm{I}\Sigma_1$, luego tampoco en ARP y, por lo tanto, no admite una demostración estrictamente finitista. La teoría $\mathrm{I}\Sigma_1$ no es estrictamente finitista, pero es "reducible al finitismo' en el sentido de que no permite demostrar teoremas con enunciado finitista que no admitan una demostración finitista.

Definición 4.9 A cada lenguaje formal de primer orden $\mathcal{L}^1$ le asociamos un *lenguaje formal de segundo orden* $\mathcal{L}^2$, que consta de los mismos signos que $\mathcal{L}^1$ más un conjunto (numerable) de nuevas variables a las que llamaremos *variables de segundo orden.* A las variables de $\mathcal{L}^1$ las llamaremos, por contraposición *variables de primer orden.*

Adoptaremos el convenio de usar letras minúsculas para nombrar variables de primer orden y letras mayúsculas para nombrar variables de segundo orden.

Para ilustrar las definiciones siguientes consideraremos como ejemplo concreto el lenguaje $\mathcal{L}^1$ de la teoría de cuerpos ordenados descrito en la sección 84 del capítulo I en la página 218.

Llamaremos *fórmulas atómicas* de $\mathcal{L}^2$ a las de una de las formas siguientes:

- Las fórmulas atómicas de $\mathcal{L}^1$. Por ejemplo, $x + y \leq z$, $x = 0$, etc.
- Las de la forma $X = Y$, donde X e Y son variables de segundo orden.
- Las de la forma $X(t)$, donde X es una variable de segundo orden y t es un término de $\mathcal{L}^1$, aunque en la práctica, en lugar de $X(t)$ escribiremos $t \in X$.

Las *fórmulas* de $\mathcal{L}^2$ son las que se construyen a partir de las fórmulas atómicas mediante conectores lógicos y cuantificadores.

La idea es que, en una fórmula de segundo orden, las variables de primer orden se interpretan como objetos (en nuestro ejemplo, los elementos de un cierto cuerpo ordenado) y las variables de segundo orden se interpretan como conjuntos de objetos (subconjuntos del cuerpo ordenado). Para precisar esta idea sólo tenemos que observar que, si M es un modelo del lenguaje $\mathcal{L}^1$, la definición de Tarski de la relación de satisfacción $K \vDash \alpha[v]$ que presentamos en la página 221 (particularizada al lenguaje de la teoría de cuerpos ordenados) se extiende a fórmulas de $\mathcal{L}^2$ sin más que considerar valoraciones v que asignen a cada variable de primer orden un elemento de K y a cada variable de segundo orden un elemento de $\mathcal{P}K$ y distinguir dos casos en la definición de la satisfacción de los cuantificadores según si la variable es de primer o de segundo orden:

7. $K \vDash \bigwedge x\alpha(x)[v]$ si para todo elemento a en K, se cumple $K \vDash \alpha(x)[v^a_x]$. (Una fórmula $\bigwedge x\, \alpha(x)$ es satisfecha si la fórmula $\alpha(x)$ es satisfecha con cualquier interpretación que se le dé a la variable x en K.)
8. $K \vDash \bigvee x\alpha(x)[v]$ si existe un elemento a en K tal que $K \vDash \alpha(x)[v^a_x]$. (Una fórmula $\bigvee x\, \alpha(x)$ es satisfecha si la fórmula $\alpha(x)$ es satisfecha si elegimos adecuadamente la interpretación que le damos a la variable x en K.)
9. $K \vDash \bigwedge X\alpha(X)[v]$ si para todo elemento A en $\mathcal{P}K$, se cumple $K \vDash \alpha(X)[v^A_X]$. (Una fórmula $\bigwedge X\, \alpha(X)$ es satisfecha si la fórmula $\alpha(X)$ es satisfecha con cualquier interpretación que se le dé a la variable X en $\mathcal{P}K$.)
10. $K \vDash \bigvee X\alpha(X)[v]$ si existe un elemento A en K tal que $K \vDash \alpha(X)[v^A_X]$. (Una fórmula $\bigvee X\, \alpha(X)$ es satisfecha si la fórmula $\alpha(X)$ es satisfecha si elegimos adecuadamente la interpretación que le damos a la variable X en $\mathcal{P}K$.)

Por ejemplo, consideremos la sentencia:

$$\mathrm{Comp} \equiv \bigwedge X(\bigvee u\, u \in X \wedge \bigvee v \bigwedge u(u \in X \to u \leq v) \to$$
$$\bigvee s(\bigwedge u(u \in X \to u \leq s) \wedge \bigwedge v(\bigwedge u(u \in X \to u \leq v) \to s \leq v))).$$

Si aplicamos a esta sentencia la definición de satisfacción de la página 221 con las modificaciones que acabamos de señalar obtendremos que $K \vDash \mathrm{Comp}$ equivale a lo que uno entiende sin más que "leer" la fórmula de forma natural:

Todo subconjunto X de K no vacío y acotado superiormente tiene supremo s (una mínima cota superior).

En resumen, un cuerpo ordenado K, como modelo de $\mathcal{L}^2$, satisface la sentencia de segundo orden Comp si y sólo si es un cuerpo completo en el sentido usual que este concepto tiene en análisis, o en topología.

Lo más destacable es que esta propiedad de completitud no puede expresarse mediante ninguna sentencia de $\mathcal{L}^1$, es decir, mediante ninguna sentencia de primer orden, porque con ellas es imposible hacer referencia a todos los subconjuntos del cuerpo.[8]

[8]Una demostración de que esto es así consiste en observar que cualquier conjunto de sentencias de primer orden del lenguaje de la teoría de cuerpos ordenados admite infinitos modelos no isomorfos entre sí. Por ejemplo, admite un modelo de cada cardinal infinito, por la versión general del teorema de Löwenheim-Skolem. En cambio, es un hecho conocido que $\mathbb{R}$ es el único cuerpo ordenado completo, lo cual significa que, si a los axiomas de cuerpo ordenado les añadimos Comp, la teoría (de segundo orden) resultante no admite (salvo isomorfismo) más modelo que $\mathbb{R}$.

La aritmética de Peano de segundo orden I Algo similar sucede si añadimos a la aritmética de Peano de primer orden la versión de segundo orden del principio de inducción:

$$\bigwedge X(0 \in X \wedge \bigwedge u(u \in X \to u+1 \in X) \to \bigwedge u\, u \in X).$$

Sabemos que la aritmética de Peano de primer orden admite, además del modelo natural, muchos otros modelos "no estándar". En cambio:

Teorema 4.10 *El único modelo de la aritmética de Peano dotada del axioma de inducción de segundo orden es (salvo isomorfismo) el natural.*

DEMOSTRACIÓN: Sea M un modelo arbitrario de estos axiomas. Esto significa que las variables de primer orden se interpretan como objetos de M y las de segundo orden como objetos de $\mathcal{P}M$. Sea m_0 el objeto denotado por la constante 0 en M, y definimos recurrentemente

$$m_{k+1} = M(S)(m_k),$$

donde $M(S) : M \longrightarrow M$ es la función que interpreta en M el funtor S. Llamamos $M^* = \{m_k \mid k \in \mathbb{N}\} \subset M$. El hecho de que M satisfaga los axiomas 1 y 2 de la página 60 se traduce fácilmente en que la aplicación $f : \mathbb{N} \longrightarrow M^*$ dada por $f(k) = m_k$ es inyectiva. Por otro lado, si consideramos una valoración tal que $v(X) = M^*$, se cumple

$$M \vDash (0 \in X \wedge \bigwedge u(u \in X \to Su \in X))[v],$$

luego el hecho de que M satisfaga el principio de inducción se traduce en que

$$M \vDash (\bigwedge u\, u \in X)[v],$$

lo cual a su vez implica que $M^* = M$. Por lo tanto, $f : \mathbb{N} \longrightarrow M$ biyectiva. Más aún, el hecho de que M satisfaga los axiomas de Peano que definen la suma y el producto se traduce fácilmente en que f es un isomorfismo de modelos. ∎

Esto se expresa diciendo que la aritmética de Peano de segundo orden es *categórica* (determina un único modelo salvo isomorfismo), al igual que lo es la teoría (de segundo orden) de cuerpos ordenados completos. En cambio, si una teoría de primer orden es categórica, su único modelo tiene que ser finito.

Pero esto tiene su reverso negativo. Los teoremas de incompletitud valen igualmente para la lógica de segundo orden (de hecho, Gödel los demostró primero para la lógica de los *Principia Mathematica,* que tiene variables de primer orden, de segundo orden, de tercer orden, etc.), lo que se traduce en que cualquier cálculo deductivo razonable de segundo orden que queramos considerar para deducir consecuencias lógicas de los axiomas de la aritmética de Peano de segundo orden AP^* será semánticamente incompleto: hay sentencias, como $\mathrm{Consis}(\ulcorner \mathrm{AP}^* \urcorner)$, que son verdaderas en todos los modelos de AP^* (en el único que existe), pero que no se pueden deducir de los axiomas de AP^*.

La semántica estándar y la semántica de Henkin El hecho de que las teorías de segundo orden puedan ser categóricas con modelos infinitos depende esencialmente de que, en la definición de satisfacción de una fórmula de segundo orden, hemos establecido que las variables de segundo orden recorren necesariamente la totalidad de los subconjuntos del conjunto de todos los objetos de primer orden. Pero esto hace que la semántica de la lógica de segundo orden (de cualquier teoría con un modelo infinito) trascienda los límites de nuestra intuición. Podemos tratar intuitivamente con lenguajes de segundo orden, como el de la aritmética de Peano de segundo orden, pero lo que no podemos hacer es afirmar que ésta tiene un modelo bien definido en términos intuitivos, porque no podemos precisar cómo tiene que interpretarse un $\bigwedge X$ o un $\bigvee X$. ¿Qué interpretación intuitiva tiene un "para todo conjunto de números naturales"? ¿En qué sentido podemos decir que una afirmación que contenga cuantificadores de segundo orden es intuitivamente verdadera o falsa? Incluso un platonista razonable admitirá que la lógica de segundo orden es "teoría de conjuntos disfrazada", en el sentido de que para estudiarla con rigor es necesario tomar como metateoría una teoría de conjuntos suficientemente potente como para hablar de conjuntos $\mathcal{P}M$.

Ahora bien, la definición de satisfacción que hemos dado, aunque es la tradicional y la pretendida para la lógica de segundo orden, no es la única posible. La semántica de la lógica de segundo orden en la que se exige (como hemos hecho) que las variables de segundo orden puedan recorrer todos los subconjuntos del conjunto de

los objetos de primer orden se conoce como *semántica estándar* o *semántica plena* de la lógica de segundo orden y, como decimos, es "teoría de conjuntos disfrazada". Pero en 1950 Henkin publicó su trabajo *Completitud en la teoría de tipos,* en el que definió lo que hoy se conoce como *modelos de Henkin* de un lenguaje formal de segundo orden, que consisten en especificar, no sólo un conjunto de objetos P de modo que las variables de primer orden pueden recorrer todos los objetos de P (junto con los objetos, relaciones y funciones necesarios para interpretar los signos específicos del lenguaje), sino también un subconjunto $S \subset \mathcal{P}P$ de modo que las variables de segundo orden recorran los elementos de S. El conjunto P se llama *parte de primer orden* del modelo, y el conjunto S es la *parte de segundo orden.* De este modo puede haber varios modelos M de una misma teoría con una misma parte de primer orden, pero cuyas partes de segundo orden sean distintas. La semántica de la lógica de segundo orden que admite modelos de Henkin arbitrarios y no sólo *modelos plenos* (modelos en los que necesariamente $S = \mathcal{P}P$) se conoce como *semántica de Henkin,* y Henkin probó que la lógica de segundo orden con la semántica de Henkin se comporta exactamente igual que la lógica de primer orden. De hecho, lo que sucede es que es "lógica de primer orden disfrazada", en el sentido de que toda teoría de segundo orden puede expresarse a través de una teoría de primer orden adecuada. Vamos a ilustrar esto considerando el caso concreto de la aritmética de Peano, aunque es sólo un ejemplo de una situación general.

La Aritmética de Peano de segundo orden II A continuación damos una definición alternativa del lenguaje formal de la aritmética de segundo orden, pero esta vez de modo que sea un lenguaje formal de primer orden:

Definición 4.11 Llamaremos *lenguaje formal de la aritmética de segundo orden* al lenguaje formal de primer orden cuyos signos no definidos son los del lenguaje de la aritmética $(0, S, +, \cdot)$ más un relator monádico cto y un relator diádico $\in$.

La fórmula $\operatorname{cto} X$ la leeremos "X es un conjunto", mientras que $\operatorname{Nat} x \equiv \neg \operatorname{cto} x$ la leeremos "x es un número natural".[9] Así, en este lenguaje podemos hablar (únicamente) de dos clases de objetos: números naturales y conjuntos (de números naturales).

Dividimos las infinitas variables en dos conjuntos infinitos. A unas las llamaremos *variables de primer orden* y a las otras *variables de segundo orden.* Adoptamos el convenio de usar letras minúsculas para las variables de primer orden y mayúsculas para las de segundo orden.

Llamaremos *fórmulas atómicas estructuradas* a las fórmulas de los tipos siguientes:

- Las fórmulas atómicas del lenguaje de la aritmética (de primer orden) cuyas variables sean todas de primer orden.

  Por ejemplo, $x + y = z + S0$.

- Las de la forma $X = Y$, donde X e Y son variables de segundo orden.

- Las de la forma $t \in X$, donde X es una variable de segundo orden y t es un término del lenguaje de la aritmética (de primer orden) cuyas variables sean todas de primer orden.

Las *fórmulas estructuradas* son las que se construyen a partir de fórmulas atómicas estructuradas mediante conectores lógicos y cuantificadores de la forma:

$$\bigwedge x\, \alpha \equiv \bigwedge x(\operatorname{Nat} x \to \alpha), \quad \bigvee x\, \alpha \equiv \bigvee x(\operatorname{Nat} x \wedge \alpha), \quad \bigwedge X\, \alpha \equiv \bigwedge X(\operatorname{cto} X \to \alpha), \quad \bigvee X\, \alpha \equiv \bigvee X(\operatorname{cto} X \wedge \alpha).$$

No merece la pena entrar en detalles técnicos, pero es claro que las fórmulas estructuradas en este sentido pueden identificarse con las fórmulas de la aritmética de segundo orden en el sentido de la definición 4.9. Una diferencia, que a efectos prácticos es irrelevante, es que según la definición 4.9 un lenguaje formal de segundo orden no tiene más fórmulas que las allí definidas, mientras que con la definición que acabamos de dar existen también fórmulas no estructuradas, como $X \in 0$, que no nos van a interesar para nada. La única excepción es esta sentencia:

$$\mathrm{E} \equiv \bigwedge \alpha\beta(\alpha \in \beta \to \operatorname{Nat} \alpha \wedge \operatorname{cto} \beta),$$

donde hemos usado letras griegas para indicar que α y β son variables arbitrarias, de primer o de segundo orden. Lo que expresa el *axioma estructural* E es que si dos objetos cumplen $\alpha \in \beta$, necesariamente α es un número natural y β es un conjunto.

[9] En otros ejemplos en los que los elementos de los conjuntos no sean números naturales la negación de "ser un conjunto" puede leerse "ser un objeto de primer orden", por ejemplo.

Otro axioma básico es el axioma de extensionalidad:

$$\bigwedge XY(\bigwedge u(u \in X \leftrightarrow u \in Y) \to X = Y).$$

Sólo vamos a considerar modelos del lenguaje de la aritmética de segundo orden que cumplan estos dos *axiomas estructurales* (E y el axioma de extensionalidad). De este modo, en cualquier modelo M (en el sentido usual de modelo para la lógica de primer orden), podremos distinguir el conjunto P de los objetos que cumplen la fórmula $\mathrm{Nat}\, x$ y el conjunto S de los objetos que no la cumplen. Estos conjuntos se llaman *parte de primer orden* y *parte de segundo orden* del modelo. El axioma E y el axioma de extensionalidad nos dicen que cada elemento de S puede identificarse con un subconjunto de P, es decir, que $S \subset \mathcal{P}P$.

En otras palabras, en cualquier modelo del lenguaje de la aritmética de segundo orden (que cumpla los dos axiomas estructurales), podemos distinguir una parte de primer orden, que contiene a los números naturales del modelo, y una parte de segundo orden formada por algunos conjuntos de números naturales, pero no necesariamente todos. Si $S = \mathcal{P}P$ se dice que M es un *modelo pleno.*

La *Aritmética de Peano de segundo orden* (AP^2) es la teoría axiomática (de primer orden) que consta de los axiomas siguientes:

Axioma estructural $\bigwedge\alpha\beta(\alpha \in \beta \to \mathrm{Nat}\alpha \wedge \mathrm{cto}\,\beta)$, donde α y β son variables arbitrarias (y los cuantificadores no están acotados ni por Nat ni por cto).

Extensionalidad $\bigwedge XY(\bigwedge u(u \in X \leftrightarrow u \in Y) \to X = Y)$.

Comprensión Para toda fórmula estructurada $\phi(v, x_1, \ldots, x_r, X_1, \ldots, X_s)$, la sentencia siguiente es un axioma:

$$\bigwedge x_1 \cdots x_r \bigwedge Y_1 \cdots Y_s \bigvee U \bigwedge v(v \in U \leftrightarrow \phi(v, x_1, \ldots, x_r, Y_1, \ldots, Y_s)).$$

AP1 $\mathrm{Nat}\, 0$.

AP2 $\bigwedge x\, \mathrm{Nat}\, Sx$.

AP3 $\bigwedge x\, Sx \neq 0$.

AP4 $\bigwedge xy(Sx = Sy \to x = y)$.

Inducción $\bigwedge X(0 \in X \wedge \bigwedge u(u \in X \to Su \in X) \to \bigwedge u\, u \in X)$.

S1 $\bigwedge x\, x + 0 = x$.

S2 $\bigwedge xy(x + Sy = S(x + y))$.

M1 $\bigwedge x\, x \cdot 0 = 0$.

M2 $\bigwedge xy(x \cdot Sy = x \cdot y + x)$.

Observemos que el conjunto U cuya existencia afirma el axioma de comprensión es único en virtud del axioma de extensionalidad, por lo que podemos darle un nombre:

$$\{v \mid \phi(v, x_1, \ldots, x_r, Y_1, \ldots, Y_s)\}.$$

A primera vista, puede parecer que los axiomas de AP^2 tienen una interpretación intuitiva muy clara y, en particular, que son verdaderos: afirman que existen números naturales y conjuntos de números naturales, que los números naturales cumplen los axiomas de Peano y que los conjuntos cumplen el axioma de extensionalidad (dos conjuntos con los mismos elementos son iguales) y el de comprensión (podemos hablar del conjunto U de los números que cumplen cualquier propiedad prefijada $\phi(v)$).

Sin embargo, no debemos perder de vista que no podemos dar una interpretación intuitiva clara a un "para todo conjunto de números naturales". Es cierto que no estamos obligados a que $\bigwedge X$ signifique "para todo conjunto de números naturales", sino que tenemos libertad para definir un modelo de AP^2 especificando una familia concreta de conjuntos de números naturales como parte de segundo orden, pero no es evidente en absoluto cómo puede elegirse esta parte de segundo orden para que se satisfaga el axioma de comprensión, ya que éste no es predicativo. Para que se satisfaga, tendríamos que escoger una familia de conjuntos de números naturales de modo que siempre exista uno formado por todos los números naturales que cumplen una propiedad dada $\phi(v)$ que puede hacer referencia a la totalidad de los conjuntos considerados. No es inmediato qué familia de conjuntos podemos tomar para que se cumpla esto.

Si ahora abandonamos ZF como metateoría y queremos trabajar intuitivamente, nos encontramos con que la definición de AP^2 tiene perfecto sentido intuitivo, así como el concepto de demostración formal a partir de los axiomas de AP^2 (pues se trata de una teoría axiomática de primer orden como cualquier otra), pero lo que no podemos afirmar es que los axiomas de AP^2 son verdaderos en ningún sentido intuitivo de la palabra, a menos que especifiquemos qué conjuntos tomamos como parte de segundo orden de un posible modelo de AP^2. Por esto mismo, ni siquiera podemos asegurar que AP^2 sea consistente. La Aritmética de Peano AP es consistente, pues admite como modelo al "modelo estándar" formado por los números naturales (intuitivos) con las operaciones usuales, pero no podemos especificar ninguna elección de una parte de segundo orden con la que podamos comprobar que se cumple el axioma de comprensión.

4.4 Comprensión aritmética y comprensión recursiva

Comprensión aritmética La situación cambia drásticamente si restringimos el axioma de comprensión. Para ello, diremos que una fórmula estructurada del lenguaje de la aritmética de segundo orden es *aritmética* si todos sus cuantificadores afectan a variables de primer orden (aunque pueda tener variables libres de segundo orden), y una fórmula es *de primer orden* si además todas sus variables libres son de primer orden. Las fórmulas de primer orden se corresponden con las fórmulas del lenguaje de la aritmética de primer orden, donde la correspondencia consiste en sustituir cada $\bigwedge x$ y $\bigvee x$ por $\bigwedge x(\mathrm{Nat}\, x \to \cdots)$ y $\bigvee x(\mathrm{Nat}\, x \wedge \cdots)$, respectivamente.

Definición 4.12 Llamaremos ACA_0 a la teoría axiomática (de primer orden) que resulta de restringir en AP^2 el esquema axiomático de comprensión a fórmulas aritméticas. Este esquema restringido se llama *Axioma de Comprensión Aritmética.*

Ahora la situación es diferente, porque el teorema siguiente admite una demostración intuitivamente válida (y formalizable en ZF, naturalmente):

Teorema 4.13 *Todo modelo M de* AP *se extiende a un modelo de* ACA_0 *cuya parte de primer orden en M y cuya parte de segundo orden está formada por los subconjuntos de M definibles mediante fórmulas de primer orden.*

La demostración es esencialmente la misma que la que esbozamos en la sección 75 del capítulo I (página 175) por la que todo modelo M de ZF se puede extender a un modelo de NBG tomando como clases propias los subconjuntos de M definibles mediante fórmulas:

Idea de la demostración En términos intuitivos, partiendo de un modelo numerable M de AP, podemos construir explícitamente una enumeración $\Phi_0, \Phi_1, \Phi_2, \ldots$ de todos los pares $\Phi = (\phi, (a_1, \ldots, a_n))$, donde $\phi(x_0, \ldots, x_n)$ es una fórmula del lenguaje de AP y $a_1, \ldots, a_n$ son elementos de M (números naturales, si partimos del modelo estándar). A cada Φ le podemos asociar el conjunto C_Φ formado por todos los números naturales k tales que $M \vDash \phi[k, a_1, \ldots, a_n]$. Tenemos que admitir que C_Φ está bien definido, aunque en la la práctica podamos no disponer de ningún criterio para saber si un número natural k está o no en C_Φ. Así tenemos una sucesión bien definida $C_{\Phi_0}, C_{\Phi_1}, C_{\Phi_2}, \ldots$ de subconjuntos de M, aunque no tenemos ningún criterio para determinar si un C_{Φ_i} es igual o no a un C_{Φ_j}, pero cada afirmación $C_{\Phi_i} = C_{\Phi_j}$ tiene un significado intuitivo preciso, aunque en algunos casos no podamos saber si es cierta o no.

Ahora podemos considerar el modelo $\mathcal{M}$ del lenguaje de la aritmética de segundo orden cuya parte de primer orden es M y cuya parte de segundo orden S está formada por todos los conjuntos C_{Φ_i} (teniendo presente que no son necesariamente distintos dos a dos).

Así, para cada fórmula ϕ del lenguaje de la aritmética de segundo orden y cada valoración v, la afirmación $\mathcal{M} \vDash \phi[v]$ está bien definida. Los puntos clave son que, por una parte, la hipótesis de que M es un modelo (numerable) bien definido, supone que sabemos dar un sentido preciso a cada afirmación del tipo "todo elemento a de M cumple $\mathcal{M} \vDash \phi[v_x^a]$" o "existe un a en M que cumple $\mathcal{M} \vDash \phi[v_x^a]$" y, por otra parte, también tiene un significado intuitivo cualquier afirmación del tipo "todo conjunto A de S cumple $\mathcal{M} \vDash \phi[v_X^A]$" (pues significa que se cumple cuando A es C_{Φ_0}, y cuando A es C_{Φ_1}, y cuando A es C_{Φ_2}, etc., lo sepamos comprobar o no) y también cualquier afirmación del tipo "existe un conjunto A en S tal que $\mathcal{M} \vDash \phi[v_X^A]$" (pues significa que esto se cumple cuando A es C_{Φ_0}, o cuando A es C_{Φ_1}, o cuando A es C_{Φ_2}, etc., lo sepamos comprobar o no). Notemos que el hecho de que en la sucesión de los C_{Φ_i} haya repeticiones no afecta en nada a esto.

Con esto podemos afirmar que $\mathcal{M}$ es un modelo bien definido (lo que incluye que la relación $\mathcal{M} \vDash \phi[v]$ está bien definida (para toda fórmula ϕ del lenguaje de la aritmética de segundo orden y cada valoración v que asigne un elemento de M a sus variables libres de primer orden y un elemento de S a sus variables libres de segundo orden). A partir de aquí es pura rutina comprobar que todos[10] los axiomas de ACA_0 son verdaderos en $\mathcal{M}$. ∎

El parecido entre la demostración de este teorema y la de su análogo para ZF y NBG no es casual. En general, toda teoría de primer orden tiene una *extensión predicativa,* que es la teoría de segundo orden que resulta de añadir (aparte del axioma estructural E) el axioma de extensionalidad y el *axioma de comprensión predicativa,* que afirma que toda fórmula sin variables cuantificadas de segundo orden define un conjunto, y se demuestra que todo modelo de la teoría de primer orden es la parte de primer orden de un modelo de su extensión predicativa. En estos términos, ACA_0 es la extensión predicativa de AP y NBG es la extensión predicativa de ZFC.

La idea que hemos dado de la demostración del teorema 4.13 basta para advertir que, aunque se pueda considerar intuitivamente válida, desde luego no es constructiva. Sin embargo, el teorema siguiente, que es una consecuencia de 4.13 y del teorema de completitud de Gödel, admite también una demostración absolutamente constructiva, sin modelos, formalizable en ARP, basada en técnicas de la teoría de la demostración:

Teorema 4.14 *Los teoremas de primer orden demostrables en* ACA_0 *son exactamente los mismos que los demostrables en* AP.

Así pues, alguien que admita que los axiomas (y, por tanto, los teoremas) de la Aritmética de Peano son afirmaciones verdaderas sobre los números naturales no puede objetar el uso de ACA_0. O bien considera que los conjuntos de los que habla ACA_0 son conceptos "ideales" sin un significado preciso, pero que simplifican las demostraciones de teoremas aritméticos (de primer orden) sin introducir ninguna verdad aritmética nueva, o bien admite que ACA_0 habla de conjuntos aritméticos, que tienen una interpretación intuitiva precisa, de modo que ACA_0 demuestra afirmaciones verdaderas sobre ellos no demostrables en AP simplemente porque no son expresables en su lenguaje. Incluso en el primer caso el uso de ACA_0 está justificado.[11]

Señalamos que, del mismo modo que ZFC no es finitamente axiomatizable, mientras que NBG sí que lo es, también sucede que AP no es finitamente axiomatizable, pero puede probarse que ACA_0 sí que lo es.

Inducción de primer y segundo orden En AP^2 (y, por consiguiente, en ACA_0) hemos expresado el principio de inducción mediante una fórmula de segundo orden. Alternativamente, para cada fórmula estructurada

$$\alpha(u) \equiv \alpha(u, x_1, \ldots, x_n, Y_1, \ldots, Y_m),$$

podemos considerar la fórmula

$$\mathrm{Ind}(\alpha) \equiv \alpha(0) \wedge \bigwedge u(\alpha(u) \to \alpha(Su)) \to \bigwedge u\, \alpha(u).$$

En AP^2, el principio de inducción de segundo orden es equivalente al esquema axiomático formado por todas las fórmulas $\mathrm{Ind}(\alpha)$, para toda fórmula estructurada α, en el sentido de que cualquiera de ellas es demostrable en AP^2 y, recíprocamente, si suprimimos de AP^2 el principio de inducción de segundo orden y añadimos el esquema axiomático Ind, podemos demostrar el principio de inducción de segundo orden. De hecho, el principio de inducción de segundo orden es concretamente $\mathrm{Ind}(\alpha)$, para $\alpha(u) \equiv u \in X$.

Recíprocamente, para demostrar $\mathrm{Ind}(\alpha)$, basta aplicar el esquema de comprensión para formar el conjunto $X = \{u \mid \alpha(u, x_1, \ldots, x_n, Y_1, \ldots, Y_m)\}$ y aplicar el principio de inducción de segundo orden a este X.

[10] A la hora de comprobar el axioma de comprensión aritmética hemos de considerar una fórmula ϕ que puede tener parámetros Y_i de segundo orden, pero cada uno de ellos se interpretará como un objeto de S definido por una fórmula de primer orden, luego sustituyendo en ϕ cada $u \in Y_i$ por la fórmula de primer orden que define al conjunto $v(Y_i)$, obtenemos una fórmula de primer orden que determina un conjunto C_{Φ_i} que satisface el axioma de comprensión para la fórmula y los parámetros considerados.

[11] Aunque es difícil imaginar que alguien pueda admitir que una fórmula $\phi(x)$ del lenguaje de AP tenga un significado bien definido y, al mismo tiempo, cuestione la existencia intuitiva objetiva del conjunto (aritmético) de todos los números naturales que cumplen $\phi(x)$. Esto no puede fundamentarse en una concepción finitista de la aritmética, pues las fórmulas aritméticas pueden contener cuantificadores que obligan a considerar a los números naturales como un infinito actual para atribuirles un sentido, aunque, sin duda, cualquiera es libre de poner los límites de "su finitismo" en cualquier parte que no exceda los límites del contenido intuitivo.

En el caso de ACA_0, el principio de inducción de segundo orden sólo equivale al esquema de inducción para fórmulas aritméticas, pues si tratamos de imitar la prueba precedente, para definir X necesitamos que α sea aritmética. El recíproco no es problema, porque la fórmula $u \in X$ es aritmética.

Esto es precisamente lo que indica el subíndice 0 en ACA_0, que el principio de inducción sólo está disponible para fórmulas aritméticas. La teoría ACA es la que resulta de sustituir en ACA_0 el principio de inducción de segundo orden por el esquema Ind para todas las fórmulas α (no necesariamente aritméticas).

Comprensión recursiva Hemos visto que $\mathrm{I}\Sigma_1$ no es una restricción arbitraria de AP, sino que el efecto de restringir el principio de inducción a fórmulas de tipo Σ_1 es que los teoremas demostrables con esta restricción y expresables en la Aritmética Recursiva Primitiva sean precisamente los demostrables en la Aritmética Recursiva Primitiva, es decir, los que admiten una demostración constructiva. Ahora vamos a ver que, restringiendo adecuadamente ACA_0 podemos obtener una teoría de segundo orden análoga a $\mathrm{I}\Sigma_1$.

Para ello definimos las fórmulas de tipo Δ^0_0 como las fórmulas aritméticas (es decir, sin variables de segundo orden cuantificadas) cuyas cuantificaciones de primer orden son todas de la forma $\bigwedge x \le t$ o $\bigvee x \le t$, donde el término t no tiene libre la variable x. A su vez, las fórmulas de tipo Σ^0_1 y Π^0_1 son, respectivamente las de la forma

$$\bigvee z_1 \cdots z_r\, \alpha, \qquad \bigwedge z_1 \cdots z_r\, \alpha,$$

donde α es una fórmula de tipo Δ^0_1. Una fórmula es de tipo Δ^0_1 si es equivalente a una fórmula Σ^0_1 y a una Π^0_1.

Definición 4.15 Llamaremos ACR_0 a la teoría axiomática que resulta de sustituir en ACA_0 el axioma de comprensión aritmética y el axioma de inducción por los esquemas siguientes:

Axioma de Comprensión Recursiva Para cada fórmula $\phi(v) \equiv \phi(v, x_1, \ldots, x_n, Y_1, \ldots, Y_m)$ de tipo Σ^0_1 y cada fórmula $\psi(v) \equiv \psi(v, x_1, \ldots, x_n, Y_1, \ldots, Y_m)$ de tipo Π^0_1, la fórmula siguiente es un axioma:

$$\bigwedge x_1 \cdots x_n \bigwedge Y_1 \cdots Y_m (\bigwedge v(\phi(v) \leftrightarrow \psi(v)) \to \bigvee U \bigwedge v(v \in U \leftrightarrow \phi(v))).$$

$\boldsymbol{\Sigma^1_1}$-inducción Para cada fórmula $\phi(v) \equiv \phi(v, x_1, \ldots, x_n, Y_1, \ldots, Y_m)$ de tipo Σ^0_1, la fórmula siguiente es un axioma:

$$\bigwedge x_1 \cdots x_n \bigwedge Y_1 \cdots Y_m (\phi(0) \wedge \bigwedge v(\phi(v) \to \phi(Sv)) \to \bigwedge v\, \phi(v)).$$

Así, en ACR_0, para justificar la existencia de un conjunto de la forma

$$\{v \mid \phi(v, x_1, \ldots, x_n, Y_1, \ldots, Y_m\}$$

es necesario demostrar que, fijados unos valores para los parámetros, la fórmula ϕ equivale a una fórmula de tipo Σ^0_1 y también a una fórmula de tipo Π^0_1. Este cambio hace que el principio de inducción (tal y como lo hemos formulado para ACA_0) sólo permita justificar la inducción respecto a fórmulas ϕ que cumplan esto mismo, pero lo extendemos ligeramente para aceptar cualquier fórmula de tipo Σ^0_1 (sin necesidad de que sea equivalente a otra de tipo Π^0_1) y esto permite probar que también es válido para fórmulas de tipo Π^0_1.

Como sucede con $\mathrm{I}\Sigma_1$, estas modificaciones pueden parecer arbitrarias, pero están justificadas por el teorema siguiente, demostrable en ARP, es decir, por medios constructivos, mediante técnicas (no triviales) de la teoría de la demostración que no involucran modelos:

Teorema 4.16 *Los teoremas de primer orden demostrables en* ACR_0 *son exactamente los mismos que los demostrables en* $\mathrm{I}\Sigma_1$.

En particular, según la observación tras el teorema 4.8, una sentencia expresable en el lenguaje de ARP es demostrable en ARP si y sólo si lo es en ACR_0.

Así pues, la teoría ACR_0 nos permite hablar formalmente de conjuntos de números naturales con la garantía de que cualquier teorema que tenga un sentido finitista admitirá una demostración constructiva.

Si no le hacemos ascos a la teoría de modelos, tanto intuitivamente como en ZF, podemos demostrar lo siguiente:

Teorema 4.17 *Un modelo de* ACR_0 *es el que tiene como parte de primer orden el modelo natural de la Aritmética de Peano y como parte de segundo orden los conjuntos recursivos de números naturales.*

De hecho, éste es el menor modelo de ACR_0, en el sentido de que está contenido en cualquier otro, del mismo modo que el modelo que se obtiene al tomar como parte de segundo orden a los conjuntos aritméticos es el menor modelo de ACA_0.

En particular —como debe ser— en ACR_0 no se puede demostrar la existencia de ningún conjunto que no sea recursivo.

El axioma de comprensión recursiva puede parecer complicado (está motivado por el hecho de que los conjuntos recursivos pueden caracterizarse como los conjuntos aritméticos de tipo Δ^0_1, es decir, definibles simultáneamente por fórmulas Σ^0_1 y Π^0_1), pero no podemos extenderlo sin salirnos de ACR_0, como muestra el teorema siguiente:

Teorema 4.18 *Si a* ACR_0 *le añadimos el principio de comprensión para fórmulas de tipo* Σ^0_1*, entonces podemos demostrar todos los axiomas de* ACA_0*.*

La teoría ACR_0 es la primera (la más débil) de "las cinco grandes" teorías de la matemática inversa (véase el final de la introducción de este capítulo), mientras que ACA_0 es la tercera. Observemos que hemos encontrado una cadena de extensiones:

$$\mathrm{ARP}_\mathrm{G} \quimplies \mathrm{ARP} \quimplies \mathrm{I}\Sigma_1 \quimplies \mathrm{ACR}_0,$$

donde ARP_G representa la formulación de Goodstein de la Aritmética Recursiva Primitiva (sin lógica), de modo que si alguien acepta la validez intuitiva de los modestos axiomas y reglas de inferencia de ARP_G, tiene que aceptar las teorías sucesivas, al menos como formas válidas de demostrar teoremas de ARP_G, lo cual incluye la demostración de que es legítimo usar la lógica clásica para demostrar teoremas de ARP_G.

Las matemáticas formalizables en ACR_0 se corresponden "más o menos" a las matemáticas constructivas de Bishop. Por ejemplo, Bishop no aceptaba la lógica clásica, mientras que en ACR_0 trabajamos con ella (pero hemos justificado su uso). En cambio, Bishop aceptaba el principio de inducción para fórmulas arbitrarias, mientras que en ACR_0 sólo lo suponemos para fórmulas Σ^0_1.

Matemáticas en $\mathbf{ACR}_0$ Ahora necesitamos hacernos una idea de qué clase de conceptos y de resultados es posible formalizar en ACR_0. Empecemos con algunos hechos sencillos:

1. El axioma de comprensión recursiva es aplicable a fórmulas sin cuantificadores (que son a la vez Σ^0_1 y Π^0_1), como $x = x$ o $x \neq x$, lo que nos da los conjuntos:

$$\mathbb{N} \equiv \{x \mid x = x\}, \qquad \varnothing \equiv \{x \mid x \neq x\}.$$

2. Las fórmulas pueden tener parámetros de segundo orden, como $x \in A \vee x \in B$, lo que nos permite definir

$$A \cup B \equiv \{x \mid x \in A \vee x \in B\}, \quad A \cap B \equiv \{x \mid x \in A \wedge x \in B\}, \quad \bar{A} = \{x \mid x \notin A\},$$

$$\{x_1, \ldots, x_n\} \equiv \{x \mid x = x_1 \vee \cdots \vee x = x_n\},$$

   y podemos demostrar obviamente las propiedades básicas del álgebra conjuntista. También podemos definir, naturalmente, $A \subset B \equiv \bigwedge x(x \in A \to x \in B)$.

3. Hay muchas formas recursivas de identificar un par de números naturales con un número natural. Por ejemplo, aunque no es la más elegante, podemos convenir en que $(x, y) = 2^x \cdot 3^y$, y esto es definible en ARP (porque la función $f(x, y) = 2^x \cdot 3^y$ es recursiva primitiva), luego también es definible en $\mathrm{I}\Sigma_1$ a través de una fórmula Δ_1, luego en ACR_0 a través de una fórmula Δ^0_1. Esto nos permite definir

$$A \times B \equiv \{(x, y) \mid x \in A \wedge y \in B\} \equiv \{z \mid \bigvee x \leq z \bigvee y \leq z\, z = (x, y)\},$$

   donde las cotas $x \leq z$, $y \leq z$ permiten probar que la fórmula es Δ^0_1 y, por lo tanto, que la aplicación del axioma de comprensión es legítima.

   Más en general, pueden definirse productos cartesianos $A_1 \times \cdots \times A_n$.

4. A su vez, esto permite definir funciones $F : A \longrightarrow B$ o relaciones $R \subset A \times A$, etc., con todos los conceptos conjuntistas relacionados, incuyendo el de composición de funciones. Más aún, podemos definir funciones por recursión y por minimización, en virtud de los dos teoremas siguientes:

5. **(Recursión)** *Si* $G : X \longrightarrow Y$ *y* $H : X \times \mathbb{N} \times Y \longrightarrow Y$*, existe una única función* $F : X \times \mathbb{N} \longrightarrow Y$ *tal que*

$$\bigwedge u \in X\ F(u,0) = G(u), \qquad \bigwedge u \in X \bigwedge n \in \mathbb{N}\ F(u,n+1) = H(u,n,F(n)).$$

6. **(Minimización)** *Sea* $G : X \times \mathbb{N} \longrightarrow \mathbb{N}$ *una función tal que*

$$\bigwedge u \in X \bigvee v\, G(u,v) = 0.$$

Entonces existe una única función $F : X \longrightarrow \mathbb{N}$ *tal que* $F(x)$ *es el mínimo número natural* n *que cumple* $G(x,n) = 0$*.*

7. Teniendo en cuenta la definición de las funciones recursivas que hemos discutido en la sección 46 del capítulo I (página 94), de aquí se sigue que en ACR_0 podemos definir todas las funciones recursivas.[12]

8. Puesto que no hemos dado los detalles técnicos sobre la teoría de la recursión, para distinguir las funciones recursivas podemos usar la tesis de Church-Turing: cualquier función que sepamos cómo calcular en la práctica es recursiva. Por ejemplo, la función que enumera los números primos es recursiva,[13] por lo que en ACR_0 podemos definir la función $p : \mathbb{N} \longrightarrow \mathbb{N}$ tal que p_i es el primo $i+1$-ésimo.

   También es recursiva (primitiva) la función $e : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ tal que $e_i(n)$ es el exponente de p_i en la descomposición en primos de n, etc. Podemos definir una *sucesión finita* como un número natural $s > 0$ con la propiedad de que si $s > 1$ y n es el mayor número natural tal que $e_n(s) > 0$, entonces, todo $i < n$ cumple $e_i(s) > 0$, es decir, los números naturales de la forma $s = p_0^{e_0} \cdots p_n^{e_n}$ con $e_i > 0$ para todo i (más el 1). En tal caso, llamamos $\ell(s) = n+1$, con el convenio de que $\ell(1) = 0$ y, para $i < \ell(s)$, llamamos $s_i = e_i(s) - 1$. Es claro que siempre podemos determinar si un número natural s cumple o no estas condiciones, luego podemos definir la función $F : \mathbb{N} \longrightarrow \mathbb{N}$ que vale 1 sobre las sucesiones finitas y 0 en el resto de números naturales, y a su vez podemos definir el conjunto $\mathbb{S} = \{n \mid F(n) = 1\}$ de todas las sucesiones finitas. Así, cada sucesión finita de números naturales $n_0, \ldots, n_{l-1}$ se identifica con

$$s = (n_0, \ldots, n_{l-1}) = p_0^{n_0+1} \cdots p_{l-1}^{n_{l-1}+1} \in \mathbb{S}.$$

   Por ejemplo, $(3,0,2) = 2^4 \cdot 3 \cdot 5^3 \in \mathbb{S}$. Sumamos 1 a los exponentes para que no se confunda $(3,0,2)$ con $(3,0,2,0)$, por ejemplo. La sucesión $s = 1$, de longitud 0, representa la sucesión vacía.

   También podemos definir en ACR_0 todos los conceptos básicos relacionados con sucesiones finitas. Por ejemplo, si $s \in \mathbb{S}$, $\ell(s) = n$ y $m \leq n$, podemos definir $s|_m$ como la sucesión que consta de los primeros m términos de s (hasta s_{m-1}). También podemos definir la concatenación de dos o más sucesiones, etc.

   Utilizando estas sucesiones podemos formular un teorema de recursión más fuerte:

9. **(Recursión completa)** *Dada una función* $G : X \times \mathbb{N} \times \mathbb{N} \longrightarrow Y$*, existe una única función* $F : X \times \mathbb{N} \longrightarrow Y$ *que cumple:*

$$\bigwedge x \in X \bigwedge n \in \mathbb{N}\, F(x,n) = G(x,n,F|_n(x)),$$

   donde $F|_n(x) = (F(x,0), \ldots, F(x,n-1)) \in \mathbb{S}$*.*

   Esto significa que podemos definir $F(x,n)$ supuesto que ya están definidos $F(x,0), \ldots, F(x,n-1)$.

La formalización de la lógica en $\mathbf{ACR}_0$ Ahora es fácil formalizar en ACR_0 la definición general de lenguaje formal de primer orden. Hay muchas formas equivalentes de hacerlo, y en la práctica es irrelevante emplear una u otra. Por ejemplo, podemos definir un lenguaje formal $\mathcal{L}$ como una aplicación $\mathcal{L} : S \longrightarrow \mathbb{N}$, cuyo dominio S recibe el nombre de conjunto de *signos* de $\mathcal{L}$, de modo que se cumplan las propiedades siguientes:

1. Existen unos únicos signos cuyas imágenes son los números del 0 al 6, a los que llamaremos respectivamente, $\neg, \to, \wedge, \vee, \leftrightarrow, \bigwedge, \bigvee$ (es decir, $\neg$ es el único signo que cumple $\mathcal{L}(\neg) = 0$, etc.)

2. Existen infinitos signos cuya imagen es 7, a los cuales llamaremos *variables* de $\mathcal{L}$.

[12] En realidad, todas las funciones demostrablemente recursivas, es decir, aquellas para las que la condición $\bigwedge u \in X \bigvee v\, G(u,v) = 0$ sea demostrable en ACR_0. Esto incluye a todas las funciones recursivas primitivas, en las que no hay nada que demostrar. De hecho, no es trivial, pero las únicas funciones demostrablemente recursivas en ACR_0 son las recursivas primitivas.

[13] De hecho, es recursiva primitiva, pues no necesitamos bucles de tipo WHILE para calcularla, sino que siempre podemos acotar de antemano el número de iteraciones de un bucle.

3. Los signos cuya imagen es 8 (si los hay) se llaman *constantes.*

4. Los signos cuya imagen es de la forma 2^n, con $n \geq 4$, se llaman *relatores* $n-3$*-ádicos.* Siempre existe un signo tal que $\mathcal{L}(s) = 2^5$, es decir, un relator diádico, y al menor de todos ellos lo llamamos igualador (=).

5. Los signos cuya imagen es de la forma 3^n, con $n \geq 2$, (si los hay) se llaman *funtores* $n-1$*-ádicos.*

A partir de aquí es pura rutina definir los conjuntos $\mathrm{Term}(\mathcal{L}) \subset \mathbb{S}$ y $\mathrm{Form}(\mathcal{L}) \subset \mathbb{S}$ formados por los términos y las fórmulas de $\mathcal{L}$, así como todos los conceptos lógicos relacionados (como lo que es una variable libre o ligada en una fórmula, etc.).

También podemos definir la relación $\Gamma \overset{d}{\vdash} \alpha$, que se da cuando $d \in \mathbb{S}$ es una deducción de $\alpha \in \mathrm{Form}(\mathcal{L})$ a partir de las premisas de $\Gamma \subset \mathrm{Form}(\mathcal{L})$.

La fórmula $\Gamma \overset{d}{\vdash} \alpha$ es Δ_1^0 (y puede usarse para definir conjuntos, pero $\Gamma \vdash \alpha \equiv \bigvee d\, \Gamma \overset{d}{\vdash} \alpha$ sólo es Σ_1^0, y por lo tanto en ACR_0 no podemos definir el conjunto de todas las consecuencias lógicas de un conjunto de fórmulas Γ, lo cual es lo que cabía esperar, pues dicho conjunto no tiene por qué ser recursivo.

Modelos en $\mathbf{ACR}_0$ Todo lo que hemos hecho en el apartado precedente se puede hacer también en $\mathrm{I}\Sigma_1$ usando fórmulas en lugar de conjuntos. Lo que aporta ACR_0 es que permite formalizar el concepto general de modelo de un lenguaje formal.

Para ello observamos primero que todo conjunto A determina una sucesión de conjuntos A_i dados por

$$A_i = \{n \mid (i,n) \in A\}.$$

Cualquier sucesión finita de conjuntos $A_0, A_1, \ldots, A_n$ puede expresarse en términos de un único conjunto A sin más que tomar

$$A = (A_0, A_1, \ldots, A_n) \equiv (\{0\} \times A_0) \cup (\{1\} \times A_1) \cup \cdots \cup (\{n\} \times A_n).$$

Definición 4.19 Un *premodelo* de un lenguaje formal $\mathcal{L}$ es un conjunto $\mathcal{M}$ que cumpla las condiciones siguientes:

1. $M = \mathcal{M}_0$ es un conjunto no vacío, al que se llama *universo* del premodelo.

2. $I^M = \mathcal{M}_1$ es un conjunto que cumple las condiciones siguientes:

   (a) Si c es una constante de $\mathcal{L}$, entonces $I_c^M = \{a\}$, para cierto $a \in M$ que representaremos por $M(a)$, y lo llamaremos *objeto denotado* por la constante c en M.

   (b) Si r es un relator n-ádico de $\mathcal{L}$, entonces $I_r^M \subset M^n$ es una relación n-ádica en M, que representaremos por $M(r)$, con la condición de que $M(=) = \{(a,a) \mid a \in M\}$.

   (c) Si f es un funtor n-ádico de $\mathcal{L}$, entonces $I_f^M : M^n \longrightarrow M$ es una función n-ádica, que representaremos por $M(f)$.

   Si θ es una expresión de $\mathcal{L}$ (un término o una fórmula), una *valoración* de θ en M es una sucesión $v \in \mathbb{S}$ tal que, si x es una variable (libre o ligada) de θ, entonces $v_x \in M$.

   El teorema de recursión completa nos permite definir, para cada término t de $\mathcal{L}$ y cada valoración v de t, el *objeto denotado* por t en M, que representaremos por $M(t)[v]$, de modo que se cumplan las condiciones siguientes:

   (a) Si x es una variable de $\mathcal{L}$, entonces $M(x)[v] = v_x$.

   (b) Si c es una constante de $\mathcal{L}$, entonces $M(c)[v] = M(c)$.

   (c) Si f es un funtor n-ádico de $\mathcal{L}$ y $t_1, \ldots, t_n$ son términos de $\mathcal{L}$, entonces

   $$M(ft_1 \cdots t_n)[v] = M(f)(M(t_1)[v], \ldots, M(t_n)[v]).$$

   En efecto, estas condiciones determinan cómo hay que definir $M(t)[v]$ supuesto que $M(t')[v]$ está definido para todo $t' < t$ (donde la definición es cualquier valor arbitrario prefijado en M si t' no es un término o si v no es una valoración de t'), por lo que el teorema de recursión completa es aplicable.

Llamaremos P_M al conjunto de todos los pares (θ, v) tales que θ es un término o una fórmula de $\mathcal{L}$ y $v \in \mathbb{S}$ cumple que si x es una variable libre o ligada de θ, entonces $x \leq \ell(s)$ y $v_x \in M$ (y diremos que v es una valoración de θ en M). Diremos que $\mathcal{M}$ es un *modelo* de $\mathcal{L}$ si además

4. $\mathcal{M}_4 : P_M \longrightarrow \{0,1\}$ es una aplicación tal que, si escribimos $M \vDash \alpha[v]$ para indicar que $\mathcal{M}_4(t,v) = 1$ (y en tal caso decimos que M *satisface* la fórmula α respecto de la valoración v), se cumplen las propiedades siguientes:[14]

   (d) Si R es un relator n-ádico de $\mathcal{L}$ y $t_1, \ldots, t_n$ son términos de $\mathcal{L}$, entonces

   $$M \vDash Rt_1 \cdots t_n[v] \quad \text{si y sólo si} \quad M(R)(M(t_1)[v], \ldots, M(t_n)[v]).$$

   (e) Si α y β son fórmulas de $\mathcal{L}$, entonces

   i. $M \vDash \neg\alpha[v]$ si y sólo si no $M \vDash \alpha[v]$.
   ii. $M \vDash (\alpha \to \beta)[v]$ si y sólo si no $M \vDash \alpha[v]$ o $M \vDash \beta[v]$.
   iii. $M \vDash (\alpha \vee \beta)[v]$ si y sólo si $M \vDash \alpha[v]$ o $M \vDash \beta[v]$.
   iv. $M \vDash (\alpha \wedge \beta)[v]$ si y sólo si $M \vDash \alpha[v]$ y $M \vDash \beta[v]$.
   v. $M \vDash (\alpha \leftrightarrow \beta)[v]$ si y sólo si $M \vDash \alpha[v]$ y $M \vDash \beta[v]$ o bien no $M \vDash \alpha[v]$ y no $M \vDash \beta[v]$.

   (f) Si x es una variable y α es una fórmula, entonces

   i. $M \vDash \bigwedge x\, \alpha[v]$ si y sólo si para todo $a \in M$, se cumple $M \vDash \alpha[v^a_x]$, donde v^a_x se diferencia de v únicamente en que $v_x = a$.
   ii. $M \vDash \bigvee x\, \alpha[v]$ si y sólo si existe un $a \in M$ tal que $M \vDash \alpha[v^a_x]$.

En la práctica no distinguiremos en cuanto a notación un modelo $\mathcal{M}$ de su universo M. Si M es un modelo de $\mathcal{L}$, diremos que una fórmula α de $\mathcal{L}$ es *verdadera* en M si se cumple $M \vDash \alpha[v]$ para toda valoración v de α.

Vemos así que la definición que hemos dado de "premodelo" es la definición usual de "modelo", mientras que en la definición de "modelo" hemos añadido como condición que esté definida las relación de satisfacción $M \vDash \alpha[v]$. La razón es que en ACR_0 no es posible demostrar que todo premodelo es un modelo, es decir, que, dado un premodelo M, no es posible formalizar la definición de "verdad" de Tarski o, más precisamente, la relación de satisfacción $M \vDash \alpha[v]$ de una fórmula α respecto de una valoración v. Y es razonable que así sea, porque ACR_0 sólo permite formalizar definiciones constructivas, pero la definición de $M \vDash \alpha[v]$ no lo es, ya que no nos da un criterio para comprobar si $M \vDash \alpha[v]$ se cumple o no. Por ello, si la definición de "verdad" de Tarski pudiera formalizarse en ACR_0 significaría que esta teoría no sería lo que pretendíamos que fuera.

En otras palabras, que todo premodelo determina un único modelo es un hecho intuitivamente verdadero, pero no es formalizable en ACR_0, porque ello requeriría definir en ACR_0 una relación no recursiva $M \vDash \alpha$ sobre el conjunto de las fórmulas de $\mathcal{L}$. Esto significa que será necesaria una teoría más fuerte para formalizarlo.

En cambio, sí que podemos formalizar en ACR_0 la demostración del teorema de corrección del cálculo deductivo:

Teorema 4.20 (de corrección) *Si Γ es un conjunto de fórmulas de un lenguaje formal y α es otra fórmula tal que $\Gamma \vdash \alpha$, entonces, si $M \vDash \Gamma$ (es decir, si M es un modelo del lenguaje formal en el que las fórmulas de Γ son verdaderas), también $M \vDash \alpha$.*

El teorema de corrección es el teorema más elemental que es necesario demostrar al menos una vez en una metamatemática intuitiva para justificar que la definición técnica de deducción formal no es arbitraria, sino que cumple el requisito fundamental de que sólo extrae consecuencias verdaderas de premisas verdaderas. De este modo, cada vez que tenemos una teoría axiomática cuyos axiomas pueden ser considerados verdaderos en una interpretación adecuada, tenemos la garantía de que todos sus teoremas serán también verdaderos y podemos usar teorías formales con axiomas intuitivamente verdaderos para demostrar formalmente hechos intuitivamente verdaderos.

Pero la demostración del teorema de corrección usa modelos, es decir, conjuntos, relaciones, funciones, etc., por lo que es legítimo plantearse qué porción de la teoría de conjuntos abstracta podemos manejar intuitivamente, o qué supuestos sobre conjuntos, relaciones, funciones, etc. necesita la demostración del teorema de corrección.

[14] Compárese con la página 221.

El teorema anterior muestra que, para demostrarlo, no es necesaria una teoría de conjuntos como ZF, cuyos presupuestos exceden con creces el alcance de nuestra intuición, sino que basta la modesta ACR_0, cuya parte de primer orden es $\mathrm{I}\Sigma_1$, una extensión conservativa de la Aritmética Recursiva Primitiva (de modo que su consistencia está garantizada por la de ARP), y cuya parte de segundo orden sólo afirma (aparte del axioma de extensionalidad, que es un mero convenio trivial) la existencia de los conjuntos definibles mediante fórmulas Δ^0_1, lo que garantiza que son recursivos,[15] es decir, sólo estamos suponiendo que si tenemos una propiedad que un número natural puede poseer o no, de modo que disponemos de un procedimiento finito para comprobar si se da o no el caso, podemos considerar al conjunto C formado por todos los números naturales que tienen dicha propiedad como un conjunto bien definido intuitivamente.

Observemos que una consecuencia inmediata del teorema de corrección es que si un conjunto de fórmulas tiene un modelo, entonces es consistente. Por otra parte, es fácil construir en ACR_0 el premodelo $\mathcal{N}$ del lenguaje de la aritmética que tiene por universo a $\mathbb{N}$, en el que la constante 0 se interpreta como el 0 y en el que los funtores $S, +, \cdot$ tienen su interpretación natural. Si pudiéamos probar que este premodelo $\mathcal{N}$ determina un modelo, sería fácil probar que sería un modelo de los axiomas de AP, luego podríamos demostrar $\mathrm{Consis}(\ulcorner \mathrm{AP} \urcorner)$ en ACR_0, pero en ARP (luego en ACR_0) se puede demostrar que

$$\mathrm{Consis}(\ulcorner \mathrm{AP} \urcorner) \leftrightarrow \mathrm{Consis}(\ulcorner \mathrm{ACA}_0 \urcorner) \to \mathrm{Consis}(\ulcorner \mathrm{ACR}_0 \urcorner),$$

(pues estos resultados pueden demostrarse con técnicas de la teoría de la demostración, totalmente finitistas), luego podríamos demostrar $\mathrm{Consis}(\ulcorner \mathrm{ACR}_0 \urcorner)$ en ACR_0, en contra del segundo teorema de incompletitud. Tenemos así otro motivo de peso por el que no es posible demostrar en ACR_0 que todo premodelo determina un modelo. Queda pendiente, pues, encontrar la teoría adecuada para formalizar este hecho, pero antes de ocuparnos de esta cuestión vamos a abordar la formalización del teorema de completitud semántica. Puesto que su demostración no es constructiva, no podemos aspirar a demostrarlo en ACR_0. Sin embargo, sí que es demostrable en ACA_0, pero vamos a ver que, de hecho, es demostrable en una teoría intermedia (la segunda de "las cinco grandes").

4.5 El lema de Kőnig débil

Recordemos el enunciado del teorema de completitud de Gödel:

Teorema 4.21 (Teorema de completitud semántica de Gödel) *Si Γ es un conjunto de fórmulas de un lenguaje formal $\mathcal{L}$ y α es una fórmula de $\mathcal{L}$ que es verdadera en todos los modelos de Γ, entonces $\Gamma \vdash \alpha$.*

En la página 83 vimos que este teorema se demuestra fácilmente a partir del resultado siguiente, al que a menudo se le llama también teorema de completitud de Gödel:

Teorema 4.22 *Si una colección de fórmulas de un lenguaje formal es consistente, entonces tiene un modelo.*

La demostración de que 4.22 implica 4.21 es completamente elemental y, en particular, es formalizable en ACR_0. Por otro lado, en la sección 73 del capítulo I (página 167) discutimos la demostración de Henkin del teorema 4.22. Recordemos que si Γ es un conjunto de sentencias de un lenguaje formal $\mathcal{L}$, se dice que es *maximalmente consistente* si es consistente, pero al añadirle cualquier sentencia que no esté ya en Γ se vuelve contradictorio. Sucede que toda la demostración de Henkin de 4.22 es formalizable en ACR_0 excepto un hecho que se emplea en ella:

Teorema 4.23 (Lema de Lindenbaum) *Todo conjunto consistente de sentencias de un lenguaje formal puede extenderse a un conjunto maximalmente consistente.*

Dicho de otro modo, en ACR_0 se puede demostrar que 4.23 implica 4.22 y, por consiguiente, 4.21.

[15] SI un conjunto puede definirse tanto por una fórmula Σ^0_1, como $\bigvee x\, \alpha(x, n)$ como por una fórmula Π^0_1, como $\bigwedge x\, \beta(x, n)$, donde $\alpha(x)$ y $\beta(x)$ son fórmulas de tipo Δ^0_0, el hecho de que éstas tengan cuantificadores acotados hace que siempre se pueda comprobar mediante una cantidad finita de cálculos si se cumple o no $\alpha(x, n)$ o $\beta(x, n)$, para cualquier par de números x, n. Por lo tanto, para comprobar si un número n está o no en el conjunto, sólo hay que ir calculando $\alpha(0, n), \beta(0, n), \alpha(1, n), \beta(1, n), \ldots$, y tarde o temprano encontraremos un x tal que $\alpha(x, n)$ (si es que n está en el conjunto) o bien un x tal que $\neg\beta(x, n)$ (si es que x no está en el conjunto), y así sabremos cuál es el caso.

En efecto, la demostración discutida en la sección 73 del capítulo I consiste en partir de un conjunto consistente Γ de sentencias de un lenguaje $\mathcal{L}$ (allí consideramos, por simplicidad, el lenguaje de la teoría de conjuntos, pero todo el argumento vale en general) y considerar un lenguaje $\mathcal{L}'$ que contenga una sucesión infinita $\{c_n\}_{n=0}^{\infty}$ de nuevas constantes y extender Γ hasta un conjunto Γ_∞ maximalmente consistente y ejemplificado de sentencias de $\mathcal{L}'$, donde "ejemplificado" significa que si una sentencia $\bigvee x\,\beta(x)$ está en Γ_∞, existe una constante c de $\mathcal{L}'$ tal que $\beta(c)$ está en Γ_∞.

La ejemplificación no es ningún problema en ACR_0. Basta considerar una enumeración $\{\alpha_n\}_{k=0}^{\infty}$ de todas las fórmulas de $\mathcal{L}'$ que tienen una única variable libre y, para cada k, considerar el mínimo n tal que la constante c_n no aparece en ninguna de las fórmulas $\alpha_0, \ldots, \alpha_k$, para definir

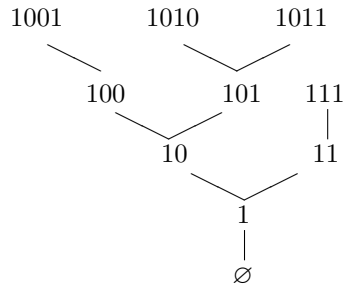
$$\eta_k = \bigvee u\,\alpha_k(u) \to \alpha_k(c_n).$$

Se demuestra que si Γ^+ es el conjunto que resulta de añadir a Γ las sentencias η_k, entonces Γ^+ es consistente, y es fácil ver que cualquier extensión maximalmente consistente de Γ^+ estará ejemplificada.

Admitiendo el lema de Lindenbaum obtenemos el conjunto ejemplificado y máximamente consistente Γ_∞, y el resto de la prueba descrita en la sección 73 es formalizable sin cambios esenciales en ACR_0, y nos da el modelo deseado.

Sin embargo, el lema de Lindenbaum no es demostrable en ACR_0, cosa que no debería sorprendernos, porque, salvo en casos muy simples, no es posible definir un modelo de una teoría axiomática consistente de forma constructiva. Sucede que el lema de Lindenbaum sí que es demostrable en ACA_0, pero vamos a ver que también puede probarse en una teoría intermedia mucho más próxima a ACR_0 que a ACA_0. Para presentarla necesitamos algunas definiciones (siempre trabajando en ACR_0):

Definición 4.24 Un *árbol* es un conjunto de sucesiones finitas $A \subset \mathbb{S}$ con la propiedad de que si $s \in A$ y $n \le \ell(s)$, entonces $s|_n \in A$.



A los elementos de un árbol los llamaremos *nodos.* Se llama *altura* de un nodo a su longitud. En un árbol A consideramos la relación de orden parcial dada por $s \preceq t$ si $\ell(s) \le \ell(t)$ y $s = t|_{\ell(s)}$, es decir, una sucesión es posterior a otra si es una prolongación suya.

Un árbol es *finitamente ramificado* si cada nodo tiene un número finito de sucesores inmediatos, es decir, si cada nodo de altura n tiene un número finito de nodos posteriores de altura $n+1$.

El *árbol binario completo* es el conjunto $\mathbb{S}_2 \subset \mathbb{S}$ formado por todas las sucesiones que toman únicamente los valores 0 y 1. Un árbol binario es un árbol $A \subset \mathbb{S}_2$. Claramente todo árbol binario es finitamente ramificado. La figura muestra un ejemplo de árbol binario.

Un *camino* en un árbol A es una función $F : \mathbb{N} \longrightarrow A$ tal que, para cada número natural n, se cumple que $F(n)$ tiene altura n y si $m \le n$, entonces $F(m) \preceq F(n)$.

El teorema siguiente es un ejemplo típico de teorema de las *matemáticas inversas:*

Teorema 4.25 (ACR_0) *Las afirmaciones siguientes son equivalentes:*

1. *El Axioma de Comprensión Aritmética.*
2. **El lema de Kőnig** *Todo árbol infinito finitamente ramificado tiene un camino.*
3. *Todo árbol infinito en el que cada nodo tiene a lo sumo dos sucesores inmediatos tiene un camino.*

La prueba de que $1 \Rightarrow 2$ es la que vimos en la sección 37 del capítulo I (página 77), que necesita el Axioma de Comprensión Aritmética para ser formalizada, porque, dado un árbol A finitamente ramificado, requiere definir el conjunto

$$A^* = \{s \mid s \in A \wedge \bigwedge m \bigvee t(m \le t \wedge t \in A \wedge s \preceq t)\},$$

es decir, el conjunto de los nodos de A que tienen por encima infinitos nodos. La fórmula que define A^* es de tipo Π^0_2, pero no es[16] Δ^0_1. El hecho de que A sea finitamente ramificado implica que la sucesión vacía está en A^*, así como que si $s \in A^*$, entonces existe un n tal que la prolongación de s con n está en A^*. Admitiendo la existencia de A^*, en ACR_0 es posible definir la función $H : \mathbb{N} \longrightarrow \mathbb{N}$ tal que si $s \in A^*$, entonces $H(s)$ es la prolongación de s con el mínimo natural que hace que $H(s) \in A^*$, la cual a su vez permite definir, por recurrencia, un camino $F : \mathbb{N} \longrightarrow A$.

Así pues, el único punto no constructivo de la demostración es la definición de A^*, y no es constructiva porque, aunque sepamos determinar si cualquier sucesión s está o no en A, no nos da un método para determinar si una sucesión dada está o no en A^*, es decir, no tenemos necesariamente un criterio para determinar si un nodo s de A tiene o no infinitos nodos por encima.[17]

La implicación $2 \Rightarrow 3$ es trivial, mientras que $3 \Rightarrow 1$ es bastante técnica, así que no la vamos a discutir aquí, pero, como decíamos, es un ejemplo típico de *matemáticas inversas*. No solamente demostramos el lema de Kőnig, sino que se demuestra que para demostrarlo es imprescindible el Axioma de Comprensión Aritmética. En particular, si alguien considera intuitivamente evidente el lema de Kőnig (o simplemente el caso particular 3 del teorema anterior) y acepta como intuitivamente válidas las demostraciones en ACR_0, entonces tiene que admitir que ACA_0 es una teoría intuitivamente válida.

Sucede que para demostrar el lema de Lindenbaum necesitamos suponer un principio aún más débil que la afirmación 3 del teorema anterior:

Teorema 4.26 ($\mathbf{ACR}_0$) *Las afirmaciones siguientes son equivalentes:*

1. **El lema de Kőnig débil** *Todo árbol binario infinito tiene un camino.*
2. **El lema de Lindenbaum** *Todo conjunto consistente de sentencias puede extenderse a un conjunto maximalmente consistente.*
3. **El teorema de completitud semántica** *Un conjunto de fórmulas de un lenguaje formal es consistente si y sólo si tiene un modelo.*
4. **El teorema de compacidad** *Si Γ es un conjunto de fórmulas de un lenguaje formal tal que todo subconjunto finito tiene un modelo, entonces Γ tiene un modelo.*

Demostración: Veamos que $1 \Rightarrow 2$. Para ello fijamos un conjunto consistente Γ de sentencias de un lenguaje formal $\mathcal{L}$. Definimos A como el conjunto formado por las sucesiones $s \in \mathbb{S}_2$ que cumplen las condiciones siguientes, donde llamamos $[s] = \{n \mid n < \ell(s) \wedge s_n = 1\}$:

1. Si $s_n = 1$, entonces $n \in \mathbb{S}$ es una sentencia de $\mathcal{L}$.
2. Si $n < \ell(s)$ y $n \in \Gamma$, entonces $s_n = 1$.
3. Si $m, n < \ell(s)$ son sentencias y $n = \neg m$, entonces $s_m = 1$ o $s_n = 1$, pero no se dan los dos casos a la vez.
4. Si $n < \ell(s)$ es una sentencia tal que $\Gamma \cup [s] \overset{d}{\vdash} n$, con $d < \ell(s)$, entonces $s_n = 1$.

Se puede comprobar que la definición de A es Δ^0_1, por lo que es correcta en ACR_0. Un hecho clave es que en 4. pedimos que $d < \ell(s)$, lo que hace que la condición $\Gamma \cup [s] \overset{d}{\vdash} n$ sea comprobable en un número finito de pasos, ya que sólo hay una cantidad finita de demostraciones posibles d.

Es obvio que A es un árbol binario, es decir, que si $s \in A$ y $n \leq \ell(s)$, entonces $s|_n \in A$. Además, para cada número natural i, existe un $s \in A$ tal que $\ell(s) = i$ y $\Gamma \cup [s]$ es consistente. Esto se demuestra por inducción sobre i. La parte delicada es que, mediante algunos artificios, la fórmula a la que se aplica el principio de inducción puede tomarse de tipo Σ^0_1, por lo que la inducción es legítima en ACR_0. Prescindiendo de dichos artificios, la idea es muy simple:

[16] Como se sigue del propio teorema, pues si A^* pudiera definirse en ACR_0, entonces en ACR_0 podría demostrarse el Axioma de Comprensión Aritmética, y eso es imposible, porque en ACA_0 se puede demostrar la consistencia de ACR_0.

[17] No es el mismo caso, pero esta analogía puede ayudar a ver el problema: tenemos un algoritmo finito para determinar si un número p forma parte de un par de primos gemelos, pero eso no nos ayuda a saber si por encima de un primo gemelo hay una cantidad finita o infinita de primos gemelos.

Es trivial que la sucesión vacía está en A y cumple lo requerido para $i = 0$. Suponemos ahora que existe una sucesión s de longitud i que cumple lo requerido. Si i no es una sentencia de $\mathcal{L}$, basta extender s a s' con $s'_i = 0$, mientras que si i es una sentencia, definimos $s'_i = 1$ si $\Gamma \cup [s] \cup \{i\}$ es consistente y $s'_i = 0$ en caso contrario. Es fácil ver que s' está en A.

En particular concluimos que el árbol A es infinito, y en este punto podemos aplicar el lema de Kőnig débil para concluir que tiene un camino F. Así, para cada n, tenemos que $F(n) \in A$ tiene altura n. Llamamos Γ_∞ al conjunto de las sentencias α tales que $F(\alpha + 1)_\alpha = 1$. Es claro entonces que Γ_∞ contiene a Γ y es consistente, porque si existieran deducciones d y d' de dos sentencias α y $\neg\alpha$, respectivamente, a partir de Γ_∞, podríamos tomar un n suficientemente grande como para que $d, d' < n$, y entonces $s = F(n) \in A$ contradiría la definición de A, pues por 4. debería ser $s_\alpha = s_{\neg\alpha} = 1$, en contra de 3.

Más aún, Γ_∞ es maximalmente consistente, pues si α es una sentencia que no está en Γ_∞, podemos tomar un n mayor que α y $\neg\alpha$, con lo que $s = F(n) \in A$ cumple que $s_\alpha = 1$ o $s_{\neg\alpha} = 1$ (pero sólo uno de los dos), luego $\alpha \in \Gamma_\infty$ o bien $\neg\alpha \in \Gamma_\infty$. El primer caso se descarta por hipótesis, y el segundo implica que Γ_∞ se vuelve contradictorio al añadirle α.

Ya hemos explicado por qué $2 \Rightarrow 3$, mientras que $3 \Rightarrow 4$ es trivial: Si Γ no tiene un modelo, es que es contradictorio (por 3), luego existe una deducción de una contradicción a partir de premisas de Γ, pero esa deducción empleará sólo una cantidad finita de premisas de Γ, luego existe un subconjunto finito de Γ contradictorio que, por lo tanto, no tiene un modelo.

Omitimos la demostración de $4 \Rightarrow 1$. ∎

En contra de lo que podría parecer, el lema de Kőnig débil no es equivalente al apartado 3 del teorema 4.25. En ACR_0 no puede demostrarse que todo árbol cuyos nodos tengan a lo sumo dos sucesores inmediatos sea isomorfo a un árbol binario. Por el contrario, en este punto tenemos que introducir la definición siguiente:

Definición 4.27 Llamaremos LKD_0 a la teoría axiomática que resulta de añadirle como axioma ACR_0 el lema de Kőnig débil.

Es obvio que el apartado 3 del teorema 4.25 (y, por consiguiente, el Axioma de Comprensión Aritmética) implica el lema de Kőnig débil, luego todo teorema de TKD_0 es un teorema de ACA_0, y es obvio que todo teorema de ACR_0 es un teorema de TKD_0.

El teorema anterior prueba que TKD_0 es la teoría justa en la que pueden demostrarse los teoremas fundamentales de la teoría de modelos que no pueden faltar en un estudio metamatemático de la lógica de primer orden. A las afirmaciones del teorema anterior hay que añadir la forma propiamente dicha del teorema de completitud (el teorema 4.21) y el teorema de Löwenheim-Skolem, que es trivial en nuestro contexto, pues todo modelo construido en cualquiera de las teorías que estamos considerando tiene necesariamente universo numerable. Más aún, en TKD_0 puede demostrarse la existencia de modelos no estándar de cualquier teoría aritmética igual que lo razonamos en la sección 48 del capítulo I (página 100).

Lo más sorprendente de LKD_0 es el teorema siguiente, cuya prueba es formalizable en ARP, pues se basa en técnicas estrictamente finitistas de la teoría de la demostración:

Teorema 4.28 *Los teoremas de primer orden demostrables en* TKD_0 *son exactamente los mismos que los demostrables en* $\mathrm{I}\Sigma_1$.

Así pues, la consistencia de TKD_0 se sigue de la consistencia de la Aritmética Recursiva Primitiva. En TKD_0 es posible demostrar más teoremas de segundo orden que en ACR_0, pero los teoremas de primer orden son los mismos en ambas teorías. Podemos pensar que TKD_0 se corresponde con el "reduccionismo finitista" de Hilbert, es decir, que introduce elementos no finitistas de segundo orden (pues el Teorema de Kőnig Débil es, sin duda, de naturaleza no constructiva), pero con la garantía de que todos sus teoremas de primer orden admiten demostraciones finitistas. Con el paso a ACA_0 ya introducimos teoremas "nuevos" de enunciado finitista, pero que requieren demostraciones no finitistas, como $\mathrm{Consis}(\ulcorner \mathrm{I}\Sigma_1 \urcorner)$.

En conclusión, acabamos de ver que los presupuestos de la metamatemática necesaria para introducir justificadamente la matemática formal son mucho más débiles de lo que se podría imaginar. La parte sintáctica sólo requiere presuponer los débiles axiomas y reglas de inferencia de la Aritmética Recursiva Primitiva en su presentación sin lógica de Goodman, mientras que la parte semántica ni siquiera requiere los postulados de ACA_0, sino que le bastan los de TKD_0, cuya consistencia se reduce también a la de ARP.

Un finitista estricto puede considerar que todas las teorías entre ARP y TKD_0 introducen elementos ideales que pueden usarse con la garantía de que los teoremas de enunciado constructivo admiten demostraciones constructivas, mientras que un predicativista que no tenga nada que objetar a las construcciones predicativas aceptará que los axiomas de ACA_0 y, por consiguiente, los de sus subteorías, tienen una interpretación intuitiva verdadera, con lo que estas teorías permiten demostrar teoremas intuitivamente verdaderos utilizando técnicas formales, mucho más prácticas que el razonamiento intuitivo informal, en cuanto que sólo requieren seguir ciertas reglas de rigor formal para garantizar su corrección.

En cualquier caso, concluimos que, para construir la matemática formal (en particular ZFC) basta construir intuitivamente ARP y, a partir de ahí, ya es posible formalizar toda la metamatemática en ARP con la seguridad de que todos los razonamientos formales en la propia ARP o en sus extensiones sucesivas (hasta TKD_0, que es lo máximo necesario para demostrar los metateoremas fundamentales) dan lugar a teoremas intuitivamente verdaderos.

El único resultado relevante que no hemos conseguido formalizar es que todo premodelo determina un único modelo. Como ya hemos señalado, de ahí se sigue que el premodelo natural de la Aritmética de Peano determina un modelo, el cual demuestra la consistencia de AP. En virtud del segundo teorema de incompletitud, no vamos a poder demostrar tal cosa en ACA_0, pues en tal caso podríamos demostrar la consistencia de ACA_0 en ACA_0 (ya que es equivalente a la de AP). Por lo tanto, para demostrar que todo premodelo determina un modelo necesitamos una teoría más fuerte que ACA_0. Nos ocupamos de ello en la sección siguiente.

4.6 Recursión aritmética

Ya hemos señalado que en ACR_0 no es posible demostrar que todo premodelo de un lenguaje formal determina un modelo y, por la misma razón, tampoco es posible demostrarlo en ACA_0. En efecto, en tal caso podríamos definir el modelo natural $\mathbb{N}$ y demostrar $\mathrm{Consis}(\ulcorner\mathrm{AP}\urcorner)$, que es equivalente a $\mathrm{Consis}(\ulcorner\mathrm{ACA}_0\urcorner)$, y no podemos demostrar tal cosa en ACA_0.

Con la notación de la definición de modelo (página 374), el problema es definir $F : P_M \longrightarrow \{0,1\}$ de modo que, escribiendo $M \vDash \alpha[v]$ para indicar que $F(\alpha, v) = 1$, se cumplan las propiedades (d), (e) y (f).

Y la dificultad consiste, concretamente, en que no podemos aplicar el teorema de recursión completa (página 372) porque dichas condiciones no determinan $F(\theta, v)$ a partir de los valores $F(\alpha, v)$, con $\alpha < \theta$, sino que la condición (f) requiere conocer $F(\alpha, w)$ para un $\alpha < \theta$ y toda valoración w de α en M. En otras palabras, en la definición recursiva del teorema de recursión completa, para definir $F(x, n)$, el parámetro x está fijo y sólo suponemos definidos un número finito de valores de F, a saber, los valores $F(x, 0), \ldots, F(x, n-1)$, mientras que para definir $F(\theta, v)$ necesitamos suponer que F ya está definida para infinitos pares (α, w).

Por lo tanto, si queremos convertir a cada premodelo en un modelo, lo que necesitamos es un teorema de recursión más fuerte que el teorema de recursión completa.

En general, consideremos una fórmula aritmética $\phi(n, Z)$, que puede tener más parámetros de primer y segundo orden, además de las dos variables indicadas. Fijados dichos parámetros, la fórmula ϕ determina una forma de construir un conjunto $\Phi(Z)$ a partir de cualquier conjunto dado Z, a saber, el conjunto

$$\Phi(Z) = \{n \mid \phi(n, Z)\}.$$

Tenemos así una "aplicación" metamatemática que asigna conjuntos a conjuntos, y vamos a tratar de usarla para definir una sucesión de conjuntos $\{Y_i\}_{i=0}^{\infty}$ de forma análoga a como interviene G en el teorema de recursión completa para definir la función F (que puede verse como una sucesión de números naturales $\{F(i)\}_{i=0}^{\infty}$).

Ante todo, técnicamente no podemos hablar de una sucesión de conjuntos $\{Y_i\}_{i=0}^{\infty}$ entendida como una aplicación que a cada i le asigna un conjunto Y_i, pero podemos formalizarla como un conjunto Y tal que $Y_i = \{n \mid (i, n) \in Y\}$. La idea es definir $Y_i = \Phi(Y^i)$, donde

$$Y^i = (\{0\} \times Y_0) \cup \cdots \cup (\{i-1\} \times Y_{i-1}) = \{Y_j\}_{j<i},$$

de modo que la fórmula ϕ es la que determina cómo se construye Y_i en función de los términos precedentes de la sucesión. En particular tenemos que $Y^0 = \varnothing$, que es un conjunto aritmético definido por la fórmula $\bar{\phi}_0(z) \equiv z \neq z$, y el primer término de la sucesión que queremos definir será

$$Y_0 = \{n \mid \phi(n, \varnothing)\},$$

que es un conjunto aritmético. Más explícitamente, si llamamos $\phi_0(n)$ a la fórmula[18] que resulta de sustituir cada subfórmula $i \in Z$ de $\phi(n, Z)$ por $i \neq i$ (la fórmula que define a $Y^0 = \varnothing$) y hacemos

$$\phi^1(z) \equiv \bigvee n(z = (0, n) \wedge \phi_0(n)),$$

tenemos que $\phi^1(z)$ es una fórmula aritmética y en ACA_0 podemos definir

$$Y_0 = \{n \mid \phi_0(n)\}, \qquad Y^1 = Y^0 \cup (\{0\} \times Y_0) = \{z \mid \phi^1(z)\}.$$

A su vez, podemos definir

$$Y_1 = \Phi(Y^1) = \{n \mid \phi(n, Y^1)\}, \qquad Y^2 = Y^1 \cup (\{1\} \times Y_1).$$

Si llamamos $\phi_1(n)$ a la fórmula aritmética que resulta de sustituir en $\phi(n, Z)$ cada subfórmula $z \in Z$ por $\phi^1(z)$ (la fórmula que define a Y^1) y

$$\phi^2(z) \equiv \phi^1(z) \vee \bigvee n(z = (1, n) \wedge \phi_1(n)),$$

tenemos que

$$Y_1 = \{z \mid \phi_1(z)\}, \qquad Y^2 = \{z \mid \phi^2(z)\}.$$

A su vez, podemos definir

$$Y_2 = \Phi(Y^2) = \{n \mid \phi(n, Y^2)\}, \qquad Y^3 = Y^2 \cup (\{2\} \times Y_2).$$

En general, para cada numeral $\ulcorner n \urcorner$, en ACA_0 podemos definir recurrentemente las sucesiones

$$Y^0 = \varnothing, \qquad Y_{\ulcorner n+1 \urcorner} = \Phi(Y^{\ulcorner n \urcorner}), \qquad Y^{\ulcorner n+1 \urcorner} = Y^{\ulcorner n \urcorner} \cup (\{\ulcorner n \urcorner\} \times Y_{\ulcorner n \urcorner})$$

donde ponemos los ángulos de Quine para enfatizar que podemos definir los conjuntos $Y_0, Y_1, Y_2, \ldots$, así como los conjuntos $Y^0, Y^1, Y^2, \ldots$, pero no tenemos expresiones generales Y_n o Y^n, donde n es una variable.[19]

El razonamiento precedente muestra que los conjuntos $Y_{\ulcorner n \urcorner}$, $Y^{\ulcorner n \urcorner}$ son aritméticos, pero cada uno de ellos está definido por una fórmula aritmética diferente, $\phi_0(n), \phi_1(n), \phi_2(n), \ldots$ y $\phi^0(z), \phi^1(z), \phi^2(z), \ldots$, cada una más complicada que la anterior, por lo que, en general, no tenemos una forma de definir en ACA_0 la sucesión

$$Y = \{Y_i\}_{i=0}^{\infty} = \{(i, n) \mid n \in Y_i\}.$$

No obstante, podemos describir Y mediante una fórmula. Para ello definimos $I_i = \{j \mid j < i\}$ y, para cualquier conjunto Z:

$$Z_i = \{n \mid (i, n) \in Z\}, \qquad Z^i = Z \cap (I_i \times \mathbb{N}) = \{z \mid z \in Z \wedge \bigvee jn(j < i \wedge z = (j, n))\},$$

Si llamamos $\phi^*(n, Z, i)$ a la fórmula (aritmética) que resulta de sustituir cada subfórmula $z \in Z$ de $\phi(n, Z)$ por $z \in Z \wedge \bigvee jn(j < i \wedge z = (j, n))$, en ACR_0 podemos probar:

$$\phi^*(n, Z, i) \leftrightarrow \phi(n, Z^i).$$

Así, el conjunto Y que queremos definir está caracterizado por la fórmula

$$Y \subset \mathbb{N} \times \mathbb{N} \wedge \bigwedge i\ Y_i = \Phi(Y^i),$$

que equivale a la fórmula aritmética

$$\mathrm{RA}_\phi(Y) \equiv \bigwedge z(z \in Y \leftrightarrow \bigvee in(z = (i, n) \wedge \phi^*(n, Y, i))).$$

[18] Podemos suponer que la fórmula $\phi(n, Z)$ no contiene subfórmulas de tipo $U = V$, porque siempre pueden sustituirse por $\bigwedge u(u \in U \leftrightarrow u \in V)$ y el resultado es una fórmula lógicamente equivalente.

[19] Una situación análoga es que, en ZF, podemos definir $0 = \varnothing$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}, \ldots$ y así tenemos infinitas definiciones, pero éstas no equivalen a la definición de una fórmula "n es un número natural". Para definir esta fórmula hacen falta ideas nuevas que no están presentes en las infinitas definiciones anteriores. Nosotros tenemos también infinitas definiciones, y nos gustaría tener una idea análoga a la que en ZF permite definir la fórmula "n es un número natural".

El problema es que en ACA_0 no podemos demostrar que exista un conjunto Y que cumpla esta fórmula. Más detalladamente, si definimos

$$\mathrm{RA}^k_\phi(Y) \equiv \bigwedge z(z \in Y \leftrightarrow \bigvee in(z = (i,n) \wedge i < k \wedge \phi^*(n,Y,i))),$$

podemos demostrar que existen conjuntos aritméticos $Y^0, Y^1, Y^2, \ldots$, que cumplen las fórmulas

$$\mathrm{RA}^0_\phi(Y^0), \quad \mathrm{RA}^1_\phi(Y^1), \quad \mathrm{RA}^2_\phi(Y^2), \quad \ldots$$

pero no podemos demostrar que $\bigwedge k \bigvee Y\, \mathrm{RA}^k_\phi(Y)$. Similarmente, las fórmulas

$$\mathrm{RA}_\phi(Z,k) \equiv \bigwedge n(n \in Z \leftrightarrow \bigvee Y(\mathrm{RA}^{k+1}_\phi(Y) \wedge (k,n) \in Y))$$

caracterizan los conjuntos Y_k, es decir, que podemos demostrar que existen conjuntos aritméticos $Y_0, Y_1, Y_2, \ldots$, que cumplen las fórmulas

$$\mathrm{RA}_\phi(Y_0,0), \quad \mathrm{RA}_\phi(Y_1,1), \quad \mathrm{RA}_\phi(Y_2,2), \quad \ldots$$

pero no podemos demostrar que $\bigwedge k \bigvee Y\, \mathrm{RA}_\phi(Y,k)$.

Lo que sí que podemos demostrar es la unicidad de estos hipotéticos conjuntos:

Teorema 4.29 *Para cada fórmula aritmética $\phi(n,Z)$, la fórmula siguiente se demuestra en* ACR_0*:*

$$\bigwedge YY'(\mathrm{RA}_\phi(Y) \wedge \mathrm{RA}_\phi(Y) \to Y = Y').$$

Demostración: Supongamos que se cumple $\mathrm{RA}_\phi(Y)$ y $\mathrm{RA}_\phi(Y')$, pero que $Y \neq Y'$. Entonces existe un $z \in (Y \setminus Y') \cup (Y' \setminus Y)$. En particular, z será de un par $z = (i,n)$. Entonces podemos tomar el mínimo i tal que[20]

$$\bigvee zn(z = \langle i,n\rangle \wedge z \in (Y \setminus Y') \cup (Y' \setminus Y)).$$

Tenemos entonces que existe un n tal que $(i,n) \in (Y \setminus Y') \cup (Y' \setminus Y)$, pero

$$\bigwedge j < i \bigwedge m((j,m) \in Y \leftrightarrow (j,m) \in Y'),$$

es decir, que $Y^i = Y'^i$. No perdemos generalidad si suponemos que $(i,n) \in Y \setminus Y'$. Por la definición de $\mathrm{RA}_\phi(Y)$, tenemos que se cumple $\phi^*(n,Y,i)$, lo cual equivale a $\phi(n,Y^i)$, o también a $\phi(n,Y'^i)$, o también a $\phi^*(n,Y',i)$, pero entonces tendría que ser $(i,n) \in Y'$, y tenemos una contradicción. ∎

Similarmente se demuestra la unicidad de los conjuntos que cumplen $\mathrm{RA}^k_\phi(Y)$ y $\mathrm{RA}_\phi(Y,k)$.

Así pues, fijada una fórmula aritmética $\phi(n,Z)$ (y unos valores para los parámetros que pueda tener), en ACA_0 se demuestra que existe el conjunto $Y_0 = \Phi(\varnothing)$, que es el único que cumple $\mathrm{RA}_\phi(Y_0,0)$, así como el conjunto $Y_1 = \Phi(\{0\} \times Y_0)$, que es el único que cumple $\mathrm{RA}_\phi(Y_1,1)$, así como $Y_2 = \Phi((\{0\} \times Y_0) \cup (\{1\} \times Y_1))$, que es el único conjunto que cumple $\mathrm{RA}_\phi(Y_2,2)$, etc., pero no podemos asegurar la existencia de la sucesión $\{Y_i\}_{i=0}^\infty$ o, equivalentemente, del conjunto Y formado por los pares (i,n), con $n \in Y_i$, que sería el único que cumpliría $\mathrm{RA}_\phi(Y)$, porque Y no es necesariamente aritmético.

Ahora bien, si aceptamos que los axiomas y los teoremas de ACA_0 expresan afirmaciones verdaderas sobre los números naturales, tenemos que admitir que el conjunto Y existe realmente, aunque su existencia no pueda ser demostrada en ACA_0, por lo que es razonable extender la teoría tomándolo como axioma:

Definición 4.30 Llamaremos RA_0 a la teoría axiomática que resulta de añadirle a ACR_0 el esquema axiomático de *Recursión Aritmética*, según el cual, para cada fórmula aritmética $\phi(n,Z)$, tal vez con más variables libres, la fórmula $\bigvee Y\, \mathrm{RA}_\phi(Y)$ es un axioma.

Acabamos de demostrar que el conjunto Y cuya existencia postula el axioma es único, por lo que podemos referirnos a él como *el conjunto definido por recursión aritmética* a partir de la fórmula aritmética ϕ y de los parámetros que haya en ella.

De forma más desarrollada, recordando la notación $\Phi(Z) \equiv \{n \mid \phi(n,Z)\}$, lo que afirma el axioma es que existe una única sucesión $Y = \{Y_i\}_{i=0}^\infty$ tal que $Y_i = \Phi(\{Y_j\}_{j<i})$.

[20] En ACR_0 sólo se puede demostrar la existencia de mínimos para fórmulas Σ^0_1, pero ésta lo es.

Observemos que en la definición partimos de ACR_0, pero en RA_0 se puede demostrar el Axioma de Comprensión Aritmética, por lo que RA_0 extiende a ACA_0.

En efecto, dada cualquier fórmula aritmética $\phi(v, x_1, \ldots, x_r, X_1, \ldots, X_s)$, tomamos una variable Z que no esté en ϕ y aplicamos el axioma de Recursión Aritmética a $\phi(v, Z)$ (si se quiere, se puede cambiar ϕ por $\phi \wedge Z = Z$, pero es irrelevante que Z no esté en ϕ). Entonces,

$$Y_0 = \Phi(\varnothing) = \{v \mid \phi(v, x_1, \ldots, x_r, X_1, \ldots, X_s)\}$$

es el conjunto aritmético definido por ϕ.

Ahora podemos completar la formalización de la teoría de modelos:

Teorema 4.31 ($\mathbf{RA}_0$) *Todo premodelo de un lenguaje formal se extiende a un único modelo.*

Demostración: Según hemos discutido al principio de esta sección, fijado un modelo M de un lenguaje formal $\mathcal{L}$, todo se reduce a definir la aplicación $F : P_M \longrightarrow \{0, 1\}$ tal que, definiendo $M \vDash \alpha[v]$ si y sólo si $F(\alpha, v) = 1$, se cumplan las condiciones (d), (e) y (f) de la definición de modelo. Para ello definiremos una sucesión de conjuntos $\{Y_i\}_{i=0}^{\infty}$ de modo que, para cada fórmula α de $\mathcal{L}$, podamos definir

$$F(v, \alpha) = k \leftrightarrow (v, k) \in Y_\alpha.$$

Es fácil ver que, para que se cumplan las condiciones (d), (e) y (f), basta definir adecuadamente (mediante una fórmula aritmética) Y_α en función de los conjuntos Y_β, con $\beta < \alpha$, que es justo lo que permite el esquema de Recursión Aritmética. ∎

En particular, en RA_0 se puede dotar a $\mathbb{N}$ de modelo de AP, con lo que se puede demostrar $\mathrm{Consis}(\ulcorner \mathrm{AP} \urcorner)$, que a su vez equivale a $\mathrm{Consis}(\ulcorner \mathrm{ACA}_0 \urcorner)$, por lo que RA_0 permite demostrar más teoremas aritméticos que ACA_0.

La consistencia de $\mathbf{RA}_0$ Vamos a dar una demostración intuitiva de la consistencia de RA_0. Sea $\{\Phi_n\}_{n=0}^{\infty}$ una enumeración de todos los pares $\Phi = (\phi, (a_1, \ldots, a_k))$, donde $\phi(x_0, x_1, \ldots, x_k)$ es una fórmula del lenguaje de la aritmética de primer orden con las variables libres indicadas y $a_1, \ldots, a_k$ son números naturales. Cada par Φ define el conjunto aritmético $C_\Phi = \{m \mid \mathbb{N} \vDash \phi[m, a_1, \ldots, a_k]\}$. Llamemos C_n^0 al conjunto definido por Φ_n. Entonces $S_0 = \{C_n^0 \mid n \in \mathbb{N}\}$, es decir, el conjunto de todos los conjuntos aritméticos, es la parte de segundo orden de un modelo M_0 de ACA_0.

Supongamos que hemos construido unos conjuntos $S_r = \{C_n^r \mid n \in \mathbb{N}\}$ que constituyen la parte de segundo orden de un modelo M_r de ACA_0. Sea $\{\Psi_n\}_{n=0}^{\infty}$ una enumeración de las ternas $\Psi = (\psi, (a_1, \ldots, a_k), (A_1, \ldots, A_l))$, donde $\psi(x_0, X_0, x_1, \ldots, x_k, X_1, \ldots, X_l)$ es una fórmula aritmética del lenguaje de la aritmética de segundo orden con las variables libres indicadas, $a_1, \ldots, a_k$ son números naturales y $A_1, \ldots, A_l$ son conjuntos C_n^r. Cada terna Ψ define un único conjunto Y_Ψ definido por recursión aritmética mediante la fórmula ψ con los parámetros $a_1, \ldots, a_k, A_1, \ldots, A_l$. Llamemos Y_n al conjunto definido por Ψ_n y sea S_r^* la unión de S_r y el conjunto de todos los Y_n.

Sea $\{\Phi_n\}_{n=0}^{\infty}$ una enumeración de todas las ternas $\Phi = (\phi, (a_1, \ldots, a_k), (A_1, \ldots, A_l))$, donde

$$\phi(x_0, x_1, \ldots, x_k, X_1, \ldots, X_l)$$

es una fórmula aritmética del lenguaje de la aritmética de segundo orden con las variables libres indicadas, $a_1, \ldots, a_k$ son números naturales y $A_1, \ldots, A_l$ son conjuntos de S_r^*. Cada Φ define un conjunto

$$C_\Phi = \{m \mid (\mathbb{N}, S_r^*) \vDash \phi[m, a_1, \ldots, a_k, A_1, \ldots, A_k]\}.$$

Llamemos C_n^{r+1} al conjunto definido por Φ_n y sea S_{r+1} el conjunto de todos los C_n^{r+1}, que es la parte de segundo orden de un modelo de ACA_0. Además $S_r \subset S_{r+1}$.

Con esto tenemos definida una sucesión $\{S_r\}_{r=0}^{\infty}$ de (partes de segundo orden de) modelos de ACA_0. Llamamos S a la unión de todos los S_r, y entonces $(\mathbb{N}, S)$ es un modelo de RA_0.

En efecto, el axioma de extensionalidad se cumple trivialmente (hemos generado S mediante sucesiones en la que cada conjunto puede aparecer infinitas veces, pero hay que entender que cada conjunto se incluye una única vez, aunque no sea decidible si dos términos de una sucesión son o no el mismo conjunto). El axioma

de comprensión aritmética se cumple también, pues si fijamos una fórmula $\phi(x_0, x_1, \ldots, x_k, X_1, \ldots, X_l)$ y unos parámetros $a_1, \ldots, a_k$ en $\mathbb{N}$ y $A_1, \ldots, A_l$ en S, existirá un r tal que $A_1, \ldots, A_l$ estarán en S_r, luego en S_r^*, luego $\Phi = (\phi, (a_1, \ldots, a_k), (A_1, \ldots, A_l))$ será una de las ternas Φ_n consideradas en la construcción de S_{r+1}, luego S incluye al conjunto

$$C_n^{r+1} = \{m \mid (\mathbb{N}, S_r^*) \vDash \phi[m, a_1, \ldots, a_k, A_1, \ldots, A_k]\} = \{m \mid (\mathbb{N}, S) \vDash \phi[m, a_1, \ldots, a_k, A_1, \ldots, A_k]\},$$

donde la segunda igualdad se debe a que ϕ es aritmética, luego no tiene variables cuantificadas de segundo orden, luego no deja de satisfacerse por que se añadan conjuntos al modelo.

Similarmente se comprueba que $(\mathbb{N}, S)$ satisface el axioma de Recursión Aritmética, pues si fijamos una fórmula aritmética $\psi(x_0, X_0, x_1, \ldots, x_k, X_1, \ldots, X_l)$ y unos parámetros $a_1, \ldots, a_k$ en $\mathbb{N}$ y $A_1, \ldots, A_l$ en S, existirá un r tal que $A_1, \ldots, A_l$ estarán en S_r, luego $\Psi = (\psi, (a_1, \ldots, a_k), (A_1, \ldots, A_l))$ será una de las ternas Ψ_n consideradas en la construcción de S_r^*. Entonces el conjunto Y_n está en S_r^*, luego en S_{r+1}, luego en S y cumple el axioma de Recursión Aritmética para ψ con los parámetros dados en el modelo $(\mathbb{N}, S_r)$, luego también en el modelo $(\mathbb{N}, S)$, porque la fórmula $\mathrm{RA}_\phi(Y)$ es aritmética, luego no deja de satisfacerse si se añaden nuevos conjuntos al modelo.

El axioma de inducción se cumple trivialmente. Así pues, RA_0 tiene un modelo formado por una familia numerable de conjuntos de números naturales que hemos definido explícitamente de forma predicativa. Notemos que todas las enumeraciones que hemos considerado pueden definirse explícitamente. Lo único no constructivo es que no es posible determinar si dos de los conjuntos que hemos definido son iguales o no. ∎

Recursión transfinita La teoría RA_0 no es ninguna de "las cinco grandes", porque las ideas que hemos usado para definirla se pueden explotar aún más. En efecto, dada una fórmula $\phi(n, Z)$ (tal vez con parámetros), hemos visto que define una sucesión $Y = \{Y_i\}_{i=0}^\infty$ de modo que

$$Y_i = \Phi(\{Y_j\}_{j<i}),$$

pero a Y podríamos haberlo llamado Y^ω, a partir del cual podemos definir $Y_\omega = \Phi(Y^\omega)$, que a su vez nos da $Y^{\omega+1} = Y^\omega \cup (\{\omega\} \times Y_\omega)$, a partir del cual podemos definir $Y_{\omega+1} = \Phi(Y_\omega)$, etc.

En definitiva, el método que hemos mostrado para definir recursivamente sucesiones de conjuntos puede usarse para definir sucesiones transfinitas. Más concretamente, podemos definir $\mathrm{BO}(X)$ como la conjunción de las fórmulas

1. $X \subset \mathbb{N} \times \mathbb{N}$,
2. $\bigwedge ij((i,j) \in X \to (i,i) \in X \wedge (j,j) \in X)$,
3. $\bigwedge in((i,j) \in X \wedge (j,i) \in X \to i = j)$,
4. $\bigwedge ijk((i,j) \in X \wedge (j,k) \in X \to (i,k) \in X)$,
5. $\neg\bigvee F(F : \mathbb{N} \longrightarrow \mathbb{N} \wedge \bigwedge i((F(i+1), F(i)) \in X)$.

Claramente, estas fórmulas expresan que X define un buen orden en su dominio $\mathcal{D}_X = \{i \mid (i,i) \in X\}$. Escribiremos $i \leq_X j \equiv (i,j) \in X$ y $i <_X j \equiv (i \leq_X j \wedge i \neq j)$.

Para cada fórmula aritmética $\phi(n, Z)$ (con posibles parámetros), definimos la fórmula aritmética

$$\mathrm{RTA}_\phi(X, Y) \equiv \bigwedge z(z \in Y \leftrightarrow \bigvee in(z = (i,n) \wedge i \in \mathcal{D}_X \wedge \phi^*(n, X, Y, i))),$$

donde $\phi^*(n, X, Y, i)$ es la fórmula que resulta de sustituir cada subfórmula $z \in Z$ en ϕ por la fórmula

$$z \in Z \wedge \bigvee jn(j <_X i \wedge z = (j,n)).$$

La teoría RRA_0 es la que resulta de añadir a ACA_0 el esquema axiomático según el cual, para cada fórmula $\phi(n, Z)$, la fórmula siguiente es un axioma:

$$\bigwedge X(\mathrm{BO}(X) \to \bigvee Y\, \mathrm{RTA}_\phi(X, Y)).$$

Esto significa que cualquier fórmula aritmética ϕ permite definir una sucesión $\{Y_i\}_{i\in\mathcal{D}_X}$ por recursión transfinita sobre el dominio de cualquier buen orden X, de modo que $Y_i = \Phi(\{Y_j\}_{j<_X i})$.

En el caso particular en que $X = \{(i,j) \mid i \leq j\}$, obtenemos los axiomas de RA_0, por lo que RTA_0 extiende a RA_0, y es la cuarta teoría de "las cinco grandes". Un análisis mucho más complicado que el que hemos presentado en el apartado precedente permite probar que RTA_0 tiene un modelo construido mediante definiciones predicativas.

Finalmente, la quinta teoría de las *matemáticas inversas* es la teoría AC-Π^1_1 que resulta de añadirle a ACR_0 el Axioma de Comprensión Π^1_1, que resulta a su vez de restringir el axioma de comprensión de AP^2 a fórmulas de tipo Π^1_1, es decir, de la forma

$$\phi(n) \equiv \bigwedge X_1 \cdots X_k\, \alpha(n, X_1, \ldots, X_k),$$

donde la fórmula α (que puede tener parámetros) es aritmética. Esta teoría ya no es predicativa, pues permite definir conjuntos cuantificando sobre la totalidad de los conjuntos a la que debe pertenecer el conjunto definido. En AC-Π^1_1 se pueden demostrar los axiomas de RTA_0 y, de hecho, se puede demostrar la consistencia de RTA_0. No nos detenemos a analizar estas teorías porque no nos han hecho falta para formalizar la metamatemática.

Apéndice A

Glosario de términos mencionados en el capítulo I

En general, para combinaciones de palabras, debe buscarse en función de la más restrictiva. Por ejemplo, para buscar "conjunto de unicidad", hay que buscar en UNICIDAD, no en "conjunto".

Absoluto Un concepto es absoluto para un modelo transitivo numerable M de ZF si alguien que sólo vea los conjuntos de M aplicará el concepto exactamente igual que alguien que vea todos los conjuntos. Por ejemplo, $x \cup y$ es absoluto, porque si alguien "que viva en M" ve dos conjuntos $x, y \in M$, cuando calcule $x \cup y$, calculará la auténtica unión de x e y, la misma que calculará alguien que vea todos los conjuntos. En cambio, $\mathcal{P}x$ no es absoluto, porque alguien que "viva en M", aunque vea un conjunto x, al calcular $\mathcal{P}x$ se quedará con el conjunto $\mathcal{P}^M x = \mathcal{P}x \cap M$, que no tiene por qué ser el mismo $\mathcal{P}x$ que calcule alguien que vea todos los conjuntos. Véase la página 230 para más ejemplos de conceptos absolutos y no absolutos.

Acumulación (punto de) Cantor definió el concepto de punto de acumulación de un subconjunto $C \subset \mathbb{R}$ como el conjunto de los puntos $x \in \mathbb{R}$ tales que, para todo $\epsilon > 0$, el conjunto $]x - \epsilon, x + \epsilon[\cap C$ es infinito. El concepto se puede generalizar a espacios topológicos arbitrarios.

Aislado (punto) Un punto aislado x en un conjunto $C \subset \mathbb{R}$ es un punto que no es de acumulación. Equivalentemente, es un punto $x \in C$ tal que existe un $\epsilon > 0$ tal que $]x - \epsilon, x + \epsilon[\cap C = \varnothing$. La definición puede generalizarse a espacios topológicos arbitrarios.

Álef La función álef: $\aleph : \Omega \longrightarrow K \setminus \omega$ biyecta los ordinales con los cardinales infinitos conservando el orden. Por lo tanto, los cardinales infinitos son $\aleph_0, \aleph_1, \ldots \aleph_\omega, \aleph_{\omega+1}, \ldots$ Si no suponemos el axioma de elección, estos cardinales son únicamente los cardinales de los conjuntos que admiten un buen orden.

Álgebra (de conjuntos) Véase álgebra de BOOLE, al igual que para σ-álgebra.

Analítico (conjunto) Un conjunto analítico es un subconjunto de $\mathbb{R}^N$ que es la imagen de un conjunto de Borel por una aplicación continua. El concepto se puede generalizar a una clase más amplia de espacios topológicos. Admite varias caracterizaciones alternativas. Por ejemplo, el conjunto de Borel puede sustituirse por un cerrado en $\mathbb{R}^n$ y, también, un conjunto analítico puede definirse como la imagen del espacio de Baire $\mathcal{N}$ [o también de un cerrado en el espacio de Baire] por una aplicación continua.

ARP La *Aritmética Recursiva Primitiva* es una teoría aritmética que permite formalizar los razonamientos que se consideran estrictamente finitistas. En particular, en ella se puede formalizar todos los resultados metamatemáticos puramente sintácticos, es decir, que no involucran modelos. Para más detalles véase la sección 80 en la página 197.

Autorreferencia (lema de) El *lema de autorreferencia de Gödel* afirma que, en una teoría axiomática recursiva T, para cada fórmula $\phi(x)$ con x como única variable libre, existe una sentencia ψ tal que en T se demuestra que $\psi \leftrightarrow \phi(\ulcorner \psi \urcorner)$, es decir, que ψ equivale a que su formalización tiene cualquier propiedad ϕ fijada de antemano.

Baire (espacio de) El *espacio de Baire* es el conjunto $\mathcal{N} = \mathbb{N}^\omega$ de todas las sucesiones de números naturales, dotado de estructura de espacio métrico de modo que dos sucesiones están más próximas cuanto mayor es el primer término en el que difieren. Es un espacio topológico separable completamente metrizable, y es homeomorfo al espacio de los números irracionales con su topología usual.

Banach-Tarski (paradoja de) La *paradoja de Banach-Tarski* no es realmente una paradoja, en cuanto que no es nada contradictorio, sino que es el teorema que afirma que una esfera maciza puede descomponerse en un número finito de partes (de hecho, bastan cinco) que, puestas en otra posición se recombinan para formar dos esferas macizas idénticas a la original.

Berry (paradoja de) La *paradoja de Berry* es la que surge al considerar, por ejemplo, *el menor número natural no definible en castellano con menos de* 100 *letras y espacios.*

Bien ordenado (conjunto) Véase BUEN ORDEN.

Boole (álgebra de) Las álgebras de Boole son una estructura algebraica consistente en un conjunto B dotado de tres operaciones: complememento a', supremo $a \vee b$ e ínfimo $a \wedge b$, que satisfacen ciertos axiomas. El caso típico es el de un álgebra de conjuntos sobre un conjunto X, que es una familia de subconjuntos de X tal que $X \in B$ y está cerrada para uniones, intersecciones y complementos, que es un álgebra de Boole con las operaciones $a' = X \setminus a$, $a \vee b = a \cup b$, $a \wedge b = a \cap b$. Si está cerrada para uniones e intersecciones numerables, entonces se dice que es una *σ-álgebra.*

Un álgebra de Boole B es *completa* si cada conjunto $X \subset B$ tiene supremo $\bigvee X$ e ínfimo $\bigwedge X$.

Booleano (modelo) Los modelos booleanos son una construcción matemática que simplifica la aplicación de la teoría de extensiones genéricas y que incluso puede sustituirla en muchas ocasiones. Consiste en fijar un álgebra de Boole completa $\mathbb{B}$ y asignar a cada fórmula $\phi(x_1,\dots,x_n)$ del lenguaje de la teoría de conjuntos y a unos "nombres" $a_1,\dots,a_n$) un valor booleano $\|\phi(a_1,\dots,a_n)\|$ de modo que todos los teoremas de ZFC cumplen $\|\phi\| = 1$. De este modo, si se prueba que una fórmula ϕ cumple $\|\phi\| \neq 1$, se puede concluir que dicha fórmula no es demostrable en ZFC.

Borel (medida de) La medida de Borel es una medida que extiende el contenido de Jordan a una familia más amplia de subconjuntos de $\mathbb{R}^n$, concretamente a la σ-álgebra de los conjuntos medibles Borel, que es la menor σ-álgebra de subconjuntos de $\mathbb{R}^n$ que contiene a los conjuntos abiertos (o a los cerrados). Al extender al contenido de Jordan, se trata de una generalización del concepto de longitud, área, volumen, etc. a una familia más amplia de subconjuntos.

Lebesgue demostró que los conjuntos medibles Borel en $\mathbb{R}$ (y, en general, en cualquier espacio topológico) pueden generarse en una sucesión transfinita que, con notación moderna, se define así: $\mathbf{\Sigma}^0_1$ es la clase de los conjuntos abiertos, $\mathbf{\Pi}^0_1$ es la clase de los conjuntos cerrados. En general, si $\alpha < \omega_1$, las clases $\mathbf{\Sigma}^0_\alpha$ y $\mathbf{\Pi}^0_\alpha$ se definen como las formadas por las uniones e intersecciones numerables (respectivamente) de conjuntos de las clases precedentes $\mathbf{\Pi}^0_\beta$ y $\mathbf{\Sigma}^0_\beta$ (respectivamente), con $\beta < \alpha$. Entonces la clase de los conjuntos de Borel es la unión de las clases $\mathbf{\Sigma}_\alpha$ o, equivalentemente, la de las clases $\mathbf{\Pi}_\alpha$, para $\alpha < \omega_1$.

Buen orden Un conjunto ordenado A está *bien ordenado* si todo subconjunto de A no vacío tiene un mínimo elemento. Es el caso de todos los conjuntos totalmente ordenados finitos, y también el del conjunto de los números naturales con el orden usual.

Buena ordenación (teorema de) El *teorema de buena ordenación* afirma que todo conjunto admite un buen orden. Es equivalente al axioma de elección.

Burali-Forti (antinomia de) La *antinomia de Burali-Forti* fue la primera contradicción que Cantor descubrió en su teoría de conjuntos. Tiene que ver con el ordinal Ω del conjunto de todos los ordinales. Admite distintas variantes ligeras, como que puede probarse que $\Omega < \Omega$ (y también lo contrario), o como que puede probarse que $\Omega < \Omega + 1$ y a la vez $\Omega + 1 < \Omega$.

Cantor (conjunto de) El conjunto de Cantor es el subconjunto $C \subset [0,1]$ formado por los números reales cuyas expresiones decimales en base 3 no contienen la cifra 2. Es un cerrado perfecto de cardinal $\mathfrak{c}$, pero de "longitud" 0.

Cantor (paradoja de) La paradoja de Cantor consiste en que en la teoría ingenua de conjuntos es posible demostrar que el conjunto V de todos los conjuntos tiene cardinal estrictamente menor que su conjunto de partes $\mathcal{P}V$ y también lo contrario.

Cantor (teorema de) El teorema de Cantor afirma que todo conjunto X es estrictamente minuspotente a (es decir, tiene cardinal menor que) el conjunto $\mathcal{P}X$ de todos sus subconjuntos.

Cantor-Bendixson (teorema de) El teorema de Cantor-Bendixson afirma que todo cerrado en $\mathbb{R}$ se descompone en unión disjunta de un cerrado perfecto y un conjunto numerable. Puede generalizarse a una clase amplia de espacios topológicos. Su interés reside en que implica que todo cerrado es numerable o tiene el cardinal del continuo (según si el subconjunto perfecto es vacío o no). En otras palabras, un subconjunto cerrado no puede ser un contraejemplo a la hipótesis del continuo.

Cantor-Bernstein (teorema de) El teorema de Cantor-Bernstein, o de Schröder-Bernstein, es el que afirma que si existen aplicaciones inyectivas $f : A \longrightarrow B$ y $g : B \longrightarrow A$, entonces existe una biyección entre A y B.

Cardinal Para Cantor, el cardinal de un conjunto era simplemente un concepto abstracto que medía su potencia, de modo que dos conjuntos tienen el mismo cardinal si y sólo si se pueden biyectar.

A la hora de formalizar el concepto de cardinal en la teoría axiomática de conjuntos, lo habitual es definir un cardinal como un ordinal (de von Neumann) que no se puede biyectar con ningún ordinal anterior. Así, los ordinales finitos $0, 1, 2, \dots$, son cardinales, ω es el primer cardinal infinito, y cuando se piensa como tal se representa por $\aleph_0$, el menor ordinal no numerable es ω_1 y, cuando se piensa como cardinal se representa por $\aleph_1$, etc.

El cardinal de un conjunto X es el único cardinal en este sentido biyectable con él, y se representa por $|X|$, pero esta definición presupone el axioma de elección, sin el cual no es cierto que todo conjunto se pueda biyectar con un ordinal, luego tampoco con un cardinal.

Para trabajar con cardinales sin suponer el axioma de elección, una forma de definir el cardinal de un conjunto x es definirlo como el conjunto $\overline{\overline{x}}$ de todos los conjuntos biyectables con x cuyo rango α en la jerarquía de von Neumann es el menor posible. De este modo $\overline{\overline{x}} \subset V_{\alpha+1}$ es un conjunto.

Los cardinales se dividen en tres clases: el 0, que no tiene anteriores, los *cardinales sucesores,* que tienen un inmediato anterior y los *cardinales límite,* que tienen anteriores, pero no un inmediato anterior, como es el caso de $\aleph_\omega$.

La relación $\kappa \leq \mu$ entre cardinales se define como la que se da cuando existe una aplicación inyectiva de un conjunto de cardinal κ en otro de cardinal μ (aunque, si los cardinales se definen como ordinales, se trata de la relación de orden usual entre los ordinales).

Las operaciones $\kappa+\mu$, $\kappa\cdot\mu$ y κ^μ entre dos cardinales se definen, respectivamente, como el cardinal de la unión de un conjunto de cardinal κ con otro conjunto disjunto de cardinal μ, el cardinal del producto cartesiano de un conjunto de cardinal κ por otro de cardinal μ y el cardinal del conjunto de las aplicaciones de un conjunto de cardinal μ en otro de cardinal κ.

Categorias El concepto de *categoría,* junto con el de *funtor* y el de *transformación natural* permiten expresar en términos abstractos un gran número de estructuras matemáticas con los conceptos definibles en ellas, hasta el punto de que se puede plantear una fundamentación alternativa de las matemáticas en términos de categorías. Para más detalles véase la sección 71 en la página 165.

Church-Turing (tesis de) La *tesis de Church-Turing* afirma que las funciones recursivas (parciales) coinciden con las que pueden calcularse mediante un algoritmo explícito.

Clase El concepto de clase es uno de los conceptos primitivos de la teoría de clases NBG, y es más amplio que el concepto de conjunto, de modo que se puede hablar de la clase de todos los conjuntos, o de la clase de todos los ordinales, sin caer en contradicciones gracias a que son *clases propias,* es decir, clases que no son conjuntos.

En ZF también es posible hablar de clases en términos metamatemáticos, entendiendo que las clases son las colecciones de conjuntos definidas por fórmulas, aunque no haya ningún conjunto que contenga sus elementos. En la página 176 se explica cómo hacerlo.

Clase numérica Cantor llamó *primera clase numérica* (I) al conjunto de los ordinales finitos (los números naturales), mientras que la *segunda clase numérica* (II) era el conjunto de todos los ordinales correspondientes a formas de ordenar bien un conjunto numerable. El cardinal de la primera clase numérica es, por definición $\aleph_0$, mientras que el de la segunda es $\aleph_1$. A su vez, la *tercera clase numérica* (III) es el conjunto de todos los ordinales que corresponden a formas de ordenar bien un conjunto de cardinal $\aleph_1$, y su cardinal es $\aleph_2$, etc. Cantor demostró que $\aleph_0$ es el menor cardinal infinito, que $\aleph_1$ es el menor cardinal mayor que $\aleph_0$, y así sucesivamente.

Cofinalidad La cofinalidad de un cardinal infinito κ es el menor cardinal μ tal que la unión de μ conjuntos disjuntos dos a dos de cardinal menor que κ tiene cardinal κ. Se representa por $\mu = \operatorname{cf}\kappa$. En estos términos, un cardinal κ es REGULAR si y sólo si $\operatorname{cf}\kappa = \kappa$, y es singular si $\operatorname{cf}\kappa < \kappa$.

Compacidad (teorema de) El *teorema de compacidad de Gödel* afirma que si un conjunto de fórmulas tiene la propiedad de que todo subconjunto finito admite un modelo, entonces el conjunto completo tiene un modelo. Es una consecuencia inmediata del teorema de completitud de Gödel, aunque también se puede demostrar por otros medios, por ejemplo usando ultraproductos. Véase la sección 88 en la página 236.

Completitud semántica (teorema de) El *teorema de completitud semántica* de Gödel afirma que si una fórmula es verdadera en todos los modelos donde unos axiomas son verdaderos, entonces la fórmula se puede deducir formalmente de dichos axiomas.

Una versión equivalente afirma que una teoría axiomática (o un conjunto de fórmulas) es consistente si y sólo si admite un modelo, que puede tomarse numerable.

Continuo (hipótesis del) Cantor llamaba "continuos" a los espacios en los que era posible moverse de forma continua. Eso incluía la recta real $\mathbb{R}$, los intervalos en $\mathbb{R}$ y también $\mathbb{R}^n$ y determinados subconjuntos de $\mathbb{R}^n$. Todos ellos tenían el mismo cardinal, que se representa por $\mathfrak{c}$ o, en términos de la aritmética cardinal, como $2^{\aleph_0}$.

La *hipótesis del continuo* es la conjetura de Cantor de que no hay ningún cardinal intermedio entre el cardinal de $\mathbb{N}$ y el de $\mathbb{R}$. En términos de la aritmética cardinal se puede expresar mediante la igualdad $2^{\aleph_0} = \aleph_1$.

La *hipótesis del continuo generalizada* afirma que $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ para todo ordinal α.

Consis(T) Si T es una teoría axiomática recursiva, la sentencia Consis(T) (o Consis($\ulcorner T \urcorner$), para enfatizar que $\ulcorner T \urcorner$ es una formalización de T) es una sentencia aritmética, es decir, formulable en el lenguaje de la aritmética de Peano, pero que equivale a que la teoría T sea consistente. Más concretamente, T afirma que no existe ningún número natural que codifique la demostración de una contradicción en T. Sucede que "codificar una demostración de una contradicción en T" es una propiedad que puede tener o no un número natural y que se puede expresar exclusivamente en términos aritméticos, como "ser un número primo".

Consistencia Una teoría (o un conjunto de fórmulas) es *consistente* cuando no se puede demostrar una contradicción en ella (o a partir de ellas). En caso contrario es *contradictoria.*

Una teoría aritmética es ω-*contradictoria* cuando hay una fórmula $\phi(x)$ de su lenguaje formal para la que se pueden demostrar los teoremas $\phi(0), \phi(1), \phi(2), \ldots$, pero también se puede demostrar $\bigvee x\, \neg\phi(x)$. En caso contrario la teoría es ω-*consistente.* Toda teoría ω-consistente es consistente, pero el recíproco no es cierto.

Constructible (conjunto) La clase L de los conjuntos *constructibles* se define mediante la jerarquía $L_0 = \varnothing$, $L_{\alpha+1} = \mathcal{D}L_\alpha$, $L_\lambda = \bigcup_{\delta<\lambda} L_\delta$, de modo que $L = \bigcup_{\alpha\in\Omega} L_\alpha$, donde $\mathcal{D}$ es el operador de las partes DEFINIBLES. El axioma de constructibilidad afirma que $V = L$, e implica el axioma de elección y la hipótesis del continuo generalizada. De hecho, sin el axioma de elección, se puede definir una fórmula explícita $x \trianglelefteq y$ que define un buen orden sobre L.

Es posible definir dos variantes $L(A)$ y $L[A]$ del modelo L. La primera, para un conjunto transitivo A, consiste en partir de $L_0(A) = A$, y así se obtiene una clase transitiva $L(A)$ que es un modelo de ZF, pero no necesariamente de ZFC. La segunda parte de $L_0[A] = \varnothing$, pero luego define $L_{\alpha+1}[A] = \mathcal{D}_A L_\alpha[A]$ (véase DEFINIBLES), y así se obtiene siempre un modelo transitivo de ZFC, aunque no sucede necesariamente que $A \in L[A]$. Si llamamos $\bar{A} = A \cap L[A]$, entonces $L[A] = L[\bar{A}]$ y $\bar{A} \in L[\bar{A}]$.

Cota Véase SUPREMO.

Definibles (partes) El conjunto $\mathcal{D}X$ de las *partes definibles* de un conjunto X está formado por todos los subconjuntos de X de la forma $\{x \in X \mid X \vDash \phi[x, x_1, \ldots, x_n]\}$, donde $x_1, \ldots, x_n \in X$ y ϕ es una fórmula del lenguaje de la teoría de conjuntos, considerando a X como el modelo en el que el relator de pertenencia se interpreta como la relación de pertenencia. Así $\mathcal{D}X \subset \mathcal{P}X$, pero, si X es infinito, el cardinal de $\mathcal{D}X$ es el mismo que el de X, mientras que el de $\mathcal{P}X$ es superior.

Una variante es $\mathcal{D}_A X$, donde A es un conjunto arbitrario. La diferencia es que en este caso ϕ es una fórmula del lenguaje de la teoría de conjuntos extendido con un relator monádico R y X se considera como modelo de este lenguaje interpretando el relator R como la relación $x \in A$. Así, para definir subconjuntos de X, se admite que se pueda distinguir entre los conjuntos que pertenecen a A y los que no pertenecen, aunque A no pertenezca a X.

Demostración (teoría de la) La *Teoría de la demostración* es la rama de la lógica matemática que estudia las demostraciones formales, es decir, las formas de razonamiento consistentes en fijar unos axiomas y unas reglas de inferencia formales constructivas que indiquen qué fórmulas se pueden deducir de otras dadas y considerar como teoremas las fórmulas que pueden deducirse de los axiomas en un número finito de pasos aplicando las reglas de inferencia.

Denso Si $\mathbb{P}$ es un conjunto parcialmente ordenado, un conjunto $D \subset \mathbb{P}$ es *denso* en $\mathbb{P}$ si para toda condición $p \in \mathbb{P}$ existe otra $d \in D$ tal que $d \le p$.

Derivado (conjunto) Si $C \subset \mathbb{R}$, Cantor definió su conjunto derivado como el conjunto de los puntos de acumulación de C. A su vez, Cantor definió los derivados sucesivos de un conjunto $C^{(\alpha)}$, donde α es un ordinal, mediante:

$$C^{(0)} = C, \qquad C^{(\alpha+1)} = (C^{(\alpha)})', \qquad C^{(\lambda)} = \bigcap_{\delta<\lambda} C^{(\delta)}.$$

Determinación (axioma de) El axioma de determinación AD es un axioma formulable en ZF que es incompatible con el axioma de elección, pues implica, entre otras cosas que todo subconjunto de $\mathbb{R}^n$ es medible Lebesgue. Para más detalles véase la sección 78 en la página 190.

Elección (axioma de) El axioma de elección admite varias formulaciones equivalentes. Entre ellas se encuentran:

1) Si A es una familia de conjuntos no vacíos, existe una función f que a cada conjunto $X \in A$ le hace corresponder uno de sus elementos $f(X) \in X$.

2) Si A es una familia de conjuntos no vacíos disjuntos dos a dos, existe un conjunto E tal que, para cada $X \in A$, la intersección $X \cap E$ consta de un único elemento.

3) Si $\{X_i\}_{i\in I}$ es una familia de conjuntos no vacíos, el producto cartesiano $\prod_{i\in I} X_i$ es no vacío.

Entre las formas débiles del axioma de elección se encuentran el *axioma de elección numerable,* que es 1) o 2) restringido a familias A numerables, o el *principio de elecciones dependientes,* que afirma que si R es una relación en una clase A tal que, para cada $a \in A$, existe un $b \in A$ de modo que $b\,R\,a$, entonces para cada $a \in A$ existe una sucesión $\{a_n\}_{n=0}^{\infty}$ tal que $a = a_0$ y $a_{n+1}\,R\,a_n$.

Eliminación de cortes (teoremas de) Los teoremas de eliminación de cortes son teoremas fundamentales de la teoría de la demostración, que dan lugar a pruebas de consistencia o a teoremas que relacionan los teoremas de unas teorías con los de otras. Explicar su relevancia queda fuera del alcance de este libro. Para más detalles véase la sección 57 en la página 117.

Equipotencia Dos conjuntos X e Y son *equipotentes* si existe una aplicación $f : X \longrightarrow Y$ biyectiva, lo que equivale a que tengan el mismo cardinal.

Estándar (modelo, número) Un modelo de una teoría aritmética es *estándar* si los únicos objetos que contiene que tienen la propiedad de ser números naturales son los nombrados por los numerales $0, 1, 2, 3, \ldots$ En cambio, un modelo es *no estándar* si contiene números naturales *no estándar,* es decir, objetos que tienen la propiedad de ser números naturales, según se definen o se presentan axiomáticamente en la teoría, pero que no son ni el 0, ni el 1, ni el 2, etc. También se les llama *números naturales infinitos.*

Expresable (relación) Una relación sobre números naturales es *expresable* en una teoría aritmética si existe una fórmula del lenguaje de la teoría que puede demostrarse para los números naturales que cumplen la relación y refutarse para los que no la cumplen. Para más detalles véase la página 106.

Filtro Un *filtro* en un álgebra de Boole B es un conjunto $F \subset B$ tal que 1) $0 \notin F$,$1 \in F$, 2) si $a \in F$ y $b \in B$ y $a \le b$, entonces $b \in F$ y 3) Si $a, b \in F$, entoncces $a \wedge b \in F$. El filtro es un *ultrafiltro* si además todo elemento $a \in B$ cumple $a \in F$ o bien $a' \in F$.

Finitismo El *finitismo* es la doctrina según la cual sólo las matemáticas interpretables en términos de procesos finitos tienen significado real, mientras que el resto de afirmaciones matemáticas carecen de tal significado, y son como novelas de ficción en las que se habla de personajes inexistentes.

Forcing La *teoría de extensiones genéricas* o *forcing* es una técnica muy versátil de construir modelos de ZFC que da lugar a una cantidad ingente de pruebas de consistencia. Es imposible resumirla en pocas palabras. Véanse las secciones 91, 95, 96, 97 y 98.

Forcing (lenguaje del) En las formulaciones antiguas del *forcing* se definía un *lenguaje del forcing* con una sintaxis complicada (véase Ramificado) de modo que, si M es un modelo transitivo numerable de ZFC, el *lenguaje del forcing* cuenta con términos para nombrar a cada uno de los elementos de la extensión genérica $M[G]$ y para expresar cualquier hecho que pueda cumplirse o no en $M[G]$. Esto se usaba, por una parte, para definir $M[G]$ como el conjunto de todos los conjuntos nombrados por los términos del *lenguaje del forcing* y, por otra parte, para definir la relación $p \Vdash \phi$, que expresa que si $p \in G$, entonces ϕ es verdadera en $M[G]$. La clave de esta relación es que puede calcularse en M a pesar de que ni el filtro genérico G ni el modelo $M[G]$ son accesibles a "alguien que viva en M".

Forma normal de Cantor Todo ordinal α se puede expresar de forma única como $\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_n}$, donde $\eta_0 \ge \eta_1 \ge \cdots \ge \eta_n$. Esta expresión se llama *forma normal de Cantor* de α. (Hay que entender que, para $\alpha = 0$, su forma normal es una suma sin sumandos.)

Formal (razonamiento) Un razonamiento es formal si el paso de una afirmación a otra se justifica meramente por la forma de las afirmaciones involucradas, sin tener en cuenta para nada su posible significado. Por ejemplo, si tenemos las premisas $A \vee B$ y $\neg A$, no necesitamos saber qué significan A y B para concluir que tiene que cumplirse B.

Fórmula En lógica, se llaman fórmulas a todas las cadenas de signos de un lenguaje formal que son susceptibles de ser interpretadas como afirmaciones sobre unos objetos prefijados. Por ejemplo, $\bigwedge xy\,(x+y = y+x)$ es una fórmula del lenguaje de la aritmética de Peano, cuya interpretación usual es que la suma de números naturales es conmutativa. Las fórmulas con variables libres expresan propiedades. Por ejemplo, $\alpha(x) \equiv \bigvee y\, x = 2y$ expresa la propiedad "x es un número par".

Generador (principio) Cantor llamó *principios generadores* a los principios que definían la sucesión de los ordinales transfinitos. El primer principio generador afirma que todo ordinal tiene un siguiente, mientras que el segundo afirma que todo conjunto de ordinales tiene un mínimo ordinal mayor que todos sus elementos.

Hausdorff (fórmula de) La *fórmula de Hausdorff* es una relación aritmética entre cardinales infinitos, según la cual se cumple que $\aleph_{\alpha+1}^{\aleph_\beta} = \aleph_{\alpha+1}\aleph_\alpha^{\aleph_\beta}$.

Genérico La teoría de extensiones genéricas (o *forcing*) consiste esencialmente en partir de un modelo transitivo M de ZFC en el que se ha fijado un conjunto ordenado $\mathbb{P}$ de *condiciones* y construir una *extensión genérica* $M[G]$, que es el menor modelo transitivo de ZFC que contiene a M y a uno o varios objetos "genéricos". El principal, desde un punto de vista teórico es un *filtro genérico* G, que es un subconjunto $G \subset \mathbb{P}$ con la propiedad de que corta a todo subconjunto denso de $\mathbb{P}$ que pertenezca a M. En formulaciones más antiguas de la teoría la genericidad se define en otros términos equivalentes. Por ejemplo, se habla de una *sucesión genérica* de condiciones $p_0 \ge p_1 \ge p_2 \ge \cdots$ con la propiedad de que, para toda fórmula del *lenguaje del forcing* existe una condición en la sucesión que fuerza la fórmula o su negación. También se llama genéricos a los conjuntos en $M[G]$ que determinan y están determinados por el filtro genérico G.

Hilbert (programa de) El programa de Hilbert para fundamentar la matemática era el proyecto de formular una teoría axiomática de conjuntos capaz de formalizar todos los teoremas matemáticos y cuya consistencia pudiera demostrarse por medios finitistas, es decir, mediante medios que sólo involucraran procesos finitos para demostrar constructivamente que de los axiomas fijados era imposible derivar una contradicción. Además, Hilbert pedía que pudiera demostrarse que la teoría axiomática fuera completa (es decir, que pudiera resolver cualquier problema matemático demostrando cualquier sentencia o bien su negación).

Hilbert-Bernays (condiciones de) Las *condiciones de Hilbert-Bernays* son tres condiciones que debe satisfacer cualquier formalización razonable del concepto de "demostrabilidad", a partir de las cuales se demuestran fácilmente los teoremas de incompletitud de Gödel. Están formuladas en la página 148.

Ideal Un *ideal* en un álgebra de Boole B es un conjunto $I \subset B$ tal que 1) $0 \in I$,$1 \notin I$, 2) si $a \in B$ y $b \in I$ y $a \leq b$, entonces $a \in I$ y 3) Si $a, b \in I$, entoncces $a \vee b \in I$. El ideal es *primo* si además todo elemento $a \in B$ cumple $a \in I$ o bien $a' \in I$.

Inaccesible Un cardinal κ es *débilmente inaccesible* si es un cardinal límite regulare no numerable. Que sea un cardinal límite quiere decir que no tiene un inmediato anterior, que sea regular quiere decir que la unión de menos de κ conjuntos de cardinal κ tiene cardinal menor que κ.

Se dice que κ es *fuertemente inaccesible* si cumple además que cuando $\mu < \kappa$, entonces $2^\mu < \kappa$.

Incompletitud (teoremas de) El *primer teorema de incompletitud de Gödel* afirma que toda teoría aritmética (es decir, que permita demostrar las propiedades básicas de los números naturales) recursiva (es decir, que se pueda determinar qué fórmulas son axiomas y cuáles no) y consistente (que no permita probar contradicciones) es incompleta (existen sentencias que no son demostrables ni refutables en la teoría).

El *segundo teorema de incompletitud de Gödel* afirma que toda teoría aritmética recursiva consistente T no puede demostrar la fórmula aritmética $\text{Consis}(T)$ que afirma su propia consistencia.

Inducción Hay muchos principios de inducción. El más básico es el siguiente:

Si el número natural 0 tiene una propiedad P y, supuesto que un número natural n tiene la propiedad P, podemos asegurar que $n+1$ también la tiene, entonces todos los números naturales tienen la propiedad P.

Una variante es:

Si, bajo el supuesto de que todos los números naturales menores que uno n tienen una propiedad P, se cumple necesariamente que n también la tiene, entonces todos los números naturales tienen la propiedad P.

Esto vale en general para conjuntos bien ordenados:

Si A es un conjunto bien ordenado y, para cada $a \in A$, el supuesto de que todos los $x \in A$ que cumplen $x < a$ tienen una propiedad P implica necesariamente que a también la tiene, entonces todos los elementos de A tienen la propiedad P.

Los ordinales cumplen el principio de *inducción transfinita:*

Si 0 cumple una propiedad P, si cuando un ordinal α cumple P también la cumple $\alpha + 1$ y si, bajo el supuesto de que todos los ordinales menores que un ordinal límite λ cumplen P, se cumple necesariamente que λ cumple P, entonces todos los ordinales cumplen P.

Ínfimo Véase SUPREMO.

Infinito Hay diversas formas de definir formalmente el concepto de conjunto finito / infinito. Una consiste en definir los conjuntos finitos como los que pueden biyectarse con un conjunto $I_n = \{0, 1, \ldots, n-1\}$, donde n es un número natural, y es infinito en caso contrario.

Otra, debida a Dedekind, consiste en definir que un A es infinito si existe una aplicación $S : A \longrightarrow A$ inyectiva y no suprayectiva, y es finito en caso contrario.

Inmersión Una inmersión $i : M \longrightarrow N$ entre dos modelos de un mismo lenguaje formal es una aplicación entre ellos que conserva las interpretaciones de todos los signos del lenguaje. Véase la página 225. Una inmersión biyectiva es un *isomorfismo* de modelos.

Una *inmersión elemental* es una inmersión que conserva todas las fórmulas del lenguaje formal, es decir, que, para toda fórmula $\phi(x_1, \ldots, x_n)$ y todos los elementos $a_1, \ldots, a_n \in M$, se cumple $M \vDash \phi[a_1, \ldots, a_n] \leftrightarrow N \vDash \phi[a_1, \ldots, a_n]$ (véase la página 226).

Intuición A la palabra intuición se le dan sentidos muy diferentes en contextos muy diferentes. Por ello es importante entender que, en ciertos contextos, sobre todo cuando se habla de razonar intuitivamente, hay que entender que hablamos de razonar sobre afirmaciones a las que se les puede dar una interpretación intuitiva precisa y rigurosa, de modo que podamos garantizar que cada cosa que se afirma es verdad. Para más detalles véase la página 74 y siguientes.

Intuicionismo El *intuicionismo* es la doctrina que sostiene que la mayor parte de las matemáticas modernas son incorrectas porque usan conceptos mal definidos que no tienen sentido alguno. Entre las restricciones que los intuicionistas imponen al razonamiento matemático para darlo por válido se incluye la negación de algunos principios lógicos fundamentales, como la doble negación (p es equivalente a $\neg\neg p$) o el tercio excluso (siempre se cumple $p \vee \neg p$) cuando se pretenden aplicar a razonamientos con conjuntos infinitos. Además, los intuicionistas rechazan las definiciones impredicativas.

Jerarquía de von Neumann La *jerarquía de von Neumann* es la estratificación $\{V_\alpha\}_{\alpha\in\Omega}$ de la clase V de los conjuntos definida mediante $V_0 = \varnothing$, $V_{\alpha+1} = \mathcal{P}V_\alpha$, $V_\lambda = \bigcup_{\delta<\lambda} V_\delta$. El axioma de regularidad equivale a que $V = \bigcup_{\alpha\in\Omega} V_\alpha$. En tal caso, cada conjunto x tiene determinado un *rango* α, que es el menor ordinal tal que $x \subset V_\alpha$ (o $x \in V_{\alpha+1}$) y que es una medida de su complejidad.

Jordan (medida o contenido de) El contenido de Jordán está definido para ciertos subconjuntos acotados de $\mathbb{R}^n$, los que se llaman *medibles Jordan,* y es una determinación de su longitud, área, volumen, etc., según el valor de n. Para su definición véase la sección 11 en la página 19.

Kőnig (teorema de) Hay dos teoremas de Kőnig famosos. Uno, debido a Gyula Kőnig, afirma que si $\{\kappa_i\}_{i\in I}$ y $\{\mu_i\}_{i\in I}$ son dos familias de cardinales tales que $\mu_i < \nu_i$, entonces $\sum_{i\in I}\kappa_i < \prod_{i\in I}\mu_i$. La suma se define como el cardinal de una unión disjunta de un conjunto de cada cardinal κ_i, mientras que el producto es el cardinal del producto cartesiano de un conjunto de cada cardinal μ_i. Esto implica a su vez que $\kappa^{\mathrm{cf}\,\kappa} > \kappa$ y que $\mathrm{cf}(2^\kappa) > \kappa$. (Véase la página 253.)

El segundo, debido a Dénes Kőnig, admite varias formulaciones, pero la más habitual hoy en día es la que afirma que si un árbol numerable tiene niveles finitos, entonces tiene una rama infinita. Véase la sección 37 en la página 77.

Lebesgue (medida de) La *medida de Lebesgue* en $\mathbb{R}^n$ es una medida que extiende el contenido de Jordan y la medida de Borel a una familia de subconjuntos de $\mathbb{R}^n$ mucho mayor, la de los conjuntos medibles Lebesgue, por lo que se trata de una generalización del concepto de longitud, área, volumen, etc. a una familia mayor de conjuntos. Para su definición véase la sección 19 en la página 33.

Lenguaje formal Un *lenguaje formal* es un lenguaje definido de forma que se pueda estudiar su gramática sin necesidad de tener en consideración en ningún momento el posible significado de sus signos. Un lenguaje formal típico consta de unas variables $x_0, x_1, x_2, \ldots$, unos signos lógicos, como $\neg, \wedge, \vee, \to, \leftrightarrow, =, \bigwedge, \bigvee$ y unos signos específicos para referirse a objetos, relaciones o funciones de una determinada teoría. Por ejemplo, el lenguaje de la teoría de conjuntos tiene al relator $\in$ como único signo específico, que hace referencia a la relación de pertenencia, mientras que el lenguaje de la Aritmética de Peano tiene una constante 0 para referirse al número natural 0, un funtor monádico S para referirse al siguiente de un número natural, y los funtores diádicos $+$ y $\cdot$ para referirse a la suma y el producto de números naturales. En ocasiones se le añade también un relator diádico $\leq$ para referirse a la relación de orden de los números naturales.

Libre/ligada (variable) Una variable está libre en una fórmula de un lenguaje formal si no queda bajo el alcance de un cuantificador. En caso contrario está ligada. Por ejemplo, en la fórmula $\bigwedge u(u \in x \to u \in y)$, las variables x, y están libres, mientras que u está ligada por el generalizador.

Löb (teorema de) El teorema de Löb afirma que una sentencia de una teoría aritmética recursiva que equivalga a su propia demostrabilidad siempre es demostrable.

Löwenheim-Skolem (teorema de) El *teorema de Löwenheim-Skolem* afirma que si un conjunto de axiomas admite un modelo, entonces admite un modelo de universo numerable (tal vez finito). Una versión más general (expresable en el seno de una teoría de conjuntos) afirma que si una teoría tiene un modelo, entonces admite modelos de cualquier cardinal mayor o igual que el número de signos de su lenguaje formal.

Medible (cardinal) Un cardinal infinito κ es $\mathbb{R}$-*medible* si existe una medida κ-aditiva no trivial en κ. Si existe una medida no trivial en un conjunto X, entonces el menor cardinal κ en el que existe tal medida es un cardinal $\mathbb{R}$-medible $\kappa \leq |X|$.

Si un cardinal $\mathbb{R}$-medible admite una medida *bivaluada,* es decir, que sólo toma los valores $0, 1$, se dice que es *medible.* Esto equivale a que exista un ultrafiltro en κ no principal y κ-completo.

Un cardinal κ con un ultrafiltro no principal σ-completo se llama *medible Ulam.* El menor cardinal medible Ulam es medible.

Un cardinal $\mathbb{R}$-medible κ puede encontrarse en dos casos: o bien es medible, y entonces es fuertemente inaccesible, o bien $\kappa \leq 2^{\aleph_0}$, y entonces es débilmente inaccesible y la medida de Lebesgue se extiende a una medida κ-aditiva en $\mathcal{P}[0,1]$.

La existencia de un cardinal $\mathbb{R}$-medible implica que $V \neq L$. Para más detalles, véase la página 90 y la sección 89 en la página 240.

Medida Si $\mathcal{M}$ es un σ-álgebra de conjuntos, es decir, un álgebra cerrada para uniones e intersecciones numerables, una *medida* en $\mathcal{M}$ es una aplicación $\mu : \mathcal{M} \longrightarrow [0, +\infty]$ tal que $\mu(\varnothing) = 0$ y si $\{A_n\}_{n=0}^\infty$ es una sucesión de elementos de $\mathcal{M}$ disjuntos dos a dos, entonces $\mu\Big(\bigcup_{n=0}^\infty A_n\Big) = \sum_{n=0}^\infty \mu(A_n)$.

Una *medida* en un conjunto X es una medida $\mu : \mathcal{P}X \longrightarrow [0,1]$. Se dice que *no es trivial* si los puntos tienen medida nula, pero hay conjuntos de medida no nula. Si κ es un cardinal, la medida es κ-*aditiva* si la unión de menos de κ conjuntos nulos es nula.

Metamatemática La *metamatemática* es, en principio, el estudio informal, constructivo, de las teorías axiomáticas que permiten exponer formalmente la matemática. La metamatemática puede formalizarse en muchas teorías axiomáticas, y entonces es fundamental distinguir entre los conceptos y afirmaciones metamatemáticas informales y los términos y sentencias matemáticas que expresan formalmente tales conceptos y afirmaciones. Para más detalles véase la sección 47 en la página 97 y la sección 49 en la página 103.

Minuspotencia Un conjunto X es *minuspotente* a otro conjunto Y si existe una aplicación $f : X \longrightarrow Y$ inyectiva. Esto equivale a que el cardinal de X sea menor o igual que el de Y. Se dice que X es *estrictamente minuspotente* a Y si además no existe una aplicación $g : X \longrightarrow Y$ biyectiva. (No basta con que f no sea biyectiva, tiene que ser imposible que exista otra que sí que lo sea.) Esto equivale a que el cardinal de X sea menor que el de Y.

Modelo Un *modelo* de un lenguaje formal es un conjunto (llamado *universo* del modelo) dotado de las relaciones y funciones necesarias para dar una interpretación a los signos de un lenguaje formal. Por ejemplo, un modelo de la aritmética de Peano es un conjunto en el que se ha seleccionado uno de sus elementos para interpretar la constante 0 y se han fijado tres funciones para interpretar los funtores S, $+$, $\cdot$. En principio, las fórmulas de un lenguaje formal no tienen ningún significado asignado, pero en cuanto se fija un modelo para dicho lenguaje y una interpretación para cada variable, ya tiene sentido plantearse si una fórmula es satisfecha o no en dicho modelo (véase Verdad).

Se llama *modelo* de una teoría axiomática a un modelo de su lenguaje formal en el que sus axiomas (y, por consiguiente, sus teoremas) son verdaderos.

Morse-Kelley La teoría de conjuntos de *Morse-Kelley* (MK) es la teoría que resulta de extender NBG tomando como esquema axiomático el esquema de comprensión sin la restricción de que las fórmulas tengan que tener sus cuantificadores restringidos a conjuntos para definir conjuntos. En MK se puede demostrar la consistencia de ZFC, que es equivalente a la de NBG, luego en MK se pueden demostrar teoremas no demostrables en NBG (supuesto que sean consistentes).

Mostowski (colapso de) Si M es un conjunto en el que hay definida una relación R que sea extensional y bien fundada, la *función colapsante* de Mostowski es la única biyección $\pi : M \longrightarrow M^*$ de M en un conjunto transitivo M^* que transforma la relación R en la relación de pertenencia. El conjunto M se llama *colapso de Mostowski* de (M, R). Para los detalles véase la página 232, sobre todo las definiciones previas al teorema.

El teorema es válido también si M es una clase propia a condición de que añadamos la hipótesis de que, para cada $a \in M$, la clase $\{x \in M \mid x\, R\, a\}$ sea un conjunto.

Multiplicidad inconsistente Cantor llamaba *multiplicidades inconsistentes* a los "conjuntos" que daban lugar a contradicciones cuando se pretendía trabajar con ellos, como el conjunto de todos los conjuntos, el conjunto de todos los ordinales, etc. En las teorías de conjuntos de von Neuman, von Neuman-Bernays o von Neuman-Bernays-Gödel, las multiplicidades inconsistentes de Cantor se formalizan mediante el concepto de clase propia.

NBG La teoría de conjuntos de von Neumann-Bernays-Gödel (NBG) es una teoría que adopta como conceptos primitivos los conceptos de *clase* y de *pertenencia,* en la que los conjuntos se definen como las clases que pertenecen al menos a otra clase. Es finitamente axiomatizable, pero sus ocho axiomas de formación de clases equivalen al esquema teoremático de comprensión, que afirma que, para toda fórmula $\phi(x)$ cuyos cuantificadores estén restringidos a conjuntos, existe una (única) clase cuyos elementos son los conjuntos que cumplen $\phi(x)$. Esto permite definir clases como la clase de todos los conjuntos, o la clase de todos los ordinales, que no dan lugar a contradicciones porque son *clases propias,* es decir, clases que no son conjuntos y formalizan la noción de *multiplicidad inconsistente* de Cantor. Su relación con ZFC es que toda sentencia que no mencione clases propias es demostrable en ZFC si y sólo si es demostrable en NBG. En particular la consistencia de NBG es equivalente a la de ZFC.

Nuevos fundamentos Los *nuevos fundamentos* de Quine NF es una teoría de conjuntos con un axioma de formación de conjuntos que permite definir el conjunto de todos los conjuntos o el conjunto de todos los ordinales, al precio de prohibir la existencia de otros conjuntos naturales, como la aplicación que a cada conjunto x le asigna el conjunto $\{x\}$. En incompatible con el axioma de elección.

Nombre Si M es un modelo transitivo numerable de ZFC y $\mathbb{P}$ es un conjunto de condiciones, los nombres son ciertos conjuntos $a \in M$ tales que, fijado un filtro genérico G, determinan un conjunto a_G, de modo que estos conjuntos forman la extensión genérica $M[G]$. En las formulaciones antiguas, los nombres eran términos del *lenguaje del forcing,* un lenguaje formal con una sintáxis compleja, mientras que en las formulaciones modernas los nombres se definen por recursión transfinita sobre el rango de un conjunto. Un conjunto b es un nombre si y sólo si sus elementos son de la forma (a, p), donde a es un nombre y $p \in \mathbb{P}$.

Numerable Un conjunto A es *numerable* si existe una aplicación biyectiva $f : \mathbb{N} \longrightarrow A$. Ejemplos de conjuntos numerables son $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, mientras que $\mathbb{R}$ y $\mathbb{C}$ son no numerables. Si A y B son conjuntos numerables, $A \times B$ también lo es. Admitiendo el axioma de elección, toda unión numerable de conjuntos numerables es numerable.

Ordenado (conjunto) Un *conjunto (parcialmente) ordenado* es un conjunto A en el que hay definida una relación $\leq$ que, para todos los elementos a, b, c de A, cumple 1) $a \leq a$ 2) si $a \leq b$ y $b \leq a$, entonces $a = b$ y 3) si $a \leq b$ y $b \leq c$, entonces $a \leq c$.

Dos elementos $a, b \in A$ se dicen *comparables* si $a \leq b$ o $b \leq a$. Si todos los elementos de A son comparables, se dice que la relación de orden es *total,* o que A es un conjunto totalmente ordenado.

Ordinal En su sentido más amplio, Cantor llegó a llamar ordinales a las distintas formas de ordenar conjuntos, de modo que dos conjuntos ordenados tienen el mismo ordinal si y sólo si existe una biyección entre ellos que conserva el orden.

Pero actualmente se llama *ordinales* a lo que Cantor llamaba *números ordinales,* que representan las formas de ordenar bien un conjunto (véase BUEN ORDEN), de modo que dos conjuntos bien ordenados tienen el mismo ordinal si y sólo si existe una biyección entre ellos que conserva el orden (y entonces se dice que son *similares*).

En la actualidad se llama ordinales a los *ordinales de von Neumann,* que son unos conjuntos concretos de modo que cada conjunto bien ordenado es similar a un único ordinal. De acuerdo con esta definición, cada ordinal de von Neumann es el conjunto de los ordinales menores que él. Por ejemplo:

$$0 = \varnothing, \quad 1 = \{0\}, \quad 2 = \{0, 1\}, \quad 3 = \{0, 1, 2\}, \quad \ldots$$

Los ordinales finitos coinciden con los números naturales. El primer ordinal infinito es ω, que coincide con el conjunto de todos los números naturales.

Los ordinales pueden ser de tres tipos: el 0 (que no tiene anteriores), los *ordinales sucesores* (que tienen un inmediato anterior) y los *ordinales límite* que tienen anteriores, pero no un inmediato anterior, como es el caso de ω.

Peano (aritmética de) La aritmética de Peano (de primer orden) es una teoría axiomática cuyo lenguaje incluye los signos específicos $0, S, +, \cdot$ (para nombrar al cero, la operación siguiente y la suma y el producto de números naturales) y cuyos axiomas son los que se indica en la página 60.

Peano (axiomas de) Los *axiomas de Peano* son los axiomas con los que Dedekind y Peano caracterizaron a los números naturales: 1) el 0 es un número natural [en realidad, Dedekind y Peano tomaban al 1 y al 0 como primer número natural], 2) el sucesor de un número natural es otro número natural, 3) Si dos números naturales son distintos, sus siguientes también son distintos, 4) El 0 no es el siguiente de ningún número natural, 5) el principio de inducción.

No obstante, también es habitual que se llame *axiomas de Peano* a los axiomas de la ARITMÉTICA DE PEANO de primer orden (véase la entrada correspondiente).

Perfecto (conjunto) Cantor definió un conjunto *perfecto* como un conjunto que coincide con su derivado o equivalentemente, como un cerrado sin puntos aislados.

Platonismo El *platonismo* es la doctrina que considera que las afirmaciones matemáticas pueden ser interpretadas literalmente. Por ejemplo, si se demuestra que $\mathbb{R}$ es no numerable, eso quiere decir que existe (en un sentido adecuado de la palabra "existir", distinto de la existencia física) un conjunto $\mathbb{R}$ que tiene la propiedad de que no es numerable. Se opone a quienes consideran que sólo una parte de las afirmaciones matemáticas tienen un significado real, mientras que otras son como una

novela de ficción, que habla de personajes que no existen realmente. Esto incluye a los finitistas (que sólo atribuyen un significado real a las afirmaciones que puedan interpretarse en términos de conjuntos finitos) y otras posiciones que pueden poner más o menos lejos la frontera de la matemática significativa, como los intuicionistas, o quienes admiten la realidad objetiva de afirmaciones con un contenido intuitivo preciso, no necesariamente finitista, pero a quienes no se les puede llamar "intuicionistas" porque no niegan la validez de la lógica clásica ni rechazan la matemática sin contenido intuitivo.

Potencia Cantor llama *potencia* de un conjunto a su cardinal. Véase también MINUSPOTENCIA, EQUIPOTENCIA.

Predicativismo El *predicativismo* es la doctrina que rechaza las definiciones *impredicativas,* es decir las definiciones que definen un concepto haciendo referencia a una totalidad a la que pertenece el objeto definido, por considerar que las definiciones impredicativas son la causa de las paradojas. Véase la sección 23 en la página 41.

Primitivo (concepto) En una teoría axiomática formal, un *concepto primitivo* es un concepto que se presenta sin definición en la teoría, cuyo comportamiento se regula mediante los axiomas. Por ejemplo, en la teoría de conjuntos ZFC los únicos conceptos primitivos son el de "conjunto" y el de "pertenencia". En la aritmética de Peano, los conceptos primitivos son "número natural", "cero", "sucesor", "suma" y "producto".

Primitivo (elemento) Un elemento primitivo en una teoría de conjuntos es un objeto que puede ser elemento de otros conjuntos, pero que él mismo no es un conjunto. Las teorías modernas de conjuntos no admiten elementos primitivos, porque son superfluos, pero basta una modificación trivial para incluirlos, si así se desea.

Proyectivo (conjunto) Los *conjuntos proyectivos* son una jerarquía de subconjuntos de $\mathbb{R}^n$ (aunque se pueden definir en una clase más amplia de espacios topológicos) construida como sigue: $\mathbf{\Sigma}^1_1$ es la clase de los conjuntos ANALÍTICOS (las imágenes continuas de los conjuntos de Borel), $\mathbf{\Pi}^1_1$ es la clase de los conjuntos *coanalíticos* (los complementarios de los conjuntos analíticos) y, en general, los conjuntos $\mathbf{\Sigma}^1_{n+1}$ son las imágenes continuas del los conjuntos $\mathbf{\Pi}^1_n$ y los conjuntos $\mathbf{\Pi}^1_{n+1}$ son los complementarios de los conjuntos $\mathbf{\Sigma}^1_{n+1}$. Los conjuntos $\mathbf{\Delta}^1_n$ son los que son a la vez $\mathbf{\Sigma}^1_n$ y $\mathbf{\Pi}^1_n$.

$\mathbb{R}$-medible (cardinal) Véase cardinal MEDIBLE.

Ramificado (lenguaje del forcing) Las formulaciones antiguas del *forcing* usaban un lenguaje ramificado, que es una extensión del lenguaje de la teoría de conjuntos que permite expresar cuantificaciones limitadas de tipo $\bigwedge_\alpha x$ o $\bigvee_\alpha x$ que se interpretan como "para todo conjunto de rango menor que α" y "existe un conjunto de rango menor que α". Esto puede materializarse en el uso de infinitos cuantificadores (uno para cada ordinal α) o mediante el uso de infinitos juegos de variables (con infinitas variables de cada rango).

Rango El *rango* de un conjunto x respecto de la JERARQUÍA de von Neumann es el menor ordinal α tal que $x \subset V_\alpha$. Si $x \in y$, entonces $\operatorname{rang} x < \operatorname{rang} y$.

Recursión transfinita El principio de recursión transfinita afirma que para definir una sucesión $\{x_a\}_{a\in A}$ sobre todos los elementos de un conjunto bien ordenado, podemos definir x_a supuesto que la sucesión ya está definida para los x_b, con $b < a$.

En el caso de los ordinales podemos distinguir casos: para definir una sucesión $\{x_\alpha\}_{\alpha<\Omega}$ sobre todos los ordinales (o hasta uno dado) basta 1) definir x_0, 2) definir $x_{\alpha+1}$ suponiendo definido x_α y 3), para cada ordinal límite λ, definir x_λ supuesto que la sucesión ya está definida para los ordinales $\delta < \lambda$.

Recursiva (función) Una función *recursiva* es una función (de n variables naturales y con valores naturales) que puede calcularse en la práctica mediante un algoritmo finito. De entre ellas, las funciones *recursivas primitivas* son las que pueden calcularse usando a lo sumo bucles FOR ... NEXT, en los que se sabe desde el principio cuántas iteraciones hay que hacer, pero no bucles de tipo WHILE, en los que no se sabe cuántas veces se repetirá la iteración.

Un concepto un poco más general es el de *función recursiva parcial,* que es una función que puede calcularse mediante un algoritmo, pero dejando abierta la posibilidad de que, para algunos valores, el cálculo no termine nunca (esencialmente, porque un bucle de tipo WHILE nunca se acaba). Las funciones recursivas parciales definidas para todos los argumentos posibles coinciden con las funciones recursivas.

Recursiva Primitiva (Aritmética) Véase ARP.

Reemplazo (axioma del) El axioma del reemplazo es el axioma que hay que añadir a la teoría de Zermelo para obtener la teoría de Zermelo-Fraenkel. Afirma que si una fórmula $\phi(x, y)$ determina un único conjunto y para cada elemento x de un conjunto a, entonces existe un conjunto b que se forma reemplazando cada elemento $x \in a$ por el conjunto y que le asocia la fórmula ϕ.

En la teoría de conjuntos NBG su formulación es mucho más sencilla. El axioma afirma que si una clase $F : a \longrightarrow X$ es una aplicación suprayectiva cuyo dominio es un conjunto a y cuya imagen es una clase X, entonces la clase X es un conjunto o, equivalentemente, que toda imagen de un conjunto por una aplicación es un conjunto.

Reflexión (teorema de) El *teorema de reflexión* afirma que, dadas unas sentencias $\phi_1, \ldots, \phi_n$, existe un conjunto transitivo numerable M de modo que las sentencias ϕ_i se cumplen en M si y sólo si se cumplen en la clase V de todos los conjuntos. Para más detalles véase la sección 85 en la página 228.

Regular (cardinal) Un cardinal infinito κ es regular si la unión de menos de κ conjuntos de cardinal menor que κ tiene cardinal menor que κ. Esto le sucede a $\aleph_0$ y a todos los cardinales sucesores. Los cardinales que no son regulares se llaman *singulares.*

Regularidad (axioma de) El axioma de regularidad afirma que todo conjunto no vacío x tiene un elemento $y \in x$ tal que $y \cap x = \varnothing$. Es equivalente a que todo conjunto aparece en la jerarquía de von Neumann, y también a que todo conjunto x está bien fundado, en el sentido de que no existen sucesiones infinitas de la forma $x = x_0 \ni x_1 \ni x_2 \ni \cdots$

Representable (función) Una función sobre números naturales es *representable* en una teoría aritmética si existe una fórmula del lenguaje de la teoría que puede demostrarse para los números naturales tales que el último es la imagen de los primeros y puede refutarse para los números naturales tales que el último no es la imagen de los primeros, y además se puede demostrar que la fórmula determina una función. Para más detalles véase la página 106.

Robinson (aritmética de) La *aritmética de Robinson* es esencialmente la aritmética de Peano sin el principio de inducción. Su interés radica, entre otras cosas, en que el primer teorema de incompletitud es válido para teorías aritméticas en el sentido débil de que permiten demostrar los axiomas de la aritmética de Robinson, sin necesidad de que en ellas se pueda demostrar el principio de inducción.

Russell (paradoja de) La *paradoja de Russell* es la contradicción que se obtiene al considerar el conjunto R de todos los conjuntos que no se pertenecen a sí mismos. Es inmediato que tal conjunto R da lugar a una contradicción tanto si suponemos que $R \in R$ como si suponemos lo contrario.

Schröder-Bernstein (teorema de) Véase CANTOR-BERNSTEIN.

Sección inicial Si A es un conjunto ordenado y $a \in A$, la *sección inicial* determinada por a es el conjunto $A_a = \{x \in A \mid x < a\}$.

Secuente En la teoría de la demostración, un *secuente* es una expresión de la forma $\gamma_1, \ldots, \gamma_m \Rightarrow \delta_1, \ldots, \delta_n$, donde γ_i y δ_j son fórmulas, y que es otra forma de expresar la fórmula $\neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n$. Sucede que la teoría de la demostración se formula mucho más eficientemente en términos de secuentes que en términos de fórmulas.

Sentencia En lógica, una *sentencia* es una fórmula que no tiene variables libres.

Similitud Una similitud entre dos conjuntos ordenados A y B es una biyección $f : A \longrightarrow B$ que conserva el orden, es decir, tal que $a_1 \leq a_2$ si y sólo si $f(a_1) \leq f(a_2)$. En tal caso se dicd que A y B son *similares.*

Singular (cardinal) Véase REGULAR (CARDINAL).

Skolem (núcleo de) Si M es un modelo infinito de un lenguaje formal y $X \subset N$, el *núcleo de Skolem* de X en M es un submodelo elemental $X \subset N(X) \prec M$ cuyo cardinal es $|N(X)| \leq \aleph_0|X|$. Véase la página 226.

Skolem (paradoja de) La *paradoja de Skolem* no es realmente una paradoja, en cuanto no es ninguna contradicción, sino que simplemente es el resultado sorprendente según el cual la teoría de conjuntos admite un modelo numerable, a pesar de que permite demostrar la existencia de conjuntos no numerables. Véase la página 63.

Submodelo (elemental) Un *submodelo* M de un modelo N es un modelo cuyo universo está contenido en el de N y de modo que las interpretaciones de los signos del lenguaje coinciden en M (ambos interpretan las constantes igual, cada relación en M es la restricción de la relación correspondiente en N y cada función de M es la restricción de la función correspondiente de N, véase la página 225). Esto equivale a que la inclusión $i : M \longrightarrow N$ es una inmersión de modelos. Si es una inmersión elemental se dice que M es un *submodelo elemental* de N, y se expresa $M \prec N$.

Supremo Si A es un conjunto ordenado y $X \subset A$, una *cota superior* de X es un $c \in A$ tal que todo $x \in X$ cumple $x \leq c$; una *cota inferior* es un $c \in A$ tal que todo $x \in X$ cumple $c \leq x$.

Un conjunto se dice *acotado (superior o inferiormente)* si tiene una cota (superior o inferior).

El *supremo* de X (si existe) es su menor cota superior, es decir, un elemento $s \in A$ que es cota superior de X y, si c es cualquier otra cota superior, entonces $s \leq c$.

El *ínfimo* de X (si existe) es su mayor cota inferior, es decir, un elemento $i \in A$ que es cota inferior de X y, si c es cualquier otra cota inferior, entonces $c \leq i$.

En la recta real, todo conjunto no vacío acotado superiormente (inferiormente) tiene supremo (ínfimo).

En el intervalo $\mathbb{I} = [0, 1]$, todo subconjunto está acotado, por lo que todo subconjunto no vacío tiene supremo e ínfimo.

Suslin (árbol de) Un *árbol* es un conjunto parcialmente ordenado A en el que, para cada $a \in A$, la sección inicial A_a (formada por los elementos anteriores a a) está bien ordenada. Un *árbol de Suslin* es un árbol de altura $\aleph_1$ en el que todas las cadenas y las anticadenas son numerables (donde una *cadena* es un conjunto de elementos comparables dos a dos y una *anticadena* es un conjunto de elementos no comparables dos a dos).

Suslin (problema de) El *problema de Suslin* plantea si todo conjunto totalmente ordenado completo, denso en sí mismo, sin máximo ni mínimo y en el que toda familia de intervalos no vacíos es a lo sumo numerable es similar a (es decir, tiene el mismo tipo de orden que) la recta real. Si se cambia la condición sobre los intervalos disjuntos por la condición de tener un subconjunto denso numerable, entonces la respuesta es afirmativa.

Un conjunto ordenado en dichas condiciones que no sea semejante a $\mathbb{R}$ recibe el nombre de *recta de Suslin.*

La *hipótesis de Suslin* es que la respuesta al problema de Suslin es afirmativa, es decir, que no existen rectas de Suslin, y es equivalente a que no existan árboles de Suslin.

Tarski (teorema de) El *teorema de Tarski de indefinibilidad de la verdad* dice que, fijado un modelo de una teoría aritmética, no existe ninguna fórmula $V(x)$ que signifique "la sentencia x es verdadera en el modelo". En particular, no existe ninguna fórmula $V(x)$ tal que, para toda sentencia metamatemática ϕ, en la teoría se pueda demostrar $V(\ulcorner\phi\urcorner) \leftrightarrow \phi$. Para más detalles véase la sección 54 en la página 110.

Tarski-Vaugh (criterio de) El *criterio de Tarski-Vaught* es un criterio que caracteriza los submodelos elementales M de un modelo N en términos exclusivamente de la satisfacción en N. La condición es que, para toda fórmula $\phi(x_0, x_1, \ldots, x_n)$ y todos los elementos $a_1, \ldots, a_n \in M$, se cumple $\bigvee a \in N\, N \vDash \phi[a, a_1, \ldots, a_n] \to \bigvee a \in M\, N \vDash \phi[a, a_1, \ldots, a_n]$.

Término En lógica, un *término* es una cadena de signos de un lenguaje formal que es susceptible de ser interpretada como el nombre de un objeto. Por ejemplo, $(x + y)z$ es un término del lenguaje de la aritmética de Peano.

Tipos (teoría de) La *teoría de tipos (ramificada)* es la lógica que crearon Whitehead y Russell para sus *Principia mathematica.* Está descrita en la sección 26 en la página 48.

Transfinito Cantor usa la palabra "transfinito" para referirse a la infinitud de los ordinales y los cardinales, con la que expresa que trascienden toda sucesión infinita, en el sentido de que si X es cualquier conjunto infinito de ordinales, o de cardinales, siempre hay otro ordinal (o cardinal) por encima de ellos. Así, aunque tengamos una sucesión infinita de ordinales, como $\omega, \omega^2, \omega^3, \ldots$, no podemos pensar que con ella estamos recorriendo todos los ordinales, sino que por encima de todos ellos habrá otro ordinal, en este caso, el mínimo es ω^ω.

Turing (máquina de) Una máquina de Turing es un modelo de ordenador con memoria potencialmente infinita que permite poner en evidencia que las funciones recursivas parciales son exactamente las que pueden calcularse con un programa de ordenador (lo que recibe el nombre de *tesis de Church-Turing*).

Ultraproducto El *ultraproducto* es una operación que permite construir un modelo a partir de una familia dada de modelos. Entre otras cosas, permite demostrar el teorema de compacidad de Gödel. Véase la sección 88 en la página 236.

Unicidad (conjunto de) Un conjunto $E \subset [-\pi, \pi]$ es un conjunto de unicidad si toda serie trigonométrica de la forma

$$f(x) = a_0 + \sum_{n=1}^{\infty} (a_n \cos nx + b_n \operatorname{sen} nx), \qquad -\pi \leq x \leq \pi,$$

que converja a una función f en $[-\pi, \pi] \setminus E$ tiene sus coeficientes unívocamente determinados. Equivalentemente, si cuando una serie converge en $[-\pi, \pi] \setminus E$ a la función nula, sus coeficientes son idénticamente nulos. Naturalmente, la definición se generaliza fácilmente a intervalos $[a, b]$ arbitrarios.

Cantor demostró en 1971 que los conjuntos finitos son conjuntos de unicidad, y sus investigaciones para entender la estructura de los conjuntos de unicidad fueron el punto de partida de la teoría de conjuntos.

Verdad Fijado un modelo M de un lenguaje formal, la relación de satisfacción $M \vDash \alpha[v]$ es la relación que afirma que lo que afirma α es cierto en M si sus signos no lógicos se interpretan como especifica M y sus variables se interpretan como indica la valoración v (que asigna a cada variable un objeto de M). Si se cumple para toda valoración v, se dice que la fórmula α es *verdadera* en el modelo M, y se representa por $M \vDash \alpha$. Para más detalles véase la sección 84 en la página 218.

von Neumann (jerarquía de) Véase Jerarquía de von Neumann.

von Neumann (ordinal de) Véase ordinal.

von Neumann (teoría de) La *teoría de von Neumann* es una teoría de conjuntos que formalizaba el concepto de "multiplicidad inconsistente" de Cantor. Era una teoría bastante atípica, porque partía de los conceptos primitivos de "función" y "argumento de función". Bernays la simplificó y la transformó en la teoría de von-Neuman-Bernays, que a su vez fue simplificada por Gödel (véase NBG).

von Neuman-Bernays (teoría de) La *teoría de conjuntos de von Neuman-Bernays* es una reformulación de la teoría de von Neumann, en la que los conceptos primitivos pasan a ser el de "conjunto", el de "clase" el de "pertenencia entre conjuntos" y el de"pertenencia de un conjunto a una clase". Fue simplificada por Gödel (véase NBG).

von Neuman-Bernays-Gödel (teoría de) Véase NBG.

Zermelo (teoría de) La *Teoría axiomática de Zermelo* es la teoría axiomática de conjuntos que consta de los axiomas que se indican en la página 46.

ZF La teoría de conjuntos de Zermelo-Fraenkel es la que resulta de añadirle a la teoría de Zermelo el axioma del reemplazo y el axioma de regularidad, pero sin incluir el axioma de elección. Si se incluye, tenemos la teoría ZFC.

Zorn (lema de) El *lema de Zorn* es una forma equivalente del axioma de elección descubierta por Hausdorff y Kuratowski que permite evitar el uso de ordinales en algunas demostraciones, y es especialmente adecuada para probar algunos resultados fundamentales en álgebra, como la existencia de base en espacios vectoriales, la existencia de clausuras algebraicas de cuerpos, etc. Véase la sección 58 en la página 121.