CONTINUIDAD Y NÚMEROS IRRACIONALES

POR EL

Sr. R. DEDEKIND

Primera edición 1872. Quinta edición 1927.

Traducción provisional y comentarios por J. Bares y J. Climent.

Dedicado a mi querido padre
Consejero áulico secreto, Profesor,
Doctor en Derecho
Julius Levin Ulrich Dedekind
con ocasión de su 50º aniversario de actividad profesional
en Brunswick, el 26 de abril de 1872

Las consideraciones que componen el objeto de este breve escrito [opúsculo] datan del otoño del año 1858. Me encontraba entonces, en tanto que profesor del Politécnico federal de Zürich, obligado por primera vez a exponer los elementos del cálculo diferencial, y sentí en esta ocasión, más vivamente todavía que antes, cuán falta está la aritmética de una fundamentación auténticamente científica. A propósito del concepto de una magnitud variable que tiende hacia un valor límite fijo y ciertamente para demostrar el teorema de que toda magnitud que crece constantemente, pero no más allá de todo límite, debe necesariamente tender hacia un valor límite, busqué refugio en las evidencias geométricas. Ahora también [Todavía hoy, considero que en el primer curso sobre cálculo diferencial, esta llamada a la intuición geométrica se revela (resulta) extremadamente útil en el plano didáctico, e incluso indispensable a quién no quiera perder demasiado tiempo], admitir de este modo a la intuición geométrica en la primera enseñanza del cálculo diferencial me parece, desde el punto de vista didáctico, extraordinariamente útil, en verdad imprescindible, si no se quiere perder demasiado tiempo. Pero nadie negará, por supuesto, que este tipo de introducción al cálculo diferencial, no puede en absoluto tener ninguna pretensión de cientificidad. Fue para mí entonces tan poderoso este sentimiento de insatisfacción [Por mi parte, este sentimiento de insatisfacción me obnubilaba entonces hasta tal punto] que tomé la firme decisión de reflexionar el tiempo que hiciera falta hasta que hubiera encontrado una fundamentación puramente aritmética y perfectamente rigurosa de los principios del análisis infinitesimal. Se dice muy frecuentemente que el cálculo infinitesimal se ocupa de magnitudes continuas, y sin embargo no se proporciona nunca una explicación de esta continuidad, e incluso la exposiciones más rigurosas del cálculo diferencial no fundamentan sus demostraciones sobre la continuidad, sino que o bien apelan, más o menos conscientemente, a representaciones geométricas, o a representaciones permitidas [sugeridas] por la geometría, o bien se apoyan en teoremas que[, por su parte,] nunca son demostrados de manera puramente aritmética. Uno de ellos es, p.ej., el teorema mencionado más arriba, y una investigación más precisa me convenció de que este teorema, o cualquier otro equivalente a él, puede [podría] ser considerado en cierto modo [cierta medida] como un fundamento suficiente para el análisis infinitesimal.

No se trataba entonces más que de descubrir su auténtico origen en los elementos de la aritmética y de conseguir [adquirir por ello mismo] con ello al mismo tiempo una auténtica [verdadera] definición de la esencia de la continuidad. Lo conseguí el 24 de noviembre de 1858 y pocos días después, comuniqué el resultado de mi[mis] reflexión [reflexiones] a mi querido amigo Durège, lo cual ocasionó una larga y animada discusión. Después he expuesto [expuse], desde luego, a algún que otro alumno esta[s] idea[s] sobre una fundamentación científica de la aritmética, y he dado una conferencia sobre este tema aquí en Brunswick en la asociación científica de los profesores, pero no podía decidirme verdaderamente a [consagrarle[s] una publicación] publicarla[s] efectivamente, porque en primer lugar la exposición no es muy fácil, y porque además el asunto es muy poco fructífero [fecundo]. Entretanto, había pensado ya más o menos, a pesar de todo, elegir este tema como objeto de mi escrito de celebración, cuando hace pocos días, el 14 de marzo, llegó a mis manos, gracias a la amabilidad de su muy estimado autor, el tratado *Los elementos de la teoría de las funciones*, de E. Heine (Crelles Journal, vol. 74), que me confirmó [animó] en mi intención. En lo esencial coincido por completo con el contenido de este escrito, como no podría ser de otro modo, pero confieso que, francamente [sinceramente], me parece que mi exposición es más simple en la forma y subraya de manera más precisa lo que es propiamente el punto central. Y mientras escribo este prólogo (20 de marzo de 1872), recibo el interesante trabajo [tratado] *Sobre la extensión de un teorema de la teoría de las series trigonométricas*, de G. Cantor (Math. Annalen de Clebsch y Neumann, vol. 5), que agradezco vivamente al agudo [a su penetrante] autor. Según constato después de una rápida lectura, el axioma del [de su] §2, aparte de la forma externa con que está revestido, coincide [concuerda] por completo [completamente] con el que yo más abajo señalo en el §3 como la esencia de la continuidad. Sin embargo, en virtud de mi concepción del dominio de los números reales como completo en sí, no consigo todavía reconocer [entrever] qué utilidad [interés] hay que atribuir a la distinción [diferenciación], salvo que sea de manera conceptual [semántica], de magnitudes numéricas reales de una especie todavía superior.

§1.

Propiedades de los números racionales.

El desarrollo de la aritmética de los números racionales se presupone ciertamente aquí, aunque me parece apropiado subrayar, sin discutirlos, algunos puntos principales [momentos claves], sólo para indicar de antemano el punto de vista que voy a adoptar en lo que sigue. Considero a la aritmética en su conjunto como una consecuencia necesaria, o al menos natural, del acto aritmético más simple, el [de] contar, y el contar mismo [la acción de contar] no es [siendo] otra cosa que la creación sucesiva de la sucesión infinita de los números enteros positivos, en la cual cada individuo se [está] define [definido] por el que le precede inmediatamente; el acto más simple [este acto simplísimo consiste en el] es el paso de un individuo ya creado a aquél que está a su vez por crear y le sigue inmediatamente. La cadena de estos números constituye ya en sí misma un instrumento extremadamente

útil [precioso] para el espíritu humano, y ofrece una riqueza inagotable en leyes maravillosas [insignes], a las que se accede por la introducción de las cuatro operaciones aritméticas fundamentales. La adición es la [reducción a un solo acto de una] repetición arbitraria del acto más simple anterior concebida como un acto único, y a partir de ella surge de la misma manera la multiplicación. Mientras que estas dos operaciones son siempre posibles [se pueden efectuar siempre], las dos operaciones inversas, la sustracción y la división, están sometidas a restricciones. Cuál ha podido ser la causa más próxima, cuáles han podido ser las comparaciones o las analogías establecidas con experiencias o intuiciones que han podido conducir a estas operaciones, no vamos a tratarlo; es suficiente considerar que precisamente esta limitación que encuentra el desarrollo de las operaciones indirectas se ha convertido en la verdadera causa de un nuevo acto de creación; así han sido creados por el espíritu humano los números negativos y fraccionarios, y se gana [conquista] en [con] el sistema de todos los números racionales un instrumento de una perfección infinitamente mayor. Este sistema, que quiero denotar [designaré por] con R, posee ante todas las cosas la propiedad de ser cerrado y completo, rasgo [propiedad] que yo he señalado en otro lugar[1] como característico de un cuerpo numérico, y que consiste en que las cuatro operaciones fundamentales siempre se pueden efectuar con cualquier par de individuos en R, i.e., que el resultado de éstas es siempre a su vez un individuo determinado en R, si se excluye el único caso de la división por el número cero.

Para nuestro fin inmediato, sin embargo, otra propiedad del sistema R es [se revela] todavía [como] más importante; que se puede expresar [y se la puede explicar] diciendo que el sistema R constituye un dominio bien ordenado, unidimensional, el cual se extiende al infinito en dos sentidos opuestos. Lo que se quiere decir con esto está señalado suficientemente por la elección de las expresiones, que están tomadas de las representaciones geométricas; tanto más necesario es subrayar las propiedades [características] puramente [estrictamente] aritméticas correspondientes, para que no se mantenga en modo alguno la impresión de que la aritmética necesite de [sea tributaria de] tales representaciones que le son ajenas.

Para expresar [indicar] que los signos a y b significan [designan] un sólo y el mismo número racional, puede establecerse tanto $a = b$ como $b = a$. La diversidad de dos números racionales a, b se muestra en [por el hecho de] que la diferencia $a - b$ tiene un valor o bien positivo, o bien negativo. En el primer caso, a se dice que es mayor que b, y que b es menor que a, lo que se denota a través de los signos $a > b$, $b < a$[2]. Puesto que en el segundo caso $b - a$ tiene un valor positivo, entonces es $b > a$, $a < b$. En relación con esta doble posibilidad en el modo de diferir valen ahora las siguientes leyes.

I. Si $a > b$, y $b > c$, entonces $a > c$. Cada vez que a y c sean dos números diferentes (o desiguales), y que b sea mayor que uno y menor que el otro, lo expresaremos brevemente, sin miedo [temer a las resonancias] ante la

[1] Vorlesungen über Zahlentheorie von P.G. Lejeune Dirichlet, 2ª. ed., §159.

[2] En lo que sigue nos referimos siempre al llamado "mayor" y "menor" algebraicos, si no se añade la palabra "absoluto"

resonancia de representaciones geométricas, así: b está situado entre los dos números a, c.

II. Si a y c son dos números diferentes, entonces hay siempre infinitos números b que están situados entre a y c.

III. Si a es un número determinado, entonces todos los números del sistema R se subdividen en dos clases, A_1 y A_2, conteniendo cada una de las cuales infinitos [una infinidad de] individuos; la primera clase A_1 comprende todos los números a_1 que son $< a$, la segunda clase A_2 comprende todos los números a_2, que son $> a$; el número a mismo puede ser atribuido a voluntad a la primera o a la segunda clase, y es entonces respectivamente el número máximo de la primera clase, o el mínimo de la segunda. En cualquier caso, la división del sistema R en dos clases A_1 y A_2 es tal que todo número de la primera clase A_1 es menor que todo número de la segunda clase A_2.

§2.

Comparación de los números racionales con los puntos de una línea recta.

Las propiedades que acabamos de subrayar [poner en evidencia] de los números racionales recuerdan a las relaciones recíprocas de posición que existen entre los puntos de una línea recta L. Si se diferencian [distinguen] los dos sentidos opuestos existentes en ella por "derecha" e "izquierda", y si p y q son dos puntos diferentes, entonces o bien p está situado a la derecha de q, y al mismo tiempo q a la izquierda de p, o bien, inversamente, q está situado a la derecha de p, y al mismo tiempo p a la izquierda de q. Un tercer caso es imposible, si p y q son de hecho [realmente] puntos diferentes. Concerniendo a esta diferencia de posición, subsisten las siguientes leyes

I. Si p está situado a la derecha de q, y q a su vez a la derecha de r, entonces p está situado también a la derecha de r; y se dice que q está situado entre los puntos p y r.

II. Si p y r son dos puntos diferentes, entonces hay siempre infinitos [una infinidad de] puntos q que está situados entre p y r.

III. Si p es un punto determinado de L, entonces todos los puntos en L se subdividen en dos clases, P_1 y P_2, conteniendo cada una de las cuales infinitos [una infinidad de] individuos; la primera clase P_1 comprende todos los puntos p_1 que están situados a la izquierda de p, y la segunda clase P_2 contiene todos los puntos p_2, que están situados a la derecha de p; el punto p mismo puede atribuirse a voluntad a la primera o a la segunda clase. En cualquier caso la división de la recta L en dos clases o partes P_1 y P_2 es tal que cada punto de la primera clase P_1 está situado a la izquierda de cada punto de la segunda clase P_2.

Como es sabido, esta analogía entre los números racionales y los puntos de una recta se convierte en una verdadera y propia correspondencia, cuando se elige en la recta un determinado punto o, de origen o punto cero, y una determinada unidad de longitud para medir los segmentos [distancias]. Con la ayuda de ésta última puede construirse para cada número racional a una longitud correspondiente, y si se transporta ésta desde el punto o hacia la derecha o hacia a la izquierda sobre la línea, según que a sea positivo o

negativo, se alcanza entonces una extremidad determinada p, que puede ser designada como el punto correspondiente al número a; al número racional 0 le corresponde al punto o. De este modo, a cada número racional a, i.e, a cada individuo en R, corresponde uno y sólo un punto p, i.e., un individuo en L. Si a los dos números a y b les corresponden, respectivamente, los dos puntos p y q, y si $a > b$, entonces p está situado a la derecha de q. A las leyes I, II, III, del parágrafo previo le [les] corresponden completamente [perfectamente] las leyes I, II, III del actual.

§3.

Continuidad de la línea recta.

Ahora, sin embargo, es muy importante el hecho de que en la línea L hay infinitos [una infinidad de] puntos que no corresponden a ningún número racional. En efecto, si el punto p corresponde al número racional a, entonces, como es sabido, la longitud op es conmensurable con la unidad de longitud invariable utilizada para efectuar la construcción, i.e., hay una tercera longitud, que se llama una medida común, y de la cual estas dos longitudes son múltiplos enteros. Pero ya los griegos de la antigüedad supieron y demostraron que hay longitudes que son inconmensurables con una unidad de longitud dada, p. ej., la diagonal del cuadrado, cuyo lado es la unidad de longitud. Si se transporta una tal longitud sobre la recta desde el punto o, entonces el punto extremo que se obtiene no corresponde a ningún número racional. Puesto que, además, se puede demostrar fácilmente que hay infinitas longitudes que son inconmensurables con la unidad de longitud, entonces podemos afirmar: La recta L es infinitamente más rica en individuos puntuales que el dominio R de los números racionales en individuos numéricos.

Si ahora se quiere, y eso es lo que se desea, deducir aritméticamente de este modo todos los fenómenos en la recta, entonces los números racionales no bastan para ello, y será por ello inevitablemente necesario refinar de manera esencial el instrumento R construido por la creación de los números racionales, creando nuevos números tales que el dominio de los números se convierta en tan completo o, como inmediatamente diremos, tan *continuo* como la línea recta.

Las consideraciones expuestas hasta ahora son tan conocidas y tan corrientes, que muchos tendrán su repetición por superflua. Sin embargo, he juzgado necesaria esta recapitulación, para preparar adecuadamente la pregunta principal. La hasta ahora usual introducción a los números irracionales alude directamente al concepto de las magnitudes extensivas –el cual sin embargo nunca se define rigurosamente– y explica el número como el resultado de la medida de una tal magnitud por una segunda de la misma naturaleza[3]. En lugar de ello exijo que la aritmética se desarrolle desde sí misma. Que tales puntos de contacto con representaciones no aritméticas han proporcionado la ocasión inmediata para la ampliación del concepto de número,

[3]La aparente superioridad que esta definición del número extrae de su generalidad desaparece inmediatamente si se piensa en los números complejos. A mi parecer, a la inversa, el concepto de la razón entre dos magnitudes de la misma naturaleza sólo puede ser desarrollado claramente cuando ya se han introducido los números irracionales.

puede concederse en general (aunque éste no ha sido seguramente el caso para la introducción de los números complejos); pero en ello no reside, desde luego, ningún motivo para admitir estas consideraciones extrañas mismas a la aritmética, a la ciencia de los números. Así como han sido construidos los números racionales negativos y fraccionarios con un libre acto creativo, y como las leyes de los cálculos efectuados con estos números deben y pueden reconducirse a las leyes de los cálculos con los números enteros positivos, del mismo modo hay que esforzarse por que los números irracionales sean definidos completamente por los números racionales solamente. Sólo que, ¿cómo?, tal es la pregunta.

La anterior comparación del dominio R de los números racionales con una recta ha llevado al reconocimiento de la lacunariedad, incompletud y discontinuidad en el primero, mientras que atribuimos a la recta completud, ausencia de lagunas, o sea continuidad. Pero ¿en qué consiste entonces propiamente esta continuidad? En la respuesta a esta pregunta debe estar contenido todo, y sólo a través de ella se proporcionará un fundamento científico para la investigación de *todos* los dominios continuos. Naturalmente, con discursos vagos sobre la conexión ininterrumpida en las partes más ínfimas no se alcanza nada; se trata de proporcionar una precisa marca característica de la continuidad que pueda ser usada como base para las deducciones efectivas. Durante mucho tiempo he reflexionado en vano sobre esto, pero finalmente encontré lo que buscaba. Este hallazgo será juzgado tal vez de manera diferente por diferentes personas, pero creo que la mayoría encontrará su contenido muy trivial. Consiste en lo siguiente. En el parágrafo anterior se ha llamado la atención sobre el hecho de que cada punto p de la recta determina una división de ésta en dos partes tales que cada punto de una parte está situado a la izquierda de cada punto de la otra. Encuentro ahora la esencia de la continuidad en la recíproca, por lo tanto en el siguiente principio:

"Si se reparten todos los puntos de la recta en dos clases, tales que cada punto de la primera clase está situado a la izquierda de cada punto de la segunda clase, entonces existe un único punto que determina esta partición de todos los puntos en dos clases, esta corte de la recta en dos partes".

Como ya se ha dicho, no creo equivocarme si supongo que todo el mundo concederá de inmediato la verdad de esta afirmación; la mayoría de mis lectores quedarán muy decepcionados al aprender que el misterio de la continuidad va a ser desvelado por esta trivialidad. Sobre este asunto haré la siguiente observación. Me alegrará que todos juzguen el principio anterior tan evidente y tan concordante con sus representaciones de una línea; pues ni yo ni nadie está en condiciones de proporcionar ninguna demostración de su corrección. La asunción de esta propiedad de la línea no es otra cosa que un axioma, en virtud del cual se reconocerá solamente para la línea la continuidad, por el cual pensamos la línea como continua. Si el espacio tiene una existencia real, entonces no debe ser necesariamente continuo; innumerables propiedades suyas permanecerían inalterables aunque fuera discontinuo. Y, desde luego, aunque supiéramos con certeza que el espacio es discontinuo, nada nos impediría, en el caso de que quisiéramos, hacerlo continuo rellenando en el pensamiento sus huecos; este relleno, sin embargo, consistiría

en la creación de nuevos individuos puntuales y debería realizarse según el principio más arriba mencionado.

§4.

Creación de los números irracionales.

Con las últimas palabras ya se ha indicado suficientemente de qué modo debe ser completado el dominio discontinuo R de los números racionales en uno continuo. En el §1 se ha subrayado (III) que cada número racional a determina una división del sistema R en dos clases A_1 y A_2 tales que cada número a_1 de la primera clase A_1 es menor que cada número a_2 de la segunda clase A_2; el número a es, o bien el número máximo de la clase A_1, o bien el número mínimo de la clase A_2. Ahora, si se ha dado una partición cualquiera del sistema R en dos clases A_1 y A_2, que sólo posee la propiedad característica de que cada número a_1 en A_1 es menor que cada número a_2 en A_2, entonces queremos, por mor de la brevedad, denominar a una tal partición una *cortadura*, y denotarla con $(A_1,\ A_2)$. Podemos decir entonces que todo número racional a determina una cortadura o, a decir verdad, dos cortaduras, a las que sin embargo no consideramos como esencialmente diferentes; esta cortadura tiene *además* la propiedad de que o bien entre los números de la primera clase existe uno máximo, o entre los números de la segunda clase existe uno mínimo. Y viceversa, si una cortadura posee también esta propiedad, entonces está determinada por este número racional que es el máximo o el mínimo.

Pero es fácil convencerse de que también existen infinitas cortaduras que no pueden ser determinadas por los números racionales. El ejemplo más inmediato es el siguiente.

Sea D un número entero positivo, pero que no sea el cuadrado de un número entero, entonces hay un número entero positivo λ tal que

$$\lambda^2 < D < (\lambda + 1)^2.$$

Si se coloca en la segunda clase A_2 cada número racional positivo a_2 cuyo cuadrado es $> D$, y en la primera clase A_1 todos los demás números racionales a_1, entonces esta partición constituye una cortadura (A_1, A_2), i.e., cada número a_1 es menor que cada número a_2. Pues si $a_1 = 0$ o a_1 es un número negativo, entonces a_1 es ya por este motivo menor que cada número a_2, porque éste es, de acuerdo con la definición, positivo; pero si a_1 es positivo, entonces su cuadrado es $\leq D$, y por consiguiente a_1 es menor que cada número positivo a_2, cuyo cuadrado es $> D$.

Esta cortadura, sin embargo, no está determinada por ningún número racional. Para demostrar esto, debe mostrarse ante todo, que no hay ningún número racional, cuyo cuadrado sea $= D$. Aunque esto es conocido desde los primeros elementos de la teoría de los números, incluiremos de todos modos aquí la siguiente demostración indirecta. Si hay un número racional cuyo cuadrado es $= D$, entonces hay también dos números enteros positivos t y u, que satisfacen la ecuación

$$t^2 - Du^2 = 0,$$

y se puede suponer que u es el mínimo número entero positivo que posee la propiedad de que su cuadrado al multiplicarse por D se transforma en el cuadrado de un número entero t. Ahora, puesto que evidentemente

$$\lambda u < t < (\lambda + 1)u,$$

entonces el número

$$u' = t - \lambda u$$

será un número entero positivo, y ciertamente menor que u. Si por otra parte se pone que

$$t' = Du - \lambda t,$$

entonces t' será un número entero positivo, y se tendrá que

$$t'^2 - Du'^2 = (\lambda^2 - D)(t^2 - Du^2) = 0,$$

lo que está en contradicción con lo que habíamos supuesto sobre u.

Con esto el cuadrado de cada número racional x es, o bien $< D$, o bien $> D$. De aquí se sigue fácilmente que ni en la clase A_1 hay un número máximo, ni en la clase A_2 hay un número mínimo. Pues si se pone que

$$y = \frac{x(x^2 + 3D)}{3x^2 + D},$$

entonces

$$y - x = \frac{2x(D - x^2)}{3x^2 + D}$$

e

$$y^2 - D = \frac{(x^2 - D)^3}{(3x^2 + D)^2}.$$

Si aquí se toma para x un número positivo de la clase A_1, entonces $x^2 < D$, y por consiguiente tendremos que $y > x$ y que $y^2 < D$, y por lo tanto y pertenece igualmente a la clase A_1. Pero si se toma para x un número de la clase A_2, entonces $x^2 > D$, y por consiguiente tendremos que $y < x$, $y > 0$ e $y^2 > D$, por lo tanto y pertenece igualmente a la clase A_2. Por esto, esta cortadura no está determinada por ningún número racional.

En esta propiedad, la de que no todas las cortaduras están determinadas por números racionales, consiste la incompletud o discontinuidad del dominio R de todos los números racionales.

Ahora, cada vez que se da una cortadura (A_1, A_2) que no está determinada por ningún número racional *creamos* un nuevo número, un número *irracional* α, que consideramos como perfectamente definido por esta cortadura (A_1, A_2); diremos que el número α corresponde a esta cortadura, o que él determina esta cortadura. Por lo tanto, de ahora en adelante, a cada cortadura determinada le corresponde un y sólo un número determinado, racional o irracional, y consideramos a dos números como *diferentes* o *desiguales* si y sólo si corresponden a dos cortaduras esencialmente diferentes.

Ahora, para obtener una base sobre la que fundamentar la ordenación de todos los números *reales*, i.e., de todos los números racionales e irracionales, debemos investigar en primer lugar las relaciones entre dos cortaduras cualesquiera (A_1, A_2) y (B_1, B_2), determinadas por dos números cualesquiera α y β. Es evidente que una cortadura (A_1, A_2) ya está completamente dada si una de las dos clases, p.ej., la primera A_1, es conocida, porque la

segunda A_2 consiste en todos los números racionales no contenidos en A_1, y la propiedad característica de una tal primera clase A consiste en que, si el número a_1 está contenido en ella, entonces también contiene a todos los números menores que a_1. Si se comparan ahora entre sí dos primeras clases A_1 y B_1, entonces puede ser 1º. que sean perfectamente idénticas, i.e., que cada número a_1 contenido en A_1 también esté contenido en B_1, y que cada número b_1 contenido en B_1 también esté contenido en A_1. En este caso también A_2 es necesariamente idéntico a B_2, las dos cortaduras son perfectamente idénticas, lo cual se escribe simbólicamente como $\alpha = \beta$ o $\beta = \alpha$.

Pero si las dos clases A_1 y B_1 no son idénticas, entonces hay en una, p.ej. en A_1, un número $a_1' = b_2'$, que no está contenida en la otra clase B_1, y que por consiguiente se encuentra en B_2; luego, ciertamente todos los números b_1 contenidos en B_1 son menores que este número $a_1' = b_2'$; y por consiguiente, todos los números b_1 también están contenidos en A_1.

Ahora, si 2º. este número a_1' es el único en A_1 que no está contenido en B_1, entonces cualquier otro número a_1 contenido en A_1 está contenido en B_1, y es por consiguiente menor que a_1', i.e., a_1' es el número máximo entre todos los números a_1, con lo que la cortadura (A_1, A_2) estará determinada por el número racional $\alpha = a_1' = b_2'$. De la otra cortadura (B_1, B_2) sabemos ya que todos los números b_1 en B_1 también están contenidos en A_1 y son menores que el número $a_1' = b_2'$ que está contenido en B_2; pero cualquier otro número b_2 contenido en B_2 debe ser mayor que b_2', porque en caso contrario sería también menor que a_1', y por lo tanto estaría contenido en A_1 y por consiguiente también en B_1; luego b_2' es el número mínimo entre todos los números contenidos en B_2, y por consiguiente también la cortadura (B_1, B_2) está determinada por el mismo número racional $\beta = b_2' = a_1' = \alpha$. Las dos cortaduras son por esto sólo inesencialmente diferentes.

Pero si hay 3º. en A_1 al menos dos números diferentes $a_1 = b_2'$ y $a_1'' = b_2''$ que no están contenidos en B_1, entonces hay también infinitos de ellos, porque todos los infinitos números que están situados entre a_1' y a_1'' (§1. II) están evidentemente contenidos en A_1, pero no en B_1. En este caso, decimos que los dos números α y β correspondientes a estas dos cortaduras esencialmente diferentes (A_1, A_2) y (B_1, B_2), son ellos también *diferentes* entre sí, y en particular decimos que α es *mayor* que β, y que β es *menor* que α, lo que expresamos en signos tanto por $\alpha > \beta$, como por $\beta < \alpha$. Al mismo tiempo ha de subrayarse que esta definición coincide completamente con la anterior, si los dos números α y β son racionales.

Son todavía posibles los casos siguientes. Si hay 4º. en B_1 un y un sólo un número $b_1' = a_2'$ que no está contenido en A_1, entonces las dos cortaduras (A_1, A_2) y (B_1, B_2) son sólo inesencialmente diferentes y están determinadas por uno y el mismo número racional $\alpha = a_2' = b_1' = \beta$. Pero, si hay 5º. en B_1 al menos dos números diferentes que no están contenidos en A_1, entonces $\beta > \alpha$, $\alpha < \beta$.

Puesto que con esto se agotan todos los casos, se sigue que de dos números diferentes, necesariamente uno debe ser el mayor, y el otro el menor, lo que entraña dos posibilidades. Un tercer caso es imposible. Esto estaba presupuesto, por cierto, ya en la elección del *comparativo* (mayor, menor) para la

denotación de la relación entre α y β; pero esta elección ha sido justificada solamente ahora, a posteriori. Es en investigaciones de este tipo, precisamente, donde uno debe poner el máximo cuidado para no caer, aunque sea con la mejor buena fe, en el error de efectuar transposiciones ilegítimas de un dominio en otro por una elección precipitada de expresiones tomada de prestado de otras representaciones ya desarrolladas.

Ahora volviendo al caso $\alpha > \beta$, resulta que el número menor β, si es racional, pertenece sin duda a la clase A_1; puesto que hay ciertamente en A_1 un número $a_1' = b_2'$ que pertenece a la clase B_2, entonces el número β, sea el número máximo en B_1 o el mínimo en B_2, es sin duda $\leq a_1$ y por consiguiente está contenido en A_1. Igualmente resulta de $\alpha > \beta$, que el número mayor α, si es racional, pertenece sin duda a la clase B_2, porque $\alpha \geq a_1'$. Si se reúnen ambas consideraciones, entonces se obtiene el siguiente resultado: Si una cortadura (A_1, A_2) está determinada por el número α, entonces un número racional cualquiera pertenece a la clase A_1 o a la clase A_2 según que sea menor o mayor que α; si el número α mismo es racional, entonces puede pertenecer a una o a la otra clase.

De aquí, en fin, se obtiene todavía el siguiente resultado. Si $\alpha > \beta$, si por consiguiente hay infinitos números en A_1 que no están contenidos en B_1, entonces hay también infinitos números que son al mismo tiempo diferentes de α y de β; cada número racional c que cumple las condiciones es $< \alpha$, porque está contenido en A_1, y es al mismo tiempo $> \beta$, porque está contenido en B_2.

§5.

Continuidad del dominio de los números reales.

Como consecuencia de las distinciones ya establecidas, el sistema $\mathfrak{R}$ de todos los números reales constituye un dominio bien ordenado unidimensional; con esto no se dice otra cosa que el que valen las siguientes leyes.

I. Si $\alpha > \beta$, y $\beta > \gamma$, entonces también $\alpha > \gamma$. Queremos decir que el número β está situado entre los números α y γ.

II. Si α y γ son dos números diferentes, entonces hay siempre infinitos números diferentes que están situados entre α y γ.

III. Si α es un número determinado, entonces todos los números del sistema $\mathfrak{R}$ se subdividen en dos clases, $\mathfrak{A}_1$ y $\mathfrak{A}_2$, cada una de las cuales contiene infinitos individuos; la primera clase $\mathfrak{A}_1$ comprende todos los números α_1, que son $< \alpha$, la segunda clase $\mathfrak{A}_2$ comprende todos los números α_2, que son mayores que α. El número α mismo puede atribuirse a voluntad a la primera o a la segunda clase, y es entonces, respectivamente, o el número máximo de la primera clase o el número mínimo de la segunda clase. En cualquier caso, la subdivisión del sistema $\mathfrak{R}$ en las dos clases $\mathfrak{A}_1$ y $\mathfrak{A}_2$ es tal que cada número de la primera clase $\mathfrak{A}_1$ es menor que cada número de la segunda clase $\mathfrak{A}_2$, y decimos, que esta división está determinada por el número α.

Por mor de la brevedad, y para no cansar al lector, omito las demostraciones de aquellos teoremas que se siguen directamente de las definiciones de los parágrafos previos.

Pero además de estas propiedades el dominio $\mathfrak{R}$ posee también la *continuidad*, i.e., es válido el siguiente teorema:

IV. Si el sistema $\mathfrak{R}$ de todos los números reales se subdivide en dos clases, $\mathfrak{A}_1$ y $\mathfrak{A}_2$ tales que cada número α_1 de la clase $\mathfrak{A}_1$ es menor que cada número α_2 de la clase $\mathfrak{A}_2$, entonces existe un y sólo un número α por el cual esa división está determinada.

Demostración. Por la división o la cortadura de $\mathfrak{R}$ en $\mathfrak{A}_1$ y $\mathfrak{A}_2$ está dada al mismo tiempo una cortadura $(A_1, A_2$ del sistema R de todos los números racionales, definida por el hecho de que A_1 contiene a todos los números racionales de la clase $\mathfrak{A}_1$, y A_2 a todos los demás números racionales, i.e., a todos los números racionales de la clase $\mathfrak{A}_2$. Sea α el número completamente determinado que determina esta cortadura $(A_1, A_2$. Ahora, si β es un número cualquiera diferente de α, entonces hay siempre infinitos números racionales c que están situados entre α y β. Si $\beta < \alpha$, entonces $c < \alpha$; luego c pertenece a la clase A_1 y por consiguiente también a la clase $\mathfrak{A}_1$, y puesto que al mismo tiempo $\beta < c$, entonces también β pertenece a la misma clase $\mathfrak{A}_1$, porque cada número en $\mathfrak{A}_2$ es mayor que cada número c en $\mathfrak{A}_1$. Pero si $\beta > \alpha$, entonces $c > \alpha$; luego c pertenece a la clase A_2 y por consiguiente también a la clase $\mathfrak{A}_2$, y puesto que al mismo tiempo $\beta > c$, entonces también β pertenece a la misma clase $\mathfrak{A}_2$, porque cada número en $\mathfrak{A}_1$ es menor que cada número c en $\mathfrak{A}_2$. Luego cada número β diferente de α pertenece a la clase $\mathfrak{A}_1$ o a la clase $\mathfrak{A}_2$, según que sea $\beta < \alpha$ o $\beta > \alpha$; por consiguiente α mismo es, o bien el número máximo en $\mathfrak{A}_1$, o bien el número mínimo en $\mathfrak{A}_2$, i.e., α es un número, y evidentemente el único, que determina la división de $\mathfrak{R}$ en dos clases $\mathfrak{A}_1$ y $\mathfrak{A}_2$, que es lo que había que demostrar.

§6.

Cálculos con los números reales.

Para reconducir cualquier cálculo con dos números reales α, β a los cálculos con números racionales, sólo hay que definir la cortadura (C_1, C_2), que debe corresponder al resultado de cálculo γ, a partir de las cortaduras (A_1, A_2) y (B_1, B_2) determinadas en el sistema R por los números α y β. Me limito aquí a desarrollar del ejemplo más simple, el de la adición.

Si c es un número racional cualquiera, entonces se le coloca en la clase C_1 si hay un número a_1 en A_1 y un número b_1 en B_1 tales que su suma sea $a_1 + b_1 \geq c$. Todos los demás números racionales c se colocan en la clase C_2. Esta partición de todos los números racionales en las dos clases C_1 y C_2 constituye evidentemente una cortadura, porque cada número c_1 en C_1 es menor que cada número c_2 en C_2. Ahora, si ambos números α y β son racionales, entonces cada número c_1 contenido en C_1 es $\leq \alpha + \beta$, porque $a_1 \leq \alpha$ y $b_1 \leq \beta$, luego también $a_1 + b_1 \leq \alpha + \beta$; además, si C_2 contuviese un número $c_2 < \alpha + \beta$, y por lo tanto $\alpha + \beta = c_2 + p$, donde p significa un número racional positivo, entonces se tendría que

$$c_2 = (\alpha - \tfrac{1}{2}p) + (\beta - \tfrac{1}{2}p),$$

lo cual está en contradicción con la definición del número c_2, porque $\alpha - \frac{1}{2}p$ es un número en A_1, y $\beta - \frac{1}{2}p$ es un número en B_1; por consiguiente cada

número c_2 contenido en C_2 es $\geq \alpha + \beta$. Luego, en este caso, la cortadura (C_1, C_2) está determinada por la suma $\alpha + \beta$. Por esta razón, no se va en contra de la definición válida en la aritmética de los números racionales, si se entiende, en todos los casos, por la suma $\alpha + \beta$ de dos números reales arbitrarios α y β el número γ que determina la cortadura (C_1, C_2). Además, si sólo uno de los dos números α y β es racional, p. ej. α, entonces es fácil convencerse que no tiene ninguna influencia sobre la suma $\gamma = \alpha+\beta$, colocar el número α sea en la clase A_1 sea en la clase A_2.

Del mismo modo que la adición, pueden definirse también las restantes operaciones de la llamada aritmética elemental, a saber la formación de las diferencias, productos, cocientes, potencias, raíces, logaritmos, y se consigue de este modo demostraciones auténticas de teoremas (como p. ej. $\sqrt{2}.\sqrt{3} = \sqrt{6}$), que no han sido, que yo sepa, hasta ahora jamás demostrados. La excesiva longitud que es de temer en las definiciones de las operaciones más complicadas residen en parte en la naturaleza del asunto, pero en su mayor parte pueden evitarse. Desde este punto de vista, es muy útil el concepto de un *intervalo*, i.e., un sistema A de números racionales, que posee la siguiente propiedad característica: Si a y a' son números del sistema A, entonces todos los números racionales que están situados entre a y a' están contenidos también en A . El sistema R de todos los números racionales, así como las dos clases de cada una de las cortaduras son intervalos. Pero si hay un número racional a_1 que es menor, y un número racional a_2 que es mayor que cada número del intervalo A, entonces se dice que A un intervalo finito; es entonces evidente que hay infinitos números de las mismas características que a_1, e infinitos números de las mismas características que a_2; todo el dominio R se subdivide en tres partes A_1, A y A_2, y hay dos números racionales o irracionales α_1 y α_2 perfectamente determinados, que pueden ser denominados respectivamente las cotas inferior y superior (o menor y mayor) del intervalo A; la cota inferior α_1 está determinada por la cortadura en la que la primera clase está constituida por el sistema A_1, y la cota superior α_2 lo está por la cortadura en la que A_2 constituye la segunda clase. De cada número racional o irracional α, que está situado entre α_1 y α_2 se dirá que está situado en el interior del intervalo A. Si todos los números de un intervalo A son también números de un intervalo B, entonces A se denomina una parte de B.

Parece ser que hay que esperar longitudes todavía más excesivas, cuando nos preocupemos después de transferir los innumerables teoremas de la aritmética de los números racionales (como p. ej. el teorema $(a+b)c = ac+bc$) a los números reales arbitrarios. Pero las cosas no son así, pronto se convence uno de que aquí todo depende de demostrar que las operaciones aritméticas poseen ellas mismas una cierta continuidad. Lo que quiero decir con esto lo expresaré bajo la forma de un teorema general:

"Si el número λ es el resultado de un cálculo efectuado sobre los números α, β, γ ..., y si λ está situado en el interior del intervalo L, entonces pueden indicarse intervalos A, B, C ..., en el interior de los cuales están situados los números α, β, γ ..., y tales que, si en el cálculo se reemplazan los números α, β, γ ... por números arbitrariamente tomados de los intervalos A, B, C ..., entonces el resultado será siempre un número situado en el interior del

intervalo L". Sin embargo, la terrible pesadez que está ligada a la formulación de un tal teorema nos convence de que aquí debe hacerse algo que vaya en ayuda del lenguaje, y esto se alcanzará de hecho del modo más perfecto, si se introducen los conceptos de *magnitudes variables*, de *funciones* y de *valores límite*, y será ciertamente lo más apropiado, fundamentar las definiciones de las operaciones aritméticas más simples en estos conceptos, lo cual, sin embargo, no puede desarrollarse más allá aquí.

§7.

Análisis infinitesimal.

Para acabar, todavía es necesario [conviene] iluminar la conexión [relación] que existe entre las consideraciones que hemos hecho hasta aquí y determinados teoremas fundamentales del análisis infinitesimal.

Se dice que una magnitud variable x, que recorre [toma] sucesivamente valores numéricos determinados, tiende hacia un *valor límite* fijo α, si, en el curso del proceso, x se mantiene situado [acaba por situarse] definitivamente entre cualquier par de números entre los cuales esté situado α mismo, o, lo que es equivalente, si la diferencia $x - \alpha$ tomada absolutamente [en valor absoluto], queda [desciende] definitivamente por debajo de todo valor dado diferente de cero.

Uno de los teoremas más importantes dice lo siguiente: "Si una magnitud x crece constantemente, pero no más allá de todo límite, entonces tiende hacia un valor límite".

Lo demuestro del modo siguiente. Según la hipótesis, hay uno, y por consiguiente también infinitos [una infinidad de] números α_2, tales que siempre se tiene que $x < \alpha_2$ [tales que x siempre permanece $< \alpha_2$]. Denoto con $\mathfrak{A}_2$ el sistema de todos estos números α_2, y con $\mathfrak{A}_1$ el sistema de todos los números α_1 restantes; cada uno de los últimos tiene la propiedad [se caracteriza por el hecho] de que, en el curso del proceso, se obtiene definitivamente que $x \geq \alpha_1$ [x se hace definitivamente $\geq \alpha_1$]; luego cada número α_1 es menor que cada número α_2, y por consiguiente existe un número α que o bien es el máximo en $\mathfrak{A}_1$, o bien es el mínimo en $\mathfrak{A}_2$ (§5, IV). Lo primero no puede ser el caso [El primer caso queda excluido] porque x nunca deja de crecer, luego α es el número mínimo en [de] $\mathfrak{A}_2$. Ahora [Pero], sea cual sea el número α_1 que se tome, finalmente se tiene en definitiva que $\alpha_1 < x < \alpha$, i.e., que x tiende al valor límite α.

Este teorema es equivalente al principio de la continuidad, i.e., pierde su validez en cuanto [tan pronto como] se contemplara [considerara aunque sólo fuera] un sólo número real en el dominio $\mathfrak{R}$ como no presente [ausente]; o expresado de otro modo: si este teorema es correcto, entonces también es correcto el teorema IV en el §5.

Otro teorema del análisis infinitesimal, igualmente equivalente a éste [y] que se utiliza aún más frecuentemente [y cuyo uso es todavía más frecuente], dice lo siguiente: "Si en el proceso de variación de una magnitud x, se puede siempre [también] indicar [asignar] para [a] cada [toda] magnitud positiva δ dada un lugar [una posición] correspondiente, a partir del cual x varía en una cantidad inferior a δ, entonces x tiende hacia un valor límite".

Este recíproco del teorema fácilmente demostrable, de que [según el cual] cada [toda] magnitud variable que tienda hacia un valor límite acaba siempre por tener valores de variación menores que cualquier magnitud positiva dada, puede ser deducido tanto del teorema anterior, como directamente [a partir] del principio de la continuidad. Tomo el último camino [Adopto la segunda vía]. Sea δ una magnitud positiva dada arbitraria (i.e., $\delta > 0$), entonces, por la hipótesis, llegará un momento a partir del cual x variará en una cantidad menor que δ, i.e., que si x posee en ese momento el valor a, entonces será en lo sucesivo siempre $x > a - \delta$ y $x < a + \delta$. Dejo de lado ahora de momento [provisionalmente] la hipótesis inicial y [no] retengo más que el hecho [lo] que se acaba de demostrar, a saber que todos los valores posteriores de la variable x están situados entre dos valores finitos [y] que se pueden indicar [asignar]. Sobre este hecho, fundamento una doble repartición de todos los números reales. En el sistema $\mathfrak{A}_2$ coloco un número α_2 (p. ej., $a + \delta$) si, en el curso del proceso, se tiene definitivamente que $x \leq \alpha_2$; en el sistema $\mathfrak{A}_1$ coloco cada número no contenido en $\mathfrak{A}_2$; si α_1 es un número tal, entonces, por avanzado que esté el proceso, tendrá lugar infinitamente a menudo que $x > \alpha_1$. Puesto que cada número α_1 es menor que cada número α_2, entonces hay un número α perfectamente determinado que determina [produce] esta cortadura $(\mathfrak{A}_1, \mathfrak{A}_2)$ del sistema $\mathfrak{R}$, y que denominaré el valor límite superior de la variable x que permanece constantemente [siempre] finita. Del mismo modo, el comportamiento de la variable x determina [produce] una segunda cortadura $(\mathfrak{B}_1, \mathfrak{B}_2)$ del sistema $\mathfrak{R}$: un número β_1 (p.ej., $a - \delta$) será colocado en $\mathfrak{B}_1$ si, en el curso del proceso, se tiene definitivamente que $x > \beta_1$; todo otro número β_2 a colocar en $\mathfrak{B}_2$, tiene la propiedad de que no se tiene jamás definitivamente que $x \geq \beta_2$, por lo tanto siempre se tendrá que infinitamente a menudo $x < \beta_2$; el número β que determina esta cortadura se llama el valor límite inferior de la variable x. Ambos números, α y β están evidentemente también caracterizados por la siguiente propiedad: si ε es una magnitud positiva arbitrariamente pequeña, entonces se tendrá siempre definitivamente que $x < \alpha + \varepsilon$ y $x > \beta - \varepsilon$, pero jamás se tendrá definitivamente ni que $x < \alpha - \varepsilon$ ni que $x > \beta + \varepsilon$. Ahora son posibles dos casos. Si α y β son diferentes entre sí, entonces necesariamente $\alpha > \beta$, porque siempre se tiene que $\alpha_2 \geq \beta_1$; la variable x oscila y, por avanzado que esté el proceso, sufre [experimenta] siempre (todavía) variaciones cuyo valor es superior a $(\alpha - \beta) - 2\varepsilon$, donde ε es una magnitud positiva arbitrariamente pequeña. Pero la hipótesis inicial, a la cual vuelvo [finalmente] ahora, está sin embargo en contradicción con esta consecuencia; queda por esto sólo el segundo caso $\alpha = \beta$, y puesto que ya ha sido demostrado que, tan pequeña como [por pequeña que] sea la magnitud positiva ε, se tiene siempre definitivamente que $x < \alpha + \varepsilon$ y $x > \beta - \varepsilon$, entonces x tiende hacia el valor límite α, que era lo que había que demostrar.

Estos ejemplos pueden bastar [deberían ser suficientes] para demostrar [hacer ver] la conexión [relación] entre el principio de la continuidad y el análisis infinitesimal.

[El desarrollo relacionado con este escrito clásico es tan conocido que creemos poder renunciar a las explicaciones. Por lo demás, remitimos a las

cartas a Lipschitz del 10 de julio y del 27 de julio de 1876 (LXV) que exponen las propias explicaciones de Dededind y especialmente a la concepción axiomática que ellas contienen.]

DE LAS CARTAS A R. LIPSCHITZ.

Traducción provisional y comentarios por J. Bares y J. Climent.

Brunswick, 29 de abril de 1876.

Me ha producido Vd. con su carta una alegría muy grande y al mismo tiempo muy inesperada, pues desde hace algunos años había casi perdido la esperanza de que mi exposición y concepción de una teoría general de los ideales le pudiera interesar a alguien más que a mí en estos tiempos. Con la excepción del Prof. Weber en Königsberg, que como editor de las *Obras completas* de Riemann, de próxima aparición, entró en estrecho contacto conmigo, y recientemente, motivado naturalmente por esta circunstancia, me ha dado a conocer su intención de ocuparse de esta teoría, es Vd. el primero que no se limita a manifestar su interés en el asunto, sino que lo hace de un modo tan práctico, que extraigo de ello la esperanza de no haber trabajado completamente en vano. Creí que incluir esta investigación en la teoría de los números de Dirichlet sería el medio más seguro para ganar un círculo más amplio de matemáticos para que trabajaran este campo, y yo solo me he convencido poco a poco de que la exposición misma tiene, desde luego, la culpa del fracaso de este plan. Debo sospechar que la exposición ha amedrentado a los lectores por su excesiva concisión y condensación, y por ello he utilizado desde el otoño el tiempo libre que he ganado por el cese en mi cargo de director del Politécnico de esta ciudad, para elaborar una exposición más detallada de la teoría de los ideales, en la que también he avanzado tanto, que el auténtico fundamento (del contenido del § 163) se ha conseguido en una forma algo mejorada. La modificación no es, con todo, esencial, y creo también que no son posibles grandes modificaciones, al menos en el camino emprendido por mí; las dificultades que tuve que superar hace seis años en la construcción de esta teoría general y sin excepciones, encuentran a mi juicio su fundamento interno en la circunstancia de que junto a esta teoría, que comprende todos los números enteros de un cuerpo cualquiera, circulan al mismo tiempo una infinidad de teorías que adolecen de excepciones, que siempre se refieren sólo a una parte de los números enteros (en órdenes, formas derivadas). Y esta dificultad, por la cual el proceso demostrativo se alarga mucho, la tengo por completamente inevitable. ¡Lástima! pues cada lector creerá a mitad de camino estar muy próximo a la conclusión de la demostración, y luego advertirá para su disgusto que deben añadirse nuevos recursos. Por lo demás llega luego por fin la conclusión, pero el camino es largo.

Le pido disculpas por no haberle expresado ya desde hace tiempo mi agradecimiento por su participación grata y valiosa; mi retraso, que, me temo, será para Vd. sorprendente y apenas explicable, tiene en parte su causa en la gran cantidad de asuntos y trabajos que tuve que atender justo en ese tiempo, y en parte ante todo en mi indecisión sobre el modo en que se pueden plasmar adecuadamente los pensamientos expresados por Vd. Así ha sucedido que varias veces ya he empezado a escribirle, pero luego, nuevas dudas en la realizabilidad de mis propuestas, me han llevado a desistir. Tras una ulterior y más madura reflexión me permito ahora transmitirle mi

punto de vista, con la esperanza de no haberle hecho perder el interés que Vd. tomó en el asunto a causa de mi dejadez.

El trabajo mencionado más arriba, comenzado este invierno, pero aún no terminado, que he destinado o para el *Borchardt'sche Journal* o para los *Göttinger Abhandlungen*, sería demasiado detallado para el presente fin; por otra parte sería para mí difícil de conseguir una exposición resumida parecida a la que Vd. ha elaborado sobre sus interesantísimas investigaciones sobre las ecuaciones diferenciales homogéneas para el *Bulletin*; Vd. ha conseguido muy felizmente presentar al lector una imagen sinóptica de sus investigaciones, y de un modo tan comprensible, que se estaría en todo caso en posición de reconstruir a partir de él el trabajo original. En mi asunto, sin embargo, en la naturaleza tan exactamente conocida por Vd. de la deducción en la teoría de los números, me parece inevitable la fundamentación efectiva a través de demostraciones completas; sin ella sería difícil la transmisión de un modo comprensible de los resultados fundamentales solos, y en todo caso no despertaría ningún interés. Tampoco es posible transmitir las demostraciones más o menos sólo indicativamente; si la demostración agrada o no, pende en la mayor parte de los casos de un cabello. Aunque entonces el fin a alcanzar lo tenía claro frente a mí, no obstante sólo conseguí tras esfuerzos verdaderamente indecibles, avanzar paso a paso y llenar por fin todos los huecos; tenía mientras realizaba esta tarea la sensación de que pendía de un hilo, con el temor de no conseguir alcanzar el siguiente peldaño, y si no hubiera tenido impresa o escrita ante mí mi exposición de entonces de estas demostraciones, supondría para mí ahora de nuevo un gran esfuerzo componer todos los pequeños pasos demostrativos cada uno en su lugar de nuevo, de manera que se alcanzara realmente el objetivo. Por este motivo creo firmemente que sólo una exposición completa de las demostraciones que proporcione una visión de conjunto puede interesar al lector por el tema. Si el editor del *Bulletin* quiere proceder a ello y permitirme incluso, que desarrolle algo más algunos puntos concretos, y que por el contrario elimine todo lo superficial, entonces el contenido se dispondría más o menos así.

Del §159 se mantendría la parte I, y las partes II y III serían suprimidas por completo; el §160 se mantendría con la eliminación de los números. 5 y 7; el §161 se mantendría, aunque completándolo aún algo; el §162 se mantendría esencialmente; el §163 se mantendría con una exposición cambiada, más detallada; y el §164 se mantendría.

Con ello se alcanzaría una cierta integridad , que podría ser satisfactoria, pues se habrían conseguido entonces los verdaderos fundamentos de la teoría. Esto daría más o menos 50 páginas de imprenta, quizás aún más. En verdad he llevado más adelante mis investigaciones, de las que entonces sólo se publicó una parte, tanto en general como también en su aplicación a las clases de cuerpos especiales, en la medida en que me lo ha permitido mi muy limitado tiempo en los últimos años; no se puede prever por lo tanto un auténtico final de este campo de trabajo. Si se quisiera más, podría proporcionarse una continuación, pero me parece provisionalmente adecuada la limitación anterior, y se podría dar justificadamente el título *Éléments de la théorie des idéaux* a la exposición prevista, si este plural de *ideal* es correcto. Por lo demás, ya no estaría en condiciones de elaborar yo mismo

esta exposición en lengua francesa, pues desde mi partida de Zürich me ha faltado el ejercicio necesario.

Pido ahora, estimado señor colega, que estudie mi propuesta, y en caso de que cuente con su aprobación, la transmita al editor del *Bulletin*; pero si Vd. llegara a tener la convicción de que el tipo de exposición propuesto por mí es inapropiado para los fines estrictos del *Bulletin*, le pido que me lo manifieste sin más; yo tendría entonces que renunciar a una exposición en el *Bulletin*, por muy mal que me supiera. Sea cual sea su juicio sobre esto, puede Vd. estar convencido de que le estoy sinceramente agradecido por la gran alegría que me ha proporcionado su amistosa participación; pues no soy en modo alguno insensible al reconocimiento, que viene de una parte tan competente. . . .

Brunswick, 30 de mayo de 1876.

He leído con gran interés su carta del 4 de mayo, y le expreso mi mayor agradecimiento por la participación que Vd. sigue dedicándole a mi trabajo sobre los ideales; pero estoy firmemente convencido de que Vd. vería con una luz algo diferente las relaciones entre las partes individuales del mismo y su situación con respecto a las investigaciones de otros matemáticos, si se me permitiera, tener una conversación oral detallada con Vd. sobre ello. Me es imposible seguir en lo fundamental el plan proporcionado por Vd. como propuesta, tanto respecto al ordenamiento como al contenido. Para no dejar ninguna duda sobre ello y para no tener que renunciar aún por completo a la realización de la publicación promovida por Vd., me he decidido finalmente a redactar la *Introducción* que le adjunto, en la que me esfuerzo por señalar claramente el verdadero objeto y el punto central de la teoría de los números ideales, a la exposición de los cuales me debo limitar por completo, si ésta no debe tener una inadecuada y ciertamente indeseada extensión; aun dentro de esta limitación teme ser ya demasiado largo. A la introducción que adjunto le seguirían tres capítulos:

I. Teoremas auxiliares de la teoría de los módulos (exposición algo más precisa del §161 de la teoría de los números de Dirichlet, con la demostración del teorema indicado en la última nota del mismo lugar).

II. El núcleo de la teoría de los ideales (recordatorio de la doctrina de la divisibilidad y de sus métodos de demostración en los números racionales y en los números complejos de Gauss. Comportamiento diferente en el dominio de los número de la forma $x+y\sqrt{-5}$, en los ejemplos más simples de los cuales serán explicados los conceptos fundamentales que aparecen en la teoría que sigue).

III. Teoría de los números enteros algebraicos (en la sucesión indicada en la introducción; ¡una larga cadena de teoremas!).

Espero haber escrito la introducción de tal manera que de ella se desprenda una amplia justificación del plan presentado, y me alegraría mucho, conseguir también su aprobación para éste, pues no podría proceder a un cambio y tendría en ese caso que renunciar por completo a la realización. . . .

10 de junio de 1876

... Estoy muy lejos de tomar a mal las observaciones que Vd. hace sobre mi "Introducción" [XLVIII]; por el contrario, me alegra mucho la sincera comunicación de sus dudas y el interés en el tema, que se expresa claramente en las mismas. Pero espero también que Vd. no atribuya a una obstinación tenaz si yo, tras una ocupación prolongada durante veinte años con estos pensamientos no comparto sus dudas y no puedo decidirme a hacer aún más concesiones admitiendo cambios en esta introducción, en la que he escrito cada palabra sólo tras la más cuidadosa reflexión. Mi esfuerzo en la teoría de los números tiene como fin, apoyar la investigación, no en formas de exposición o expresiones ocasionales, sino en simples conceptos fundamentales, y a través de ello –si bien esta comparación puede sonar quizás presuntuosa– conseguir algo parecido en este dominio a lo que Riemann en el dominio de la teoría de funciones, donde no puedo omitir la observación incidental, de que los principios riemannianos no son empleados de manera consecuente por la mayoría de los escritores, p.ej. también en la más recientes obras sobre funciones elípticas; casi siempre la simple teoría queda desfigurada por la mezcla de formas de exposición innecesarias, que a pesar de todo estrictamente deberían ser sólo resultado, no medios auxiliares de la teoría. De un modo parecido desfiguro en la introducción el concepto de un cuerpo finito Ω porque proporciono una forma de exposición en la que están contenidos todos los números del cuerpo y que podría ser cambiada igualmente bien por infinitas otras formas de exposición, si en lugar del número θ de allí se tomaran otros números del mismo cuerpo como medio de expresión; se necesita manifiestamente ya alguna reflexión o incluso una aunque ligera demostración para ver que con ello el contenido total de números del cuerpo permanece completamente inalterado.Por esto ha de anteponerse ampliamente la definición dada en la teoría de los números §159 [XLVII]: "Un cuerpo finito es aquel que sólo tiene una cantidad finita de números independientes entre sí". Pero he hecho esta concesión, para tomar prestado lo menos posible de la teoría general de los cuerpos y para enlazar con cosas generalmente conocidas ...

. . . . . .

... 3º. Con respecto a mi nota referente a los números irracionales, escribe Vd. .... "Debo dejar sentado ahora, que no niego la corrección de su definición, pero soy de la opinión de que ésta se diferencia sólo en la forma de la expresión pero no en el contenido de la que los antiguos establecieron." Sólo puedo decir que la definición establecida por Euclides V, 5, que cito en latín:

> rationem habere inter se magnitudines dicuntur, quae possunt multiplicatae sese mutuo *superare*[4],

y lo que sigue, lo tengo por exactamente tan satisfactorio como su definición. Por este motivo querría que quitara ciertamente la afirmación de que teoremas como $\sqrt{2}.\sqrt{3} = \sqrt{6}$ no hayan sido demostrados hasta ahora. Pues creo que los lectores franceses en especial tendrán conmigo el convencimiento de que el libro citado de Euclides contiene los principios que son necesarios y suficientes para la demostración de este teorema. No puedo por lo demás

[4] se dice que unas magnitudes tienen entre sí una razón, si pueden superarse mutuamente al ser multiplicadas

cerrar esta observación sin decir lo difícil que es para mí escribírsela. Estas cuestiones tocan, para usar una expresión de Jacobi, en lo más profundo a un corazón analítico, y sólo quisiera que no me lo tomara a mal.

En este punto fui interrumpido ayer (viernes) por la tarde por una visita, y por eso se ha retrasado mi respuesta. —En primer lugar le pido otra vez que esté convencido de que en este asunto no soy en modo alguno susceptible; no he pretendido nunca que mi concepción de los números irracionales tenga un valor especial, en otro caso no la habría retenido para mí alrededor de catorce años; por el contrario, siempre he estado convencido de que todo matemático bien formado de nuestro tiempo, que por una vez se propusiera la tarea de resolver este asunto de modo riguroso, también llegaría con toda seguridad a la meta; al mismo tiempo estoy bastante lejos de hacer un reproche eventualmente a los matemáticos que no se plantean esta pregunta en general; cada uno de ellos tendrá justificadamente el sentimiento inequívoco de que él podría hacerlo sólo con que quisiera y se tomara el trabajo de dedicarle tiempo a ello; por esto, aunque no soy en absoluto insensible a la alabanza y la censura, realmente no me sentiré ofendido en este caso si se me deniega a mí mismo el pequeño mérito que creo tener en ello. Sin embargo quiero, puesto que el asunto realmente me interesa mucho, permitirme exponerle los motivos por los que no puedo adherirme a su punto de vista. Presupongo en esto como base, sobre la que es necesario naturalmente haberse puesto de acuerdo, la aritmética de los números racionales firmemente fundamentada y nada más; en mi escrito señalo, sin ninguna intromisión de cosas ajenas, que en el dominio mismo de los números racionales se puede indicar un fenómeno (la cortadura), que puede usarse para completar este dominio con una única creación de nuevos números irracionales, y demuestro que el dominio así generado de todos los números reales posee la propiedad, en la que veo la esencia de la continuidad (§ 3) (si no se quiere introducir ningunos números nuevos, no tengo nada en contra; el teorema por mí demostrado (§5, IV) reza entonces así: el sistema de todas las cortaduras en el dominio de por sí discontinuo de los números racionales constituye una multiplicidad continua); señalo además (§6) que la adición de cada dos números reales es definible con toda precisión, y afirmo, que lo mismo vale para las restantes operaciones, y que apoyado en esto se pueden demostrar también con todo rigor los teoremas en los que consiste el edificio de la aritmética. Naturalmente, estas últimas afirmaciones me comprometen, de modo que si alguien dudara aún de la demostrabilidad de un teorema desde mis principios, yo puedo proporcionarle verdaderamente esta demostración. Al mismo tiempo afirmo que estos teoremas de la aritmética en gran parte (en realidad casi todos) hasta ahora no han sido demostrados y para hacer lo más patente posible la contradicción digo que el teorema $\sqrt{2}.\sqrt{3} = \sqrt{6}$ no ha sido nunca demostrado hasta ahora. Si alguien quiere contradecirme en esto, querrá afirmar también que el teorema ya está demostrado, y por lo tanto la carga de la prueba reside ahora en el otro y él debe indicarme una demostración realmente publicada de este teorema o de uno que lo implique. Ahora bien, ¿cree Vd. realmente que una tal demostración se encuentra en libro alguno? Naturalmente he examinado en este punto toda una cantidad

de obras de las diferentes naciones, y ¿qué se encuentra allí? No otra cosa que los más groseros argumentos circulares, más o menos así: $\sqrt{a}.\sqrt{b}$ es $= \sqrt{ab}$, porque $(\sqrt{a}.\sqrt{b})^2 = (\sqrt{a})^2.(\sqrt{b})^2 = ab$; no adelantan la más mínima explicación del producto de dos números irracionales, y sin la menor vacilación se toma en consideración el teorema $(mn)^2 = m^2n^2$ demostrado para los números racionales m y n también para los números irracionales. Ahora bien, ¿no es verdaderamente indignante que la enseñanza de la matemática en las escuelas se tenga como un medio especialmente sobresaliente de formación de la razón, mientras que sin embargo en ninguna otra disciplina (como p.ej. la gramática) tales burdas infracciones contra la lógica no serían permitidos ni un instante? Séase al menos honesto si es que no se quiere proceder científicamente o también si no se puede por falta de tiempo, y reconózcase esto abiertamente al alumno, que sin más está muy inclinado a creer un teorema bajo la palabra del profesor; esto es mejor que aniquilar con demostraciones aparentes el sentido puro y noble para las verdaderas demostraciones.

Creo ahora verdaderamente que con lo anterior ya me he justificado ampliamente; pero no quiero salir tan bien librado de esto y quiero abordar el giro completamente diferente que Vd. ha dado a la pregunta; Vd. no afirma que se encuentre en algún lugar una demostración estricta del teorema anterior, sino que expresa el punto de vista de que en la conocida y con derecho admirada definición euclídea de razón (ratio, λογος) de magnitudes homogéneas, así como en el contenido restante del quinto libro de los Elementos estarían contenidos los principios que son necesarios y suficientes para la demostración del teorema. Aparte de que no me agrada, como ya he señalado más arriba, la introducción de las magnitudes en la teoría pura de los números, debo declararme decididamente contra este punto de vista; la base mencionada no es, en mi opinión, suficiente si no se añade a los principios euclídeos además el punto central de mi escrito, en modo alguno contenido en Euclides, la esencia de la continuidad (§4). La definición de Euclides dice en nuestro modo de expresión lo siguiente: las magnitudes homogéneas A y B guardan la misma razón que las magnitudes homogéneas A_1 y B_1 si para cada par de números enteros racionales m y n o bien se dan simultáneamente $nA < mB$ y $nA_1 < mB_1$, o bien se dan simultáneamente $nA > mB$ y $nA_1 > mB_1$. Si esta definición ha de tener algún sentido, se han de presuponer únicamente dos cosas sobre las cosas llamadas magnitudes:

1º. De cada dos magnitudes diferentes y homogéneas siempre se reconocerá a una como la mayor y a otra como la menor.

2º. Si A es una magnitud, y n un número entero, hay siempre una magnitud nA homogénea con A, el múltiplo correspondiente al número n de A.

Por lo demás no se observa, fuera de ese presupuesto hecho tácitamente y contenido en sus palabras latinas (le pido que me escriba ¿por qué subraya Vd. la palabra *superare* tan significativamente?)[5] nada sobre la extensión o

[5][Lipschitz responde aquí: "he subrayado la palabra *superare* porque Euclides se abre la posibilidad con ella de considerar las razones entre magnitudes que no tienen entre sí la razón de dos números enteros". Continúa luego con las palabras citadas por Dedekind en la carta siguiente (pag. 476 ss.): la . . . definición de la igualdad de los razones . . . E.N.]

multiplicidad de un dominio de magnitudes homogéneas, y la definición dice sólo cuándo dos individuos presentes en un dominio de magnitudes guardan la misma razón que otros dos. Sin embargo, concedo de buen grado por lo demás, que la razón puede valer como definición general de un número, aunque Euclides nunca usa ἀριθμος y λογος como sinónimos. Ahora, p. ej., si A es una magnitud determinada, el conjunto de todos los múltiplos nA forma un dominio de magnitudes, que satisface por sí solo ya los anteriores presupuestos, y no se encuentra en este libro de Euclides la menor indicación de que puedan existir dominios de magnitudes aún más completos: un tal dominio de magnitudes llevaría claramente a través de la razón entre dos cualesquiera de estas magnitudes a la definición de todos los números racionales; y este dominio numérico tampoco se extendería más aunque se pase a dominios de magnitudes un nivel más completos, que consisten en todas las partes propias (Definición 1) de una determinada magnitud y de las magnitudes múltiplos de ella y por lo tanto todas las magnitudes conmensurables con una magnitud. Un tal dominio posee ya una muy respetable multiplicidad de gradaciones de magnitudes y sería muy fácil que nadie llegara a exigir dominios aún más completos. El concepto de número como razón de magnitudes homogéneas nunca iría entonces más allá de lo racional. Ahora cualquiera dirá: si Euclides no hubiera querido tomar en consideración más que tales dominios de magnitudes, entonces no le hubiera sido necesario hacer tan complicada su definición de razón, podría haber dicho simplemente: la razón de A a B es igual a la de A_1 a B_1, si hay dos números enteros m y n, tales que se da la mismo tiempo que $nA = mB$ y que $nA_1 = mB_1$. Por lo tanto se entiende por sí mismo que Euclides ha tenido en perspectiva dominios de magnitudes más completos; y de hecho se trata en el libro X también de magnitudes inconmensurables, a cuyas nuevas razones corresponden por ende nuevos números, los irracionales. Pero no se encuentra en ninguna parte ni en Euclides ni en un escritor posterior la realización de una tal complección, el concepto de un dominio de magnitudes continuo, i.e., el más completo pensable, cuya esencia consiste en la propiedad: "si se reparten todas las magnitudes de un dominio de magnitudes con una gradación continua en dos clases tales que cada magnitud de la primera clase es menor que cada magnitud de la segunda clase, entonces existe, o bien una magnitud máxima en la primera clase, o bien una mínima en la segunda clase". Si esta propiedad no se recoge explícitamente en el concepto de dominio de magnitudes, entonces queda incompleto el dominio numérico correspondiente, y son ya imposibles definiciones de las operaciones aritméticas con validez general, justo porque en tales dominios numéricos discontinuos la suma, diferencia, etc. de dos números realmente existentes allí quizás no exista. Claro está que si se renuncia a una definición general de la adición, sustracción, multiplicación y división, sólo se necesita decir: entiendo como el producto $\sqrt{2}.\sqrt{3}$ el número $\sqrt{6}$, y por consiguiente $\sqrt{2}.\sqrt{3} = \sqrt{6}$, q.e.d. Esto sería sólo el extremo más patente de un modo de proceder en sí pensable, pero desde luego, en modo alguno recomendable, en el que una operación, p.ej. la multiplicación, sería definida siempre de nuevo, en cuanto tienen que sometérsele nuevos números. Por todo esto sostengo mi afirmación de que los principios euclídeos solos, sin el añadido del principio de continuidad,

que no está contenido en ellos, son incapaces de fundamentar una doctrina completa de los números reales como las razones entre magnitudes; y tengo la observación provocadora de que el teorema $\sqrt{2}.\sqrt{3} = \sqrt{6}$ no está demostrado, no sólo por verdadera, sino también por útil. Por el contrario, sin embargo, mi teoría de los números irracionales crea el modelo perfecto de un dominio continuo, que precisamente por eso es capaz de caracterizar a cada razón entre magnitudes por un determinado individuo numérico contenido en él. –Y ahora le pido que disculpe una pregunta franca a mi corazón analítico: ¿No es verdad, que el punto de vista expresado por Vd. en 3º sobre la relación de mis principios con los Elementos de Euclides es hasta ahora sólo una conjetura, cuyo acierto no ha comprobado Vd. mismo hasta el fundamento más profundo? en caso contrario le estaría muy agradecido, si me comunicara una fundamentación de su punto de vista. . . .

27 de julio de 1876.

. . . Aunque tengo ahora, como ya le he dicho, pocas esperanzas de que nos pongamos de acuerdo, porque apenas tenemos algo nuevo que ofrecernos el uno al otro, y aunque sería quizás más apropiado demorar la discusión hasta que su obra [trabajo] esté acabada [finalizado], en el caso de que entonces aún se pudiera presentar una ocasión [otro motivo] para la continuación de nuestro debate, le pido sin embargo que, tras su segunda carta, me conceda también por segunda vez la palabra [le estaría no obstante agradecido si me dejara también replicar a su segunda carta], pues quisiera subrayar una vez más lo más claramente posible su posición frente a la mía [mi punto de vista por oposición al suyo]. En primer lugar, quisiera de buen grado defenderme contra una afirmación suya, de la que me parece desprenderse, que Vd. me sigue atribuyendo constantemente una opinión incorrecta sobre el *valor* de mi escrito sobre la continuidad, mientras que yo, sin embargo me he expresado sobre ello en mi última carta dirigida a Vd. de tal modo que creía haber despejado [disipado] cualquier duda. Después de tratar [discutir] sobre el ejemplo de la $\sqrt{2}$ añade Vd. las palabras: "también esto nos lo han enseñado los antiguos, y, ¿tiene la definición de su cortadura un contenido diferente de esto? Creo que no. [En lo que concierne a lo] Lo que Vd. menciona de la completud del dominio, que es deducido de sus principios, esto mismo coincide de hecho [esto coincide en esta cuestión] con la propiedad fundamental de una línea, sin la que ningún hombre [nadie] podría representarse una línea". La primera mitad de este *passus [pasaje]*, a la que me refiero exclusivamente en primer lugar [sobre la cual me concentro en primer lugar], suena ahora exactamente como si Vd. [da exactamente la impresión de que Vd.] me atribuyera la opinión [idea] de que yo hubiera observado y destacado [encontrado y puesto en evidencia] por primera vez el fenómeno, que principalmente por mor de la *brevedad*, porque es mencionado tan frecuentemente en mi escrito, yo habría denotado con un nombre especial –cortadura–. Le pido que descarte por completo esa suposición [hipótesis]; nunca he creído haber sacado a la luz en mi escrito ni un solo nuevo fenómeno ni ningún nuevo objeto [propio para la] de la investigación matemática. El fenómeno de la cortadura es introducido [mencionado] ciertamente en casi todos los manuales de aritmética cuando se trata de representar números irracionales [mediante una aproximación arbitraria por números racionales] con una aproximación

tan pequeña como se quiera a través de números racionales (con lo que desde luego se comete siempre un error lógico importante). Tampoco he pretendido haber creado con mi definición de los números irracionales ningún número, que no hubiera sido ya antes concebido más o menos claramente en la mente [el espíritu] de todo matemático; esto se desprende de mi declaración expresa (p. 10 y 30) de que la completud o continuidad (A) del dominio numérico real, alcanzada [obtenida] con mi definición de los números irracionales, es esencialmente equivalente al teorema (B) reconocido y empleado por todos los matemáticos: "Si una magnitud crece continuamente [de manera constante], pero no más allá de todo límite, [entonces] se aproxima a un valor límite". Asimismo, he señalado expresamente (p.18) que no creo decirle a nadie nada nuevo con el teorema (C): "se reparten todos los puntos [Si todos los puntos]... produce en dos trozos [partes]". Tampoco, en fin, tengo por nuevo el teorema (D) expuesto en mi última carta dirigida a Vd.: "se reparten todas las magnitudes [Si todas las magnitudes]... una magnitud mínima [una magnitud que es la mínima en ala segunda clase]". La tendencia en [del] conjunto de mi escrito, que creo hacer señalado [caracterizado] claramente en la introducción y en el §3 se dirige más bien sólo a demostrar con el uso del fenómeno generalmente [universalmente] conocido de la cortadura (lo cual, que yo sepa, aún no había sucedido nunca [aún no había tenido lugar en ninguna parte]), que con el único fundamento [basándose únicamente en la] de la aritmética de los números racionales, y por lo tanto sin [recurrir a] la introducción del concepto de magnitud, bastante oscuro y complicado, se pueden definir los números irracionales de un solo golpe, y, por cierto, lo que es lo más importante, [que pueden serlo] con la completud (continuidad) [que es] suficiente, y al mismo tiempo imprescindible, para la [una] construcción absolutamente rigurosa y científica de una [la] aritmética de los números reales. Que esto se ha[ya] conseguido realmente, creo que Vd., no lo discute (lo mismo vale para la exposición de los señores Heine y Cantor en Halle, que sólo se diferencia externamente de la mía); nuestra diferencia de opinión se refiere *exclusivamente* al punto de vista expresado por Vd., de que estos principios, aunque con otro ropaje, estarían sin embargo contenidos por completo en los elementos de Euclides, y Vd. repite en su última carta esta expresión en parte expresamente, en parte implícitamente al declarar en la segunda parte del *passus [pasaje]* citado más arriba que es algo sobreentendido la completud o continuidad, —sólo alrededor de la cual gira mi escrito, y debía hacerlo, si tenía que alcanzar el resultado que se proponía—, y en parte, en fin, al escribir: "La... definición de la igualdad de dos razones... lo decide todo de un solo golpe". Si Vd. no reconoce esto, sólo puedo explicármelo porque Vd. no ha tenido en cuenta que Euclides presupone en aquella definición la existencia de razones que no son iguales a la razón de dos números enteros. Vd. tiene [desde el principio] la intención de presuponer de aquí en adelante sólo números racionales y magnitudes que son medidas por números racionales. Euclides procede de otro modo en este pasaje, y éste es también el núcleo [corazón] de su diferencia con Euclides. Euclides piensa en [concibe] una magnitud [como] determinada por la medida de una línea definida nítidamente [con precisión], y desde este punto de vista puede mostrar [presentar] líneas que están, con una determinada

línea, en una razón que no puede ser expresada por dos números enteros". Sigue entonces el tratamiento [la discusión] del *ejemplo* de la razón de la diagonal con el lado del cuadrado, cuya irracionalidad (en sentido moderno) también he mencionado en mi escrito (pág. 16) como algo conocido por los antiguos griegos [griegos en la antigüedad]. Desde mis trece o catorce años conozco y admiro a Euclides, y tampoco ahora veo en qué medida mi opinión diverge de la suya; también he hablado detalladamente en mi última carta de su tratamiento de las magnitudes inconmensurables, sin ninguna objeción contra su proceder, de manera que puedo con todo derecho descartar el designio [refutar la intención] que Vd. me atribuye en lo anterior. Euclides puede aplicar su definición de razones iguales a todas las magnitudes que se le presentan [*ocurren*] en su sistema, i.e., cuya *existencia* se infiere [revela] por buenos motivos, y esto basta por completo para Euclides. Pero para el fin de querer edificar la aritmética sobre el concepto de razones entre magnitudes (que no fue el propósito de Euclides), esto no basta en absoluto; pues, más aún [al contrario], puesto que en esta [manera de fundamentar] fundamentación de la aritmética la completud del concepto de número depende exclusivamente de la completud del concepto de magnitud, y puesto que la completud continua de los números reales es imprescindible para la fundamentación científica de la aritmética, es por tanto indispensable desde un principio *saber* exactamente, cuán [hasta que punto es] completo es el dominio de las magnitudes, porque no hay nada más peligroso en la matemática que *presuponer [suponer]* existencias [la existencia de cosas] sin demostración suficiente [demostraciones suficientes], y por cierto sólo cuando la necesidad, la urgencia momentánea [inmediata] presiona a ello [lo exigen]. ¿En qué deben reconocerse las suposiciones de existencia permitidas [lícitas] y en qué deben diferenciarse de las innumerables no permitidas [ilícitas], como p.ej. la de la suposición de la existencia de una magnitud A, que es al mismo tiempo el doble de B y el triple de la mitad de B? ¿Debe depender esto sólo del éxito [de la suerte], del descubrimiento ocasional [fortuito] de una contradicción interna? Si Euclides hubiera previsto investigaciones que fueran más allá, de lo que fue en verdad el caso, es decir, aquellas en las que la *continuidad* juega un papel esencial, y si en los manuscritos se encontrara entre las definiciones o axiomas del quinto libro el *passus [pasaje]* (D) evocado más arriba, soy de la opinión de que nadie lo declararía superfluo o sobreentendido [evidente]; es más, creo que entonces entre aquellos que quieren edificar la aritmética sobre el concepto de número como razón de magnitudes, se habría encontrado ya alguien que habría reconocido y dicho: "con *esta* completud definida con precisión del concepto de magnitud está dada también la completud del concepto de número, que es suficiente e imprescindible para la construcción rigurosa de la aritmética de los números reales". Y creo que tendríamos en ese caso mejores manuales de aritmética que los que tenemos realmente [de hecho]. Pero Euclides calla por completo sobre este punto, el más importante para la aritmética, y por esto no puedo estar de acuerdo con su punto de vista de que se puedan encontrar en Euclides los fundamentos completos para la teoría de los números irracionales. Si Euclides no tuviera por superfluo, en la definición del libro quinto que Vd. en su penúltima carta ha citado en latín, nombrar [señalar] una propiedad

tan simple de las magnitudes, habría asimismo tenido que definir, a su modo, desde luego el carácter (D) mucho más complicado de la continuidad, si él lo hubiera *necesitado* en su sistema. Vd. dice, por el contrario, que esta completud o continuidad es sobreentendida [evidente] y por lo tanto no necesita ser expresada [expresamente evocada], que ningún hombre [nadie] puede pensar una *linea* sin ella, y por lo tanto sin la propiedad (C) de más arriba. Aunque este recurrir a la *geometría* para la fundamentación de la aritmética pura, como Vd. supuso en lo anterior, va completamente contra mis inclinaciones, quiero ponerme sin embargo ahora yo mismo en ese punto de vista; pero tampoco entonces puedo estar de acuerdo con Vd.; como ya expresé con precisión en la conclusión del §3 de mi escrito tras (C), *puedo* representarme todo el espacio y toda línea en él [sin excepción] como completamente discontinuos; un segundo hombre [individuo] de este tipo será desde luego el Sr. Profesor Cantor en Halle, al menos eso parece desprenderse de su trabajo citado por mí; y yo opinaría que todos los hombres pueden hacer lo mismo. Se me objetará quizás que me engaño acerca de mis capacidades de representación espaciales, que ciertamente todo el que es capaz de pensar el espacio continuo, precisamente por esto debería de ser incapaz de representárselo como discontinuo, porque desde el principio la representación de la mayor completud pensable estaría contenida en el concepto de espacio. Pero esto debo negarlo por completo [refutarlo completamente]; es más, el concepto de espacio es para mí completamente independiente, completamente separable de la representación de la continuidad, y la propiedad (C) sólo sirve para separar [discriminar] a partir del concepto *general* de espacio el *específico* del espacio continuo. ¿Y cómo queda esto en este respecto en Euclides? Si se analizan todas las suposiciones [hipótesis], tanto las hechas expresamente como las implícitas, en las que se basa el edificio completo de la geometría de Euclides, si se concede la verdad a todos sus teoremas, y la realizabilidad a todas sus construcciones (un método infalible de un tal análisis consiste para mí en reemplazar todas las expresiones técnicas por palabras arbitrarias [términos inventados cualesquiera] (hasta ahora [despojados de sentido] sin sentido), el edificio no debe derrumbarse por esto, si está bien construido, y afirmo, p. ej. que mi teoría de los números reales supera esta prueba)[6]: *nunca*, hasta donde yo he investigado, se alcanza de este modo la *continuidad* del espacio como una condición vinculada inseparablemente [indisolublemente] a la geometría de Euclides; todo su sistema se mantiene también sin la continuidad —un resultado que desde luego para muchos es sorprendente y que por eso me parecía por descontado digno de mención.

Con estas observaciones, que sólo son ulteriores aclaraciones de los pensamientos expresados en mi escrito, creo haber determinado [caracterizado] mi punto de vista tan precisamente como para no necesitar añadir nada más. Más aún, debo pedirle disculpas por la prolijidad de mis explicaciones; [pero] Vd. sabe hasta qué punto mi corazón analítico es sensible a estas cuestiones, y por esto confío [espero] en su indulgencia ...

[6] A este respecto hablar sobre Hilbert.

DE LAS CARTAS A H. Weber.

Traducción provisional y comentarios por J. Bares y J. Climent.

1876.

...pero antes déjeme explicarle, que acepto agradecidísimo su amable invitación, para, a pesar del contrato previamente cerrado, aparecer sin embargo ahora junto a Vd. con mi nombre en el título de la obra. Ciertamente, Vd. no tendría necesidad de tener remordimientos por mostrarse como el único editor, pues Vd. no sólo ha hecho la mayor parte del trabajo, sino que también ha dirigido la totalidad gracias a su completo dominio de las creaciones riemannianas de tal manera que el mundo dirá: bien hecho. Para mí esto hubiera sido completamente imposible; innumerables veces me lo he dicho en este invierno, y ante el progreso efectivo de su trabajo he visto por primera vez tan justamente, todo lo que esto implica, y cuán poco hubiera bastado para ello mi saber. He seguido su trabajo con el mayor interés, del que he aprendido mucho, y la alegría de haber llegado a una relación tan próxima con Vd. sería por sí sola una rica recompensa para mi participación en el trabajo. Ahora he reflexionado sobre su renovada petición, y encuentro tan tentador y honorable, precisamente aparecer en su compañía, que no puedo oponerme; sólo que esto debe llevarse a cabo en una forma que no deje al público ninguna duda de que Vd. es el auténtico editor; he reflexionado sobre ello y he llegado, p.ej., a la siguiente forma de título: "Obras matemáticas reunidas de Riemann. Editadas por H. Weber en unión con R. Dedekind", o "O.m.r. R. editadas por H. V. con la colaboración de R. Dedekind". Quizás consiga Vd. encontrar una forma que se ajuste aun mejor a la relación real. Además, será correcto, que Vd. firme solo el prólogo. Sin embargo, si Vd. encuentra en una reflexión más pormenorizada, que mi aparición conjunta conlleva algunas dificultades formales (¿qué dirá de ello, p.ej., Teubner?), entonces permita que volvamos a nuestro antiguo acuerdo, y esté Vd. convencido de que el sentimiento amistoso, del que ha partido su petición, me ha alegrado de corazón y ha satisfecho por completo mis pretensiones.

Puesto que he mencionado el prólogo, quisiera preguntarle si tiene Vd. previsto transmitir con algunas palabras también la historia de esta edición. Entonces habría que nombrar en particular a Clebsch, que abordó el asunto realmente con gran celo, aunque desde luego creo que él no habría investigado con tan gran cuidado el legado, como Vd. ha hecho.

Esto me lleva en primer lugar a su pregunta sobre el título de la biografía; opino que podría rezar simplemente así: "Vida de Bernhard Riemann "sin ningún añadido, y desearía que Vd. en su prólogo muy brevemente señalara más o menos lo siguiente: .[El] esbozo biográfico ha sido redactado a petición mía por R. Dedekind, fundamentalmente a partir de comunicaciones de la familia de Riemann". A ello me mueve lo siguiente: me he expresado algunas veces en tercera persona, porque tenía y tengo aún un sentimiento difuso, de que el "yo", o "a mí", o "en mi compañía" habría de perturbar algo el de otro modo sereno tono, lo cual yo quería evitar. Cuando Henle hubo leído mi manuscrito en Göttingen, me preguntó de inmediato: "¿Quiere Vd. firmar como autor? Eso no es posible si Vd. habla de sí mismo en tercera persona".

Esta fue también mi opinión, y sólo le pregunté, qué es lo que él preferiría: tercera persona con mención del autor en un lugar completamente alejado, a saber, en el prólogo, –o primera persona con mención del autor en la firma– sobre lo que él expresó inmediatamente su preferencia por el primer tipo; y a mí me parece igualmente que es lo mejor. Apartarme por completo de la narración, sería directamente antinatural; pero si yo no me expresara en primera persona, así se haría notar al lector, que yo p. ej. no hablo porque haya conocido a Riemann, y otra cosa; y yo quisiera de buen grado evitar todo lo que pudiera molestar ...

Brunswick, 8 de noviembre de 1878.

... Tu apostolado por la infinitud e irracionalidad me alegra; la conexión con la exposición de Heine (o mejor de Cantor) la he recomendado también al final del § 6; la abreviación que se alcanza con esto no es sin embargo considerable, y creo ahora incluso que para alumnos que aún no saben nada de valores límite de magnitudes variables, mi definición de la suma, diferencia, etc. es más fácil de concebir, y en una exposición apropiada no ofrece en general ninguna dificultad. De hecho, soy tan optimista como para creer que la aritmética puede ser enseñada rigurosamente también en los institutos; pues hasta ahora la clase correspondiente sólo proporciona estrictamente un excelente ejemplo de con qué facilidad se puede engañar a los alumnos, en cuanto se tiene el valor de renunciar al uso de la lógica. ¡Un importante instrumento de educación, para desarrollar las capacidades mentales de la juventud, esta aritmética, tal y como se enseña! Fick ha roto recientemente una lanza en favor de las Escuelas Técnicas, pero yo pienso de modo diferente sobre el valor de la clase de matemáticas en el bachillerato, y quizás escriba próximamente sobre ello.

Brunswick, 19 de noviembre de 1878.

... Me alegra mucho que el tema de la enseñanza de la aritmética en los institutos te interese tanto, y creo que en una conversación oral nos pondremos de acuerdo sobre ello. El libro de Schröder lo conozco a fondo; está destinado no a los alumnos, sino a los profesores. Contiene muchas cosas buenas, pero también muchas superficiales, no está destinado a ser un manual. Yo no quiero, por descontado, fatigar más las cabezas de los alumnos, sino menos. De la continuidad no necesita hablarse; pero los alumnos deben alcanzar una visión de conjunto clara del dominio de los números, en primer lugar de los números racionales; la distinción según mayor y menor (por medio de la sustracción) debe transmitírseles en carne y hueso. Entonces es cuando estarán preparados para lo irracional. Y aquí tenemos, si comprendo tu carta correctamente, quizás una diferencia de opinión. Tú escribes: "luego yo no puedo ver nada falso, si p.ej. se dice que buscar $\sqrt{2}$ significa buscar un número cuyo cuadrado se diferencie de dos tan poco como esté prescrito, y que $\sqrt{2}.\sqrt{3} = \sqrt{6}$ está entonces también demostrado". En primer lugar no me parece correcto que esté más definida la operación que el resultado de la operación; preferiría, p. ej. que la suma se defina como un número determinado completamente por los sumandos, a que se defina el sumar; esto ya en los números racionales. Ahora sin embargo piensa justo en un alumno que ha comprendido bien la aritmética racional, y al que le sea demostrado precisamente por el profesor con todo rigor que $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ no existen, ¿no

deberá confundirse, si ahora a pesar de todo se habla de $\sqrt{2}$, por cierto, no de $\sqrt{2}$ misma, sino de la búsqueda de la $\sqrt{2}$? Además, él ha aprendido en la aritmética racional, a vincular una representación completamente determinada a la palabra producto. ¿Puede él ahora entender la notación $\sqrt{2}.\sqrt{3}$? Me parece que él comprenderá mucho más fácilmente el fenómeno de una "cortadura", en la cual los números racionales que conoce bien se presentan completamente en una manera tan determinada, si caen en una u otra clase; algunos ejemplos le aclararán la esencia de este fenómeno por completo; la nitidez de este concepto es beneficiosa para su pensamiento, y no se opondrá mucho tampoco, cuando este fenómeno se emplee para la introducción de nuevos números: tantas cortaduras, tantos números. También las definiciones de las sumas, diferencias, etc de los nuevos números son muy fáciles de producir. Tú quieres, a pesar de todo, también que los alumnos aprendan a manejarse con $\sqrt{2}$, $\sqrt{3}$, etc; ahora bien, ¿quieres que los alumnos vean sólo en ello símbolos de cálculos aproximados? ¿o prefieres que vean en ello símbolos de nuevos números, tan justificados como los anteriores? ¿Cuál de las dos representaciones ayudará al pensamiento más preciso y más agudo, a ejercitar mejor la mente? Sin embargo, es difícil ponerse de acuerdo en esto por escrito.

Preguntas también por mi investigación sobre el comienzo originario de la aritmética: "¿Qué son y para qué sirven los números". Está en reposo, y dudo si la publicaré alguna vez. También está puesta por escrito sólo en un tosco esbozo, con el lema: "o que se puede demostrar, no debe ser creído en la ciencia sin demostración". El tema principal es la distinción de lo numerable y lo innumerable, y el concepto de cantidad, y la fundamentación de la llamada inducción completa ...

19 de enero de 1880

... Pero la teoría de las funciones enteras ω, la definición de $\Delta(\Omega)$ y muchas otras cosas ocasionan grandes rodeos, a mi parecer, y aun cuando no fuera así, un tal tratamiento fantasmal del cuerpo esencial Ω [7] habría de ahuyentar a cualquier otro, como a mí (¿y a tí?) en el más alto grado, y tampoco él se conformaría con la vivificación añadida de este fantasmal ω; sin embargo, yo por mi parte no tengo que objetar contra esta concepción en sí nada más que la prolijidad, y debo incluso asegurarte que la temible cerrazón en la que se muestra el cuerpo Ω y la determinación completa y rígida de cada individuo esencial particular contenido en él me agrada desde luego mucho; ¡y sería bonito, que este mundo de repente por un golpe de magia se despertara a la vida de los números! Sin embargo, no tengo nada en contra, si tú te ríes de mí justamente por mi entusiasmo.

Ahora, si no se quiere bajar a este Hades, sino permanecer siempre en la claridad solar de la vida de los números (–nos hemos acostumbrado tanto

[7] Si es dada una función irreductible $f(t) = t^n + a_1 t^{n-1} + \ldots + a_n$ con coeficientes a, que son funciones racionales de z, entonces se puede producir un sistema Ω de esencias (funciones) ω, cada una de las cuales está completamente determinada por n funciones racionales $x_0, x_1, \ldots, x_{n-1}$. Se puede establecer, por mor de la simplicidad, que debe entenderse por ω la función x_0 misma si todos los siguientes $x_1, x_2 \ldots$ desaparecen idénticamente; se entiende por ϑ la esencia que corresponde a $x_1 = 1, x_0 = x_2 = \ldots = x_{n-1} = 0$, luego tenemos ya con todo rigor que $\omega = x_0 + x_1\vartheta + x_2\vartheta^2 + \ldots + x_{n-1}\vartheta^{n-1}$ en virtud de esta definición.

ya a los números complejos, que experimentamos como claridad solar lo que para nuestros predecesores aparecía como oscuridad nocturna–), entonces se puede, para poder disfrutar también de los conjugados, proceder de manera que al principio se contemple sólo un pequeño trozo arbitrario del plano-z, sobre el cual corren la hojas de la superficie riemanniana completamente separadas unas de otras, y se investiguen las funciones ω fundamentalmente para este trozo; tómese por ϑ una de estas hojas, arbitraria, pero determinada, entonces se obtiene un cuerpo determinado de funciones correspondiente Ω, en el cual cada función ω tiene un sólo valor; cada relación entre las funciones ω contenidas en él, que se pueden expresar mediante ecuaciones racionales, llegan a tener validez en este trozo, y después se mostrará que todos los fenómenos que salen en la lejanía más lejana, ya están completamente "determinadas" y "decididas" por los fenómenos dentro de este pequeño trozo ...

30 de octubre de 1880

... Aprovecho la ocasión para expresarte mi agradecimiento más personal por el trabajo completo de alrededor de dos años que te ha causado un esfuerzo tan interminable, y en el que tomar parte me ha aportado la mayor alegría y un enriquecimiento significativo en saber; es un sentimiento hermoso completamente especial, enfrentarse así en la investigación de la verdad, lo que Pascal expresa en su primera carta a Fermat tan acertadamente: "Car je voudrais désormais vous ouvir mon coeur, s'il se pouvait, tan j'ai de joie de voir notre rencontre. Je vois bien que la vérité est la même à Toulouse et à Paris". A menudo he tenido que pensar en este fragmento en el progreso de nuestro trabajo, que tras varias oscilaciones a pesar de todos ha tomado siempre más el carácter de necesidad interna. Me alegraría de corazón si el asunto encontrara alguna aceptación, con lo que no cuento demasiado, porque los aburridos módulos desde luego arredrarán a más de uno ...

Brunswick, 24 de enero de 1888.

... Que tomes ese interés en mi escrito sobre los números, me alegra mucho; serán muy pocos, lo que lo hagan. Cantor me ha llamado la atención sobre el hecho de que él había subrayado ya la diferencia entre lo finito y lo infinito ya en 1877 (Crelle vol. 84, pág. 242), pero que no se propone ninguna reclamación por prioridad. Sobre esto se puede decir mucho; en cierto sentido tiene él ciertamente razón, y sin embargo él dudó en 1882 de la posibilidad de una definición simple y quedó muy sorprendido, cuando yo, motivado por su duda, y por deseo suyo le transmití la mía; a veces se tiene algo, sin valorar apropiadamente su valor y significación. Pero yo no tengo la menor gana de una discusión sobre la prioridad. –He leído y pensado repetidamente tus observaciones y propuestas; pero si a través de ellas se alcanzaría una simplificación y abreviación esencial, es difícil de juzgar, antes de ver lo nuevo en una exposición completa. Además debo asegurarte que hasta hora he considerado al número ordinal, y no al cardinal (cantidad) como el concepto numérico originario. Habría hecho quizás mejor en no mencionar estos nombres (ordinal, cardinal) en me escrito, pues en la gramática usual se emplean en otro sentido. Mis números ordinales, los elementos abstractos de un sistema simplemente infinito ordenado, no tienen naturalmente nada que ver con la forma adjetival de los llamados números ordinales en la gramática,

de cuya forma podría en general tomarse un fundamento para la prioridad conceptual de los números cardinales (cantidades); esta forma adjetival se usa también donde no se trata de una ordenación (por lo tanto, de mis números ordinales), p.ej., cuando se habla de las cinco partes de un segmento. El número cardinal (cantidad) lo tengo por una aplicación del número ordinal, y también en nuestro ἀριθμετίζειν se alcanza el concepto cinco sólo a través del concepto cuatro. Sin embargo, si se quiere tomar tu camino –y yo recomendaría recorrerlo alguna vez por completo–, entonces yo quisiera aconsejar, mejor no entender por número (cantidad, número cardinal) la clase (el sistema de todos los sistemas finitos semejantes entre sí) misma, sino algo nuevo (correspondiente a esta clase), que el espíritu crea. Somos de un género divino y poseemos sin ninguna duda capacidad creadora no sólo en las cosas materiales (ferrocarriles, telégrafos), sino muy especialmente en las cosas espirituales. Esto es exactamente la misma pregunta que tú formulas al final de tu carta sobre mi teoría de los irracionales, donde dices que el número irracional no sería en general ninguna otra cosa que la cortadura misma, mientras que yo señalo, el crear algo nuevo (diferente de la cortadura), que corresponde a la cortadura, y de lo que digo, que esto produce, genera la cortadura. Tenemos el derecho de atribuirnos una tal capacidad creadora, y además, por mor de la equiparación de todos los números es mucho más oportuno, proceder así. Los números racionales generan sin embargo también cortaduras, pero no consideraré al número racional desde luego idéntico a la cortadura generada por él; y también tras la introducción de los números irracionales se hablará de los fenómenos de la cortadura a menudo con tales expresiones, que les reconocen tales atributos, que empleados para los números correspondientes mismos sonarían ciertamente desacostumbrados. Algo por completo semejante vale también para la definición del número cardinal (cantidad) como clase; se dirá mucho de la clase (p.ej., que es un sistema de infinitos elementos, a saber, de todos los sistemas semejantes), lo que sin embargo se atribuiría al número mismo de muy mal grado (por pesado); ¿piensa alguien en esto, o no se olvida pronto de buena gana, que el número cuatro es un sistema de infinitos elementos? (pero que el número 4 es el hijo del número 3 y la madre del número 5 le estará presente siempre a todo el mundo). Por el mismo motivo he tenido siempre la creación de los número ideales de Kummer por completamente justificada, pero solamente si se realiza con rigor. Si además los signos lingüísticos bastan para denotar individualmente todos los nuevos individuos que se han de crear, no hace al caso; bastan siempre para denotar los individuos que surgen en cualquier investigación (limitada).

SOBRE LA TEORÍA DE LOS NÚMEROS ENTEROS ALGEBRAICOS;

POR EL

Sr. R. DEDEKIND.

Traducción provisional y comentarios por J. Bares y J. Climent.

Introducción

Como respuesta a la invitación que se me ha hecho el honor de dirigirme, me propongo, en la presente Memoria, desarrollar los *principios fundamentales* de la teoría general, libres de toda excepción, de los números enteros algebraicos, principios que he publicado en la segunda edición de las *Lecciones sobre la Teoría de los números* de Dirichlet. Pero, debido a la extraordinaria amplitud de este campo de investigaciones matemáticas, me limitaré aquí a proseguir un único objetivo, que voy a tratar de definir claramente mediante las observaciones siguientes.

La teoría de la divisibilidad de los números, que sirve de fundamento a la aritmología, ha sido ya establecida por Euclides en lo esencial; por lo menos, el teorema capital de que todo número entero compuesto puede siempre ponerse, y eso de una sola manera, bajo la forma de un producto de números todos primos, es una consecuencia inmediata del teorema demostrado por Euclides([8]), de que un producto de dos números no puede ser divisible por un número primo salvo si éste divide al menos a uno de los factores.

Dos mil años después, Gauss dio, por primera vez, una extensión de la noción de número entero; mientras que, hasta él, no se designaba bajo este nombre más que a los números 0, ± 1, ± 2, ..., que llamaré de ahora en adelante números *enteros racionales*, Gauss introdujo([9]) los números *enteros complejos*, de la forma $a + b\sqrt{-1}$, donde a y b designan números enteros racionales cualesquiera, y demostró que las leyes generales de la divisibilidad de estos números son idénticas a las que gobiernan el dominio de los números enteros racionales.

La generalización más amplia de la noción de número entero consiste en lo que sigue. Un número θ se denomina un número *algebraico* cuando satisface una ecuación

$$\theta^n + a_1\theta^{n-1} + a_2\theta^{n-2} + \ldots + a_{n-1}\theta + a_n = 0,$$

de grado finito n y con coeficientes racionales a_1, a_2, ..., a_{n-1}, a_n; se denomina un número *entero algebraico*, o más brevemente un número *entero*, cuando satisface una ecuación de la forma anterior, en la cual los coeficientes a_1, a_2, ..., a_{n-1}, a_n son todos números enteros racionales. De esta definición resulta inmediatamente que las sumas, las diferencias y los productos de números enteros son todos también números enteros; por consiguiente, un números entero α se denominará *divisible* por un números entero β, si se tiene que $\alpha = \beta\gamma$, siendo γ igualmente un números entero. Un número entero ε se llamará una *unidad*, cuando cualquier número entero sea divisible por ε. Por analogía, se debería entender por número *primo* un número

[8] Elementos, VII, 32.

[9] Theoria residuorum biquadraticorum, II; 1832.

entero α que no fuera una unidad y que sólo tuviera como divisores las unidades ε y los productos de la forma $\varepsilon\alpha$; pero es fácil de reconocer que, en el dominio de todos los números enteros que consideramos aquí, no existen tales números primos, puesto que todo número entero que no es una unidad puede siempre ser puesto bajo la forma de un producto de dos factores o más bien de un número cualquiera de factores, que son todos números enteros, pero no unidades.

No obstante, la existencia de números primos y la analogía con los dominios de los números enteros racionales o complejos empieza a mostrarse de nuevo, cuando del dominio de todos los números enteros se separa una parte infinitamente pequeña, de la manera siguiente. Si θ es un número algebraico determinado, entonces de entre las ecuaciones con coeficientes racionales, en número infinito de las que θ es raíz, hay una y sólo una,

$$\theta^n + a_1\theta^{n-1} + a_2\theta^{n-2} + \ldots + a_{n-1}\theta + a_n = 0,$$

cuyo grado es menor que el de todas las demás, y que se llama por ello *irreducible*. Si x_0, x_1, x_2, $\ldots$, x_{n-1} designan números racionales arbitrarios, entonces todos los números de la forma

$$\varphi(\theta) = x_0 + x_1\theta + x_2\theta^2 + \ldots + x_{n-1}\theta_{n-1},$$

cuyo complejo representaremos por Ω, serán también números algebraicos, y gozarán de la propiedad fundamental de que sus sumas, sus diferencias, sus productos y sus cocientes pertenecerán todos también al mismo complejo Ω; llamaré a un tal complejo Ω *un cuerpo finito de grado n*. Todos los números $\varphi(\theta)$ pertenecientes al cuerpo Ω se dividen ahora, de acuerdo con la definición anterior, en dos grandes clases, a saber, en números enteros cuyo complejo designaremos por $\mathfrak{o}$, y en números no enteros o números fraccionarios. *El problema que nosotros nos proponemos consiste en establecer las leyes generales de la divisibilidad que gobiernan a un tal sistema* $\mathfrak{o}$.

El sistema $\mathfrak{o}$ es evidentemente idéntico al sistema de todos los números enteros racionales, cuando se tiene que $n = 1$, o al de los números enteros complejos, cuando se tiene que $n = 2$ y $\theta = \sqrt{-1}$. Ciertos fenómenos que se presentan en estos dos dominios $\mathfrak{o}$ especiales se reproducen también en todo dominio $\mathfrak{o}$ de esta naturaleza; es necesario observar ante todo que la descomposición ilimitada de la que nos hemos ocupado antes, y que reina en el dominio que comprende a todos los números enteros algebraicos, no se encuentra jamás en el dominio $\mathfrak{o}$ de la especie indicada, de lo cual uno puede fácilmente asegurarse mediante la consideración de las normas. Si se entiende, en efecto, por *norma* de un número cualquiera $\mu = \varphi(\theta)$, perteneciente al cuerpo Ω, el producto

$$\mathrm{N}(\mu) = \mu\mu_1\mu_2 \ldots \mu_{n-1},$$

en el que los factores son los números conjugados

$$\mu = \varphi(\theta),\ \mu_1 = \varphi(\theta_1),\ \mu_2 = \varphi(\theta_2),\ \ldots,\ \mu_{n-1} = \varphi(\theta_{n-1}),$$

donde θ, θ_1, θ_2, $\ldots$, , θ_{n-1} designan todas las raíces de la misma ecuación irreducible de n-simo grado, entonces $\mathrm{N}(\mu)$ será siempre, como se sabe, un número racional, y no será $= 0$ salvo si $\mu = 0$; al mismo tiempo, se tiene siempre que

$$\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta),$$

siendo α y β dos números cualesquiera del cuerpo Ω. Si ahora μ es un número entero y por consiguiente un número incluido en $\mathfrak{o}$, entonces los otros números conjugados μ_1, μ_2, $\ldots$, , μ_{n-1} serán de la misma manera números enteros, y por consiguiente $\mathrm{N}(\mu)$ será un número entero racional. Esta norma juega un papel extremadamente importante en la teoría de los números del dominio $\mathfrak{o}$; en efecto, si dos números cualesquiera α, β de este dominio se denominan *congruentes* o *incongruentes* con respecto a un tercero μ, tomado como *módulo*, según que su diferencia $\pm(\alpha - \beta)$ sea o no divisible por μ, se podrá, exactamente como en la teoría de los números enteros racionales o complejos, dividir todos los números del sistema $\mathfrak{o}$ en *clases de números*, de modo que cada clase comprenda al conjunto de todos los números que son congruentes con un número determinado, el cual será el representante de esta clase, y un estudio más profundo nos enseña que el número de estas clases (con la excepción del único caso en que $\mu = 0$) es siempre finito, y además igual al valor absoluto de $\mathrm{N}(\mu)$. Una consecuencia inmediata de este resultado, es que $\mathrm{N}(\mu)$ será siempre $= \pm 1$ en el caso, y solamente en el caso, en el que μ sea una unidad. Si ahora un número del sistema $\mathfrak{o}$ se denomina *descomponible*, cuando es el producto de dos números de este sistema, no siendo ninguno de ellos una unidad, se sigue evidentemente de lo que precede que todo número descomponible puede siempre ser representado como el producto de un número finito de factores *indescomponibles*.

Este resultado corresponde aún completamente a la ley que tiene lugar en la teoría de los números enteros racionales o complejos, a saber que todo número compuesto puede ser representado como el producto de un número finito de factores primos; pero al mismo tiempo este es el punto donde la analogía, observada hasta aquí, con la antigua teoría amenaza con romperse para siempre. En sus investigaciones sobre el dominio de los números que pertenecen a la teoría de la división del círculo, y que corresponden por consiguiente a las ecuaciones de la forma $\theta^m = 1$, Kummer ha observado la existencia de un fenómeno en virtud del cual los números de este dominio se distinguen en general de aquéllos que se han considerado con anterioridad, de una manera tan completa y tan esencial, que apenas quedaba la más mínima esperanza de conservar las leyes simples que gobiernan la antigua teoría de los números. En efecto, mientras que, en el dominio de los números enteros, tanto racionales como complejos, todo número compuesto no puede ponerse *más que de una sola manera* bajo la forma de un producto de números primos, se reconoce que, en los dominios numéricos considerados por Kummer, un número descomponible puede a menudo representarse *de varias maneras, completamente diferentes entre sí*, bajo la forma de un producto de números indescomponibles, o, lo que en el fondo es lo mismo, se reconoce que los números *indescomponibles* no poseen todos el carácter de un número *primo* propiamente dicho, el cual consiste en que un número primo no puede dividir a un producto de dos o de varios factores, si no divide al menos a uno de estos factores. Pero cuanto más difícil pudiera parecer alcanzar el éxito en las investigaciones ulteriores sobre tales dominios numéricos([10]), tanto más se

[10]En la memoria: *De numeris complexis qui radicibus unitatis et numeris integri realibus constant*(Vratislaviae, 1844, §8), Kummer dijo: "Maxime dolendum videtur, quod haec numerorum realium virtus, ut in factores primos dissolvi possint qui pro eodem numero

debe reconocimiento a los esfuerzos perseverantes de Kummer, que han sido finalmente recompensados por un descubrimiento verdaderamente grande y fecundo. Este geómetra ha logrado([11]) reconducir todas las irregularidades aparentes a leyes rigurosas, y considerando a los números indescomponibles, pero desprovistos del carácter de verdaderos números primos, como productos de factores primos *ideales*, que no aparecen y no manifiestan su efecto más que combinados conjuntamente, y no aislados, ha obtenido el resultado sorprendente, de que las leyes de la divisibilidad en los dominios de números estudiados por él coinciden ahora completamente con aquéllas que gobiernan el dominio de los números enteros racionales. Todo número que no es una unidad se comporta, en todas las cuestiones de divisibilidad, tanto en un papel activo ⟦divisor⟧ como en un papel pasivo ⟦dividendo⟧, o como un número primo, o como un número formado por la multiplicación de factores primos, existentes o ideales, completamente determinados. Dos números ideales, sean primos, sean compuestos, que se convierten en dos números existentes al combinarlos con un sólo y mismo número ideal, se denominan *equivalentes*, y todos los números ideales equivalentes a un mismo número ideal determinado constituyen una *clase de números ideales*; el conjunto de todos los números existentes, que son considerados como un caso especial de los números ideales, constituye la *clase principal*; a cada clase le corresponde un sistema de una infinidad de *formas* homogéneas equivalentes, en n variables y de grado n, que son descomponibles en n factores lineales con coeficientes algebraicos; el número de estas clases es finito, y Kummer consiguió extender a la determinación de este número los principios por los cuales Dirichlet ha determinado el número de las clases de las formas cuadráticas binarias.

El gran éxito de las investigaciones de Kummer, en el dominio de la división del círculo, dio lugar a presumir que las mismas leyes subsistían en *todos* los dominios numéricos $\mathfrak{o}$ de la especie más general, de los que nos hemos ocupado antes. En mis investigaciones, que tenían por objetivo llevar la cuestión a una solución definitiva, empecé apoyándome sobre la teoría de las congruencias de orden superior, porque yo ya había observado con anterioridad que aplicando esta teoría las investigaciones de Kummer podían ser considerablemente abreviadas; pero, aunque este medio conducía hasta un punto muy próximo del objetivo de mis esfuerzos, no he podido sin embargo tener éxito por esta vía en someter ciertas excepciones aparentes a las leyes constatadas para los otros casos. No conseguí la teoría general y sin excepciones, que publiqué por primera vez en el lugar indicado con anterioridad, más que después de haber abandonado completamente la antigua aproximación más formal y haberla reemplazado por otra que parte de la concepción fundamental más simple, y fijando la mirada inmediatamente sobre el objetivo. En esta aproximación, no tengo necesidad de ninguna creación nueva, como la de *número ideal* de Kummer, y es completamente suficiente que consideremos un *sistema de números realmente existentes*, que llamo un *ideal*. Reposando la potencia de este concepto sobre su extrema

---

semper iidem sint, non eadem est numerorum complexorum, quae si esset tota haec doctrina, quae magnis adhuc difficultatibus laborat, facile absolvi et ad finem perduci posset."

[11] *Zur Theorie der complexen Zahlen (Journal de Crelle, t. 35).*

simplicidad, y siendo mi designio ante todo inspirar confianza en esta noción, voy a intentar desarrollar la sucesión de las ideas que me han conducido a este concepto.

Kummer no ha definido los números ideales, sino solamente la divisibilidad por estos números. Si un número α posee una cierta propiedad A, consistente siempre en que α satisface una o varias congruencias, entonces él dice que α es divisible por un número ideal determinado, que corresponde a la propiedad A. Aunque esta introducción de nuevos números sea del todo legítima, no obstante es de temer en principio que, por el modo de expresión que se ha elegido, en el cual se habla de números ideales determinados y de sus productos, y también por la analogía presumida con la teoría de los números racionales, uno pueda ser conducido a conclusiones precipitadas y por ello a demostraciones insuficientes, y en efecto este peligro no es siempre completamente evitado. Por otra parte, una definición exacta y que sea común a *todos* los números ideales que se trata de introducir en un dominio numérico determinado $\mathfrak{o}$, y al mismo tiempo una definición general de su multiplicación parecen tanto más necesarias, cuanto que estos números ideales no existen de ningún modo en el dominio numérico considerado $\mathfrak{o}$. Para satisfacer estas exigencias, será necesario y suficiente establecer de una vez por todas el carácter común de todas las propiedades A, B, C, ..., que siempre, y sólo ellas, sirven para la introducción de números ideales determinados, y a continuación indicar en general cómo de dos de estas propiedades A, B, a las cuales corresponden dos números ideales determinados, se podrá deducir la propiedad C que debe corresponder al producto de estos dos números ideales([12])

[12]La legitimidad o más bien la necesidad de tales exigencias, que deberían siempre imponerse en la introducción o la creación de nuevos elementos aritméticos, se hará todavía más evidente comparándola con la introducción de los números *reales irracionales*, asunto del que me he ocupado en un escrito especial (*Stetigkeit und irrationale Zahlen*; Brunswick, 1872). Admitiendo que la aritmética de los números *racionales*, cuyo conjunto designaremos por R, esté definitivamente fundamentada, se trata de saber de qué manera se deberán introducir los números *irracionales*, y definir las operaciones de adición, de substracción, de multiplicación y de división a llevar a cabo sobre esos números. Como primera exigencia, reconozco que la Aritmética debe ser mantenida exenta de toda mezcla de elementos extraños, y por esta razón rechazo la definición según la cual el número sería la razón de dos magnitudes de la misma especie; por el contrario, la definición o la creación del número irracional debe estar fundamentada únicamente sobre fenómenos que se puedan antes constatar claramente *en el dominio R*. En segundo lugar, se deberá exigir que todos los números reales irracionales puedan ser engendrados simultáneamente mediante una definición común, y no sucesivamente como raíces de ecuaciones, como logaritmos, etc. La definición deberá, en tercer lugar, ser de una naturaleza tal que permita también una definición perfectamente clara de los cálculos (adición, etc.) que se tendrán que hacer sobre los nuevos números. Se consigue todo esto de la manera siguiente, que no haré aquí más que indicar:

1.º Llamo *sección* del dominio R a una partición cualquiera de todos los números racionales en dos categorías, tal que cada número de la primera categoría sea algebraicamente menor que cada número de la segunda categoría.

2.º Todo número racional determinado a *engendra* una sección determinada (o dos secciones, no esencialmente diferentes), en virtud de lo cual cualquier número racional será clasificado en la primera o la segunda categoría, según que sea algebraicamente menor o mayor que a (mientras que a mismo podrá ser inscrito a voluntad en una u otra de las dos categorías).

Este problema es esencialmente simplificado por las siguientes reflexiones. Puesto que una tal propiedad característica A sirve para definir, no un número ideal mismo, sino solamente la divisibilidad de los números contenidos en $\mathfrak{o}$ por un número ideal, uno es llevado de manera natural a considerar el conjunto $\mathfrak{a}$ de *todos* los números α del dominio $\mathfrak{o}$ que son divisibles por un número ideal determinado; llamaré desde ahora, para abreviar, a un tal sistema $\mathfrak{a}$ un *ideal*, de modo que, a todo número ideal determinado, le corresponde un *ideal* determinado $\mathfrak{a}$. Ahora como, recíprocamente, la propiedad A, es decir la divisibilidad de un número α por el número ideal, consiste únicamente en que α pertenece al ideal correspondiente $\mathfrak{a}$, se podrá, en lugar de las propiedades A, B, C, ..., por las cuales ha sido definida la introducción de los números ideales, considerar los ideales correspondientes $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, ..., para establecer su carácter común y exclusivo. Tomando ahora en consideración que la introducción de los números ideales no tiene otra finalidad que la de restituir las leyes de la divisibilidad en el dominio numérico $\mathfrak{o}$ hasta su completa conformidad con la teoría de los números racionales, es evidentemente necesario que los números realmente existentes en $\mathfrak{o}$, y que sin embargo se presentan en primera línea como factores de los números compuestos, no sean considerados más que como un caso particular de los números ideales; si μ es pues un número determinado de $\mathfrak{o}$, entonces el sistema $\mathfrak{a}$ de todos los números $\alpha = \mu\omega$ del dominio $\mathfrak{o}$ divisibles por μ tendrá igualmente el carácter esencial de un ideal, y será llamado un *ideal principal*; este sistema evidentemente no queda alterado, cuando se reemplaza μ por $\varepsilon\mu$, donde ε designa una unidad cualquiera comprendida en $\mathfrak{o}$. Ahora, de la noción de número entero establecida antes resultan inmediatamente los dos teoremas elementales siguientes sobre la divisibilidad:

1.º Si los dos números enteros $\alpha = \mu\omega$, $\alpha' = \mu\omega'$ son divisibles por el número entero μ, entonces su suma $\alpha + \alpha' = \mu(\omega + \omega')$ y su diferencia $\alpha - \alpha' = \mu(\omega - \omega')$ serán también divisible por μ, puesto que la suma $\omega + \omega'$ y la diferencia $\omega - \omega'$ de dos números enteros ω, ω' son ellos mismos también números enteros.

2.º Si $\alpha = \mu\omega$ es divisible por μ, entonces todo número $\alpha\omega' = \mu(\omega\omega')$, divisible por α, será también divisible por μ, puesto que todo producto $\omega\omega'$ de dos números enteros ω, ω' es también él mismo un número entero.

3.º Hay una infinidad de secciones que *no pueden* ser engendradas por números racionales, de la manera indicada: para toda sección de esta especie, se crea y se introduce en la aritmética un número *irracional* especial, que corresponde a esta sección (o la engendra).

4.º Sean α, β dos números reales cualesquiera (racionales o irracionales); entonces es fácil según las secciones que engendran, definir si se tiene $\alpha > \beta$ o $\beta > \alpha$; además, se puede definir fácilmente, por medio de estas dos secciones, las cuatro secciones a las cuales deben corresponder la suma, la diferencia, el producto, y el cociente de los dos números α, β. De ese modo son definidas sin ninguna obscuridad las cuatro operaciones fundamentales de la Aritmética para dos números reales cualesquiera, y se pueden *demostrar* realmente proposiciones tales como, por ejemplo, que la igualdad $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$, lo cual no ha sido todavía hecho, que yo sepa, en el sentido riguroso de la palabra.

5.º Los números irracionales así definidos constituyen, reunidos junto con los números racionales, un dominio $\mathfrak{R}$ sin lagunas y *contínuo*; toda sección de este dominio $\mathfrak{R}$ será producida por un número determinado del mismo dominio; es imposible añadir aún nuevos números en este dominio $\mathfrak{R}$.

Si se aplican estos teoremas, verdaderos para todos los números enteros, a los números ω de nuestro dominio numérico $\mathfrak{o}$, designando por μ uno de estos números determinados, y por $\mathfrak{a}$ el ideal principal que le corresponde, se obtendrán las dos propiedades fundamentales siguientes de un tal sistema numérico $\mathfrak{a}$:

I. *Las sumas y las diferencias de dos números cualesquiera del sistema* $\mathfrak{a}$ *son siempre números del mismo sistema* $\mathfrak{a}$.

II. *Todo producto de un número del sistema* $\mathfrak{a}$ *por un número del sistema* $\mathfrak{o}$ *es un número del sistema* $\mathfrak{a}$.

Ahora, puesto que perseguimos el objetivo de restituir en general, mediante la introducción de los números ideales y de una modalidad de lenguaje correspondiente, las leyes de la divisibilidad en el dominio numérico $\mathfrak{o}$ hasta su completa conformidad con las que reinan en el dominio de los números enteros racionales, se sigue que las definiciones de los números ideales y de la divisibilidad por estos números deberán enunciarse de tal manera que los dos teoremas elementales anteriores, 1.º y 2.º, continúen subsistiendo incluso cuando μ no sea un número existente, sino un número ideal, y por consiguiente las dos propiedades I y II pertenecerán no sólo a los ideales principales, sino a *todos* los ideales. Hemos pues encontrado con ello un carácter *común* a todos los ideales; a todo número existente o ideal le corresponde un ideal completamente determinado $\mathfrak{a}$, que goza siempre de las dos propiedades I y II.

Pero un hecho de la máxima importancia, y del que no he podido demostrar rigurosamente la verdad más que después de numerosos y vanos intentos y después de haber sobrepasado grandes dificultades, es que, recíprocamente, todo sistema $\mathfrak{a}$ que goza de las propiedades I y II es también un ideal, es decir que $\mathfrak{a}$ constituye el conjunto de todos los números α del dominio $\mathfrak{o}$ que son divisibles por un número existente determinado, o por un número ideal, indispensable para completar la teoría. Las dos propiedades I y II son pues no solamente las condiciones necesarias, sino también las condiciones suficientes para que un sistema numérico $\mathfrak{a}$ sea un ideal; cualquier otra condición a la que se quisieran sujetar los sistemas numéricos $\mathfrak{a}$, salvo que sea una simple consecuencia de las propiedades I y II, haría imposible la explicación completa de todos los fenómenos de la divisibilidad en el dominio $\mathfrak{o}$.

Esta constatación me ha conducido naturalmente a fundamentar toda la teoría de los números del dominio $\mathfrak{o}$ sobre esta definición simple, completamente liberada de toda obscuridad y de la admisión de los números ideales([13]):

Todo sistema $\mathfrak{a}$ *de números enteros del cuerpo* Ω*, que posea las propiedades* I *y* II*, es denominado* UN IDEAL DE ESTE CUERPO.

La divisibilidad de un número α por un número μ consiste en que α es un número $\mu\omega$ del ideal principal, que corresponde al número μ y puede ser convenientemente designado por $\mathfrak{o}(\mu)$ o $\mathfrak{o}\mu$; y de la propiedad II o del teorema 2.º, resulta también que todos los números del ideal principal $\mathfrak{o}\alpha$

[13]Está naturalmente permitido, aunque esto no sea de ningún modo necesario, hacer corresponder a todo *ideal* tal como $\mathfrak{a}$ un *número ideal* que lo engendra, si no es un ideal principal.

son también números del ideal principal $\mathfrak{o}\mu$. Recíprocamente, es evidente que α es ciertamente divisible por μ, cuando todos los números del ideal $\mathfrak{o}\alpha$, y por consiguiente α mismo, están contenidos en el ideal $\mathfrak{o}\mu$. De ahí uno es llevado a establecer la siguiente noción de *divisibilidad*, no solamente para los ideales principales, sino también para todos los ideales:

Un ideal $\mathfrak{a}$ *se denomina* divisible *por un ideal* $\mathfrak{b}$*, o un múltiplo de* $\mathfrak{b}$*, y* $\mathfrak{b}$ *un divisor de* $\mathfrak{a}$*, cuando todos los números del ideal* $\mathfrak{a}$ *están al mismo tiempo contenidos en* $\mathfrak{b}$*. Un ideal* $\mathfrak{p}$*, diferente de* $\mathfrak{o}$*, sin más divisores que* $\mathfrak{o}$ *y* $\mathfrak{p}$*, se denomina un* ideal primo([14]).

De esta divisibilidad de los ideales, *que incluye evidentemente la de los números*, es necesario desde el principio distinguir muy bien la noción siguiente de la *multiplicación* y de los *productos* de dos ideales:

Si α *recorre todos los números de un ideal* $\mathfrak{a}$*, y* β *todos los números de un ideal* $\mathfrak{b}$*, entonces todos los productos de la forma* $\alpha\beta$ *y todas las sumas de estos productos constituirán un ideal que se llamará el producto de los ideales* $\mathfrak{a}$*,* $\mathfrak{b}$*, y que se designará por* $\mathfrak{ab}$([15]).

Ahora bien, se ve inmediatamente, es verdad, que el producto $\mathfrak{ab}$ es divisible tanto por $\mathfrak{a}$ como por $\mathfrak{b}$; pero el establecimiento completo de la conexión entre las dos nociones de la divisibilidad y de la multiplicación de los ideales sólo se consigue una vez se han vencido dificultades características, profundamente ligadas a la naturaleza del sujeto; esta conexión se expresa esencialmente por medio de los dos teoremas siguientes:

Si el ideal $\mathfrak{c}$ *es divisible por el ideal* $\mathfrak{a}$*, entonces existirá siempre un ideal* $\mathfrak{b}$*, y sólo uno, tal que el producto* $\mathfrak{ab}$ *sea idéntico a* $\mathfrak{c}$*.*

Todo ideal diferente de $\mathfrak{o}$ *o es un ideal primo, o puede ser representado, y esto de una sola manera, bajo la forma de un producto de ideales todos primos.*

En la presente Memoria, me limito a demostrar estos resultados con un rigor completo y por vía sintética. En esto consiste el *fundamento* propio de la teoría completa de los ideales y de las formas descomponibles, la cual ofrece a los matemáticos un campo inagotable de investigaciones. De todos los desarrollos ulteriores, para los cuales debo remitir a la exposición hecha en las *Vorlesungen über Zahlentheorie* de Dirichlet y a algunas Memorias que aparecerán más tarde, no he incluido en la Memoria actual más que la partición de los ideales en *clases*, y la demostración de que el número de estas *clases de ideales* (o de las clases de formas correspondientes) es finito. La primera Sección contiene solamente las proposiciones indispensables para el presente objetivo, extraidas de una teoría auxiliar, importante también para otra investigaciones, y de la que publicaré en otra parte la exposición completa. La segunda Sección, que tiene por objetivo el de aclarar mediante ejemplos numéricos completamente determinados las nociones generales que deberán ser introducidas más tarde, podría ser completamente suprimida; pero la he conservado porque puede ser útil para facilitar la comprensión de

[14] Al mismo tiempo, el número ideal correspondiente al ideal $\mathfrak{a}$ se llamaría *divisible* por el número ideal correspondiente al ideal $\mathfrak{b}$; a un ideal primo correspondería un número ideal *primo*.

[15] El número ideal correspondiente al ideal $\mathfrak{ab}$ se llamaría el *producto* de los dos números ideales correspondientes a $\mathfrak{a}$ y $\mathfrak{b}$.

las Secciones siguientes, donde se encontrará la teoría de los números enteros de un cuerpo finito cualquiera desarrollada hasta el punto indicado antes. Para eso, es suficiente tomar en préstamo solamente los primeros elementos de la teoría general de los cuerpos, teoría cuyo desarrollo ulterior conduciría fácilmente a los principios algebraicos inventados por Galois, los cuales sirven a su vez de base para las más profundas investigaciones en la teoría de los ideales.

I

Teoremas auxiliares de la teoría de los módulos.

Como se desprende de la *Introducción*, en lo que sigue tendremos que considerar muy a menudo sistemas de números que son estables bajo la *adición* y la *substracción*; el desarrollo de las propiedades generales de semejantes sistemas constituye el objeto de una teoría bastante extensa, que puede también ser utilizada para otra investigaciones, mientras que para nuestro objetivo, los primeros elementos de esta teoría son suficientes. Para no interrumpir más tarde el curso de nuestra exposición, y al mismo tiempo para hacer perceptible más claramente el alcance de los diversos conceptos sobre los cuales se apoya nuestra siguiente teoría de los números enteros algebraicos, nos parece apropiado establecer previamente un pequeño número de teoremas muy simples, aunque no puedan ofrecer un verdadero interés mas que en virtud de sus aplicaciones.

§1.– *Módulos y su divisibilidad.*

1.º Un sistema $\mathfrak{a}$ de números reales o complejos se denominará un *módulo* cuando todas las sumas y las diferencias de estos números pertenezcan a este mismo sistema $\mathfrak{a}$.

Luego si α es un número determinado del módulo $\mathfrak{a}$, todos los números

$$\alpha + \alpha = 2\alpha,\ 2\alpha + \alpha = 3\alpha,\ \ldots,$$

$$\alpha - \alpha = 0,\ 0 - \alpha = -\alpha,\ -\alpha - \alpha = -2\alpha,\ \ldots,$$

y, por consiguiente, todos los números de la forma $x\alpha$ pertenecerán también al módulo $\mathfrak{a}$, pudiendo x ser igual a cada uno de los números racionales enteros, es decir a cada uno de los números

$$0,\ \pm 1,\ \pm 2,\ \pm 3,\ \ldots.$$

Un tal sistema de números $x\alpha$ constituye por sí mismo un módulo, que designaremos por $[\alpha]$; si, por consiguiente, un módulo contiene un número α diferente de cero, entonces contendrá también una infinidad de números diferentes los unos de los otros. Pero es evidente que el número cero, que está contenido en cada módulo, constituye también ya por sí mismo un módulo.

2.º Un módulo $\mathfrak{a}$ se denominará *divisible* por el módulo $\mathfrak{b}$ o un *múltiplo* de $\mathfrak{b}$, y $\mathfrak{b}$ un *divisor* de $\mathfrak{a}$, cuando todos los números del módulo $\mathfrak{a}$ estén contenidos también en el módulo $\mathfrak{b}$.

El módulo cero es pues un múltiplo común de todos los módulos; si, además, α es un número determinado de un módulo $\mathfrak{a}$, entonces el módulo $[\alpha]$ será divisible por $\mathfrak{a}$. Es, además, evidente que todo módulo es divisible por sí mismo, y que dos módulos $\mathfrak{a}$ y $\mathfrak{b}$, de los que cada uno es divisible por el otro, son idénticos, lo que indicaremos siempre por $\mathfrak{a} = \mathfrak{b}$. Si, además, cada uno de los módulos $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$, ..., es divisible por el que le sigue inmediatamente, entonces está claro que cada uno de ellos será divisible por todos aquéllos que le sigan.

3.º Sean $\mathfrak{a}$, $\mathfrak{b}$ dos módulos cualesquiera; entonces el sistema $\mathfrak{m}$ de todos los números que pertenecen a la vez a estos dos módulos será él mismo un módulo; será denominado el *mínimo común múltiplo* de $\mathfrak{a}$, $\mathfrak{b}$, pues todo múltiplo común de $\mathfrak{a}$, $\mathfrak{b}$ es divisible por $\mathfrak{m}$.

Sean, en efecto μ, μ' dos números cualesquiera del sistema $\mathfrak{m}$, y contenidos por consiguiente tanto en $\mathfrak{a}$ como en $\mathfrak{b}$; entonces cada uno de los dos números $\mu \pm \mu'$ pertenecerá (según 1.º) tanto al módulo $\mathfrak{a}$ como al módulo $\mathfrak{b}$, y por lo tanto también al sistema $\mathfrak{m}$, de donde se sigue que $\mathfrak{m}$ es un módulo. Puesto que todos los números de este módulo $\mathfrak{m}$ están contenidos en $\mathfrak{a}$ y también en $\mathfrak{b}$, $\mathfrak{m}$ es un múltiplo común de $\mathfrak{a}$, $\mathfrak{b}$. Si, además, el módulo $\mathfrak{m}'$ es un múltiplo común cualquiera de $\mathfrak{a}$, $\mathfrak{b}$, y por lo tanto $\mathfrak{m}'$ se compone completamente de números contenidos a la vez en $\mathfrak{a}$ y en $\mathfrak{b}$, entonces estos números (en virtud de la definición del sistema $\mathfrak{m}$) estarán también contenidos en $\mathfrak{m}$, es decir que $\mathfrak{m}'$ es divisible por $\mathfrak{m}$.

4.º Si α se hace sucesivamente igual a todos los números de un módulo $\mathfrak{a}$, y lo mismo β a todos los números de un módulo $\mathfrak{b}$, entonces el sistema $\mathfrak{d}$ de todos los números de la forma $\alpha + \beta$ constituirá un módulo; este módulo será denominado el *máximo común divisor* de $\mathfrak{a}$, $\mathfrak{b}$, pues todo divisor común de $\mathfrak{a}$, $\mathfrak{b}$ es también un divisor de $\mathfrak{d}$.

En efecto, pudiéndose poner dos números cualesquiera δ, δ' del sistema $\mathfrak{d}$ bajo la forma $\delta = \alpha + \beta$, $\delta' = \alpha' + \beta'$, donde α, α' pertenecen al módulo $\mathfrak{a}$, y β, β' al módulo $\mathfrak{b}$, se obtiene que

$$\delta \pm \delta' = (\alpha \pm \alpha') + (\beta \pm \beta');$$

y, puesto que los números $\alpha \pm \alpha'$ están contenidos en $\mathfrak{a}$ y los números $\beta \pm \beta'$ en $\mathfrak{b}$, entonces los números $\delta \pm \delta'$ pertenecerán igualmente al sistema $\mathfrak{d}$, es decir que $\mathfrak{d}$ es un módulo. Estando el número cero contenido en cada módulo, todos los números $\alpha = \alpha + 0$ del módulo $\mathfrak{a}$ y todos los números $\beta = 0 + \beta$ del módulo $\mathfrak{b}$ pertenecen al módulo $\mathfrak{d}$, el cual es, como consecuencia, un divisor común de $\mathfrak{a}$ y $\mathfrak{b}$. Si, además, el módulo $\mathfrak{d}'$ es un divisor común cualquiera de $\mathfrak{a}$, $\mathfrak{b}$, y por lo tanto todos los números α y todos los números β están contenidos en $\mathfrak{d}'$, entonces (en virtud de 1.º) todos los números $\alpha + \beta$, es decir todos los números del módulo $\mathfrak{d}$, pertenecerán también al módulo $\mathfrak{d}'$; luego $\mathfrak{d}$ es divisible por $\mathfrak{d}'$.

Después de haber desarrollado rigurosamente estas demostraciones, podremos eximirnos de hacer ver cómo las nociones de mínimo común múltiplo y de máximo común divisor deberán ser entendidas para un número cualquiera (incluso infinito) de módulos. No obstante tal vez sea útil justificar el modo de expresión elegido, mediante la siguiente observación: Si a, b son dos números racionales enteros determinados, m su mínimo común múltiplo, y d su máximo común divisor, entonces resulta de los primeros elementos de

la teoría de los números que $[m]$ será el mínimo común múltiplo, y $[d]$ el máximo común divisor de los dos módulos $[a]$ y $[b]$. Por lo demás se reconocerá pronto que las proposiciones de la teoría de los números que se refieren a este caso pueden deducirse recíprocamente de la teoría de los módulos.

§2.– *Congruencias y clases de números.*

1.º Sea $\mathfrak{a}$ un módulo; dos números cualesquiera ω, ω' serán denominados *congruentes* o *incongruentes* según $\mathfrak{a}$, según que su diferencia $\pm(\omega - \omega')$ esté contenida o no en $\mathfrak{a}$. La *congruencia* de los números ω, ω' con respecto al módulo $\mathfrak{a}$ será indicada por la notación

$$\omega \equiv \omega' \pmod{\mathfrak{a}}.$$

Se obtienen de ahí inmediatamente las proposiciones simples siguientes, de las que podremos eximirnos de dar las demostraciones:

Si $\omega \equiv \omega' \pmod{\mathfrak{a}}$, y $\omega' \equiv \omega'' \pmod{\mathfrak{a}}$, entonces se tendrá también que $\omega \equiv \omega'' \pmod{\mathfrak{a}}$.

Si $\omega \equiv \omega' \pmod{\mathfrak{a}}$, y x es cualquier número racional entero, entonces se tendrá que $x\omega \equiv x\omega' \pmod{\mathfrak{a}}$.

Si $\omega \equiv \omega' \pmod{\mathfrak{a}}$, y $\omega'' \equiv \omega''' \pmod{\mathfrak{a}}$, entonces se tendrá también que $\omega \pm \omega'' \equiv \omega' \pm \omega''' \pmod{\mathfrak{a}}$.

Si $\omega \equiv \omega' \pmod{\mathfrak{a}}$, y el módulo $\mathfrak{b}$ es un divisor de $\mathfrak{a}$, entonces se tendrá también que $\omega \equiv \omega' \pmod{\mathfrak{b}}$.

Si $\omega \equiv \omega' \pmod{\mathfrak{a}}$, y $\omega \equiv \omega' \pmod{\mathfrak{b}}$, entonces se tendrá también que $\omega \equiv \omega' \pmod{\mathfrak{m}}$, siendo $\mathfrak{m}$ el mínimo común múltiplo de $\mathfrak{a}$, $\mathfrak{b}$.

2.º El primero de los teoremas precedentes conduce a la introducción de la noción de una *clase de números* relativa al módulo $\mathfrak{a}$: entenderemos por ello el conjunto de todos los números, y sólo de ellos, que son congruentes con un número determinado y por consiguiente también entre sí, según $\mathfrak{a}$. Una clase tal según $\mathfrak{a}$ está pues completamente determinada cuando se da uno solo de los números que ella contiene, y todo número puede ser considerado como *representante* de toda una clase. Los números del módulo $\mathfrak{a}$, por ejemplo, constituyen ellos mismos una tal clase, representada por el número cero.

Si ahora $\mathfrak{b}$ es un segundo módulo, se podrá siempre elegir en este módulo un número finito o infinito de números,

$$(\beta_r) \qquad \beta_1, \quad \beta_2, \quad \beta_3, \quad \ldots,$$

de tal manera que todo número contenido en $\mathfrak{b}$ sea congruente según el módulo $\mathfrak{a}$ con uno de estos números, y con uno solo. A un tal sistema de números β_r en el módulo $\mathfrak{b}$, que son mutuamente incongruentes con respecto de $\mathfrak{a}$, pero que representan también a todas las clases que tienen números en común con $\mathfrak{b}$, lo llamaré *un sistema completo de representantes del módulo* $\mathfrak{b}$ *según el módulo* $\mathfrak{a}$, y el número de estos números β_r o de las clases a las que representan, cuando sea finito, será designado por $(\mathfrak{b}, \mathfrak{a})$; si, por el contrario, el número de los representantes β_r es infinito, entonces conviene atribuir al símbolo $(\mathfrak{b}, \mathfrak{a})$ el valor cero. El examen en profundidad de un tal sistema de representantes (β_r) conduce ahora al siguiente teorema:

3.º Sean $\mathfrak{a}$, $\mathfrak{b}$ dos módulos cualesquiera, $\mathfrak{m}$ su mínimo común múltiplo y $\mathfrak{d}$ su máximo común divisor; entonces todo sistema completo de representantes del módulo $\mathfrak{b}$ con respecto de $\mathfrak{a}$ será al mismo tiempo un sistema completo

de representantes del módulo $\mathfrak{b}$ con respecto de $\mathfrak{m}$, así como del módulo $\mathfrak{d}$ con respecto de $\mathfrak{a}$, y por consiguiente se tendrá que

$$(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{b}, \mathfrak{m}) = (\mathfrak{d}, \mathfrak{a}).$$

En primer lugar es evidente que dos números cualesquiera β, β' del módulo $\mathfrak{b}$, congruentes según $\mathfrak{a}$, son congruentes según $\mathfrak{m}$, puesto que $\beta - \beta'$ está contenido tanto en $\mathfrak{a}$ como en $\mathfrak{b}$, y, por consiguiente, también en $\mathfrak{m}$. Ahora, puesto que todo número β del módulo $\mathfrak{b}$ es congruente a uno de los representantes β_r según $\mathfrak{a}$ y por consiguiente también según $\mathfrak{m}$, y ya que dos cualesquiera de estos representantes β_r, diferentes entre sí, son incongruentes según $\mathfrak{a}$ y por consiguiente también según $\mathfrak{m}$, estos números β_r pertenecientes al módulo $\mathfrak{b}$ constituirán un sistema completo de representantes del módulo $\mathfrak{b}$ según $\mathfrak{m}$. Se demostrará exactamente del mismo modo la segunda parte: los mismos números β_r, puesto que $\mathfrak{b}$ es divisible por $\mathfrak{d}$, están contenidos en $\mathfrak{d}$, y, según la hipótesis, incongruentes según $\mathfrak{a}$, y, puesto que todo número δ contenido en $\mathfrak{d}$ es de la forma $\alpha + \beta$, estando α contenido en $\mathfrak{a}$ y β en $\mathfrak{b}$, se tendrá que

$$\delta = \alpha + \beta \equiv \beta \pmod{\mathfrak{a}};$$

y, como β y por consiguiente también δ son congruentes a uno de los números β_r según $\mathfrak{a}$, entonces los números β_r constituirán un sistema completo de representantes del módulo $\mathfrak{d}$ según $\mathfrak{a}$.

Q.E.D.

Si $\mathfrak{b}$ es divisible por $\mathfrak{a}$, se tendrá $(\mathfrak{b}, \mathfrak{a}) = 1$, puesto que todos los números contenidos en $\mathfrak{b}$ son $\equiv 0 \pmod{\mathfrak{a}}$; recíprocamente, si $(\mathfrak{b}, \mathfrak{a}) = 1$, entonces $\mathfrak{b}$ será divisible por $\mathfrak{a}$, puesto que todos los números contenidos en $\mathfrak{b}$ son congruentes entre sí y por consiguiente $\equiv 0 \pmod{\mathfrak{a}}$; se tiene evidentemente al mismo tiempo que $\mathfrak{m} = \mathfrak{b}$, $\mathfrak{d} = \mathfrak{a}$.

4.º Si $\mathfrak{b}$ es un divisor de $\mathfrak{a}$ y al mismo tiempo un múltiplo de $\mathfrak{c}$, y si además β_r, se hace sucesivamente igual a todos los representantes de $\mathfrak{b}$ según $\mathfrak{a}$, y lo mismo γ_s igual a todos los representantes de $\mathfrak{c}$ según $\mathfrak{b}$, entonces todos los números $\beta_r + \gamma_s$ constituirán un sistema completo de representantes del módulo $\mathfrak{c}$ según $\mathfrak{a}$, y por consiguiente se tendrá que

$$(\mathfrak{c}, \mathfrak{a}) = (\mathfrak{c}, \mathfrak{b})(\mathfrak{b}, \mathfrak{a}).$$

Pues, *en primer lugar*, todos estos números $\beta_r + \gamma_s$, pertenecen al módulo $\mathfrak{c}$, puesto que β_r está contenido en $\mathfrak{b}$ y por consiguiente también en $\mathfrak{c}$, y γ_s está igualmente contenido en $\mathfrak{c}$. *En segundo lugar*, son todos incongruentes según $\mathfrak{a}$; si se designan, en efecto, por β', β'' valores particulares de β_r, y por γ', γ'' valores particulares de γ_s, entonces de la hipótesis $\beta' + \gamma' \equiv \beta'' + \gamma'' \pmod{\mathfrak{a}}$, puesto que $\mathfrak{a}$ es divisible por $\mathfrak{b}$ y $\beta' \equiv \beta'' \equiv 0 \pmod{\mathfrak{b}}$, se seguiría en primer lugar que $\gamma' \equiv \gamma'' \pmod{\mathfrak{b}}$; pero como γ', γ'' son términos particulares de la sucesión de números recorrida por γ_s, y dos cualesquiera de estos números diferentes entre sí son al mismo tiempo incongruentes según $\mathfrak{b}$, deberemos tener que $\gamma' = \gamma''$, y por consiguiente la suposición precedente se transformará en $\beta' \equiv \beta'' \pmod{\mathfrak{a}}$; ahora, como β', β'' son igualmente términos particulares de la sucesión de números recorrida por β_r, y dos cualesquiera de estos números diferentes entre sí son al mismo tiempo incongruentes según $\mathfrak{a}$, deberemos tener que $\beta' = \beta''$, lo que demuestra la aserción anterior. *En tercer lugar*, es necesario hacer ver que todo número

γ contenido en $\mathfrak{c}$ es congruente con uno de los números $\beta_r + \gamma_s$ según $\mathfrak{a}$; en efecto, siendo cada número γ congruente con uno de los números γ_s según $\mathfrak{b}$, se puede poner $\gamma = \beta + \gamma_s$, donde β designa un número del módulo $\mathfrak{b}$; además, siendo cada uno de estos números β congruente con uno de los números β_r según $\mathfrak{a}$, se puede poner $\beta = \alpha + \beta_r$, donde α designa un número del módulo $\mathfrak{a}$; se tendrá pues que

$$\gamma = \beta + \gamma_s = \alpha + \beta_r + \gamma_s \equiv \beta_r + \gamma_s \pmod{\mathfrak{a}}.$$

Q.E.D.

5.º Sean $\mathfrak{m}$ el mínimo común múltiplo, $\mathfrak{d}$ el máximo común divisor de dos módulos $\mathfrak{a}$, $\mathfrak{b}$, y sean ρ, σ dos números dados; entonces el sistema de las dos congruencias

$$\omega \equiv \rho \pmod{\mathfrak{a}}, \quad \omega \equiv \sigma \pmod{\mathfrak{b}}$$

tendrá siempre una raíz común, cuando se tenga, y en este caso solamente, que

$$\rho \equiv \sigma \pmod{\mathfrak{d}},$$

y todos los números ω formarán una clase determinada de números según el módulo $\mathfrak{m}$.

Si existe, en efecto, un número ω que satisface las dos congruencias, entonces los números $\omega - \rho$, $\omega - \sigma$ estarán contenidos respectivamente en $\mathfrak{a}$, $\mathfrak{b}$, y por lo tanto contenidos los dos en $\mathfrak{d}$, y por consiguiente su diferencia $\rho - \sigma$ estará contenida igualmente en $\mathfrak{d}$, es decir que la condición indicada $\rho \equiv \sigma \pmod{\mathfrak{d}}$ es necesaria; recíprocamente, si ella es satisfecha, entonces existirá (en virtud de la definición de $\mathfrak{d}$ en el §1, 4.º) un número α en $\mathfrak{a}$ y un número β en $\mathfrak{b}$, cuya suma es tal que $\alpha + \beta = \rho - \sigma$, y por consiguiente el número $\omega = \rho - \alpha = \sigma + \beta$ satisfará las dos congruencias; luego la condición indicada es también suficiente. Si, además, ω' es un número cualquiera que cumple las mismas condiciones que ω, entonces $\omega' - \omega$ estará contenido tanto en $\mathfrak{a}$ como en $\mathfrak{b}$, y por consiguiente también en $\mathfrak{m}$, es decir que se tendrá $\omega' \equiv \omega \pmod{\mathfrak{m}}$, y recíprocamente, todo número ω' de la clase representada por ω según $\mathfrak{m}$ satisfará las dos congruencias.

Q.E.D.

§3.– *Módulos finitos.*

1.º Sean β_1, β_2, β_3, …, β_n números determinados; entonces todos los números de la forma

$$\beta = y_1\beta_1 + y_2\beta_2 + y_3\beta_3 + \ldots + y_n\beta_n,$$

donde y_1, y_2, y_3, …, y_n designan números racionales enteros arbitrarios, constituyen evidentemente un módulo, que llamaremos un módulo *finito*, y que designaremos por $[\beta_1, \beta_2, \beta_3, \ldots, \beta_n]$; el complejo de las constantes β_1, β_2, β_3, …, β_n se denominará la *base* del módulo.

Este módulo $[\beta_1, \beta_2, \ldots, \beta_n]$ es evidentemente el máximo común divisor de los n módulos finitos $[\beta_1]$, $[\beta_2]$, …, $[\beta_n]$; sería fácil hacer ver que todo múltiplo de un módulo finito es igualmente un módulo finito; pero me limitaré aquí a demostrar el teorema fundamental siguiente, del que se harán más adelante aplicaciones importantes.

2.º Si todos los números de un módulo finito $\mathfrak{b} = [\beta_1, \beta_2, \ldots, \beta_n]$ pueden, multiplicándolos por números racionales diferentes de cero, ser transformados en números de un módulo $\mathfrak{a}$, entonces el mínimo común múltiplo $\mathfrak{m}$ de $\mathfrak{a}$, $\mathfrak{b}$ será un módulo finito, y se podrá elegir un sistema de $\frac{1}{2}(n+1)n$ números racionales enteros a, tal que los n números

$$\begin{aligned}
\mu_1 &= \; a'_1\beta_1, \\
\mu_2 &= \; a''_1\beta_1 + a''_2\beta_2, \\
\mu_3 &= \; a'''_1\beta_1 + a'''_2\beta_2 + a'''_3\beta_3, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ , \\
\mu_n &= \; a_1^{(n)}\beta_1 + a_2^{(n)}\beta_2 + a_3^{(n)}\beta_3 + \ldots + a_n^{(n)}\beta_n
\end{aligned}$$

formen una base de $\mathfrak{m}$, y que se tenga al mismo tiempo que

$$(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{b}, \mathfrak{m}) = a'_1 a''_2 a'''_3 \ldots a_n^{(n)}.$$

Por hipótesis, existen n fracciones, diferentes de cero,

$$\frac{s_1}{t_1}, \quad \frac{s_2}{t_2}, \quad \frac{s_3}{t_3}, \quad \ldots, \quad \frac{s_n}{t_n},$$

cuyos numeradores y denominadores son números racionales enteros, tales que los n productos

$$\frac{s_1}{t_1}\beta_1, \quad \frac{s_2}{t_2}\beta_2, \quad \frac{s_3}{t_3}\beta_3, \quad \ldots, \quad \frac{s_n}{t_n}\beta_n$$

pertenecen al módulo $\mathfrak{a}$; ahora, puesto que cualesquiera números de un módulo $\mathfrak{a}$, cuando se les multiplica por números racionales enteros t_1, t_2, t_3, …, t_n se transforman siempre en números del mismo módulo $\mathfrak{a}$ (§1, 1.º), entonces igualmente los productos $s_1\beta_1$, $s_2\beta_2$, $s_3\beta_3$, $\ldots s_n\beta_n$, y lo mismo, designando por s el valor absoluto del producto $s_1 s_2 s_3 \ldots s_n$, los números $s\beta_1$, $s\beta_2$, $s\beta_3$, $\ldots s\beta_n$, y por consiguiente también todos los productos $s\beta$ pertenecerán al módulo $\mathfrak{a}$, donde β designa un número arbitrario cualquiera del módulo $\mathfrak{b}$.

Sea ahora ν un índice determinado de la sucesión 1, 2,…, n; de entre los números del módulo $[\beta_1, \beta_2, \ldots, \beta_\nu]$ divisible por $\mathfrak{b}$, designemos por

$$\mu'_\nu = y_1\beta_1 + y_2\beta_2 + \ldots + y_\nu\beta_\nu,$$

todos aquéllos que, como, por ejemplo, $s\beta_\nu$, pertenecen al mismo tiempo al módulo $\mathfrak{a}$ y por consiguiente también al módulo $\mathfrak{m}$; de entre estos números μ'_ν, debe haber al menos un número

$$\mu_\nu = a_1^{(\nu)}\beta_1 + a_2^{(\nu)}\beta_2 + \ldots + a_\nu^{(\nu)}\beta_\nu,$$

en el cual y_ν toma su *mínimo* valor *positivo* $a_\nu^{(\nu)}$. Se puede entonces hacer ver que, en *todos* los números μ'_ν, el coeficiente y_ν es divisible por $a_\nu^{(\nu)}$, pues, ya que siempre se puede poner

$$y_\nu = x_\nu a_\nu^{(\nu)} + y'_\nu,$$

donde x_ν, y'_ν designan números racionales enteros, de los que el último satisface la condición([16])

$$0 \leq y'_\nu < a_\nu^{(\nu)},$$

[16]Es sobre eso sobre lo que reposa la teoría de la divisibilidad de los números racionales enteros.

entonces, si se pone

$$y'_1 = y_1 - x_\nu a_1^{(\nu)}, \quad y'_2 = y_2 - x_\nu a_2^{(\nu)}, \quad \ldots, \quad y'_{\nu-1} = y_{\nu-1} - x_\nu a_{\nu-1}^{(\nu)}$$

el número

$$\mu'_\nu - x_\nu \mu_\nu = y'_1\beta_1 + y'_2\beta_2 + \ldots + y'_{\nu-1}\beta_{\nu-1} + y'_\nu\beta_\nu$$

pertenecerá a la vez al módulo $[\beta_1, \beta_2, \ldots, \beta_\nu]$, y también al módulo $\mathfrak{m}$, porque μ'_ν y μ_ν están contenidos en $\mathfrak{m}$. Pero, puesto que (según la definición de μ_ν) en ninguno de estos números el coeficiente de β_ν es menor que $a_\nu^{(\nu)}$ y al mismo tiempo positivo, es necesario que se tenga $y'_\nu = 0$, y por lo tanto que $y_\nu = x_\nu a_\nu^{(\nu)}$ sea divisible por $a_\nu^{(\nu)}$, que es lo que se trataba de demostrar; al mismo tiempo,

$$\mu'_\nu - x_\nu \mu_\nu = \mu'_{\nu-1}$$

se convierte en un número contenido en $[\beta_1, \beta_2, \ldots, \beta_{\nu-1}]$ y en $\mathfrak{m}$, o se hace igual a cero, en el caso en el que $\nu = 1$.

Se deduce de ahí fácilmente que los n números μ_ν, que se obtienen poniendo sucesivamente $\nu = n, n-1, \ldots, 2, 1$, gozan de las propiedades enunciadas en el teorema a demostrar; pues todo número μ del módulo $\mathfrak{m}$, es decir todo número μ'_n contenido a la vez en $\mathfrak{a}$ y en $\mathfrak{b} = [\beta_1, \beta_2, \ldots, \beta_n]$, es de la forma

$$\mu = \mu'_{n-1} + x_n \mu_n,$$

donde x_n designa un número racional entero, y μ'_{n-1} un número perteneciente a los dos módulos $\mathfrak{a}$ y $[\beta_1, \beta_2, \ldots, \beta_{n-1}]$, y por consiguiente también al módulo $\mathfrak{m}$; todo número μ'_{n-1} de esta naturaleza es de la forma

$$\mu'_{n-1} = \mu'_{n-2} + x_{n-1}\mu_{n-1},$$

donde x_{n-1} designa un número racional entero, y μ'_{n-2} un número perteneciente a los dos módulos $\mathfrak{a}$ y $[\beta_1, \beta_2, \ldots, \beta_{n-2}]$, y así sucesivamente; por último todo número μ'_1, perteneciente a los dos módulos $\mathfrak{a}$ y $[\beta_1]$ es de la forma

$$\mu'_1 = x_1\mu_1,$$

donde x_1 designa un número racional entero. Queda pues demostrado que todo número μ del módulo $\mathfrak{m}$ puede ser representado bajo la forma

$$\mu = x_1\mu_1 + x_2\mu_2 + \ldots + x_n\mu_n,$$

siendo x_1, x_2, $\ldots$, x_n números racionales enteros; y como, recíprocamente, todo sistema elegido arbitrariamente de números racionales enteros x_1, x_2, $\ldots$, x_n produce ciertamente un número μ perteneciente al módulo $\mathfrak{m}$, puesto que μ_1, μ_2, $\ldots$, μ_n están ellos mismos contenidos en $\mathfrak{m}$, estos n números μ_1, μ_2, $\ldots$, μ_n constituirán una base del módulo $\mathfrak{m}$.

Para demostrar finalmente la última parte del teorema, vamos a considerar todos los números

$$\beta' = z'_1\beta_1 + z'_2\beta_2 + \ldots + z'_n\beta_n$$

del módulo $\mathfrak{b}$, en los cuales los números racionales enteros z'_1, z'_2, $\ldots$, z'_n cumplen las n condiciones

$$0 \leq z'_\nu < a_\nu^{(\nu)},$$

y demostraremos que estos números β', cuyo número es evidentemente igual a $a'_1 a''_2 \ldots a_\nu^{(\nu)}$, constituyen un sistema completo de representantes del módulo

$\mathfrak{b}$ según $\mathfrak{m}$ (o $\mathfrak{a}$). En efecto, *en primer lugar*, todos estos números β' pertenecientes al módulo $\mathfrak{b}$ son incongruentes según $\mathfrak{m}$; pues sea

$$z_1'\beta_1 + z_2'\beta_2 + \ldots + z_n'\beta_n \equiv z_1''\beta_1 + z_2''\beta_2 + \ldots + z_n''\beta_n \quad (\text{mód } \mathfrak{a}),$$

donde los números z_1'', z_2'', $\ldots$, z_n'' cumplen las mismas n condiciones que los números z_1', z_2', $\ldots$, z_n'; si las n diferencias

$$z_n' - z_n'', \quad z_{n-1}' - z_{n-1}'', \quad , \quad z_2' - z_2'', \quad z_1' - z_1''$$

no son todas nulas, sea $z_\nu' - z_\nu''$ la primera de entre ellas que tiene un valor diferente de cero, valor que, debido a la simetría, supondremos positivo, y que además es $< a_\nu^{(\nu)}$, puesto que los dos números z_ν', y z_ν'' son $< a_\nu^{(\nu)}$; entonces la diferencia

$$(z_1' - z_1'')\beta_1 + \ldots + (z_\nu' - z_\nu'')\beta_\nu$$

será evidentemente un número μ_ν', contenido en $\mathfrak{a}$ y en $[\beta_1, \beta_2, \ldots, \beta_\nu]$, y en el cual el coeficiente β_ν será positivo y $< a_\nu^{(\nu)}$, lo cual es contrario a la definición del número μ_ν; luego dos sistemas diferentes cualesquiera de n números z_1', z_2', $\ldots$, z_n', que satisfacen las condiciones anteriores, producen también dos números β' del módulo $\mathfrak{b}$, incongruentes según $\mathfrak{a}$. *En segundo lugar*, es fácil ver que todo número arbitrario

$$\beta = z_1\beta_1 + z_2\beta_2 + \ldots + z_n\beta_n$$

del módulo $\mathfrak{b}$ es congruente según $\mathfrak{a}$ (o $\mathfrak{m}$) con uno de estos números β'; pues, si z_1, z_2, $\ldots$, z_n están dados, está claro que se podrán elegir sucesivamente los n números racionales enteros

$$x_n, \quad x_{n-1}, \quad \ldots, x_2, \quad x_1,$$

de manera que los n números

$$\begin{aligned}
z_n' &= z_n + a_n^{(n)}x_n,\\
z_{n-1}' &= z_{n-1} + a_{n-1}^{(n)}x_n + a_{n-1}^{(n-1)}x_{n-1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots ,\\
z_2' &= z_2 + a_2^{(n)}x_n + a_2^{(n-1)}x_{n-1} + \ldots + a_2''x_2,\\
z_1' &= z_1 + a_1^{(n)}x_n + a_1^{(n-1)}x_{n-1} + \ldots + a_1''x_2 + a_1'x_1,
\end{aligned}$$

cumplan las n condiciones anteriores $0 \leq z_\nu' < a_\nu^{(\nu)}$; si se pone ahora

$$\beta' = z_1'\beta_1 + z_2'\beta_2 + \ldots + z_n'\beta_n,$$

se tendrá que

$$\beta' = \beta + x_1\mu_1 + x_2\mu_2 + \ldots + x_n\mu_n,$$

y por lo tanto que $\beta \equiv \beta'$ (mód $\mathfrak{m}$).

Q.E.D.

§4.− *Sistemas irreducibles.*

1.º Un sistema de n números α_1, α_2, $\ldots$, α_n se denominará un *sistema irreducible*, y estos números serán denominados *independientes* entre sí, cuando la suma

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n,$$

para todo sistema de números racionales enteros (o fraccionarios) x_1, x_2, $\ldots$, x_n, que no sean todos nulos, tome un valor diferente de cero; entonces dos sistemas diferentes cualesquiera de números racionales x_1, x_2, $\ldots$, x_n producirán evidentemente también dos sumas α desiguales. En el caso contrario, es decir cuando exista un sistema de números racionales x_1, x_2, $\ldots$, x_n, que no sean todos nulos y para los cuales la suma α sea igual a cero, el sistema de los números $\alpha_1, \alpha_2, \ldots, \alpha_n$ se denominará *reducible*, y estos números mismos serán *dependientes* entre sí. Si se quiere también conservar esta terminología para el caso en que $n = 1$, un único número constituirá evidentemente un sistema reducible o un sistema irreducible, según que sea igual a cero o no. De la definición precedente se deducen fácilmente los teoremas siguientes, cuyo número podría ser extraordinariamente acrecentado, sobre los *determinantes* de los números racionales.

2.º Si los n números $\alpha_1, \alpha_2, \ldots, \alpha_n$ son independientes entre sí, entonces los n números

$$\begin{aligned}
\alpha'_1 &= c'_1\alpha_1 + c'_2\alpha_2 + \ldots + c'_n\alpha_n,\\
\alpha'_2 &= c''_1\alpha_1 + c''_2\alpha_2 + \ldots + c''_n\alpha_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\alpha'_n &= c_n^{(n)}\alpha_1 + c_2^{(n)}\alpha_2 + \ldots + c_n^{(n)}\alpha_n,
\end{aligned}$$

donde los n^2 coeficientes c designan números racionales enteros o fraccionarios, constituirán un sistema irreducible o reducible, según que el determinante

$$C = \sum \pm c'_1 c''_2 \ldots c_n^{(n)}$$

sea o no diferente de cero.

Pues, si x_1, x_2, $\ldots$, x_n designan números racionales arbitrarios, no todos nulos, entonces la suma

$$x_1\alpha'_1 + x_2\alpha'_2 + \ldots + x_n\alpha'_n = \alpha',$$

puesto que α_1, α_2, $\ldots$, α_n son independientes entre sí, no podrá anularse más que si se tiene a la vez que

$$\begin{aligned}
c'_1x_1 + c''_1x_2 + \ldots + c_1^{(n)}x_n &= 0,\\
c'_2x_1 + c''_2x_2 + \ldots + c_2^{(n)}x_n &= 0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
c'_nx_1 + c''_nx_2 + \ldots + c_n^{(n)}x_n &= 0,
\end{aligned}$$

lo cual es imposible cuando C tiene un valor diferente de cero, y por consiguiente, en este caso, los números α'_1, α'_2, $\ldots$, α'_n son independientes entre sí. Pero, si se tiene $C = 0$, entonces existirá siempre un sistema de números racionales x_1, x_2, $\ldots$, x_n que satisfarán las ecuaciones precedentes, no siendo sin embargo todos nulos; eso se ve inmediatamente, cuando todos los n^2 coeficientes c se anulan; si no es ése el caso, entonces, de entre los determinantes menores de C que no se anulan, habrá uno, por ejemplo el determinante

$$\sum \pm c'_1 c''_2 \ldots c_r^{(r)},$$

que será de grado *máximo* $r < n$, de modo que todos los determinantes menores de grado superior se anulen; en este caso, como se sabe, las $n - r$

últimas ecuaciones anteriores serán consecuencias idénticas de las r precedentes, y se podrá dar a éstas la forma

$$\begin{aligned} x_1 = &\quad p'_{r+1}x_{r+1} + \ldots + p'_n x_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_r = &\quad p^{(r)}_{r+1}x_{r+1} + \ldots + p^{(r)}_n x_n, \end{aligned}$$

donde los $r(n-r)$ coeficientes p son números racionales; atribuyendo ahora a las cantidades $x_{r+1},\ldots,\ x_n$, en el número de $n-r \geq 1$, valores racionales arbitrarios, solamente con tal que no sean todos nulos, las cantidades $x_1,\ldots,\ x_r$ tomarán igualmente valores racionales, y se tendrá por consiguiente un sistema de n números racionales $x_1,\ldots,\ x_n$, no todos nulos, y para los cuales la suma α' será igual a cero; luego, en este caso, los n números $\alpha'_1,\ \alpha'_2,\ \ldots,\ \alpha'_n$ serán dependientes entre sí.

Q.E.D.

3.º Si los n números independientes entre sí $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n$, por una parte, y por otra parte los n números $\alpha'_1,\ \alpha'_2,\ \ldots,\ \alpha'_n$ constituyen los unos y los otros una base de un solo y mismo módulo $\mathfrak{a}$, se tendrá entonces que

$$\alpha'_\nu = c^{(\nu)}_1\alpha_1 + c^{(\nu)}_2\alpha_2 + \ldots + c^{(\nu)}_n\alpha_n,$$

donde los n^2 coeficientes c designan números racionales enteros, cuyo determinante es $= \pm 1$, y por consiguiente los números $\alpha'_1,\ \alpha'_2,\ \ldots,\ \alpha'_n$ serán también independientes entre sí.

En efecto, puesto que los números α'_ν están contenidos en el módulo $\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_n]$, existirán en todos los casos n ecuaciones de la forma precedente, en las cuales los coeficientes c serán números racionales enteros. Puesto que recíprocamente los n números α_ν están contenidos en el módulo $\mathfrak{a} = [\alpha'_1, \alpha'_2, \ldots, \alpha'_n]$, existirán también n ecuaciones de la forma

$$\alpha_\nu = e^{(\nu)}_1\alpha'_1 + e^{(\nu)}_2\alpha'_2 + \ldots + e^{(\nu)}_n\alpha'_n,$$

con coeficientes e igualmente racionales y enteros. Substituyendo las n primeras ecuaciones por los n números α'_ν, y considerando que los n números α_ν constituyen un sistema irreducible, se sigue que la suma

$$e^{(\nu)}_1 c^{\prime}_{\nu'} + e^{(\nu)}_2 c^{\prime\prime}_{\nu'} + \ldots + e^{(\nu)}_n c^{(n)}_{\nu'} = 1 \text{ o } 0,$$

según que los índices $\nu,\ \nu'$ sean iguales o desiguales. Luego el producto de los determinantes

$$\sum \pm c'_1 c''_2 \ldots c^{(n)}_n \cdot \sum \pm e'_1 e''_2 \ldots e^{(n)}_n = 1,$$

y por consiguiente, puesto que los dos factores son números racionales enteros,

$$\sum \pm c'_1 c''_2 \ldots c^{(n)}_n = \sum \pm e'_1 e''_2 \ldots e^{(n)}_n = \pm 1.$$

Q.E.D.

Recíprocamente, está claro que $[\alpha'_1, \alpha'_2, \ldots, \alpha'_n] = [\alpha_1, \alpha_2, \ldots, \alpha_n]$, cuando existan n ecuaciones de la forma

$$\alpha'_\nu = c^{(\nu)}_1\alpha_1 + \ldots + c^{(\nu)}_n\alpha_n,$$

donde los coeficientes c son números racionales enteros, cuyo determinante es $= \pm 1$.

4.º Si los n números independientes entre sí $\beta_1, \ldots, \beta_n$ constituyen la base de un módulo $\mathfrak{b}$, y de estos números dependen los n números $\alpha_1, \alpha_2, \ldots, \alpha_n$ de la base de un módulo $\mathfrak{a}$, por medio de n ecuaciones de la forma

$$\alpha_\nu = b_1^{(\nu)}\beta_1 + \ldots + b_n^{(\nu)}\beta_n,$$

donde los coeficientes b designan números racionales enteros, cuyo determinante B es diferente de cero, entonces el número de las clases será

$$(\mathfrak{b}, \mathfrak{a}) = \pm B.$$

En efecto, puesto que cada uno de los números $\beta_1, \ldots, \beta_n$, y por consiguiente todo número β del módulo $[\beta_1, \beta_2, \ldots, \beta_n]$ puede, multiplicándolo por el número racional B diferente de cero, ser transformado en un número del módulo $\mathfrak{a}$, que es divisible por $\mathfrak{b}$, y que por consiguiente también es el mínimo común múltiplo de $\mathfrak{a}$ y $\mathfrak{b}$, $\mathfrak{a}$ poseerá (según el §3, 2.º) una base de n números de la forma

$$\alpha'_\nu = a_1^{(\nu)}\beta_1 + a_2^{(\nu)}\beta_2 + \ldots + a_\nu^{(\nu)}\beta_\nu,$$

donde los coeficientes a son números racionales enteros y elegidos de tal manera que se tenga

$$(\mathfrak{b}, \mathfrak{a}) = a'_1 a''_2 \ldots a_n^{(n)} = \sum \pm a'_1 a''_2 \ldots a_n^{(n)}.$$

Como, además, los n números $\alpha_1, \ldots, \alpha_n$ constituyen igualmente una base del módulo $\mathfrak{a}$, y (según 2.º) cada uno de estos dos sistemas de n números es irreducible, puesto que se ha supuesto que el sistema $\beta_1, \ldots, \beta_n$ lo era, se tendrán entonces (según 3.º) n ecuaciones de la forma

$$\alpha'_\nu = c_1^{(\nu)}\alpha_1 + \ldots + c_n^{(\nu)}\alpha_n,$$

que tienen coeficientes racionales enteros c, cuyo determinante es tal que

$$\sum \pm c'_1 c''_2 \ldots c_n^{(n)} = \pm 1.$$

Substituyendo, en lugar de los números $\alpha_1, \ldots, \alpha_n$, sus expresiones anteriores por medio de los n números independientes entre sí $\beta_1, \ldots, \beta_n$, se ve, comparándolos con las expresiones precedentes de los números α'_ν, por medio de los mismos números $\beta_1, \ldots, \beta_n$, que

$$\alpha_{\nu'}^{(\nu)} = c_1^{(\nu)} b'_{\nu'} + c_2^{(\nu)} b''_{\nu'} + \ldots + c_n^{(\nu)} b_{\nu'}^{(n)},$$

y por consiguiente que

$$\sum \pm a'_1 \ldots a_n^{(n)} = \sum \pm c'_1 \ldots c_n^{(n)} \cdot \sum \pm b'_1 \ldots b_n^{(n)};$$

se tiene pues que $(\mathfrak{b}, \mathfrak{a}) = \pm B$.

Este teorema importante puede fácilmente (y de la manera más simple por medio del teorema siguiente) extenderse al caso más general en el que los coeficientes b son números racionales *fraccionarios*; se obtiene de este modo este teorema

$$(\mathfrak{b}, \mathfrak{a}) = \pm B(\mathfrak{a}, \mathfrak{b}),$$

y cada uno de los dos números de clases $(\mathfrak{a}, \mathfrak{b})$ y $(\mathfrak{b}, \mathfrak{a})$ puede determinarse según una regla simple, por medio del determinante B y de todos sus determinantes menores.

5.º Si, de entre los m números $\alpha_1, \alpha_2, \ldots, \alpha_m$, que constituyen una base del módulo $\mathfrak{a}$, no hay más que n que sean independientes entre sí,

entonces existirá una base del mismo módulo $\mathfrak{a}$ compuesta por n números independientes entre sí α'_1, α'_2, ..., α'_n.

La hipótesis de este teorema se verificará siempre, evidentemente, cuando todos los m números α_1,..., α_m estén representados por medio de n números independientes entre sí ω_1, ..., ω_n bajo la forma

$$\alpha_\mu = r_1^{(\mu)}\omega_1 + r_2^{(\mu)}\omega_2 + \ldots + r_n^{(\mu)}\omega_n,$$

componiéndose el sistema de coeficientes

$$(r) \qquad \left\{\begin{array}{llll} r'_1, & r'_2, & \ldots, & r'_n, \\ r''_1, & r''_2, & \ldots, & r''_n, \\ \ldots & \ldots & \ldots, & \ldots, \\ r_1^{(m)}, & r_2^{(m)}, & \ldots, & r_n^{(m)} \end{array}\right.$$

únicamente de números racionales, y uno al menos de los determinantes parciales R de grado n, que se pueden formar con este sistema y que son en el número de

$$\frac{m(m-1)\ldots(m-n+1)}{1.2\ldots n},$$

teniendo un valor diferente de cero, puesto que sin eso n cualesquiera de los m números α_μ serían dependientes entre sí. Recíprocamente, resulta de la hipótesis del teorema que los m números α_μ podrán siempre ser representados por medio de n números independientes ω_ν entre sí; pues, si se eligen como esos últimos, por ejemplo, los n números, de entre los m números α_μ que constituyen realmente un sistema irreducible, entonces, puesto que los $n+1$ números α_μ, ω_1, ..., ω_n son dependientes entre sí, existirá, para cada índice μ, una ecuación correspondiente, de la forma

$$x_0\alpha_\mu + x_1\omega_1 + x_2\omega_2 + \ldots + x_n\omega_n = 0,$$

cuyos coeficientes x son racionales y no todos nulos; como, además, los números $\omega_1, \omega_2, \ldots, \omega_n$ son independientes entre sí, x_0 deberá diferir de cero, y por consiguiente α_μ podrá ser representado de la manera indicada, por medio de los n números ω_ν; como por último de entre los m números α_μ se encuentran también los n números ω_ν, entonces uno al menos de los determinantes R será diferente de cero.

Voy a partir, como consecuencia, de la hipótesis de que los m números α_μ están representados de la manera indicada por medio de n números ω_ν, independientes entre sí, y voy a demostrar que, sea cual sea la manera como se elijan esos números ω_ν, existirán siempre n números α'_ν de la forma

$$\alpha'_\nu = c_1^{(\nu)}\omega_1 + c_2^{(\nu)}\omega_2 + \ldots + c_n^{(\nu)}\omega_\nu,$$

con coeficientes racionales c, que constituirán una base del mismo módulo $\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_m]$. Para eso, observo en primer lugar que evidentemente se puede siempre elegir un número racional, entero y positivo k, de tal manera que todos los mn productos $kr_\nu^{(\mu)}$ sean números enteros; si se pone ahora

$$\omega_1 = k\beta_1, \quad \omega_2 = k\beta_2, \quad \ldots, \quad \omega_n = k\beta_n,$$

y se expresan los números α_μ por medio de los números β_ν, resultará que el módulo $\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_m]$ es divisible por el módulo $\mathfrak{b} = [\beta_1, \beta_2, \ldots, \beta_n]$, y por consiguiente que es el mínimo común múltiplo de $\mathfrak{a}$, $\mathfrak{b}$. Como, además, los n números β_ν, siendo multiplicados por k, se transforman en los n números

ω_ν, y éstos, siendo multiplicados por un determinante R diferente de cero, se transforman en números de la forma

$$x_1\alpha_1 + x_2\alpha_2 + \ldots + x_m\alpha_m,$$

donde los coeficientes x designan números racionales enteros o fraccionarios, está claro que todo número β del módulo $\mathfrak{b}$, multiplicado por un número racional diferente de cero, puede transformarse él mismo en un número del módulo $\mathfrak{a}$, y resulta de ahí (según el §3, 2.º) que el mínimo común múltiplo $\mathfrak{a}$ de los dos módulos $\mathfrak{a}$, $\mathfrak{b}$ posee una base compuesta por n números de la forma

$$\alpha'_\nu = a_1^{(\nu)}\beta_1 + a_2^{(\nu)}\beta_2 + \ldots + a_\nu^{(\nu)}\beta_\nu,$$

donde los coeficientes a designan números racionales enteros, y siendo el producto $a'_1 a''_2 \ldots a_n^{(n)}$ diferente de cero. Si se expresan de nuevo los n números β_ν por medio de los n números ω_ν, se concluye la verdad de la aserción anterior, lo que demuestra al mismo tiempo el teorema.

6.º A la demostración precedente adjuntaría también las observaciones siguientes. Como los m números α_μ constituyen, tanto como los n números α'_ν, una base del mismo módulo $\mathfrak{a}$, existirán m ecuaciones de la forma

$$\alpha_\mu = p_1^{(\mu)}\alpha'_1 + p_2^{(\mu)}\alpha'_2 + \ldots + p_n^{(\mu)}\alpha'_n,$$

y n ecuaciones de la forma

$$\alpha'_\nu = q'_\nu\alpha_1 + q''_\nu\alpha_2 + \ldots + q_\nu^{(m)}\alpha_m,$$

en donde los $2mn$ coeficientes p y q son todos números racionales *enteros*; substituyendo las primeras expresiones en las segundas, y considerando que los n números α'_ν son independientes entre sí, se deduce que la suma

$$q'_\nu p'_{\nu'} + q''_\nu p''_{\nu'} + \ldots + q_\nu^{(m)} p_{\nu'}^{(m)} = 1 \text{ o } = 0,$$

según que los dos índices ν, ν', contenidos en la sucesión $1, 2, \ldots, n$, sean iguales o desiguales. Designando pues por P respectivamente todos los determinantes parciales del n-simo grado formados con el sistema de coeficientes (p), y por Q los determinantes correspondientes formados de la misma manera con el sistema de coeficientes (q), se sabe que la suma

$$\sum PQ,$$

extendida a todas las combinaciones diferentes de n índices superiores, es igual a la unidad, y, por consiguiente, todos los determinantes P no tienen ningún divisor común; y recíprocamente, esta propiedad de los determinantes P es esencial para que los n números α'_ν, así como los m números

$$\alpha_\mu = p_1^{(\mu)}\alpha'_1 + \ldots + p_n^{(\mu)}\alpha'_n,$$

formen bases del mismo módulo $\mathfrak{a}$.

Un sistema de coeficientes, tal como (p), no es evidentemente más que un caso particular del sistema de coeficientes precedente (r). Ahora, pudiendo, los n números α'_ν, representarse igualmente bajo la forma

$$\alpha'_\nu = e_1^{(\nu)}\omega_1 + e_2^{(\nu)}\omega_2 + \ldots + e_n^{(\nu)}\omega_n,$$

con n^2 coeficientes racionales e, cuyo determinante

$$E = \sum \pm e'_1 e''_2 \ldots e_n^{(n)}$$

es diferente de cero, obtenemos que

$$r_\nu^{(\mu)} = p_1^{(\mu)} e'_\nu + p_2^{(\mu)} e''_\nu + \ldots + p_n^{(\mu)} e_\nu^{(n)},$$

y, por consiguiente, dos determinantes correspondientes cualesquiera R, P, formados con los sistemas de coeficientes (r), (p), tienen entre sí la relación

$$R = PE.$$

El problema de encontrar, por medio de un sistema dado (r), todos los sistemas (p) correspondientes puede resolverse de la manera más comprensiva y más elegante mediante la generalización de un método aplicado por Gauss([17])) en casos especiales, y en el cual se utilizan las relaciones idénticas que tienen lugar entre los determinantes parciales; sin embargo eso nos conduciría aquí demasiado lejos, y me contentaré con haber demostrado la *existencia* de un tal sistema (p), del cual, como se ve inmediatamente (según §3) se pueden obtener todos los otros sistemas (p) mediante la composición con todos los sistemas posibles de los n^2 números racionales enteros cuyo determinante sea $= \pm 1$.

En la práctica, es decir en todos los caso en los que se dan numéricamente los coeficientes r, que se pueden, sin pérdida de generalidad, suponer números *enteros*, se llegará al objetivo, de la manera más rápida, mediante un encadenamiento de transformaciones elementales, apoyándose sobre la proposición evidente, de que un módulo $[\alpha_1, \alpha_2, \ldots, \alpha_m]$ no es alterado cuando se reemplaza, por ejemplo, el número α_1 por $\alpha_1 + x\alpha_2$, siendo x un número racional entero cualquiera. Los determinantes parciales R^0, correspondientes a todas las combinaciones de n números de la nueva base

$$\alpha_1^0 = \alpha_1 + x\alpha_2, \quad \alpha_2^0 = \alpha_2, \quad \alpha_3^0 = \alpha_3, \quad \ldots, \quad \alpha_m^0 = \alpha_m,$$

y al nuevo sistema de coeficientes (r^0), coincidirán en parte con los determinantes R correspondientes a la antigua base

$$\alpha_1 = \alpha_1^0 - x\alpha_2^0, \quad \alpha_2 = \alpha_2^0, \quad \alpha_3 = \alpha_3^0, \quad \ldots, \quad \alpha_m = \alpha_m^0;$$

serán en parte de la forma $R_1^0 = R_1 + xR_2$, y de ahí se deduce fácilmente que el máximo común divisor E de los determinantes R es al mismo tiempo el de los determinantes R^0; luego los determinantes R^0 no pueden anularse todos a la vez. De estas transformaciones de la base del módulo $\mathfrak{a}$, se hará ahora el uso siguiente:

Los m coeficientes $r_n^{(\mu)}$ del número ω_n no pueden ser todos nulos, pues entonces todos los determinantes R serían nulos. Si ahora *dos* al menos de estos coeficientes, por ejemplo r'_n y r''_n son diferentes de cero, y se tiene, en valor absoluto, $r'_n \geq r''_n$, entonces se podrá elegir el número racional entero x de manera que se tenga, en valor absoluto, $r'_n + xr''_n < r''_n$([18]); se obtiene entonces, mediante la transformación elemental anterior, una nueva base, en la cual todos los m coeficientes $r_n^{(\mu)}$, con la excepción del primero r'_n, permanecen invariables, y este único coeficiente es reemplazado por otro de valor (absoluto) *menor*. Repitiendo sucesivamente este procedimiento se llegará pues necesariamente a una base, en la cual todos los m coeficientes

[17] *Disquisitiones arithmeticae*, arts., 234, 236, 279.

[18] Aquí tenemos otra vez el mismo principio que sirve de fundamento para la teoría de los números racionales enteros.

de ω_n, con la excepción de uno solo, serán nulos. Designemos el número de la base, en el cual ocurre este coeficiente $a_n^{(n)}$ diferente de cero, por

$$\alpha'_n = a_1^{(n)}\omega_1 + a_2^{(n)}\omega_2 + \ldots + a_n^{(n)}\omega_n,$$

y conservémoslo invariable en todas las transformaciones subsiguientes de la base. Los determinantes parciales correspondientes a la base actual o se anulan, o son de la forma $Sa_n^{(n)}$, siendo S un determinante parcial de grado $(n-1)$-ésimo que corresponde a una combinación arbitraria de $n-1$ de los $m-1$ números de la base diferentes de α'_n, y que está formado con los $(n-1)^2$ coeficientes correspondientes de ω_1, ω_2, …, ω_{n-1}. No pudiendo anularse todos los determinantes S, se procederá ahora, con estos $m-1$ números de la base actual, con respecto a ω_{n-1}, como acabamos de hacer con los m números α_μ de la base primitiva, con respecto a ω_n, y, si se continúa siempre con estas transformaciones, se acabará por obtener una base de $\mathfrak{a}$, compuesta por n números α'_1, α'_2, …, α'_{n-1}, α'_n, de la forma

$$\alpha'_\nu = a_1^{(\nu)}\omega_1 + a_2^{(\nu)}\omega_2 + \ldots + a_n^{(\nu)}\omega_\nu,$$

y por $m-n=s$ números α''_1, α''_2, …, α''_s, que serán todos nulos, y por consiguiente podrán ser suprimidos; los n coeficientes $a_\nu^{(\nu)}$ diferentes de cero podrán ser elegidos positivos, puesto que α'_ν puede ser reemplazado, sin alteración del módulo, por $-\alpha'_\nu$, y su producto $a'_1 a''_2 \ldots, a_s^{(n)}$ es evidentemente el máximo común divisor E de todos los determinantes parciales R.

De ese modo obtenemos una segunda demostración del importante teorema (5.º), y es evidente al mismo tiempo que, mediante la composición de transformaciones sucesivas y mediante su inversión, se encuentra tanto el sistema de coeficientes (p) como un sistema de coeficientes (q). En efecto, se obtienen en primer lugar de esta manera m ecuaciones de la forma

$$\alpha_\mu = \textstyle\sum_\nu p_\nu^{(\mu)}\alpha'_\nu + \sum_\sigma h_\sigma^{(\mu)}\alpha''_\sigma,$$

o, siendo los s números α''_σ nulos,

$$\alpha_\mu = \textstyle\sum_\nu p_\nu^{(\mu)}\alpha'_\nu;$$

y, como el determinante de cada una de las substituciones o transformaciones es igual a 1, entonces el determinante de m-simo grado es

$$\begin{vmatrix} p'_1 & \ldots & p'_n & h'_1 & \ldots & h'_s \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ p_1^{(m)} & \ldots & p_n^{(m)} & h_1^{(m)} & \ldots & h_s^{(m)} \end{vmatrix} = \textstyle\sum PH = 1,$$

siendo las cantidades H los determinantes de s-simo grado complementarios de los determinantes P, y formados con el sistema de coeficientes (h). Por inversión, se obtiene el determinante adjunto

$$\begin{vmatrix} q'_1 & \ldots & q'_n & k'_1 & \ldots & k'_s \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ q_1^{(m)} & \ldots & q_n^{(m)} & k_1^{(m)} & \ldots & k_s^{(m)} \end{vmatrix} = \textstyle\sum QK = 1,$$

donde K designa el determinante complementario de Q; y, si P y Q son dos determinantes correspondientes, entonces se tiene, como se sabe, $H = Q$,

$K = P$; al mismo tiempo se obtienen n ecuaciones de la forma

$$\alpha'_\nu = \sum_\mu q_\nu^{(\mu)} \alpha_\mu$$

y s ecuaciones de la forma

$$\alpha''_\sigma = \sum_\mu k_\sigma^{(\mu)} \alpha_\mu = 0.$$

Estas últimas ecuaciones expresan de nuevo bajo otra forma la suposición primitiva, de que solamente n de los m números α_μ son independientes entre sí, y se hubiera podido fundamentar todo este estudio sobre un tal sistema de s ecuaciones.

Se puede generalmente abreviar el cálculo mismo, llevando a cabo a la vez varias transformaciones elementales. Sea, por ejemplo, $m = 4$, $n = 2$, de donde $s = 2$, y

$$\alpha_1 = 21\omega_1, \quad \alpha_2 = 7\omega_1 + 7\omega_2, \quad \alpha_3 = 9\omega_1 - 3\omega_2, \quad \alpha_4 = 8\omega_1 + 2\omega_2,$$

por lo tanto

$$(r) \qquad \left\{ \begin{array}{llll} r'_1 = 21, & r''_1 = 7, & r'''_1 = 9, & r_1^{\mathrm{iv}} = 8, \\ r'_2 = 0, & r''_2 = 7, & r'''_2 = -3, & r_2^{\mathrm{iv}} = 2; \end{array} \right.$$

entonces se obtienen los seis determinantes parciales

$$(R) \qquad \left\{ \begin{array}{lll} R_{1,2} = 147, & R_{1,3} = -63, & R_{1,4} = 42, \\ R_{3,4} = 42, & R_{2,4} = -42, & R_{2,3} = -84, \end{array} \right.$$

donde se ha puesto, para abreviar

$$r_1^{(\mu)} r_2^{(\mu')} - r_1^{(\mu')} r_2^{(\mu)} = R_{\mu,\mu'};$$

entre estos determinantes se tiene la relación idéntica

$$R_{1,2}R_{3,4} - R_{1,3}R_{2,4} + R_{1,4}R_{2,3} = 0.$$

Como ahora ω_2 tiene en α_4 el mínimo coeficiente diferente de cero, se formará la nueva base

$$\begin{array}{ll} \beta_1 = \alpha_1 = 21\omega_1, & \beta_2 = \alpha_2 - 3\alpha_4 = -17\omega_1 + \omega_2, \\ \beta_3 = \alpha_3 + 2\alpha_4 = 25\omega_1 + \omega_2, & \beta_4 = \alpha_4 = 8\omega_1 + 2\omega_2, \end{array}$$

de donde se sigue, inversamente que

$$\alpha_1 = \beta_1, \quad \alpha_2 = \beta_2 + 3\beta_4, \quad \alpha_3 = \beta_3 - 2\beta_1, \quad \alpha_4 = \beta_4.$$

Ahora, como ω_2, por ejemplo, en β_2 tiene el mínimo coeficiente 1 diferente de cero, se formará la tercera base

$$\begin{array}{ll} \gamma_1 = \beta_1 = 21\omega_1, & \gamma_2 = \beta_2 = -17\omega_1 + \omega_2, \\ \gamma_3 = -\beta_2 + \beta_3 = 42\omega_1, & \gamma_4 = \alpha_4 = 8\omega_1 + 2\omega_2, \end{array}$$

de donde se sigue, inversamente que,

$$\beta_1 = \gamma_1, \quad \beta_2 = \gamma_2, \quad \beta_3 = \gamma_2 + \gamma_3, \quad \beta_4 = 2\gamma_2 + \gamma_4.$$

Siendo γ_2 de hecho el único número en el cual ω_2 tiene un coeficiente diferente de cero, y siendo γ_1, de entre los otros tres números, aquél en el cual ω_1 tiene el mínimo coeficiente 21, se formará la cuarta base

$$\begin{array}{ll} \delta_1 = \gamma_1 = 21\omega_1, & \delta_2 = \gamma_2 = -17\omega_1 + \omega_2, \\ \delta_3 = -2\gamma_1 + \gamma_3 = 0, & \delta_4 = -2\gamma_1 + \gamma_4 = 0, \end{array}$$

de donde se obtiene, inversamente que,

$$\gamma_1 = \delta_1, \quad \gamma_2 = \delta_2, \quad \gamma_3 = 2\delta_1 + \delta_3, \quad \gamma_4 = 2\delta_1 + \delta_4.$$

Como $\delta_3 = \delta_4 = 0$, la transformación está completada, y las substituciones sucesivas dan

$$\begin{array}{ll} \alpha_1 = \delta_1 & = \delta_1, \\ \alpha_2 = 6\delta_1 + 7\delta_2 + 3\delta_4 & = 6\delta_1 + 7\delta_2, \\ \alpha_3 = -2\delta_1 - 3\delta_2 + \delta_3 - 2\delta_4 & = -2\delta_1 - 3\delta_2, \\ \alpha_4 = 2\delta_1 + 2\delta_2 + \delta_4 & = 2\delta_1 + 2\delta_2, \end{array}$$

e inversamente

$$\begin{array}{ll} \delta_1 = \alpha_1 & = 21\omega_1, \\ \delta_2 = \alpha_2 - 3\alpha_4 & = -17\omega_1 + \omega_2, \\ \delta_3 = -2\alpha_1 - \alpha_2 + \alpha_3 + 5\alpha_4 & = 0, \\ \delta_4 = -2\alpha_1 - 2\alpha_2 + 7\alpha_4 & = 0. \end{array}$$

Como δ_1, δ_2, δ_3, δ_4 son cantidades que, en la teoría general, han sido designadas por α_1', α_2', α_1'', α_2'', se tendrá que

$$(p) \qquad \left\{ \begin{array}{llll} p_1' = 1, & p_1'' = 6, & p_1''' = -2, & p_1^{\text{iv}} = 2, \\ p_2' = 0, & p_2'' = 7, & p_2''' = -3, & p_2^{\text{iv}} = 2; \end{array} \right.$$

se obtiene pues, para los determinantes proporcionales a los R,

$$(P) \qquad \left\{ \begin{array}{lll} P_{1,2} = 7, & P_{1,3} = -3, & P_{1,4} = 2, \\ P_{3,4} = 2, & P_{2,4} = -2, & P_{2,3} = -4; \end{array} \right.$$

se tiene igualmente

$$(q) \qquad \left\{ \begin{array}{llll} q_1' = 1, & q_1'' = 0, & q_1''' = 0, & q_1^{\text{iv}} = 0, \\ q_2' = 0, & q_2'' = 1, & q_2''' = 0, & q_2^{\text{iv}} = -3, \end{array} \right.$$

y

$$(Q) \qquad \left\{ \begin{array}{lll} Q_{1,2} = 1, & Q_{1,3} = 0, & Q_{1,4} = -3, \\ Q_{3,4} = 0, & Q_{2,4} = 0, & Q_{2,3} = 0. \end{array} \right.$$

Después, de los sistemas de coeficientes

$$(h) \qquad \left\{ \begin{array}{llll} h_1' = 0, & h_1'' = 0, & h_1''' = 1, & h_1^{\text{iv}} = 0, \\ h_2' = 0, & h_2'' = 3, & h_2''' = -2, & h_2^{\text{iv}} = 1, \end{array} \right.$$

y

$$(k) \qquad \left\{ \begin{array}{llll} k_1' = -2, & k_1'' = -1, & k_1''' = 1, & k_1^{\text{iv}} = 5, \\ k_2' = -2, & k_2'' = -2, & k_2''' = 0, & k_2^{\text{iv}} = 7, \end{array} \right.$$

se obtienen los determinantes $H_{\mu,\mu'} = Q_{\mu,\mu'}$ y $K_{\mu,\mu'} = P_{\mu,\mu'}$, que son respectivamente complementarios de $P_{\mu,\mu'}$ y $Q_{\mu,\mu'}$,

$$(H) \left\{ \begin{array}{llll} H_{1,2} = h_1'''h_2^{\text{iv}} - h_1^{\text{iv}}h_2''', & H_{1,3} = h_1^{\text{iv}}h_2'' - h_1''h_2^{\text{iv}}, & H_{1,4} = h_1''h_2''' - h_1'''h_2'', \\ H_{3,4} = h_1'h_2'' - h_1''h_2', & H_{2,4} = h_1'''h_2' - h_1'h_2''', & H_{2,3} = h_1'h_2^{\text{iv}} - h_1^{\text{iv}}h_2', \end{array} \right.$$

$$(K) \left\{ \begin{array}{llll} K_{1,2} = k_1'''k_2^{\text{iv}} - k_1^{\text{iv}}k_2''', & K_{1,3} = k_1^{\text{iv}}k_2'' - k_1''k_2^{\text{iv}}, & K_{1,4} = k_1''k_2''' - k_1'''k_2'', \\ K_{3,4} = k_1'k_2'' - k_1''h_2', & K_{2,4} = k_1'''k_2' - k_1'k_2''', & K_{2,3} = k_1'k_2^{\text{iv}} - k_1^{\text{iv}}k_2', \end{array} \right.$$

y de este modo el ejemplo se encuentra completamente tratado.

Para acabar, observaré que la aplicación al caso $n = 1$ conduce al teorema fundamental sobre el máximo común divisor de un número cualquiera de

números racionales enteros, teorema sobre el cual reposa toda la teoría de la divisibilidad de estos números.

Las investigaciones en esta primera Sección han sido expuestas bajo la forma especial que responde a nuestro objetivo; pero está claro que no dejan en modo alguno de ser verdaderas, cuando las letras griegas designan, no ya *números*, sino elementos cualesquiera, objetos del estudio que se prosigue, de los que dos cualesquiera α, β, mediante una operación conmutativa y uniformemente invertible (composición), ocupando el lugar de la adición, producirán un elemento determinado $\gamma = \alpha + \beta$ de la misma especie; los módulos $\mathfrak{a}$ se transforman en *grupos* de elementos, cuyos resultados (los *compuestos*) pertenecen siempre al mismo grupo; los coeficientes racionales enteros indican cuántas veces un elemento contribuye a la generación de otro.

II

El germen de la teoría de los ideales.

En esta Sección, me propongo, como ya lo he indicado en la *Introducción*, explicar con un ejemplo determinado la naturaleza del fenómeno que condujo a Kummer a la creación de los *números ideales*, y utilizaré el mismo ejemplo para aclarar el concepto de *ideal* introducido por mí, y el de la multiplicación de los ideales.

§5.– *Los números racionales enteros.*

La teoría de los números se ocupa en principio exclusivamente del sistema de los números racionales enteros 0, ± 1, ± 2, ± 3, ..., y será apropiado recordar aquí en pocas palabras las leyes importantes que gobiernan este dominio. Ante todo, es necesario recordar que estos números son estables bajo la adición, substracción y multiplicación, es decir que las sumas, las diferencias y los productos de dos números cualesquiera de este dominio pertenecen al mismo dominio. La teoría de la *divisibilidad* considera preferentemente la combinación de los números mediante la multiplicación; el número a se denomina divisible por el número b, cuando $a = bc$, siendo c igualmente un número racional entero. El número 0 es divisible por cualquier número; las dos unidades ± 1 dividen a todos los números, y son los únicos números que gozan de esta propiedad. Si a es divisible por b, entonces $\pm a$ será también divisible por $\pm b$, y podremos, por consiguiente, restringirnos a considerar números positivos. Todo número positivo, diferente de la unidad, es o un número *primo*, es decir un número divisible solamente por sí mismo y por la unidad, o un número *compuesto*; en este último caso, siempre se le podrá poner bajo la forma de un producto de números primos, y, lo que es más importante, no se podrá más que de una sola manera, es decir que el sistema de todos los números primos que entran a formar parte como factores en este producto está completamente determinado, así como el número

de veces que un número primo designado entra como factor. Esta propiedad reposa esencialmente sobre el teorema, de que un producto de dos factores no es divisible por un número primo más que cuando éste divide a al menos uno de los dos factores.

La manera más simple de demostrar estas proposiciones fundamentales de la teoría de los números está fundamentada enla consideración del procedimiento ya enseñado por Euclides, y que sirve para encontrar el máximo común divisor de dos números([19]): Esta operación tiene, como se sabe, por base la aplicación repetida del teorema, de que, si m designa un número positivo, entonces un número cualquiera z podrá siempre ser puesto bajo la forma $qm + r$, donde q y r designan también números enteros, de los que el segundo es *menor* que m; pues resulta de ahí que la operación deberá detenerse después de un número finito de divisiones.

La noción de la *congruencia* de los números ha sido introducida por Gauss([20]); dos números z, z' se denominan *congruentes* con respecto al módulo m, lo que se expresa por la notación

$$z \equiv z' \pmod{m},$$

cuando la diferencia $z - z'$ es divisible por m; en el caso contrario, z y z' se denominan *incongruentes* con respecto a m. Si se colocan los números, tomados dos a dos en la misma clase([21])de números o en dos clase diferentes según que sean congruentes o incongruentes con respecto a m, se concluye fácilmente del teorema recordado con anterioridad que el número de estas clases es finito, y que es igual al valor absoluto del módulo m. Esto es lo que resulta evidentemente también de los estudios de la Sección precedente; pues la definición de la congruencia establecida en la Sección I contiene a la de Gauss como caso particular. El sistema $\mathfrak{o}$ de todos los números enteros racionales es idéntico al módulo finito [1], y del mismo modo el sistema $\mathfrak{m}$ de todos los números divisibles por m es idéntico a $[m]$; la congruencia de dos números con respecto al número m coincide con su congruencia con respecto al sistema $\mathfrak{m}$; luego (según §3, 2.º, o §4, 4.º), el número de las clases es $= (\mathfrak{o}, \mathfrak{m}) = \pm m$.

§6.– *Los números complejos enteros de Gauss.*

El primer y mayor avance hacia la generalización de estas nociones ha sido hecho por Gauss, en su segunda Memoria sobre los restos bicuadráticos al transportarlos al dominio de los números complejos enteros $x + yi$, donde x e y designan números racionales enteros cualesquiera, e i siendo $= \sqrt{-1}$, es decir una raíz de la ecuación cuadrática irreducible $i^2 + 1 = 0$. Los números de este dominio son estables también bajo la adición, substracción y multiplicación, y se puede por consiguiente definir para estos números la noción de divisibilidad de la misma manera que para los números racionales. Se puede establecer muy simplemente, como Dirichlet lo ha mostrado de una

[19] *Ver*, por ejemplo, las *Vorlesungen über Zahlentheorie* de Dirichlet.

[20] *Disquisitiones arithmeticae*, art. 1.

[21] La palabra *clase* parece haber sido empleada por Gauss por primera vez en este sentido a propósito de los números *complejos*. (*Theoria residuorum biquadraticorum*, II, art. 42.)

manera muy elegante([22]), que las proposiciones generales sobre la composición de los números por medio de los números primos subsistirán también en este nuevo dominio, apoyándose sobre la siguiente observación. Si se entiende por la *norma* $\mathrm{N}(w)$ de un número $w = u + vi$, donde u y v designan números racionales cualesquiera, el producto $u^2 + v^2$ de los dos números conjugados $u + vi$ y $u - vi$, entonces la norma de un producto será igual al producto de las normas de los factores, y además está claro que, estando dado w, se podrá siempre elegir un número complejo *entero* q, de tal manera que se tenga que $\mathrm{N}(w - q) \leq \frac{1}{2}$; designando ahora por z y m dos números complejos enteros cualesquiera, en el que el segundo sea diferente de cero, resulta, si se toma $w = \frac{z}{m}$, que se podrá siempre poner $z = qm + r$, siendo q y r números complejos enteros, y esto de tal manera que se tenga que $\mathrm{N}(r) < \mathrm{N}(m)$. Se podrá pues, exactamente como para los números racionales, encontrar mediante un número finito de divisiones el máximo común divisor de dos números complejos enteros cualesquiera, y las demostraciones de las leyes generales de la divisibilidad de los números racionales enteros podrán aplicarse casi literalmente al dominio de los números complejos enteros. Hay cuatro unidades ± 1, $\pm i$, es decir cuatro números que que dividen a todos los números, y cuya norma es, por consiguiente, $= 1$. Cualquier otro número diferente de cero se denomina un número compuesto, cuando puede ser representado como el producto de dos factores de los que ninguno es una unidad; en el caso contrario, el número se denomina un número primo, y un tal número no puede dividir a un producto si no divide a al menos uno de los factores. Todo número compuesto puede siempre, y de una sola manera ser puesto bajo la forma de un producto de números primos, no contando naturalmente los cuatro números primos asociados $\pm q$, $\pm qi$ más que como los representantes de un sólo y mismo número primo q. El conjunto de todos los números primos q del dominio de los números complejos enteros se compone:

1.º De todos los números primos racionales que (tomados positivamente) son de la forma $4n + 3$;

2.º Del número $1 + i$, que divide al número primo racional $2 = (1 + i)(1 - i) = -i(1 + i)^2$;

3.º De los pares de los dos factores $a + bi$ y $a - bi$, contenidos en todo número primo racional p de la forma $4n + 1$, y cuya norma es $a^2 + b^2 = p$.

La existencia de los números primos $a \pm bi$, citados en último lugar, que resulta inmediatamente del célebre teorema de Fermat contenido en la ecuación $p = a^2 + b^2$, y que implica recíprocamente este teorema como consecuencia, se deduce aquí sin el auxilio de este teorema, con una maravillosa facilidad, y esto no es más que un primer ejemplo de la potencia extraordinaria de los principios a los cuales llegaremos mediante la máxima generalización de la idea de número entero.

La congruencia de los números complejos enteros con respecto a un número dado de la misma naturaleza m puede también definirse exactamente de la misma manera que en la teoría de los números racionales; los números z, z' se denominan congruentes con respecto a m, y se pone $z \equiv z' \pmod{m}$

[22] *Recherches sur les formes quadratiques à coefficients et à indéterminées complexes.* (Journal de Crelle, t. 24.)

cuando la diferencia $z - z'$ es divisible por m. Si se colocan los números, tomados dos a dos, en la misma clase o en dos clase diferentes según que sean congruentes o incongruentes con respecto a m, entonces el número de las clases diferentes será finito, e $= \mathrm{N}(m)$. Esto resulta muy fácilmente de las investigaciones de la primera Sección; pues el sistema $\mathfrak{o}$ de todos los números complejos enteros $x + yi$ constituye un módulo finito $[1, i]$, e igualmente el sistema $\mathfrak{m}$ de todos los números $m(x + yi)$ divisibles por m constituye un módulo $[m, mi]$, cuya base está ligada con la de $\mathfrak{o}$ por dos ecuaciones de la forma

$$m = a \cdot 1 + b \cdot i, \quad mi = -b \cdot 1 + a \cdot i;$$

por consiguiente, se tiene (§4, 4º) que

$$(\mathfrak{o}, \mathfrak{m}) = \begin{vmatrix} a & b \\ -b & a \end{vmatrix} = \mathrm{N}(m).$$

§7.– *El dominio* $\mathfrak{o}$ *de los números* $x + y\sqrt{-5}$.

Hay también otros dominios numéricos que pueden tratarse exactamente de la misma manera. Designemos, por ejemplo, por θ una raíz de una de las cinco ecuaciones

$$\theta^2 + \theta + 1 = 0, \quad \theta^2 + \theta + 2 = 0,$$
$$\theta^2 + 2 = 0, \quad \theta^2 - 2 = 0, \quad \theta^2 - 3 = 0,$$

y hagamos tomar a x, y todos los valores racionales y enteros; entonces los números $x + y\theta$ constituirán un dominio numérico correspondiente. En cada uno de estos dominios, como es fácil de comprobar, se puede encontrar el máximo común divisor de dos números mediante un número finito de divisiones, y de ahí se sigue inmediatamente que las leyes generales de la divisibilidad coinciden con las que tienen lugar para los números racionales, aunque, en los dos últimos ejemplos, se manifiesta esta particularidad, la de que el número de las unidades es infinito.

Este método, por el contrario, no es aplicable al dominio $\mathfrak{o}$ de los números enteros

$$\omega = x + y\theta,$$

donde θ es una raíz de la ecuación

$$\theta^2 + 5 = 0,$$

x, y tomando también todos los valores racionales y enteros. Aquí se encuentra ya el fenómeno que sugirió a Kummer la creación de los números ideales, y que vamos ahora a describir detalladamente con algunos ejemplos.

Los números ω del dominio $\mathfrak{o}$, de los que nos ocuparemos exclusivamente en lo que seguirá, son estables también bajo la adición, substracción y multiplicación, y definiremos, por consiguiente, exactamente como en lo que precede, las nociones de divisibilidad y de congruencia de números. Si se llama, además, norma $\mathrm{N}(\omega)$ de un número $\omega = x + y\theta$ al producto $x^2 + 5y^2$ de dos números conjugados $x \pm y\theta$, entonces la norma de un producto será igual al producto de las normas de todos los factores; y si μ es un número determinado, diferente de cero, se concluye, exactamente como antes, que $\mathrm{N}(\mu)$ expresa cuántos números hay no congruentes con respecto a μ. Si μ es una

unidad, y por lo tanto divide a todos los números, entonces necesariamente se tiene que $\mathrm{N}(\mu) = 1$, de donde $\mu = \pm 1$.

Llamaremos a un número (diferente de cero y de ± 1) *descomponible*, cuando sea el producto de dos factores ninguno de los cuales sea una unidad; en el caso contrario, el número se denominará *indescomponible*. Entonces se sigue del teorema sobre la norma de un producto que todo número descomponible puede ser puesto bajo la forma de un producto de un número finito de factores indescomponibles; pero en una infinidad de casos se presenta aquí un fenómeno totalmente nuevo, a saber, que un solo y mismo número es susceptible de varias representaciones de este tipo, esencialmente diferentes entre ellas. Los ejemplos más simples de estos casos son los siguientes. Es fácil convencerse de que cada uno de los quince números siguientes:

$$\begin{array}{cccc} a = 2, & b = 3, & c = 7; & \\ b_1 = -2 + \theta, & b_2 = -2 - \theta, & c_1 = 2 + 3\theta, & c_2 = 2 - 3\theta, \\ d_1 = 1 + \theta, & d_2 = 1 - \theta, & e_1 = 3 + \theta, & e_2 = 3 - \theta, \\ f_1 = -1 + 2\theta, & f_2 = -1 - 2\theta, & g_1 = 4 + \theta, & g_2 = 4 - \theta, \end{array}$$

es indescomponible. En efecto, para que un número primo racional p sea descomponible y, por consiguiente, de la forma $\omega\omega'$, es necesario que $\mathrm{N}(p) = p^2 = \mathrm{N}(\omega)\mathrm{N}(\omega')$, y puesto que ω, ω' no son unidades, se deberá tener que $p = \mathrm{N}(\omega) = \mathrm{N}(\omega')$, es decir que p deberá poder ser representado por la forma cuadrática binaria $x^2 + 5y^2$. Ahora bien los tres números primos 2, 3, 7, como se ve por la teoría de estas formas([23]), o también mediante un pequeño número de pruebas directas, no pueden representarse de esta manera; son pues indescomponibles. Es fácil demostrar la misma cosa, y de una manera semejante, para los otros doce números, cuyas normas son los productos de dos de estos tres números primos. Pero, a pesar de la indescomponibilidad de estos quince números, existen entre sus productos numerosas relaciones, que pueden deducirse todas de las siguientes:

$$\begin{array}{lccc} (1) & ab = d_1 d_2, & b^2 = b_1 b_2, & ab_1 = d_1^2, \\ (2) & ac = e_1 e_2, & c^2 = c_1 c_2, & ac_1 = e_1^2, \\ (3) & bc = f_1 f_2 = g_1 g_2, & af_1 = d_1 e_2, & ag_1 = d_1 e_2. \end{array}$$

En cada una de estas diez relaciones, un mismo número está representado de dos o tres maneras *diferentes* bajo la forma de un producto de dos números indescomponibles; se ve pues que un número indescomponible puede muy bien dividir a un producto, sin dividir no obstante a uno u otro de los factores; un tal número indescomponible no posee pues la propiedad que, en la teoría de los números racionales, es completamente característica para un *número primo*.

Imaginemos por un momento que los quince números precedentes sean números *racionales* enteros; entonces, según las leyes generales de la divisibilidad, se deduciría fácilmente de las relaciones (1) una descomposición de la forma

$$\begin{array}{ccc} a = \mu\alpha^2, & d_1 = \mu\alpha\beta_1, & d_2 = \mu\alpha\beta_2, \\ b = \mu\beta_1\beta_2, & b_1 = \mu\beta_1^2, & b_2 = \mu\beta_2^2, \end{array}$$

[23] *Ver* Dirichlet, *Vorlesungen über Zahlentheorie,* §71.

y del mismo modo, de las relaciones (2) una descomposición de la forma

$$a = \mu'\alpha'^2, \qquad e_1 = \mu'\alpha'\gamma_1, \qquad e_2 = \mu'\alpha'\gamma_2,$$
$$c = \mu'\gamma_1\gamma_2, \qquad c_1 = \mu'\gamma_1^2, \qquad c_2 = \mu'\gamma_2^2,$$

donde todas las letra griegas designan números racionales enteros, y resultaría inmediatamente, en virtud de la ecuación $\mu\alpha^2 = \mu'\alpha'^2$, que los cuatro números f_1, f_2, g_1, g_2, que forman parte de las relaciones (3), serían igualmente números *enteros*. Estas descomposiciones se simplifican si se introduce, además, la hipótesis de que a es un número primo con b y con c, pues de ahí se obtiene que $\mu = \mu' = 1$, $\alpha = \alpha'$, y se obtienen los quince números, expresados como sigue, por medio de los cinco números α, β_1, β_2, γ_1, γ_2,

$$(4) \qquad \begin{cases} a = \alpha^2, & b = \beta_1\beta_2, & c = \gamma_1\gamma_2; & \\ b_1 = \beta_1^2, & b_2 = \beta_2^2; & c_1 = \gamma_1^2, & c_2 = \gamma_2^2; \\ d_1 = \alpha\beta_1, & d_2 = \alpha\beta_2; & e_1 = \alpha\gamma_1, & e_2 = \alpha\gamma_2; \\ f_1 = \beta_1\gamma_1, & f_2 = \beta_2\gamma_2; & g_1 = \beta_1\gamma_2, & g_2 = \beta_2\gamma_1. \end{cases}$$

Aunque ahora nuestros quince números sean en realidad indescomponibles, se comportan no obstante, cosa notable, en todas las cuestiones de divisibilidad relativas al dominio $\mathfrak{o}$, exactamente como si fueran compuestos, de la manera indicada antes, por medio de los cinco *números primos* α, β_1, β_2, γ_1, γ_2, diferentes los unos de los otros. Voy a exponer dentro de poco con detalle lo que es menester entender por esta relación entre los números.

§8.– *Papel del número* 2 *en el dominio* $\mathfrak{o}$.

Con tal objeto, observo ante todo que, en la teoría de los números racionales enteros, se puede reconocer completamente la constitución esencial de un número, sin *llevar a cabo la descomposición* en factores primos, observando solamente la manera de la que se comporta como *divisor*. Si se sabe, por ejemplo, que un número positivo a no divide a un producto de dos cuadrados más que si uno al menos de estos cuadrados es divisible por a, entonces se concluye con certeza que a es igual a 1, o que es un número primo o el cuadrado de un número primo. Es igualmente cierto que un número a debe contener al menos un factor cuadrado, aparte de la unidad, cuando se puede demostrar la existencia de un número no divisible por a, y cuyo cuadrado es divisible por a. Si se puede pues constatar, para un número a, uno y otro de estos dos caracteres, entonces se concluye de una manera segura que a es el *cuadrado de un número primo*.

Vamos ahora a examinar, en este sentido, como se comporta el número 2 en nuestro dominio $\mathfrak{o}$ de los números $\omega = x + y\theta$. Puesto que dos números conjugados cualesquiera son congruentes con respecto al módulo 2, se tendrá que

$$\omega^2 \equiv \mathrm{N}(\omega) \pmod 2,$$

y por consiguiente también que $\omega^2\omega'^2 \equiv \mathrm{N}(\omega)\mathrm{N}(\omega')$ (mód 2); ahora, para que el número 2 divida al producto $\omega^2\omega'^2$, y por consiguiente también al producto de los dos números *racionales* $\mathrm{N}(\omega)$, $\mathrm{N}(\omega')$, es necesario que al menos una de estas normas, y por consiguiente también que uno al menos de los dos cuadrados ω^2, ω'^2 sean divisibles por 2. Si además se eligen como x, y dos números impares cualesquiera, entonces se obtiene un número $\omega = x+y\theta$

que no es divisible por 2, y cuyo cuadrado es divisible por 2. Tomando en consideración las observaciones precedentes sobre los números racionales, diremos pues que el número 2 se comporta en nuestro dominio $\mathfrak{o}$ como si fuera el cuadrado de un número primo α.

Aunque un tal número primo α no existe de ningún modo en el dominio $\mathfrak{o}$, nosotros no introduciremos sin embargo, tal como ha hecho Kummer con gran éxito en circunstancias semejantes, un tal número α bajo el nombre de *número ideal*, y nos dejaremos en primer lugar conducir por la analogía con la teoría de los números racionales, para definir con precisión la presencia del número α dentro de los números *existentes* cualesquiera ω del dominio $\mathfrak{o}$. Ahora bien, cuando un número racional a ya es reconocido como siendo el cuadrado de un número primo racional α, se puede fácilmente, *sin incluso tener que hacer intervenir* a α, juzgar si α está contenido y cuántas veces está contenido como factor en un número racional entero cualquiera z; pues está claro que z es divisible por a^n siempre, y entonces solamente, cuando z^2 es divisible por a^n. Extenderemos pues este criterio al caso que nos ocupa, y diremos que un número ω del dominio $\mathfrak{o}$ es *divisible* por la n-sima *potencia* α^n del número primo ideal α, cuando ω^2 sea divisible por 2^n. El *éxito* hará ver que esta definición está muy felizmente([24]) elegida, porque conduce a un modo de expresión que está en perfecta harmonía con las leyes de la teoría de los números racionales.

Se sigue en primer lugar, para $n = 1$, que un número $x + y\theta$ es divisible por α en el caso, y solamente en el caso, en que $\mathrm{N}(\omega)$ es un número par, y donde se tiene, por consiguiente, que

$$(\alpha) \qquad x \equiv y \pmod 2.$$

El número ω *no es* divisible por α, cuando $\mathrm{N}(\omega)$ es un número impar, y se tiene por consiguiente que $x \equiv 1 + y \pmod 2$; y de ahí resulta evidentemente el teorema en el cual se reconocerá el carácter del número ideal α como número primo: "Todo producto de dos números no divisibles por α es también no divisible por α".

Relativamente a las potencias superiores de α, se concluye en primer lugar de la definición que un número ω divisible por α^n lo es también por todas las potencias inferiores de α, puesto que un número ω^2 divisible por 2^n lo es también por todas las potencias inferiores de 2. Vamos ahora, si ω es diferente de cero, a buscar el exponente m de la *más alta* potencia de α que divide a ω, es decir el exponente de la más alta potencia de 2 que divide a ω^2. Sea s el exponente de la más alta potencia de 2 que divide a ω mismo; entonces se tendrá que

$$\omega = 2^s\omega_1 = 2^s(x_1 + y_1\theta),$$

y uno al menos de los dos números racionales enteros x_1, y_1 será impar; si los dos son impares, entonces ω_1 será divisible por α, y se tendrá que

$$\omega_1^2 = x_1^2 - 5y_1^2 + 2x_1y_1\theta = 2\omega_2,$$

[24] *Felizmente*, pues, por ejemplo, el intento de determinar de una manera análoga el papel del número 2 en el dominio de los números $x+y\sqrt{-3}$ habría fracasado completamente; más tarde descubriremos claramente la razón de este fenómeno.

no siendo $\omega_2 = x_2 + y_2\theta$ divisible por α, puesto que x_2 es par e y_2 impar; pero si uno de los dos números x_1, y_1 es par , y por lo tanto el otro impar, entonces ω_1, y por consiguiente también ω_1^2, no serán divisibles por α. Luego, en el primer caso, $m = 2s + 1$; en el segundo caso, $m = 2s$; pero en los dos casos $\omega^2 = 2^m\omega'$, donde ω' designa un número no divisible por α. Se ve al mismo tiempo que m es también el exponente de la más alta potencia de 2 que divide la norma $\mathrm{N}(\omega)$; se tiene pues el teorema: "El exponente de la más alta potencia de α que divide a un producto es igual a la suma de los exponentes de las más altas potencias de α que dividen a los factores". Es igualmente evidente que todo número ω divisible por α^{2n} es también divisible por 2^n; pues si el exponente designado antes por s fuera $< n$, entonces los números $2s$, $2s + 1$, y por consiguiente también m serían $< 2n$, contrariamente a la hipótesis. Se sigue inmediatamente de la definición que, recíprocamente, todo número divisible por 2^n lo es también por α^{2n}.

Siendo el número $1 + \theta$ divisible por α, pero no por α^2, se reconoce fácilmente, con la ayuda del teorema precedente, que la congruencia $\omega^2 \equiv 0$ (mód 2^n), que ha servido de definición para la divisibilidad del número ω por α^n, puede ser completamente reemplazada por la congruencia

$$(\alpha^n) \qquad \omega(1 + \theta)^n \equiv 0 \pmod{2^n},$$

que tiene la ventaja de no contener el número ω más que a la *primera* potencia.

§9.– *Papel de los números* 3 *y* 7 *en el dominio* $\mathfrak{o}$.

Cuando todas las cantidades que ocurren en las ecuaciones (4) del §7 son números *racionales* enteros, y al mismo tiempo a es primo con b y con c, entonces es evidente que un número racional entero cualquiera z será o no será divisible por β_1, β_2, γ_1, γ_2, según que satisfaga o no satisfaga la congruencia correspondiente

$$\begin{aligned} zd_2 \equiv 0, \quad zd_1 \equiv 0 \pmod{b}, \\ ze_2 \equiv 0, \quad ze_1 \equiv 0 \pmod{c}. \end{aligned}$$

Estas congruencias tienen ahora la peculiariedad de que los números β_1, β_2, γ_1, γ_2 no ocurren allí de ningún modo por ellos mismos, y es precisamente por eso por lo que, en el caso que tratamos efectivamente, y en el que se trata de números del dominio $\mathfrak{o}$, son apropiados para servir para la introducción de cuatro números ideales β_1, β_2, γ_1, γ_2. Diremos que que un número cualquiera $\omega = x + y\theta$ es *divisible* por uno de estos cuatro números, si ω es una raíz de la congruencia correspondiente

$$\begin{aligned} (1 - \theta)\omega \equiv 0, \quad (1 + \theta)\omega \equiv 0 \pmod{3}, \\ (3 - \theta)\omega \equiv 0, \quad (3 + \theta)\omega \equiv 0 \pmod{7}. \end{aligned}$$

Efectuando la multiplicación, estas congruencias se transforman en las siguientes

$$(\beta_1) \qquad z \equiv y \pmod 3,$$
$$(\beta_2) \qquad z \equiv -y \pmod 3,$$
$$(\gamma_1) \qquad z \equiv 3y \pmod 7,$$
$$(\gamma_2) \qquad z \equiv -3y \pmod 7.$$

A esto añadiremos las observaciones siguientes.

Cada una de estas condiciones puede ser satisfecha por uno de los números $\omega = 1+\theta$, $1-\theta$, $3+\theta$, $3-\theta$, no satisfaciendo el número en cuestión a ninguna de las otras tres, y se sigue de ahí que es legítimo llamar a estos cuatro números ideales *diferentes entre sí*. Como, además, todo número ω divisible por β_1 y por β_2 es también divisible por 3, puesto que se debe tener que $x \equiv y \equiv -y \equiv 0$ (mód 3), y recíprocamente todo número divisible por 3 es también divisible por cada uno de los números β_1, β_2, se debería, por analogía con la teoría de los números racionales, considerar al número 3 como el mínimo común múltiplo de los dos números ideales β_1, β_2. Pero cada uno de estos dos números ideales posee también el carácter de un número primo, es decir que no divide a un producto $\omega\omega'$ más que cuando divide a uno al menos de los factores ω, ω'; si se pone, en efecto,

$$\omega = x + y\theta, \quad \omega' = x' + y'\theta, \quad \omega'' = \omega\omega' = x'' + y''\theta,$$

entonces se tendrá que

$$x'' = xx' - 5yy', \quad y'' = xy' - yx',$$

y por consiguiente que

$$x'' \pm y'' \equiv (x \pm y)(x' \pm y') \pmod 3,$$

lo cual verifica inmediatamente nuestra aserción, tomando en consideración las congruencias anteriores (β_1), (β_2). Según eso, el número 3 deberá ser considerado, desde un cierto punto de vista, como el producto de los dos números primos ideales diferentes β_1, β_2.

Como, además, cada uno de estos dos números primos ideales β_1, β_2 es diferente (en el sentido indicado anteriormente) del número primo ideal α introducido antes, entonces, observando que 2 se comporta como el cuadrado de α, y que $1+\theta$ es divisible por α y por β_1, lo mismo que $1-\theta$ es divisible por α y por β_2, se deberá concluir, de la ecuación $2.3 = (1+\theta)(1-\theta)$, que $1+\theta$ se comporta como el producto de α y de β_1, y $1-\theta$ como el producto de α y de β_2. Esta *presunción* se confirma en efecto plenamente: todo número $\omega = x + y\theta$ divisible por $1+\theta$ es, en efecto, divisible por α y por β_1, puesto que

$$x + y\theta = (1+\theta)(x' + y'\theta),$$

de donde

$$x = x' - 5y', \quad y = x' + y',$$

y por consiguiente

$$x \equiv y \pmod 2, \quad x \equiv y \pmod 3;$$

y recíprocamente, todo número $\omega = x+y\theta$, divisible por α y por β_1, es decir que satisface las dos congruencias precedentes, es también divisible por $1+\theta$, puesto que se tiene que $y = x + 6y'$, y por consiguiente

$$x + y\theta = (1 + \theta)(x + 5y' + y'\theta).$$

Se pueden ahora introducir también las *potencias* de los números primos ideales β_1, β_2, como se ha hecho antes para las potencias del número ideal α; por analogía con la teoría de los números racionales, definiremos la divisibilidad de un número cualquiera ω por β_1^n o por β_2^n, respectivamente por las congruencias

$$(\beta_1^n) \qquad \omega(1-\theta)^n \equiv 0 \pmod{3^n},$$

$$(\beta_2^n) \qquad \omega(1+\theta)^n \equiv 0 \pmod{3^n},$$

y resultaría una sucesión de teoremas que coincidirían perfectamente con aquéllos de la teoría de los números racionales. Se trataría de la misma manera a los números primos ideales γ_1, γ_2.

§10.– *Leyes de la divisibilidad en el dominio* $\mathfrak{o}$.

Estudiando de una manera semejante todo el dominio $\mathfrak{o}$ de los números $\omega = x + y\theta$, se encuentran los resultados siguientes:

1.º Todos los números primos racionales positivos que son $\equiv 11, 13, 17, 19 \pmod{20}$ se comportan también, en el caso actual, como números primos.

2.º El número θ, cuyo cuadrado es $= -5$, posee el carácter de un número primo; el número 2 se comporta como el cuadrado de un número primo ideal α.

3.º Todo número primo racional positivo que es $\equiv 1, 9 \pmod{20}$ puede descomponerse en dos factores diferentes, realmente existentes, de los que cada uno tiene el carácter de un número primo.

4.º Todo número primo racional positivo que es $\equiv 3, 7 \pmod{20}$ se comporta como un producto de dos números primos ideales diferentes entre sí.

5.º Todo número existente ω, diferente de cero y de ± 1, es o uno de los números designados antes que tienen el carácter de número primo, o bien se comporta, en todas las cuestiones de divisibilidad, como si fuera un producto compuesto de una manera completamente determinada por factores primos existentes e ideales.

Pero, para llegar a este resultado y adquirir una certeza completa sobre la cuestión de saber si, en realidad, todas las leyes generales de la divisibilidad que gobiernan el dominio de los números racionales pueden extenderse a nuestro dominio $\mathfrak{o}$ con la ayuda de los números ideales que hemos introducido([25]), es necesario también, como se verá pronto cuando se intente una deducción rigurosa, realizar un estudio muy profundo, aun cuando se quisiera suponer conocida aquí la teoría de los restos cuadráticos y la de las formas cuadráticas binarias (teoría que, recíprocamente, se deriva con la máxima

[25]Es posible que a algunas personas les parezca evidente *a priori* que el restablecimiento de esta harmonía con la teoría de los números racionales deba poder *imponerse*, suceda lo que suceda, con la introducción de los números ideales; pero el ejemplo, ya dado más arriba, del papel irregular del número 2 en el dominio de los números $x + y\sqrt{-3}$, es más que suficiente para disipar esta ilusión.

facilidad de la teoría general de los números algebraicos enteros). Se puede de hecho alcanzar con todo el rigor el objetivo propuesto, siguiendo la vía indicada; pero, como hemos observado en la Introducción, es necesaria la máxima circunspección para no dejarse arrastrar a conclusiones prematuras y, en particular, la noción de *producto* de factores cualesquiera, existentes o ideales, no puede ser exactamente definida más que con la ayuda de detalles bastante minuciosos. Debido a estas dificultades, parecerá deseable reemplazar el número ideal de Kummer, que no es jamás definido en sí mismo, sino solamente como divisor de los números existentes ω del dominio $\mathfrak{o}$, por un *substantivo* realmente existente, y esto se puede hacer de varias maneras.

Se podría, por ejemplo (y si no me engaño, esta sería la vía que Kronecker habría elegido en sus investigaciones), introducir, en lugar de los números ideales, números algebraicos existentes, pero no incluidos en el dominio $\mathfrak{o}$, y *adjuntarlos* a este dominio en el sentido que Galois ha dado a esta palabra. En efecto, si se pone

$$\beta_1 = \sqrt{-2+\theta}, \quad \beta_2 = \sqrt{-2-\theta},$$

y si se eligen estas raíces cuadradas de manera que que se tenga $\beta_1\beta_2 = 3$, se tendrá que

$$\begin{array}{ccc} \theta^2 = -5, & \beta_1^2 = -2+\theta, & \beta_2^2 = -2-\theta, \\ \beta_1\beta_2 = 3, & \theta\beta_1 = -2\beta_1 - 3\beta_2, & \theta\beta_2 = 3\beta_1 + 2\beta_2, \end{array}$$

de donde se sigue que los números expresables bajo la forma de cuadrinomios

$$x + y\theta + z_1\beta_1 + z_2\beta_2,$$

donde x, y, z_1, z_2 designan números racionales enteros cualesquiera, son estables bajo la adición, substracción y multiplicación; el dominio $\mathfrak{o}'$ de estos números abarca al dominio $\mathfrak{o}$, y todos los números ideales que era menester introducir en este último podrán ser reemplazados por números existentes del nuevo dominio $\mathfrak{o}'$. Poniendo, por ejemplo,

$$\alpha = \beta_1 + \beta_2, \quad \gamma_1 = 2\beta_1 + \beta_2, \quad \gamma_2 = \beta_1 + 2\beta_2,$$

todas las ecuaciones (4) del §7 serán satisfechas; igualmente, los dos factores primos ideales del número 23 en el dominio $\mathfrak{o}$ serán reemplazados por los dos números existentes $2\beta_1 - \beta_2$ y $-\beta_1 + 2\beta_2$ del dominio $\mathfrak{o}'$, y lo mismo sucederá con todos los números ideales del dominio $\mathfrak{o}$.

No obstante esta vía, aun cuando pueda también conducir al objetivo, no me parece que presente toda la simplicidad deseable, porque se está forzado a pasar del dominio dado $\mathfrak{o}$ a un dominio más complicado $\mathfrak{o}'$; y es fácil también reconocer que en la elección de este nuevo dominio $\mathfrak{o}'$ reina una gran arbitrariedad. En la Introducción, he expuesto con tantos detalles la corriente de ideas que me ha conducido a fundamentar esta teoría sobre una base muy distinta, a saber, sobre la noción de *ideal*, que sería superfluo volver a ello aquí, y me limitaré, como consecuencia, a aclarar esta noción mediante un ejemplo.

§11.– *Ideales en el dominio* $\mathfrak{o}$.

La condición para que un número $\omega = x + y\theta$ sea divisible por el número primo ideal α consiste, según el §8, en la congruencia $x \equiv y \pmod 2$; luego,

para obtener el sistema $\mathfrak{a}$ de todos los números ω divisibles por α, pondremos $x = y + 2z$, donde y y z designan números racionales enteros cualesquiera; este sistema $\mathfrak{a}$ se compone pues de todos los números de la forma $2z+(1+\theta)y$, es decir que $\mathfrak{a}$ es un *módulo finito*, cuya base se compone de los dos números independientes 2 y $1+\theta$, y por consiguiente

$$\mathfrak{a} = [2, 1+\theta].$$

Designando del mismo modo por $\mathfrak{b}_1$, $\mathfrak{b}_2$, $\mathfrak{c}_1$, $\mathfrak{c}_2$ los sistemas de todos los números ω divisibles respectivamente por los números primos ideales β_1, β_2, γ_1, γ_2, se obtendrá, de las congruencias correspondientes del §9, que

$$\mathfrak{b}_1 = [3, 1+\theta], \quad \mathfrak{b}_2 = [3, 1-\theta],$$
$$\mathfrak{c}_1 = [7, 3+\theta], \quad \mathfrak{c}_2 = [7, 3-\theta].$$

Si se designa ahora por $\mathfrak{m}$ a uno cualquiera de estos cinco sistemas, entonces $\mathfrak{m}$ gozará de las propiedades siguientes:

I. Las sumas y las diferencias de dos números cualesquiera del sistema $\mathfrak{m}$ serán siempre números de este mismo sistema $\mathfrak{m}$.

II. Todo producto de un número del sistema $\mathfrak{m}$ y de un número del sistema $\mathfrak{o}$ es un número del sistema $\mathfrak{m}$.

La primera propiedad, característica de cada módulo, es evidente. Para constatar la segunda propiedad relativamente al sistema $\mathfrak{m}$, cuya base se compone de los dos números μ, μ', es suficiente evidentemente que se demuestre que los dos productos $\theta\mu$, $\theta\mu'$ pertenecen al mismo sistema; para el sistema $\mathfrak{a}$, eso resulta de las dos igualdades

$$2\theta = -1 \cdot 2 + 2(1+\theta), \quad (1+\theta)\theta = -3 \cdot 2 + (1+\theta),$$

y lo mismo exactamente para los otros sistemas. Pero estas dos propiedades pueden también establecerse sin estas verificaciones, apoyándose en que cada uno de los cinco sistemas $\mathfrak{m}$ es el conjunto de todos los números ω del dominio $\mathfrak{o}$ que satisfacen una congruencia de la forma

$$\nu\omega \equiv 0 \pmod{\mu},$$

siendo μ, ν dos números dados del dominio $\mathfrak{o}$.

Llamaremos ahora a *todo* sistema $\mathfrak{m}$, compuesto por números del dominio $\mathfrak{o}$ y que goza de las dos propiedades I y II, un *ideal*, y nos plantearemos en primer lugar el problema de encontrar la *forma* general de todos los ideales. Excluyendo el caso singular en el que $\mathfrak{m}$ se componga sólo del número cero, y eligiendo arbitrariamente un número μ (diferente de cero), del ideal $\mathfrak{m}$, entonces, si se designa por μ' el número conjugado, la norma $\mathrm{N}(\mu) = \mu\mu'$, así como el producto $\theta\mathrm{N}(\mu)$, pertenecerá también, en virtud de II, al ideal $\mathfrak{m}$; luego todos los números del módulo $\mathfrak{o} = [1, \theta]$, multiplicándolos por el número racional $\mathrm{N}(\mu)$ diferente de cero, se transformarán en números del módulo $\mathfrak{m}$, el cual es al mismo tiempo un *múltiplo* de $\mathfrak{o}$; ahora bien, se sigue de ahí (§3, 2°) que $\mathfrak{m}$ es un módulo finito, de la forma $[k, l+m\theta]$, siendo k, l, m números racionales enteros, entre los cuales k y m podrán ser elegidos *positivos*. Puesto que $\mathfrak{m}$ posee ya, como módulo, la propiedad I, ahora no se trata más que de someterlo a la propiedad II, que consiste en que los dos productos $k\theta$ y $(l+m\theta)\theta$ pertenecen al mismo módulo $\mathfrak{m}$. Las condiciones necesarias y suficientes para esto consisten, como se ve sin esfuerzo, en que

k y l sean divisibles por m y que los números racionales enteros a, b, que ocurren en la expresión

$$\mathfrak{m} = [ma, m(b+\theta)],$$

satisfagan, además, la congruencia

$$b^2 \equiv -5 \pmod{a};$$

si se reemplaza b por un número cualquiera que sea $\equiv b \pmod{a}$, entonces el ideal $\mathfrak{m}$ no cambiará. Los cinco ideales anteriores $\mathfrak{a}$, $\mathfrak{b}_1$, $\mathfrak{b}_2$, $\mathfrak{c}_1$, $\mathfrak{c}_2$ están evidentemente contenidos en esta forma, pues $(b+\theta)$ puede también ser reemplazado por $-(b+\theta)$.

El conjunto de todos los números conjugados de los números del ideal $\mathfrak{m}$ es evidentemente también un ideal

$$\mathfrak{m}_1 = [ma, m(-b+\theta)];$$

dos ideales de este tipo $\mathfrak{m}$, $\mathfrak{m}_1$ pueden ser llamados ideales *conjugados*.

Sea μ un número cualquiera del dominio $\mathfrak{o}$; entonces el sistema $[\mu, \mu\theta]$ de todos los números divisibles por μ constituirá un ideal, que llamaremos un *ideal principal*([26]), y que designaremos por $\mathfrak{o}(\mu)$ o también por $\mathfrak{o}\mu$; es fácil darle la forma anterior $[ma, m(b+\theta)]$; m es el máximo número racional entero que divide a $\mu = m(u+v\theta)$, y se tiene, además que

$$a = \frac{\mathrm{N}(\mu)}{m^2}, \quad vb \equiv u \pmod{a}.$$

Encontramos así, por ejemplo,

$$\mathfrak{o}(\pm 1) = \mathfrak{o} = [1, \theta],$$

y

$$\begin{gathered}
\mathfrak{o}(2) = [2, 2\theta], \quad \mathfrak{o}(3) = [3, 3\theta], \quad \mathfrak{o}(7) = [7, 7\theta], \\
\mathfrak{o}(1 \pm \theta) = [6, \pm 1 + \theta], \qquad \mathfrak{o}(3 \pm \theta) = [14, \pm 3 + \theta], \\
\mathfrak{o}(-2 \pm \theta) = [9, \mp 2 + \theta], \qquad \mathfrak{o}(2 \pm 3\theta) = [49, \pm 17 + \theta], \\
\mathfrak{o}(-1 \pm 2\theta) = [21, \pm 10 + \theta], \quad \mathfrak{o}(4 \pm \theta) = [21, \pm 4 + \theta].
\end{gathered}$$

Puesto que todos los ideales son al mismo tiempo módulos, diremos (según el §2, 1.º) que dos números ω, ω' son *congruentes* con respecto al ideal $\mathfrak{m}$, y pondremos $\omega \equiv \omega' \pmod{\mathfrak{m}}$, cuando la diferencia $\omega - \omega'$ sea un número contenido en $\mathfrak{m}$; la norma $\mathrm{N}(\mathfrak{m})$ del ideal $\mathfrak{m} = [ma, m(b+\theta)]$ será el número

$$(\mathfrak{o}, \mathfrak{m}) = m^2 a$$

de las *clases* en las cuales se descompone el dominio $\mathfrak{o}$ con respecto al módulo $\mathfrak{m}$ (§4, 4.º). Si $\mathfrak{m}$ es un ideal principal $\mathfrak{o}\mu$, entonces la congruencia precedente coincidirá con $\omega \equiv \omega' \pmod{\mu}$, y se tendrá que

$$\mathrm{N}(\mathfrak{m}) = \mathrm{N}(\mu).$$

La norma de un número cualquiera $m(ax + (b+\theta)y)$ contenido en el ideal $\mathfrak{m} = [ma, m(b+\theta)]$ es igual al producto de $\mathrm{N}(\mathfrak{m}) = m^2 a$ por la forma

[26] Si se extiende la definición de ideal al dominio $\mathfrak{o}$ de los números racionales enteros, o al de los números complejos enteros de Gauss, o a uno de los cinco dominios $\mathfrak{o}$ de los que nos hemos ocupado en §7, entonces se ve fácilmente que todo ideal es un ideal principal; también es evidente que, en el dominio de los números racionales enteros, la propiedad II está ya contenida en la propiedad I.

cuadrática binaria $ax^2 + 2bxy + cy^2$, cuyo determinante, según la definición de Gauss, es $b^2 - ac = -5$ ([27]).

§12.– *Divisibilidad y multiplicación de los ideales en el dominio* $\mathfrak{o}$.

Voy ahora a mostrar de qué manera la teoría de los números $\omega = x + y\theta$ del dominio $\mathfrak{o}$ puede fundamentarse sobre la noción del ideal; no obstante, estaré obligado, para abreviar, a dejar al lector el cuidado de desarrollar algunos cálculos fáciles.

Diremos, exactamente igual que en la teoría de los módulos (§1, 2º), que un ideal $\mathfrak{m}''$ es *divisible* por un ideal $\mathfrak{m}$, cuando todos los números del primero estén contenidos también en el segundo. Según eso, un ideal principal $\mathfrak{o}\mu''$ será siempre divisible por un ideal principal $\mathfrak{o}\mu$ en el caso, y solamente en el caso, en el que el número μ'' sea divisible por el número μ; de ahí resulta que la teoría de la divisibilidad de los números *está contenida* en la de los ideales. Las condiciones necesarias y suficientes para que el ideal $\mathfrak{m}'' = [m''a'', m''(b'' + \theta)]$ sea divisible por el ideal $\mathfrak{m} = [ma, m(b + \theta)]$ consisten, como se advierte inmediatamente, en las tres congruencias

$$m''a \equiv m''a'' \equiv m''(b'' - b) \equiv 0 \pmod{ma}.$$

La definición de la *multiplicación* de los ideales es ésta: Si μ recorre todos los números del ideal $\mathfrak{m}$, y del mismo modo μ' todos los números del ideal $\mathfrak{m}'$, entonces todos los productos $\mu\mu'$ y sus sumas constituirán un ideal $\mathfrak{m}''$, que se denominará el *producto*([28]) de los factores $\mathfrak{m}$, $\mathfrak{m}'$, y que se designará por $\mathfrak{m}\mathfrak{m}'$. Se tendrá evidentemente $\mathfrak{o}\mathfrak{m} = \mathfrak{m}$, $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}'\mathfrak{m}$, $(\mathfrak{m}\mathfrak{m}')\mathfrak{n} = \mathfrak{m}(\mathfrak{m}'\mathfrak{n})$, y de ahí se siguen, para los productos de un número cualquiera de ideales, los mismos teoremas que para los productos de números([29]); además, está claro que el producto de los dos ideales principales $\mathfrak{o}\mu$ y $\mathfrak{o}\mu'$ es el ideal principal $\mathfrak{o}(\mu\mu')$.

Sean dados ahora dos ideales,

$$\mathfrak{m} = [ma, m(b + \theta)], \quad \mathfrak{m}' = [m'a', m'(b' + \theta)];$$

se deducirá de ahí su producto

$$\mathfrak{m}\mathfrak{m}' = \mathfrak{m}'' = [m''a'', m''(b'' + \theta)],$$

con la ayuda de los métodos indicados en la primera Sección (§4, 5.º y 6.º); pues está claro en principio, en virtud de la definición, que el producto $\mathfrak{m}\mathfrak{m}'$ es un módulo finito, cuya base se compone de los *cuatro* productos

$$mm'aa', \quad mm'a(b' + \theta), \quad mm'a(b + \theta),$$
$$mm'a(b + \theta)(b' + \theta) = mm'[bb' - 5 + (b + b')\theta],$$

de los que solo *dos* son independientes entre sí. Se encuentra de este modo, por ejemplo, para los ideales considerados con anterioridad,

$$\mathfrak{b}_1 = [3, 1 + \theta], \quad \mathfrak{c}_2 = [7, 3 - \theta],$$

---

[27] La teoría de las formas cuadráticas se simplifica sin embargo un poco si se admiten también las formas $Ax^2 + Bxy + Cy^2$, donde B es impar, y si se entiende siempre por determinante de la forma el número $B^2 - 4AC$.

[28] La misma definición se aplica también a la multiplicación de dos *módulos* cualesquiera.

[29] *Ver* Dirichlet, *Vorlesungen über Zahlentheorie*, §2.

el producto

$$\mathfrak{b}_1\mathfrak{c}_2 = [21, 9-3\theta, 7+7\theta, 8+2\theta];$$

este módulo se deduce del que ha sido considerado al final de la primera Sección (§4, 6.º), haciendo $\omega_1 = 1$, $\omega_2 = \theta$, y se obtiene que

$$\mathfrak{b}_1\mathfrak{c}_2 = [21, -17+\theta] = [21, 4+\theta] = \mathfrak{o}(4+\theta);$$

se obtendrían exactamente de la misma manera los resultados siguientes, totalmente análogos a las ecuaciones hipotéticas (4) del §7:

$$\begin{aligned}
\mathfrak{o}(2) &= \mathfrak{a}^2, \quad \mathfrak{o}(3) = \mathfrak{b}_1\mathfrak{b}_2, \quad \mathfrak{o}(7) = \mathfrak{c}_1\mathfrak{c}_2;\\
\mathfrak{o}(-2+\theta) &= \mathfrak{b}_1^2, \qquad \mathfrak{o}(-2-\theta) = \mathfrak{b}_2^2;\\
\mathfrak{o}(2+3\theta) &= \mathfrak{c}_1^2, \qquad \mathfrak{o}(2-3\theta) = \mathfrak{c}_2^2;\\
\mathfrak{o}(1+\theta) &= \mathfrak{a}\mathfrak{b}_1, \qquad \mathfrak{o}(1-\theta) = \mathfrak{a}\mathfrak{b}_2;\\
\mathfrak{o}(3+\theta) &= \mathfrak{a}\mathfrak{c}_1, \qquad \mathfrak{o}(3-\theta) = \mathfrak{a}\mathfrak{c}_2;\\
\mathfrak{o}(-1+2\theta) &= \mathfrak{b}_1\mathfrak{c}_1, \qquad \mathfrak{o}(-1-2\theta) = \mathfrak{b}_2\mathfrak{c}_2;\\
\mathfrak{o}(4+\theta) &= \mathfrak{b}_1\mathfrak{c}_2, \qquad \mathfrak{o}(4-\theta) = \mathfrak{b}_2\mathfrak{c}_1.
\end{aligned}$$

Para llevar a cabo *en general* la multiplicación de dos ideales cualesquiera $\mathfrak{m}$, $\mathfrak{m}'$, es necesario transformar la base compuesta por los cuatro números anteriores en otra compuesta solamente por los dos números $m''a''$, $m''(b''+\theta)$. Se llega a ello (en virtud del §4), por medio de las cuatro ecuaciones de la forma

$$\begin{aligned}
mm'aa' &= pm''a'' + qm''(b''+\theta),\\
mm'a(b'+\theta) &= p'm''a'' + q'm''(b''+\theta),\\
mm'a'(b+\theta) &= p''m''a'' + q''m''(b''+\theta),\\
mm'[bb'-5+(b+b')\theta] &= p'''m''a'' + q'''m''(b''+\theta),
\end{aligned}$$

donde p, p',..., q''' designan ocho números racionales enteros elegidos de tal modo que los seis determinantes, formados con estos números,

$$\begin{aligned}
&P = pq' - qp', \qquad Q = pq'' - qp'', \qquad R = pq''' - qp''',\\
&U = p''q''' - q''p''', \quad T = p'q''' - q'p''', \quad S = p'q'' - q'p'',
\end{aligned}$$

no admiten ningún divisor común. De las cuatro ecuaciones precedentes, de las que cada una se descompone en otras dos, se concluirá ahora sin dificultad que estos seis determinantes son respectivamente proporcionales a los seis números

$$\begin{aligned}
&a, \quad a', \quad b'+b,\\
&c, \quad c', \quad b'-b,
\end{aligned}$$

estando c y c' determinados por las ecuaciones

$$bb - ac = b'b' - a'c' = -5;$$

ahora bien, puesto que estos seis números no admiten ningún divisor común ([30]), deberán coincidir precisamente con estos seis determinantes. Se sigue de ahí, puesto que se tiene que $q = 0$, y que q', q'', q''' no pueden tener ningún divisor común, que se determinará como sigue el producto $\mathfrak{m}'' = \mathfrak{m}\mathfrak{m}'$ de dos

[30] Esto no será siempre así en el dominio de los números $x + y\sqrt{-3}$.

factores dados $\mathfrak{m}$, $\mathfrak{m}'$. Sea p el máximo común divisor (positivo) de los tres números dados

$$a = pq', \quad a' = pq'', \quad b + b' = pq''';$$

entonces se tendrá que

$$m'' = pmm', \quad a'' = \frac{aa'}{p^2} = q'q'',$$

y b'' estará determinado por las congruencias

$$q'b'' \equiv q'b', \quad q''b'' \equiv q''b, \quad q'''b'' \equiv \frac{bb' - 5}{p} \pmod{a''};$$

además se tendrá al mismo tiempo que $b''b'' \equiv -5 \pmod{a''}$, es decir que

$$b''b'' - a''c'' = -5,$$

donde c'' designa un número racional entero, y, según la denominación empleada por Gauss([31]), la forma cuadrática binaria (a'', b'', c'') estará *compuesta* a partir de las dos formas (a, b, c) y (a', b', c').

De los valores de m'', a'' se obtiene $m''^2 a'' = m^2 a \cdot m'^2 a'$, de donde este teorema

$$\mathrm{N}(\mathfrak{m}\mathfrak{m}') = \mathrm{N}(\mathfrak{m})\mathrm{N}(\mathfrak{m}');$$

además, es necesario notar el caso particular en el que $\mathfrak{m}'$ es el ideal $\mathfrak{m}_1$ conjugado con $\mathfrak{m}$; de las fórmulas precedentes se deduce inmediatamente este resultado

$$\mathfrak{m}\mathfrak{m}_1 = \mathfrak{o}\mathrm{N}(\mathfrak{m}).$$

Las dos nociones de la *divisibilidad* y de la *multiplicación* de los ideales están ahora ligadas entre sí de la siguiente manera. El producto $\mathfrak{m}\mathfrak{m}'$ es divisible a la vez por $\mathfrak{m}$ y por $\mathfrak{m}'$, puesto que, en virtud de la propiedad II de los ideales, todos los productos $\mu\mu'$, cuyos factores están contenidos respectivamente en $\mathfrak{m}$, $\mathfrak{m}'$, pertenecen igualmente a estos ideales; se obtendrá la misma conclusión de la forma del ideal producto encontrada con anterioridad. Recíprocamente, si el ideal $\mathfrak{m}'' = [m''a'', m''(b'' + \theta)]$ es divisible por el ideal $\mathfrak{m} = [ma, m(b + \theta)]$, entonces existirá un ideal $\mathfrak{m}'$, y solo uno, tal que se tendrá $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}''$; si se designa, en efecto, por $\mathfrak{m}$, el ideal conjugado con $\mathfrak{m}$, y se forma, según las reglas precedentes, el producto

$$\mathfrak{m}_1\mathfrak{m} = [m'''a', m'''(b' + \theta)],$$

entonces resulta, de las tres congruencias establecidas al principio de este parágrafo, que m''' es divisible por $\mathrm{N}(\mathfrak{m}) = m^2 a$, y por consiguiente que $m''' = m^2 am'$, donde m' designa un número entero; añadiendo a eso el teorema precedente, de que $\mathfrak{m}\mathfrak{m}_1 = \mathfrak{o}(m^2 a)$, se concluye fácilmente que el ideal $\mathfrak{m}' = [m'a', m'(b' + \theta)]$, y solo él, cumple la condición $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}''$. Resulta al mismo tiempo que la igualdad $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}\mathfrak{m}'''$ implica siempre la igualdad $\mathfrak{m}' = \mathfrak{m}'''$.

Para llegar ahora a la conclusión de esta teoría, no nos queda más que introducir además la siguiente noción: un ideal $\mathfrak{p}$, diferente de $\mathfrak{o}$ y que no tiene como divisor a ningún otro ideal que no sea $\mathfrak{o}$ y $\mathfrak{p}$, se denominará un *ideal primo*. Siendo η un número determinado, el sistema $\mathfrak{r}$ de *todas* las raíces ρ de la congruencia $\eta\rho \equiv 0 \pmod{\mathfrak{p}}$ constituirá un ideal, porque posee las

[31] *Disquisitiones arithmeticae*, art. 235, 242.

propiedades I y II; este ideal $\mathfrak{r}$ es un divisor de $\mathfrak{p}$, puesto que todos los números contenidos en $\mathfrak{p}$ son también raíces de esta congruencia; luego, si $\mathfrak{p}$ es un ideal primo, $\mathfrak{r}$ deberá ser o $= \mathfrak{o}$ o $= \mathfrak{p}$. Si el número dado η no está contenido en $\mathfrak{p}$, entonces el número 1, contenido en $\mathfrak{o}$, no será una raíz de la congruencia, y por lo tanto en este caso $\mathfrak{r}$ no será $= \mathfrak{o}$, sino $= \mathfrak{p}$, es decir que todas las raíces ρ deberán estar contenidas en $\mathfrak{p}$. De este modo se encuentra evidentemente establecido el siguiente teorema([32]): "Un producto $\eta\rho$ de dos números η, ρ no está contenido en un ideal primo $\mathfrak{p}$ más que si uno al menos de los dos factores está contenido en $\mathfrak{p}$". Y de ahí resulta inmediatamente este otro teorema: "Si ninguno de los dos ideales $\mathfrak{m}$, $\mathfrak{m}'$ es divisible por el ideal primo $\mathfrak{p}$, entonces su producto $\mathfrak{m}\mathfrak{m}'$ tampoco será divisible por $\mathfrak{p}$"; pues, ya que hay en $\mathfrak{m}$, $\mathfrak{m}'$ respectivamente números μ, μ' que no están contenidos en $\mathfrak{p}$, existirá también en $\mathfrak{m}\mathfrak{m}'$ un número $\mu\mu'$ que no estará tampoco contenido en $\mathfrak{p}$.

Combinando el teorema que acabamos de demostrar con los teoremas precedentes relativos a la dependencia entre las nociones de divisibilidad y de multiplicación de los ideales, y tomando en consideración que, además de $\mathfrak{o}$, no existe ningún otro ideal cuya norma sea $= 1$, se llega, por los mismos razonamientos([33]) que en la teoría de los números racionales, al siguiente teorema: "Todo ideal diferente de $\mathfrak{o}$ o es un ideal primo, o puede ponerse, y eso de una sola manera, bajo la forma de un producto de un número finito de ideales primos". De este teorema resulta inmediatamente que un ideal $\mathfrak{m}''$ es siempre divisible por un ideal $\mathfrak{m}$ en el caso, y solamente en el caso, en el que todas las potencias de los ideales primos que dividen a $\mathfrak{m}$ dividen también a $\mathfrak{m}''$. Si $\mathfrak{m} = \mathfrak{o}\mu$ y $\mathfrak{m}'' = \mathfrak{o}\mu''$ son ideales principales, entonces el mismo criterio decide también la divisibilidad del *número* μ'' por el *número* μ. Y de este modo la teoría de la divisibilidad de los números en el dominio $\mathfrak{o}$ es reconducida a leyes fijas y simples.

Toda esta teoría puede aplicarse casi literalmente a un dominio $\mathfrak{o}$ cualquiera compuesto por *todos* los números enteros de un cuerpo cualquiera Ω de segundo grado, cuando la noción de número *entero* es definida como lo ha sido en la Introducción([34]). Pero esta base de la teoría, aún cuando no deje nada que desear por lo que respecta al rigor, no es de ningún modo la que me propongo establecer. Se puede observar, en efecto, que las demostraciones de las proposiciones más importantes se sustentan sobre la representación de los ideales mediante la *expresión* $[ma, m(b+\theta)]$ y sobre la realización efectiva de la multiplicación, es decir sobre un *cálculo* que coincide con la composición de las formas cuadráticas binarias, enseñada por Gauss. Si se quisiera tratar de la misma manera todos los cuerpos Ω de cualquier grado, se chocaría con grandes dificultades, quizás insuperables. Pero, aún cuando ello no fuera así, una teoría tal, fundamentada sobre el cálculo, no ofrecería

[32] Este teorema lleva fácilmente a la determinación de todos los ideales primos contenidos en $\mathfrak{o}$, y éstos corresponden exactamente a los números primos, existentes e ideales, enumerados en el §10.

[33] *Ver* Dirichlet, *Vorlesungen über Zahlentheorie*, §8.

[34] El dominio, mencionado anteriormente, de los números $x + y\sqrt{-3}$, donde x, y toman todos los valores racionales enteros, *no es* un dominio de esta naturaleza; sino que constituye solamente *una parte* del dominio $\mathfrak{o}$ de todos los números $x + y\rho$, siendo ρ una raíz de la ecuación $\rho^2 + \rho + 1 = 0$.

todavía, a mi parecer, el grado máximo de perfección; es preferible, como en la teoría moderna de las funciones, tratar de obtener las demostraciones, no ya del cálculo, sino inmediatamente de los conceptos fundamentales característicos, y edificar la teoría de manera que esté, por el contrario, en disposición de predecir los resultados del cálculo (por ejemplo, la composición de las formas descomponibles de todos los grados). Tal es el objetivo que voy a proseguir en las siguientes Secciones de esta Memoria.

III

Propiedades generales de los números algebraicos enteros.

En esta Sección consideraremos en primer lugar el dominio de todos los números algebraicos enteros; a continuación introduciremos la noción de cuerpo finito Ω, y determinaremos la constitución del dominio $\mathfrak{o}$, compuesto por todos los números enteros del cuerpo Ω.

§13.– *El dominio de todos los números algebraicos enteros.*

Un número real o complejo θ se denominará un número *algebraico* cuando satisfaga una ecuación

$$\theta^n + a_1\theta^{n-1} + a_2\theta^{n-2} + \ldots + a_{n-1}\theta + a_n = 0,$$

de grado finito n con coeficientes racionales a_1, a_2, $\ldots$, a_{n-1}, a_n; si esta ecuación tiene como coeficientes números *racionales enteros*, es decir números de la sucesión 0, ± 1, ± 2, $\ldots$, θ se denominará un número *algebraico entero*, o simplemente un número *entero*. Está claro que los números racionales enteros pertenecen igualmente a los números algebraicos enteros, y que, recíprocamente, si un número racional θ es al mismo tiempo un número algebraico entero, entonces estará también, en virtud de un teorema conocido, contenido en el dominio de los números racionales enteros 0, ± 1, ± 2, $\ldots$. De la definición de los números se deducen también fácilmente las proposiciones siguientes:

1.ª Los números enteros, son estables bajo la adición, substracción y multiplicación, es decir, las sumas, las diferencias y los productos de dos números enteros cualesquiera α, β son también números enteros.

Demostración.- A consecuencia de la hipótesis, existen dos ecuaciones de la forma

$$\varphi(\alpha) = \alpha^a + p_1\alpha^{a-1} + \ldots + p_{a-1}\alpha + p_a = 0,$$
$$\psi(\beta) = \beta^b + q_1\beta^{b-1} + \ldots + q_{b-1}\beta + q_b = 0,$$

en la cual todos los coeficientes p, q son números racionales enteros. Pongamos ahora $ab = n$, y designemos por ω_1, ω_2, $\ldots$, ω_n los n productos $\alpha^{a'}\beta^{b'}$, formados con uno de los a números

$$1,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{a-1},$$

y uno de los b números

$$1,\ \beta,\ \beta^2,\ \ldots,\ \beta^{b-1}.$$

Representando ahora por ω uno de los tres números $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, se ve fácilmente que cada uno de los n productos $\omega\omega_1$, $\omega\omega_2$, ..., $\omega\omega_n$ puede reconducirse sea inmediatamente, sea con la ayuda de las ecuaciones $\varphi(\alpha)=0$, $\psi(\beta)=0$, a la forma

$$k_1\omega_1+k_2\omega_2+\ldots+k_n\omega_n,$$

donde k_1, k_2, ..., k_n son números racionales *enteros*; se tienen pues n ecuaciones de la forma

$$\begin{aligned}
\omega\omega_1 &= k'_1\omega_1+k'_2\omega_2+\ldots+k'_n\omega_n,\\
\omega\omega_2 &= k''_1\omega_1+k''_2\omega_2+\ldots+k''_n\omega_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\omega\omega_n &= k_1^{(n)}\omega_1+k_2^{(n)}\omega_2+\ldots+k_n^{(n)}\omega_n,
\end{aligned}$$

donde todos los coeficientes k son números racionales enteros; pero eliminando los n números ω_1, ω_2, ..., ω_n, entre los cuales se encuentra el número 1, diferente de 0, se deduce de ahí la ecuación

$$\begin{vmatrix}
k'_1-\omega & k'_2 & \ldots & k'_n\\
k''_1\omega & k''_2-\omega & \ldots & k''_n\\
\cdots & \cdots & \ldots & \cdots\\
k_1^{(n)} & k_2^{(n)} & \ldots & k_n^{(n)}-\omega
\end{vmatrix}=0$$

que es evidentemente de la forma

$$\omega^n+e_1\omega^{n-1}+\ldots+e_{n-1}\omega+e_n=0,$$

donde los n coeficientes e están formados por medio de los números k por adición, substracción y multiplicación, y por lo tanto son números racionales enteros. Luego ω, y por lo tanto cada uno de los tres números $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$ es un número entero.

Q.E.D.

2.ª Toda raíz ω de una ecuación de la forma

$$F(\omega)=\omega^m+\alpha\omega^{m-1}+\beta\omega^{m-2}+\ldots+\varepsilon=0,$$

cuyo coeficiente del término de grado máximo es la unidad, siendo los otros coeficientes α, β, ..., ε números enteros, es igualmente un número entero.

Demostración.- A consecuencia de la hipótesis, los coeficientes α, β, ..., ε son raíces de ecuaciones

$$\begin{aligned}
\varphi(\alpha)&=\alpha^a+p_1\alpha_{a-1}+\ldots+p_a=0,\\
\psi(\beta)&=\beta^b+q_1\beta_{b-1}+\ldots+q_b=0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\chi(\varepsilon)&=\varepsilon^e+s_1\varepsilon_{e-1}+\ldots+s_e=0,
\end{aligned}$$

donde todos los coeficientes p, q, ..., s designan números racionales enteros. Poniendo ahora $n=mab\ldots e$, y designando por ω_1, ω_2, ..., ω_n la totalidad de los n productos de la forma

$$\omega^{m'}\alpha^{a'}\beta^{b'}\ldots\varepsilon^{e'},$$

donde los exponentes racionales enteros satisfacen las condiciones

$$0\le m'<m,\ 0\le a'<a,\ 0\le b'<b,\ \ldots,\ 0\le e'<e,$$

es fácil comprobar que cada uno de los productos $\omega\omega_1$, $\omega\omega_2$, ..., $\omega\omega_n$ puede, sea inmediatamente, sea con la ayuda de las ecuaciones $F(\omega) = 0$, $\varphi(\alpha) = 0$, $\psi(\beta) = 0$, ... $\chi(\varepsilon) = 0$, reconducirse a la forma

$$k_1\omega_1 + k_2\omega_2 + \ldots + k_n\omega_n,$$

donde k_1, k_2, ..., k_n r'presentan números racionales enteros. De ello se sigue, como en la demostración del teorema precedente, que ω es un número entero.

Q.E.D.

Del último teorema resulta, por ejemplo, que, si α designa un número entero cualquiera, y r, s números racionales enteros positivos, $\sqrt[s]{\alpha^r}$ será también un número entero.

§14.– *La divisibilidad de los números enteros.*

Diremos que un número entero α es *divisible* por un número entero β, cuando se tenga $\alpha = \beta\gamma$, siendo γ igualmente un número entero. Expresaremos también la misma cosa diciendo que α es un múltiplo de β, o que β divide α, o que β es un factor o un divisor de α. De esta definición y del teorema 1.º del §13 resultan, como ya lo hemos hecho ver en la *Introducción*, estas dos proposiciones elementales:

1.ª Si α, α' son divisibles por μ, entonces $\alpha + \alpha'$ y $\alpha - \alpha'$ serán también divisibles por μ;

2.ª Si α' es divisible por α y α es divisible por μ, entonces α' será también divisible por μ.

Pero es necesario conceder una atención particular a las *unidades*, es decir a los números enteros que dividen a *todos* los números enteros; una unidad ε deberá pues dividir al número 1, y recíprocamente es evidente que todo divisor ε de 1 es una unidad, pues todo número entero es divisible por la unidad 1, y por lo tanto también (en virtud de la proposición 2.ª anterior) divisible por ε. Se ve al mismo tiempo que que todo producto o todo cociente de dos unidades es él mismo una unidad.

Si cada uno de los dos números enteros α y α', diferentes de cero, es divisible por el otro, se tendrá que $\alpha' = \alpha\varepsilon$, siendo ε una unidad; y recíprocamente, si ε es una unidad, entonces cada uno de los dos números enteros α y $\alpha' = \alpha\varepsilon$ será divisible por el otro. Daremos a dos números de esta naturaleza α, α' el nombre de *asociados*, y está claro que dos números cualesquiera asociados con un tercero están asociados entre sí. En todas las cuestiones que se refieren únicamente a la divisibilidad, todos los números asociados se comportan como un sólo y mismo número; si, en efecto, α es divisible por β, entonces todo número asociado con α será también divisible divisible por todo número asociado con β.

Un examen más profundo haría ver que dos números enteros α, β, no siendo ambos nulos, tienen un *máximo* común divisor, que puede ponerse bajo la forma $\alpha\alpha' + \beta\beta'$, siendo α' y β' números enteros. Pero este importante teorema no es de ningún modo fácil de demostrar con la ayuda de los principios expuestos hasta aquí, mientras que más tarde (§30) se le podrá deducir muy simplemente a partir de la teoría de los ideales. Finalizaré pues estas consideraciones preliminares sobre el dominio de *todos* los números enteros con la observación de que en este dominio no existe absolutamente ningún

número que posea el carácter de los *números primos*; pues, si α es un número entero cualquiera diferente de cero, y que no sea tampoco una unidad, entonces se le podrá descomponer de una infinidad de maneras en factores que serán números enteros y que al mismo tiempo no serán unidades; así, por ejemplo, se tiene $\alpha = \sqrt{\alpha}\sqrt{\alpha}$, o también $\alpha = \beta_1\beta_2$, siendo β_1 y β_2 las dos raíces β de la ecuación $\beta^2 - \beta + \alpha = 0$; ahora bien del teorema 2º del §13 resulta que $\sqrt{\alpha}$, β_1, β_2 son números enteros al mismo tiempo que α.

§15.– *Cuerpos finitos.*

La propiedad de ser descomponibles de una infinidad de maneras, que acabamos de señalar y que se presenta en el dominio que comprende a todos los números enteros, desaparece de nuevo tan pronto como uno se limita a considerar los números enteros confinados en un *cuerpo finito*. Es necesario definir en primer lugar la extensión y la naturaleza de un tal cuerpo.

Todo número algebraico θ, sea o no un número entero, satisface evidentemente una infinidad de ecuaciones diferentes con coeficientes racionales, es decir que hay una infinidad de funciones enteras $F(t)$ de una variable t que se anulan para $t = \theta$, y cuyos coeficientes son racionales. Pero, de entre todas estas funciones $F(t)$, debe necesariamente haber una $f(t)$ cuyo grado n sea el *mínimo posible*, y del método conocido de la división de estos tipos de funciones resulta inmediatamente que cada una de las funciones $F(t)$ debe ser algebraicamente divisible por esta función $f(t)$, y que $f(t)$ no puede ser divisible por ninguna función entera de grado menor con coeficientes racionales. Por esta razón, la función $f(t)$ y también la ecuación $f(\theta) = 0$ serán llamadas *irreducibles*, y está claro, al mismo tiempo, que los n números 1, θ^1, θ^2, …, θ^{n-1} constituirán un *sistema irreducible* (§4, 1º).

Consideremos ahora el conjunto Ω de todos los números ω de la forma $\varphi(\theta)$, designando por

$$\varphi(\theta) = x_0 + x_1 t + x_2 t^2 + \ldots + x_{n-1} t^{n-1}$$

cualquier función entera de t con coeficientes racionales, enteros o fraccionarios, x_0, x_1, x_2, …, x_{n-1}, cuyo grado es $< n$, y observemos en primer lugar que todo número de esta especie $\omega = \varphi(\theta)$, en virtud de la irreducibilidad de $f(t)$, no puede ponerse bajo esta forma más que de una sola manera. Se hace ver a continuación fácilmente que estos números ω son siempre estables bajo las *operaciones racionales*, es decir bajo la adición, substracción, multiplicación y división. Para las dos primeras operaciones, esto resulta evidentemente de la forma común $\varphi(\theta)$ de todos los números ω, y para la multiplicación es suficiente observar que todo número de la forma $\psi(\theta)$, siendo $\psi(t)$ una función entera de grado *cualquiera*, con coeficientes racionales, es igualmente un número ω; pues, si se divide $\psi(t)$ entre $f(t)$, el resto de la división será una función $\varphi(t)$ de la especie indicada antes, y se tendrá al mismo tiempo $\varphi(\theta) = \varphi(\theta)$. Para tratar finalmente el caso de la división, no se tiene más que hacer ver también que, si $\omega = \varphi(\theta)$ es diferente de cero, entonces su valor recíproco ω^{-1} pertenece también al sistema Ω, pero no teniendo $\varphi(t)$ ningún divisor común con la función irreducible $f(t)$, el método por el cual se buscaría el máximo común divisor de las funciones $f(t)$, $\varphi(t)$ proporciona, como se sabe, dos funciones enteras $f_1(t)$, $\varphi_1(t)$, con

coeficientes racionales, que satisfacen la identidad

$$f(t)f_1(t) + \varphi(t)\varphi_1(t) = 1,$$

de donde resulta, para $t = \theta$, la verdad del enunciado precedente.

Llamaré *cuerpo* a todo sistema A de números a (no siendo todos nulos), tal que las sumas, las diferencias, los productos y los cocientes de dos cualesquiera de esos números a pertenezcan al sistema A. El ejemplo más simple de un cuerpo es el del sistema de todos los números racionales, y es fácil reconocer que este cuerpo está contenido en cualquier otro cuerpo A; pues, si se elige a discreción un número a del cuerpo A, diferente de cero, entonces es necesario según la definición, que el cociente 1 de los dos números a y a pertenezca igualmente al cuerpo A, de donde resulta inmediatamente la proposición enunciada, pudiendo ser todos los números racionales engendrados mediante el número 1 por adiciones, sustracciones, multiplicaciones y divisiones repetidas.

Según lo que hemos demostrado más arriba relativamente a los números $\omega = \varphi(\theta)$, nuestro sistema Ω constituirá pues también un cuerpo; los números racionales se obtienen de $\varphi(\theta)$, anulando todos los coeficientes x_1, x_2, $\ldots$, x_{n-1} que siguen a x_0. A un cuerpo Ω que es producido, de la manera indicada, por una ecuación irreducible $f(\theta) = 0$ de grado n, lo llamaremos un cuerpo *finito*([35]), y el número n se denominará su *grado*. Un cuerpo tal Ω contiene n números independientes entre sí, por ejemplo los números 1, θ, θ^2, $\ldots$, θ^{n-1}, mientras que $n+1$ números cualesquiera del cuerpo constituirán evidentemente un sistema reducible (§4, 1.º); esta propiedad, junto a la noción de cuerpo, podría servir también de definición para un cuerpo Ω de n-simo grado; no entraré sin embargo en la demostración de esta aserción.

Si se escogen ahora arbitrariamente n números

$$\omega_1 = \varphi_1(\theta),\ \omega_2 = \varphi_2(\theta),\ \ldots, \omega_n = \varphi_n(\theta)$$

del cuerpo Ω, estos números (según §4, 2.º) constituirán siempre, y solamente entonces, un sistema irreducible, cuando el determinante formado con los n^2 coeficientes racionales x sea diferente de cero; en este caso, llamaremos al sistema de los n números ω_1, ω_2, $\ldots$, ω_n una *base del cuerpo* Ω; entonces es evidente que todo número $\omega = \varphi(\theta)$ puede siempre, y de una sola manera, ponerse bajo la forma

$$\omega = h_1\omega_1 + h_2\omega_2 + \ldots + h_n\omega_n,$$

siendo los coeficientes h_1, h_2, $\ldots$, h_n números racionales, enteros o fraccionarios, y recíprocamente, todos los números ω de esta forma están contenidos en Ω; los coeficientes racionales h_1, h_2, $\ldots$, h_n se denominarán las *coordenadas del número* ω con respecto a esta base.

§16.– *Cuerpos conjugados.*

[35] Si se entiende por divisor de un cuerpo A todo cuerpo B del que todos los números están contenidos en A, entonces un cuerpo finito podrá ser también definido como un cuerpo que no posee más que un número finito de divisores. Empleando aquí la palabra *divisor* (y la palabra *múltiplo*) con un sentido directamente opuesto a aquél que le hemos adscrito, al hablar de los módulos y los ideales, no podrá con toda seguridad resultar ninguna confusión.

Se entiende de ordinario por *substitución* un acto por el cual los objetos de un estudio o los elementos de una investigación son reemplazados por objetos o elementos correspondientes, y se dice que los antiguos elementos se transforman, por la substitución, en los nuevos elementos. Sea ahora Ω un cuerpo *cualquiera*; entonces entenderemos por una *permutación de* Ω una substitución por la cual cada número determinado contenido en Ω

$$\alpha,\ \beta,\ \alpha+\beta,\ \alpha-\beta,\ \alpha\beta,\ \frac{\alpha}{\beta},$$

se transforma en un número determinado correspondiente

$$\alpha',\ \beta',\ (\alpha+\beta)',\ (\alpha-\beta)',\ (\alpha\beta)',\ \left(\frac{\alpha}{\beta}\right)',$$

y esto de tal manera que las dos condiciones

$$(\alpha+\beta)' = \alpha' + \beta', \tag{1}$$

$$(\alpha\beta)' = \alpha'\beta' \tag{2}$$

sean satisfechas, y que los números substituidos α', β', ... no se anulen todos. Vamos a hacer ver que el conjunto Ω' de esos últimos números constituye un nuevo *cuerpo*, y que la permutación satisface también las dos condiciones siguientes:

$$(\alpha-\beta)' = \alpha' - \beta', \tag{3}$$

$$\left(\frac{\alpha}{\beta}\right)' = \frac{\alpha'}{\beta'}. \tag{4}$$

Si se designa, en efecto, por α', β' dos números cualesquiera del sistema Ω', entonces existirá en el cuerpo Ω dos números α, β, que por la permutación se transformarán respectivamente en α', β'; ahora bien estando los números $\alpha+\beta$, $\alpha\beta$ igualmente contenidos en Ω, resulta de (1) y (2) que los números $\alpha'+\beta'$, $\alpha'\beta'$ estarán también contenidos en Ω'; luego los números del sistema Ω' son estables bajo la adición y la multiplicación. Además, estando los números $\alpha = (\alpha-\beta)+\beta$ y $\alpha-\beta$ igualmente contenidos en Ω, resulta de (1) que

$$\alpha' = (\alpha-\beta)' + \beta',$$

lo que constituye la condición (3); luego los números del sistema Ω también son estables bajo la sustracción. Por último, si β' es diferente de cero, entonces, en virtud de (1), β será también diferente de cero, y por lo tanto α/β es un número determinado perteneciente al cuerpo Ω; puesto que se tiene ahora que $\alpha = (\alpha/\beta)\beta$, entonces resulta de (2) que se tiene también que $\alpha' = (\alpha/\beta)'\beta'$, lo que constituye la condición (4); luego los números del sistema Ω' también son estables bajo la división, y por lo tanto Ω' es un cuerpo.

Q.E.D.

Observemos ahora, además, que, si $\beta' = 0$, se deberá tener también $\beta = 0$; pues en caso contrario *todo* número α del cuerpo Ω podría ponerse bajo la forma $(\alpha/\beta)\beta$, de donde resultaría $\alpha' = (\alpha/\beta)'\beta' = 0$, mientras que, por el contrario, hemos admitido que los números α' del sistema Ω' no son todos nulos. Se sigue de ahí evidentemente, tomando en consideración (3), que,

por una permutación, dos números *diferentes* α, β del cuerpo Ω se transformarán también en dos números *diferentes* α', β' del cuerpo Ω', y que así cada número determinado α' del cuerpo Ω' no corresponde más que a un sólo número completamente determinado α del cuerpo Ω. La correspondencia puede pues ser invertida de una manera unívoca, y la substitución por la cual cada número determinado α' del cuerpo Ω' se transformará en el número correspondiente α del cuerpo Ω será una *permutación del cuerpo* Ω', puesto que satisfará las condiciones características (1) y (2). Cada una de estas dos permutaciones se denominará la *inversa* de la otra; llamaremos, además a Ω y Ω' *cuerpos conjugados*, y del mismo modo a dos números correspondientes cualesquiera α, α' *números conjugados*. Existe evidentemente para cada cuerpo Ω una permutación a la que llamaremos la permutación *idéntica* de Ω, y que consiste en que cada número del cuerpo Ω será reemplazado por sí mismo; luego todo cuerpo es conjugado consigo mismo. Además, es fácil asegurarse que dos cuerpos conjugados con un tercero lo son también entre sí; pues, si cada número α del cuerpo Ω se transforma, por una permutación P, en un número α' del cuerpo Ω', e igualmente cada número α' de este último se transforma, por una permutación P', en un número α'' del cuerpo Ω'', entonces está claro que que la substitución por la cual cada número α del cuerpo Ω se transforma en el número correspondiente α'' del cuerpo Ω'' es igualmente una *permutación* del cuerpo Ω, y la designaremos por PP'. Si se designa por P^{-1} la permutación inversa de P, entonces PP^{-1} será la permutación idéntica de Ω, y Ω'' se transformará en Ω por la permutación

$$(PP')^{-1} = P'^{-1}P^{-1}.$$

Ya hemos observado que cada cuerpo contiene a todos los números racionales, y es fácil mostrar que cada uno de éstos, por una permutación del cuerpo, se transforma siempre en sí mismo; pues, si se establece que $\alpha = \beta$, entonces resulta de (4) que se tendrá $1' = 1$; ahora bien, pudiendo ser engendrado todo número racional a partir del número 1 por una serie de operaciones racionales, nuestra proposición se sigue inmediatamente de las propiedades (1), (2), (3) y (4). Sea además θ un número cualquiera del cuerpo Ω, y $R(t)$ una función racional cualquiera de la variable t con coeficientes racionales; entonces el número $R(\theta)$, en el caso de que el denominador de la función $R(t)$ no se anule para $t = \theta$, estará también contenido en Ω, y si, por una permutación del cuerpo, θ se transforma en el número θ', entonces el número ω, estando formado por operaciones racionales ejecutadas sobre el número θ y sobre los coeficientes racionales de $R(t)$, se transformará, por la misma permutación, en el número $\omega' = R(\theta')$. De ahí resulta inmediatamente que, si θ es un número algebraico y satisface, por consiguiente, una ecuación de la forma $0 = F(\theta)$ cuyos coeficientes sean números racionales, se deberá tener también $0 = F(\theta')$; luego todo número θ' conjugado con un número algebraico es igualmente un número algebraico; y si θ es un número entero, entonces θ' será también un número entero.

Después de estas consideraciones generales, que son relativas a *todos* los cuerpos, volvamos a nuestro ejemplo, en el que se trata de un cuerpo finito Ω, de grado n, y planteémonos el problema de encontrar *todas* las permutaciones de Ω. Siendo todos los números ω de un tal cuerpo Ω, según el §15, de la forma $\varphi(\theta)$, donde θ designa una raíz de una ecuación irreducible

$0 = f(\theta)$ de grado n, una permutación de Ω, en virtud de lo que precede, estará ya completamente determinada por la elección de la raíz θ' de la ecuación $0 = f(\theta')$, en la que θ se transforma, pues al mismo tiempo todo número $\omega = \varphi(\theta)$ deberá transformarse en $\omega' = \varphi(\theta')$. Recíprocamente, si se elige como θ' una raíz cualquiera de la ecuación $0 = f(\theta')$ y se reemplaza cada número $\omega = \varphi(\theta)$ del cuerpo Ω por el número correspondiente $\omega' = \varphi(\theta')$, entonces esta substitución será realmente una permutación de Ω, es decir satisfará las condiciones (1) y (2). Para demostrarlo, designemos por $\varphi_1(t)$, $\varphi_2(t)$, ... funciones especiales cualesquiera, de la forma $\varphi(t)$; si se tiene ahora que

$$\alpha = \varphi_1(\theta),\ \beta = \varphi_2(\theta),\ \alpha + \beta = \varphi_3(\theta),\ \alpha\beta = \varphi_4(\theta),$$

y por consiguiente que

$$\alpha' = \varphi_1(\theta'),\ \beta' = \varphi_2(\theta'),\ (\alpha + \beta)' = \varphi_3(\theta'),\ (\alpha\beta)' = \varphi_4(\theta')$$

entonces resulta de las ecuaciones

$$\varphi_3(\theta) = \varphi_1(\theta) + \varphi_2(\theta),\ \varphi_4(\theta) = \varphi_1(\theta) + \varphi_2(\theta),$$

y de la irreducibilidad de la función $f(t)$, que se tendrá idénticamente que

$$\varphi_3(t) = \varphi_1(t) + \varphi_2(t),\ \varphi_4(t) = \varphi_1(t)\varphi_2(t) + \varphi_5(t)f(t),$$

lo que da, haciendo $t = \theta'$, las ecuaciones (1) y (2) que se trataba de demostrar. Si se pone pues

$$f(t) = (t - \theta)(t - \theta') \dots (t - \theta^{(n)}),$$

entonces las n raíces θ, θ',..., $\theta^{(n)}$ serán desiguales, puesto que la función irreducible $f(t)$ no puede tener ningún divisor común con su derivada $f'(t)$, y a cada una de ellas le corresponderá una permutación P', P'',..., $P^{(n)}$ del cuerpo Ω, de tal manera que, por la permutación $P^{(r)}$, cada número $\omega = \varphi(\theta)$ del cuerpo Ω se transforma en el número conjugado $\omega^{(r)} = \varphi(\theta^{(r)})$ del cuerpo conjugado $\Omega^{(r)}$. Para evitar los malentendidos, haremos observar que estos n cuerpos conjugados $\Omega^{(r)}$, aunque se deducen de Ω por n permutaciones *diferentes*, pueden muy bien ser no obstante idénticos entre sí en cuanto al conjunto de los números que contienen, sea en parte, sea en su totalidad; si son todos idénticos, entonces Ω se denominará un *cuerpo de Galois* o un *cuerpo normal*. Los principios algebraicos de Galois consisten en que el estudio de cualesquiera cuerpos finitos es reconducido al de los cuerpos normales; pero la falta de espacio no me permite ahora extenderme más sobre este asunto.

§17.– *Normas y discriminantes.*

Por la *norma* $\mathrm{N}(\omega)$ de un número cualquiera ω del cuerpo Ω de grado n entenderemos el producto

$$\mathrm{N}(\omega) = \omega'\omega'' \dots \omega^{(n)} \tag{1}$$

de los n números conjugados ω', ω'', ..., $\omega^{(n)}$, en los cuales ω se transforma por las permutaciones P', P'',..., $P^{(n)}$. Ésta no puede anularse más que si se tiene $\omega = 0$. Si ω es un número racional, entonces los n números $\omega^{(r)}$ serán iguales a ω, y por lo tanto la norma de un número racional es la n-sima

potencia de este número. Si α, β son dos números cualesquiera del cuerpo Ω, entonces se tendrá que $(\alpha\beta)^{(r)} = \alpha^{(r)}\beta^{(r)}$, y por consiguiente que

$$\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta). \tag{2}$$

Por el *discriminante* $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ de un sistema cualquiera de n números α_1, α_2,..., α_n del cuerpo Ω, entenderemos el cuadrado

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\sum \pm \alpha_1' \alpha_2'', \ldots, \alpha_n^{(n)})^2 \tag{3}$$

del determinante formado con los n^2 números $\alpha_i^{(r)}$. De ahí resulta, en virtud de una proposición bien conocida de la teoría de los determinantes, la relación

$$\Delta(1, \theta, \theta^2, \ldots, \theta^{n-1}) = (-1)^{\frac{1}{2}n(n-1)}\mathrm{N}(f'(\theta)), \tag{4}$$

y como $f'(\theta)$ no puede, debido a la irreducibilidad de la función $f(t)$, ser igual a cero, se sigue que el discriminante (4) tiene un valor diferente de cero.

Si ahora los n números ω_1, ω_2, ..., ω_n constituyen una base del cuerpo Ω (§15), y si

$$\omega = h_1\omega_1 + h_2\omega_2 + \ldots + h_n\omega_n$$

es un número cualquiera de este cuerpo, puesto que sus coordenadas h_1, h_2, ..., h_n son números racionales, la permutación $P^{(r)}$ transformará ω en el número

$$\omega^{(r)} = h_1\omega_1^{(r)} + h_2\omega_2^{(r)} + \ldots + h_n\omega_n^{(r)},$$

y de ahí se obtiene que

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = a^2\Delta(\omega_1, \omega_2, \ldots, \omega_n), \tag{5}$$

donde a designa el determinante formado con las n^2 coordenadas de los n números α_1, α_2,..., α_n. Se concluye en primer lugar que el discriminante de la base ω_1, ω_2,..., ω_n no puede anularse, porque, en el caso contrario, *todo* discriminante debería anularse, mientras que, por el contrario, se ha hecho ver con anterioridad que $\Delta(1, \theta, \ldots, \theta^{n-1})$ es diferente de cero. Se sigue al mismo tiempo que $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ se anula siempre, y solamente en ese caso cuando los números α_1, α_2,..., α_n son dependientes los unos de los otros (§4, 2.º), y por consiguiente no forman una base de Ω.

Puesto que los números del cuerpo son estables bajo la multiplicación, se podrá poner, siendo μ un número cualquiera comprendido en Ω,

$$\begin{cases} \mu\omega_1 = & m_{1,1}\omega_1 + m_{2,1}\omega_2 + \ldots + m_{n,1}\omega_n, \\ \mu\omega_2 = & m_{1,2}\omega_1 + m_{2,2}\omega_2 + \ldots + m_{n,2}\omega_n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots , \\ \mu\omega_n = & m_{1,n}\omega_1 + m_{2,n}\omega_2 + \ldots + m_{n,n}\omega_n, \end{cases} \tag{6}$$

donde las n^2 coordenadas $m_{i,i'}$ son números racionales; de ahí resultan, mediante las n permutaciones $P^{(r)}$, n^2 nuevos números de la forma

$$\mu^{(r)}\omega_i^{(r)} = m_{1,i}\omega_1^{(r)} + m_{2,i}\omega_2^{(r)} + \ldots + m_{n,i}\omega_n^{(r)},$$

y, como su determinante es

$$\mathrm{N}(\mu) \sum \pm \omega_1'\omega_2'' \ldots \omega_n^{(n)} = \sum \pm m_{1,1}m_{2,2} \ldots m_{n,n} \sum \pm \omega_1'\omega_2'' \ldots \omega_n^{(n)},$$

se concluye que

$$\mathrm{N}(\mu) = \sum \pm m_{1,1} m_{2,2} \dots m_{n,n}, \tag{7}$$

puesto que el determinante

$$\sum \pm \omega_1' \omega_2'' \dots \omega_n^{(n)} = \sqrt{\Delta(\omega_1 \omega_2 \dots \omega_n)}$$

no es nulo.

Se sigue de ahí que toda norma es un número *racional*, y la misma consecuencia, en virtud de (4) y (5), se aplica también a todo discriminante; estas dos proposiciones también hubieran podido deducirse a partir de la teoría de la transformación de las funciones simétricas, de la que, voluntariamente, he evitado servirme aquí.

Si se reemplaza, en las ecuaciones (6), el número μ por $\mu - z$, siendo z un número racional cualquiera, entonces las coordenadas $m_{i,i'}$ no experimentarán ningún cambio, con la excepción de las coordenadas $m_{i,i}$, que se encuentran en la diagonal, y que deberán ser reemplazadas por $m_{i,i} - z$. El teorema (7) queda de este modo transformado en la igualdad

$$\begin{vmatrix} m_{1,1} - z & m_{2,1} & \dots & m_{n,1} \\ m_{1,2} & m_{2,2} - z & \dots & m_{n,2} \\ \dots & \dots & \dots & \dots \\ m_{1,n} & m_{2,n} & \dots & m_{n,n} - z \end{vmatrix} = (\mu' - z)(\mu'' - z) \dots (\mu^{(n)} - z),$$

la cual, teniendo lugar para *todo* valor racional de z, deberá necesariamente ser una *identidad* relativamente a z. Se ve al mismo tiempo que los n números μ', μ'', …, $\mu^{(n)}$, conjugados con un número μ, forman el conjunto de las raíces de una ecuación de n-simo grado, cuyos coeficientes son números racionales.

§18.– *El dominio* $\mathfrak{o}$ *de todos los números enteros de un cuerpo finito* Ω.

Después de estos preliminares, vamos a pasar al objeto mismo en el que tenemos puesta la mirada, a saber, la consideración de todos los números *enteros* contenidos en el cuerpo Ω de grado n, números cuyo conjunto designaremos por $\mathfrak{o}$. Puesto que las sumas, las diferencias y los productos de dos números enteros cualesquiera (según el §13, 1.ª) son también números enteros y (en virtud del §15) están también contenidos en Ω, los números del dominio $\mathfrak{o}$, entre los cuales se encuentran también todos los números *racionales* enteros, serán estables también bajo la adición, substracción y multiplicación. Pero se trata ante todo de poner a todos estos números bajo una forma común y simple. Las consideraciones siguientes nos llevan a ello:

Siendo todo número algebraico ω raíz de una ecuación de la forma

$$c\omega^m + c_1\omega^{m-1} + \dots + c_{m-1}\omega + c_m = 0,$$

cuyos coeficientes c, c_1, …, c_{m-1}, c_m son números racionales enteros, resulta que, multiplicando por c^{m-1}, todo número ω de esta especie por medio de la multiplicación por un número racional entero c, diferente de cero, puede ser transformado en un número entero $c\omega$. Si ahora los n números ω_1, ω_2, …, ω_n forman una base del cuerpo Ω, entonces se podrán tomar los números racionales a_1, a_2, …, a_n, diferentes de cero, de tal manera que los n números

$$\alpha_1 = a_1\omega_1, \quad \alpha_2 = a_2\omega_2, \quad \dots, \alpha_n = a_n\omega_n$$

se conviertan en números *enteros*, y éstos evidentemente formarán también una base del cuerpo Ω, puesto que son (en virtud del §4, 2.º) independientes los unos de los otros. Por consiguiente (según el §17), su discriminante $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ será un número racional, e incluso *entero*, diferente de cero, puesto que, según su definición, está formado por adición, substracción y multiplicación de números $\alpha_i^{(r)}$ que son todos enteros. Se obtienen, además, todos los números ω del del cuerpo Ω, haciendo tomar, en la expresión

$$\omega = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n,$$

a los coeficientes x_1, x_2, $\ldots$, x_n todos los valores racionales; si no se les atribuye más que valores racionales *enteros*, entonces ciertamente no se obtienen más que números *enteros* ω (§13); pero es muy posible que no se puedan representar de esta manera *todos* los números enteros del cuerpo Ω. A este caso se refiere este teorema muy importante:

Si existe un número entero β de la forma

$$\beta = \frac{k_1\alpha_1 + k_2\alpha_2 + \ldots + k_n\alpha_n}{k},$$

siendo k, k_1, k_2, $\ldots$, k_n números racionales enteros sin ningún divisor común, entonces existirá una base del cuerpo Ω, formada por n números enteros β_1, β_2, $\ldots$, β_n que satisfará la condición

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = k^2\Delta(\beta_1, \beta_2, \ldots, \beta_n).$$

Demostración.— Puesto que β, α_1, α_2,$\ldots$, α_n son números enteros, formarán la base de un módulo $\mathfrak{b} = [\beta, \alpha_1, \alpha_2, \ldots, \alpha_n]$, que no contiene más que números enteros del cuerpo Ω; pero como, de estos $n+1$ números, solamente n son independientes entre sí, entonces existirán (§4, 5.º) n números independientes β_1, β_2, $\ldots$, β_n, que formarán una base del mismo módulo $\mathfrak{b} = [\beta_1, \beta_2, \ldots, \beta_n]$, y que serán, por consiguiente, números enteros del cuerpo. Se tendrán pues $n+1$ igualdades de la forma

$$\begin{aligned}
\beta &= c_1\beta_1 +_2 \beta_2 + \ldots + c_{n,1}\beta_n,\\
\alpha_1 &= c_{1,1}\beta_1 + c_{2,1}\beta_2 + \ldots + c_{n,1}\beta_n,\\
\alpha_2 &= c_{1,2}\beta_1 + c_{2,2}\beta_2 + \ldots + c_{n,2}\beta_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\alpha_n &= c_{1,n}\beta_1 + c_{2,n}\beta_2 + \ldots + c_{n,n}\beta_n,
\end{aligned}$$

en las que todos los $n(n+1)$ coeficientes serán números racionales enteros, y al mismo tiempo serán tales que los $n+1$ determinantes parciales de n-simo grado que se pueden formar suprimiendo una fila horizontal cualquiera no tendrán *ningún* divisor común (§4, 6.º). Si se pone

$$\sum \pm c_{1,1}c_{2,2}\ldots c_{n,n} = c,$$

entonces se tendrá [§17 (5)] que

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = c^2\Delta(\beta_1, \beta_2, \ldots, \beta_n).$$

Ahora bien, substituyendo las expresiones precedentes de β, α_1, α_2,$\ldots$, α_n en la ecuación $k\beta = k_1\alpha_1 + k_2\alpha_2 + \ldots + k_n\alpha_n$, y observando que β_1, β_2,$\ldots$,

β_n son independientes entre sí, resulta que

$$\begin{aligned} kc_1 &= k_1c_{1,1} + k_2c_{2,1} + \ldots + k_nc_{n,1}, \\ kc_2 &= k_1c_{1,2} + k_2c_{2,2} + \ldots + k_nc_{n,2}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ kc_n &= k_1c_{1,n} + k_2c_{2,n} + \ldots + k_nc_{n,n}; \end{aligned}$$

si se reemplazan ahora los elementos

$$c_{1,r}, \quad c_{2,r}, \quad \ldots, c_{n,r}$$

de la r-sima fila horizontal del determinante c respectivamente por los elementos

$$c_1, \quad c_2, \quad \ldots, c_n,$$

se concluirá a partir de las ecuaciones precedentes, en virtud de un teorema conocido, que el determinante parcial así obtenido tiene como valor $\frac{ck_r}{k}$. Luego las $n+1$ cantidades

$$\frac{ck}{k}, \quad \frac{ck_1}{k}, \quad \frac{ck_2}{k}, \quad \ldots, \frac{ck_n}{k}$$

son números racionales enteros sin ningún divisor común, y como ocurre lo mismo con los $n+1$ números k, k_1, k_2, …, k_n, es necesario pues que se tenga $c = \pm k$.

Q.E.D.

Si se tiene que $k > 1$, de modo que el número entero β no esté contenido en el módulo $\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_n]$, existirá, pues, una base del cuerpo, compuesta por n números enteros β_1, β_2,…, β_n, cuyo discriminante $\Delta(\beta_1, \beta_2, \ldots, \beta_n)$, tomado en valor absoluto, será $< \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Ahora bien, puesto que, como se ha mostrado con anterioridad, el discriminante de toda base del cuerpo Ω compuesta por números enteros es un número racional entero diferente de cero, deberá existir también una base tal ω_1, ω_2, …, ω_n, cuyo discriminante

$$\Delta(\omega_1, \omega_2, \ldots, \omega_n) = D,$$

tomado en valor absoluto, tendrá el valor *mínimo*, y de lo que precede, se sigue inmediatamente que, relativamente a una tal base, todo número entero

$$\omega = h_1\omega_1 + h_2\omega_2 + \ldots + h_n\omega_n$$

del cuerpo Ω deberá necesariamente tener como coordenadas números *enteros* h_1, h_2, …, h_n, y que un número entero ω no es divisible por un número racional entero k más que si todas sus coordenadas son divisibles por k. Como, recíprocamente, todo sistema de coordenadas enteras h_1, h_2, …, h_n produce siempre un número entero ω, *el conjunto* $\mathfrak{o}$ *de todos los números enteros del cuerpo* Ω *es idéntico al módulo finito* $[\omega_1, \omega_2, \ldots, \omega_n]$ cuya base se compone de n números enteros independientes ω_1, ω_2, …, ω_n.

El discriminante D de una tal base es un invariante del cuerpo Ω, de una importancia fundamental; lo llamaremos por esta razón el *número fundamental* o el *discriminante del cuerpo* Ω, y lo representaremos por $\Delta(\Omega)$. En el caso singular en el que $n = 1$, Ω es el cuerpo de los números *racionales*, y por su discriminante entenderemos el número $+1$. Como aclaración, vamos también a considerar el caso en el que $n = 2$, es decir el caso de un *cuerpo cuadrático*.

Toda raíz θ de una ecuación cuadrática irreducible es de la forma

$$\theta = a + b\sqrt{d},$$

siendo d un número racional entero completamente determinado, que no es un cuadrado, y que, además, no es divisible por ningún cuadrado (con la excepción de 1); a, b son números racionales, y b es diferente de cero. El conjunto de todos los números $\varphi(\theta)$ del cuerpo cuadrático correspondiente Ω es evidentemente idéntico al conjunto de todos los números de la forma

$$\omega = t + u\sqrt{d},$$

donde t, u toman todos los valores racionales. Por la permutación no idéntica del cuerpo, $\sqrt{d}$ se transforma en $-\sqrt{d}$, y por consiguiente ω en el número conjugado

$$\omega' = t - u\sqrt{d},$$

el cual está igualmente contenido en Ω; luego Ω es un cuerpo normal (§16). Para investigar todos los números *enteros* ω, pongamos

$$t = \frac{x}{z}, \quad u = \frac{y}{z},$$

siendo x, y, z números racionales enteros sin ningún divisor común, en el que el último, z, puede suponerse positivo. Si ahora ω es un número entero, entonces ω' lo será también (§16), y por consiguiente

$$\omega + \omega' = \frac{2x}{z}, \quad \omega\omega' = \frac{x^2 - dy^2}{z^2}$$

deberán ser también números enteros; y recíprocamente, si ello es así, entonces ω será evidentemente un número entero (§13). Sea de hecho e el máximo común divisor de z y de x; entonces será necesario que e^2 divida a $x^2 - dy^2$, y por consiguiente también a dy^2 y finalmente a y^2, puesto que d no es divisible por ningún cuadrado que no sea 1; luego e deberá también dividir a y, y por consiguiente ser $= 1$, puesto que z, x, y no tienen ningún divisor común. Puesto que de este modo z es primo con x y divide no obstante a $2x$, será necesario que se tenga, o bien $z = 1$, o bien $z = 2$. En el primer caso, $\omega = x + y\sqrt{d}$ es ciertamente un número entero; en el segundo caso, x es impar, por lo tanto $x^2 \equiv 1$ (mód 4), y como se debe tener que $x^2 \equiv dy^2$ (mód 4), es necesario que y sea también impar, y que se tenga por consiguiente que $d \equiv 1$ (mód 4). Luego si esta condición no se cumple, es decir si se tiene que $d \equiv 2$ o $d \equiv 3$ (mód 4), entonces z deberá ser $= 1$, y por consiguiente se tendrá que $\mathfrak{o} = [1, \sqrt{d}]$, y

$$D = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d.$$

Pero si se tiene que $d \equiv 1$ (mód 4), entonces z podrá también ser $= 2$ ([36]) y se tendrá que

$$\mathfrak{o} = \left[1, \frac{1+\sqrt{d}}{2}\right], \quad \text{y} \quad D = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = d.$$

[36] De ahí resulta, por ejemplo, para el caso en el que $d = -3$, que los números enteros del cuerpo no están *todos* contenidos en la forma $s + y\sqrt{-3}$, donde x, y toman todos los valores racionales.

Estos dos casos pueden también reunirse en uno solo, observando que se tiene, en los dos, $\mathfrak{o} = \left[1, \frac{D+\sqrt{D}}{2}\right]$. Está claro al mismo tiempo que un cuerpo *cuadrático* está ya completamente determinado por su discriminante D. Esto no es así para el caso que sigue inmediatamente, a saber, para el caso en el que $n = 3$, en el cual, además del discriminante, se presentan también otros invariantes, que son necesarios para la determinación completa de un cuerpo *cúbico*; sin embargo no se podrá dar la explicación general de este hecho más que con la ayuda de la teoría de los *ideales*.

Volvamos a la consideración de un cuerpo cualquiera Ω de grado n, y añadamos también las siguientes observaciones sobre la divisibilidad y la congruencia de los números en el dominio $\mathfrak{o}$. Sean λ, μ dos de estos números, y supongamos que λ sea divisible por μ; entonces se tendrá, según la definición general de la divisibilidad (§14), que $\lambda = \mu\omega$, siendo ω un número entero, y como, en virtud de la definición de un cuerpo, el cociente ω de los dos números λ, μ pertenece al cuerpo Ω, ω será igualmente un número del dominio $\mathfrak{o}$. El sistema $\mathfrak{m}$ de todos los números del cuerpo Ω divisibles por μ se compone pues de todos los números de la forma $\mu\omega$, recorriendo ω todos los números del dominio $\mathfrak{o} = [\omega_1, \omega_2, \ldots, \omega_n]$, es decir todos los números de la forma

$$\omega = h_1\omega_1 + h_2\omega_2 + \ldots + h_n\omega_n,$$

cuyas coordenadas h_1, h_2, $\ldots$, h_n son números racionales enteros; se tiene por consiguiente que $\mathfrak{m} = [\mu\omega_1, \mu\omega_2, \ldots, \mu\omega_n]$. Diremos ahora que dos números enteros α, β del dominio $\mathfrak{o}$ son *congruentes* con respecto al *módulo* μ, y pondremos

$$\alpha \equiv \beta \pmod{\mu},$$

cuando la diferencia $\alpha - \beta$ sea divisible por μ, y estará así contenida en $\mathfrak{m}$; por consiguiente, esta congruencia es totalmente equivalente a la siguiente:

$$\alpha \equiv \beta \pmod{\mathfrak{m}},$$

cuyo sentido ha sido explicado en el §2; en el caso contrario, α, β se denominan *incongruentes* con respecto a μ. Si se entiende por una *clase* con respecto al módulo μ al conjunto de todos aquéllos números contenidos en $\mathfrak{o}$ que son congruentes a un número determinado y por consiguiente también congruentes entre sí según μ, entonces, según la notación introducida en el §2, el número de estas clases diferentes será $= (\mathfrak{o}, \mathfrak{m})$, y como los números enteros $\mu\omega_1$, $\mu\omega_2$, $\ldots$, $\mu\omega_n$, que forman la base de $\mathfrak{m}$, están ligados a los números ω_1, ω_2, $\ldots$, ω_n por n ecuaciones de la forma (6), (§17), en las cuales los coeficientes $m_{i,i'}$ son necesariamente números racionales *enteros*, resulta de la ecuación que sigue a (7), junto con el teorema 4.º del §4, que el número de estas clases es

$$(\mathfrak{o}, \mathfrak{m}) = \pm \mathrm{N}(\mu).$$

El sistema $\mathfrak{m}$ es idéntico a $\mathfrak{o}$ siempre, y solamente entonces, cuando μ es una unidad, y se tiene al mismo tiempo que $\pm\mathrm{N}(\mu) = (\mathfrak{o}, \mathfrak{o}) = 1$.

Ahora, mientras que, con esta concepción de la congruencia, donde un número determinado μ no cabe más que como divisor o módulo, reina una completa analogía con la teoría de los números racionales, se manifiestan, como ya lo hemos indicado detalladamente en la Introducción y en la Sección

II, fenómenos totalmente nuevos a propósito de la cuestión de la composición de los números del dominio $\mathfrak{o}$ por medio de factores pertenecientes a este mismo dominio $\mathfrak{o}$. Estos fenómenos serán reconducidos a leyes determinadas y simples mediante la *Teoría de los ideales*, de la que trataremos los elementos en la Sección siguiente.

IV

Elementos de la teoría de los ideales.

En esta Sección, desarrollaremos la teoría de los ideales hasta el punto indicado en la Introducción, es decir demostraremos las leyes fundamentales que se aplican por igual a todos los cuerpos finitos sin excepción, y que gobiernan y explican los fenómenos de la divisibilidad en el dominio $\mathfrak{o}$ de todos los números enteros de un tal cuerpo Ω. No nos ocuparemos, en lo que va a seguir, más que de estos números, a menos que indiquemos expresamente lo contrario. La teoría se fundamenta sobre la noción de *ideal*, cuyo origen hemos mencionado en la Introducción, y cuya importancia ha sido suficientemente puesta de relieve mediante el ejemplo de la Sección II (§§11 y 12). La siguiente exposición de la teoría coincide en el fondo con la que di en la segunda edición de las *Vorlesungen über Zahlentheorie* de Dirichlet (§163); pero difiere notablemente por la forma externa; en virtud de estos cambios la teoría, aun no siendo abreviada, ha sido no obstante un poco simplificada, y en particular la principal dificultad que se trataba de vencer es ahora puesta más claramente de relieve.

§19.– *Los ideales y su divisibilidad.*

Sean, como en la Sección precedente, Ω un cuerpo finito de grado n, y $\mathfrak{o}$ el dominio de todos los números enteros ω contenidos en Ω. Entendemos por un *ideal* de este dominio $\mathfrak{o}$ todo sistema $\mathfrak{a}$ de números α del dominio $\mathfrak{a}$ que posee las dos propiedades siguientes:

I. Las sumas y las diferencias de dos números α cualesquiera del sistema $\mathfrak{a}$ pertenecen al mismo sistema $\mathfrak{a}$, es decir que $\mathfrak{a}$ es un módulo.

II. Todo producto $\alpha\omega$ de un número α del sistema $\mathfrak{a}$ por un número ω del sistema $\mathfrak{o}$ es un número del sistema $\mathfrak{a}$.

Señalemos en primer lugar un caso particularmente importante de esta concepción de *ideal*. Sea μ un número determinado; entonces el sistema $\mathfrak{a}$ de todos los números $\alpha = \mu\omega$ divisibles por μ constituirá un ideal. Llamaremos a un tal ideal un *ideal principal*, y lo designaremos por por $\mathfrak{o}(\mu)$, o más simplemente por $\mathfrak{o}\mu$ o $\mu\mathfrak{o}$; es evidente que este ideal no será alterado si se reemplaza μ por un número asociado, es decir por un número de la forma $\varepsilon\mu$, donde ε designa una unidad. Si μ es él mismo una unidad, se tendrá que $\mathfrak{o}\mu = \mathfrak{o}$, puesto que todos los números contenidos en $\mathfrak{o}$ son divisibles por μ. También es fácil reconocer que ningún otro ideal puede contener una unidad; pues si la unidad ε está contenida en el ideal $\mathfrak{a}$, entonces (según II) todos los productos $\varepsilon\omega$, y por consiguiente también todos los números

ω del ideal principal $\mathfrak{o}$ están contenidos en $\mathfrak{a}$, y como, por definición, todos los números del ideal $\mathfrak{a}$ están igualmente contenidos en $\mathfrak{o}$, se tendrá que $\mathfrak{a} = \mathfrak{o}$. Este ideal $\mathfrak{o}$ juega el mismo papel entre los ideales que el número 1 entre los números racionales enteros. En la noción de un ideal principal $\mathfrak{o}\mu$ está incluido también el caso singular en el que $\mu = 0$, y en el que por consiguiente el ideal se compone sólo del número cero; no obstante, excluiremos este caso en lo que seguirá.

En el caso en que $n = 1$, en el que nuestra teoría se transforma en la antigua teoría de los números, todo ideal es evidentemente un ideal principal, es decir un módulo de la forma $[m]$, siendo m un número racional entero (§§1 y 5); ocurre lo mismo con los cuerpos cuadráticos especiales, que han sido considerados en la Sección II (§6 y principio del §7). En todos estos casos, en los que todo ideal del cuerpo Ω es un ideal principal, reinan las mismas leyes de la divisibilidad de los números que en la teoría de los números racionales enteros; puesto que todo número *indescomponible* posee también el carácter de un número *primo* (*ver* la Introducción y el §7). De lo cual se podrá uno fácilmente convencer en lo que debe seguir; no obstante presento desde ahora esta observación para recomendar a los lectores que hagan la comparación continua con los casos mencionados y principalmente con la antigua teoría de los números racionales, porque sin ninguna duda eso facilitará mucho la comprensión de nuestra teoría general.

Puesto que todo ideal (en virtud de I) es un módulo, transportaremos inmediatamente a los ideales la noción de la divisibilidad de los módulos (§1). Se dice que un ideal $\mathfrak{m}$ es *divisible* por un ideal $\mathfrak{a}$, o que es un *múltiplo* de $\mathfrak{a}$, cuando todos los números contenidos en $\mathfrak{m}$ están también contenidos en $\mathfrak{a}$; se dice al mismo tiempo que $\mathfrak{a}$ es un *divisor* de $\mathfrak{m}$. Según eso, todo ideal es divisible por el ideal $\mathfrak{o}$. Si α es un número del ideal $\mathfrak{a}$, entonces el ideal principal $\mathfrak{o}\alpha$ será (según II) divisible por $\mathfrak{a}$; diremos, por esta razón, que el *número* α, y por consiguiente todo número contenido en $\mathfrak{a}$, es *divisible* por el ideal $\mathfrak{a}$.

Diremos del mismo modo que un ideal $\mathfrak{a}$, es *divisible* por el *número* η, cuando $\mathfrak{a}$ sea divisible por el ideal principal $\mathfrak{o}\eta$; entonces todos los números α del ideal $\mathfrak{a}$ serán de la forma $\eta\rho$, y es fácil ver que el sistema $\mathfrak{r}$ de todos los números $\rho = \frac{\alpha}{\eta}$ constituirá un ideal. Recíprocamente, si ρ se hace igual sucesivamente a todos los números de un ideal cualquiera $\mathfrak{r}$, mientras que η designa un número determinado, diferente de cero, entonces todos los productos $\eta\rho$ constituirán también un ideal divisible por $\mathfrak{o}\eta$; designaremos a un tal ideal, constituido por medio del ideal $\mathfrak{r}$ y del número η, para abreviar, por $\mathfrak{r}\eta$ o $\eta\mathfrak{r}$; se tendrá evidentemente que $(\mathfrak{r}\eta)\eta' = \mathfrak{r}(\eta\eta') = (\mathfrak{r}\eta')\eta$, y $\eta\mathfrak{r}'$ será siempre divisible por $\eta\mathfrak{r}$ en el caso, y solamente en el caso, en el que $\mathfrak{r}'$ sea divisible por $\mathfrak{r}$; luego la ecuación $\eta\mathfrak{r}' = \eta\mathfrak{r}$ implica la ecuación $\mathfrak{r}' = \mathfrak{r}$. La noción de un ideal principal $\mathfrak{o}\mu$ se deduce de la de $\mathfrak{r}\mu$, cuando se supone $\mathfrak{r} = \mathfrak{o}$.

Finalmente, ha de observarse que la divisibilidad del ideal principal $\mathfrak{o}\mu$ por el ideal principal $\mathfrak{o}\eta$ es completamente idéntica a la divisibilidad del *número* μ por el *número* η; las leyes de la divisibilidad de los *números* de $\mathfrak{o}$ están, pues, enteramente contenidas en las leyes de la divisibilidad de los *ideales*.

El mínimo común múltiplo $\mathfrak{m}$ y el máximo común divisor $\mathfrak{d}$ de dos ideales cualesquiera $\mathfrak{a}$, $\mathfrak{b}$ son también ideales; pues, en todos los casos, $\mathfrak{m}$ y $\mathfrak{d}$ son módulos (§1, 3.º y 4.º), y módulos divisibles por $\mathfrak{o}$, puesto que $\mathfrak{a}$ y $\mathfrak{b}$ son divisibles por $\mathfrak{o}$; si, además, $\mu = \alpha = \beta$ es un número contenido en $\mathfrak{m}$ y por lo tanto también en $\mathfrak{a}$ y en $\mathfrak{b}$, y si $\delta = \alpha' + \beta'$ es un número del módulo $\mathfrak{d}$, entonces el producto $\mu\omega = \alpha\omega = \beta\omega$ estará igualmente contenido en $\mathfrak{m}$, y el producto $\delta\omega = \alpha'\omega + \beta'\omega$ contenido en $\mathfrak{d}$, puesto que (en virtud de II) los productos $\alpha\omega$, $\alpha'\omega$ están contenidos en $\mathfrak{a}$ y los productos $\beta\omega$, $\beta'\omega$ están contenidos en $\mathfrak{b}$. Luego $\mathfrak{m}$ y $\mathfrak{d}$ gozan de todas las propiedades de un ideal. Está claro al mismo tiempo que $\mathfrak{m}\eta$ será el mínimo común múltiplo, y $\mathfrak{d}\eta$ el máximo común divisor de los dos ideales $\mathfrak{a}\eta$, $\mathfrak{b}\eta$.

Si $\mathfrak{b}$ es un ideal principal $\mathfrak{o}\eta$, entonces el mínimo común múltiplo $\mathfrak{m}$ de $\mathfrak{a}$ y $\mathfrak{b}$ será en todo caso de la forma $\eta\mathfrak{r}$, siendo $\mathfrak{r}$ también un ideal y, además, un divisor de $\mathfrak{a}$, puesto que $\eta\mathfrak{a}$ es un múltiplo común de $\mathfrak{a}$ y de $\mathfrak{o}\eta$, y por consiguiente divisible por $\eta\mathfrak{r}$; este caso se presentará muy frecuentemente en lo que sigue, y por esta razón llamaremos, para abreviar, al ideal $\mathfrak{r}$ el divisor del ideal $\mathfrak{a}$ *correspondiente* al número η. Ahora, si $\mathfrak{r}'$ es el divisor de $\mathfrak{r}$ correspondiente al número η', entonces $\mathfrak{r}'$ será al mismo tiempo el divisor de $\mathfrak{a}$ correspondiente al producto $\eta\eta'$, pues $\eta\eta'\mathfrak{r}'$ es el mínimo común múltiplo de $\eta\mathfrak{r}$ y de $\mathfrak{o}\eta\eta'$, y por consiguiente también el de $\mathfrak{a}$ y de $\mathfrak{o}\eta\eta'$, puesto que $\eta\mathfrak{r}$ es el mínimo común múltiplo de $\mathfrak{a}$ y de $\mathfrak{o}\eta$, y $\mathfrak{o}\eta\eta'$ es divisible por $\mathfrak{o}\eta$.

§20.– *Normas.*

Puesto que todo ideal $\mathfrak{a}$ es también un módulo, diremos que dos números cualesquiera ω, ω' del dominio $\mathfrak{o}$ son *congruentes* o *incongruentes según* $\mathfrak{a}$, según que su diferencia $\omega - \omega'$ sea o no divisible por $\mathfrak{a}$; representaremos la congruencia de ω, ω' módulo $\mathfrak{a}$ (§2) mediante la notación

$$\omega \equiv \omega' \pmod{\mathfrak{a}}.$$

Además de los teoremas establecidos previamente, que se cumplen para las congruencias con respecto a módulos cualesquiera, es también necesario observar que dos de estas congruencias

$$\omega \equiv \omega',\ \omega'' \equiv \omega''' \pmod{\mathfrak{a}},$$

relativas al mismo ideal $\mathfrak{a}$, pueden también ser multiplicadas entre ellas, y que ellas implican de este modo la congruencia

$$\omega\omega'' \equiv \omega'\omega''' \pmod{\mathfrak{a}};$$

pues los productos $(\omega - \omega')\omega''$ y $(\omega'' - \omega''')\omega'$, y por consiguiente también su suma $\omega\omega'' - \omega'\omega'''$, son números del ideal $\mathfrak{a}$. Si, además, $\mathfrak{m}$ es un ideal principal $\mathfrak{o}\mu$, entonces (en virtud del §18) la congruencia $\omega \equiv \omega' \pmod{\mathfrak{m}}$ será idéntica a la congruencia $\omega \equiv \omega' \pmod{\mu}$.

Una consideración particularmente importante es la del *número* de las clases de números diferentes respecto al ideal $\mathfrak{a}$, y de las que se compone el dominio $\mathfrak{o}$. Si μ es un número determinado del ideal $\mathfrak{a}$, y diferente de cero, entonces el ideal principal $\mathfrak{o}\mu$ será divisible por $\mathfrak{a}$, y puesto que $\mathfrak{a}$ es divisible por $\mathfrak{o}$, resulta que (§2, 4.º)

$$(\mathfrak{o}, \mathfrak{o}\mu) = (\mathfrak{o}, \mathfrak{a})(\mathfrak{o}, \mathfrak{o}\mu);$$

ahora bien (§18), el número $(\mathfrak{o}, \mathfrak{o}\mu) = \pm N(\mu)$, y por consiguiente el dominio $\mathfrak{o}$ sólo contiene un número finito de números incongruentes respecto al ideal $\mathfrak{a}$ (§2, 2.º). Este número $(\mathfrak{o}, \mathfrak{a})$ será denominado la *norma del ideal* $\mathfrak{a}$, y lo representaremos por $N(\mathfrak{a})$; la norma del ideal principal $\mathfrak{o}\mu$ es igual a $\pm N(\mu)$, y $\mathfrak{o}$ es evidentemente el único ideal cuya norma es igual a 1.

Si ρ recorre un sistema completo de $N(\mathfrak{a})$ números incongruentes (mód $\mathfrak{a}$), entonces lo mismo tendrá lugar para $(1 + \rho)$, y de las congruencias correspondientes $1 + \rho \equiv \rho'$, donde ρ' recorre los mismos valores que ρ, resulta, por adición, que $N(\mathfrak{a}) \equiv 0$ (mód $\mathfrak{a}$), es decir que $N(\mathfrak{a})$ siempre es divisible por $\mathfrak{a}$. Como caso particular, este resultado contiene este teorema evidente por sí mismo, que $N(\mu)$ es divisible por μ (ver §17).

Sea, además, $\mathfrak{r}$ un ideal cualquiera, y η un número diferente de cero; entonces se tendrá siempre que

$$(\mathfrak{o}\eta, \mathfrak{r}\eta) = (\mathfrak{o}, \mathfrak{r}) = N(\mathfrak{r});$$

pues dos números $\eta\omega'$ y $\eta\omega''$ del ideal principal $\eta\mathfrak{o}$ son congruentes o incongruentes (mód $\eta\mathfrak{r}$), según que los números ω', ω'' del dominio $\mathfrak{o}$ sean congruentes o incongruentes (mód $\mathfrak{r}$).

Sean $\mathfrak{a}$, $\mathfrak{b}$ dos ideales cualesquiera, $\mathfrak{m}$ su mínimo común múltiplo, y $\mathfrak{d}$ su máximo común divisor; entonces se tendrá (§2, 3.º y 4.º) que

$$(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{b}, \mathfrak{m}) = (\mathfrak{d}, \mathfrak{a}),$$

y, siendo $\mathfrak{d}$ divisible por $\mathfrak{o}$, que

$$(\mathfrak{o}, \mathfrak{a}) = (\mathfrak{o}, \mathfrak{d})(\mathfrak{d}, \mathfrak{a}), \quad (\mathfrak{o}, \mathfrak{m}) = (\mathfrak{o}, \mathfrak{b})(\mathfrak{b}, \mathfrak{m}),$$

por lo tanto

$$N(\mathfrak{a}) = (\mathfrak{b}, \mathfrak{a})N(\mathfrak{d}), \quad N(\mathfrak{m}) = (\mathfrak{b}, \mathfrak{a})N(\mathfrak{b}),$$

y

$$N(\mathfrak{m})N(\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Si se aplican estos teoremas al caso en el que $\mathfrak{b}$ es un ideal principal $\mathfrak{o}\eta$, y donde por consiguiente $\mathfrak{m}$ es de la forma $\mathfrak{r}\eta$, entonces siendo el ideal $\mathfrak{r}$ el divisor de $\mathfrak{a}$ correspondiente al número η (§19), obtenemos que

$$(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{o}\eta, \mathfrak{r}\eta) = N(\mathfrak{r}),$$

y por consiguiente que

$$N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{d}).$$

El ideal $\mathfrak{r}$ puede ahora también ser definido como el sistema de todas las raíces ρ de la congruencia $\eta\rho \equiv 0$ (mód $\mathfrak{a}$), como es fácil comprobar.

§21.– *Ideales primos.*

Un ideal $\mathfrak{p}$ se denomina un *ideal primo*, cuando es diferente de $\mathfrak{o}$, y no admite como divisor ningún otro ideal que no sea $\mathfrak{o}$ y $\mathfrak{p}$. De esta definición resultan los teoremas siguientes:

1.º Todo ideal $\mathfrak{a}$ diferente de $\mathfrak{o}$ es divisible al menos por un ideal primo.

Pues, de entre todos los ideales que son diferentes de $\mathfrak{o}$ y divisores de $\mathfrak{a}$, existe un $\mathfrak{p}$ cuya norma es la *mínima*, y ése es ciertamente un ideal primo; si, en efecto, $\mathfrak{d}$ fuera un ideal que dividiera a $\mathfrak{p}$, pero diferente de $\mathfrak{p}$ y $\mathfrak{o}$, se tendría que $(\mathfrak{d}, \mathfrak{p}) > 1$, por consiguiente $N(\mathfrak{p}) = (\mathfrak{d}, \mathfrak{p})N(\mathfrak{d}) > N(\mathfrak{d})$, y $\mathfrak{d}$ sería

un divisor del ideal $\mathfrak{a}$, diferente de $\mathfrak{o}$ y cuya norma sería $< \mathrm{N}(\mathfrak{p})$, contra la hipótesis; luego $\mathfrak{p}$ es un ideal primo.

Q.E.D.

2.º Si el número η no es divisible por el ideal primo $\mathfrak{p}$, entonces $\eta\mathfrak{p}$ será el mínimo común múltiplo de los dos ideales $\mathfrak{p}$ y $\mathfrak{o}\eta$.

Pues el mínimo común múltiplo de $\mathfrak{p}$ y de $\mathfrak{o}\eta$ es en todos los casos de la forma $\eta\mathfrak{r}$, siendo el ideal $\mathfrak{r}$ un divisor de $\mathfrak{p}$, y por consiguiente o $= \mathfrak{o}$ o $= \mathfrak{p}$ (§19); pero $\mathfrak{r}$ no puede ser $= \mathfrak{o}$, puesto que $\eta\mathfrak{o}$ no es divisible por $\mathfrak{p}$; por consiguiente $\mathfrak{r} = \mathfrak{p}$.

Q.E.D.

3.º Si ninguno de los dos números η, ρ es divisible por el ideal primo $\mathfrak{p}$, su producto $\eta\rho$ tampoco será divisible por $\mathfrak{p}$.

Pues de lo contrario el ideal $\eta(\mathfrak{o}\rho)$ sería un múltiplo común de $\mathfrak{p}$, $\mathfrak{o}\eta$; y por lo tanto sería divisible por el mínimo común múltiplo $\eta\mathfrak{p}$ de $\mathfrak{p}$, $\mathfrak{o}\eta$; pero de la divisibilidad de $\eta(\mathfrak{o}\rho)$ por $\eta\mathfrak{p}$ resultaría (§19) que $\mathfrak{o}\rho$ sería divisible por $\mathfrak{p}$, lo que contradiría la suposición; luego $\eta\rho$ no es divisible por $\mathfrak{p}$.

Q.E.D.

De ahí se sigue inmediatamente que todos los números *racionales* divisibles por un ideal primo $\mathfrak{p}$, y a los cuales pertenece también $\mathrm{N}(\mathfrak{p})$ (§20), constituyen un módulo $[p]$, siendo p un *número primo* racional positivo completamente determinado; pues el *mínimo* número racional positivo p, divisible por $\mathfrak{p}$, no puede ser de ningún modo un número compuesto ab, puesto que entonces uno de los dos números menores a, b sería igualmente divisible por $\mathfrak{p}$; y como p no puede ser $= 1$, puesto que se tendría entonces que $\mathfrak{p} = \mathfrak{o}$ (§19), p deberá ser un número primo; y todo número racional entero m divisible por $\mathfrak{p}$ deberá ser divisible por p, lo cual se hace inmediatamente evidente, poniendo m bajo la forma $pq + r$, puesto que el resto $r = m - pq$ es también divisible por $\mathfrak{p}$. Ahora, siendo $\mathfrak{o}p$ divisible por $\mathfrak{p}$, y por consiguiente $\mathrm{N}(\mathfrak{o}p) = p^n$ divisible por $\mathrm{N}(\mathfrak{p})$ (§20), $\mathrm{N}(\mathfrak{p}) = p^f$ será una potencia de p, y el exponente f se denominará el *grado del ideal primo* $\mathfrak{p}$.

4.º Si el ideal $\mathfrak{a}$ es divisible por el ideal primo $\mathfrak{p}$, entonces existirá un número η tal que $\eta\mathfrak{p}$ sea el mínimo común múltiplo de $\mathfrak{a}$ y de $\mathfrak{o}\eta$.

Este teorema importante es evidente, si se tiene que $\mathfrak{a} = \mathfrak{p}$, puesto que todo número η no divisible por $\mathfrak{p}$, por ejemplo, el número $\eta = 1$, satisface la condición indicada. Pero si $\mathfrak{a}$ es diferente de $\mathfrak{p}$, entonces nos limitaremos en primer lugar a demostrar la existencia de un número η tal que el divisor $\mathfrak{r}$ del ideal $\mathfrak{a}$, correspondiente a η, sea al mismo tiempo divisible por $\mathfrak{p}$, pero tenga una norma *menor* que la de $\mathfrak{a}$. Puesto que se tiene que $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{r})\mathrm{N}(\mathfrak{d})$, siendo $\mathfrak{d}$ el máximo común divisor de $\mathfrak{a}$ y de $\mathfrak{o}\eta$ (§20), la última condición equivale a elegir η de manera que $\mathrm{N}(\mathfrak{d})$ sea > 1, y por lo tanto $\mathfrak{d}$ diferente de $\mathfrak{o}$. Para alcanzar este objetivo, y hacer al mismo tiempo que $\mathfrak{r}$ sea divisible por $\mathfrak{p}$, distinguiremos dos casos:

Primero, si todos los ideales (con la excepción de $\mathfrak{o}$) que dividen a $\mathfrak{a}$ son divisibles por $\mathfrak{p}$, se elegirá como η un número divisible por $\mathfrak{p}$, pero no divisible por $\mathfrak{a}$, lo cual siempre es posible, puesto que $\mathfrak{p}$ no es divisible por $\mathfrak{a}$; entonces está claro que $\mathfrak{d}$ será divisible por $\mathfrak{p}$, y por consiguiente diferente de

$\mathfrak{o}$; como, además, η no es divisible por $\mathfrak{a}$, pero $\eta\mathfrak{r}$ es divisible por $\mathfrak{a}$, entonces $\mathfrak{r}$ será igualmente diferente de $\mathfrak{o}$, y por consiguiente divisible por $\mathfrak{p}$.

Segundo, si existe un ideal $\mathfrak{e}$ que divide a $\mathfrak{a}$, y que sea diferente de $\mathfrak{o}$ y no divisible por $\mathfrak{p}$, elijamos como η un número divisible por $\mathfrak{e}$, pero no divisible por $\mathfrak{p}$; entonces $\mathfrak{d}$ será divisible por $\mathfrak{e}$, y por lo tanto también diferente de $\mathfrak{o}$; como, además, $\eta\mathfrak{r}$ es divisible por $\mathfrak{a}$ y por consiguiente también por $\mathfrak{p}$, entonces $\mathfrak{r}$ será también divisible por $\mathfrak{p}$, puesto que η no es divisible por $\mathfrak{p}$ (según 2.º).

Después de haber establecido de este modo para los dos casos la existencia de al menos un número η que tiene la propiedad exigida, se reconoce sin esfuerzo que se tiene ciertamente que $\mathfrak{r} = \mathfrak{p}$, si se escoge, además, η de manera que $\mathrm{N}(\mathfrak{r})$ sea *tan pequeña como sea posible*; pues, si el ideal $\mathfrak{r}$, divisible por $\mathfrak{p}$, no es $= \mathfrak{p}$, entonces se puede proceder con $\mathfrak{r}$ como se acaba de hacer con $\mathfrak{a}$, y elegir un número η' de manera que el divisor $\mathfrak{r}'$ de $\mathfrak{r}$, correspondiente a este número, tenga una norma aun menor que la de $\mathfrak{r}$, y sea igualmente divisible por $\mathfrak{p}$; pero como (§19) $\mathfrak{r}'$ es al mismo tiempo el divisor de $\mathfrak{a}$ correspondiente al número $\eta\eta'$, esto entra en contradicción con la suposición que se acaba de hacer sobre η y sobre $\mathfrak{r}$. Por lo tanto $\mathfrak{r} = \mathfrak{p}$, es decir que $\eta\mathfrak{p}$ es el mínimo común múltiplo de $\mathfrak{a}$ y de $\mathfrak{o}\eta$.

Q.E.D.

§22.– *Multiplicación de los ideales.*

Si α recorre todos los números de un ideal $\mathfrak{a}$, y del mismo modo β todos los números del ideal $\mathfrak{b}$, entonces todos los productos de la forma $\alpha\beta$ y todas las sumas de estos productos constituirán un ideal $\mathfrak{c}$; pues todos estos números están contenidos en $\mathfrak{o}$; además, son estables bajo la adición, y también bajo la substracción, puesto que los números $(-\alpha)$ están igualmente contenidos en $\mathfrak{a}$; y finalmente todo producto de un número $\sum\alpha\beta$ del sistema $\mathfrak{c}$ y de un número ω del dominio $\mathfrak{o}$ pertenece igualmente al sistema $\mathfrak{c}$, puesto que todo producto $\alpha\omega$ está también contenido en $\mathfrak{a}$. Este ideal $\mathfrak{c}$ se denominará el *producto* de los dos factores $\mathfrak{a}$, $\mathfrak{b}$, y lo designaremos por $\mathfrak{ab}$.

De esta definición se sigue inmediatamente que se tiene $\mathfrak{oa} = \mathfrak{a}$, $\mathfrak{ab} = \mathfrak{ba}$, y, si $\mathfrak{c}$ es un tercer ideal cualquiera, $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc})$, y se concluye por el razonamiento conocido([37]) que, en la formación de un producto de un número cualquiera de ideales $\mathfrak{a}_1$, $\mathfrak{a}_2$, …, $\mathfrak{a}_m$, el orden de las multiplicaciones sucesivas, por las cuales se reúnen cada vez *dos* ideales en un solo producto, no tiene ninguna influencia sobre el resultado final, el cual puede ser designado, para abreviar, por $\mathfrak{a}_1\mathfrak{a}_2\ldots\mathfrak{a}_m$, y se compone evidentemente de todos los números de la forma $\sum\alpha_1\alpha_2\ldots\alpha_m$, donde α_1, α_2, …, α_m designan números cualesquiera de los factores $\mathfrak{a}_1$, $\mathfrak{a}_2$, …, $\mathfrak{a}_m$. Si todos los m factores son $= \mathfrak{a}$, entonces su producto se denominará la m-sima *potencia* de $\mathfrak{a}$, y se la representará por $\mathfrak{a}^m$; poniendo, además, $\mathfrak{a}^0 = \mathfrak{o}$, $\mathfrak{a}^1 = \mathfrak{a}$, se tendrá en general $\mathfrak{a}^r\mathfrak{a}^s = \mathfrak{a}^{r+s}$, $(\mathfrak{a}^r)^s = \mathfrak{a}^{rs}$. Además, se tendrá evidentemente $\mathfrak{a}(\mathfrak{o}\eta) = \mathfrak{a}\eta$ y $(\mathfrak{o}\eta)(\mathfrak{o}\eta') = \mathfrak{o}\eta\eta'$. Finalmente estableceremos además los teoremas siguientes:

1.º El producto $\mathfrak{ab}$ es divisible por los factores $\mathfrak{a}$ y $\mathfrak{b}$; pues (en virtud de la propiedad II) todo producto $\alpha\omega$, luego también todo producto $\alpha\beta$,

[37] Ver §2 de las *Vorlesungen über Zahlentheorie* de Dirichlet.

y consecuentemente (según I) toda suma de semejantes productos están contenidos en $\mathfrak{a}$, es decir que $\mathfrak{ab}$ será divisible por $\mathfrak{a}$.

2.º Si $\mathfrak{a}$ es divisible por $\mathfrak{a}'$, y $\mathfrak{b}$ divisible por $\mathfrak{b}'$, entonces $\mathfrak{ab}$ será divisible por $\mathfrak{a}'\mathfrak{b}'$. Porque todos los números $\sum \alpha\beta$ contenidos en $\mathfrak{ab}$ están contenidos en $\mathfrak{a}'\mathfrak{b}'$, puesto que α está contenido en $\mathfrak{a}$ y por consiguiente en $\mathfrak{a}'$, y β está contenido en $\mathfrak{b}$ y por consiguiente en $\mathfrak{b}'$.

3.º Si ninguno de los ideales $\mathfrak{a}$, $\mathfrak{b}$ es divisible por el ideal primo $\mathfrak{p}$, entonces el producto $\mathfrak{ab}$ tampoco será divisible por $\mathfrak{p}$; pues existen en $\mathfrak{a}$, $\mathfrak{b}$ respectivamente números α, β que no son divisibles por $\mathfrak{p}$, y como consecuencia el número $\alpha\beta$ contenido en $\mathfrak{ab}$ tampoco es divisible por $\mathfrak{p}$ (§21, 3.º).

§23.– *La dificultad de la teoría.*

Sería fácil aumentar considerablemente el número de estos teoremas, que se refieren a la dependencia entre las dos nociones de la *divisibilidad* y de la *multiplicación* de los ideales, y enunciaremos también sin demostración las proposiciones siguientes, únicamente para hacer resaltar la semejanza con las proposiciones correspondientes de la teoría de los números racionales:

Si $\mathfrak{a}$, $\mathfrak{b}$ son ideales *primos entre sí*, es decir tales que su máximo común divisor sea $= \mathfrak{o}$, entonces su mínimo común múltiplo será $= \mathfrak{ab}$, y se tendrá al mismo tiempo que

$$\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}).$$

Si $\mathfrak{p}$ es un ideal primo, y $\mathfrak{a}$ un ideal cualquiera, entonces o $\mathfrak{a}$ será divisible por $\mathfrak{p}$, o $\mathfrak{a}$ y $\mathfrak{p}$ serán ideales primos entre sí.

Si $\mathfrak{a}$ es un ideal primo con $\mathfrak{b}$ y con $\mathfrak{c}$, entonces $\mathfrak{a}$ será también primo con $\mathfrak{bc}$.

Si $\mathfrak{ab}$ es divisible por $\mathfrak{c}$, y $\mathfrak{a}$ es primo con $\mathfrak{c}$, entonces $\mathfrak{b}$ será divisible por $\mathfrak{c}$.

Pero todas estas proposiciones no son suficientes para completar la analogía con la teoría de los números racionales. Es necesario no olvidar que la divisibilidad de un ideal $\mathfrak{c}$ por un ideal $\mathfrak{a}$, según nuestra definición (§19), consiste solamente en que todos los números del ideal $\mathfrak{c}$ están contenidos también en $\mathfrak{a}$; ahora bien, se ha visto muy fácilmente (§22, 1.º) que todo producto de $\mathfrak{a}$ por un ideal cualquiera $\mathfrak{b}$ es divisible por $\mathfrak{a}$, pero no es de ningún modo fácil demostrar la recíproca, a saber, que todo ideal divisible por $\mathfrak{a}$ es también un producto de $\mathfrak{a}$ por un ideal $\mathfrak{b}$. Esta dificultad, la máxima y, hablando con propiedad, la única que presenta la teoría, no puede de ninguna manera ser vencida con la ayuda solamente de los medios de demostración que hemos empleado hasta aquí, y es necesario que examinemos aquí cuidadosamente la razón de este fenómeno, porque está relacionada con una generalización muy importante de la teoría. Considerando con atención la teoría desarrollada hasta ahora, se reconocerá que todas las definiciones conservan un sentido determinado, y que las demostraciones de todos los teoremas siguen teniendo toda su fuerza, aunque ya *no se suponga* que el dominio designado por $\mathfrak{o}$ abarque a *todos* los números enteros del cuerpo Ω. Las propiedades del sistema $\mathfrak{o}$ sobre las cuales nos hemos apoyado se reducen en realidad a las siguientes:

(a) El sistema $\mathfrak{o}$ es un módulo finito $[\omega_1, \omega_2, \ldots, \omega_n]$, cuya base forma al mismo tiempo una base del cuerpo Ω.

(b) El número 1, y por lo tanto también todos los números racionales enteros están contenidos en $\mathfrak{o}$.

(c) Todo producto de dos números del sistema $\mathfrak{o}$ pertenece al mismo sistema $\mathfrak{o}$.

Cuando un dominio $\mathfrak{o}$ goce de estas tres propiedades, lo llamaremos un *orden*. De la conjunción de (a) y de (c) resulta inmediatamente que un orden se compone solamente de números *enteros* del cuerpo Ω, pero no contiene necesariamente a *todos* estos números enteros (a excepción del caso $n = 1$). Si ahora un número α del orden $\mathfrak{o}$ es llamado *divisible* por un segundo número semejante μ solamente en el caso en el que se tiene $\alpha = \mu\omega$, donde ω designa igualmente un número contenido en $\mathfrak{o}$, y si se modifica de la misma manera la noción de la *congruencia* de los números en la extensión del dominio $\mathfrak{o}$, entonces se ve inmediatamente que el número $(\mathfrak{o}, \mathfrak{o}\mu)$ de los números del dominio $\mathfrak{o}$ incongruentes con respecto a μ es también ahora $= \pm\mathrm{N}(\mu)$ (§18), y es también fácil reconocer que todas las definiciones y todos los teoremas de la presente Sección conservarán su significado y su verdad, si se entiende siempre por *número* un número de este orden $\mathfrak{o}$. En todo orden $\mathfrak{o}$ del cuerpo Ω existe, pues, una teoría particular de los ideales, y esta teoría es la misma para todos los órdenes (que son en número infinito), hasta el punto en el que ha sido desarrollada en lo que precede. Pero, mientras que la teoría de los ideales, en el orden $\mathfrak{o}$ que contiene a *todos* los números enteros del cuerpo Ω, conduce finalmente a leyes generales que no admiten ninguna excepción y que coinciden completamente con las leyes de la divisibilidad de los números racionales, la teoría de los ideales de cada uno de los otros órdenes está sujeta a ciertas excepciones, o, más bien, exige una cierta restricción de la noción de ideal. Pero esta teoría general de los ideales de un orden cualquiera, cuyo desarrollo es igualmente indispensable para las necesidades de la teoría de los números, y que, en el caso $n = 2$, coincide con la teoría de los diversos *órdenes* de las *formas* cuadráticas binarias([38]), la dejaremos enteramente de lado en lo que sigue([39]), y me contentaré aquí con dar un ejemplo para llamar la atención sobre el carácter de las excepciones de las que acabamos de hablar.

En el cuerpo cuadrático, resultante de una raíz

$$\theta = \frac{-1 + \sqrt{-3}}{2}$$

de la ecuación $\theta^2 + \theta + +1 = 0$, el módulo $[1, \sqrt{-3}]$ constituye un orden $\mathfrak{o}$ que no contiene a todos los números enteros de este cuerpo. Los módulos $[2, 1 + \sqrt{-3}] = \mathfrak{p}$ y $[2, 2\sqrt{-3}] = \mathfrak{o}(2)$ deberían ser considerados como ideales de este orden, en tanto que gozan de las propiedades I y II (§19); pero, aunque $\mathfrak{o}(2)$ sea divisible por $\mathfrak{p}$, no existe sin embargo en $\mathfrak{o}$ ningún ideal $\mathfrak{q}$ tal que se tenga $\mathfrak{pq} = \mathfrak{o}(2)$.

§24.– *Proposiciones auxiliares.*

[38] *Disquisitiones arithmeticae*, art. 226.

[39] Trato esta teoría en detalle en la Memoria recientemente publicada: *"Ueber die Anzahl der Ideal-Classen in den verschiedenen Ordnungen eines endlichen Körpers."* (*Festchrift zur Säcularfeier des Geburtstages von C.-F. Gauss.* Brunswick, 30 Abril 1877).

Para acabar ahora completamente la teoría de los ideales de aquél de los órdenes $\mathfrak{o}$ que contiene a *todos* los números enteros del cuerpo Ω, tenemos necesidad de los lemas siguientes, que no son verdaderos sin restricción más que para un tal dominio $\mathfrak{o}$.

1.º Sean ω, μ, ν tres números de $\mathfrak{o}$, diferentes de cero, y tales que ν no sea divisible por μ; entonces los términos de la progresión geométrica

$$\omega, \quad \omega\frac{\nu}{\mu}, \quad \omega\left(\frac{\nu}{\mu}\right)^2, \quad \omega\left(\frac{\nu}{\mu}\right)^3, \ldots,$$

hasta un término

$$\omega\left(\frac{\nu}{\mu}\right)^e,$$

situado a una distancia finita, estarán todos contenidos en $\mathfrak{o}$, y ninguno de los términos siguientes será un número entero.

En efecto, si el número de los términos que son números enteros fuera mayor que el valor absoluto k de $\mathrm{N}(\omega)$, sería necesario (§18) que, de entre $k+1$ de estos términos, hubiera al menos dos diferentes que correspondieran a los exponentes s y $r > s$, y que fueran congruentes entre sí según el módulo ω; ahora bien, de una tal congruencia

$$\omega\left(\frac{\nu}{\mu}\right)^r \equiv \omega\left(\frac{\nu}{\mu}\right)^s \pmod{\omega}$$

resultaría que el número

$$\eta = \frac{\nu}{\mu},$$

perteneciente al cuerpo Ω, satisfaría una ecuación de r-simo grado de la forma

$$\eta^r = \eta^s + \omega'$$

siendo ω' un número entero, y por consiguiente (§13, 2.ª) sería él mismo un número entero, lo cual es contrario a nuestra hipótesis de que ν no es divisible por μ. Luego a lo sumo k términos de la sucesión precedente pueden ser números enteros, y por consiguiente estar contenidos en $\mathfrak{o}$. Si, además, el término

$$\rho = \omega\left(\frac{\nu}{\mu}\right)^r,$$

siendo $r \geq 1$, es un número entero, y s es uno cualquiera de los r exponentes $0, 1, 2, \ldots, r-1$, entonces el término

$$\sigma = \omega\left(\frac{\nu}{\mu}\right)^s$$

será también un número entero, puesto que

$$\sigma^r = \omega^{r-s}\rho^s$$

es un número entero (§13, 2.ª). De este modo la proposición queda completamente demostrada.

2.º Sean μ, ν dos números de $\mathfrak{o}$, diferentes de cero, no siendo ν divisible por μ; entonces existen siempre en $\mathfrak{o}$ dos números κ, λ, diferentes de cero, y tales que que se tenga

$$\frac{\kappa}{\lambda} = \frac{\nu}{\mu},$$

y κ^2 no sea divisible por λ.

Pues si

$$\lambda = \mu\left(\frac{\nu}{\mu}\right)^{e-1}, \kappa = \mu\left(\frac{\nu}{\mu}\right)^{e}$$

son los dos últimos términos de la sucesión

$$\mu, \quad \mu\frac{\nu}{\mu}, \quad \mu\left(\frac{\nu}{\mu}\right)^2, \quad \mu\left(\frac{\nu}{\mu}\right)^3, \ldots$$

que son números enteros y por consiguiente contenidos en $\mathfrak{o}$, se tendrá evidentemente que $e \geq 1$, y

$$\frac{\kappa}{\lambda} = \frac{\nu}{\mu}, \frac{\kappa^2}{\lambda} = \mu\left(\frac{\nu}{\mu}\right)^{e+1};$$

luego κ^2 no es divisible por λ.

Q.E.D.

§25.– *Leyes de la divisibilidad.*

Con la ayuda de estos lemas, es fácil aportar a la teoría de los ideales del dominio $\mathfrak{o}$ el complemento deseado, que se encuentra contenido en las leyes siguientes:

1.ª Si $\mathfrak{p}$ es un ideal primo, entonces existe un número λ divisible por $\mathfrak{p}$, y un número κ no divisible por $\mathfrak{p}$, tales que $\kappa\mathfrak{p}$ sea el mínimo común múltiplo de $\mathfrak{o}\lambda$ y $\mathfrak{o}\kappa$.

Demostración.— Sea μ un número cualquiera, pero distinto de cero, del ideal primo $\mathfrak{p}$; siendo $\mathfrak{o}\mu$ divisible por $\mathfrak{p}$, existirá un número ν tal que $\nu\mathfrak{p}$ sea el mínimo común múltiplo de $\mathfrak{o}\mu$ y $\mathfrak{o}\nu$ (§21, 4.º). Este número ν no puede ser divisible por μ; pues en el caso contrario el mínimo común múltiplo de $\mathfrak{o}\mu$ y de $\mathfrak{o}\nu$ sería $= \mathfrak{o}\nu$, y no $= \mathfrak{p}\nu$. Si se eligen ahora (§24, 2.º) los dos números κ, λ de tal manera que se tenga $\kappa\mu = \lambda\nu$, y que κ^2 no sea divisible por λ, entonces (§19) el ideal $\kappa\nu\mathfrak{p}$ será el mínimo común múltiplo de $\kappa(\mathfrak{o}\mu) = \mathfrak{o}\lambda\nu$ y de $\mathfrak{o}\kappa\nu$, de donde se sigue (§19) que $\kappa\mathfrak{p}$ es el mínimo común múltiplo de $\mathfrak{o}\lambda$ y $\mathfrak{o}\kappa$; luego $\mathfrak{p}$ es el divisor correspondiente al número κ del ideal principal $\mathfrak{o}\lambda$; pero κ no es divisible por $\mathfrak{p}$, puesto que, si lo fuera, entonces κ^2 sería divisible por $\kappa\mathfrak{p}$ y por consiguiente también por λ.

2.ª Todo ideal primo $\mathfrak{p}$ puede, por medio de la multiplicación por un ideal $\mathfrak{d}$, ser transformado en un ideal principal.

Demostración.— Conservemos para κ y λ el mismo significado que antes, y sea $\mathfrak{d}$ el máximo común divisor de $\mathfrak{o}\lambda$ y de $\mathfrak{o}\kappa$; entonces vamos a demostrar que se tiene $\mathfrak{p}\mathfrak{d} = \mathfrak{o}\lambda$. En efecto, siendo todos los números del ideal $\mathfrak{d}$ de la forma $\delta = \kappa\omega + \lambda\omega'$, donde ω, ω' son dos números de $\mathfrak{o}$, entonces, si ϖ es un número cualquiera de $\mathfrak{p}$, se tendrá que $\varpi\delta = \kappa\varpi\omega + \lambda\varpi\omega' \equiv 0$ (mód λ), puesto que $\kappa\mathfrak{p}$ y por consiguiente también $\kappa\varpi$ son divisibles por $\mathfrak{o}\lambda$; luego $\mathfrak{p}\mathfrak{d}$ es divisible por $\mathfrak{o}\lambda$. Recíprocamente, no siendo κ divisible por $\mathfrak{p}$, y siendo por lo tanto $\mathfrak{o}$ el máximo común divisor de $\mathfrak{o}\kappa$ y $\mathfrak{p}$, se puede poner el número 1, contenido en $\mathfrak{o}$, $= \kappa\omega + \varpi$, estando ω contenido en $\mathfrak{o}$ y ϖ en $\mathfrak{p}$; entonces se tendrá que $\lambda = \lambda.\kappa\omega + \varpi\lambda \equiv 0$ (mód $\mathfrak{p}\mathfrak{d}$), puesto que los primeros factores λ, ϖ están contenidos en $\mathfrak{p}$, y los segundos factores $\kappa\omega$, λ contenidos en $\mathfrak{d}$.

De este modo cada uno de los dos ideales $\mathfrak{p}\mathfrak{d}$ y $\mathfrak{o}\lambda$ es divisible por el otro, y por consiguiente $\mathfrak{p}\mathfrak{d} = \mathfrak{o}\lambda$.

Q.E.D.

3.ª Si el ideal $\mathfrak{a}$ es divisible por el ideal primo $\mathfrak{p}$, entonces existirá un ideal $\mathfrak{a}'$, y solo uno, tal que se tendrá $\mathfrak{p}\mathfrak{a}' = \mathfrak{a}$, y al mismo tiempo se tendrá que $\mathrm{N}(\mathfrak{a}') < \mathrm{N}(\mathfrak{a})$.

Demostración.— Sea, como justo antes, $\mathfrak{p}\mathfrak{d} = \mathfrak{o}\lambda$; siendo $\mathfrak{a}$ divisible por $\mathfrak{p}$, y por consiguiente $\mathfrak{a}\mathfrak{d}$ por $\mathfrak{p}\mathfrak{d}$ (§22, 2.º), se tendrá que $\mathfrak{a}\mathfrak{d} = \lambda\mathfrak{a}'$, representando $\mathfrak{a}'$ un ideal (§19); entonces multiplicando por $\mathfrak{p}$, se obtiene de ahí que $\lambda\mathfrak{a} = \lambda\mathfrak{p}\mathfrak{a}'$, y por consiguiente también que $\mathfrak{a} = \mathfrak{p}\mathfrak{a}'$. Sea ahora $\mathfrak{b}$ un ideal, que satisface igualmente la condición $\mathfrak{p}\mathfrak{b} = \mathfrak{a}$; entonces de la igualdad $\mathfrak{p}\mathfrak{b} = \mathfrak{p}\mathfrak{a}'$ resulta, multiplicando por $\mathfrak{d}$, que se deberá tener $\lambda\mathfrak{b} = \lambda\mathfrak{a}'$, de donde $\mathfrak{b} = \mathfrak{a}'$. Existe además (§21, 4.º) un número η tal que $\eta\mathfrak{p}$ es el mínimo común múltiplo de $\mathfrak{a}$ y de $\mathfrak{o}\eta$; ahora bien, siendo $\eta\mathfrak{p}$ divisible por $\mathfrak{a} = \mathfrak{a}'\mathfrak{p}$, se sigue, multiplicando por $\mathfrak{d}$, que $\mathfrak{o}\eta\lambda$ es divisible por $\lambda\mathfrak{a}'$, y por consiguiente η por $\mathfrak{a}'$; pero η ciertamente no es divisible por $\mathfrak{a}$, pues en el caso contrario sería $\mathfrak{o}\eta$, y no $\eta\mathfrak{p}$, el mínimo común múltiplo de $\mathfrak{a}$ y $\mathfrak{o}\eta$. Luego, siendo η divisible por $\mathfrak{a}'$, pero no divisible por $\mathfrak{a}$, es necesario que $\mathfrak{a}'$ sea *diferente* de $\mathfrak{a}$, y por consiguiente que se tenga que $\mathrm{N}(\mathfrak{a}') < \mathrm{N}(\mathfrak{a})$, puesto que $\mathfrak{a}'$ es un divisor de $\mathfrak{a}$.

Q.E.D.

4.ª Todo ideal $\mathfrak{a}$ diferente de $\mathfrak{o}$ es él mismo un ideal primo, o bien puede ponerse bajo la forma de un producto de ideales todos primos, y esto de una sola manera.

Demostración.— Puesto que $\mathfrak{a}$ diferente de $\mathfrak{o}$, existe (§21, 1.º) un ideal primo $\mathfrak{p}_1$ que divide a $\mathfrak{a}$ y por consiguiente se puede poner (según 3º) $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1$, donde $\mathrm{N}(\mathfrak{a}_1) < \mathrm{N}(\mathfrak{a})$. Si se tiene que $\mathfrak{a}_1 = \mathfrak{o}$, entonces $\mathfrak{a} = \mathfrak{p}_1$ será un ideal primo; pero si $\mathrm{N}(\mathfrak{a}_1)$ es > 1, y por lo tanto $\mathfrak{a}_1$ es diferente de $\mathfrak{o}$, entonces se podrá poner de la misma manera $\mathfrak{a}_1 = \mathfrak{p}_2\mathfrak{a}_2$, siendo $\mathfrak{p}_2$ un ideal primo, y $\mathrm{N}(\mathfrak{a}_2) < \mathrm{N}(\mathfrak{a}_1)$. Si $\mathrm{N}(\mathfrak{a}_2)$ es > 1, entonces se podrá continuar de la misma manera, hasta que, de entre los ideales $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{a}_3$, ..., cuyas normas son cada vez más pequeñas, ocurra el ideal $\mathfrak{o} = \mathfrak{a}_m$, lo cual debe tener lugar después de un número finito de descomposiciones. Se tendrá entonces

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_m,$$

puesto bajo la forma de un producto de m ideales primos. Si ahora se tiene al mismo tiempo que

$$\mathfrak{a} = \mathfrak{q}_1\mathfrak{q}_2 \ldots \mathfrak{q}_r,$$

donde $\mathfrak{q}_1$, $\mathfrak{q}_2$, ..., $\mathfrak{q}_r$ designan igualmente ideales primos, entonces $\mathfrak{q}_1$ será un divisor del producto $\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_m$, y por consiguiente (§22, 3.º) uno al menos de los factores, por ejemplo $\mathfrak{p}_1$, deberá ser divisible por $\mathfrak{q}_1$, y como $\mathfrak{p}_1$ no es divisible más que por los dos ideales $\mathfrak{o}$ y $\mathfrak{p}_1$, necesariamente se tendrá que $\mathfrak{q}_1 = \mathfrak{p}_1$, puesto que $\mathfrak{q}_1$ es diferente de $\mathfrak{o}$. Se tendrá pues que

$$\mathfrak{p}_1(\mathfrak{p}_2\mathfrak{p}_3 \ldots \mathfrak{p}_m) = \mathfrak{p}_1(\mathfrak{q}_2\mathfrak{q}_3 \ldots \mathfrak{q}_r),$$

de donde (según 3.ª)

$$\mathfrak{p}_2\mathfrak{p}_3 \ldots \mathfrak{p}_m = \mathfrak{q}_2\mathfrak{q}_3 \ldots \mathfrak{q}_r.$$

Se podrá continuar de la misma manera, exactamente igual que en la teoría de los números racionales([40]), y se llegará de este modo al resultado de que todo ideal primo que ocurra como factor en uno de los productos ocurrirá exactamente el mismo número de veces como factor en el otro producto.

Q.E.D.

5.ª Todo ideal $\mathfrak{a}$ puede, mediante la multiplicación por un ideal $\mathfrak{m}$, ser transformado en un ideal principal.

Demostración.— Sea, en efecto, $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_m$; entonces se podrá (según 2º), multiplicando los ideales primos $\mathfrak{p}_1$, $\mathfrak{p}_2$, …, $\mathfrak{p}_m$ por los ideales correspondientes $\mathfrak{d}_1$, $\mathfrak{d}_2$, …, $\mathfrak{d}_m$, transformarlos en ideales principales $\mathfrak{p}_1\mathfrak{d}_1$, $\mathfrak{p}_2\mathfrak{d}_2$, …, $\mathfrak{p}_m\mathfrak{d}_m$. Si se pone ahora

$$\mathfrak{m} = \mathfrak{d}_1\mathfrak{d}_2 \dots \mathfrak{d}_m,$$

entonces $\mathfrak{a}\mathfrak{m} = (\mathfrak{p}_1\mathfrak{d}_1)(\mathfrak{p}_2\mathfrak{d}_2) \dots (\mathfrak{p}_m\mathfrak{d}_m)$ será un producto únicamente de ideales principales, y por consiguiente será él mismo un ideal principal.

Q.E.D.

6.ª Si el ideal $\mathfrak{c}$ es divisible por el ideal $\mathfrak{a}$, entonces existirá un ideal $\mathfrak{b}$, y uno solo, que satisface la condición $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$.— Si el producto $\mathfrak{a}\mathfrak{b}$ es divisible por el producto $\mathfrak{a}\mathfrak{b}'$, entonces $\mathfrak{b}$ será divisible por $\mathfrak{b}'$; y de $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{b}'$ se seguirá que $\mathfrak{b} = \mathfrak{b}'$.

Demostración.— Elijamos el ideal $\mathfrak{m}$ de tal modo que $\mathfrak{a}\mathfrak{m}$ sea un ideal principal $\mathfrak{o}\mu$; si ahora $\mathfrak{c}$ es divisible por $\mathfrak{a}$, y por consiguiente $\mathfrak{c}\mathfrak{m}$ es divisible por $\mathfrak{a}\mathfrak{m}$ (§22, 2.º), entonces se podrá (§19) poner $\mathfrak{c}\mathfrak{m} = \mu\mathfrak{b}$, siendo $\mathfrak{b}$ un ideal. Multiplicando por $\mathfrak{a}$, obtenemos que $\mu\mathfrak{c} = \mu\mathfrak{a}\mathfrak{b}$, de donde $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$.— Sean ahora $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{b}'$ ideales cualesquiera, y supongamos que $\mathfrak{a}\mathfrak{b}$ sea divisible por $\mathfrak{a}\mathfrak{b}'$; entonces también resultará, multiplicando por $\mathfrak{m}$ (§22, 2.º), que $\mu\mathfrak{b}$ es divisible por $\mu\mathfrak{b}'$, y por lo tanto (§19) que $\mathfrak{b}$ es divisible por $\mathfrak{b}'$. Si, además, se tiene que $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{b}'$, entonces cada uno de los dos ideales $\mathfrak{b}$, $\mathfrak{b}'$ deberá ser divisible por el otro, es decir que se tendrá que $\mathfrak{b} = \mathfrak{b}'$.

Q.E.D.

7.ª La norma de un producto de ideales es igual al producto de las normas de los factores; $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$.

Demostración.— Consideremos en primer lugar el caso de un producto $\mathfrak{a} = \mathfrak{p}\mathfrak{a}'$, en el que el factor $\mathfrak{p}$ es un ideal primo. Como $\mathfrak{a}$ es divisible por $\mathfrak{p}$, existirá (según 3.ª) un número η divisible por $\mathfrak{a}'$, pero no por $\mathfrak{a}$, y $\eta\mathfrak{p}$ será el mínimo común múltiplo de $\mathfrak{a}$ y de $\mathfrak{o}\eta$; luego se tendrá (§20) $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{p})\mathrm{N}(\mathfrak{d})$, siendo $\mathfrak{d}$ el máximo común divisor de los mismos ideales $\mathfrak{a}$ y $\mathfrak{o}\eta$. Como $\mathfrak{a}$ y $\mathfrak{o}\eta$ son divisibles por $\mathfrak{a}'$, $\mathfrak{d}$ deberá ser también divisible por $\mathfrak{a}'$ (§1, 4.º) y por consiguiente existe (según 6.ª) un ideal $\mathfrak{n}$ que satisface la condición $\mathfrak{n}\mathfrak{a}' = \mathfrak{d}$. Además, siendo $\mathfrak{a}$ divisible por $\mathfrak{d}$, y consiguientemente $\mathfrak{p}\mathfrak{a}'$ por $\mathfrak{n}\mathfrak{a}'$, el ideal primo $\mathfrak{p}$ deberá (según 6.ª) ser divisible por $\mathfrak{n}$, y se deberá, por consiguiente, tener que $\mathfrak{n} = \mathfrak{p}$ o $= \mathfrak{o}$. La primera igualdad es imposible, ya que de lo contrario se tendría $\mathfrak{d} = \mathfrak{p}\mathfrak{a}' = \mathfrak{a}$, y por consiguiente η sería divisible por $\mathfrak{a}$, lo cual no tiene lugar; se tendrá pues que $\mathfrak{n} = \mathfrak{o}$, de donde $\mathfrak{d} = \mathfrak{a}'$, y también $\mathrm{N}(\mathfrak{p}\mathfrak{a}') = \mathrm{N}(\mathfrak{p})\mathrm{N}(\mathfrak{a}')$, lo cual demuestra el teorema para el caso considerado.

---

[40] Ver las *Vorlesungen über Zahlentheorie* de Dirichlet, §8.

Pero de ahí se concluye inmediatamente el teorema general. Porque siendo (según 4.ª) todo ideal (distinto de $\mathfrak{o}$) de la forma

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_m,$$

donde $\mathfrak{p}_1$, $\mathfrak{p}_2$, …, $\mathfrak{p}_m$ son ideales primos, resulta que

$$\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{p}_1)\mathrm{N}(\mathfrak{p}_2\mathfrak{p}_3 \dots \mathfrak{p}_m) = \mathrm{N}(\mathfrak{p}_1)\mathrm{N}(\mathfrak{p}_2)\mathrm{N}(\mathfrak{p}_3 \dots \mathfrak{p}_m) = \dots,$$

y por consiguiente también que

$$\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{p}_1)\mathrm{N}(\mathfrak{p}_2) \dots \mathrm{N}(\mathfrak{p}_m);$$

si se tiene además que

$$\mathfrak{b} = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_r,$$

donde $\mathfrak{q}_1$, $\mathfrak{q}_2$, …, $\mathfrak{q}_r$ también designan ideales primos, entonces obtendremos que

$$\mathfrak{a}\mathfrak{b} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_m\mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_r,$$

y por consiguiente que

$$\mathrm{N}(\mathfrak{b}) = \mathrm{N}(\mathfrak{q}_1)\mathrm{N}(\mathfrak{q}_2) \dots \mathrm{N}(\mathfrak{q}_r),$$

$$\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{p}_1) \dots \mathrm{N}(\mathfrak{p}_m)\mathrm{N}(\mathfrak{q}_1) \dots \mathrm{N}(\mathfrak{q}_r);$$

se tiene por consiguiente también que

$$\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}).$$

Q.E.D.

8.ª Un ideal $\mathfrak{a}$ (o un número α) es siempre, y solamente entonces, divisible por un ideal $\mathfrak{d}$ (o un número δ), cuando todas las potencias de los ideales primos que dividen a $\mathfrak{d}$ (o δ) dividen también a $\mathfrak{a}$ (o α).

Demostración.— Si $\mathfrak{p}$ es un ideal primo, y $\mathfrak{p}^m$ un divisor de un ideal $\mathfrak{d}$, entonces se tiene (según 6.ª) que $\mathfrak{d} = \mathfrak{d}_1\mathfrak{p}^m$, donde $\mathfrak{d}_1$ designa un ideal; si se supone a este último descompuesto en todos sus factores primos, entonces $\mathfrak{d}$ se encontrará también bajo la forma de un producto de ideales todos primos, y de entre éstos el factor $\mathfrak{p}$ ocurrirá al menos m veces; recíprocamente, si, en la descomposición de $\mathfrak{d}$ en factores primos, el ideal primo $\mathfrak{p}$ ocurre al menos m veces como factor, entonces $\mathfrak{d}$ será evidentemente divisible por $\mathfrak{p}^m$. Si se supone, pues, que toda potencia de un ideal primo que divide a $\mathfrak{d}$ divide también a un ideal $\mathfrak{a}$, eso quiere decir que todos los factores primos que ocurren en la descomposición de $\mathfrak{d}$ ocurren también, al menos tantas veces, como factores en la descomposición de $\mathfrak{a}$; entre los factores de $\mathfrak{a}$ se encuentran pues en primer lugar todos los factores de $\mathfrak{d}$, y, si se designa el producto de los otros factores de $\mathfrak{a}$ por $\mathfrak{d}'$, entonces se tendrá que $\mathfrak{a} = \mathfrak{d}\mathfrak{d}'$, y por consiguiente $\mathfrak{a}$ es divisible por $\mathfrak{d}$. La proposición recíproca, que si $\mathfrak{d}$ es un divisor de $\mathfrak{a}$, entonces toda potencia de un ideal primo que divida a $\mathfrak{d}$ divide también a $\mathfrak{a}$, se verifica por sí sola.

Q.E.D.

Si se reúnen bajo la forma de potencia todos los factores primos de un ideal $\mathfrak{a}$ que son iguales entre sí, se encuentra que

$$\mathfrak{a} = \mathfrak{p}^a\mathfrak{q}^b\mathfrak{r}^c \dots,$$

siendo $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$, ... ideales primos diferentes entre sí, y en virtud de los teoremas que acabamos de demostrar, todos los divisores $\mathfrak{d}$ de $\mathfrak{a}$ están comprendidos en la fórmula

$$\mathfrak{d} = \mathfrak{p}^{a'}\mathfrak{q}^{b'}\mathfrak{r}^{c'}\ldots,$$

donde los exponentes a', b', c', ... satisfacen las condiciones

$$0 \leq a' \leq a, \quad 0 \leq b' \leq b, \quad 0 \leq c' \leq c, \ldots;$$

como a dos combinaciones diferentes cualesquiera de los exponentes a', b', c', ... corresponden (según 4.ª) ideales $\mathfrak{d}$ diferentes, entonces el número total de los divisores diferentes será $= (a+1)(b+1)(c+1)\ldots$.

9.ª Si $\mathfrak{d}$ es el máximo común divisor de los dos ideales $\mathfrak{a}$, $\mathfrak{b}$, entonces se tendrá

$$\mathfrak{a} = \mathfrak{d}\mathfrak{a}', \mathfrak{b} = \mathfrak{d}\mathfrak{b}',$$

donde $\mathfrak{a}'$ y $\mathfrak{b}'$ designan dos ideales primos entre sí, y el mínimo común múltiplo $\mathfrak{m}$ de $\mathfrak{a}$, $\mathfrak{b}$ será $= \mathfrak{d}\mathfrak{a}'\mathfrak{b}' = \mathfrak{a}\mathfrak{b}' = \mathfrak{b}\mathfrak{a}'$. Además, si $\mathfrak{a}\mathfrak{e}$ es divisible por $\mathfrak{b}$, entonces $\mathfrak{e}$ será divisible por $\mathfrak{b}'$.

Dejaremos al lector la tarea de buscar la demostración de esta proposición y las reglas que sirven para deducir los ideales $\mathfrak{m}$, $\mathfrak{d}$ de las descomposiciones de $\mathfrak{a}$, $\mathfrak{b}$ en factores primos.

§26.– *Congruencias.*

Después de haber establecido las leyes de la divisibilidad de los ideales y, por consiguiente, también de los *números* contenidos en $\mathfrak{o}$, vamos a añadir también algunas consideraciones sobre las congruencias, importantes para la teoría de los ideales; no obstante nos contentaremos, por el momento, con dar simples indicaciones sobre las demostraciones.

1.ª Siendo $\mathfrak{o}$ el máximo común divisor de dos ideales cualesquiera $\mathfrak{a}$, $\mathfrak{b}$, *primos entre sí*, y siendo $\mathfrak{a}\mathfrak{b}$ su mínimo común múltiplo, entonces (§2, 5.º) el sistema de las dos congruencias

$$\omega \equiv \rho \pmod{\mathfrak{a}}, \quad \omega \equiv \sigma \pmod{\mathfrak{b}},$$

siendo ρ, σ dos números dados contenidos en $\mathfrak{o}$, tendrá siempre raíces ω, y todas estas raíces estarán comprendidas bajo la forma

$$\omega \equiv \tau \pmod{\mathfrak{a}\mathfrak{b}},$$

siendo τ el representante de una clase de números con respecto a $\mathfrak{a}\mathfrak{b}$, la cual está completamente determinada por los dos números ρ y σ, o por las clases que les corresponden con respecto a $\mathfrak{a}$, $\mathfrak{b}$. Recíprocamente, toda clase τ (mód $\mathfrak{a}\mathfrak{b}$) se determinará de esta manera por medio de una combinación, y de una sola, ρ (mód $\mathfrak{a}$), σ (mód $\mathfrak{b}$).

Diremos ahora que el número ρ es *primo con* el ideal $\mathfrak{a}$, cuando $\mathfrak{o}\rho$ y $\mathfrak{a}$ sean ideales primos entre sí, y designaremos por $\psi(\mathfrak{a})$ el número de todos los números incongruentes según $\mathfrak{a}$ que son números primos con $\mathfrak{a}$. Se obtiene fácilmente de ahí, para dos ideales primos entre sí $\mathfrak{a}$, $\mathfrak{b}$, el teorema

$$\psi(\mathfrak{a}\mathfrak{b}) = \psi(\mathfrak{a})\psi(\mathfrak{b});$$

pues τ es siempre, y solamente entonces, un número primo con $\mathfrak{a}\mathfrak{b}$, cuando ρ es un número primo con $\mathfrak{a}$, y σ un número primo con $\mathfrak{b}$. No se tiene, pues, la necesidad de determinar la función $\psi(\mathfrak{a})$ más que en el caso en que

$\mathfrak{a}$ es una potencia $\mathfrak{p}^m$ del ideal primo $\mathfrak{p}$. El número de todos los números incongruentes según $\mathfrak{p}^m$ es, en el caso de que $m > 0$, igual a

$$\mathrm{N}(\mathfrak{p}^m) = [\mathrm{N}(\mathfrak{p})]^m = (\mathfrak{o}, \mathfrak{p}^m) = (\mathfrak{o}, \mathfrak{p})(\mathfrak{p}, \mathfrak{p}^m) = (\mathfrak{p}, \mathfrak{p}^m)\mathrm{N}(\mathfrak{p});$$

es necesario restarle el número de todos los números que no son primos con $\mathfrak{p}^m$ y que, por consiguiente, son divisibles por $\mathfrak{p}$; siendo este número igual a

$$(\mathfrak{p}, \mathfrak{p}^m) = [\mathrm{N}(\mathfrak{p})]^{m-1},$$

obtenemos que

$$\psi(\mathfrak{p}^m) = [\mathrm{N}(\mathfrak{p})]^m - [\mathrm{N}(\mathfrak{p})]^{m-1} = \mathrm{N}(\mathfrak{p}^m)\left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})}\right),$$

de donde se obtendrá inmediatamente, en virtud del teorema precedente, que

$$\psi(\mathfrak{a}) = \mathrm{N}(\mathfrak{a}) \prod \left(1 - \tfrac{1}{\mathrm{N}(\mathfrak{p})}\right),$$

donde el signo de multiplicación $\prod$ se refiere a todos los ideales primos $\mathfrak{p}$, diferentes entre sí, que dividen al ideal $\mathfrak{a}$. Como se tiene, además, que

$$\psi(\mathfrak{o}) = 1,$$

se concluye también, exactamente igual que en la teoría de los números racionales([41]), el teorema

$$\sum \psi(\mathfrak{a}') = \mathrm{N}(\mathfrak{a}),$$

donde el signo sumatorio es relativo a todos los ideales $\mathfrak{a}'$ divisores de $\mathfrak{a}$.

2.ª Si $\mathfrak{d}$ es el máximo común divisor de los ideales $\mathfrak{a}$ y $\mathfrak{o}\eta$, se tendrá que $\mathfrak{a} = \mathfrak{d}\mathfrak{a}'$, y $\eta\mathfrak{a}'$ será (§25, 9.ª) el mínimo común múltiplo de $\mathfrak{a}$ y de $\mathfrak{o}\eta$, es decir que $\mathfrak{a}'$ será el divisor de $\mathfrak{a}$ correspondiente al número η (§19); recíprocamente, si $\eta\mathfrak{a}'$ es el mínimo común múltiplo de $\mathfrak{a}$ y $\mathfrak{o}\eta$, entonces se tendrá que $\mathfrak{a} = \mathfrak{d}\mathfrak{a}'$, siendo $\mathfrak{d}$ el máximo común divisor de $\mathfrak{a}$ y de $\mathfrak{o}\eta$. Está claro también que los factores complementarios $\mathfrak{d}$ y $\mathfrak{a}'$ del ideal $\mathfrak{a}$ siguen siendo los mismos para todos los números η congruentes entre sí según $\mathfrak{a}$; se dará también lo mismo, evidentemente, si se reemplaza η por un número $\eta' \equiv \eta\omega$ (mód $\mathfrak{a}$), donde ω designa un número primo con $\mathfrak{a}'$; y recíprocamente, si el máximo común divisor $\mathfrak{d}$ de $\mathfrak{a}$, $\mathfrak{o}\eta$ es al mismo tiempo el de $\mathfrak{a}$, $\mathfrak{o}\eta'$; entonces resulta que

$$\eta' \equiv \eta\omega, \quad \eta \equiv \eta'\omega' \pmod{\mathfrak{a}},$$

de donde se obtiene que

$$\eta\omega\omega' \equiv \eta \pmod{\mathfrak{a}}, \quad \omega\omega' \equiv 1 \pmod{\mathfrak{a}'},$$

y por consiguiente ω es un número primo con $\mathfrak{a}'$. Luego el número de todos los números η incongruentes según $\mathfrak{a}$, a los cuales corresponde el mismo divisor $\mathfrak{a}'$ de $\mathfrak{a}$, es $= \psi(\mathfrak{a}')$. Pero es necesario poner cuidado en que aquí se ha supuesto la existencia de al menos un tal número η; luego, dado un divisor cualquiera $\mathfrak{a}'$ del ideal $\mathfrak{a}$, todo lo que podemos afirmar hasta aquí es que el número $\chi(\mathfrak{a}')$ de todos los números η incongruentes según $\mathfrak{a}$, a los cuales corresponde el mismo divisor $\mathfrak{a}'$, será igual a $\psi(\mathfrak{a}')$ o a cero. Para decidir esta alternativa, consideremos *todos* los números incongruentes según $\mathfrak{a}$, que son

[41] *Ver* Dirichlet, *Vorlesungen über Zahlentheorie*, §14.

$\mathrm{N}(\mathfrak{a})$ en número, y ordenémoslos, según los divisores $\mathfrak{a}'$ que les corresponden, en grupos respectivos de $\chi(\mathfrak{a}')$ números; entonces se deberá tener que

$$\sum \chi(\mathfrak{a}') = \mathrm{N}(\mathfrak{a}),$$

extendiéndose la suma a todos los divisores $\mathfrak{a}'$ de $\mathfrak{a}$; ahora bien, como se tiene también (1º) que

$$\sum \psi(\mathfrak{a}') = \mathrm{N}(\mathfrak{a}),$$

se sigue inmediatamente que $\chi(\mathfrak{a}')$ no es jamás $= 0$, sino siempre $= \psi(\mathfrak{a}')$. De este modo queda demostrado este teorema muy importante:

"Si $\mathfrak{d}$ y $\mathfrak{a}'$ son dos ideales cualesquiera, entonces se podrá siempre, multiplicando $\mathfrak{d}$ por un ideal $\mathfrak{b}'$, primo con $\mathfrak{a}$, transformarlo en un ideal principal $\mathfrak{d}\mathfrak{b}' = \mathfrak{o}\eta$."

Porque, poniendo $\mathfrak{d}\mathfrak{a}' = \mathfrak{a}$, siempre existirá, ya que $\psi(\mathfrak{a}')$ es diferente de cero, un número η, al cual corresponderá el divisor $\mathfrak{a}'$ de $\mathfrak{a}$, de forma tal que $\mathfrak{d}$ será el máximo común divisor de $\mathfrak{a}$ y de $\mathfrak{o}\eta$; si se pone pues que $\mathfrak{o}\eta = \mathfrak{d}\mathfrak{b}'$, entonces $\mathfrak{b}'$ será un ideal primo con $\mathfrak{a}'$.

Q.E.D.

3.ª Como todo producto $\rho\rho'$ de números ρ, ρ' primos con un ideal $\mathfrak{a}$ es igualmente un número primo con $\mathfrak{a}$, y puesto que, cuando ρ permanece constante y ρ' varía, entonces $\rho\rho'$ recorre un sistema de $\psi(\mathfrak{a})$ números incongruentes (mód $\mathfrak{a}$), se deduce por el método conocido([42]), para cada valor del número ρ, la congruencia

$$\rho^{\psi(\mathfrak{a})} \equiv 1 \pmod{\mathfrak{a}},$$

que encierra la máxima generalización de un célebre teorema de Fermat. Para un ideal primo $\mathfrak{p}$, se concluye fácilmente que *todo* número ω del dominio $\mathfrak{o}$ satisface la congruencia

$$\omega^{\mathrm{N}(\mathfrak{p})} \equiv \omega \pmod{\mathfrak{p}},$$

es decir la congruencia

$$\omega^{p^f} \equiv \omega \pmod{\mathfrak{p}},$$

siendo p el número primo racional positivo divisible por $\mathfrak{p}$, y f el grado del ideal primo $\mathfrak{p}$ (§21, 3.º). Este teorema tiene la misma importancia para la teoría del dominio $\mathfrak{o}$ que el teorema de Fermat para la teoría de los números racionales, y es esto lo que vamos al menos a tratar de hacer ver con las siguientes observaciones, no permitiéndonos la falta de espacio desarrollar más la teoría general.

Si los coeficientes de la función racional entera $F(x)$, de grado m, están incluidos en $\mathfrak{o}$, y el coeficiente del término de grado máximo no es divisible por el ideal primo $\mathfrak{p}$, entonces se deduce, por el razonamiento conocido ([43]), que la congruencia $F(\omega) \equiv 0$ (mód $\mathfrak{p}$) no puede tener más de m raíces incongruentes entre ellas, y esta proposición, combinada con el teorema precedente, conduce a una teoría completa de la congruencias binomiales según el módulo $\mathfrak{p}$; se deduce, entre otras, la existencia de *raíces primitivas* del ideal primo $\mathfrak{p}$, entendiendo al respecto números γ tales que sus potencias

$$1, \gamma, \gamma^2, \ldots, \gamma^{\mathrm{N}(\mathfrak{p})-2}$$

[42] *Ver* Dirichlet, *Vorlesungen über Zahlentheorie*, §19.

[43] *Ver* Dirichlet, *Vorlesungen über Zahlentheorie*, §26.

sean todas incongruentes entre ellas. En general, la teoría de las congruencias de grado superior con coeficientes racionales puede aplicarse completamente a las funciones $F(x)$ cuyos coeficientes son números del dominio $\mathfrak{o}$.

No obstante, se puede ya constatar también una dependencia íntima entre la teoría de los ideales y la teoría de las congruencias de grado superior, restringida al caso de los coeficientes *racionales*, cuyo establecimiento se debe a los trabajos de Gauss, de Galois, de Schönemann, de Serret([44]). Estando todos los ideales compuestos por ideales primos, y dividiendo cada ideal primo $\mathfrak{p}$ a un número racional primo determinado p, se obtendrá una visión completa de todos los ideales del dominio $\mathfrak{o}$, descomponiendo todos los ideales de la forma $\mathfrak{o}p$ en sus factores primos. La teoría de las congruencias proporciona para eso un procedimiento suficiente en un gran número de casos. Sea, en efecto, θ un número entero del cuerpo Ω, y

$$\Delta(1, \theta, \theta^2, \ldots, \theta^{n-1}) = k^2 \Delta(\Omega);$$

entonces *si p no es un un divisor de k*, se reconocerá de la manera siguiente la descomposición de $\mathfrak{o}p$ en ideales primos. Si $f(t)$ es la función entera [[polinomio]] de grado n en la variable t que se anula para $t = \theta$, se podrá poner

$$f(t) \equiv P_1(t)^{a_1} P_2(t)^{a_2} \ldots P_e(t)^{a_e} \pmod{p},$$

siendo $P_1(t)$, $P_2(t)$, $\ldots$, $P_e(t)$ funciones primas [[polinomios irreducibles]], diferentes entre ellas, de grados respectivos f_1, f_2, $\ldots$, f_e, y entonces se tiene ciertamente que

$$\mathfrak{o}p = \mathfrak{p}_1^{a_1} \mathfrak{p}_2^{a_2} \ldots \mathfrak{p}_e^{a_e},$$

siendo $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\ldots$, $\mathfrak{p}_e$ ideales primos, diferentes entre sí, de grados respectivos f_1, f_2, $\ldots$, f_e. Se obtiene de ahí fácilmente este teorema extremadamente importante:

"El número primo racional p divide siempre, y solamente entonces, al número fundamental $\Delta(\Omega)$ del cuerpo Ω, cuando p es divisible por el cuadrado de un ideal primo."

Este teorema es también verdadero, aunque bastante más difícil de demostrar, cuando los números k, que corresponden a todos los números θ posibles, son todos divisibles por p; tales casos se encuentran de hecho([45]), y ésa es una de las razones que me han determinado a fundamentar la teoría de los ideales no sobre la de las congruencias de grado superior, sino sobre principios enteramente nuevos que son al mismo tiempo mucho más simples, y que responden mejor a la verdadera naturaleza del asunto.

§27.– *Ejemplos tomados de la división del círculo.*

Mediante la teoría general de los ideales, cuyas bases he desarrollado en lo que precede, los fenómenos de la divisibilidad de los números para todo dominio $\mathfrak{o}$, compuesto por todos los números enteros de un cuerpo finito Ω, han sido reconducidos a las mismas leyes fijas que reinan en la antigua teoría de los números racionales. Si se piensa en la variedad infinita de estos cuerpos Ω, de los que cada uno posee su teoría de números especial, el espíritu del

[44] *Ver* mi Memoria: *Abriss einer Theorie der höheren Congruenzen in Bezug auf einen reellen Primzahl-Modulus. (Journal de Crelle)*, t. 54.

[45] Ver las *Göttingische gelehrte Anzeigen* del 20 de Septiembre de 1871, p. 1490.

geómetra tendrá motivos, sin duda alguna, para estar satisfecho constatando la unidad o la identidad de las leyes generales a las cuales estas diversas teorías obedecen sin excepción. Pero no es solamente un interés estético o puramente teórico, sino también un interés que no puede ser más práctico el que está ligado a esta constatación; pues la certidumbre de que estas leyes generales existen realmente facilita en el grado máximo la demostración y el descubrimiento de los fenómenos especiales que se presentan en un cuerpo determinado Ω. El establecimiento de esta verdad en toda su extensión exigiría, ciertamente, que se llevara mucho mas lejos el desarrollo de la teoría general de los ideales de lo que podemos hacer aquí, y que se la combinara en particular con los principios algebraicos de Galois; pero trataré al menos de mostrar, con el ejemplo simple a propósito del cual Kummer introdujo por primera vez sus números ideales, que ya los primeros elementos de la teoría general, expuestos en lo que precede, conducen al objetivo con la máxima facilidad.

Sea m un *número primo* racional positivo, y Ω el cuerpo de grado n-simo, que resulta, de la manera indicada con anterioridad (§15), a partir de una raíz primitiva θ de la ecuación $\theta^m = 1$, es decir de una raíz de la ecuación

$$f(\theta) = \theta^{m-1} + \theta^{m-2} + \ldots + \theta^2 + \theta^1 + 1 = 0;$$

al ser los coeficientes racionales, se tendrá siempre que $n \leq m-1$. Como, además, θ, θ^2, $\ldots$, θ^{m-1} son todas las raíces de esta ecuación, se tendrá, designando por t una variable, que

$$f(t) = \frac{t^m - 1}{t-1} = (t-\theta)(t-\theta^2)\ldots(t-\theta^{m-1}),$$

y, por consiguiente, que

$$m = (1-\theta)(1-\theta^2)\ldots(1-\theta^{m-1}).$$

Los $m-1$ factores del segundo miembro son números enteros y asociados entre sí; pues, si r designa uno de los números 1, 2, $\ldots$, $m-1$, entonces

$$\frac{1-\theta^r}{1-\theta} = 1 + \theta + \theta^2 + \ldots + \theta^{r-1}$$

será un número entero, y si s es positivo y elegido de manera que se tenga que $rs \equiv 1$ (mód m), entonces

$$\frac{1-\theta}{1-\theta^r} = \frac{1-\theta^{rs}}{1-\theta^r} = 1 + \theta^r + \theta^{2r} + \ldots + \theta^{(s-1)r}$$

será también un número entero: Estableciendo pues, para abreviar, que

$$1 - \theta = \mu,$$

obtenemos que

$$m = \varepsilon \mu^{m-1},$$

donde ε designa una unidad del cuerpo Ω, y por consiguiente, formando la norma, que

$$m^n = [\mathrm{N}(\mu)]^{m-1}.$$

Ahora bien, siendo m un número primo, $\mathrm{N}(\mu)$ deberá ser una potencia de m; si se pone $\mathrm{N}(\mu) = m^e$, entonces resulta que $n = e(m-1)$, y puesto que, como ha sido observado con anterioridad, n es siempre $\leq m-1$, se concluye que $e = 1$, y $n = m-1 = \varphi(m)$. La ecuación precedente $f(\theta) = 0$ es pues

irreducible; los números θ, θ^2, $\ldots\theta^{m-1}$ son conjugados, y a estos números les corresponden $m-1$ permutaciones, por las cuales el cuerpo normal Ω se transforma en sí mismo; se tiene al mismo tiempo que

$$\mathrm{N}(\mu) = m, \quad \mathfrak{o}m = \mathfrak{o}\mu^{m-1}.$$

El ideal principal $\mathfrak{o}\mu$ es un *ideal primo*; si se tuviera, en efecto, que $\mathfrak{o}\mu = \mathfrak{a}\mathfrak{b}$, siendo $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales diferentes de $\mathfrak{o}$, entonces se seguiría que $m = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$, y puesto que m es un número primo, sería necesario que se tuviera, por ejemplo, $\mathrm{N}(\mathfrak{a}) = m$, $\mathrm{N}(\mathfrak{b}) = 1$, de donde $\mathfrak{b} = \mathfrak{o}$, lo cual es contrario a la hipótesis. Al mismo tiempo (§21, 3.º), m es el mínimo número racional divisible por μ; los números $0, 1, 2, \ldots, m-1$ constituyen un sistema completo de números incongruentes según el módulo μ. De ahí resulta también que un número de la forma

$$\omega = k_0 + k_1\mu + k_2\mu^2 + \ldots + k_{m-2}\mu^{m-2},$$

donde k_0, k_1, k_2, $\ldots$, k_{m-2} designan números enteros, no es divisible por m, ni consecuentemente por μ^{m-1}, más que si todos los números k_0, k_1, k_2, $\ldots$, k_{m-2} son divisibles por m; pues, ya que ω debe ser también divisible por μ, es necesario que k_0 sea divisible por μ, y por lo tanto también por m; es necesario a continuación que $\omega - k_0$ sea divisible por m, y por lo tanto también por μ^2, de donde se concluye del mismo modo que k_1 debe ser divisible por μ, y por lo tanto también por m; y, continuando de este modo, se deduce que los otros números k_2, k_3, $\ldots$, k_{m-2} son divisibles por m.

Con la ayuda de este resultado, es fácil demostrar que que los $m-1$ números 1, θ, θ^2, $\ldots$, θ^{m-2} constituyen una base del dominio de todos los números enteros del cuerpo Ω. Puesto que se tiene que

$$t^m - 1 = (t-1)f(t), \quad m\theta^{m-1} = (\theta - 1)f'(\theta),$$

resulta, excluyendo el caso poco interesante en el que $m = 2$, que

$$\mathrm{N}(f'(\theta)) = m^{m-2},$$

debido a que $\mathrm{N}(\theta) = 1$ y $\mathrm{N}(\theta - 1) = m$, y se sigue de ahí (§17) que

$$\Delta(1, \theta, \theta^2, \ldots, \theta^{m-2}) = (-1)^{\frac{m-1}{2}} m^{m-2}.$$

Como, además, $\mu = 1 - \theta$, $\theta = 1 - \mu$, está claro que los dos módulos $[1, \theta, \ldots, \theta^{m-2})]$, $[1, \mu, \ldots, \mu^{m-2})]$ son idénticos, de donde resulta [§4, 3.º, y §17, (5)] que se tiene también que

$$\Delta(1, \mu, \mu^2, \ldots, \mu^{m-2}) = (-1)^{\frac{m-1}{2}} m^{m-2}.$$

Puesto que los números 1, μ, μ^2, $\ldots$, μ^{m-2} son independientes entre sí, todo número del cuerpo Ω puede ahora ponerse bajo la forma

$$\frac{k_0 + k_1\mu + k_2\mu^2 + \ldots + k_{m-2}\mu^{m-2}}{k} = \frac{\omega}{k},$$

donde k, k_0, k_1, k_2, $\ldots$, k_{m-2} designan números enteros *sin ningún divisor común*; para que este número sea entero, es decir, para que ω sea divisible por k, será necesario (§18) que k^2 divida al discriminante de la base 1, μ, μ^2, $\ldots$, μ^{m-2}, y, por consiguiente, k no podrá contener más factores primos que el número m; como, además, ha sido demostrado con anterioridad que ω no

puede ser divisible por m más que si los números k_0, k_1, k_2, …, k_{m-2} son todos divisibles por m, k no podrá tampoco ser divisible por m; será pues necesario que se tenga que $k = \pm 1$; luego todos los números enteros del cuerpo son de la forma

$$\omega = k_0 + k_1\mu + k_2\mu^2 + \ldots + k_{m-2}\mu^{m-2},$$

y, por consiguiente, se tendrá que

$$\mathfrak{o} = [1, \mu, \ldots, \mu^{m-2}] = [1, \theta, \ldots, \theta^{m-2}],$$

o también, debido a que $1 + \theta + \theta^2 + \ldots + \theta^{m-2} + \theta^{m-1} = 0$, que

$$\mathfrak{o} = [\theta, \theta^2, \ldots, \theta^{m-1})], \quad \Delta(\Omega) = (-1)^{\frac{m-1}{2}} m^{m-2}.$$

Sea ahora $\mathfrak{p}$ un ideal primo cualquiera, diferente de $\mathfrak{o}\mu$; entonces el número primo racional positivo p, divisible por $\mathfrak{p}$, será diferente de m, y se tendrá que

$$\mathrm{N}(\mathfrak{p}) = p^f,$$

donde f designa el grado del ideal primo $\mathfrak{p}$. Dos potencias θ^r, θ^s no son congruentes relativamente a un tal ideal primo $\mathfrak{p}$ más que si son iguales entre sí, es decir si se tiene que $r \equiv s \pmod{m}$; pues, en el caso contrario, se tiene que $\theta^r - \theta^s = \theta^r(1 - \theta^{r-s}) = \varepsilon\mu$, donde ε designa una unidad, y, por consiguiente, θ^r no podrá ser $\equiv \theta^s \pmod{\mathfrak{p}}$. Como se tiene ahora (§26, 3.ª) que

$$\theta^{\mathrm{N}(\mathfrak{p})} \equiv \theta \pmod{\mathfrak{p}},$$

resulta que

$$p^f \equiv 1 \pmod{m}.$$

Sea a el divisor de $\varphi(m) = m - 1$ al cual *pertenece* el número p con respecto al módulo m, es decir, sea a el mínimo exponente positivo para el cual se tiene que

$$p^a \equiv 1 \pmod{m};$$

entonces f deberá ser, como es sabido, divisible por a, y por lo tanto se tendrá que $f \geq a$. Ahora bien, siendo todos los números enteros del cuerpo Ω de la forma

$$\omega = F(\theta) = x_1\theta + x_2\theta^2 + \ldots + x_{m-1}\theta^{m-1},$$

donde x_1, x_2, …, x_{m-1} representan números racionales enteros, resulta de teoremas conocidos, verdaderos para todo número primo p, que se tiene

$$\omega^p \equiv F(\theta^p), \quad \omega^{p^r} \equiv F(\theta^{p^r}) \pmod{p},$$

y, como consecuencia, que

$$\omega^{p^a} \equiv \omega \pmod{p}.$$

Se concluye de ahí en primer lugar que el ideal $\mathfrak{o}p$ es un producto de ideales primos todos *diferentes entre sí*; pues, si se tuviera que $\mathfrak{o}p = \mathfrak{p}^2\mathfrak{q}$, entonces existiría un número ω divisible por $\mathfrak{p}\mathfrak{q}$, pero no divisible por p, y ω^2, y como consecuencia también ω^{p^a} serían por lo tanto divisibles por $\mathfrak{p}^2\mathfrak{q}^2 = p\mathfrak{p}$, luego también por p, lo cual entra en contradicción con la congruencia precedente. Como, además, p es divisible por $\mathfrak{p}$, entonces *todo* número entero ω del cuerpo Ω satisface por consiguiente la congruencia

$$\omega^{p^a} \equiv \omega \pmod{\mathfrak{p}};$$

el número de sus raíces incongruentes ω es, pues, $= \mathrm{N}(\mathfrak{p}) = p^f$, y como su grado es $= p^a$, es necesario que p^f sea $\leq p^a$, y por lo tanto $f \leq a$; pero ya ha sido demostrado con anterioridad que f es $\geq a$; por consiguiente $f = a$. Se llega de este modo al resultado siguiente, que constituye el teorema principal de la teoría de Kummer([46]):

"Si el número primo p, diferente de m, pertenece, con respecto al módulo m, al exponente f, que es siempre un divisor de $\varphi(m) = ef$, entonces se tiene que

$$\mathfrak{o}p = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_e,$$

siendo $\mathfrak{p}_1$, $\mathfrak{p}_2$,..., $\mathfrak{p}_e$ ideales primos, diferentes entre sí, de grado f."

Todo el resto se deduce fácilmente. Se puede tratar de una manera totalmente semejante el caso general, en el que m es un número compuesto cualquiera. El grado del cuerpo normal Ω es siempre igual al número $\varphi(m)$ de aquéllos de los números 1, 2, 3, ..., m que son primos con m; la ley precedente no experimenta ningún cambio, y la determinación de los ideales primos que dividen a m no presenta tampoco ninguna dificultad.

Según investigaciones muy generales, que publicaré próximamente, se pueden, siendo conocidos los ideales de un cuerpo normal Ω, indicar inmediatamente también los ideales de un *divisor* cualquiera de Ω, es decir de un cuerpo cualquiera H, cuyos números estén todos contenidos en Ω. Según esto, se conocerán, por ejemplo, los ideales de *todos* los cuerpos H que resultan de la división del círculo, y, para dar una idea más precisa del alcance de estas investigaciones, me permitiré señalar el caso siguiente.

Sea además m un número primo, de donde $\varphi(m) = m - 1$, y sea e un divisor cualquiera de $m - 1 = ef$; entonces en la teoría de los números racionales, la congruencia

$$h^f \equiv 1 \pmod{m}$$

tendrá precisamente f raíces h incongruentes entre ellas, que serán estables bajo la multiplicación, y que, en este sentido, formarán un *grupo*. Si θ es también una raíz primitiva de la ecuación $\theta^m = 1$, y Ω el cuerpo correspondiente de grado $m - 1$, entonces todos los números $F(\theta)$ contenidos en este cuerpo y que satisfacen las condiciones $F(\theta) = F(\theta^h)$ formarán un cuerpo H de grado e, y los e *periodos*([47]) conjugados η_1, η_2, ..., η_e, formados cada uno por f términos, y de los que uno es

$$\eta = \sum \theta^h,$$

formarán una base del dominio $\mathfrak{e}$ compuesto por todos los números enteros contenidos en H. Con la ayuda de las investigaciones generales de las que acabo de hablar (o también, inmediatamente, por conclusiones semejantes a aquéllas que se han extraido anteriormente para el caso en que $e = m-1$), se obtiene ahora la siguiente determinación de los ideales primos pertenecientes a este divisor H del cuerpo normal Ω. Si se pone

$$\rho = \prod(1 - \theta^h),$$

[46] Las investigaciones de Kummer se encuentran en el *Journal de Crelle*, t. 35, en el *Journal de Liouville*, t. XVI; en las *Memorias de la Academia de Berlín* del año 1856.

[47] *Disquisitiones arithmeticae*, art. 343.

entonces ρ es un número entero del cuerpo H, m está asociado con ρ^e, y $\mathfrak{e}\rho$ es un ideal primo; si, además, p es un número primo racional diferente de m, y p^f pertenece al exponente f' con respecto a m, entonces f' será necesariamente un divisor de $e = e'f'$, y el ideal principal $\mathfrak{e}p$ será el producto de e' ideales primos, diferentes entre sí, de grado f'. En el caso en que $e = m-1$, $f = 1$, H es idéntico a Ω, y se obtiene también el resultado demostrado más arriba. Examinemos ahora con más cuidado el caso en que $e = 2$, $f = \frac{m-1}{2}$.

En este caso, los f números h son los restos cuadráticos de m; entonces designando por k el conjunto de los no-restos cuadráticos, los dos periodos conjugados

$$\eta = \sum \theta^h, \quad \eta' = \sum \theta^k$$

forman una base del dominio $\mathfrak{e}$ compuesto por todos los números enteros contenidos en el cuerpo cuadrático H, y, por consiguiente, su discriminante será

$$\Delta(H) = \begin{vmatrix} \eta & \eta' \\ \eta' & \eta \end{vmatrix}^2 = (\eta - \eta')^2,$$

por el motivo de que $\eta + \eta' = -1$; el número m está asociado con el cuadrado del número $\rho = \prod(1-\theta^h)$, y $\mathfrak{e}\rho$ es un ideal primo; además, $\mathfrak{e}p$ es el producto de dos ideales primos diferentes, de primer grado, o bien $\mathfrak{e}p$ es un ideal primo de segundo grado, según que se tenga

$$p^{\frac{m-1}{2}} \equiv +1 \text{ o } \equiv -1 \pmod{m},$$

es decir, usando la notación de Legendre, según que se tenga

$$\left(\frac{p}{m}\right) = +1 \text{ o } = -1.$$

Pero se pueden estudiar directamente todos los cuerpos cuadráticos, sin recurrir a la división del círculo, y ya hemos (§18) determinado el discriminante D' de un tal cuerpo H. Se puede deducir también muy fácilmente de D' los ideales primos([48]) pertenecientes al cuerpo H: si el número primo racional p divide a D', entonces el ideal principal $\mathfrak{e}p$ que le corresponde será el cuadrado de un ideal primo; pero, si p no divide a D', y p es impar, entonces $\mathfrak{e}p$ será el producto de dos ideales primos diferentes de primer grado, o bien un ideal primo de segundo grado, según que se tenga

$$\left(\frac{D'}{p}\right) = +1 \text{ o } = -1;$$

si, además, D' es impar y, por consiguiente, $\equiv 1 \pmod 4$, entonces $\mathfrak{e}(2)$ será el producto de dos ideales primos de primer grado, o bien un ideal primo de segundo grado, según que se tenga

$$D' \equiv 1 \text{ o } \equiv 5 \pmod 8.$$

Comparando estas leyes, verdaderas para todos los cuerpos cuadráticos, con el resultado deducido de la división del círculo para el cuerpo especial precedente H, se ve en primer lugar que D' debe ser divisible por m, pero no por ningún otro número primo, y, por consiguiente, que se debe tener (§18) que

$$\Delta(H) = D' = (-1)^{\frac{m-1}{2}} m;$$

[48] *Ver* Dirichlet, *Vorlesungen über Zahlentheorie*, §168.

de esta manera se deduce de principios enteramente generales, sin ningún cálculo, el resultado conocido

$$(\eta - \eta')^2 = (-1)^{\frac{m-1}{2}} m,$$

que se demuestra en la división del círculo mediante la formación efectiva del cuadrado de $\eta - \eta'$([49]). Prosiguiendo esta comparación, se es conducido también al teorema

$$\left(\frac{p}{m}\right) = \left(\frac{\pm m}{m}\right),$$

siendo $\pm 1 \equiv 1 \pmod 4$, y al teorema

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}.$$

Esta demostración de la ley de reciprocidad, por la cual se determina al mismo tiempo el carácter cuadrático del número -1, coincide, en el fondo, con la célebre sexta demostración de Gauss([50]), reproducida más tarde bajo las formas más diferentes por Jacobi, Eisenstein y otros, y haré observar expresamente que es meditando sobre el nervio de esta demostración y de las demostraciones análogas de la ley de reciprocidad cúbica y bicuadrática, como fui llevado a las investigaciones generales que he indicado con anterioridad y que publicaré próximamente.

Como último ejemplo, consideramos el caso en el que $m = 4$; entonces se tiene que $\theta = i = \sqrt{-1}$, y los números enteros del cuerpo cuadrático Ω son los números complejos enteros, introducidos por primera vez por Gauss, de la forma

$$\omega = x + yi,$$

donde x e y designan números racionales enteros (§6); el discriminante de este cuerpo es

$$\begin{vmatrix} 1 & i \\ 1 & -i \end{vmatrix}^2 = -4.$$

El número $2 = i(1-i)^2$ es un asociado del cuadrado del número primo $1 - i$. Si p es un número primo racional positivo impar, entonces se tiene que

$$i^p = (-1)^{\frac{p-1}{2}} i,$$

y, por consiguiente, que

$$\omega^p = (x + yi)^p \equiv x + (-1)^{\frac{p-1}{2}} yi \pmod p;$$

si se tiene ahora que $p \equiv 1 \pmod 4$, entonces todo número entero ω satisfará la congruencia

$$\omega^p \equiv \omega \pmod p,$$

de donde se sigue inmediatamente que $\mathfrak{o}p$ es el producto de dos ideales primos de primer grado diferentes; pero, si se tiene que $p \equiv 3 \pmod 4$, entonces se sigue que

$$\omega^p \equiv \omega', \quad \omega^{p^2} \equiv \omega \pmod p,$$

---

[49] *Disquisitiones arithmeticae*, art. 356.

[50] *Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae;* 1817.

donde ω' designa el número conjugado con ω, y se concluye fácilmente que $\mathfrak{o}p$ es un ideal primo de segundo grado. Ahora bien, todo ideal $\mathfrak{a}$ de este cuerpo debe ser un ideal principal; si, en efecto, α_0 es uno de los números del ideal $\mathfrak{a}$ cuyas normas tienen un valor positivo *mínimo*, entonces todo número α del ideal $\mathfrak{a}$ será divisible por α_0; pues se puede (§6) elegir el número entero ω de manera que se tenga

$$\mathrm{N}(\alpha - \omega\alpha_0) < \mathrm{N}(\alpha_0),$$

y como los números α, α_0 y, por consiguiente también, $\alpha - \omega\alpha_0$ pertenecen al ideal $\mathfrak{a}$, será necesario que se tenga $\mathrm{N}(\alpha - \omega\alpha_0) = 0$, de donde $\alpha = \omega\alpha_0$, y por consiguiente $\mathfrak{a} = \mathfrak{o}\alpha_0$.

Q.E.D.

Ahora, puesto que, en el caso en el que p es un número primo racional y $\equiv 1$ (mód 4), $\mathfrak{o}p$ es el producto de dos ideales primos de primer grado, resulta que se tiene

$$p = \mathrm{N}(\alpha_0) = \mathrm{N}(a + bi) = a^2 + b^2,$$

lo cual constituye el célebre teorema de Fermat.

§28.– *Clases de ideales.*

Volvamos ahora a la consideración de un cuerpo cualquiera Ω de grado n, para establecer la distribución de sus ideales en *clases*. Esta distribución se basa en principio sobre [la ley] el teorema (§25, 5.ª), de que todo ideal $\mathfrak{a}$ puede, por medio de la multiplicación por un ideal $\mathfrak{m}$, transformarse en un ideal principal, y sobre la siguiente definición: Dos ideales $\mathfrak{a}$, $\mathfrak{a}'$ se dirán *equivalentes*, cuando, por medio de la multiplicación por un sólo y mismo ideal $\mathfrak{m}$, puedan transformarse en ideales principales $\mathfrak{am} = \mathfrak{o}\mu$, $\mathfrak{a}'\mathfrak{m} = \mathfrak{o}\mu'$. Entonces se tiene evidentemente que $\mu'\mathfrak{a} = \mu\mathfrak{a}'$; y recíprocamente, si existen dos números η, η' diferentes de cero, que satisfacen la condición $\eta'\mathfrak{a} = \eta\mathfrak{a}'$, entonces los ideales $\mathfrak{a}$, $\mathfrak{a}'$ serán ciertamente equivalentes; pues si, multiplicando $\mathfrak{a}$ por $\mathfrak{m}$, se le transforma en un ideal principal $\mathfrak{am} = \mathfrak{o}\mu$, entonces se sigue que $\mathfrak{o}\mu\eta' = \eta'\mathfrak{am} = \eta\mathfrak{a}'\mathfrak{m}$, luego $\mu\eta'$ es divisible por η, de donde $\mu\eta' = \mu'\eta$, $\mathfrak{o}\mu'\eta = \eta\mathfrak{a}'\mathfrak{m}$, y por lo tanto $\mathfrak{a}'\mathfrak{m} = \mathfrak{o}\mu'$.

Q.E.D.

Si dos ideales $\mathfrak{a}'$, $\mathfrak{a}''$ son equivalentes a un tercero $\mathfrak{a}$, entonces $\mathfrak{a}'$, $\mathfrak{a}''$ serán también equivalentes entre sí; pues, según la hipótesis, existen cuatro números μ, μ', η, η'', que satisfacen las condiciones $\mu'\mathfrak{a} = \mu\mathfrak{a}'$, $\eta''\mathfrak{a} = \eta\mathfrak{a}''$, y se tiene, por consiguiente, que $(\eta''\mu)\mathfrak{a}' = (\mu'\eta)\mathfrak{a}''$.

Q.E.D.

De ahí resulta la distribución de todos los ideales en clases: si $\mathfrak{a}$ es un ideal determinado, entonces el sistema A de todos los ideales $\mathfrak{a}$, $\mathfrak{a}'$, $\mathfrak{a}''$, ... equivalentes a $\mathfrak{a}$ se llamará una *clase de ideales*, y $\mathfrak{a}$ se denominará el *representante* de esta clase A. Dos ideales cualesquiera contenidos en A serán equivalentes, y en el lugar de $\mathfrak{a}$ se podrá siempre escoger como representante cualquier otro ideal $\mathfrak{a}'$ contenido en A.

Está claro que el sistema de todos los ideales principales constituye él mismo una clase; pues cada uno de ellos se transforma en sí mismo cuando

se le multiplica por el ideal $\mathfrak{o}$, y, por consiguiente, son equivalentes; y si un ideal $\mathfrak{a}$ es equivalente a un ideal principal, y por lo tanto también a $\mathfrak{o}$, entonces $\mathfrak{a}$ deberá ser él mismo un ideal principal; pues existen dos números μ, μ', que satisfacen la condición $\mu'\mathfrak{a} = \mathfrak{o}\mu$, y de ahí resulta además que μ es divisible por μ', de donde $\mu = \mu'\mu''$, y consiguientemente $\mathfrak{a} = \mathfrak{o}\mu''$. Luego la clase representada por $\mathfrak{o}$ contiene a todos los ideales principales y no contiene a ningún otro ideal. Llamaremos a esta clase la *clase principal*, y la designaremos por O.

Si ahora $\mathfrak{a}$ representa sucesivamente a todos los ideales de la clase A, y del mismo modo $\mathfrak{b}$ a todos los de la clase B, entonces todos los productos $\mathfrak{ab}$ pertenecerán a una sola y misma clase K; pues si $\mathfrak{a}'$, $\mathfrak{a}''$ están contenidos en A, y $\mathfrak{b}'$, $\mathfrak{b}''$ en B, entonces existen cuatro números α', α'', β', β'' que satisfacen las condiciones $\alpha''\mathfrak{a}' = \alpha'\mathfrak{a}''$, $\beta''\mathfrak{b}' = \beta'\mathfrak{b}''$, y de ahí se sigue que $(\alpha''\beta'')(\mathfrak{a}'\mathfrak{b}') = (\alpha'\beta')(\mathfrak{a}''\mathfrak{b}'')$, es decir que $\mathfrak{a}'\mathfrak{b}'$ y $\mathfrak{a}''\mathfrak{b}''$ son ideales equivalentes. Designaremos a esta clase K, a la cual pertenecen todos los productos $\mathfrak{ab}$, como AB, y la llamaremos el *producto* de A por B, o la clase *compuesta* de A y de B. Se tiene evidentemente que $AB = BA$, y de la igualdad $\mathfrak{a}(\mathfrak{bc}) = (\mathfrak{ab})\mathfrak{c}$ resulta, para tres clases cualesquiera A, B, C, el teorema $(AB)C = A(BC)$. Se pueden, pues, aplicar aquí los mismos razonamientos que para la multiplicación de los números o de los ideales, y demostrar que, en la composición de un número cualquiera de clases A_1, A_2, $\ldots$, A_m, el orden de las multiplicaciones sucesivas, que reúnen cada vez dos clases en su producto, no tiene ninguna influencia sobre el resultado final, que se puede designar simplemente por $A_1A_2 \ldots A_m$. Si los ideales $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\ldots$, $\mathfrak{a}_m$ son representantes de las clases A_1, A_2, $\ldots$, A_m, entonces el ideal $\mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_m$ será un representante de la clase $A_1A_2 \ldots A_m$. Si los m factores son todos $= A$, entonces su producto se denominará la m-sima potencia de A, y lo designaremos por A^m; pondremos, además, $A^1 = A$ y $A^0 = O$. Los dos siguientes casos son particularmente importantes:

De la igualdad $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$ resulta el teorema, verdadero para una clase cualquiera A, $OA = A$.

Puesto que, además, todo ideal $\mathfrak{a}$ puede, por medio de la multiplicación por un ideal $\mathfrak{m}$, ser transformado en un ideal principal $\mathfrak{am}$, existirá para cada clase A una clase correspondiente M, que satisface la condición $AM = O$, y existirá una sola; pues si la clase N satisface también la condición $AN = O$, entonces resultará que

$$N = NO = N(AM) = M(AN) = MO = M.$$

Esta clase M se llamará la clase *opuesta* o la clase *inversa* de A, y la designaremos por A^{-1}; está claro que, recíprocamente, A será la clase inversa de A^{-1}. Si se define, además, A^{-m} como siendo la clase inversa de A^m, entonces se tendrán, para cualesquiera exponentes racionales enteros r, s, los teoremas

$$A^rA^s = A^{r+s},\ (A^r)^s = A^{rs},\ (AB)^r = A^rB^r.$$

Por último, es evidente que de $AB = AC$ se concluirá, multiplicando por A^{-1}, que se tiene siempre que $B = C$.

§29.– *El número de las clases de ideales.*

Tomando a discreción n números enteros $\omega_1, \omega_2, \ldots, \omega_n$, que formen una base del cuerpo Ω, todo número

$$\omega = h_1\omega_1 + h_2\omega_2 + \ldots + h_n\omega_n$$

con coordenadas racionales enteras $h_1, h_2, \ldots, h_n$, será igualmente un número entero del mismo cuerpo. Si se atribuyen a las coordenadas todos los valores enteros que, tomados en valor absoluto, no excedan de un valor positivo determinado k, entonces es evidente que los valores absolutos de los números correspondientes ω, si son reales, o sus módulos analíticos, si son imaginarios, serán todos $\leq rk$, siendo r la suma de los valores absolutos o de los módulos de $\omega_1, \omega_2, \ldots, \omega_n$, y, por consiguiente, una constante totalmente independiente de k. Como, además, la norma $\mathrm{N}(\omega)$ es un producto de n números conjugados ω de la forma anterior, se tendrá al mismo tiempo que

$$\pm\mathrm{N}(\omega) \leq sk^n,$$

donde s designa igualmente una constante dependiente únicamente de la base. Se obtiene de ahí el teorema siguiente:

En toda clase de ideales M *existe al menos un ideal* $\mathfrak{m}$ *cuya norma no excede a la constante* s*.*

Demostración.— Tomemos a discreción un ideal $\mathfrak{a}$ de la clase inversa M^{-1}, y elijamos como k el número racional entero positivo determinado por las condiciones

$$k^n \leq \mathrm{N}(\mathfrak{a}) < (k+1)^n;$$

si se atribuyen ahora a cada una de las n coordenadas $h_1, h_2, \ldots, h_n$ cada uno de los $k+1$ valores 0, 1, 2,..., k, no se obtendrán más que números diferentes ω, y puesto que su número es $= (k+1)^n$, y, por consiguiente, $> \mathrm{N}(\mathfrak{a})$, existen necesariamente, entre estos números ω, dos números diferentes entre sí,

$$\beta = b_1\omega_1 + \ldots + b_n\omega_n,\ \gamma = c_1\omega_1 + \ldots + c_n\omega_n,$$

que son congruentes entre sí según $\mathfrak{a}$; por consiguiente, su diferencia

$$\alpha = (b_1 - c_1)\omega_1 + \ldots + (b_n - c_n)\omega_n$$

será un número diferente de cero y divisible por $\mathfrak{a}$. Ahora bien, estando incluidas las coordenadas b, c de los números β, γ en la sucesión 0, 1, 2,..., k, las coordenadas $b-c$ del número α, tomadas en valor absoluto, no exceden del valor k, y, por consiguiente, se tiene que

$$\pm\mathrm{N}(\alpha) \leq sk^n.$$

Pero, siendo α divisible por $\mathfrak{a}$, se tiene que $\mathfrak{o}\alpha = \mathfrak{a}\mathfrak{m}$, donde $\mathfrak{m}$ designa un ideal de la clase M, y, por consiguiente, que

$$\pm\mathrm{N}(\alpha) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{m}) \leq sk^n;$$

como se tiene, además, que $k^n \leq \mathrm{N}(\mathfrak{a})$, resulta que $\mathrm{N}(\mathfrak{m}) \leq s$.

Q.E.D.

Si se considera ahora que la norma m de un ideal $\mathfrak{m}$ es siempre divisible por $\mathfrak{m}$ (§20), entonces está claro que no puede existir más que un número finito de ideales $\mathfrak{m}$ que tengan una norma dada m, porque todo ideal, y por lo tanto también $\mathfrak{o}\mathfrak{m}$, es solamente divisible por un número finito de ideales (§25, 8.ª). Como, además, no hay más que un número finito de números

racionales enteros m que no exceden a una constante dada s, no puede haber más que un número finito de ideales $\mathfrak{m}$ que satisfagan la condición $\mathrm{N}(\mathfrak{m}) \leq s$, y de ahí resulta evidentemente este teorema fundamental:

El número de las clases de ideales del cuerpo Ω *es finito.*

La determinación *exacta* del número de las clases de ideales forma incontestablemente uno de los problemas más importantes, pero también de los más difíciles de la Teoría de números. Para los cuerpos cuadráticos, cuya teoría coincide esencialmente con la de las *formas* cuadráticas binarias, el problema ha sido, como es sabido, completamente resuelto por primera vez por Dirichlet([51]); esta solución, expresándolo todo con la terminología de la teoría de los *ideales*, reposa sobre el estudio de la función

$$\sum \frac{1}{\mathrm{N}(\mathfrak{a})^s} = \prod \frac{1}{1-\frac{1}{\mathrm{N}(\mathfrak{p})^s}}$$

para valores positivos infinitamente pequeños de la variable independiente $s-1$; la suma se extiende a todos los ideales $\mathfrak{a}$, el producto a todos los ideales primos $\mathfrak{p}$, y la identidad de las dos expresiones es una consecuencia inmediata de las leyes de la divisibilidad (§25). Con la ayuda de estos principios, el número de las clases de formas o de ideales ha sido, después, determinado por Eisenstein([52]) para un caso particular de los cuerpos de tercer grado, y por Kummer([53]) para los cuerpos de grado superior que provienen de la división del círculo. Los resultados de estas investigaciones excitan el más vivo interés por las asombrosas relaciones que ofrecen con el Análisis, el Álgebra y las otras partes de la Teoría de los números; de este modo, por ejemplo, el problema tratado por Kummer está muy estrechamente enlazado con la célebre demostración que ha sido dada por Dirichlet del teorema sobre la progresión aritmética, y que puede ser considerablemente simplificado con la ayuda de estas investigaciones. No se puede dudar de que prosiguiendo el estudio del problema general no quepa esperar realizar importantes progresos en estas ramas de las Matemáticas; pero aunque se haya tenido éxito en terminar de una manera general una parte de esta investigación para un cuerpo cualquiera Ω([54]), sin embargo se está todavía muy lejos de la solución completa, y habrá que limitarse por el momento limitarse a estudiar nuevos casos particulares.

§30.– *Conclusión.*

Vamos además a deducir algunas consecuencias interesantes del teorema fundamental que acabamos de demostrar. (Ver *Disquisitiones arithmeticae*, art. 305– 307.)

Sea h el número de todas las clase de ideales del cuerpo Ω, y A una clase determinada; entonces las $h+1$ potencias

$$O, A, A^2, \ldots, A^{h-1}, A^h$$

no podrán ser todas diferentes; se encontrarán, pues, ciertamente, en la sucesión 0, 1, 2, ..., h, dos exponentes diferentes r y $r+m > r$, para los

[51] *Journal de Crelle*, t. 19, 21.

[52] *Journal de Crelle*, t. 28.

[53] *Journal de Crelle*, t. 40; *Journal de Liouville,* t. XVI.

[54] Dirichlet, *Vorlesungen über Zahlentheorie*, §167.

cuales se tendrá que $A^{r+m} = A^r$, y, por consiguiente, que

$$A^m = O;$$

si, además, m es el *mínimo* exponente positivo que satisface la condición precedente, entonces es fácil ver que las m clases

$$O, A, A^2, \ldots, A^{m-1}$$

serán todas diferentes entre sí, y diremos que la clase A *pertenece* al exponente m; se tiene evidentemente que $A^{m-1} = A^{-1}$, y, con mayor generalidad, se tendrá que $A^r = A^s$ todas las veces, y solamente entonces, que r sea $\equiv s$ (mód m). Designando, además, por B a una clase cualquiera, las m clases

$$(B) \qquad B, BA, BA^2, \ldots, BA^{m-1}$$

serán también diferentes entre sí, y dos complejos de m clases cada uno, tales como el precedente (B) y el siguiente:

$$(C) \qquad C, CA, CA^2, \ldots, CA^{m-1},$$

serán o idénticos o enteramente diferentes; si se encuentra, en efecto, en las dos a la vez, una sola y la misma clase $BA^r = CA^s$, entonces se tendrá que $C = BA^{r-s}$, de donde se sigue inmediatamente que las m clases del sistema (C) coinciden completamente con las del complejo (B). Luego el sistema de todas las las h clases se compone de un número determinado g de tales complejos diferentes entre sí, y, como cada complejo contiene m clases diferentes, se tendrá que $h = mg$, es decir que el exponente m, al cual pertenece una clase A, es siempre un divisor del número de clases h. Luego, para toda clase A, se tiene el teorema

$$A^h = O.$$

Ahora, si $\mathfrak{a}$ es un ideal cualquiera de una clase cualquiera A, entonces $\mathfrak{a}^h$ pertenecerá a la clase A^h, y por consiguiente a la clase principal, es decir que la h-sima potencia de todo ideal es un ideal principal.

Con este teorema importante se llega a concebir la noción de *ideal* bajo un nuevo punto de vista, al cual se puede vincular al mismo tiempo una definición precisa de los *números ideales*. Sea $\mathfrak{a}$ un ideal cualquiera, y $\mathfrak{a}^h = \mathfrak{o}\alpha_1$; designando ahora por α un número cualquiera del ideal $\mathfrak{a}$, α^h estará contenido en $\mathfrak{a}^h$, y, por consiguiente, será divisible por el número α_1, y se sigue de ahí (§13, 2.ª) que α es divisible por el número entero $\mu = \sqrt[h]{\alpha_1}$, el cual no obstante no pertenece en general al cuerpo Ω. Pero, recíprocamente también, si α es un número entero perteneciente al cuerpo Ω y divisible por μ, entonces α^h será divisible por $\mu^h = \alpha_1$, y, por consiguiente, $(\mathfrak{o}\alpha)^h$ lo será por $\mathfrak{o}\alpha_1 = \mathfrak{a}^h$, y de ello se concluye fácilmente, según las leyes generales de la divisibilidad (§25), que $\mathfrak{o}\alpha$ es divisible por $\mathfrak{a}$, es decir que α es un número del ideal $\mathfrak{a}$. Luego el ideal $\mathfrak{a}$ *está compuesto* por todos los números enteros contenidos en Ω y divisibles por el número entero μ; por esta razón diremos que el número μ, aun cuando no esté contenido en Ω, es *un número ideal del cuerpo* Ω, y que *corresponde* al ideal $\mathfrak{a}$. O, un poco más generalmente, un número algebraico entero μ se denomina un número ideal del cuerpo Ω, cuando existe una potencia de μ, con exponente positivo entero r, que está asociado a un número *existente* η del cuerpo Ω, y al mismo tiempo existe un ideal $\mathfrak{a}$ del cuerpo Ω, que satisface la condición $\mathfrak{a}^r = \mathfrak{o}\eta$; este ideal

$\mathfrak{a}$ es el ideal correspondiente al número ideal μ, y es siempre, y solamente entonces, un ideal principal, cuando μ está asociado con un número existente del cuerpo Ω (*Ver* la Introducción y el §10.)

Acabaremos nuestras consideraciones con la demostración del teorema siguiente, anunciado ya anteriormente (§14):

Dos números algebraicos enteros cualesquiera α, β admiten un divisor común δ, que puede ser representado bajo la forma $\delta = \alpha\alpha' + \beta\beta'$, siendo α', β' igualmente números algebraicos enteros.

Demostración.— Admitamos que los dos números α, β sean diferentes de cero, puesto que en el caso contrario el teorema es evidente. Entonces existe siempre, como es fácil observar, un cuerpo finito Ω, que contiene a los dos números α, β, y sea además $\mathfrak{o}$ el dominio de todos los números enteros de este cuerpo, y además h el número de las clases de ideales. Pongamos ahora

$$\mathfrak{o}\alpha = \mathfrak{a}\mathfrak{d}, \quad \mathfrak{o}\beta = \mathfrak{b}\mathfrak{d}, \quad \mathfrak{d}^h = \mathfrak{o}\delta_1,$$

siendo $\mathfrak{d}$ el máximo común divisor de $\mathfrak{o}\alpha$, $\mathfrak{o}\beta$, y estando δ_1 contenido en $\mathfrak{o}$. Puesto que α^h, β^h son divisibles por $\mathfrak{d}^h$, se puede poner

$$\alpha^h = \alpha_1\delta_1, \quad \beta^h = \beta_1\delta_1, \quad \mathfrak{o}\alpha_1 = \mathfrak{a}^h, \quad \mathfrak{o}\beta_1 = \mathfrak{b}^h,$$

estando igualmente α_1, β_1 contenidos en $\mathfrak{o}$. Como, por otra parte, $\mathfrak{a}$ y $\mathfrak{b}$ son ideales primos entre sí, $\mathfrak{o}$ será también el máximo común divisor de $\mathfrak{o}\alpha_1$, $\mathfrak{o}\beta_1$, y, como el número 1 está contenido en $\mathfrak{o}$, habrá en $\mathfrak{o}$ dos números, α_2, β_2 que satisfacen la condición

$$\alpha_1\alpha_2 + \beta_1\beta_2 = 1, \quad \text{o} \quad \alpha^h\alpha_2 + \beta^h\beta_2 = \delta_1.$$

Si ahora se pone

$$\delta_1 = \delta^h,$$

entonces el número entero δ será un divisor común de α y β, puesto que α^h, β^h son divisibles por δ_1, y por consiguiente se podrá poner, siendo $h \geq 1$, que

$$\alpha_2\alpha^{h-1} = \alpha'\delta^{h-1}, \quad \beta_2\beta^{h-1} = \beta'\delta^{h-1},$$

donde α' y β' designan números enteros que satisfacen la condición $\alpha\alpha' + \beta\beta' = \delta$.

Q.E.D.

Si uno al menos de los dos números α, β es diferente de cero, entonces el número δ, así como todo número que le esté asociado, merecerá el nombre de *máximo* común divisor de α, β. Si δ es una unidad, entonces α, β podrán denominarse *números primos entre sí*, y dos números tales gozan de la propiedad característica de que todo número μ divisible por α y por β lo es también por el producto $\alpha\beta$; pues de las igualdades $\mu = \alpha\alpha'' = \beta\beta''$ y $1 = \alpha\alpha' + \beta\beta'$ se obtiene que

$$\mu = \alpha\beta(\alpha'\beta'' + \beta'\alpha''),$$

y la conclusión recíproca está igualmente permitida, cuando α, β son los dos diferentes de cero.

LA EXTENSIÓN DEL CONCEPTO DE NÚMERO BASÁNDOSE EN LA SUCESIÓN DE LOS NÚMEROS NATURALES;

POR EL
Sr. R. DEDEKIND.

Traducción provisional y comentarios por J. Bares y J. Climent.

La introducción del cero y de los números negativos.

En el §11 de mi escrito aparecido en el 1888 bajo el título de: *Was sind und was sollen die Zahlen?*— que será designado posteriormente por Z — se ha tratado la adición de los números naturales de manera que su substracción se halle inmediatamente fundamentada. Si α_1 y α_2 son números naturales, y si $\alpha_1 < \alpha_2$, entonces existe un único número natural n que satisface la condición $(Z, 146)$:

$$n + \alpha_1 = \alpha_2. \tag{0.1}$$

Se dice que este número n es la *diferencia* de los números α_1 y α_2, designada por $\alpha_2 - \alpha_1$ de manera tal que 0.1 pueda representarse igualmente por:

$$n = \alpha_2 - \alpha_1 \tag{0.2}$$

siendo el número α_1 el *substraendo*, y α_2 el *minuendo* de esta diferencia. Pero si la condición $\alpha_1 < \alpha_2$ *no* se cumple; luego como consecuencia de (Z,92) que $\alpha_1 \geq \alpha_2$, entonces no existe ningún número n que cumpla (Z,142) la condición 0.1; la escritura $\alpha_2 - \alpha_1$ no tiene hasta ahí ningún sentido. Si no obstante debiera adquirir el significado de un número, entonces sería necesario proceder a una extensión del concepto de número.

Para preparar una tal introducción de números nuevos, y asentarla sobre un fundamento claro y cierto, consideremos todos los *pares de números* α_1, α_2 donde $\alpha_1 < \alpha_2$ que tienen la misma diferencia $n = \alpha_2 - \alpha_1$. Llamemos congruentes a tales pares de números. Para abreviar, designemos un par de números α_1, α_2 cualquiera (que se debe distinguir del par de números α_2, α_1) mediante una sola letra α debiendo entonces significar la congruencia

$$\alpha \equiv \beta \tag{0.3}$$

la coincidencia de los pares de números, consistente en el hecho de que:

$$\alpha_2 - \alpha_1 = \beta_2 - \beta_1, \tag{0.4}$$

luego en la existencia de un número n que cumple al mismo tiempo las condiciones:

$$n + \alpha_1 = \alpha_2 \quad \text{y} \quad n + \beta_1 = \beta_2. \tag{0.5}$$

De ahí se *sigue* (Z,140) que:

$$(n + \alpha_1) + \beta_2 = (n + \beta_1) + \alpha_2, \tag{0.6}$$

luego (Z,141) igualmente que:

$$n + (\alpha_1 + \beta_2) = n + (\beta_1 + \alpha_2), \tag{0.7}$$

y por consiguiente (Z,140, 145) que:

$$\alpha_1 + \beta_2 = \beta_1 + \alpha_2. \tag{0.8}$$

Inversamente, si los pares de números α_1, α_2; β_1, β_2 cumplen la condición 0.8, y si además se tiene también que $\alpha_1 < \alpha_2$, entonces se sigue también, como se puede fácilmente establecer, que $\beta_1 < \beta_2$, y que la condición 0.4 se cumple.

Aun cuando la coincidencia representada bajo la forma de 0.4 entre los pares α y β sólo tiene sentido si $\alpha_1 < \alpha_2$ y $\beta_1 < \beta_2$, la relación entre α y β resultante y que está representada en la forma 0.8 puede ser sometida a un examen que permita decir si tiene lugar o no tiene lugar en el caso en el que estas limitaciones no tengan lugar. Podemos y queremos, por consiguiente, extender el concepto de congruencia 0.3 entre los pares de números α, β de tal manera que tenga el mismo significado que la condición 0.8 sea cual sea la naturaleza de los números α_1, α_2, β_1, β_2.

Es entonces de golpe evidente que la congruencia de dos pares de números α, β es, incluso después de esta extensión, siempre simétrica y recíproca, i.e., que si $\alpha \equiv \beta$ entonces $\beta \equiv \alpha$; además, se tiene siempre que $\alpha \equiv \alpha$; por último, de $\alpha \equiv \beta$ y $\beta \equiv \gamma$ se sigue siempre que $\alpha \equiv \gamma$.

Pues si se tiene que:

$$\alpha_1 + \beta_2 = \beta_1 + \alpha_2$$

y también:

$$\beta_1 + \gamma_2 = \gamma_1 + \beta_2$$

entonces resulta que:

$$(\alpha_1 + \beta_2) + (\beta_1 + \gamma_2) = (\beta_1 + \alpha_2) + (\gamma_1 + \beta_2)$$

o, lo que es equivalente según las leyes de la adición (Z,11)

$$(\beta_1 + \beta_2) + (\alpha_1 + \gamma_2) = (\beta_1 + \beta_2) + (\gamma_1 + \alpha_2)$$

y que (Z,145) igualmente:

$$\alpha_1 + \gamma_2 = \gamma_1 + \alpha_2,$$

Q.E.D.

Se sigue de ahí que todos los pares de números posibles pueden ser repartidos según que sean congruentes o incongruentes en *clases*. Si β es un par de números cualquiera, se debe designar por (β) la clase (el sistema, la totalidad, el conjunto) de los pares de números que le son congruentes. En virtud de la proposición justamente demostrada, dos pares de números α, γ contenidos en (β) son congruentes entre sí, y por lo tanto (α) = (β) = (γ), i.e., las clases son idénticas. Todo par contenido en una clase puede ser exhibido como su representante; dos clases son o bien perfectamente idénticas, o bien no tienen ningún par de números que les pertenezca en común.

Llamemos $\mathcal{P}$ al sistema de todas estas clases de números (α), y propongámonos la tarea de adquirir una idea general sobre este sistema, i.e., sobre todos los elementos distintos (α) que contiene. Si α es un representante elegido de manera determinada de una clase (α) y si $\alpha_1 < \alpha_2$, entonces hay un único número n que cumple la condición $n + \alpha_1 = \alpha_2$; si β pertenece a la misma clase, entonces se tiene igualmente, de acuerdo con la observación hecha con anterioridad, que $n + \beta_1 = \beta_2$; inversamente, si m designa un

número arbitrariamente elegido, entonces el par de números μ constituido por los números $\mu_1 = m$ y $\mu_2 = n + m$ pertenece a la misma clase (α). Si m recorre todos los números, entonces μ recorre igualmente todos los pares de números contenidos en la clase. Luego la clase (α) queda completamente caracterizada dando un *número* m. Tales clases se llaman *positivas*; a toda clase de este género le corresponde un número determinado, e, inversamente, a todo número le corresponde una única clase *positiva*. Se puede llamar al número n el carácter de las clases positivas. El sistema de las clases positivas (α) y el sistema N de los números naturales n (Z,32) son por consiguiente semejantes.

Una vez establecida la aplicación semejante del sistema de las clases positivas y del sistema N de los enteros naturales de modo que este quede completamente agotado, ya no es posible extender esta aplicación hasta una aplicación semejante del sistema $\mathcal{P}$ de todas las clases (α) en N. Esta es la razón que impulsa a la *extensión del concepto de número* mediante la *creación de nuevos números*

¿QUÉ SON Y PARA QUÉ SIRVEN LOS NÚMEROS?

POR EL

Sr. R. DEDEKIND

Primera edición, 1888. Sexta edición, 1930.

Traducción provisional y comentarios por J. Bares y J. Climent.

᾽Αεί ὁ ἄνθρωπος αριθμετίζει
El hombre calcula siempre

A mi hermana
Julia
y a mi hermano
Adolfo
Doctor en Derecho
juez del juzgado de Brunswick
dedicado con afecto cariñoso [cordial]

Prólogo a la primera edición

Lo que se puede demostrar, no debe en la ciencia ser creído sin demostración. A pesar de que este requisito parece tan evidente, no puede considerarse como cumplido, a lo que creo, en la fundamentación misma de la ciencia más simple, a saber, en aquella parte de la lógica que trata de la doctrina de los números, incluso según las representaciones más recientes[55]. En tanto que yo llamo a la aritmética (álgebra, análisis) sólo una parte de la lógica, declaro ya, que tengo el concepto de número por completamente independiente de la representaciones o intuiciones del espacio y el tiempo, y que lo tengo más bien por una emisión [emanación] inmediata [directa] de las puras leyes del pensamiento. Mi respuesta principal a la pregunta formulada en el título de este escrito es: los números son creaciones libres del espíritu humano, sirven como un medio para concebir con más facilidad y precisión la diferencia [diversidad] de las cosas. A través de la edificación [construcción] puramente lógica de la ciencia de los números y del dominio [reino] numérico continuo ganado [conquistado] en [con] ella, estamos por primera vez puestos en situación de investigar con precisión nuestras representaciones de espacio y tiempo, en tanto que las relacionamos con este dominio [reino] creado [engendrado] en nuestro espíritu[56]. Si se sigue con precisión [Observando atentamente] lo que hacemos al contar un conjunto o una cantidad de cosas, se llega a la consideración de la capacidad del [que

[55]De los escritos que me son conocidos menciono el meritorio *Manual de aritmética y álgebra* de E. Schröder (Leipzig 1873), en el que se encuentra también un índice bibliográfico, y además los trabajos de Kronecker y Helmholtz sobre el *Concepto de número*, y sobre *Contar y medir* (En el colectivo de artículos dedicado a E. Zeller, Leipzig, 1887). La aparición de estos trabajos es la ocasión que me ha movido a presentar ahora también mi concepción, en muchos respectos semejante, pero por su fundamentación, sin embargo, esencialmente diferente, la cual he construido desde hace muchos años y sin influencia alguna de ninguna parte.

[56]Cf. el §3 de mi escrito: *Continuidad y números irracionales* (Brunswick, 1872).

tiene el] espíritu de [relacionar cosas con cosas de] poner en correspondencia una cosa con otra cosa, o representar una cosa con otra cosa [o de hacer de una cosa la imagen de otra], facultad sin la cual no es posible ningún pensamiento en absoluto. Sobre este único, aunque también completamente imprescindible fundamento debe edificarse toda la ciencia de los números, según mi punto de vista, como también ya he expresado en un anticipo del presente escrito[57]. El propósito de una tal representación la concebí ya antes de la edición de mi escrito sobre la continuidad, pero sólo después de la aparición de éste, y con muchas interrupciones, ocasionadas por ocupaciones profesionales y otros trabajos necesarios, escribí un primer esbozo en los años 1872 a 1878 en unas pocas páginas, que luego han examinado y en parte [parcialmente] discutido conmigo varios matemáticos. Lleva el mismo título y contiene, aunque no ordenados de la mejor manera, no obstante todos los pensamientos fundamentales y esenciales de mi actual escrito, que proporciona sólo su exposición cuidadosa [meticulosa]; como tales puntos fundamentales menciono aquí la distinción nítida de lo finito y lo infinito (64), el concepto de cantidad de cosas (161), la demostración de que el procedimiento demostrativo conocido con el nombre de inducción completa (o de la inferencia de n a $n + 1$) es realmente demostrativo [concluyente] (59, 60, 80), y que también la definición por inducción (o recursión) es [también] precisa y libre de contradicción.

Este escrito puede comprenderlo cualquiera que posea lo que se llama la sana comprensión humana. No se requieren para ello lo más mínimo conocimientos académicos de tipo filosófico ni matemático. Pero sé muy bien que algunos, en las configuraciones sombrías [en las formas fantasmagóricas (espectrales)] que les presento, apenas podrán reconocer sus números, que le han acompañado toda la vida como amigos fieles y de confianza; les horrorizará la larga serie [sucesión] de simples conclusiones [inferencias] que corresponde a la constitución de nuestra razón en escala [al desarrollo gradual de nuestro entendimiento], la partición [descomposición] tediosa [austera] de las series [sucesiones] de pensamientos [ideas] en las que se basan las leyes de los números, y le impacientará tener que [deber] seguir [buscar] demostraciones para llegar a verdades [de verdades] que se le presentan luminosas y conocidas [evidentes y ciertas] de antemano en su pretendida intuición interna [en virtud de lo que suponen que sea su intuición interna]. Entreveo, por el contrario precisamente en la posibilidad de reconducir estas verdades a otras más simples, por más que la serie [sucesión] de las conclusiones [inferencias] pueda ser tan larga y artificiosa en apariencia [aparentemente artificial], una prueba convincente de que su posesión o la creencia en ella nunca se ha dado de manera inmediata a través de la intuición interna, sino que únicamente se alcanza a través de una repetición más o menos completa de las conclusiones [inferencias] singulares [separadas]. Quisiera comparar esta actividad del pensamiento difícil de seguir a causa de la rapidez de su realización con la que ejerce un lector completamente experimentado al leer. También esta lectura es siempre una repetición más o menos completa de los pasos singulares, que el principiante tiene que realizar con el penoso deletreo;

[57] *Lecciones sobre teoría de los números de Dirichlet*, tercera edición, 1879, §163, nota a la pág. 470.

una parte muy pequeña de los mismos, y por eso un trabajo o esfuerzo del espíritu muy pequeño, es suficiente para que el lector experimentado reconozca la palabra correcta y verdadera, desde luego sólo con una muy grande probabilidad; pues como es sabido le sucede también al más experimentado corrector, que de cuando en cuando se le escape una falta de impresión, es decir, leer mal, lo que sería imposible, si se hubiera repetido completamente la cadena de pensamientos que corresponde al deletrear. Así estamos abocados desde nuestro nacimiento, continuamente [constantemente], y siempre en una medida [y de manera] creciente, a relacionar unas cosas con otras, y a ejercer por ello aquella capacidad del espíritu en la que se basa la creación de los números; a través de este ejercicio constante [continuo], e incluso sin propósito [involuntario], que sucede ya en nuestros primeros años de vida, y la formación de juicios y series [sucesiones] de conclusiones [inferencias] vinculada con él, alcanzamos [adquirimos] también un tesoro de verdades estrictamente [propiamente] aritméticas, a las que se refieren después nuestros primeros profesores como a algo simple, evidente, dado en la intuición interna, y así sucede que varios conceptos, en rigor muy complejos (como p. ej. el de una cantidad de cosas) se tengan falsamente por simples. En este sentido, que yo señalo con las palabras de una conocida máxima, Ἀεί ὁ ἄνθρωπος ἀριθμετίζει[58], podrían encontrar benévola acogida las siguientes páginas como un intento de edificar la ciencia de los números sobre un fundamento unitario, y podrían animar a otros matemáticos a reconducir las largas series de conclusiones a una medida más modesta y más agradable. De acuerdo con el fin [objetivo] de este escrito me limito a la consideración de la sucesión de los llamados números naturales. En qué medida luego [De qué manera se debe proceder a continuación a] la extensión paulatina del concepto de número, la creación del cero, de los números negativos, fraccionarios, irracionales y complejos siempre ha de construirse retrotrayéndose [retrotrayéndolos sistemáticamente] a los conceptos anteriormente establecidos, y por cierto sin mezcla alguna de representaciones extrañas (como p. ej. la de magnitudes medibles), que según mi concepción sólo pueden alcanzar una claridad completa por medio de la ciencia de los números, esto lo he señalado [mostrado], al menos en el ejemplo de los números irracionales, en mi escrito anterior sobre la continuidad (1872); de un modo completamente semejante [análogo] pueden tratarse fácilmente las otras extensiones, como he expresado ya en el mismo lugar (§3), y me reservo dedicar [preparo para consagrar] a este objeto [a este asunto] una exposición [presentación] correspondiente [sistemática]. Ya en esta exposición [Dentro de esta concepción precisamente] aparece como algo evidente y en modo alguno novedoso, que todos los teoremas del álgebra y del análisis superior, aún los que quedan más alejados, pueden enunciarse como teoremas acerca de los números naturales, una afirmación que he oído repetidamente de la boca de Dirichlet. Pero no veo en modo alguno nada útil en –y es algo que era también completamente ajeno a Dirichlet– emprender realmente ese penoso rodeo y no querer utilizar ni reconocer ningún otro número que los naturales. Por el contrario, los progresos más grandes y más fructíferos en las matemáticas

[58]El hombre calcula siempre.

y en las demás ciencias han sido hechos principalmente a través de la creación e introducción de nuevos conceptos, después que ha llevado a ello la frecuente reiteración de fenómenos complejos, que sólo podía ser dominada con esfuerzo por los antiguos conceptos. Sobre este tema hube de mantener [tuve que pronunciar] una exposición [conferencia][59] en la Facultad de Filosofía en el verano de 1854 con ocasión de mi habilitación como *privatdozent* en Göttingen, cuyo asunto fue también avalado por Gauss; pero no es aquí el lugar de entrar más en esto.

En lugar de ello, aprovecho la ocasión para añadir aún algunas observaciones, que se refieren a mi escrito anterior más arriba mencionado sobre la continuidad y los números irracionales. La teoría de los números irracionales allí expuesta, concebida en el otoño de 1858 se basa en el fenómeno que aparece en el dominio de los números racionales (§4), que he denominado con el nombre de cortadura, y que he investigado por primera vez con precisión, y culmina en la demostración de la continuidad del nuevo dominio de los números reales (§5. IV). Ésta me parece algo más simple, quisiera decir más discreta [segura], que las dos teorías diferentes de ésta y entre sí, que han sido expuestas por los señores Weierstrass y G. Cantor, y que en todo caso son completamente rigurosas. Ha sido tomada [adoptada] luego sin cambio fundamental por el señor U. Dini en los *Fundamentos para la teoría de las funciones de variable real* (Pisa, 1878), pero la circunstancia de que mi nombre sea mencionado en el curso de esa exposición, no en la descripción del puro fenómeno aritmético de la cortadura, sino ocasionalmente [por hazar] justo allí donde se trata de la existencia de una magnitud medible correspondiente a la cortadura, podría llevar fácilmente a la presunción de que mi teoría se apoya en la consideración de tales magnitudes. Nada podría ser más incorrecto [falso]; es más, he introducido en el §3 de mi escrito diferentes motivos por los que rechazo por completo la intromisión de las magnitudes medibles, y por cierto, al final, con respecto a su existencia he señalado, que para una gran parte de la ciencia del espacio la continuidad de sus configuraciones [figuras] no es en modo alguno un presupuesto [condición] necesario[a], aparte por completo [sin hablar del hecho] de que ella es [especialmente mencionada de pasada] mencionada de nombre en las obras de geometría, pero nunca explicada [explicitada] claramente, y por lo tanto tampoco hecha accesible para pruebas [sin poder servir para las demostraciones]. Para explicar esto aún más de cerca [con más precisión], señalo por ejemplo lo siguiente. Se eligen tres puntos no colineales, A, B, C, arbitrariamente, con la única limitación [restricción] de que las relaciones entre sus distancias AB, AC, BC, sean números algebraicos, y se toman como dados [existentes] en el espacio sólo aquellos puntos M, para los cuales las relaciones de AM, BM, CM a AB son asimismo números algebraicos[60], así [entonces] el espacio sostenido desde este punto [constituido por estos puntos] es, como es fácil ver, completamente discontinuo; pero a pesar de la discontinuidad y la existencia de huecos de este espacio son en él, hasta

[59] "Über die Einführung neuer Functionen in der Mathematik", Gesammelte mathematische Werke, vol. 3, págs. 428 y sigs.

[60] Dirichlet, *Lecciones sobre teoría de los números*, §159 de la segunda edición, §160 de la tercera.

donde puedo ver, todas las construcciones que aparecen en los *Elementos* de Euclides, tan [exactamente] realizables como en un espacio completamente continuo; la discontinuidad de este espacio no habría sido por esto señalada ni encontrada en la ciencia de Euclides. Si alguien me dice, sin embargo, que no podríamos pensar el espacio de ninguna otra manera que continuo, yo quisiera dudarlo y llamar la atención sobre el hecho de que se requiere una muy avanzada y fina formación científica para concebir que fuera de las relaciones de magnitudes racionales también son pensables las irracionales, que fuera de las algebraicas también son pensables las trascendentes. Tanto más hermoso me parece que el hombre, sin ninguna representación de la magnitudes medibles, y ciertamente a través de un sistema finito de pasos [etapas] de pensamientos simples pueda elevarse a la creación de la región [del reino] de los números puros y continuos; y a partir de esta ayuda le será posible, a mi manera de ver, construir una representación clara del espacio continuo.

La misma teoría de los números irracionales fundada en el fenómeno de la cortadura se encuentra representada en la *Introduction à la théorie des fonctions d'une variable* de J. Tannery (París, 1886). Si yo comprendo correctamente un pasaje del prólogo de esta obra, entonces el autor ha pensado [concebido] esta teoría por sí mismo [de manera independiente], por consiguiente, en un tiempo [una época], en que le eran desconocidos, no sólo mi escrito, sino también los *Fondamenti* de Dini mencionados en el mismo prólogo. Esta coincidencia me parece una prueba satisfactoria de que mi concepción de la naturaleza de los números corresponde a la cosa, lo que también ha sido reconocido por otros matemáticos, p. ej., el señor M. Pasch en su *Introducción al cálculo diferencial e integral* (Leipzig, 1883). Por el contrario, no puedo estar de acuerdo sin más con el señor Tannery, cuando él denomina a esta teoría el desarrollo de un pensamiento proveniente del señor J. Bertrand, que estaría contenida en su *Traité d'arithmétique* y que consistiría en esto, definir un número irracional a través de la indicación de todos los números racionales que son más pequeños, y todos aquellos que son más grandes, que el número que hay que definir. Sobre esta sentencia, que es repetida, al parecer, sin ulterior prueba, por el señor O. Stolz en el prólogo a la segunda parte de sus *Lecciones sobre aritmética general*, me permito señalar lo siguiente. Que un número irracional pueda ser visto como completamente determinado por la indicación descrita, esta convicción ha sido sin duda también siempre un patrimonio común de todos los matemáticos que se han ocupado del concepto de lo irracional; todo calculador que calcula una raíz irracional de una ecuación por aproximación, tiene presente precisamente este tipo de su determinación; y si se concibe, como hace exclusivamente el señor Bertrand en su obra (tengo ante mí la octava edición del año 1885), el número irracional como la relación de magnitudes medibles, entonces este tipo determinación está ya expresada del modo más claro en la famosa definición que Euclides (*Elementos* V.5) expone para la igualdad de razones. Incluso esta antigua convicción es ahora sin duda la fuente de mi teoría como de la del intento del señor Bertrand y algunos otros, más o menos acabados, de fundamentar la introducción de los números irracionales en la aritmética. Pero si se está de acuerdo hasta aquí por completo con el

señor Tannery, debe entonces mostrarse, a pesar de todo, a través de una prueba real, que la representación del señor Bertrand, en la que el fenómeno de la cortadura en su pureza lógica no es mencionado ni una sola vez, no tiene con la mía ninguna semejanza en absoluto, en tanto que ella asume inmediatamente el recurso a la existencia de una magnitud medible, lo cual yo rechazo por completo por los motivos mencionados más arriba, y aparte de esta circunstancia, me parece que esta exposición presenta también huecos tan esenciales en las siguientes definiciones y pruebas fundadas en este presupuesto, que tengo por justificada la afirmación expresada en mi escrito (§6) de que la proposición $\sqrt{2}.\sqrt{3} = \sqrt{6}$ no habría sido nunca estrictamente probada, también a la vista de esta en todos los demás aspectos excelente obra, que yo entonces aún no conocía.

Harzburg, 5 de octubre de 1887. R. Dedekind.

Prólogo a la segunda edición

El presente escrito ha encontrado [suscitado] poco después de su aparición junto a juicios [críticas] favorables también desfavorables, [y] es verdad que se le han atribuido [reprochado] graves faltas. No he podido convencerme de la corrección de estos reproches y hago ahora [re]imprimir sin ningún cambio [ninguna modificación] el escrito agotado desde hace poco, para cuya defensa pública me falta tiempo, en tanto que sólo añado las siguientes observaciones al primer prólogo. La propiedad que he usado como definición (64) del sistema infinito ha sido puesta de relieve, ya antes de la aparición de mi escrito, por G. Cantor (*Una contribución a la doctrina de la multiplicidad*, Journal de Crelle, vol. 84, 1878), ciertamente incluso ya por Bolzano (*Paradojas del infinito*, §20, 1851). Pero ninguno de los mencionados escritores [autores] ha hecho el intento de elevar esta propiedad a [al estatuto de] definición del infinito y edificar [construir] sobre este fundamento de manera lógicamente estricta la ciencia de los números, y precisamente en eso consiste el contenido de mi esforzado [difícil] trabajo, que yo había completado, en todos los puntos fundamentales, ya varios años antes de la aparición del manual [tratado] de G. Cantor y en un tiempo [una época] en [la] que la obra de Bolzano me era, incluso de nombre, completamente desconocida. Para aquellos que tengan interés y comprensión por las dificultades de una tal investigación, señalo aún lo siguiente. Se puede construir [establecer] otra definición completamente diferente de lo finito y lo infinito, que parece más simple, en tanto que en ella no está presupuesto en absoluto el concepto de semejanza de una aplicación (26), a saber: "Un sistema S se llama finito, cuando se puede aplicar en sí mismo (36) de manera tal, que ninguna parte propia (6) de S se aplica [aplique] en sí misma; en caso contrario S se llama un sistema infinito". ¡Ahora hágase el intento de erigir [construir] el edificio sobre esta nueva base! Se choca inmediatamente con fuertes [grandes] dificultades, y creo poder afirmar, que justo [incluso] la demostración de la coincidencia completa [concordancia perfecta] de esta definición con la anterior [antigua] no es obtenida (y entonces fácilmente) más que cuando se puede considerar a la sucesión de los números naturales como ya como desarrollada, y si se pueden también tomar como ayuda mis consideraciones finales en (131); y

sin embargo de todo esto no se dice nada en una ni en otra definición. Se reconocerá en esto cuán grande es la cantidad de pasos de pensamiento, que son requeridos para una tal conformación de una definición [Se medirá de este modo el importante número de pasos del pensamiento requeridos para una tal transformación de la definición].

Alrededor de un año tras la publicación de mi escrito, conocí los *Fundamentos de la Aritmética* de G. Frege, aparecidos ya en 1884. Por muy diferente de la mía que pueda ser la visión sobre la esencia del número consignada en esta obra, se contienen, a saber, desde el §79 en adelante, a pesar de todo también puntos de contacto muy próximos con mi escrito, en especial [particular] con mi definición (44). Ciertamente, la coincidencia [concordancia] no es fácil de reconocer, por el modo de expresión divergente, pero ya la precisión con la que el autor se expresa sobre la [el modo de] inferencia de n a $n + 1$ (al pie de la pág. 93), señala [muestra] claramente que aquí él [evoluciona en] pisa el mismo terreno que yo.

Entretanto (1890–1891) han aparecido [sido publicadas] las *Lecciones sobre el álgebra de la lógica* de E. Schröder casi por completo. Es imposible entrar aquí en detalle sobre la significación [importancia] de esta obra muy interesante [de las más estimulantes], a la que tributo mi mayor [máximo] reconocimiento; es más, sólo quisiera disculparme [excusarme], porque a pesar de la observación hecha en la página 253 de la primera parte, haya mantenido [conservado] a pesar de todo mis algo pesadas expresiones (8) y (17); éstas no tienen ninguna pretensión de ser [universalmente] aceptadas en general, sino que se limitan a servir fundamentalmente [únicamente] a los fines de este escrito sobre aritmética, para lo que son desde mi punto de vista más apropiadas que los signos de suma y producto.

Harzburg, 24 de agosto de 1893. R. Dedekind.

Prólogo a la tercera edición

Cuando hace unos ocho años se me pidió reemplazar la ya entonces agotada segunda edición de este escrito por una tercera, tuve dudas [escrúpulos] de proceder a ello, porque en el tiempo intermedio se han esgrimido dudas sobre la seguridad [certeza] de importantes fundamentos de mi concepción. La significación [importancia], y en parte corrección de estas dudas no las desconozco [menosprecio] tampoco hoy. Pero mi confianza en la armonía interna de nuestra lógica no ha sido por esto quebrantada; creo que una investigación enérgica [examen riguroso] de la capacidad [fuerza] creativa de [que posee] nuestro espíritu para crear [engendrar], a partir de determinados elementos, algo [un nuevo elemento] determinado, su sistema, que necesariamente es diferente de cada uno de esos elementos, conducirá sin duda a [presentar] los fundamentos de mi escrito [de manera irreprochable] libre de objeciones. Debido a otros trabajos, sin embargo, me resulta imposible llevar a término una tan difícil investigación, y pido comprensión [indulgencia], si ahora a pesar de todo el escrito aparece en forma inalterada por tercera vez, lo que sólo puede justificarse, porque el interés en él, como muestra la continua demanda, aún no se ha agotado.

Brunswick, 30 de septiembre de 1911. R. Dedekind.

§1.

Sistemas de elementos.

1. En lo que sigue entiendo por *cosa* cualquier objeto de nuestro pensamiento. Para hablar de las cosas es cómodo designarlas por medio de signos, por ejemplo letras, y permitir hablar brevemente de la cosa a, o simplemente de a, cuando en realidad se quiere entender la cosa designada con a, y no ciertamente la letra a misma. Una cosa está completamente determinada por todo aquello que de ella puede ser dicho y pensado. La cosa a es la misma que b (idéntica a b) y b es la misma que a, si todo aquello que puede ser pensado de a puede ser pensado también de b, y viceversa. Con el signo $a = b$, así como con el signo $b = a$, se indica que a y b son sólo signos o nombres para una y la misma cosa. Si además $b = c$, y por lo tanto c es también, como a, un signo para la cosa designada con b, entonces también es $a = c$. Si la susodicha coincidencia de la cosa designada con a con aquella designada con b no subsiste, entonces las cosas a y b se llaman diferentes, a es otra cosa respecto de b, b es otra cosa respecto de a; hay al menos una propiedad que conviene a una de ellas pero no a la otra.

1. En lo que sigue comprendo como una *cosa* cualquier objeto de nuestro pensamiento. Para poder hablar cómodamente de las cosas, se denotan a través de signos, p. ej. a través de letras, y se permite hablar simplemente de la cosa a o incluso de a, donde en realidad se hace referencia a la cosa denotada por a, en ningún caso a la letra a misma. Una cosa está completamente determinada por todo aquello que puede decirse o pensarse de ella. Una cosa a es lo mismo que b (idéntica a b), y b lo mismo que a, si todo lo que puede ser pensado de a puede serlo también de b, y si todo lo que vale para b, también puede ser pensado de a. Que a y b sólo son signos o nombres para una misma cosa, se denota por el signo $a = b$ y también por $b = a$. Si además $b = c$, es igualmente también c, como a, un signo para la cosa denotada con b, y por lo tanto también $a = c$. Si no se da la anterior coincidencia de la cosa denotada por a con la cosa denotada por b, entonces se llama esta cosas, a, b, diferentes, a es otra cosa que b, b es otra cosa que a; hay alguna propiedad que corresponde a una y no a la otra.

2. Ocurre con mucha frecuencia que cosas diferentes a, b, c ..., consideradas por un motivo cualquiera desde un mismo punto de vista, vengan reunidas mentalmente; se dice entonces que ellas constituyen un *sistema* S; las cosas a, b, c ...son llamadas *elementos* del sistema S, y ellas estan *contenidas* en S; inversamente S *consiste* de estos elementos. Un tal sistema (o complejo, multiplicidad, totalidad) S, siendo un objeto de nuestro pensamiento, es a su vez una cosa (1); está completamente determinado cuando esté determinado, para cada cosa, si es o no un elemento de S([61]). El sistema

[61]De qué modo sea establecida esta determinación y si nosotros conocemos un modo para decidirla, es un hecho totalmente indiferente para todo lo que sigue; las leyes generales que queremos desarrollar no dependen en absoluto de ello, sino que valen bajo cualquier circunstancia. Hago expresamente mención de este punto porque recientemente (en el vol. 99 del *Journal für Mathematik*, pp. 334–36 [in *Werke*, vol. 3^1, Teubner, Leipzig 1899, pp. 155–6]) Kronecker ha querido imponer a la libre formación de conceptos en matemáticas ciertas limitaciones que yo no creo que estén justificadas; pero me parece que no hay ninguna obligación de entar a considerar este asunto con más detalle hasta que el

S es por lo tanto el mismo que el sistema T, in símbolos $S = T$, si cada elemento de S es también elemento de T y si cada elemento de T es también elemento de S. Por uniformidad de expresión conviene también admitir el caso particular de un sistema S que consiste de un único (uno y sólo un) elemento a, es decir, el caso en el que la cosa a es elemento de S, pero cada cosa diferente de a no es elemento de S ⟦ y en este caso se puede —*con el debido cuidado*— entender por el sistema S el propio elemento s ⟧. Por el contrario aquí queremos por ciertas razones excluir completamente el sistema vacío, que no contiene ningún elemento, aunque para otras investigaciones pueda ser cómodo imaginar tal sistema.

Comentario. [N.T.1] Dedekind, en un trabajo denominado "Peligros de la teoría se sistemas", dice que, para simplificar y con el debido cuidado, no distingue entre el sistema S que consta de un único elemento s y el propio elemento s. Ahora bien, un convenio notacional no es una confusión conceptual, y por lo que dice en el trabajo mencionado, es consciente de la necesidad de distinguir entre el sistema $S = \{s\}$ y el elemento s, para evitar caer en contradicciones.

---

2. Sucede muy a menudo, que cosas diferentes a, b, c,... comprendidas por cualquier motivo bajo un mismo punto de vista, son reunidas en la mente, y se dice entonces, que forman un *sistema* S; se llama a las cosas a, b, c,... los elementos del sistema S, estos están *contenidos* en S; y viceversa, S está *compuesto* por esos elementos. Un tal sistema S (o un conjunto, una totalidad, una multiplicidad) es como objeto de nuestro pensamiento en todo caso una cosa (1); está completamente determinado, si para cada cosa está determinado si es elemento de S o no[62]. El sistema S es, por consiguiente el mismo que el sistema T, en signos $S = T$, si todo elemento de S es también elemento de T y todo elemento de T es también elemento de S. Para homogeneizar el tipo de expresión es conveniente admitir también el caso especial en que un sistema S consiste en un único (uno y sólo uno) elemento a, es decir, que la cosa a es elemento de S pero toda cosa diferente de a no es elemento de S. Por el contrario, queremos excluir aquí por completo por determinados motivos el sistema vacío, que no contiene ningún elemento, aunque puede ser cómodo para otras investigaciones imaginar un tal sistema.

3. *Definición.* Un sistema A es llamado *parte* de un sistema S, cuando cada elemento de A es también elemento de S. Puesto que en lo que sigue se hablará continuamente de esta relación entre un sistema A y un sistema

---

distinguido matemático haya manifestado las razones que aduce para la necesidad, o por lo menos la utilidad, de estas limitaciones.

[62] De qué manera tiene lugar esta determinación, y si conocemos un camino para decidir sobre ello, es para todo lo que sigue completamente indiferente; pues las leyes generales que van a desarrollarse no dependen de ello y son válidas en todas las circunstancias. Menciono esto expresamente, porque el señor Kronecker recientemente (en el tomo 99 del *Journal für Mathematik*, págs., 334 a 336) ha querido imponer determinadas limitaciones a la libre formación de conceptos en matemáticas, que no reconozco como correctas; pero parece que será posible profundizar más en esto cuando el excelente matemático haya publicado sus razones para la necesidad, o bien sólo la idoneidad de estas limitaciones.

S, por brevedad la expresaremos con el símbolo $A \prec S$([63]). Por claridad y simplicidad evitaré totalmente el signo inverso $S \succ A$, que podría expresar el mismo hecho, pero, por falta de una palabra más adaptada diré algunas veces que S es *todo* de A, entendiendo con ello que entre los elementos de S se encuentran todos los elementos de A. Puesto que además, por 2, cada elemento s de un sistema S puede ser concebido él mismo como un sistema, podemos usar también en este caso la notación $s \prec S$([64]).

3. Definición. Un sistema A se llama *parte* de un sistema S, si todo elemento de A es también elemento de S. Puesto que en lo que sigue haremos mención continuamente de esta relación entre un sistema A y un sistema S, queremos expresarla para abreviar por el signo $A \prec S$. El símbolo contrario $S \succ A$, con el que este hecho podría ser denotado, lo evitaré por completo en pro de la claridad y simplicidad, pero diré a falta de una mejor expresión hasta ahora, que S es *todo* de A, con lo que también debe quedar expresado que entre los elementos de S se encuentran también todos los elementos de A. Puesto que además todo elemento s de un sistema S por 2 puede él mismo ser comprendido como un sistema, podemos entonces por ello emplear la denominación $s \prec S$.

4. *Teorema.* Por 3, $A \prec A$.

5. *Teorema.* Si $A \prec B$ y $B \prec A$, entonces $A = B$.

La demostración se sigue de 3 y 2.

6. *Definición.* Un sistema A se llama parte *propia* de S, si A es parte de S, pero diferente de S. Según 5, entonces S no es parte de A, es decir (3), no hay en S un elemento que no sea elemento de A.

7. *Teorema.* Si $A \prec B$ y $B \prec C$, lo que también abreviadamente puede denotarse por $A \prec B \prec C$, entonces, $A \prec C$, y ciertamente A es sin duda una parte propia de C si A es una parte propia de B, o si B es una parte propia de C.

La demostración se sigue de 3 y 6.

8. *Definición.* Por el sistema *unión* de los sistemas A, B, $C\ldots$, entendemos aquel sistema, que indicaremos por $\mathfrak{M}(A, B, C\ldots)$, cuyos elementos están determinados por medio de la siguiente regla: una cosa es un elemento de $\mathfrak{M}(A, B, C\ldots)$ si y sólo si es elemento de uno de los sistemas A, B, $C\ldots$, es decir es elemento de A, o de B, o de $C\ldots$ También admitimos el caso en el que hay un único sistema A; entonces, evidentemente, $\mathfrak{M}(A) = A$. Observamos además que el sistema $\mathfrak{M}(A, B, C\ldots)$ unión de A, B, $C\ldots$ es totalmente distinto del sistema cuyos elementos son los sistemas A, B, $C\ldots$ mismos.

Comentario. [N.T.2] Dedekind define, para un conjunto $\mathcal{A}$, la unión de $\mathcal{A}$, denotada, actualmente, por $\bigcup \mathcal{A}$, o por $\bigcup_{A \in \mathcal{A}} A$, como el conjunto que tiene como elementos precisamente aquellos que pertenecen a alguno de los conjuntos pertenecientes a $\mathcal{A}$. Además, dice que si $\mathcal{A} = \{A\}$, entonces $\bigcup\{A\} = A$. Por último, afirma que no hay que confundir $\bigcup \mathcal{A}$ con $\mathcal{A}$.

---

[63] De ahora en adelante escribiremos $A \subseteq S$.

[64] De ahora en adelante escribiremos $\{s\} \subseteq S$.

8. *Definición.* Se entenderá por sistema *compuesto* de cualesquiera sistemas A, B, $C\ldots$, que será denotado con $\mathfrak{M}(A, B, C\ldots)$, aquel sistema cuyos elementos pueden ser determinados según la siguiente prescripción: una cosa vale como elemento de $\mathfrak{M}(A, B, C\ldots)$ cuando es elemento de cualquiera de los sistemas A, B, $C\ldots$, es decir, elemento de A o de B o de $C\ldots$ Admitimos también el caso en que sólo hay un único sistema A; entonces $\mathfrak{M}(A) = A$. Señalamos además, que el sistema $\mathfrak{M}(A, B, C)$ compuesto de A, B, $C\ldots$ ha de diferenciarse del sistema cuyos elementos son los sistemas A, B, $C\ldots$ mismos.

9. *Teorema.* Los sistemas A, B, $C\ldots$ son partes de $\mathfrak{M}(A, B, C\ldots)$.

La demostración se sigue de 8 y 3.

10. *Teorema.* Si A, B, $C\ldots$ son partes de un sistema S, entonces $\mathfrak{M}(A, B, C\ldots) \prec S$.

La demostración se sigue de 8 y 3.

Comentario. [N.T.3] Los dos teoremas anteriores caracterizan al sistema $\mathfrak{M}(A, B, C\ldots)$ como la mínima cota superior, respecto de la inclusión, de los sistemas A, B, $C\ldots$.

---

11. *Teorema.* Si P es parte de uno de los sistemas A, B, $C\ldots$ entonces $P \prec \mathfrak{M}(A, B, C\ldots)$.

La demostración se sigue de 9 y 7.

12. *Teorema.* Si cada uno de los sistemas P, $Q\ldots$ es parte de uno de los sistemas A, B, $C\ldots$ entonces $\mathfrak{M}(P, Q\ldots) \prec \mathfrak{M}(A, B, C\ldots)$.

La demostración se sigue de 11 y 10.

Comentario. [N.T.4] Sean $\mathcal{P}$ y $\mathcal{A}$ dos conjuntos. Si, para cada $P \in \mathcal{P}$, existe un $A \in \mathcal{A}$ tal que $P \subseteq A$, entonces $\bigcup \mathcal{P} \subseteq \bigcup \mathcal{A}$.

---

13. *Teorema.* Si A es la unión de algunos de entre los sistemas P, $Q\ldots$ entonces $A \prec \mathfrak{M}(P, Q\ldots)$.

La demostración se sigue de 11 y 10.

Comentario. [N.T.5] Sean $\mathcal{P}$ y $\mathcal{Q}$ dos conjuntos. Si $\mathcal{Q} \subseteq \mathcal{P}$, entonces $\bigcup \mathcal{Q} \subseteq \bigcup \mathcal{P}$.

---

13. *Teorema.* Si A está compuesto de cualesquiera de los sistemas P, $Q\ldots$ entonces $A \prec \mathfrak{M}(P, Q\ldots)$.

Demostración. Pues todo elemento de A es según 8 elemento de uno de los sistemas P, $Q\ldots$ se sigue de 8 que también es elemento de $\mathfrak{M}(P, Q\ldots)$, de donde según 3 se sigue el teorema.

14. *Teorema.* Si cada uno de los sistemas A, B, $C\ldots$ es la unión de algunos de entre los sistemas P, $Q\ldots$ entonces $\mathfrak{M}(A, B, C\ldots) \prec \mathfrak{M}(P, Q\ldots)$.

La demostración se sigue de 13 y 10.

Comentario. [N.T.6] Sean $\mathcal{A}$ y $\mathcal{P}$ dos conjuntos. Si, para cada $A \in \mathcal{A}$, existe un $\mathcal{P}_A \subseteq \mathcal{P}$ tal que $A = \bigcup \mathcal{P}_A$, entonces $\bigcup \mathcal{A} \subseteq \bigcup \mathcal{P}$.

---

14. *Teorema.* Si todos los sistemas A, B, $C\ldots$ están compuestos de cualesquiera de los sistemas P,$Q\ldots$ entonces $\mathfrak{M}(A, B, C\ldots) \prec \mathfrak{M}(P, Q\ldots)$.

La demostración se sigue de 13,10.

15. *Teorema.* Si cada uno de los sistemas P, $Q\ldots$ es parte de alguno de los sistemas A, B, $C\ldots$ y si cada uno de estos últimos está compuesto de algunos de entre los primeros, entonces $\mathfrak{M}(P, Q\ldots) = \mathfrak{M}(A, B, C\ldots)$.

La demostración se sigue de 12, 14 y 5.

Comentario. [N.T.7] Sean $\mathcal{P}$ y $\mathcal{A}$ dos conjuntos. Si, para cada $P \in \mathcal{P}$, existe un $A \in \mathcal{A}$ tal que $P \subseteq A$ y, para cada $A \in \mathcal{A}$, existe un $\mathcal{P}_A \subseteq \mathcal{P}$ tal que $A = \bigcup \mathcal{P}_A$, entonces $\bigcup \mathcal{A} = \bigcup \mathcal{P}$.

---

15. *Teorema.* Si todos los sistemas P, $Q\ldots$ son parte de uno de los sistemas A, B, $C\ldots$ y cada uno de estos últimos está compuesto de cualesquiera de los primeros, entonces $\mathfrak{M}(P, Q\ldots) = \mathfrak{M}(A, B, C\ldots)$.

La demostración se sigue de 12, 14, 5.

16. *Teorema.* Si $A = \mathfrak{M}(P, Q)$, y $B = \mathfrak{M}(Q, R)$, entonces $\mathfrak{M}(A, R) = \mathfrak{M}(P, B)$.

Demostración. Pues según el anterior teorema 15, tanto $\mathfrak{M}(A, R)$ como $\mathfrak{M}(P, B) = \mathfrak{M}(P, Q, R)$.

17. *Definición.* Una cosa g se llama elemento *común* de los sistemas A, B, $C\ldots$ si está contenida en todos estos sistemas (así pues, en A y en B, y en $C\ldots$). Del mismo modo, un sistema T se llama *parte común* de A, B, $C\ldots$ si T es parte de todos estos sistemas, y por *comunidad* de los sistemas A, B, $C\ldots$ entendemos el sistema completamente determinado $\mathfrak{G}(A, B, C\ldots)$, que consiste en todos los elementos comunes g de A, B, $C\ldots$ y por lo tanto es igualmente una parte común de los mismos sistemas. Admitimos también de nuevo el caso en el que sólo hay un único sistema A; entonces hay que establecer que $\mathfrak{G}(A) = A$. Sin embargo, puede darse también el caso de que los sistemas A, B, $C\ldots$ no posean ningún elemento común, ninguna comunidad; se llaman entonces sistemas *sin* parte común, y el signo $\mathfrak{G}(A, B, C\ldots)$ no tiene significado (cf. la conclusión de 2). Sin embargo, dejaremos casi siempre al lector el atribuir la condición de existencia en las proposiciones sobre comunidades, y encontrar la significación correcta de estas proposiciones también en el caso de la no-existencia.

18. *Teorema.* Toda parte común de A, B, $C\ldots$ es parte de $\mathfrak{G}(A, B, C\ldots)$.

La demostración se sigue de 17.

19. *Teorema.* Toda parte de $\mathfrak{G}(A, B, C\ldots)$ es parte común de A, B, $C\ldots$.

La demostración se sigue de 17,7.

20. *Teorema.* Si cada uno de los sistemas A, B, $C\ldots$ contiene (3) alguno de los sistemas P, $Q\ \ldots$, entonces $\mathfrak{G}(P, Q\ldots) \prec \mathfrak{G}(A, B, C\ldots)$.

Demostración. Pues todo elemento de $\mathfrak{G}(P, Q\ldots)$ es elemento común de P, $Q\ \ldots$ por lo tanto también elemento de A, B, $C\ \ldots$, q.e.d.

Comentario. [N.T.8] Sean $\mathcal{A}$ y $\mathcal{P}$ dos conjuntos. Si, para cada $A \in \mathcal{A}$, existe un $P \in \mathcal{P}$ tal que $P \subseteq A$, entonces $\bigcap \mathcal{P} \subseteq \bigcap \mathcal{A}$.

20.Teorema. Si todos los sistemas A, B, $C\ldots$ son todos (3) de uno de los sistemas P, Q $\ldots$, entonces $\mathfrak{G}(P, Q\ldots) \prec \mathfrak{G}(A, B, C\ldots)$.

Demostración. Pues todo elemento de $\mathfrak{G}(P, Q\ldots)$ es elemento común de P, Q $\ldots$ por lo tanto también elemento de A, B, C $\ldots$, q.e.d.

§1.

Aplicación de un sistema.

21. *Definición*[65]. Por una *aplicación* φ de un sistema S se entiende una ley en base a la cual a cada elemento determinado s de S le *pertenece* una cosa determinada, que se llama la *imagen* de s y se designa con $\varphi(s)$; diremos también que $\varphi(s)$ *corresponde* al elemento s, que $\varphi(s)$ *resulta*, o es *generado*, a partir de s mediante la aplicación φ, que s es *transformado* en $\varphi(s)$ por la aplicación φ. Si T es una parte cualquiera de S, entonces la aplicación φ de S contiene al mismo tiempo una aplicación determinada de T, que nosotros para simplificar indicaremos con el mismo signo φ, es decir la aplicación que a cada elemento t del sistema T le hace corresponder la misma imagen $\varphi(t)$ que posee t como elemento de S; llamaremos también *imagen* de T al sistema que consiste de todas las imágenes $\varphi(t)$, y lo indicaremos por $\varphi(T)$; con esto queda definido también el significado de $\varphi(S)$. Se puede considerar como ejemplo de una aplicación de un sistema la asignación de signos o nombres determinados a sus elementos. La aplicación más simple de un sistema es aquélla que transforma cada uno de sus elementos en sí mismo: ésa será llamada la aplicación *idéntica* del sistema. Por comodidad en los teoremas 22, 23, 24 siguientes, relativos a una aplicación cualquiera φ de cualquier sistema S, indicaremos las imágenes de elementos s y de partes T respectivamente con s' y T'; además convendremos que las letras latinas minúsculas y mayúsculas sin acento indicarán siempre, respectivamente, elementos y partes del sistema S.

Comentario. [N.T.9] La definición de aplicación φ de un sistema S corresponde, salvo por el uso que hace Dedekind del término "ley", a lo que hoy llamamos una función φ desde un conjunto S, i.e., un conjunto φ de pares ordenados tal que cumple la condición funcional (para cada x, y, z, si (x, y) y $(x, z) \in \varphi$, entonces $y = z$) y es tal que su dominio de definición ($\mathrm{Dom}(\varphi)$) es S. Además, Dedekind considera natural y evidente que la imagen de un sistema mediante una aplicación de tal sistema es un sistema (este principio recuerda al esquema axiomático de reemplazo, según el cual la imagen de un conjunto mediante una condición funcional es un conjunto). Así que lo que Dedekind denomina aplicación φ de un sistema S es, en definitiva, lo que hoy llamamos una función φ de S en $\varphi[S]$, que necesariamente ha de ser sobreyectiva. Insistimos, Dedekind no está definiendo, aquí, aplicación de un

[65] Cf. Dirichlet, *Lecciones sobre teoría de los números*, 3. ed., 1879, §163.

sistema en otro, lo que define es el concepto de aplicación de un sistema, y, por lo tanto, no tiene ninguna necesidad de especificar, para una aplicación φ de un sistema S, ningún sistema que contenga, propia o impropiamente, a la imagen de φ, i.e., a $\varphi[S]$.

Cuando Dedekind dice que "Si T es una parte cualquiera de S, entonces la aplicación φ de S contiene al mismo tiempo una aplicación determinada de T", se está refiriendo a lo que hoy llamamos la restricción de φ a T y $\varphi[T]$, que denotamos por $\varphi|_T^{\varphi[T]}$, y que a un $t \in T$ le asigna, por definición, $\varphi|_T^{\varphi[T]}(t) = \varphi(t)$.

Hay que dilucidar el significado del término "ley". Es muy posible que no lo esté usando en el sentido de analíticamente definible (recordemos que recibió clases de Dirichlet), puesto que al decir que "Se puede considerar como ejemplo de una aplicación de un sistema la asignación de signos o nombres determinados a sus elementos", salvo por lo que hace a la univocidad de la asignación, no parece que una aplicación de un sistema deba estar sujeta a cumplir ningún otro requisito, dado que los signos o nombres, en tanto que convenciones, pueden ser totalmente arbitrarios.

En el §16 de *Theory of algebraic integers*, Dedekind dice: "We ordinarily understand *substitution* to be an act by which objects or elements being studied are replaced by corresponding objects or elements, and we say that the old elements are changed, by the substitution, into the new."

---

21. *Definición*[66]. Por *aplicación* φ de un sistema S se entiende una ley, según la cual a todo elemento determinado s de S le *pertenece* una cosa determinada, que se llama la *imagen* de s y que se indica con $\varphi(s)$; decimos también, que $\varphi(s)$ *corresponde* al elemento s, que $\varphi(s)$ se genera o es *creada* por la aplicación φ, que s se *transforma* en $\varphi(s)$ por la aplicación φ. Ahora, si T es una parte cualquiera de S, entonces en la aplicación φ de S está contenida al mismo tiempo una determinada aplicación de T, que por simplicidad se podrá denotar con el mismo signo φ y que consiste en que a todo elemento t del sistema T le corresponde la misma imagen $\varphi(t)$, que t posee como elemento de S; al mismo tiempo el sistema que consiste en todas las imágenes $\varphi(t)$, debe llamarse la *imagen* de T, e indicarse por $\varphi(T)$, con lo que también está explicado el significado de $\varphi(S)$. Como un ejemplo de una aplicación de un sistema puede considerarse ya la asignación a sus elementos de determinados signos o nombres. La aplicación más simple de un sistema es aquella a través de la cual cada uno de sus elementos se convierte en sí mismo; debe llamarse la aplicación *idéntica* del sistema. Por mor de la comodidad, en los siguientes teoremas 22, 23, 24, que se refieren a una aplicación cualquiera φ de un sistema S cualquiera, queremos denotar las imágenes de elementos s y partes T respectivamente por s' y T'; por lo demás establecemos que las letras latinas minúsculas y mayúsculas sin acento deben denotar siempre elementos y partes de ese sistema S.

22. *Teorema*[67]. Si $A \prec B$, entonces $A' \prec B'$.

---

[66]Cf. Dirichlet, *Lecciones sobre teoría de los números*, 3. ed., 1879, §163.

[67]Cf. el teorema 27.

Demostración. En efecto, cada elemento de A' es la imagen de un elemento contenido en A, luego también en B, por ello es elemento de B', q.e.d.

22. *Teorema*[68] Si $A \prec B$, entonces $A' \prec B'$.

Demostración. Pues todo elemento de A' es la imagen de un elemento en A, que es entonces también un elemento contenido en B y es consecuentemente un elemento de B', q.e.d.

23. *Teorema.* La imagen de $\mathfrak{M}(A, B, C \ldots)$ es $\mathfrak{M}(A', B', C' \ldots)$.

Demostración. Si indicamos con M el sistema $\mathfrak{M}(A, B, C \ldots)$ que, por 10, es también parte de S, entonces cada elemento de su imagen M' es la imagen m' de un elemento m de M, puesto que entonces, por 8, m es también elemento de uno de los sistemas $A, B, C \ldots$, m' es elemento de uno de los sistemas $A', B', C' \ldots$, y por lo tanto, por 8, es también elemento de $\mathfrak{M}(A', B', C' \ldots)$; luego, por 3,

$$M' \prec \mathfrak{M}(A', B', C' \ldots).$$

Por otra parte, siendo, por 9, $A, B, C \ldots$ partes de M, $A', B', C' \ldots$ son partes de M' (por 22); luego, por 10,

$$\mathfrak{M}(A', B', C' \ldots) \prec M',$$

de lo cual junto con la fórmula precedente se sigue, por 5, el teorema a demostrar

$$\mathfrak{M}(A', B', C' \ldots) = M'.$$

23. *Teorema.* La imagen de $\mathfrak{M}(A, B, C \ldots)$ es $\mathfrak{M}(A', B', C' \ldots)$.

Demostración. Si se denota el sistema $\mathfrak{M}(A, B, C \ldots)$ que por 10 es asimismo parte de S, con M, entonces todo elemento de su imagen M' es la imagen m' de un elemento m de M; ahora bien, puesto que m es por 8 también elemento de uno de los sistemas A, B, $C \ldots$, y consecuentemente m' elemento de uno de los sistemas A', B', $C' \ldots$, y por lo tanto por 9 es también elemento de $\mathfrak{M}(A', B', C' \ldots)$; entonces por 3

$$M' \prec \mathfrak{M}(A', B', C' \ldots).$$

Por otra parte, puesto que A, B, $C \ldots$ son por 9 partes de M, y también A', B', $C' \ldots$ por 22 son partes de M', entonces también por 10

$$\mathfrak{M}(A', B', C' \ldots) \prec M',$$

y de aquí en unión con lo anterior sigue por 5 el teorema que había que demostrar

$$\mathfrak{M}(A', B', C' \ldots) = M'.$$

24. *Teorema*[69]. La imagen de cada parte común de $A, B, C \ldots$, y por lo tanto también de la intersección $\mathfrak{G}(A, B, C \ldots)$, es parte de $\mathfrak{G}(A', B', C' \ldots)$.

Demostración. En efecto, por 22, aquélla es parte común de $A', B', C' \ldots$, de lo cual, por 18, se sigue el teorema.

24. *Teorema*[70]. La imagen de una parte común de A, B, $C \ldots$, y por lo tanto también la de la comunidad $\mathfrak{G}(A, B, C \ldots)$ es parte de $\mathfrak{G}(A', B', C' \ldots)$.

Demostración. Pues la misma es según 22 parte común de A', B', $C' \ldots$, de donde se sigue el teorema por 18.

---

[68] Cf. el teorema 27.

[69] Cf. el teorema 29.

[70] Cf. teorema 29

25. *Definición y teorema.* Si φ es una aplicación del sistema S y ψ es una aplicación de la imagen $S' = \varphi(S)$, de ellas resulta siempre una aplicación θ de S *compuesta*[71] de φ y ψ, es decir la aplicación que a cada elemento s de S le hace corresponder la imagen

$$\theta(s) = \psi(s') = \psi(\varphi(s)),$$

donde se pone de nuevo $\varphi(s) = s$. Esta aplicación θ se puede indicar brevemente con el símbolo $\psi.\varphi$ o $\psi\varphi$, y la imagen $\theta(s)$ se puede indicar con $\psi\varphi(s)$, estando no obstante muy atentos a la posición de los signos φ, ψ, porque en general el símbolo $\varphi\psi$ está desprovisto de significado, y está dotado de sentido sólo cuando $\psi(S') \subseteq S$. Ahora, si χ indica una aplicación del sistema $\psi(S') = \psi\varphi(S)$ y η la aplicación $\chi\psi$ del sistema S' compuesta de ψ y χ, entonces $\chi\theta(s) = \chi\psi(s') = \eta(s')$, luego, para cada elemento s de S, las aplicaciones compuestas $\chi\theta$ y $\eta\varphi$ coinciden, es decir $\chi\theta = \eta\varphi$. Dado el significado de θ y η se puede también expresar este teorema con

$$\chi.\psi\varphi = \chi\psi.\varphi,$$

y se puede indicar brevemente esta aplicación compuesta de φ, ψ, χ con $\varphi\psi\chi$.

Comentario. [N.T.10] Dedekind define la composición de dos aplicaciones φ y ψ cuando ψ es una aplicación de, precisamente, $\varphi(S)$, siendo φ una aplicación de S. Cuando dice que "$\varphi\psi$ está desprovisto de significado, y está dotado de sentido sólo cuando $\psi(S') \subseteq S$", esto hay que entenderlo como significando que de suponer $\psi[S'] = \psi[\varphi[S]] \subseteq S$, se obtiene $\varphi|_{\psi[S']}^{\varphi[\psi[S']]}$, la restricción de φ a $\psi[S']$ y $\varphi[\psi[S']]$, que es una aplicación de $\psi[S']$, y entonces, ya que ψ es una aplicación de $S' = \varphi[S]$, se obtiene la composición $\varphi|_{\psi[S']}^{\varphi[\psi[S']]}\ \psi$, que es una aplicación de $\varphi[S] = S'$. La situación queda descrita por el siguiente diagrama

$$\begin{array}{ccccc} & & S & \xrightarrow{\quad\varphi\quad} & \varphi[S] \\ & & \uparrow{\scriptstyle \text{in}} & & \uparrow{\scriptstyle \text{in}} \\ S' = \varphi[S] & \xrightarrow[\psi]{} & \psi[S'] & \xrightarrow[\varphi|_{\psi[S']}^{\varphi[\psi[S']]}]{} & \varphi[\psi[S']] \end{array}$$

---

25. *Definición y teorema.* Si φ es una aplicación de un sistema, y ψ una aplicación de la imagen $S' = \varphi(S)$, entonces se genera siempre una aplicación θ de S *compuesta*[72] de φ y ψ, que consiste en que a todo elemento s de S corresponde la imagen

$$\theta(s) = \psi(s') = \psi(\varphi(s)),$$

donde de nuevo se establece que $\varphi(s) = s'$. Esta aplicación θ puede indicarse brevemente por el símbolo $\psi.\varphi$ o $\psi\varphi$, la imagen $\theta(s)$ por $\psi\varphi(s)$, donde hay

[71] Difícilmente hay que temer que se pueda confundir la composición de aplicaciones con la de los sistemas de elementos.

[72] No hay que temer, desde luego, una confusión de esta composición de aplicaciones con la de sistemas de elementos (8).

que atender a la posición de los signos φ, ψ, porque el signo $\varphi\psi$ en general no tiene significación y sólo tiene sentido si $\psi(S') \prec S$. Ahora bien, si χ significa una aplicación del sistema $\psi(S') = \psi\varphi(S)$, y η la aplicación $\chi\psi$ compuesta de ψ y χ del sistema S', entonces $\chi\theta(s) = \chi\psi(s') = \eta(s') = \eta\varphi(s)$, y por lo tanto coinciden entre sí las aplicaciones compuestas $\chi\theta$ y $\eta\varphi$ para todo elemento s de S, i.e., $\chi\theta = \eta\varphi$. Este teorema puede, debido a la significación de θ y η, expresarse convenientemente por:

$$\chi.\psi\varphi = \chi\psi.\varphi,$$

y esta aplicación compuesta por ϕ,ψ,χ puede denotarse abreviadamente por $\chi\psi\varphi$.

§3.

Similaridad de una aplicación. Sistemas similares.

26. *Definición.* Una aplicación φ de un sistema S se dice *similar* (o *unívoca [distinta]*) cuando a elementos diferentes a, b del sistema S corresponden siempre imágenes diferentes $a' = \varphi(a)$, $b' = \varphi(b)$. Puesto que en este caso de $s' = t'$ se sigue siempre, inversamente, que $s = t$, cada elemento del sistema $S' = \varphi(S)$ es la imagen s' de un único elemento s completamente determinado del sistema S, por ello se puede contraponer a la aplicación φ de S una aplicación *inversa* del sistema S', que indicaremos con $\overline{\varphi}$, la cual hace corresponder a cada elemento s' de S' la imagen $\overline{\varphi}(s') = s$; y evidentemente también ella es inyectiva. Está claro que $\overline{\varphi}(S') = S$, que φ es la aplicación inversa de $\overline{\varphi}$, y que la aplicación $\overline{\varphi}\varphi$ compuesta de φ y $\overline{\varphi}$ (por 25) es la aplicación idéntica de S (21). Inmediatamente se tienen las siguientes adiciones al §2 (conservando las notaciones allí adoptadas).

Comentario. [N.T.11] Puesto que para Dedekind una aplicación φ de un sistema S es, usando el lenguaje actual, una función φ de S en $\varphi[S]$, se sigue de ello que en la definición anterior está considerando el concepto de inyectividad para tal tipo de función. Por lo tanto las aplicaciones similares de un sistema S son lo que actualmente denominaríamos las funciones biyectivas de S en $\varphi[S]$.

Por otra parte, según lo dicho por Dedekind $\overline{\varphi}\varphi = \mathrm{id}_S$. Además, teniendo en cuenta que $\overline{\varphi}(\varphi(S)) = S$, también ocurre que $\varphi\overline{\varphi} = \mathrm{id}_{\varphi(S)}$.

En el §16 de *Theory of algebraic integers*, Dedekind dice: "Now let Ω be a *any* field. By a *permutation of* Ω we mean a substitution which changes each number

$$\alpha,\ \beta,\ \alpha+\beta,\ \alpha-\beta,\ \alpha\beta,\ \alpha/\beta$$

of Ω into a corresponding number

$$\alpha',\ \beta',\ \alpha'+\beta',\ \alpha'-\beta',\ \alpha'\beta',\ \alpha'/\beta'$$

in such a way that the conditions ... are satisfied and the substitute numbers α', β', ... are not all zero. We shall see that the set Ω' of the latter numbers forms a new field, ..."

Vemos que Dedekind considera que una permutación de un cuerpo Ω es una función definida sobre Ω, sobreyectiva, que preserva la estructura, y

que, además, es inyectiva. Puesto que *demuestra* que Ω', la imagen de la función, es un cuerpo, en principio, del conjunto Ω' sólo está presuponiendo que está dotado de operaciones que son las homólogas de las operaciones de que está dotado el cuerpo Ω. Por otra parte, el que Ω' esté dotado de tales operaciones es necesario para que tenga sentido la preservación de la estructura.

---

26. *Definición.* Una aplicación φ de un sistema S se llama *semejante* (o *distinta*) si a diferentes elementos a, b, del sistema S les corresponden siempre diferentes imágenes $a' = \varphi(a)$, $b' = \varphi(b)$. Puesto que en este caso siempre se sigue, a la inversa, de $s = t$ que $s' = t'$, entonces, todo elemento del sistema $S' = \varphi(S)$ es la imagen de un único elemento completamente determinado s del sistema S, y se puede desde aquí contraponer a la aplicación φ de S una aplicación inversa del sistema S', que se denota con $\overline{\varphi}$, que consiste en que a todo elemento s' de S' le corresponde la imagen $\overline{\varphi}(s') = s$, y es asimismo evidentemente semejante. Se hace patente que $\overline{\varphi}(S') = S$, que además φ es la aplicación inversa que corresponde a $\overline{\varphi}$, y que la aplicación compuesta $\overline{\varphi}\varphi$ por 25 de φ y $\overline{\varphi}$ es la aplicación idéntica de S(21). Al mismo tiempo resultan los siguientes corolarios al §2 manteniendo las denotaciones de allí.

27. *Teorema*[73]. Si $A' \prec B'$, entonces, $A \prec B$.

Demostración. Pues si a es un elemento de A, entonces a' es un elemento de A', por lo tanto también de B', con lo que $= b'$, donde b es un elemento de B; pero puesto que de $a' = b'$ se sigue siempre $a = b$, entonces todo elemento a de A es también elemento de B, q.e.d.

28. *Teorema.* Si $A' = B'$, entonces $A = B$.

La demostración se sigue de 27, 4 y 5.

29. *Teorema*[74]. Si $G = \mathfrak{G}(A, B, C \ldots)$, entonces $G' = \mathfrak{G}(A', B', C' \ldots)$.

Demostración. Todo elemento de $G' = \mathfrak{G}(A', B', C' \ldots)$ está contenido asimismo en S', también lo está la imagen g' de un elemento g contenido en S; pero puesto que g' es un elemento común de A', B', $C' \ldots$, entonces g debe ser por 27 elemento común de A,B,C, por lo tanto también elemento de G, con lo que todo elemento de $\mathfrak{G}(A', B', C' \ldots)$ es imagen de un elemento g de G, por lo tanto elemento de G', i.e. $\mathfrak{G}(A', B', C' \ldots) \prec G'$, y de aquí se sigue nuestro teorema considerando 24,5.

30. *Teorema.* La aplicación idéntica de un sistema es siempre una aplicación semejante.

31. *Teorema.* Si φ es una aplicación semejante de S, y ψ una aplicación semejante de $\phi(S)$, entonces la aplicación compuesta $\psi\varphi$ de φ y ψ de S es asimismo una aplicación semejante, y la aplicación inversa correspondiente $\overline{\psi\varphi}$ es $= \overline{\varphi}\overline{\psi}$.

Demostración. Pues a elementos diferentes a, b, de S les corresponden imágenes diferentes $a' = \varphi(a)$, $b' = \varphi(b)$, y a estas de nuevo diferentes imágenes $\psi(a') = \psi\varphi(a)$, $\psi(b') = \psi\varphi(b)$, por lo tanto $\psi\varphi$ es una aplicación semejante. Además cada elemento $\psi\varphi(s) = \psi(s')$ del sistema $\psi\varphi(S)$ se

---

[73] Cf. teorema 22.

[74] Cf. teorema 24.

transforma por $\overline{\psi}$ en $s' = \varphi(s)$, y éste por $\overline{\varphi}$ en s, por lo tanto $\psi\varphi(s)$ se transforma por $\overline{\varphi}\overline{\psi}$ en s, q.e.d.

32. *Definición.* Los sistemas R, S se dicen *similares* si existe una aplicación similar φ de S tal que $\varphi(S) = R$, y por lo tanto también $\overline{\varphi}(R) = S$. Evidentemente, por 30, cada sistema es similar a sí mismo.

Comentario. [N.T.12] Al decir que $\overline{\varphi}(R) = S$, puesto que, por 26, $\overline{\varphi}$ también es inyectiva, Dedekind está afirmando que la relación de similaridad entre sistemas es simétrica. Además, puesto que cada sistema es similar a sí mismo, tal relación es reflexiva.

---

32. *Definición.* Los sistemas R, S, se llaman *semejantes*, cuando hay una aplicación unívoca φ de S tal que $\varphi(S) = R$, con lo que también se dará $\overline{\varphi}(R) = S$. Evidentemente, por 30 todo sistema es semejante consigo mismo.

33. *Teorema.* Si R, S son sistemas similares, entonces cada sistema Q similar a R es también similar a S.

Demostración. En efecto, si φ y ψ son aplicaciones similares de S y R tales que $\varphi(S) = R$ y $\psi(R) = Q$, entonces, por 31, $\psi\varphi$ es una aplicación similar de S tal que $\psi\varphi(S) = Q$, q.e.d.

Comentario. [N.T.13] De modo que la relación de similaridad es transitiva y, por lo tanto, al ser, además, reflexiva y simétrica, tiene las propiedades de una relación de equivalencia. Esto es lo que le induce a establecer la siguiente.

---

33. *Teorema.* Si R, S son sistemas semejantes, entonces todo sistema Q semejante a R es también semejante a S.

Demostración. Pues si φ, ψ son aplicaciones semejantes de S, R, tales que $\varphi(S) = R$, y $\psi(R) = Q$, entonces, por 31, $\psi\varphi$ es una aplicación semejante de S, tal que $\psi\varphi(S) = Q$, q.e.d.

34. *Definición.* Todos los sistemas se pueden por lo tanto repartir en *clases* recogiendo en una clase determinada única y exclusivamente los sistemas Q, R, $S\ldots$, similares a un sistema dado R, llamado el *representante* de la clase; por el teorema 33 previo, la clase no cambia si se elige como representante cualquier otro sistema S perteneciente a ella.

Comentario. [N.T.14] Conviene observar que en la definición anterior Dedekind introduce, por primera y única vez, en su escrito el término "clase", en tanto que no coincidente necesariamente con el de "sistema", pero del que parece razonable suponer que cae bajo el de sistema. Ahora bien, puesto que las clases son cosas, debido a que es cosa todo aquello que sea objeto del pensamiento, entonces podemos, según Dedekind, reunirlas mentalmente obteniendo un sistema, el sistema de todas las clases (relativas a la relación de semejanza). Pero incluso la sola consideración de las clases, como es bien sabido, ya conduce irremadiablemente a la obtención de contradicciones,

e.g., si $S = \{s\}$ es un sistema final, para una cosa s, arbitraria, pero fija, y R es cualquier sistema, entonces S es semejante a $\{R\}$, por lo tanto la clase correspondiente a S, i.e., representada por S, tiene como elementos precisamente a todos los sistemas $\{R\}$, cuando R varía a través de todos los sistemas, incluido el sistema $\{S\} = \{\{s\}\}$, luego, considerando la unión de tal clase, se obtiene el sistema de todos los sistemas, que no existe.

En el §5 de *Theory of algebraic integers*, de Dedekind, en nota a pie de página, dice Dedekind que: "The word *class* seems to have been employed by Gauss first à propos of complex numbers (*Theoria residuorum biquadraticorum*, II, art. 42.)". Podría decirse que reserva el término "clase" para los sistemas que constituyen los bloques de la partición inducida por una equivalencia.

---

34. *Definición.* A partir de aquí se pueden dividir todos los sistemas en *clases*, en tanto que se agrupen en una determinada clase todos y sólo los sistemas Q, R, S, que sean semejantes a un determinado sistema R, el representante de la clase; por el anterior teorema 33 no varía la clase, cuando se elige cualquier otro sistema S perteneciente a ella como representante.

35. *Teorema.* Si R, S, son sistemas semejantes, entonces toda parte de S lo es también a una parte de R, y toda parte propia de S es también semejante a una parte propia de R.

Demostración. Pues si φ es una aplicación semejante de S, $\varphi(S) = R$, y $T \prec S$, entonces se da por 22 el sistema $\varphi(T) \prec R$, que es semejante a T. Si además es T una parte propia de S, y s un elemento de S no contenido en T, entonces el elemento $\varphi(s)$ contenido en R no puede por 27 estar contenido en $\varphi(T)$, con lo que $\varphi(T)$ es parte propia de R, q.e.d.

§4.

Aplicación de un sistema en sí mismo.

36. *Definición.* Sea φ una aplicación, similar o no, de un sistema S, y sea $\varphi(S)$ parte de un sistema Z, diremos entonces que φ es una aplicación de S *en* Z y que S está representado en Z mediante φ. Por lo tanto, cuando $\varphi(S) \subseteq S$ llamamos a φ una aplicación de S *en sí mismo*, y en este parágrafo queremos estudiar las leyes generales de una aplicación de tal género. Al hacer esto usaremos las mismas notaciones que en el §2, poniendo otra vez $\varphi(s) = s'$, $\varphi(T) = T'$. Estas imágenes s' y T' son , por 22 y 7, ellas mismas a su vez elementos y partes de S, y lo mismo vale para todas las cosas designadas con letras latinas.

Comentario. [N.T.15] En la definición anterior Dedekind define, por una parte, lo que actualmente denominamos función de un conjunto en otro y, por otra, la noción de endofunción de un conjunto. Con lo cual las aplicaciones de un sistema en otro ya no son, necesariamente, sobreyectivas, a diferencia de lo que ocurría con las aplicaciones de un conjunto, que sí son sobreyectivas.

---

36. *Definición.* Si φ es una aplicación semejante o desemejante de un sistema S, y $\varphi(S)$ parte de un sistema Z, entonces llamamos a φ una aplicación de S en Z, y decimos que S es aplicado por φ en Z. Llamamos por esto a φ una aplicación del sistema S en sí mismo, si $\varphi(S) \prec S$, y queremos investigar en estos parágrafos las leyes generales de una tal aplicación. Usamos aquí las mismas denotaciones que en el §2, en tanto que de nuevo establecemos que $\varphi(s) = s'$, $\varphi(T) = T'$. Estas imágenes s', T', son, como consecuencia de 22, 7, ahora ellas mismas a su vez elementos o partes de S, como todas las cosas indicadas con letras latinas.

37. *Definición.* Decimos que K es una *cadena* si $K' \subseteq K$. Observamos expresamente que a la parte K de S no le compete en sí misma en absoluto el atributo de cadena, sino que le viene asignado sólo en relación con la aplicación φ; respecto a otra aplicación del sistema S en sí mismo, K muy bien puede no ser una cadena.

Comentario. [N.T.16] Dedekind, usando la terminología actual, empieza considerando un álgebra mono–unaria $\mathbf{S} = (S, \varphi)$, arbitraria, pero fija. A continuación define, para tal tipo de álgebras, lo que actualmente llamamos subálgebra del álgebra $\mathbf{S}$, que es una parte K de S cerrada bajo la operación estructural φ, i.e., tal que $\varphi[K] \subseteq K$. Con lo cual, y en virtud de lo que sigue en el mismo §4, podríamos decir que Dedekind, aún restringiéndose a la consideración de álgebras mono–unarias, inaugura el estudio del álgebra universal (las obras completas de Dedekind fueron publicadas entre los años 1930 y 1932, los trabajos de Birkhoff sobre álgebra universal son publicados a partir de 1933).

---

37. *Definición.* K se llama una *cadena*, cuando $K' \prec K$. Señalamos explícitamente que este nombre no corresponde de por sí a la parte K del sistema S, sino que sólo se le asigna en relación a la aplicación φ, en relación a otra aplicación del sistema S en sí mismo K puede muy bien no ser una cadena.

38. *Teorema.* S es una cadena.

Comentario. [N.T.17] Si denotamos por $\mathcal{K}(S, \varphi)$ el conjunto de todas las cadenas de (S, φ), entonces el teorema anterior afirma que $S \in \mathcal{K}(S, \varphi)$, luego que el concepto de cadena de (S, φ) no es vacuo. Además, obviamente, S es la máxima cadena de (S, φ), i.e., si K es una cadena de (S, φ), entonces $K \subseteq S$.

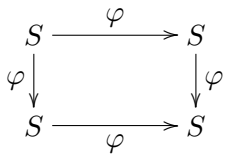
---

39. *Teorema.* La imagen K' de una cadena K es una cadena.

Demostración. Pues de $K' \prec K$ se sigue por 22 también que ($K' \prec'$ (K', q.e.d.

Comentario. [N.T.18] Las álgebras mono–unarias $\mathbf{S} = (S, \varphi)$ tienen la propiedad especial de que su misma operación estructural φ es un endomorfismo

de **S**, i.e., se cumple, obviamente, que el diagrama



conmuta. Entonces lo que establece Dedekind en el teorema anterior es que, para una subálgebra K de **S**, $\varphi[K]$, la imagen de K mediante el endomorfismo φ de **S**, es una subálgebra de **S**. Dicho de otro modo, los endomorfismos, pero no sólo ellos, preservan las subálgebras.

---

40. *Teorema.* Si A es parte de una cadena K, entonces también $A' \subseteq K$.

Demostración. Pues de $A \prec K$ se sigue (por 22) $A' \prec K'$, y puesto que (por 37) $K' \prec K$, entonces se sigue (por 7), que $A' \prec K$, q.e.d.

40. *Teorema.* Si A es parte de una cadena K, entonces se da también $A' \prec K$.

Demostración. Pues de $A \prec K$ se sigue (por 22) $A' \prec K'$, y puesto que (por 37) $K' \prec K$, entonces se sigue (por 7), que $A' \prec K$, q.e.d.

41. *Teorema.* Si la imagen A' es parte de una cadena L, entonces existe una cadena K que cumple las condiciones $A \prec K$, $K' \prec L$; y precisamente $\mathfrak{M}(A, L)$ es una tal cadena K.

Demostración. Si se establece que realmente $K = \mathfrak{M}(A, L)$, entonces, la condición $A \prec K$ queda satisfecha por 9. Puesto que por 23 además $K' = \mathfrak{M}(A', L')$ y por suposición $A' \prec L$, y $L' \prec L$, entonces queda satisfecha también la otra condición por 10, y de aquí se sigue, puesto que (por 9) $L \prec K$, también que $K' \prec K$, i.e., K es una cadena, q.e.d.

Comentario. [N.T.19] Dedekind propone, en el teorema anterior, como una posible solución del problema planteado la cadena $K = A \cup L$. Ahora bien, hemos de tener en cuenta que tal solución no es la única ni la mejor, ni dice tales cosas Dedekind. Así, e.g., $A \cup \varphi[A] \cup L$, $A \cup \varphi[A] \cup \varphi[\varphi[A]] \cup L$, etc., son soluciones del mismo problema, como también lo es $\bigcup_{n\in\mathbb{N}} \varphi^n[A] \cup L$. Además, puesto que el conjunto formado por las cadenas K tales que $A \subseteq K$ y $\varphi[K] \subseteq L$ no es vacío, está ordenado por la inclusión, y es tal que cualquier familia no vacía $(K_i)_{i\in I}$, en el conjunto en cuestión, linealmente ordenada, tiene un supremo, entonces podemos afirmar, en virtud del lema de Kuratowski-Zorn, que existen cadenas K maximales.

---

41. *Teorema.* Si la imagen A' es parte de una cadena L, entonces hay una cadena K, que satisface las condiciones $A \prec K$, $K' \prec L$, y por cierto $\mathfrak{M}(A, L)$ es una tal cadena K.

Demostración. Si se establece que realmente $K = \mathfrak{M}(A, L)$, entonces, la condición $A \prec K$ queda satisfecha por 9. Puesto que por 23 además $K' = \mathfrak{M}(A', L')$ y por suposición $A' \prec L$, y $L' \prec L$, entonces queda satisfecha también la otra condición por 10, y de aquí se sigue, puesto que (por 9) $L \prec K$, también que $K' \prec K$, i.e., K es una cadena, q.e.d.

42. *Teorema.* Un sistema M compuesto sólo de cadenas A, B, C ... es una cadena.

Demostración. Puesto que (por 23) $M' = \mathfrak{M}(A', B', C' \ldots)$ y por suposición $A' \prec A$, $B' \prec B$, $C' \prec C$, entonces se sigue (por 12) que $M' \prec M$, q.e.d.

Comentario. [N.T.20] El anterior teorema dice que, para el caso de las álgebras mono–unarias $\mathbf{S} = (S, \varphi)$, la unión de una familia no vacía de subálgebras de $\mathbf{S}$ es una subálgebra de $\mathbf{S}$, i.e., el conjunto $\mathcal{K}(S, \varphi)$ es completamente aditivo. Este resultado, como es bien sabido, sólo es válido para las álgebras, no necesariamente mono–unarias, bajo la condición adicional de que la familia de subálgebras en cuestión esté dirigida superiormente.

---

42. *Teorema.* Un sistema M compuesto sólo de cadenas A, B, C ... es una cadena.

Demostración. Puesto que (por 23) $M' = \mathfrak{M}(A', B', C' \ldots)$ y por suposición $A' \prec A$, $B' \prec B$, $C' \prec C$, entonces se sigue (por 12) que $M' \prec M$, q.e.d.

43. *Teorema.* La intersección G de sólo cadenas A, B, C ... es una cadena.

Demostración. Puesto que G por 17 es parte común de A, B, C ... también G' es parte común por 22 de A', B', C' ... y por suposición $A' \prec A$, $B' \prec B$, $C' \prec C$ ..., entonces G' es también parte común de A, B, C ... y por consiguiente por 18 también parte de G, q.e.d.

Comentario. [N.T.21] El anterior teorema dice que la intersección de una familia no vacía de subálgebras de $\mathbf{S}$ es una subálgebra de $\mathbf{S}$, i.e., el conjunto $\mathcal{K}(S, \varphi)$ es completamente multiplicativo. Este resultado, junto con el hecho de que $S \in \mathcal{K}(S, \varphi)$, nos asegura que $\mathcal{K}(S, \varphi)$ es un sistema de clausura algebraico, como ocurre para las álgebras de cualquier tipo de similaridad.

---

43. *Teorema.* La comunidad G sólo de cadenas A, B, C ... es una cadena.

Demostración. Puesto que G por 17 es parte común de A, B, C ... también G' es parte común por 22 de A', B', C' ... y por suposición $A' \prec A$, $B' \prec B$, $C' \prec C$ ..., entonces G' es también parte común de A, B, C ... y por consiguiente por 18 también parte de G, q.e.d.

44. *Definición.* Sea A una parte de S, con A_0 indicamos la intersección de todas las cadenas (como, e.g., S) de las cuales A es parte. Tal intersección A_0 existe (cf. 17), porque A mismo es ya parte común de todas estas cadenas. Dado que, por 43, A_0 es una cadena, llamaremos a A_0 la *cadena del sistema* A o, brevemente, la cadena de A. También esta definición se refiere estrictamente a la aplicación fundamental dada φ del sistema S en sí mismo, y si posteriormente, por razones de claridad, se hace necesario, preferimos usar la notación $\varphi_0(A)$ en lugar de A_0; similarmente designaremos con $\omega_0(A)$ la cadena de A correspondiente a otra aplicación ω. Para este importantísimo concepto valen los siguientes teoremas.

Comentario. [N.T.22] En la anterior definición, Dedekind procede a asociar unívocamente, a cada parte no vacía A de S, A_0, la cadena de A, y lo hace mediante un procedimiento impredicativo, porque considera la intersección del conjunto de todas las cadenas de $\mathbf{S} = (S, \varphi)$ que contienen a A, conjunto al que, en definitiva, pertenece A_0, la propia cadena de A. Obsérvese que la cadena de una parte de S no la obtiene mediante un procedimiento constructivo, tomando la unión de una familia ascendente de partes de S, obtenida por medio del principio de la definición por recursión finita, porque todavía no dispone ni siquiera del conjunto de los números naturales (que es lo que trata de obtener). La extensión del operador que a cada parte no vacía A de S le asigna A_0 se puede extender hasta la parte vacía considerando que $\varnothing_0$, la cadena de $\varnothing$, es la intersección de todas las cadenas de $\mathbf{S}$. Además, el operador en cuestión es la particularización a las álgebras mono–unarias, del operador subálgebra generada de las álgebras (ordinarias o heterogéneas) de un tipo de similaridad arbitrario.

---

44. *Definición.* Si A es una parte cualquiera de S, queremos indicar con A_0 la comunidad de todas aquellas cadenas (p.ej. S), de las cuales A es parte. Esta comunidad A_0 existe (cf.17), porque ciertamente A misma es parte común de todas estas cadenas. Puesto que además A_0 por 43 es una cadena, queremos llamar entonces a A_0 la *cadena del sistema* A, o brevemente la cadena de A. También esta definición se refiere por completo a la aplicación φ subyacente determinada del sistema S en sí mismo, y cuando más tarde sea necesario por motivos de claridad, queremos en lugar de A_0 establecer más bien el signo $\varphi_0(A)$, y del mismo modo indicaremos la cadena correspondiente de otra aplicación ω de A con $\omega_0(A)$. Ahora, los siguientes teoremas son válidos para este importantísimo concepto.

45. *Teorema.* $A \prec A_0$.

Demostración. Pues A es parte común de todas aquellas cadenas cuya comunidad es A_0, de donde se sigue el teorema por 18.

Comentario. [N.T.23] El operador subálgebra generada es extensivo.

---

46. *Teorema.* $(A_0)' \subseteq A_0$.

Demostración. Pues por 44 A_0 es una cadena (37).

47. *Teorema.* Si A es parte de una cadena K, entonces también $A_0 \subseteq K$.

Demostración. Pues A_0 es la comunidad y consecuentemente también una parte común de todas las cadenas K, de la cuales A es parte.

48. *Observación.* Se ve fácilmente que el concepto de la cadena A_0, definido en 44, está completamente caracterizado por los teoremas 45, 46, 47 precedentes.

Comentario. [N.T.24] La anterior observación significa que, dados dos subconjuntos A, K de S, son equivalentes:

1. $K = A_0$.
2. K es una cadena, $A \subseteq K$, y, para cada cadena L, si $A \subseteq L$, entonces $K \subseteq L$.

Es evidente que si $K = A_0$, entonces, en virtud de la definición de A_0, K es la mínima cadena que contiene a A.

Recíprocamente, si K es una cadena, $A \subseteq K$, y, para cada cadena L, si $A \subseteq L$, entonces $K \subseteq L$, entonces, por cumplir las dos primeras condiciones, $A_0 \subseteq K$, y, por cumplir la tercera, que $K \subseteq A_0$. Por lo tanto $K = A_0$.

---

48. *Observación.* Es fácil convencerse de que el concepto definido en 44 de la cadena A_0 está completamente caracterizado por los teoremas previos 45, 46 y 47.

49. *Teorema.* $A' \prec (A_0)'$.

La demostración se sigue de 45 y 22.

50. *Teorema.* $A' \prec A_0$.

La demostración se sigue de 49, 46 y 7.

51. *Teorema.* Si A es una cadena, $A_0 = A$.

Demostración. Puesto que A es parte de la cadena A, entonces por 47 también $A_0 \prec A$, de donde por 45 y 5, se sigue el teorema.

Comentario. [N.T.25] Para una parte A de S se cumple, obviamente, que si $A_0 = A$, entonces A es una cadena. Por lo tanto, de esto junto con lo establecido en el teorema anterior, se deduce inmediatamente que los puntos fijos del operador subálgebra generada son las subálgebras. Del teorema anterior también se obtiene, como corolario, que, para cada parte A de S, $A_0 = (A_0)_0$, i.e., que el operador subálgebra generada es idempotente, porque A_0 es una cadena.

---

51. *Teorema.* Si A es una cadena, entonces, $A_0 = A$.

Demostración. Puesto que A es parte de la cadena A, entonces por 47 también $A_0 \prec A$, de donde por 45 y 5, se sigue el teorema.

52. *Teorema.* Si $B \subseteq A$, entonces $B \subseteq A_0$.

La demostración se sigue de 45 y 7.

53. *Teorema.* Si $B \prec A_0$, entonces $B_0 \prec A_0$, y viceversa.

Demostración. Puesto que A_0 es una cadena, entonces se sigue por 47, de $B \prec A_0$ también $B_0 \prec A_0$; y viceversa, si $B_0 \prec A_0$, entonces se sigue por 7 también $B \prec A_0$, porque (por 45) $B \prec B_0$.

54. *Teorema.* Si $B \prec A$, entonces $B_0 \prec A_0$.

La demostración se sigue de 52 y 53.

Comentario. [N.T.26] El teorema anterior dice que el operador subálgebra generada es isótono o monótono creciente.

---

55. *Teorema.* Si $B \prec A_0$, entonces también $B' \prec A_0$.

Demostración. Puesto que por 53 $B_0 \prec A_0$, y puesto que (por 50) $B' \prec B_0$, entonces se sigue el teorema a probar de 7. Lo mismo se consigue, como es fácil ver, también de 22, 46 y 7, o de 40.

56. *Teorema.* Si $B \prec A_0$, entonces $(B_0)' \prec (A_0)'$.

La demostración se sigue de 53 y 22.

57. *Teorema y definición.* $(A_0)' = (A')_0$, es decir la imagen de la cadena de A es al mismo tiempo la cadena de la imagen. Por ello se puede designar este sistema simplemente con A'_0 y llamarlo indistintamente la *cadena de la imagen* o la *imagen de la cadena* de A. Adoptando la notación más precisa introducida en 44, se puede expresar este teorema como: $\varphi(\varphi_0(A)) = \varphi_0(\varphi(A))$.

Comentario. [N.T.27] El teorema anterior dice que, para las álgebras mono–unarias, la operación estructural de la misma, que es, simultáneamente, un endomorfismo, conmuta con el operador subálgebra generada, o, lo que es equivalente, que el diagrama

$$\begin{array}{ccc} \mathrm{Sub}(S) & \xrightarrow{\varphi[\cdot]} & \mathrm{Sub}(S) \\ \Big\downarrow{\scriptstyle \mathrm{Sg}_{\mathbf{S}}} & & \Big\downarrow{\scriptstyle \mathrm{Sg}_{\mathbf{S}}} \\ \mathrm{Sub}(S) & \xrightarrow[\varphi[\cdot]]{} & \mathrm{Sub}(S) \end{array}$$

conmuta.

---

57. *Teorema y definición.* $(A_0)' = (A')_0$, i.e, la imagen de la cadena de A es al mismo tiempo la cadena de la imagen de A. Se puede a partir de aquí indicar brevemente este sistema con A'_0 y a conveniencia llamarlo la *imagen de la cadena* o la *cadena de la imagen* de A. Según la denotación más clara indicada en 44, el teorema se expresaría de la siguiente manera: $\varphi(\varphi_0(A)) = \varphi_0(\varphi(A))$.

Demostración. Si se establece la abreviatura $(A')_0 = L$, entonces L es una cadena (44) y por 45 $A' \prec L$, con lo que hay por 41 una cadena K, que satisface las condiciones $A \prec K$, $K' \prec L$, de aquí se sigue por 47 también $A_0 \prec K$, luego $(A_0)' \prec K'$, y por consiguiente por 7 también $(A_0)' \prec L$, i.e.,

$$(A_0)' \prec (A')_0.$$

Por otra parte, por 49, $A' \prec (A_0)'$ y, por 44 y 39, $(A_0)'$ es una cadena, y, por lo tanto, por 47,

$$(A')_0 \prec (A_0)'.$$

de donde en conexión con el resultado anterior se sigue el teorema que había que probar (5).

58. *Teorema.* $A_0 = \mathfrak{M}(A, A'_0)$, i.e., la cadena de A está compuesta de A y de la cadena de la imagen de A.

Demostración. Se establece de nuevo para abreviar

$$L = A'_0 = (A_0)' = (A')_0 \quad \text{y} \quad K = \mathfrak{M}(A, L),$$

entonces, (por 45) $A' \prec L$, puesto que L es una cadena, entonces vale por 41 lo mismo para K; puesto que además $A \prec K$ (9), entonces se sigue por 47 también

$$A_0 \prec K.$$

Por otra parte, puesto que (por 45) $A \prec A_0$, y por 46 también $L \prec A_0$, entonces también por 10

$$K \prec A_0,$$

de donde junto al resultado anterior se sigue (5) el teorema que había que probar.

59. *Teorema de inducción completa.* Para demostrar que la cadena A_0 es parte de un sistema cualquiera Σ (sea este mismo parte de S o no), es suficiente mostrar que

ρ. que $A \subseteq \Sigma$, y
σ. que la imagen de cada elemento común de A_0 y Σ es también elemento de Σ.

Comentario. [N.T.28] El teorema anterior recibe actualmente el nombre de *principio de la demostración por inducción algebraica.*

La condición σ, i.e., que $\varphi[A_0 \cap \Sigma] \subseteq \Sigma$, equivale a que $A_0 \cap \Sigma$ sea una subálgebra de $\mathbf{S}$, i.e., a que $\varphi[A_0 \cap \Sigma] \subseteq A_0 \cap \Sigma$.

Siguiendo la pauta marcada por Dedekind, presentamos, para las álgebras (ordinarias, i.e., no heterogéneas), el principio de la demostración por inducción algebraica. Sea $\mathbf{A}$ una $\mathbf{\Sigma}$-álgebra, $X \subseteq A$ e Y un conjunto (que no sea necesariamente parte de A). Una condición suficiente para que $Y \supseteq \mathrm{Sg}_{\mathbf{A}}(X)$, es que

ρ. $X \subseteq Y$, y
σ. que, para cada $n \in \mathbb{N}$ y cada $\sigma \in \Sigma_n$, $F_\sigma[(\mathrm{Sg}_{\mathbf{A}}(X) \cap Y)^n] \subseteq Y$.

Observemos que la condición σ equivale a que $\mathrm{Sg}_{\mathbf{A}}(X) \cap Y$ sea una subálgebra de $\mathbf{A}$.

Otra versión del mismo principio es la siguiente. Sea $\mathbf{A}$ una $\mathbf{\Sigma}$-álgebra, $X \subseteq A$ e $Y \subseteq \mathrm{Sg}_{\mathbf{A}}(X)$. Una condición suficiente para que $Y = \mathrm{Sg}_{\mathbf{A}}(X)$, es que $X \subseteq Y$ y que Y sea un cerrado de $\mathrm{Sg}_{\mathbf{A}}(X)$ (o, lo que es equivalente, un cerrado de $\mathbf{A}$). En particular, si X es un conjunto de generadores de $\mathbf{A}$, una condición suficiente para que $Y = A$, es que $X \subseteq Y$ y que Y sea un cerrado de $\mathbf{A}$.

El principio de la demostración por inducción algebraica, para el caso heterogéneo, dice que dada una $\mathbf{\Sigma} = (S, \Sigma)$-álgebra heterogénea $\mathbf{A} = (A, F)$, un $X \subseteq A$ y un S-conjunto Y (que no sea necesariamente parte de A), una condición suficiente para que $Y \supseteq \mathrm{Sg}_{\mathbf{A}}(X)$, es

ρ. que $X \subseteq Y$, y
σ. que, para cada $(w, s) \in S^\star \times S$ y cada $\sigma \in \Sigma_{w,s}$, $F_\sigma[(\mathrm{Sg}_{\mathbf{A}}(X) \cap Y)_w] \subseteq Y_s$.

Recordemos que $(\mathrm{Sg}_{\mathbf{A}}(X) \cap Y)_w = \prod_{i \in |w|}(\mathrm{Sg}_{\mathbf{A}}(X)_{w_i} \cap Y_{w_i})$, siendo $|w|$ la longitud de la palabra w. Observemos que la condición σ equivale a que $\mathrm{Sg}_{\mathbf{A}}(X) \cap Y$ sea una subálgebra de $\mathbf{A}$.

---

59. *Teorema de la inducción completa.* Para demostrar que la cadena A_0 es parte de algún sistema Σ –sea éste último parte de S o no–, basta con mostrar,

ρ. $X \subseteq Y$, y
σ. que, para cada $n \in \mathbb{N}$ y cada $\sigma \in \Sigma_n$, $F_\sigma[(\mathrm{Sg}_{\mathbf{A}}(X) \cap Y)^n] \subseteq Y$.

Demostración. Pues, si ρ es verdadero, entonces existe por 45 en todo caso la comunidad $G = \mathfrak{G}(A_0, \Sigma)$ y ciertamente tenemos que $A \prec G$; puesto que

además por 17 tenemos que

$$G \prec A_0,$$

entonces G es también parte de nuestro sistema S, el cual se aplica en sí mismo por φ, y al mismo tiempo se sigue por 55 también que $G' \prec A_0$. Ahora, si σ es asimismo verdadero, i.e, si tenemos que $G' \prec S$, entonces, G', como parte común de los sistemas A_0 y Σ debe ser por 18 parte de su comunidad G, i.e., G es una cadena (37), y puesto que, como ya se ha señalado más arriba, tenemos que $A \prec G$, entonces se sigue por 47 también

$$A_0 \prec G$$

y de aquí en unión con el resultado anterior $G = A_0$, entonces por 17 también $A_0 \prec \Sigma$, q.e.d.

60. El teorema anterior constituye, como se mostrará posteriormente, el fundamento científico del método de demostración conocido bajo el nombre de *inducción completa* (inferencia de n a $n+1$), y puede ser expresado en los siguientes términos: Para demostrar que todos los elementos de la cadena A_0 poseen una cierta propiedad $\mathfrak{E}$ (o que un teorema $\mathfrak{S}$ que se refiere a una cosa n indeterminada vale efectivamente para todos los elementos de la cadena A_0), es suficiente mostrar

ρ. que todos los elementos a del sistema A poseen la propiedad $\mathfrak{E}$ (o que $\mathfrak{S}$ vale para todos los a), y

σ. que la imagen n' de cada elemento n de A_0 que posea la propiedad $\mathfrak{E}$ posee también la propiedad $\mathfrak{E}$ (o que el teorema $\mathfrak{S}$, si vale para un elemento n de A_0, vale ciertamente también para su imagen n').

De hecho, si se indica con Σ el sistema de todas las cosas que poseen la propiedad $\mathfrak{E}$ (o para las cuales vale el teorema $\mathfrak{S}$), es inmediata la coincidencia completa de la presente formulación del teorema con la adoptada en 59.

Comentario. [N.T.29] En lo anterior Dedekind hace uso del principio de comprehensión, según el cual cada propiedad tiene unívocamente asociada su extensión, i.e., el sistema de todas las cosas que poseen la propiedad en cuestión. Como es bien sabido el uso irrestricto de tal principio está en la base de las paradojas conjuntistas. Puesto que el teorema establecido en 59 sólo menciona sistemas, y en 60 Dedekind afirma la "coincidencia completa de la presente formulación del teorema ⟦en términos de propiedades⟧ con la adoptada en 59", cabe inferir que, para Dedekind, no hay ninguna diferencia entre sistema y propiedad, al menos en el sentido de que toda propiedad determina un sistema, su extensión, y cada sistema determina una propiedad, la de pertenecer al sistema en cuestión.

---

60. El teorema anterior constituye, como se mostrará más tarde, el fundamento científico para el tipo de demostración conocido por el nombre de inducción completa (de la inferencia de n a $n+1$), y puede expresarse también del modo siguiente: Para demostrar que todos los elementos de la cadena A_0 poseen una determinada propiedad $\mathfrak{G}$ (o que un teorema $\mathfrak{S}$, en el que se habla de una cosa indeterminada n, vale realmente para todos los elementos n de la cadena A_0), basta con mostrar,

ρ. que todos los elementos a del sistema A poseen la propiedad $\mathfrak{G}$ (o que $\mathfrak{S}$ vale para todos los a), y

σ. que le corresponde la misma propiedad $\mathfrak{G}$ a la imagen n' de cada elemento n de A_0, que posee la propiedad $\mathfrak{G}$ (o que el teorema $\mathfrak{S}$, en tanto que vale para un elemento n de A_0, evidentemente debe valer también para su imagen n'.

De hecho, si se denota con Σ el sistema de todas las cosas que poseen la propiedad $\mathfrak{G}$, (o para los que vale el teorema $\mathfrak{S}$), se manifiesta inmediatamente la completa coincidencia del actual modo de expresión del teorema con el empleado en 59.

61. *Teorema.* La cadena de $\mathfrak{M}(A, B, C \ldots)$ es $\mathfrak{M}(A_0, B_0, C_0 \ldots)$.

Demostración. Si se denota con M el primer sistema, y con K el último, entonces K es por 42 una cadena. Ahora bien, puesto que cada sistema A, B, C ... por 45 es parte de uno de los sistemas A_0, B_0, C_0 ..., con lo que (por 12) tenemos que $M \prec K$, entonces se sigue por 47 también

$$M_0 \prec K.$$

Por otra parte, puesto que por 9 cada uno de los sistemas A, B, C ... es parte de M, y por lo tanto, por 45 y 7, es parte también de la cadena M_0, entonces, cada uno de los sistemas A_0, B_0, C_0 ... debe ser, por 47, parte de M_0, con lo que por 10

$$K \prec M_0,$$

de donde en unión con lo anterior se sigue el teorema a probar $M_0 = K$ (5).

Comentario. [N.T.30] Esta propiedad no se cumple, en general, para las álgebras. Para las álgebras (no necesariamente mono–unarias) lo que tenemos es que, si $(X_i)_{i\in I}$ es una familia no vacía dirigida superiormente de subálgebras de un álgebra $\mathbf{A}$, entonces $\mathrm{Sg}_{\mathbf{A}}(\bigcup_{i\in I} X_i) = \bigcup_{i\in I} \mathrm{Sg}_{\mathbf{A}}(X_i)$.

---

61. *Teorema.* La cadena de $\mathfrak{M}(A, B, C \ldots)$ es $\mathfrak{M}(A_0, B_0, C_0 \ldots)$.

Demostración. Si se denota con M el primer sistema, y con K el último, entonces K es por 42 una cadena. Ahora bien, puesto que cada sistema A, B, C ... por 45 es parte de uno de los sistemas A_0, B_0, C_0 ..., con lo que (por 12) tenemos que $M \prec K$, entonces se sigue por 47 también

$$M_0 \prec K.$$

Por otra parte, puesto que por 9 cada uno de los sistemas A, B, C ... es parte de M, y por lo tanto, por 45 y 7, es parte también de la cadena M_0, entonces, cada uno de los sistemas A_0, B_0, C_0 ... debe ser, por 47, parte de M_0, con lo que por 10

$$K \prec M_0,$$

de donde en unión con lo anterior se sigue el teorema a probar $M_0 = K$ (5).

62. *Teorema.* La cadena de $\mathfrak{G}(A, B, C \ldots)$ es parte de $\mathfrak{G}(A_0, B_0, C_0 \ldots)$.

Demostración. Si se denota con G el primero, y con K el último sistema, entonces K es por 43 una cadena. Ahora bien, puesto que cada uno de los sistemas A_0, B_0, C_0 ... es por 45 todo de uno de los sistemas A, B, C ..., con lo que (por 20), tenemos que $G \prec K$, entonces de sigue de 45 el teorema a probar $G_0 \prec K$.

63. *Teorema.* Si $K' \prec L \prec K$, y por lo tanto también K, es una cadena, entonces L es también una cadena. Si ésta es una parte propia de K, y U el sistema de todos aquellos elementos de K que no están contenidos en L, y además la cadena U_0 es una parte propia de K, y V el sistema de todos aquellos elementos de K que no están contenidos en U_0, entonces tenemos que $K = \mathfrak{M}(U_0, V)$ y $L = \mathfrak{M}(U_0', V)$. Por último, si $L = K'$, entonces tenemos que $V \prec V'$.

La demostración de este teorema, del que no vamos a hacer ningún uso (así como de los dos anteriores), puede dejarse al lector.

§5.

Lo finito y lo infinito.

64. *Definición*[75]. Un sistema S se llama *infinito*, cuando es semejante a una parte propia de sí mismo (32); en caso contrario S se llama un sistema *finito*.

65. *Teorema.* Todo sistema que consiste en un solo elemento es finito.

Demostración. Pues un tal sistema no posee ninguna parte propia (2 y 6).

66. *Teorema.* Existen sistemas infinitos.

Demostración[76]. El mundo de mis pensamientos, es decir, la totalidad S de todas las cosas que pueden ser objeto de mi pensamiento es infinito. De hecho, si s indica un elemento de S, el pensamiento s' de que s puede ser objeto de mi pensamiento es él mismo un elemento de S. Si se considera s' como la imagen $\varphi(s)$ del elemento s, entonces la aplicación φ de S determinada de esa manera tiene la propiedad de que la imagen S' es parte de S; además, S' es parte propia de S, ya que en S hay elementos (e.g., mi propio yo) diferentes de cada pensamiento de la forma s', y por lo tanto no contenido en S'. Por último, está claro que si a y b son elementos distintos de S, entonces las imágenes a' y b' serán diferentes, es decir φ es una aplicación inyectiva. Por consiguiente, S es infinito.

66. *Teorema.* Hay sistemas infinitos.

Demostración[77]. El mundo de mis pensamientos, i.e., la totalidad S de las cosas que pueden ser objeto de mi pensamiento, es infinita. Pues si s significa un elemento de S, entonces el pensamiento s', que puede ser objeto de mi pensamiento, es él mismo un elemento de S. Si se considera a éste como imagen $\varphi(s)$ del elemento s, entonces por esto la aplicación φ de S así determinada tiene la propiedad de que la imagen S' es parte de S; y ciertamente S' es parte propia de S, porque hay elementos en S (p.ej. mi

[75]Si no se quiere usar el concepto de sistemas semejantes(32), entonces debe decirse: S se llama infinito, cuando hay una parte propia de S (6) en el cual S se aplica de manera clara (semejante) (26,36). En esta forma transmití en septiembre de 1882 al señor G. Cantor, y ya varios años antes a los señores Schwarz y Weber la definición de lo infinito, que es el núcleo de toda mi investigación. Todos los intentos que conozco de diferenciar lo infinito y lo finito me parece que están tan poco logrados, que creo poder renunciar a una crítica de los mismos.

[76]Una consideración análoga se encuentra en el §3 de *Paradoxien des Unendlichen*, de B. Bolzano (Leipzig, 1851).

[77]Un tratamiento semejante se encuentra en el §13 de las Paradojas de lo infinito de Bolzano (Leipzig, 1851).

propio yo) que son diferentes de cada uno de estos pensamientos s', y que por ello no están contenidos en S'. Por último, es manifiesto que, si a, b, son diferentes elementos de S, también sus imágenes a', b' son diferentes, y por esto que también la aplicación φ es una aplicación clara (semejante)(26). Con esto, S es infinito, q.e.d.

67. *Teorema.* Si R y S son sistemas semejantes, entonces R es finito o infinito, según que S sea finito infinito.

Demostración. Si S es infinito, y por lo tanto semejante a una parte propia S' de sí mismo, entonces S' debe ser, si R y S son semejantes, por 33 semejante a R y por 35 al mismo tiempo semejante a una parte propia de R, que con esto por 33 es ella misma semejante a R; por lo tanto R es infinito, q.e.d.

68. *Teorema.* Cada sistema S, que posee una parte infinita T, es asimismo infinito; o con otras palabras, cada parte de un sistema finito es finito.

Demostración. Si T es infinito, y hay por tanto una aplicación semejante ψ de T, tal que $\psi(T)$ será una parte propia de T, entonces se puede, si T es parte de S, extender esta aplicación ψ a una aplicación φ de S, en tanto que se establece que, si s se refiere a algún elemento de de S, $\varphi(s) = \psi(s)$, o $\varphi(s) = s$, según sea s elemento de T o no lo sea. Esta aplicación φ es una aplicación semejante; esto es, si a, b, se refieren a elementos diferentes de S, entonces, si éstos están al mismo tiempo contenidos en T, la imagen $\varphi(a) = \psi(a)$ es diferente de la imagen $\varphi(b) = \psi(b)$, porque ψ es una aplicación semejante; si además a está contenido en T, y b no está contenido en T, entonces $\varphi(a) = \psi(a)$ es diferente de $\varphi(b) = \psi(b)$, porque $\psi(a)$ está contenido en T; por último, si ni a ni b están contenidos en T, entonces $\varphi(a) = a$ es asimismo diferente de $\varphi(b) = b$, que era lo que había que mostrar. Puesto que además $\psi(T)$ es parte de T, y por lo tanto también parte de S por 7, entonces es manifiesto que también tenemos que $\varphi(S) \prec S$. Puesto que, por último, $\psi(T)$ es una parte propia de T, hay en T, y por lo tanto también en S, un elemento t que no está contenido en $\psi(T) = \varphi(T)$; ahora bien, puesto que la imagen $\varphi(s)$ es diferente de cada uno de los elementos s no contenidos en T es ella misma sea $= s$, y por lo tanto también es diferente de t, entonces t no puede estar de ninguna manera contenido en $\varphi(S)$, con lo que $\varphi(S)$ es una parte propia de S, y por consiguiente S es infinito, q.e.d.

69. *Teorema.* Cada sistema que es semejante a una parte de un sistema finito, es él mismo finito.

La demostración se sigue de 67 y 68.

70. *Teorema.* Si a es un elemento de S, y el conjunto T de todos los elementos de S diferentes de a es finito, entonces S es también finito.

Demostración. Tenemos que mostrar (por 64), que, si φ se refiere a alguna aplicación semejante de S, la imagen $\varphi(S)$ o S' nunca es una parte propia de S, sino que siempre es $= S$. Es claro que $S = \mathfrak{M}(a, T)$, y por consiguiente, por 23, si se denotan las imágenes de nuevo por acentos, $S' = \mathfrak{M}(a', T')$, y a causa de la semejanza de la aplicación φ, a' no está contenida en T' (26). Puesto que además tenemos por hipótesis que $S' \prec S$, entonces a', e igualmente cada elemento de T', debe, o bien ser $= a$, o bien ser elemento de T. Si por esto, –que es el caso que queremos tratar en primer lugar– a no está contenido en T', entonces debe ser $T' \prec T$, y por consiguiente $T' = T$, porque φ es una

aplicación semejante y porque T es un sistema finito; y puesto que a', como se ha señalado, no está en T', i.e., no está contenido en T, entonces debe ser $a' = a$, y por consiguiente en este caso efectivamente es $S' = S$, como se afirmó. En el caso contrario, si a está contenido en T' y por consiguiente es la imagen b' de un elemento contenido en T, queremos denotar con U el conjunto de todos aquellos elementos u de T que son diferentes de b; entonces tenemos que $T = \mathfrak{M}(b, U)$, y (por 15), $S = \mathfrak{M}(a, b, U)$, y por lo tanto $S' = \mathfrak{M}(a', b, U')$. Determinamos ahora una nueva aplicación ψ de T, en tanto que establecemos que $\psi(b) = a'$, y en general, que $\psi(u) = u'$, por lo que (por 23) tendremos que $\psi(T) = \mathfrak{M}(a', U')$. Evidentemente, ψ es una aplicación semejante, porque φ lo era, y porque a no está contenida en U, y por lo tanto tampoco lo está a' en U'. Puesto que además a, y cada elemento u, es diferente de b, entonces debe (a causa de la semejanza de φ) también a' y todo elemento u' ser diferente de a y por consiguiente estar contenido en T; con esto tenemos que $\psi(T) \prec T$, y puesto que T es finito, entonces debe ser $\psi(T) = T$, y por lo tanto $\mathfrak{M}(a', U') = T$. Pero de aquí se sigue (por 15):

$$\mathfrak{M}(a', a, U') = \mathfrak{M}(a, T),$$

i.e., según lo anterior, $S' = S$. Por lo tanto también en este caso se ha llevado a cabo la demostración requerida.

§6.

Sistemas simplemente infinitos. La sucesión de los números naturales.

71. *Definición.* Un sistema N se dice *simplemente infinito*, si existe una aplicación similar φ de N en sí mismo tal que N resulte la cadena (44) de un elemento no contenido en $\varphi(N)$. Llamamos a este elemento, que en lo que sigue indicamos con el símbolo 1, el *elemento fundamental* de N, y decimos que el sistema simplemente infinito N está *ordenado* por la aplicación φ. Conservando las notaciones precedentes §4 para las imágenes y de las cadenas, podemos decir que la esencia de un sistema N simplemente infinito está caracterizada por la existencia de una aplicación φ de N, y de un elemento 1 que satisfacen las condiciones α, β, γ, δ siguientes:

α. $N' \subseteq N$.
β. $N = 1_0$.
γ. El elemento 1 no está contenido en N'.
δ. La aplicación φ es unívoca.

De α, β, γ, δ se sigue evidentemente que cada sistema N simplemente infinito es de hecho un sistema infinito (64),porque es similar a una parte propia N' de sí mismo.

Comentario. [N.T.31] En un sistema simplemente infinito N hay un único elemento en $N - \varphi(N)$, i.e., para cada $n \in N$, se cumple que $n = 1$ o que $n = \varphi(m)$, para un único $m \in N$. La demostración es por inducción

considerando el conjunto

$$A = \{\, n \in N \mid n = 1 \vee \exists m \in N(n = \varphi(m)) \,\}.$$

Comentar la relación entre la definición axiomática de Dedekind y el sistema de axiomas de Peano.

Cuando dice que "el sistema simplemente infinito N está *ordenado* por la aplicación φ", hay que tener en cuenta que todavía no ha definido un orden sobre N, cosa que hace en la siguiente sección al estipular que $m < n$ precisamente si $n \in \varphi[m_0]$.

---

71. *Definición.* Un sistema N se llama *simplemente infinito*, cuando hay una aplicación φ de N en sí mismo, tal que N aparece como la cadena (44) de un elemento que no está contenido en $\varphi(N)$. Llamamos a ese elemento, que en lo que sigue queremos denotar por medio del símbolo 1, el *elemento fundamental* de N y decimos al mismo tiempo que el sistema N simplemente infinito está ordenado por esa aplicación φ. Si conservamos las cómodas denotaciones anteriores para las imágenes y las cadenas (§4), entonces la esencia de un sistema N simplemente infinito consiste en la existencia de una aplicación φ de N y un elemento 1, que cumplen las siguientes condiciones α, β, γ, δ:

α. $N' \subseteq N$.
β. $N = 1_0$.
γ. El elemento 1 no está contenido en N'.
δ. La aplicación φ es semejante.

Evidentemente se sigue de α, β, γ, δ, que cada sistema simplemente infinito N es efectivamente un sistema infinito (64), porque es semejante a una parte propia N' de sí mimo.

72. *Teorema.* En cada sistema S está contenido un sistema simplemente infinito N como parte.

Demostración. Hay por 64 una aplicación semejante φ tal que $\varphi(S)$ o S' será una parte propia de S; hay por lo tanto un elemento 1 en S, que no está contenido en S'. La cadena $N = 1_0$, que corresponde a esta aplicación φ del sistema S en sí mismo (44) es un sistema simplemente infinito, ordenado por φ; pues evidentemente se cumplen plenamente las condiciones características α, β, γ, δ de 71.

73. *Definición.* Si en la consideración de un sistema N simplemente infinito ordenado por un aplicación φ se prescinde por completo de las características específicas de los elementos, se mantiene fundamentalmente su distinguibilidad y sólo se consideran las relaciones que se establecen mediante la aplicación ordenadora φ, entonces estos elementos se llaman números naturales o números ordinales y también simplemente números, y el elemento fundamental 1 se llama el número fundamental de la sucesión numérica N. Con referencia a esta liberación de los elementos de todo otro contenido (abstracción) se puede denominar con derecho a los números una creación libre del espíritu humano. Las relaciones o leyes, que se derivarán exclusivamente de las condiciones α, β, γ, δ en 71 y que por esto son las mismas siempre en todos los sistemas simplemente infinitos ordenados, sean los que fueren los

nombres dados ocasionalmente a los elementos particulares (cf.134), conforman el objeto inmediato de la ciencia de los números o aritmética. De los conceptos generales y teoremas del §4 sobre la aplicación de un sistema en sí mismo tomamos por de pronto inmediatamente los siguientes teoremas fundamentales, donde se entenderá por a, b,... m, n ... siempre elementos de N, por lo tanto números; por A, B, C,... partes de N; por a', b' ... m', n' ... A', B', C' ... las imágenes correspondientes, que son generadas por la aplicación ordenadora φ y siempre son a su vez elementos o partes de N; la imagen n' de un número n se denominará el número siguiente a n.

74. *Teorema.* Cada número n está contenido por 45 en su cadena n_0, y por 53 la condición $n \prec m_0$ es equivalente a $n_0 \prec m_0$.

75. *Teorema.* Como consecuencia de 57 $n_0' = (n_0)' = (n')_0$.

76. *Teorema.* Como consecuencia de 46 $n_0' \prec n_0$.

77. *Teorema.* Como consecuencia de 58, $n_0 = \mathfrak{M}(n, n_0')$.

78. *Teorema.* Si tenemos $N = \mathfrak{M}(1, N')$, entonces todo número diferente del número fundamental 1 es elemento de N', i.e., es la imagen de un número.

La demostración se sigue de 77 y 71.

79. *Teorema.* N es la única cadena numérica en la está contenido el número fundamental 1.

Demostración. Pues si 1 es elemento de una cadena numérica K, entonces por 47 tenemos que la cadena correspondiente $N \prec K$, por consiguiente $N = K$, porque obviamente $K \prec N$.

80. *Teorema de la inducción completa* (inferencia de n a n'). Para demostrar que un teorema vale para todos los números n de una cadena m_0, basta con mostrar,

ρ. que vale para $n = m$, y

σ. que de la validez del teorema para un número n de la cadena m_0 se sigue siempre su validez para el número siguiente n'.

Esto se sigue directamente de los teoremas más generales 59 o 60. Muy frecuentemente tendrá lugar el caso en que $m = 1$, y por lo tanto m_0.

§7.

Números mayores y menores.

81. *Teorema.* Todo número n es diferente del número que le sigue n'.

Demostración por inducción completa (80). Pues

ρ. el teorema es válido para el número $n = 1$, porque no está contenido en N' (71), mientras que el número siguiente $1'$ como imagen del número 1 contenido en N es elemento de N'.

σ. Si el teorema es válido para un número n, y se establece que el número siguiente $n' = p$, entonces n es diferente de p, de donde por 26 a causa de la semejanza (71) de la aplicación ordenada φ se sigue que n', y por tanto que p es diferente de p'. Con esto vale el teorema también para el número p que sigue a n, q.e.d.

82. *Teorema.* En la cadena imagen n_0' de un número n está contenida ciertamente su imagen n', pero no el número n mismo.

Demostración por inducción completa (80). Pues

ρ. el teorema es verdadero para $n = 1$, porque $1'_0 = N$, y porque por 71 el número fundamental 1 no está contenido en N'.

σ. Si el teorema es válido para un número n, y se establece a su vez que $n' = p$, entonces n no está contenido en p_0, por lo tanto es diferente de cada número q contenido en p_0, de donde a causa de la semejanza de φ se sigue que n', y por lo tanto p es diferente de cada número q' contenido en p'_0, y por lo tanto no está contenido en p'_0. Con esto vale el teorema también para el número p siguiente a n, q.e.d.

83. *Teorema.* La cadena n'_0 es parte propia de la cadena n_0.

La demostración se sigue de 76, 74 y 82.

84. *Teorema.* De $m_0 = n_0$ se sigue que $m = n$.

Demostración. Pues (por 74) m está contenido en m_0, y tenemos (77)

$$m_0 = n_0 = \mathfrak{M}(n, n'_0)$$

entonces, si el teorema fuera falso, y por lo tanto m fuera diferente de n, m debería estar contenido en la cadena n'_0, por consiguiente por 74 también $m_0 \prec n'_0$, i.e $n_0 \prec n'_0$; puesto que esto contradice al teorema 83, queda probado nuestro teorema.

85. *Teorema.* Si el número n no está contenido en la cadena numérica K, entonces tenemos que $K \prec n'_0$.

Demostración por inducción completa (80). Pues

ρ. el teorema es por 78 verdadero para $n = 1$.

σ. Si el teorema es verdadero para un número n, entonces vale también para el número siguiente $p = n'$; pues si p no está contenido en la cadena numérica K, entonces n no puede tampoco por 40 estar contenido en K y por consiguiente tenemos de acuerdo con nuestra suposición que $K \prec n'_0$; ahora bien, puesto que (por 77) $n'_0 = p_0 = \mathfrak{M}(p, p'_0)$, y por lo tanto $K \prec \mathfrak{M}(p, p'_0)$, y p no está contenido en K, entonces debe darse $K \prec p'_0$, q.e.d.

86. *Teorema.* si el número n no está contenido en la cadena numérica K, pero sí su imagen n', entonces tenemos que $K = n'_0$.

Demostración. Puesto que n no está contenido en K, tenemos (por 85) $K \prec n'_0$, y puesto que $n \prec K$, entonces tenemos también por 47 que $n'_0 \prec K$, y por consiguiente $K = n'_0$,q.e.d.

87. *Teorema.* En cada cadena numérica K hay uno y solo un número (por 84) k, cuya cadena $k_0 = K$.

Demostración. Si el número fundamental 1 está contenido en K, entonces, tenemos (por 79), $K = N = 1_0$. En caso contrario sea Z el sistema de todos los números no contenidos en K; puesto que el número 1 está contenido en Z, pero Z es sólo una parte propia de la sucesión numérica N, entonces Z no puede (por 79) ser ninguna cadena, i.e., Z' no puede ser parte de Z; a partir de aquí hay en Z un número n, cuya imagen n' no está contenida en Z, por lo tanto [tampoco] ciertamente en K; puesto que además n está contenida en Z, y por lo tanto no en K, entonces tenemos (por 86) $K = n'_0$, y por lo tanto $k = n'$,q.e.d.

88. *Teorema.* Si m, n, son números diferentes, una y sólo una (por 83 y 84) de las cadenas m_0, n_0 es parte propia de la otra, y ciertamente o bien tenemos $n_0 \prec m'_0$, o bien $m_0 \prec n'_0$.

Demostración. Si n está contenida en m_0, entonces por 74 también $n_0 \prec m_0$, entonces m no puede estar contenido en la cadena n_0 (porque si no por

74 también $m_0 \prec n_0$, por lo tanto $m_0 = n_0$, con lo que por 84 también tendríamos que $m = n$, y de aquí se sigue por 85, que $n_0 \prec m'_0$. En caso contrario, si n no está contenido en la cadena m_0, debe darse (por 85) $m_0 \prec n'_0$,q.e.d.

89. *Teorema.* El número m se llama menor que el número n, y al mismo tiempo el número n se llama mayor que m, en signos,

$$m < n \quad \text{y} \quad n > m,$$

si la condición

$$n_0 \prec m'_0$$

se cumple, la cual puede expresarse por 74 por medio de

$$n \prec m'_0.$$

90 *Teorema.* Si m, n, son cualesquiera números, entonces tiene lugar siempre uno y sólo uno de los casos siguientes, λ, μ, ν:

λ. $m = n$, $n = m$, i.e. $m_0 = n_0$,
μ. $m < n$, $n > m$, i.e. $n_0 \prec m'_0$,
ν. $m > n$, $n < m$, i.e. $m_0 \prec n'_0$.

Demostración. Pues si λ es el caso(84), entonces no pueden darse ni μ ni ν, porque por 83 nunca tenemos que $n_0 \prec n'_0$. Pero si λ no es el caso, entonces se da por 88 uno y sólo uno de los casos μ, ν, q.e.d.

91. *Teorema.* $n < n'$.

Demostración. Pues la condición para el caso ν en 90 se cumplirá por $m = n'$.

92. *Definición.* Para expresar, que m es o bien $= n$, o bien $< n$; por lo tanto no $> n$, se emplea la denotación

$$m \leq n \quad \text{o también} \quad n \geq m,$$

y se dice que m sería como mucho igual a n, y n sería al menos igual a m.

93. *Teorema.* Cada una de las condiciones

$$m \leq n,\ m < n',\ n_0 \prec m_0$$

es equivalente a cada una de las otras.

Demostración. Pues is $m \leq n$, entonces se sigue de λ, μ en 90 siempre $n_0 \prec m_0$, porque (por 76), tenemos que $m'_0 \prec m_0$. Por el contrario, si $n_0 \prec m_0$, por tanto por 74 tenemos también que $n \prec m_0$, entonces se sigue de $m_0 = \mathfrak{M}(m, m'_0)$, que o bien $n = m$, o bien $n \prec m'_0$, i.e. que $n > m$. Con esto la condición $m \leq n$ es equivalente a $n_0 \prec m_0$. Además se sigue de 22, 27 y 75 que esta condición $n_0 \prec m_0$ es a su vez equivalente a $n'_0 \prec m'_0$, i.e., (por μ en 90), a $m < n'$,q.e.d.

94. *Teorema.* Cada una de las condiciones $m' \leq n$, $m' < n'$, $m < n$ es equivalente a cada una de las otras.

La demostración se sigue directamente de 93, si se cambia allí m por m', y de μ en 90.

95. *Teorema.* Si $l < m$ y $m \leq n$, o si $l \leq m$ y $m < n$, entonces tenemos que $l < n$. Pero si $l \leq m$ y $m \leq n$, entonces tenemos que $l \leq n$.

Demostración. Pues de las condiciones (por 89 y 93) $m' \prec l'_0$ y $n_0 \prec m_0$ se sigue (por 7) $n_0 \prec l'_0$, y lo mismo se sigue de las condiciones $m_0 \prec l_0$

y $n_0 \prec m'_0$, porque a consecuencia de las primeras también tenemos que $m'_0 \prec l'_0$. Por último, de $m_0 \prec l_0$ y $n_0 \prec m_0$ se sigue también $n_0 \prec l_0$, q.e.d.

96. *Teorema.* En cada parte T de N hay un y sólo un número mínimo k, i.e., un número k, que es más pequeño que cada uno de los otros números contenidos en T. Si T consiste en un solo número, éste es también el número más pequeño en T.

Demostración. Puesto que T_0 es una cadena (44) hay por 87 un número k, cuya cadena $k_0 = T_0$. Puesto que de aquí (por 45 y 77) se sigue que $T \prec \mathfrak{M}(k, k'_0)$, entonces debe en primer lugar la misma estar contenida en T (porque si no $T \prec k'_0$, por tanto por 47 también $T_0 \prec k'_0$, i.e, tendríamos que $k_0 \prec k'_0$, lo que es imposible por 83), y además cada número del sistema T diferente de k debe estar contenido en k'_0, ie. ser $> k$ (89), de donde se sigue inmediatamente por 90, que sólo hay un número en T que sea el mínimo, q.e.d.

97. *Teorema.* El número mínimo de la cadena n_0 es n, y el número fundamental es el más pequeño de todos los números.

Demostración. Pues por 74 y 93 la condición $m \prec n_0$ es equivalente a $m \leq n$. O se sigue nuestro teorema también directamente de la demostración del anterior teorema, porque, si allí mismo se denomina $T = n_0$, evidentemente será $k = n$ (51).

98.*Definición.* Si n es un número cualquiera, entonces queremos denotar con Z_n el sistema de todos los números que no son mayores que n, y por lo tanto no están contenidos en n'_0. La condición

$$m \prec Z_n$$

es por 92 y 93 evidentemente equivalente a cada una de las siguientes condiciones:

$$m \leq n,\ m < n',\ n_0 \prec m_0.$$

99. *Teorema.* $1 \prec Z_n$ y $n \prec Z_n$. La demostración se sigue de 98 o también de 71 y 82.

100. *Teorema.* Cada una de las condiciones equivalentes por 98

$$m \prec Z_n,\ m \leq n,\ m < n',\ n_0 \prec m_0$$

es también equivalente a la condición

$$Z_m \prec Z_n.$$

Demostración. Pues si $m \prec Z_n$, y por tanto $m \leq n$, y si $l \prec Z_m$, entonces por 95 también es $l \leq n$, i.e., $l \prec Z_n$; si también $m \prec Z_n$, entonces cada elemento l del sistema Z_m es también elemento de Z_n, i.e., $Z_m \prec Z_n$. Al contrario, si $Z_m \prec Z_n$, entonces debe por 7 también darse $m \prec Z_n$, porque (por 99) tenemos que $m \prec Z_n$, q.e.d.

101. *Teorema.* Las condiciones para los casos λ, μ, ν en 90 se pueden representar también del siguiente modo:

λ. $m = n$, $n = m$, $Z_m = Z_n$,
μ. $m < n$, $n > m$, $Z_{m'} \prec Z_n$,
ν. $m > n$, $n < m$, $Z_{n'} \prec Z_m$.

La demostración se sigue directamente de 90, si se piensa que por 100 las condiciones $n_0 \prec m_0$ y $Z_m \prec Z_n$ son equivalentes.

102. *Teorema.* $Z_1 = 1$.

Demostración. Pues el número fundamental 1 está contenido en Z_1 por 99, y cada número diferente de 1 lo está por 78 en $1'_0$, por tanto por 98 no en Z_1, q.e.d.

103. *Teorema.* A consecuencia de 98 $N = \mathfrak{M}(Z_n, n'_0)$.

104. *Teorema.* $n = \mathfrak{G}(Z_n, n_0)$, i.e., n es el único elemento común de los sistemas Z_n y n_0.

Demostración. De 99 y 74 se sigue que n está contenido en Z_n y en n_0; pero cada elemento de la cadena n_0 diferente de n está contenido por 77 en n'_0, por lo tanto por 98 no en Z_n, q.e.d.

105. *Teorema.* A consecuencia de 91 y 98 el número n' no está contenido en Z_n.

106. *Teorema.* Si $m < n$, entonces Z_m es parte propia de Z_n, y viceversa.

Demostración. Si $m < n$, entonces (por 100) $Z_m \prec Z_n$, y por lo tanto el número n contenido en Z_n por 99 no puede estar contenido en Z_m por 98, porque $n < m$, y entonces Z_m es parte propia de Z_n. Viceversa, si Z_m es parte propia de Z_n, entonces (por 100) $m \leq n$, y puesto que no puede ser $m = n$, porque si no también sería $Z_m = Z_n$, entonces debe ser $m < n$, q.e.d.

107. *Teorema.* Z_n es parte propia de $Z_{n'}$. La demostración se sigue de 106, porque (por 91, $n < n'$.

108. *Teorema.* $Z_n = \mathfrak{M}(Z_n, n')$.

Demostración. Pues todo número contenido en $Z_{n'}$ es (por 98) $\leq n'$, y por lo tanto o bien $= n'$, o bien $< n'$, y por consiguiente por 98 elemento de Z_n; con esto es obviamente $Z_{n'} \prec \mathfrak{M}(Z_n, n')$. Puesto que viceversa (por 107) $Z_n \prec Z_{n'}$, y (por 99) $n' \prec Z_{n'}$, entonces se sigue (por 10): $\mathfrak{M}(Z_n, n') \prec Z_n$, De donde se obtiene nuestro teorema por 5.

109. *Teorema.* La imagen Z'_n del sistema Z_n es parte propia del sistema $Z_{n'}$.

Demostración. Pues cada número contenido en Z'_n es la imagen m' de un número m contenido en Z_n, y puesto que $m \leq n$, y por tanto (por 94) $m' \leq n'$, entonces se sigue (por 98), que $Z'_n \prec Z_{n'}$. Puesto que además el número 1 por 99 puede estar contenido en $Z_{n'}$, pero no puede estarlo en Z'_n, entonces, Z'_n es parte propia de $Z_{n'}$, q.e.d.

110. *Teorema.* $Z_{n'} = \mathfrak{M}(1, Z'_n)$.

Demostración. Cada número diferente de 1 del sistema $Z_{n'}$, es por 78 la imagen de un número m, y éste debe ser $\leq n$, por lo tanto por 98 debe estar contenido en Z_n (porque si no $m > n$, por tanto por 94 también $m' > n'$, con lo que m' por 98 no estaría contenido en $Z_{n'}$); pero de $m \prec Z_n$ se sigue que $m' \prec Z'_n$, y por consiguiente, evidentemente,

$$Z_{n'} \prec \mathfrak{M}(1, Z'_n).$$

Puesto que, viceversa (por 99) $1 \prec Z_{n'}$, entonces se sigue $\mathfrak{M}(1, Z'_n) \prec Z_{n'}$ (por 10), y de aquí se obtiene nuestro teorema por 5.

111. *Definición.* Si hay un elemento g en un sistema E de números, que es mayor que cada uno de los otros números en E, entonces g se llama el número *máximo* del sistema E, y evidentemente puede por 90 haber sólo un número de este tipo. Si un sistema consiste en un solo número, entonces es éste mismo el número máximo del sistema.

112. *Teorema.* A consecuencia de 98 n es el número máximo del sistema Z_n.

113. *Teorema.* Si hay en E un número mayor g, entonces $E \prec Z_g$.

Demostración. Pues cada número contenido en E es $\leq g$, con lo que por 98 está contenido en Z_g, q.e.d.

114. *Teorema.* Si E es parte de un sistema Z_n, o hay, lo que quiere decir lo mismo, un número n tal que todos los números contenidos en E son $\leq n$, entonces E posee un número máximo g.

Demostración. El sistema de todos los números p, que satisfacen la condición $E \prec Z_p$ – y según nuestra suposición hay tales números – es una cadena (37), porque por 107 y 7 se sigue también $E \prec Z_{p'}$, y por esto es (por 87) $= g_0$, donde g significa el número mínimo (96 y 97). Desde aquí tenemos también que $E \prec Z_g$, y por consiguiente (98), cada número contenido en E es $\leq g$, y sólo nos queda probar todavía que el número g mismo está contenido en E. Esto es inmediatamente manifiesto si $g = 1$, porque entonces (por 102) Z_g y por consiguiente también E consisten sólo en el número 1. Pero si g es diferente de 1 y por consiguiente por 78 la imagen f' de un número f, entonces debería darse que $E \prec Z$, y habría por lo tanto entre los números p un número f, que (por 91) es $< g$, lo que contradice lo anterior; con lo que g está contenido en E, q.e.d.

115. *Definición.* Si $l < m$ y $m < n$, decimos que el número m se *encuentra entre* l y n (y también entre n y l).

116. *Teorema.* No hay ningún número que se encuentre entre n y n'.

Demostración. Pues al ser $m < n'$, también (93), es $m \leq n$, luego no puede por 90 ser $n < m$, q.e.d.

117. *Teorema.* Si t es un número en T, pero no el mínimo (96), entonces hay en T uno y sólo un número menor siguiente s, i.e., un ´número s tal que $s < t$, y tal que no hay en T ningún número que se encuentre entre s y t. Asimismo hay, si t no es en general el número máximo en T (111), siempre uno y sólo un siguiente número mayor u en T, i.e., un número u tal que $t < u$, y tal que en T no hay ningún número que se encuentre entre t y u. Al mismo tiempo t es el siguiente mayor que s y el siguiente menor que u en T.

Demostración. Si t no es el número mínimo en T, entonces sea E el sistema de todos los números de T, que son $< t$; entonces (por 98) tenemos que $E \prec Z$, y por consiguiente hay en E un número máximo s, que evidentemente posee las propiedades indicadas en el teorema y es también el único número de este tipo. Si además t no es el número máximo en T, entonces hay por 96 entre todos los números de T que son $> t$, sin duda uno mínimo u que, y ciertamente sólo él, posee las propiedades indicadas en el teorema. Del mismo modo es manifiesta la corrección de la conclusión del teorema.

118. *Teorema.* El número n' es el siguiente mayor que n en N, y n el siguiente menor que n'.

La demostración se sigue de 116 y 117.

§8.

Partes finitas e infinitas de la sucesión numérica.

119. *Teorema.* Todo sistema Z_n en 98 es finito.

Demostración por inducción completa (80). Pues

ρ. El teorema es válido para $n = 1$ a consecuencia de 65 y 102.

σ Si Z_n es finito, entonces se sigue de 108 y 70, que también $Z_{n'}$ es finito, q.e.d.

120. *Teorema.* Si m, n son números diferentes, entonces Z_m, Z_n son sistemas desemejantes.

Demostración. A causa de la simetría podemos suponer por 90, que sea $m < n$; entonces Z_m es por 106 parte propia de Z_n, y puesto que Z_n es por 119 finito, entonces Z_m y Z_n no pueden (por 64) ser semejantes., q.e.d.

121. *Teorema.* Cada parte E de la sucesión numérica N, que tiene un número máximo (111) es finita.

La demostración se sigue de 113, 119 y 68.

122. *Teorema.* Cada parte U de la sucesión numérica N, que no tienen ningún número máximo, es simplemente infinita (71).

Demostración. Si u es un número cualquiera en U, entonces hay por 117 uno y sólo un número siguiente mayor que u en U, que denotamos con $\psi(u)$ y que queremos considerar como imagen de u. La aplicación completamente determinada a partir de esto y del sistema U tiene claramente la propiedad

$$\alpha.\ \psi(U) \prec U,$$

i.e., U es aplicado por ψ en sí mismo. Si además u, v, son números diferentes en U, entonces podemos a causa de la simetría por 90 suponer, que sea $u < v$; entonces se sigue por 117 de la definición de *psi*, que $\psi(u) \leq v$ y que $v < \psi(v)$, por tanto, (por 95), $\psi(u) < \psi(v)$ con lo que por 90 las imágenes $\psi(u)$ y $\psi(v)$ son diferentes, i.e.

$$\delta.\ \text{La aplicación } \psi \text{ es semejante .}$$

Además, si u_1 se refiere al número mínimo (96) del sistema U, entonces cada número contenido en U es $u \geq u_1$, y puesto que en general $u < \psi(u)$, entonces (por 95) es $u_1 < \psi(u)$, y por lo tanto u_1 es por 90 diferente de $\psi(u)$, i.e.,

$$\gamma.\ \text{el elemento } u_1 \text{ de } U \text{ no está contenido en } \psi(U).$$

Con esto $\psi(U)$ es una parte propia de U y por consiguiente U es por 64 un sistema infinito. Si denotamos ahora de acuerdo con 44, cuando V es una parte cualquiera de U, con $\psi_0(V)$ la cadena de V correspondiente a la aplicación ψ, entonces queremos por último mostrar que

$$\beta.\ U = \psi_0(u_1).$$

De hecho, puesto que cada cadena $\psi_0(V)$ de este tipo en virtud de su definición (44) es una parte del sistema U aplicado por ψ en sí mismo, entonces por descontado $\psi_0(u_1) \prec U$, y viceversa, es manifiesto en primer lugar que el elemento u_1 está desde luego contenido en $\psi_0(u_1)$; pero si suponemos, que hubiera elementos en U que no están contenidos en $\psi_0(u_1)$, entonces debe haber entre ellos por 96 un número mínimo w, y puesto que éste por lo ya dicho es diferente del número mínimo u_1 del sistema U, entonces debe haber por 117 también un número v en U, que es el siguiente más pequeño que w, de donde se sigue inmediatamente, que $w = \psi(v)$; puesto que ahora $v < w$,

entonces, como consecuencia de la definición de w, v debe estar, desde luego, contenido en $\psi_0(u_1)$; pero de aquí se sigue por 55, que también $\psi(v)$, y por lo tanto w debe estar contenido en $\psi_0(u_1)$, y puesto que esto está en contradicción con la definición de w, entonces nuestra suposición anterior es inadmisible; con esto tenemos que $U \prec \psi_0(u_1)$ y por consiguiente también que $U = \psi_0(u_1)$, como se afirmó. Ahora, de α, β, γ, δ se sigue por 71, que U es un sistema simplemente infinito ordenado por ψ, q.e.d.

123. *Teorema.* Como consecuencia de 121 y 122 cualquier parte T de la sucesión numérica N es finita o simplemente infinita, según que haya en T un número máximo o no.

§9.

Definición de una aplicación de la sucesión numérica por inducción.

124. Denotamos también en lo que sigue los números con letras latinas minúsculas y conservamos en general todas las denotaciones de los previos §6 a §8, mientras que Ω denota un sistema cualquiera, cuyos elementos no tienen por que estar contenidos necesariamente en N.

125. *Teorema.* Dada una aplicación cualquiera (semejante o desemejante) θ de un sistema Ω en sí mismo, y además dado un elemento determinado ω en Ω, entonces corresponde a cada número n una y sólo una aplicación ψ_n del correspondiente sistema Z_n, definido en 98, que cumple las condiciones[78]

I. $\psi_n(Z_n) \prec \Omega$,
II. $\psi_n(1) = \omega$,
III. $\psi_n(t') = \theta\psi_n(t)$, si $t < n$, donde la expresión $\theta\psi_n$ tiene el significado indicado en 25.

Demostración por inducción completa (80). Pues

ρ. El teorema es verdadero para $n = 1$. En este caso el sistema Z_n consiste sólo en el número 1, por 102, y la aplicación ψ_1 está por lo tanto ya definida por II completamente, y de tal modo, que, I se cumple, mientras que III no se aplica en absoluto.

σ. Si el teorema es verdadero para un número n, entonces comenzamos con la indicación de que sólo puede haber una única aplicación ψ_p correspondiente al sistema Z_p. De hecho, una aplicación ψ_p cumple las condiciones

I′. $\psi_p(Z_p) \prec \Omega$,
II′. $\psi_p(1) = \omega$,
III′. $\psi_p(m') = \theta\psi_p(m)$, si $m < p$, entonces por 21, puesto que $Z_n \prec Z_p$ (107), está contenida en ella una aplicación de Z_n, que claramente cumple como ψ_n las mismas condiciones I, II y III, y por consiguiente coincide por completo con ψ_n; para todos los números contenidos en Z_n, y por lo tanto (98) para todos los números m, que son $< p$, i.e., $\leq n$, debe ser

$$(m) \qquad \psi_p(m) = \psi_n(m)$$

[78]Por mor de la claridad he introducido intencionadamente aquí y en el siguiente Teorema 126 la condición I, aunque ésta es estrictamente ya una consecuencia de II y III.

de donde se sigue también como caso particular

$$(n) \qquad \psi_p(n) = \psi_n(n),$$

puesto que además p es por 105 y 108 el único número del sistema Z_p no contenido en Z_n, puesto que por III′ y (n) también debe ser

$$(p) \qquad \psi_p(p) = \theta\psi_n(n),$$

se confirma así la corrección de nuestra afirmación anterior de que sólo puede haber una única aplicación ψ_p del sistema Z_p que cumpla las condiciones I', II′ y III′, porque se retrotrae completamente a ψ_n por las condiciones ya deducidas (m) y (p). Tenemos que mostrar ahora que viceversa esta aplicación ψ_p del sistema Z_p, completamente determinada por (m) y (p), cumple de hecho las condiciones I′, II′ y III′. Evidentemente I′, se obtiene de (m) y (p) considerando I, y porque $\theta(\Omega) \prec \Omega$. Asimismo, II′, se sigue de (m) y II, porque el número 1 está contenido por 99 en Z_n. La corrección deIII′, se sigue en primer lugar para aquellos números m que son $< n$, de (m) y III, y para el único número restante $m = n$ se obtiene de (p) y (n). Con esto se ha demostrado completamente que de la validez de nuestro teorema para el número n se sigue siempre también su validez para el número siguiente p, q.e.d.

126. *Teorema de la definición por inducción.* Dados una aplicación arbitraria θ (semejante o desemejante) de un sistema Ω en sí mismo y además un determinado elemento ω en Ω, entonces hay una y sólo una aplicación ψ de la sucesión numérica N que cumple las condiciones

I. $\psi(N) \prec \Omega$,
II. $\psi(1) = \omega$,
III. $\psi(n') = \theta\psi(n)$, donde n significa todo número.

Demostración. Pues, si en efecto hay una tal aplicación ψ, en ella está contenida por 21 también una aplicación ψ_n del sistema Z_n, que cumple las condiciones I, II, III, indicadas en 125, entonces puesto que siempre hay una y sólo una aplicación ψ_n de este tipo, necesariamente debe darse que

$$(n) \qquad \psi(n) = \psi_n(n)$$

Puesto que por ello ψ está completamente determinada, entonces se sigue también que sólo puede haber una aplicación ψ de este tipo (cf. la conclusión de 130). Que, viceversa, la aplicación ψ determinada por (n) también cumple nuestras condiciones I, II, III, se sigue con facilidad de (n) atendiendo a las propiedades I, II y (p) demostradas en 125, q.e.d.

Comentario. [N.T.32] La estrategia seguida por Dedekind para demostrar el principio de la definición por recursión finita es digna de que se la reconsidere en profundidad porque, analizada desde el punto de vista actual, involucra el concepto de sistema inductivo y el de límite inductivo. En primer lugar, el conjunto $\mathbb{N}$ de los números naturales es el límite inductivo de un cierto sistema inductivo. Por otra parte, el Teorema 125 determina un sistema inductivo y, por último, el Teorema 126 demuestra que existe una única aplicación del límite inductivo mencionado en el conjunto subyacente del

último sistema inductivo. Todo esto hay que escribirlo bien recordando los conceptos que intervienen y especificando lo anterior.

Definición 0.1. Un *sistema inductivo de conjuntos* es un par ordenado $(\mathbf{S}, \mathcal{A})$ en el que $\mathbf{S}$ es un conjunto preordenado y $\mathcal{A} = ((A_s)_{s\in S}, (a_{s,s'})_{(s,s')\in\preceq})$ tal que:

1. Para cada $(s, s') \in \preceq$, $a_{s,s'} \colon A_s \longrightarrow A_{s'}$.
2. Para cada $s \in S$, $a_{s,s} = \mathrm{id}_{A_s}$.
3. Para cada $s, s', s'' \in S$, si $(s, s') \in \preceq$ y $(s', s'') \in \preceq$, entonces el diagrama:

$$\begin{array}{ccc} A_s & \xrightarrow{a_{s,s'}} & A_{s'} \\ & \searrow^{a_{s,s''}} & \downarrow{\scriptstyle a_{s',s''}} \\ & & A_{s''}, \end{array}$$

   conmuta.

A las aplicaciones $a_{s,s'} \colon A_s \longrightarrow A_{s'}$ las denominamos las *aplicaciones de transición* del sistema inductivo de conjuntos $(\mathbf{S}, \mathcal{A})$.

Proposición 0.2. *Sea $(\mathbf{S}, \mathcal{A})$ un sistema inductivo de conjuntos. Entonces hay un par ordenado $(\varinjlim(\mathbf{S}, \mathcal{A}), (a_s)_{s\in S})$, el* límite inductivo *del sistema inductivo $(\mathbf{S}, \mathcal{A})$, en el que $\varinjlim(\mathbf{S}, \mathcal{A})$ es un conjunto y, para cada $s \in S$, a_s, la* inclusión canónica *s-ésima, es una aplicación de A_s en $\varinjlim(\mathbf{S}, \mathcal{A})$, tal que:*

1. *Para cada $(s, s') \in \preceq$, el diagrama:*

$$\begin{array}{ccc} A_s & \xrightarrow{a_{s,s'}} & A_{s'} \\ & \searrow_{a_s} \quad \swarrow_{a_{s'}} & \\ & \varinjlim(\mathbf{S}, \mathcal{A}) & \end{array}$$

   conmuta.
2. *Para cada par ordenado $(L, (l_s)_{s\in S})$ en el que, para cada $s \in S$, $l_s \colon A_s \longrightarrow L$, si, para cada $(s, s') \in \preceq$, el diagrama:*

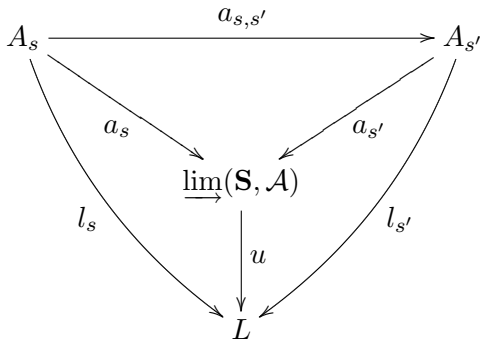
$$\begin{array}{ccc} A_s & \xrightarrow{a_{s,s'}} & A_{s'} \\ & \searrow_{l_s} \quad \swarrow_{l_{s'}} & \\ & L & \end{array}$$

   conmuta, entonces hay una única aplicación $u \colon \varinjlim(\mathbf{S}, \mathcal{A}) \longrightarrow L$ tal que, para cada $s \in S$, el diagrama:

$$\begin{array}{ccc} A_s & \xrightarrow{a_s} & \varinjlim(\mathbf{S}, \mathcal{A}) \\ & \searrow^{l_s} & \downarrow{\scriptstyle u} \\ & & L \end{array}$$

conmuta.

La situación descrita por las condiciones anteriores la expresamos diagramáticamente como:



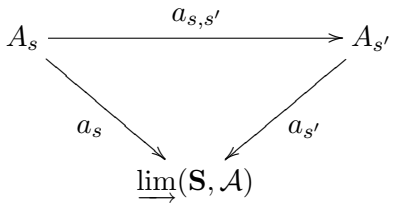
Demostración. Sea $R_{(\mathbf{S},\mathcal{A})}$ la mínima relación de equivalencia sobre $\coprod_{s\in S} A_s$ que contiene a todos los pares ordenados de $\coprod_{s\in S} A_s$ de la forma

$$((x,s),(a_{s,s'}(x),s')),\ \text{con } x\in A_s \text{ y } (s,s')\in\preceq,$$

de modo que $R_{(\mathbf{S},\mathcal{A})}$ es, por definición, precisamente:

$$\mathrm{Eg}_{\coprod_{s\in S} A_s}\big(\bigcup_{(s,s')\in\preceq}\{\,((x,s),(a_{s,s'}(x),s'))\in\big(\coprod_{s\in S} A_s\big)^2 \mid x\in A_s\,\}\big).$$

Sea $\varinjlim(\mathbf{S},\mathcal{A})$ el conjunto cociente $\coprod_{s\in S} A_s/R_{(\mathbf{S},\mathcal{A})}$ y, para cada $s\in S$, sea a_s la composición de in_s y de $\mathrm{pr}_{R_{(\mathbf{S},\mathcal{A})}}$, de manera que, para cada $s\in S$, a_s es la aplicación de A_s en $\varinjlim(\mathbf{S},\mathcal{A})$ que a un $x\in A_s$ le asigna la clase de equivalencia $[(x,s)]_{R_{(\mathbf{S},\mathcal{A})}}$. Entonces el par ordenado $(\varinjlim(\mathbf{S},\mathcal{A}),(a_s)_{s\in S})$ cumple las condiciones de la proposición. En efecto, por una parte, para cada $(s,s')\in\preceq$, el diagrama:

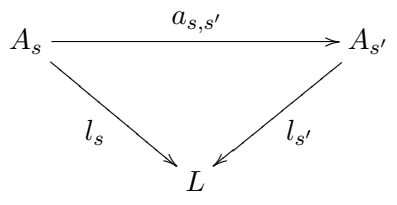


conmuta, i.e., para cada $x\in A_s$, se cumple que

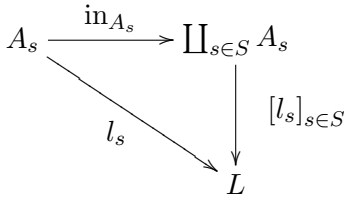
$$[(x,s)]_{R_{(\mathbf{S},\mathcal{A})}}=[(a_{s,s'}(x),s')]_{R_{(\mathbf{S},\mathcal{A})}},$$

por definición de $R_{(\mathbf{S},\mathcal{A})}$

Por otra parte, si un par ordenado $(L,(l_s)_{s\in S})$, arbitrario, pero fijo, en el que, para cada $s\in S$, $l_s\colon A_s\longrightarrow L$, es tal que, para cada $(s,s')\in\preceq$, el diagrama:



conmuta, entonces, en virtud de la propiedad universal del coproducto, hay una única aplicación $[l_s]_{s\in S} : \coprod_{s\in S} A_s \longrightarrow L$ tal que el diagrama:

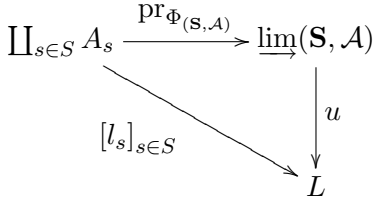


conmuta.

Además, se cumple que $R_{(\mathbf{S},\mathcal{A})} \subseteq \mathrm{Ker}([l_s]_{s\in S})$, porque, por una parte, $R_{(\mathbf{S},\mathcal{A})}$ es la mínima relación de equivalencia sobre $\coprod_{s\in S} A_s$ que contiene a

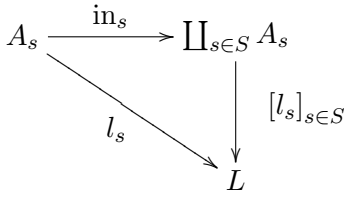
$$\bigcup_{(s,s')\in\preceq}\{\,((x,s),(a_{s,s'}(x),s')) \in \big(\coprod_{s\in S} A_s\big)^2 \mid x \in A_s\,\}$$

y, por otra, porque $\mathrm{Ker}([l_s]_{s\in S})$ es una relación de equivalencia sobre $\coprod_{s\in S} A_s$ que contiene a $\bigcup_{(s,s')\in\preceq}\{\,((x,s),(a_{s,s'}(x),s')) \in \big(\coprod_{s\in S} A_s\big)^2 \mid x \in A_s\,\}$. Entonces, en virtud de la propiedad universal del cociente, podemos afirmar que existe una única aplicación $u\colon \varinjlim(\mathbf{S},\mathcal{A}) \longrightarrow L$ tal que el diagrama:

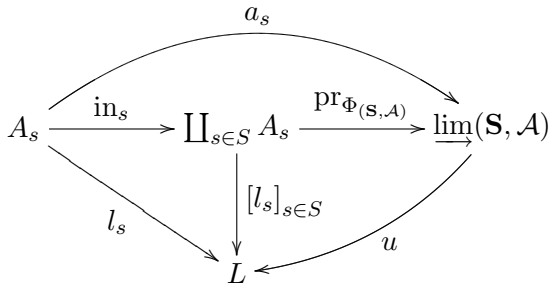


conmuta.

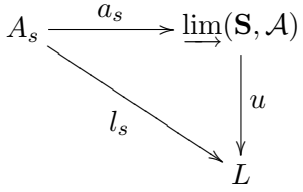
Ahora bien, puesto que, para cada $s \in S$, el diagrama:



conmuta, también, para cada $s \in S$, el diagrama:



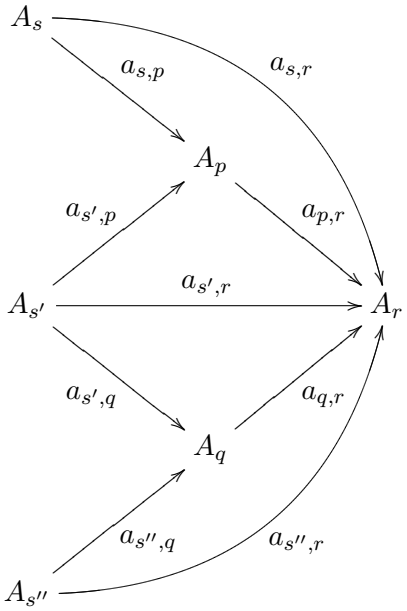
conmuta. Por consiguiente hay al menos una aplicación u de $\varinjlim(\mathbf{S}, \mathcal{A})$ en L tal que, para cada $s \in S$, el diagrama:



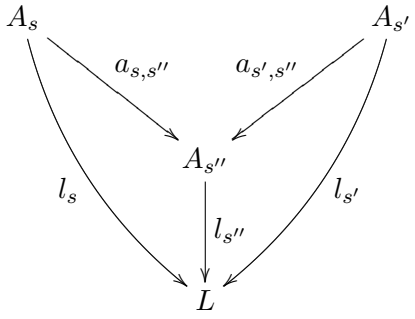
conmuta. Dejamos, como ejercicio, la demostración de que hay a lo sumo una aplicación u de $\varinjlim(\mathbf{S}, \mathcal{A})$ en L tal que, para cada $s \in S$, $u \circ a_s = l_s$.

□

La relación $\Phi_{(\mathbf{S},\mathcal{A})}$ es una relación de equivalencia sobre $\coprod_{s\in S} A_s$. Puesto que la reflexividad y la simetría son sencillas de demostrar, nos limitamos a bosquejar la transitividad. Para ello, dados $(x, s), (y, s'), (z, s'') \in \coprod_{s\in S} A_s$, es suficiente tener en cuenta que, por una parte, por ser $\mathbf{S}$ un conjunto preordenado dirigido superiormente, existirán $p, q, r \in S$ tales que $s, s' \preceq p$, $s', s'' \preceq q$ y $p, q \preceq r$ y, por otra, que por ser $(\mathbf{S}, \mathcal{A})$ un sistema inductivo, el diagrama:



conmuta. , con $((x, s), (y, s')) \in R_{(\mathbf{S},\mathcal{A})}$, entonces hay un $s'' \in S$ tal que $s, s' \preceq s''$ y $a_{s,s''}(x) = a_{s',s''}(y)$. Pero el diagrama:



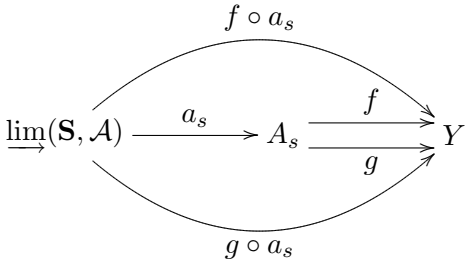
conmuta. En la proposición anterior se ha demostrado, para un sistema inductivo de conjuntos, la existencia de al menos un par ordenado, formado por un conjunto y una familia de aplicaciones desde cada uno de los conjuntos de la familia de conjuntos subyacente a la segunda coordenada del sistema inductivo, hasta el conjunto, sujeto a cumplir, por una parte, una condición de compatibilidad respecto de las aplicaciones subyacentes a la segunda coordenada del sistema inductivo, y, por otra, una cierta propiedad universal; pero, ni hemos afirmado que tal par sea absolutamente único, ni que las inclusiones canónicas sean necesariamente inyectivas, sobreyectivas o biyectivas.

Demostraremos en lo que sigue, entre otras cosas, que:

- El par ordenado de la proposición anterior, es único salvo isomorfismo.
- Una condición suficiente para que una inclusión canónica sea inyectiva, sobreyectiva o biyectiva, es que las aplicaciones de transición sean inyectivas, sobreyectivas o biyectivas.

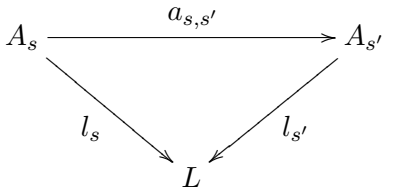
Proposición 0.3. *Sea* $(\mathbf{S}, \mathcal{A})$ *un sistema inductivo de conjuntos. Entonces:*

1. *Para cada conjunto* Y *y cualesquiera aplicaciones* $f, g\colon \varinjlim(\mathbf{S}, \mathcal{A}) \longrightarrow Y$, *si, para cada* $s \in S$, *el diagrama:*

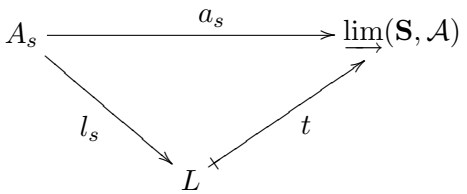


conmuta, entonces $f = g$, *i.e., la familia de aplicaciones* $(a_s)_{s\in S}$ *es* colectivamente epimórfica.

2. *Para cada par ordenado* $(L, (l_s)_{s\in S})$, *en el que* L *sea un conjunto y, para cada* $s \in S$, $l_s\colon A_s \longrightarrow L$, *si para cada* $(s, s') \in \preceq$, *el diagrama:*



conmuta, y para cada monomorfismo $t\colon L \longmapsto \varinjlim(\mathbf{S}, \mathcal{A})$, *si, para cada* $s \in S$, *el digrama:*



conmuta, entonces t *es un isomorfismo, i.e., la familia de aplicaciones* $(a_s)_{s\in S}$ *es* extremal.

Demostración. □

Lema 0.4. *Sea* $(\mathbf{S}, \mathcal{A})$ *un sistema inductivo de conjuntos,* n *un número natural no nulo y* $(X_\alpha)_{\alpha\in n} \in \varinjlim(\mathbf{S}, \mathcal{A})^n$. *Entonces hay un* $s \in S$ *y una familia* $(x_\alpha)_{\alpha\in n}$ *en* A_s^n *tal que, para cada* $\alpha \in n$, $a_s(x_\alpha) = X_\alpha$.

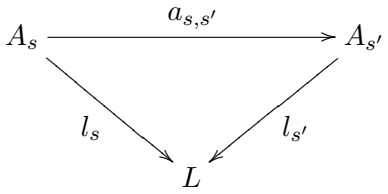
Demostración. Para cada $\alpha \in n$, en virtud de la definición de $\varinjlim(\mathbf{S}, \mathcal{A})$, hay un $s_\alpha \in S$ y algún $y_\alpha \in A_{s_\alpha}$ tal que $X_\alpha = a_{s_\alpha}(y_\alpha)$. Ahora bien, por ser $\mathbf{S}$ un conjunto preordenado dirigido superiormente, hay un $s \in S$ tal que, para cada $\alpha \in n$, $s_\alpha \preceq s$. Luego, ya que, para cada $\alpha \in n$,$a_s \circ a_{s_\alpha,s} = a_{s_\alpha}$, tomando como $(x_\alpha)_{\alpha\in n}$ la familia $(a_{s_\alpha,s}(y_\alpha))_{\alpha\in n}$ en A_s, se cumple que $a_s(x_\alpha) = X_\alpha$, para cada $\alpha \in n$. □

Lema 0.5. *Sea* $(\mathbf{S}, \mathcal{A})$ *un sistema inductivo de conjuntos,* n *un número natural no nulo,* $s \in S$ *y* $(x_\alpha)_{\alpha\in n} \in A_s^n$. *Si, para cada* $\alpha, \beta \in n$ *se cumple que* $a_s(x_\alpha) = a_s(x_\beta)$, *entonces hay un* $s' \in S$ *tal que* $s \preceq s'$ *y, para cada* $\alpha, \beta \in n$, $a_{s,s'}(x_\alpha) = a_{s,s'}(x_\beta)$.

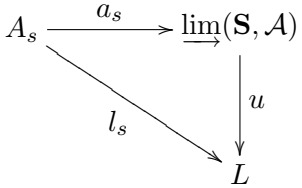
Demostración. Puesto que, para cada $\alpha, \beta \in n$, se cumple que $a_s(x_\alpha) = a_s(x_\beta)$, entonces, en virtud de la definición de a_s, tenemos que $[(x_\alpha, s)]_{\Phi_{(\mathbf{S},\mathcal{A})}} = [(x_\beta, s)]_{\Phi_{(\mathbf{S},\mathcal{A})}}$, luego, para cada $\alpha, \beta \in n$, hay un $s_{\alpha,\beta} \in S$ tal que $s \preceq s_{\alpha,\beta}$ y $a_{s,s_{\alpha,\beta}}(x_\alpha) = a_{s,s_{\alpha,\beta}}(x_\beta)$.

Ahora bien, por ser $(s_{\alpha,\beta})_{(\alpha,\beta)\in n^2}$ una familia finita no vacía en S y $\mathbf{S}$ un conjunto preordenado dirigido superiormente, hay un $s' \in S$ tal que, para cada $\alpha, \beta \in n$, $s_{\alpha,\beta} \preceq s'$, luego $s \preceq s'$. Además, para cada $\alpha, \beta \in n$, $a_{s,s'} = a_{s_{\alpha,\beta},s'} \circ a_{s,s_{\alpha,\beta}}$ y ya que $a_{s,s_{\alpha,\beta}}(x_\alpha) = a_{s,s_{\alpha,\beta}}(x_\beta)$, $a_{s_{\alpha,\beta},s'}(a_{s,s_{\alpha,\beta}}(x_\alpha)) = a_{s_{\alpha,\beta},s'}(a_{s,s_{\alpha,\beta}}(x_\beta))$, luego $a_{s,s'}(x_\alpha) = a_{s,s'}(x_\beta)$. □

Proposición 0.6. *Sea* $(\mathbf{S}, \mathcal{A})$ *un sistema inductivo de conjuntos y* $(L, (l_s)_{s\in S})$ *tal que, para cada* $s \in S$, $l_s \colon A_s \longrightarrow L$ *y, para cada* $(s, s') \in \preceq$, *el diagrama:*



conmute. Entonces para la única aplicación $u \colon \varinjlim(\mathbf{S}, \mathcal{A}) \longrightarrow L$ *tal que, para cada* $s \in S$, *el diagrama:*



conmuta, se cumple que:

1. *Una condición necesaria y suficiente para que* u *sea sobreyectiva es que* $L = \bigcup_{s\in S} \mathrm{Im}(l_s)$.
2. *Una condición necesaria y suficiente para que* u *sea inyectiva es que, para cada* $s \in S$ *y para cada* $x, y \in A_s$, *si* $l_s(x) = l_s(y)$, *entonces exista un* $s' \in S$ *tal que* $s \preceq s'$ *y* $a_{s,s'}(x) = a_{s,s'}(y)$.

Demostración. 1. Puesto que una aplicación es sobreyectiva si y sólo si su imagen coincide con su codominio, u será sobreyectiva precisamente si $u\left[\varinjlim(\mathbf{S},\mathcal{A})\right] = L$. Ahora bien, $\varinjlim(\mathbf{S},\mathcal{A}) = \bigcup_{s\in S}\mathrm{Im}(a_s)$, luego u será sobreyectiva precisamente si $u\left[\bigcup_{s\in S}\mathrm{Im}(a_s)\right] = L$, i.e., si y sólo si se cumple que $\bigcup_{s\in S}\mathrm{Im}(u\circ a_s) = L$, pero, para cada $s\in S$, $u\circ a_s = l_s$, luego u será sobreyectiva cuando y sólo cuando $\bigcup_{s\in S}\mathrm{Im}(l_s) = L$.

2. *La condición es necesaria.* Supongamos que $u\colon \varinjlim(\mathbf{S},\mathcal{A}) \longrightarrow L$ sea inyectiva y sean $s\in S$ y $x,y\in A_s$ tales que $l_s(x) = l_s(y)$. Entonces, ya que, para cada $s\in S$, $u\circ a_s = l_s$, $u(a_s(x)) = u(a_s(y))$, luego, por ser u inyectiva, $a_s(x) = a_s(y)$. Por consiguiente, en virtud del lema 0.5, hay un $s'\in S$ tal que $s\preceq s'$ y $a_{s,s'}(x) = a_{s,s'}(y)$.

La condición es suficiente. Supongamos que para cada $s\in S$ y para cada $x,y\in A_s$, si $l_s(x) = l_s(y)$, entonces exista un $s'\in S$ tal que $s\preceq s'$ y $a_{s,s'}(x) = a_{s,s'}(y)$. Sean $X,Y\in\varinjlim(\mathbf{S},\mathcal{A})$ tales que $u(X) = u(Y)$. Entonces, en virtud del lema 0.4, hay un $s\in S$ y $x,y\in A_s$ tales que $a_s(x) = X$ y $a_{s'}(y) = Y$. luego $u(a_s(x)) = u(a_s(y))$, pero $u\circ a_s = l_s$, así que $l_s(x) = l_s(y)$. Por lo tanto, en virtud de la hipótesis, existe un $s'\in S$ tal que $s\preceq s'$ y $a_{s,s'}(x) = a_{s,s'}(y)$; pero esto último significa precisamente que $X = Y$, ya que $X = [(x,s)]_{\Phi_{(\mathbf{S},\mathcal{A})}}$, $Y = [(y,s)]_{\Phi_{(\mathbf{S},\mathcal{A})}}$ y $X = Y$ si y sólo si existe un $s'\in S$ tal que $s\preceq s'$ y $a_{s,s'}(x) = a_{s,s'}(y)$

□

Proposición 0.7. *Sea $(\mathbf{S},\mathcal{A})$ un sistema inductivo de conjuntos. Entonces una condición suficiente para que $a_s\colon A_s\longrightarrow\varinjlim(\mathbf{S},\mathcal{A})$ sea inyectiva, sea cual sea $s\in S$, es que, para cada $(s,s')\in\preceq$, $a_{s,s'}\colon A_s\longrightarrow A_{s'}$ sea inyectiva.*

Demostración. □

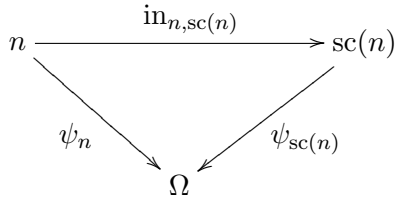
Proposición 0.8. *Sea $(\mathbf{S},\mathcal{A})$ un sistema inductivo de conjuntos. Entonces una condición suficiente para que $a_s\colon A_s\longrightarrow\varinjlim(\mathbf{S},\mathcal{A})$ sea sobreyectiva, sea cual sea $s\in S$, es que, para cada $(s,s')\in\preceq$, $a_{s,s'}\colon A_s\longrightarrow A_{s'}$ sea sobreyectiva.*

Demostración. □

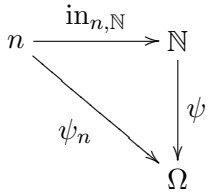
Corolario 0.9. *Sea $(\mathbf{S},\mathcal{A})$ un sistema inductivo de conjuntos. Entonces una condición suficiente para que $a_s\colon A_s\longrightarrow\varinjlim(\mathbf{S},\mathcal{A})$ sea biyectiva, sea cual sea $s\in S$, es que, para cada $(s,s')\in\preceq$, $a_{s,s'}\colon A_s\longrightarrow A_{s'}$ sea biyectiva.*

Demostración. □

Para el sistema inductivo $(\mathbf{N},\mathcal{A})$, en el que $\mathbf{N}$ es el conjunto bien ordenado $(\mathbb{N},\leq)$ y $\mathcal{A} = ((n)_{n\in\mathbb{N}-1},(\mathrm{in}_{n,\mathrm{sc}(n)})_{n\in\mathbb{N}-1})$, tenemos que $(\mathbb{N},(\mathrm{in}_{n,\mathbb{N}})_{n\in\mathbb{N}-1})$ es el límite inductivo del mismo. Por otra parte, para la familia de aplicaciones $(\psi_n)_{n\in\mathbb{N}-1}$, obtenida del Teorema 125, se cumple que, para cada $n\in\mathbb{N}-1$, el diagrama:



conmuta. Por consiguiente, en virtud de la propiedad universal del límite inductivo, hay una única aplicación $\psi\colon \mathbb{N} \longrightarrow \Omega$ tal que, para cada $n \in \mathbb{N}-1$, el diagrama:



conmuta. Creo que, para cada $i \in \mathbb{N}$, $\psi(i) = \psi_{\mathrm{sc}(i)}(i)$ (hay que comprobarlo).

---

127. *Teorema.* Bajo los supuestos hechos en el teorema precedente

$$\psi(T') = \theta\psi(T),$$

donde T significa cualquier parte de la sucesión numérica N.

Demostración. Pues si t significa cada número del sistema T, entonces $\psi(T')$ consiste en todos los elementos $\psi(t')$, y $\theta\psi(T)$ en todos elementos $\theta\psi(t)$; de aquí se sigue nuestro teorema, porque (por III en 126) $\psi(t') = \theta\psi(t)$.

128. *Teorema.* Si se mantienen los mismos supuestos y se indica con θ_0 las cadenas (44) que corresponden a la aplicación θ del sistema Ω en sí mismo, entonces

$$\psi(N) = \theta_0(\omega).$$

Demostración. Señalamos en primer lugar por inducción completa (80), que

$$\psi(N) \prec \theta_0(\omega).$$

i.e, que toda imagen $\psi(n)$ es también elemento de $\theta_0(\omega)$. De hecho,

ρ. Este teorema es verdadero para $n = 1$, porque (por 126.II) $\psi(1) = \omega$, y porque (por 45) $\omega \prec \theta_0(\omega)$.

σ. Si este teorema es verdadero para un número n, y por lo tanto tenemos que $\psi(n) \prec \theta_0(\omega)$, entonces tenemos también por 55 que $\theta(\psi(n)) \prec \theta_0(\omega)$, i.e., (por 126. III), $\psi(n') \prec \theta(\omega)$, luego el teorema es válido también para el número siguiente n', q.e.d.

Para demostrar ulteriormente que cada elemento ν de la cadena $\theta_0(\omega)$ está contenido en $\psi(N)$, y que por lo tanto

$$\theta_0(\omega) \prec \psi(N),$$

empleamos asimismo la inducción completa, a saber el teorema 59 transferido sobre Ω y la aplicación θ. De hecho,

ρ. El elemento ω es $= \psi(1)$, y por lo tanto está contenido en $\psi(N)$.

σ. Si ν es un elemento común de la cadena $\theta_0(\omega)$ y del sistema $\psi(N)$, entonces $\nu = \psi(n)$, donde n significa un número, y de aquí se sigue (por 126. III) que $\theta(\nu) = \theta\psi(n) = \psi(n')$, con lo que $\theta(\nu)$ está contenido también en $\psi(N)$, q.e.d.

De los teoremas demostrados $\psi(N) \prec \theta_0(\omega)$ y $\theta_0(\omega) \prec \psi(N)$ se sigue (por 5) $\psi(N) = \theta_0(\omega)$, q.e.d.

129. *Teorema.* Bajo los mismos supuestos, tenemos en general que

$$\psi(n_0) = \theta_0(\psi(n)).$$

Demostración por inducción completa 80. Pues

ρ. El teorema es válido como consecuencia de 128 para $n = 1$, porque $1_0 = N$ y $\psi(1) = \omega$.

σ. Si el teorema es válido para un número n, entonces se sigue

$$\theta(\psi(n_0)) = \theta(\theta_0(\psi(n)));$$

ahora bien, puesto que por 127 y 75 $\theta(\psi(n_0)) = \psi(n_0')$ y por 57 y 126. III,

$$\theta(\theta_0(\psi(n))) = \theta_0(\theta(\psi(n))) = \theta_0(\psi(n'),$$

entonces se obtiene que

$$\psi(n_0') = \theta_0(\psi(n')),$$

i.e., el teorema vale también para el número n' siguiente a n, q.e.d.

130. *Observación.* Antes de que pasemos a la aplicaciones más importantes del teorema de la definición por inducción demostrado en 126 (§10 a 14), vale la pena llamar la atención sobre una circunstancia por la cual éste se diferencia esencialmente del teorema sobre la demostración por inducción demostrados en 80, o incluso ya en 59 y 60, por grande que parezca ser el parentesco entre aquél y éste. A saber, mientras que el teorema 59 es válido por completo en general para toda cadena A_0, donde A es una parte cualquiera de un sistema S formado por una aplicación arbitraria φ en sí mismo (§4), es completamente otro el caso con el teorema 126, que sólo afirma la existencia de una aplicación ψ no contradictoria (o unívoca) de un sistema simplemente infinito 1_0. Si se quisiera en el último teorema (manteniendo los supuestos sobre Ω y θ) poner en lugar de la sucesión numérica 1_0 una cadena arbitraria A_0 de un tal sistema S, y en general definir una aplicación ψ de A_0 en Ω de modo semejante a en 126. II, III, por que

ρ. cada elemento a de A corresponde a un determinado elemento $\psi(a)$ elegido de Ω, y,

σ. que para todo elemento n contenido en A_0 y su imagen $n' = \varphi(n)$ debe de ser válida la condición $\psi(n') = \theta\psi(n)$, entonces se daría muy frecuentemente el caso de que no existiría una tal aplicación ψ, porque estas condiciones ρ, σ, pueden entrar en contradicción entre sí, incluso aunque se limite en adelante la libertad de elección contenida en ρ según la condición σ. Un ejemplo bastará para convencer de esto. Si el sistema S que consta de los elementos diferentes a y b es aplicado sobre sí mismo por φ, de tal modo que tendremos que $a' = b$ y $b' = a$, entonces claramente $a_0 = b_0 = S$; si además el sistema Ω que constara de los elementos α, β y γ, estuviera aplicado en sí mismo por θ, de modo que tuviéramos que $\theta(\alpha) = \beta$, $\theta(\beta) = \gamma$, $\theta(\gamma) = \alpha$; se pide ahora una aplicación ψ de a_0 en Ω, tal que $\psi(a) = \alpha$ y además para cada elemento n contenido en a_0 siempre se tendrá que $\psi(n') = \theta\psi(n)$, entonces se choca con una contradicción; pues para $n = \alpha$ se obtiene que $\psi(b) = \theta(\alpha) =$ *beta*, y de aquí se sigue para $n = b$, que deberíamos tener que $\psi(a) = \theta(\beta) = \gamma$, mientras que sin embargo, teníamos que $\psi(a) = \alpha$.

Pero si hay una aplicación *psi* de A_0 en Ω, que cumple sin contradicción las condiciones anteriores ρ, σ, entonces se sigue fácilmente de 60 que ésta está completamente determinada; pues si la aplicación χ cumple las mismas

condiciones, entonces en general $\chi(n) = \psi(n)$, porque según este teorema ρ es válido para todos los elementos contenidos en A que $n = a$, y porque éste, si es válido para un elemento n de A_0, a consecuencia de σ debe ser válido también para su imagen n'.

131. Para iluminar el alcance de nuestro teorema 126, queremos añadir aquí una consideración, que es útil también para otras investigaciones, p. ej. para la llamada teoría de grupos.

Consideramos un sistema Ω, entre cuyos elementos está establecida una determinada relación de manera que de un elemento ν por la acción de un elemento ω siempre surge de nuevo un determinado elemento del mismo sistema Ω, que podría ser denotado con $\omega.\nu$ o con $\omega\nu$, y que en general hay que diferenciar de $\nu\omega$. Se puede concebir esto también de manera que, a cada elemento determinado ω le corresponde una aplicación determinada, que podría denotarse, por ejemplo, por $\dot{\omega}$, en tanto que cada elemento ν proporciona la imagen determinada $\dot{\omega}(\nu) = \omega\nu$. Si se aplica a este sistema Ω y a su elemento ω el teorema 126, cambiando inmediatamente la aplicación denotada allí con θ por $\dot{\omega}$, entonces corresponde a cada número n un elemento $\psi(n)$ determinado, contenido en Ω, que podría denotarse ahora por el símbolo ω^n y a veces podría denominarse la n-sima potencia de ω. Este concepto queda completamente aclarado por las condiciones impuestas a él

II. $\omega^1 = \omega$,

III. $\omega^{n'} = \omega\omega^n$,

y su existencia está asegurada por la demostración del teorema 126.

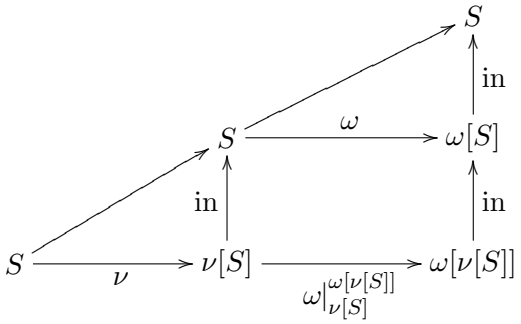
Si la anterior relación de los elementos está hecha además de tal manera que para elementos arbitrarios μ, ν, ω, siempre se da que $\omega(\nu\mu) = (\omega\nu)\mu$, entonces son válidos también los teoremas

$$\omega^{n'} = \omega^n\omega,\ \omega^m\omega^n = \omega^n\omega^m,$$

cuyas demostraciones se llevan a cabo fácilmente por inducción completa (80), y pueden dejarse al lector.

La anterior consideración general tiene una aplicación inmediata en el siguiente ejemplo. Sea S un sistema de elementos cualesquiera y sea Ω el correspondiente sistema que tiene por elementos todas las aplicaciones ν de S en sí mismo (36); entonces, por 25, los elementos de Ω siempre se pueden componer dado que $\nu(S) \subseteq S$ y que la aplicación $\omega\nu$ compuesta de las aplicaciones ν y ω también es elemento de Ω

Comentario. [N.T.33]



La observación general previa puede aplicarse directamente al siguiente ejemplo. Si S es un sistema de elementos arbitrarios, y Ω el sistema correspondiente, cuyos elementos son todas las aplicaciones ν de S en sí mismo (36), entonces estos elementos pueden por 25 siempre componerse, porque $\nu(S) \prec S$, y la aplicación $\omega\nu$ compuesta de tales aplicaciones ν y ω es ella misma de nuevo elemento de Ω. Entonces son también todos los elementos $\omega\nu$ aplicaciones de S en sí mismos, y se dice que se generan por repetición de la aplicación ω. Queremos ahora resaltar una relación [] simple que se mantiene entre este concepto y el concepto definido en 44 de la cadena $\omega_0(A)$, donde A a su vez denota una parte cualquiera de S. Si se denota por mor de la brevedad la imagen $\omega^n(A)$ generada por la aplicación ω^n con A_n, entonces se sigue de III, 25, que $\omega(A_n) = A_{n'}$. De aquí se obtiene fácilmente por inducción completa (80), que todos estos sistemas A_n son partes de la cadena $\omega_0(A)$; entonces

ρ. Esta afirmación vale como consecuencia de 50 para $n = 1$, y

σ. si vale para un número n, entonces se sigue de 55 y de $A_{n'} = \omega(A_n)$, que ella es válida también para los siguientes n', q.e.d. Puesto que además por 45 también tenemos que $A \prec \omega_0(A)$, entonces se sigue de 10, que también el sistema K compuesto de A y de todas las imágenes A_n es parte de $\omega_0(A)$. Viceversa, puesto que (por 23) $\omega(K)$ está compuesto de $\omega(A) = A_1$ y de todos los sistemas $\omega(A_n) = A_{n'}$, por lo tanto (por 78) por todos los sistemas A_n, que por 9 son partes de K, entonces se sigue por 47, que también tenemos que $\omega_0(A) \prec K$. Con esto tenemos que $\omega_0(A) = K$, i.e., se mantiene el siguiente teorema: Si w es una aplicación de un sistema S en sí mismo, y A una parte cualquiera de S, entonces la cadena de A correspondiente a la aplicación ω está compuesta de A y de todas las imágenes $\omega_n(A)$ generadas por repetición de w. Recomendamos al lector volver con esta concepción de una cadena a los anteriores teoremas 57 y 58.

§10.

La clase de los sistemas simplemente infinitos.

132. *Teorema.* Todos los sistemas simplemente infinitos son semejantes a la sucesión numérica N y por consiguiente (por 33) también entre sí.

Demostración. Sea el sistema simplemente infinito Ω, que está ordenado por la aplicación θ (71), y sea ω el elemento básico de Ω que surge aquí; si denotamos con θ_0 de nuevo las cadenas correspondientes a la aplicación θ (44), entonces es válido por 71 lo siguiente:

α. $\theta(\Omega) \prec \Omega$.
β. $\Omega = \theta_0(\omega)$.
γ. ω no está contenido en $\theta(\Omega)$.
δ. La aplicación θ es una aplicación semejante.

Si ahora ψ denota la aplicación de la sucesión numérica N definida en 126, entonces se sigue de β y 128 en primer lugar que

$$\psi(N) = \Omega,$$

y tenemos por esto por 32 sólo que probar aún, que ψ es una aplicación semejante, i.e., que a números diferentes m, n, corresponden también imágenes diferentes $\psi(m)$, $\psi(n)$. A causa de la simetría podemos suponer por 90, que $m > n$, por lo tanto que $m \prec n'_0$, y se sigue el teorema a probar de que $\psi(n)$ no está contenido en $\psi(n'_0)$, y por lo tanto (por 127) tampoco en $\theta\psi(n_0)$. Esto lo probamos para cada número por inducción completa (80). En efecto,

ρ. este teorema es válido por γ para $n = 1$, porque $\psi(1) = \omega$ y $\psi(1_0) = \psi(N) = \Omega$.

σ. Si el teorema es verdadero para un número n, entonces es válido también para el número siguiente n'; puesto que $\psi(n')$, i.e. $\theta\psi(n)$ estaría contenida en $\theta\psi(n'_0)$, entonces debería (por δ y 27), también $\psi(n)$ estar contenido en $\psi(n'_0)$, mientras que nuestro supuesto dice justo lo contrario, q.e.d.

133. *Teorema.* Cada sistema que es semejante a un sistema simplemente infinito y por consiguiente (por 132 y 33), también a la sucesión numérica N, es simplemente infinito.

Demostración. Si Ω es un sistema semejante a la sucesión numérica N, entonces hay por 32 una aplicación semejante ψ de N, tal que

I. $\psi(N) = \Omega$;

entonces establecemos que

II. $\psi(1) = \omega$.

Si se denota por 26 con $\overline{\psi}$ la aplicación inversa, asimismo semejante, de Ω, entonces corresponde a cada elemento ν de Ω un número determinado $\overline{\psi}(\nu) = n$, a saber, aquel, cuya imagen $\psi(n) = \nu$. Ahora bien, puesto que a este número n le corresponde un número siguiente determinado $\varphi(n) = n'$, y a éste a su vez un elemento determinado $\psi(n')$ en Ω, entonces cada elemento ν del sistema Ω también tiene asociado un elemento determinado $\psi(n')$ del mismo sistema, que queremos denotar como imagen de ν con $\theta(\nu)$. De este modo se determina completamente una aplicación θ de Ω en sí mismo[79], y para probar nuestro teorema, queremos mostrar, que Ω está ordenado por θ como un sistema simplemente infinito (71), i.e., que las condiciones α, β, γ, δ indicadas en la demostración de 132 se cumplen por completo. En primer lugar, α es manifiesta directamente desde la definición de θ. Además, puesto que a todo número n le corresponde un elemento $\nu = \psi(n)$, para el cual tendremos que $\theta(\nu) = \psi(n')$, entonces, en general,

III. $\psi(n') = \theta\psi(n)$,

y de aquí en unión con I, II y α se obtiene que las aplicaciones θ y ψ cumplen todas las condiciones del teorema 126; con lo que se sigue β de 128 y I. Además, por 127 y I tenemos que

$$\psi(N') = \theta\psi(N) = \theta(\Omega),$$

y de aquí en unión con II y de la semejanza de la aplicación ψ se sigue γ, porque de no ser así $\psi(1)$ debería estar contenido en $\psi(N')$, y por lo tanto (por 27) lo estaría el número 1 en N', lo que (por 71. γ) no es el caso. Si por último μ, ν denotan elementos de Ω, y m, n los números correspondientes, cuyas imágenes son $\psi(m) = \mu$, $\psi(n) = \nu$, entonces se sigue del supuesto $\theta(m) = \theta(n)$ según lo anterior, que $\psi(m') = \psi(n')$, y de aquí, debido a la

[79]Evidentemente, θ es la aplicación compuesta $\psi\varphi\overline{\psi}$ de $\overline{\psi}$, φ, ψ por 25.

semejanza de ψ, φ, que $m' = n'$, $m = n$, y por lo tanto también que $\mu = \nu$; con esto es válido también δ, q.e.d.

134. *Observación.* Como consecuencia de los teoremas previos 132 y 133, todos los sistemas simplemente infinitos forman una clase en el sentido de 34. Al mismo tiempo es claro atendiendo a 71 y 73, que cada teorema sobre los números, i.e., sobre los elementos n del sistema simplemente infinito N ordenado por la aplicación φ, y ciertamente cualquier teorema en el que se prescinde por completo de las propiedades particulares de los elementos n y en los que sólo se habla de los conceptos que surgen de la ordenación φ, posee una validez completamente general también para todo otro sistema simplemente infinito Ω ordenado por una aplicación θ y sus elementos ν, y que la transferencia de N a Ω (p. ej. también la traducción de un teorema aritmético de una lengua a otra), tiene lugar por la aplicación contemplada en 132 y 133, que transforma cada elemento n de N en un elemento ν de Ω, a saber, en $\psi(n)$. Puede denominarse a este elemento ν el n-simo elemento de Ω, y según esto el número n mismo es el n-simo número de la sucesión numérica N. La misma significación que posee la aplicación φ para las leyes en el dominio N, en tanto que a cada elemento n le sigue un elemento determinado $\varphi(n) = n'$, le corresponde a la aplicación θ según la transformación operada por ψ para las mismas leyes en el dominio Ω, en tanto que al elemento $\nu = \psi(n)$ generado por transformación de n, le sigue el elemento $\theta(\nu) = \psi(n')$, generado por transformación de n'; se puede por esto decir con razón que φ se transforma en θ, lo que se expresa simbólicamente por $\theta = \psi\varphi\overline{\psi}$, $\varphi = \overline{\psi}\theta\psi$. Con estas observaciones creo que quedará completamente justificado el concepto de los números establecido en 73. Pasamos ahora a ulteriores aplicaciones del teorema 126.

§11.

Adición de los números.

135. *Definición.* Es fácil aplicar la definición expuesta en el teorema 126 de una aplicación ψ de la sucesión numérica N o de la *función* $\psi(n)$ determinada por la misma al caso en que el sistema denotado allí con Ω, en el que debe estar contenida la imagen $\psi(N)$, es la sucesión numérica N misma, porque para este sistema Ω hay ya una aplicación θ de Ω en sí mismo, a saber, aquella aplicación φ, a través de la cual N está ordenado como un sistema simplemente infinito (71 y 73). Entonces tendremos también que $\Omega = N$, $\theta(n) = \varphi(n) = n'$, con lo que

I. $\psi(N) \prec N$,

y queda, para determinar completamente ψ, sólo elegir a voluntad el elemento ω de Ω, i.e., de N. Si ponemos que $\omega = 1$, entonces ψ será manifiestamente la aplicación idéntica (21) de N, porque se satisfacen las condiciones

$$\psi(1) = 1, \quad \psi(n') = (\psi(n))'$$

en general por $\psi(n) = n$. Si se creara también otra aplicación ψ de N, entonces debe elegirse para ω un número m' diferente de 1, contenido por 78 en N', donde m mismo significa cualquier número; puesto que la aplicación ψ es evidentemente dependiente de la elección de este número m, denotamos

la imagen correspondiente $\psi(n)$ de un número cualquiera n por el símbolo $m+n$ y llamamos a este número la *suma*, que surge del número m por la *adición* del número n, o brevemente la suma de los números m y n. Esta está por esto por 126 completamente determinada por la condiciones[80]

II. $m+1=m'$,

III. $m+n'=(m+n)'$.

136. *Teorema.* $m'+n=m+n'$. Demostración por inducción completa (80). Pues

ρ. el teorema es verdadero para $n=1$, porque (por 135.II)

$$m'+1=(m')'=(m+1)'$$

y (por 135.III) $(m+1)'=m+1'$.

σ. Si el teorema es válido para un número n, y se establece que el siguiente número $n'=p$, entonces $m'+n=m+p$, por lo tanto también $(m'+n)'=(m+p)'$, de donde se sigue (por 135.III) $m'+p=m+p'$; con lo que es válido el teorema también para el número siguiente p, q.e.d.

137. *Teorema.* $m'+n=(m+n')$.

La demostración se sigue de 136 y 135. III.

138. *Teorema.* $1+n=n'$.

Demostración por inducción completa. Pues

ρ. el teorema es por 135.II verdadero para $n=1$.

σ. si el teorema es válido para un número n, y se establece que $n'=p$, entonces $1+n=p$, y por lo tanto también $(1+n)'=p'$, con lo que (por 135.III) $1+p=p'$, i.e., el teorema es válido también para el número siguiente p, q.e.d.

139 *Teorema.* $1+n=n+1$.

La demostración se sigue de 138 y 135. II.

140. *Teorema.* $m+n=n+m$.

Demostración por inducción completa (80). Pues

ρ. el teorema es por 139 verdadero para $n=1$.

σ. Si el teorema es válido para un número n, entonces se sigue de ahí también que $(m+n)'=(n+m)'$, i.e., (por 135.III) $m+n'=n+m'$, con lo que (por 136) $m+n'=n'+m$; con lo que el teorema es válido también para el número siguiente, n', q.e.d.

141. *Teorema.* $(l+m)+n=l+(m+n)$.

Demostración por inducción completa (80). Pues

ρ. el teorema es verdadero para $n=1$, porque (por 135. II,III, II) $(l+m)+1=(l+m)'=l+m'=l+(m+1)$.

σ Si el teorema es válido para un número n, entonces se sigue de ahí también que $((l+m)+n)'=(l+(m+n)'$, i.e, (por 135. III)

$$(l+m)+n'=l+(m+n)'=l+(m+n'),$$

[80]La definición anterior, fundamentada directamente en el teorema 126, me parece que es la más simple. Empleando el concepto desarrollado en 131 se puede sin embargo definir la suma $m+n$ también por $\varphi^n(m)$ o también por $\varphi^m(n)$, donde φ a su vez tiene la significación de arriba. Para demostrar la completa coincidencia de esta definición con la de arriba, se necesita por 126 sólo mostrar que si se denota $\varphi^n(m)$ o $\varphi^m(n)$ por $\psi(n)$, se satisfacen las condiciones $\psi(1)=m'$, $\psi(n')=\varphi\psi(n)$, lo que se consigue fácilmente con ayuda de la inducción completa (80) empleando 131.

luego el teorema es válido también para el número siguiente n', q.e.d.

142. *Teorema.* $m + n > m$. Demostración por inducción completa (80). Pues

ρ. el teorema es por 135.II y 91 verdadero para $n = 1$.

σ. Si el teorema es válido para un número n, entonces vale por 95 también para el número siguiente n', porque (por 135. III y 91)

$$m + n' = (m + n)' > m + n$$

q.e.d.

143. *Teorema.* la condiciones $m > a$ y $m + n > a + n$ son equivalentes.

Demostración por inducción completa.(80). Pues

ρ. el teorema es válido como consecuencia de 135.II y 94 para $n = 1$.

σ si el teorema es válido para un número n, entonces es válido también para el número siguiente n', porque la condición $m+n > a+n$ es equivalente por 94 a $(m + n)' > (a + n)'$, y por lo tanto por 135.III también a

$$m + n' > a + n'$$

q.e.d.

144. *Teorema.* Si tenemos que $m > a$ y $n > b$, entonces tenemos también que

$$m + n > a + b.$$

Demostración. Pues de nuestras suposiciones se sigue (por 143) que $m + n > a + n$ y $n + a > b + a$, o, lo que por 140 es lo mismo, que $a + n > a + b$, de donde se obtiene el teorema por 95.

145. *Teorema.* Si $m + n = a + n$, entonces $m = a$.

Demostración. Pues si m no $= a$, y por lo tanto por 90 o $m > a$ o $m < a$, entonces correspondientemente por 143 $m + n > a + n$ o $m + n < a + n$, por lo tanto $m + n$ (por 90) no puede por descontado ser $= a + n$, q.e.d.

146. *Teorema.* Si $l > n$, entonces hay y (por 145) un solo número m, que satisface la condición $m + n = l$.

Demostración por inducción completa (80). Pues

ρ. el teorema es verdadero para $n = 1$. De hecho, si $l > 1$, i.e. (89) si l está contenido en N', y por lo tanto es la imagen m' de un número m, entonces se sigue de 135. II, que $l = m + 1$, q.e.d.

σ. Si el teorema es válido para un número n, entonces mostramos que él también es válido para el número siguiente n'. De hecho, si $l > n'$, entonces por 91,95, también tenemos que $l > n$, y por consiguiente hay un número k, que satisface la condición $l = k + n$; pues éste por 138 es diferente de 1 (porque si no tendríamos que $l = n'$), entonces es éste la imagen m' de un número m, y por consiguiente $l = m' + n$, y por lo tanto por 136 también $l = m + n'$, q.e.d.

§12.

Multiplicación de los números.

147. *Definición.* Después de haber encontrado en el precedente §11 un sistema infinito de nuevas aplicaciones de la sucesión numérica N en sí misma, pueden usarse cada una de ellas por 126, para construir reiteradamente

nuevas aplicaciones ψ de N. En tanto que se establece que el mismo $\Omega = N$ y $\theta(n) = m + n = n + m$, donde m es un número determinado, tendremos en todo caso de nuevo que

I. $\psi(N) \prec N$,

y queda, para determinar completamente ψ, elegir a voluntad el elemento Ω de N. El caso más simple surge cuando cuando se pone esta elección en una cierta coincidencia con la elección de θ, en tanto que se establece que $\omega = m$. Puesto que la aplicación ψ completamente determinada a través de esto depende de este número m, denotamos la imagen correspondiente $\psi(n)$ de un número arbitrario por el símbolo $m \times n$ o $m.n$, y denominamos a este número el *producto*, que se genera del número m por *multiplicación* con el número n, o brevemente el producto de los números m y n. El mismo está por esto por 126 completamente determinado por la condiciones

II. $m1 = m$
III. $mn' = mn + m$

148. *Teorema.* $m'n = mn + m$.

Demostración por inducción completa(80). Pues

ρ. el teorema es por 147.II y 135.II verdadero para $n = 1$.

σ. Si el teorema es válido para un número n, entonces se sigue que $m'n + m' = (mn + n) + m'$ y de aquí (por 147. III, 141, 140, 136, 141 y 147. III)

$$\begin{aligned} m'n' &= mn + (n + m') \\ &= mn + (m' + n) \\ &= mn + (m + n') \\ &= (mn + m) + n' = mn' + n'; \end{aligned}$$

y por lo tanto el teorema es válido también para el número siguiente n', q.e.d.

149. *Teorema.* $1.n = n$.

Demostración por inducción completa (80). Pues

ρ. el teorema es por 147.II verdadero para $n = 1$.

σ. Si el teorema es válido para un número n, entonces se sigue que $1.n+1 = n+1$, i.e, (por 147.III y 135.II) $1.n' = n'$, y por lo tanto el teorema es válido también para el número siguiente n', q.e.d.

150. *Teorema.* $mn = nm$.

Demostración por inducción completa (80). Pues

ρ. El teorema es válido por 147.II, 149 para $n = 1$.

σ. Si el teorema es válido para un número n, entonces se sigue que $mn + m = nm + m$, i.e. (por 147.III y 148) $mn' = n'm$, y por lo tanto el teorema es válido también para el número siguiente n', q.e.d.

151. *Teorema.* $l(m + n) = lm + ln$.

Demostración por inducción completa(80). Pues

ρ. el teorema es por 135.II, 147.III y 147.II verdadero para $n = 1$.

σ. Si el teorema es válido para un número n, entonces se sigue que

$$l(m + n) + l) = (lm + ln) + l;$$

pero por 147.III y 135.III tenemos que $l(m+n)+l = l(m+n)' = l(m+n')$ y por 141 y 147.III tenemos que

$$(lm+ln)+l = lm+(ln+l) = lm+ln',$$

con lo que tenemos que $l(m+n') = lm+ln'$, i.e. el teorema es válido también para el número siguiente n', q.e.d.

152. *Teorema.* $(m+n)l = ml+nl$.

La demostración se sigue de 151 y 150.

153. *Teorema.* $(lm)n = l(mn)$.

Demostración por inducción completa(80). Pues

ρ. el teorema es válido por 147.II para $n = 1$.

σ. Si el teorema es válido para un número n, entonces se sigue

$$(lm)n+lm = l(mn)+lm,$$

i.e. (por 147. III, 151 y 147. III)

$$(lm)n' = l(mn+m) = l(mn'),$$

y por lo tanto el teorema es válido también para el número siguiente n', q.e.d.

154. *Observación.* Si no se hubiera supuesto en 147 ninguna relación entre ω y θ, sino que se hubiera establecido que $\omega = k$, $\theta(n) = m+n$, entonces se produciría desde aquí por 126 una aplicación *psi* menos simple de la sucesión numérica N: para el número 1 sería $\psi(1) = k$, y para cada otro número contenido también en la forma n' tendríamos que $\psi(n') = mn+k$; luego por esto se satisfará la condición $\psi(n') = \theta\psi(n)$, i.e. $\psi(n') = m+\psi(n)$ para todos los números n, de lo que es fácil convencerse invocando los teoremas anteriores.

§13.

Potenciación de los números.

155. *Definición.* Si en el teorema 126 de nuevo se establece que $\Omega = N$, y además que $\omega = a$, $\theta(n) = an = na$, entonces se produce una aplicación ψ de N, que por consiguiente cumple la condición

I. $\psi(N) \prec N$;

la imagen correspondiente $\psi(n)$ de un número arbitrario la denotamos con el símbolo a^n y llamamos a ese número una *potencia* de *base* a, mientras que n se denomina el *exponente* de esta potencia de a. Este concepto está por esto completamente determinado por las condiciones

II. $a^1 = a$

III. $a^{n'} = a.a^n = a^n.a$.

156. *Teorema.* $a^{m+n} = a^m.a^n$.

Demostración por inducción completa (80). Pues

ρ. el teorema es válido por 135. II, 155. III, 155. II, para $n = 1$.

σ. Si el teorema es válido para un número n, entonces se sigue

$$a^{m+n}.a = (a^m.a^n)a$$

pero por 155. III, y 135. III tenemos que $a^{m+n}.a = a^{(m+n)'} = a^{m+n'}$, y por 153 y 155. III tenemos que $(a^m.a^n)a = a^m(a^n.a) = a^m.a^{n'}$; con lo que tenemos que $a^{m+n'} = a^m.a^{n'}$, i.e., el teorema vale también para el número siguiente n', q.e.d.

157. *Teorema.* $(a^m)^n = a^{mn}$.

Demostración por inducción completa. Pues

ρ. el teorema es válido por 155. II, y 147. II para $n = 1$.

σ. Si el teorema es válido para un número n, entonces se sigue que

$$(a^m)^n.a^m = a^{mn}.a^m;$$

pero por 155. III tenemos que $(a^m)^n.a^m = (a^m)^{n'}$, y por 156 y 147. III, tenemos que $a^{mn}.a^m = a^{mn+m} = a^{mn'}$; con lo que $(a^m)^{n'} = a^{mn'}$, i.e., el teorema es válido también para el número siguiente n', q.e.d.

158. *Teorema.* $(ab)^n = a^n.b^n$.

Demostración por inducción completa. Pues

ρ. el teorema es válido por 155. II, para $n = 1$.

σ. Si el teorema es válido para un número n, entonces se sigue por 150, 153, y 155. III que también $(ab)^n.a = a(a^n.b^n) = (a.a^n)b^n = a^{n'}.b^n$, y de ahí $((ab)^n.a)b = (a^{n'}.b^n)b$; pero por 153, 155. III tenemos que $((ab)^n.a)b = (ab)^n.(ab) = (ab)^{n'}$, y asimismo

$$(a^{n'}.b^n)b = a^{n'}.(b^n.b) = a^{n'}.b^{n'};$$

con lo que tenemos que $(ab)^{n'} = a^{n'}.b^{n'}$, i.e., el teorema es válido también para el número siguiente n', q.e.d.

§14.

Cantidad de elementos de un sistema finito.

159. *Teorema.* Si Σ es un sistema infinito, entonces cada uno de los sistemas numéricos Z_n definidos en 98 es aplicable de manera semejante en Σ (i.e., semejante a una parte de Σ), y viceversa.

Demostración. Si Σ es infinito, entonces hay desde luego por 72 una parte T de Σ que es simplemente infinita, y por lo tanto por 132 semejante a la sucesión numérica N, y por consiguiente cada sistema Z, como parte de N es también semejante a una parte de T, y por lo tanto también a una parte de Σ, q.e.d.

La demostración de lo inverso –por muy evidente que esto pudiera parecer– es más complicado. Si cada sistema Z_n es aplicable de manera semejante en Σ, entonces corresponde a cada número n una aplicación semejante α_n de Z_n tal que se tendrá que $a_n(Z_n) \prec \Sigma$. De la existencia de una tal sucesión de aplicaciones α_n que se toma como dada, pero sobre la que no se presupone nada más, deducimos en primer lugar con la ayuda del teorema 126 la existencia de una nueva sucesión de las mismas aplicaciones ψ_n, que posee la propiedad particular, que siempre, si $m \leq n$, y por lo tanto (por 100), $Z_m \prec Z_n$, la aplicación ψ_m de la parte Z_m está contenida en la aplicación ψ_n de Z_n (21), i.e., que las aplicaciones ψ_m y ψ_n para todos los números contenidos en Z_m coinciden entre sí por completo, y por lo tanto siempre se

tendrá también que

$$\psi_m(m) = \psi_n(m).$$

Para utilizar el mencionado teorema según este fin, entendemos por Ω aquel sistema, de cuyos elementos todas las aplicaciones semejantes posibles en general de todos los sistemas Z_n están en Σ, y definimos con ayuda de los elementos α_n dados, contenidos asimismo en Ω, una aplicación θ de Ω en sí mismo de la manera siguiente. Si β es un elemento arbitrario de Ω, y por lo tanto p. ej. una aplicación semejante del sistema determinado Z_n en Σ, entonces el sistema $\alpha_{n'}(Z_{n'})$ no puede ser parte de $\beta(Z_n)$, porque si no $Z_{n'}$ sería semejante por 35 a una parte de Z_n, y por lo tanto por 107 a una parte propia de sí mismo, con lo que sería infinito, lo que contradiría al teorema 119; hay por esto en $Z_{n'}$ desde luego uno o varios números p tales que $\alpha_{n'}(p)$ no está contenido en $\beta(Z_n)$; de estos números p elegimos –sólo para constatar algo determinado– siempre el más pequeño k (96) y definimos, puesto que $Z_{n'}$ está compuesto de Z_n y n', una aplicación γ de Z_n por que para todos los números m contenidos en Z_n debe darse que la aplicación $\gamma_m = \beta_m$, y además que $\gamma(n') = \alpha_{n'}(k)$; esta aplicación γ de $Z_{n'}$ en Σ, evidentemente semejante, la consideramos ahora como una imagen $\theta(\beta)$ de la aplicación β, y a través de ello se define por completo una aplicación θ del sistema Ω en sí mismo. Como quiera que las cosas Ω y θ mencionadas en 126 están determinadas, elegimos finalmente para el elemento de Ω denotado con ω la aplicación dada α_1; a través de lo cual está determinada por 126 una aplicación ψ de la sucesión numérica N en Ω, que, si denotamos la imagen correspondiente de un número arbitrario n no con $\psi(n)$, sino con ψ_n, cumple las condiciones

II. $\psi_1 = \alpha_1$,
III. $\psi_{n'} = \theta(\psi_n)$.

A continuación, se obtiene por inducción completa (80), que $\psi(n)$ es una aplicación semejante de Z_n en Σ; luego

ρ. esto es verdadero por II para $n = 1$, y

σ. si esta afirmación está justificada para un número n, entonces se sigue de III y del tipo de paso descrito más arriba θ de β a γ, que la afirmación es válida para el número siguiente n', q.e.d. A partir de aquí demostramos asimismo por inducción completa (80), que, si m es un número cualquiera, la propiedad enunciada más arriba

$$\psi_n(m) = \psi_m(m)$$

corresponde realmente a todos los números n, que son $\geq m$, y por lo tanto por 93 y 74 pertenecen a la cadena m_0; de hecho,

ρ. esto es inmediatamente evidente para $n = m$ y

σ. si esta propiedad corresponde a un número n, entonces se sigue de nuevo de III y de la característica de θ, que ella corresponde también al número n', q.e.d. Una vez que también se ha constatado esta propiedad particular de nuestra nueva sucesión de aplicaciones ψ_n, podemos demostrar fácilmente nuestro teorema. Definimos una aplicación χ de la sucesión numérica N, en tanto que hacemos corresponder cada número n con la imagen $\chi(n) = \psi_n(n)$; evidentemente todas las aplicaciones ψ_n están contenidas (por 21) en esta aplicación χ. Puesto que ψ_n era una aplicación de Z_n en Σ entonces se sigue

a continuación, que la sucesión numérica N es aplicada por χ igualmente en Σ, y por lo tanto que $\chi(N) \prec \Sigma$. Si además m y n son números diferentes, entonces se puede suponer por mor de la simetría por 90, que se dé que $m < n$; luego tenemos por lo anterior que $\chi(m) = \psi_m(m) = \psi_n(m)$ y $\chi(n) = \psi_n(m)$; pero puesto que ψ_n era una aplicación semejante de Z_n en Σ, y m y n son diferentes elementos de Z_n, entonces $\psi_n(m)$ es diferente de $\psi_n(n)$, y por lo tanto también $\chi(m)$ es diferente de $\chi(n)$, i.e., χ es una aplicación semejante de N. Puesto que además N es un sistema infinito (71), entonces es válido por 67 lo mismo del sistema $\chi(N)$ semejante a él, y por 68, porque $\chi(N)$ es parte de Σ, también de Σ, q.e.d.

160. *Teorema.* Un sistema Σ es finito o infinito según que haya o no un sistema Z_n semejante a él.

Demostración. Si Σ es finito, entonces hay por 159 sistemas Z_n, que no son aplicables de modo semejante en Σ; puesto que por 102 el sistema Z_1 consiste sólo en el número 1 y por consiguiente es aplicable en cada sistema semejante, entonces el número mínimo k (96), que corresponde a un sistema Z_k no aplicable de modo semejante en Σ, debe ser diferente de 1, y por lo tanto (por 78) $= n'$, y puesto que $n < n'$ (91), entonces hay una aplicación semejante ψ de Z_n en Σ; ahora, si $\psi(Z_n)$ fuera sólo una parte propia de Σ, habría entonces un elemento α en Σ, que no estaría contenido en $\psi(Z_n)$, luego se podría, puesto que $Z_{n'} = \mathfrak{M}(Z_n, n')$ (108), ampliar esta aplicación ψ a una aplicación semejante ψ de $Z_{n'}$ en Σ, en tanto que se establezca que $\psi(n') = \alpha$, mientras que a pesar de todo según nuestro supuesto $Z_{n'}$ no es aplicable de manera semejante en Σ. Con esto tenemos que $\psi(Z_n) = \Sigma$, i.e., Z_n y Σ son sistemas semejantes. Viceversa, si un sistema Σ es semejante a un sistema Z_n, entonces Σ es por 119 y 67 finito, q.e.d.

161. *Definición.* Si Σ es un sistema finito, entonces hay por 160 uno, y por 120 y 33 también un sólo número n, que corresponde a un sistema Z_n semejante al sistema Σ; este número n se llama la *cantidad* de los elementos contenidos en Σ (o también el *grado* del sistema Σ), y se dice que Σ consiste en o es un sistema de n elementos, o que el número n indica cuántos elementos están contenidos en Σ[81] Si se emplean los números para expresar exactamente esta propiedad determinada de los sistemas finitos, entonces se llaman *números cardinales.* Tan pronto como se escoge una determinada aplicación semejante ψ del sistema Z_n, gracias a la cual tendremos que $\psi(Z_n = \Sigma$, entonces corresponde a cada número m contenido en Z_n (i.e., a cada número m, que es $\leq n$) un determinado elemento $\psi(m)$ del sistema Σ, y viceversa corresponde por 26 a cada elemento de Σ por la aplicación inversa $\overline{\psi}$ un número determinado m en Z_n. Muy a menudo se denotan todos los elementos de Σ con una única letra, p.ej. α, a la que se le añade el número diferenciante m como índice, de manera que $\psi(m)$ se denota con a_m. Se dice también, que estos elementos estarían *contados*, y *ordenados* en cierto modo por ψ, y se llama α_m al m-simo elemento de Σ; si $m < n$, entonces se denomina $a_{m'}$ al elemento siguiente a α_m, y se denomina α_n al

[81] Por mor de la claridad y de la simplicidad limitamos completamente en lo que sigue el concepto de cantidad a sistemas finitos; por esto, si hablamos de una cantidad de determinadas cosas, debe por esto expresarse siempre ya, que el sistema, cuyos elementos son estas cosas, es un sistema finito.

último elemento. En estos números de los elementos se presentan por esto los números m de nuevo como números ordinales (73).

162. *Teorema.* Todos los sistemas semejantes a un sistema finito poseen la misma cantidad de elementos.

La demostración se sigue directamente de 33 y 161.

163. *Teorema.* La cantidad de los números contenidos en Z_n, i.e., aquellos números que son $\leq n$, es n.

Demostración. Pues por 32 Z_n es semejante a sí mismo.

164. *Teorema.* Si un sistema consiste en un solo elemento, entonces la cantidad de sus elementos es $= 1$, y viceversa.

La demostración se sigue directamente de 2, 26, 32, 102 y 161.

165. *Teorema.* Si T es parte propia de un sistema finito Σ, entonces la cantidad de los elementos de T es menor que la de los elementos de Σ.

Demostración. Por 68, T es un sistema finito, y por lo tanto semejante a un sistema Z_n, donde m significa la cantidad de los elementos de T; si n es además la cantidad de los elementos de Σ, y por lo tanto Σ es semejante a Z_n, entonces T es por 35 semejante a una parte propia E de Z_n, y por 33 Z_m y E son semejantes entre sí; ahora, si tuviéramos que $n \leq m$, y por lo tanto $Z_n \prec Z_m$, entonces E sería por 7 parte propia de Z_m, y por consiguiente Z_m sería un sistema infinito, lo que contradice al teorema 119; con lo que (por 90), tenemos que $m < n$, q.e.d.

166. *Teorema.* Sea $\Gamma = \mathfrak{M}(B, \gamma)$, donde B significa un sistema de n elementos y γ un elemento de Γ no contenido en B, entonces Γ consiste en n' elementos.

Demostración. Pues si $B = \psi(Z_n)$, donde ψ significa una aplicación semejante de Z_n, entonces ésta se puede ampliar por 105 y 108 a una aplicación semejante ψ de $Z_{n'}$, en tanto que se establezca que $\psi(n') = \gamma$, y ciertamente tendremos que $\psi(Z_{n'}) = \Gamma$, q.e.d.

167. *Teorema.* Si γ es un elemento de un sistema Γ consistente en n' elementos, entonces n es la cantidad de todos los demás elementos de Γ.

Demostración. Pues si B significa el conjunto de todos los elementos diferentes de γ en Γ, entonces $\Gamma = \mathfrak{M}(B, \gamma)$; ahora, si b es la cantidad de los elementos del sistema finito B, entonces, por el teorema precedente, b' es la cantidad de los elementos de Γ, por lo tanto $= n'$, de donde también por 26 se sigue que $b = n$, q.e.d.

168. *Teorema.* Si A consiste en m elementos, y B en n elementos, y A y B no tienen ningún elemento común, entonces $\mathfrak{M}(A, B)$ consiste en $m + n$ elementos.

Demostración por inducción completa (80). Pues

ρ. el teorema es verdadero para $n = 1$ en virtud de 166, 164 y 135. II.

σ. Si el teorema es válido para el número n, entonces es válido también para el número siguiente n'. De hecho, si Γ es un sistema de n' elementos, entonces se puede establecer (por 167) que $\Gamma = \mathfrak{M}(B, \gamma)$, donde γ significa un elemento de Γ, y B el sistema de los n demás elementos de Γ. Ahora, si A es un sistema de m elementos, de los que ninguno está contenido en Γ, y por tanto tampoco en B, y se establece que $\mathfrak{M}(A, B) = \Sigma$, entonces, de acuerdo con nuestro supuesto, la cantidad de los elementos de Σ es $m+n$, y puesto que γ no está contenido en Σ, entonces la cantidad de los elementos contenidos

en $\mathfrak{M}(\Sigma, \gamma)$ es por 166 $= (m+n)'$, y por lo tanto (por 135. III) $= m + n'$; pero puesto que por 15 evidentemente $\mathfrak{M}(\Sigma, \gamma) = \mathfrak{M}(A, B, \gamma) = \mathfrak{M}(A, \Gamma)$, entonces $m + n'$ es la cantidad de los elementos de $\mathfrak{M}(A, \Gamma)$, q.e.d.

169. *Teorema.* Si A, B son sistemas finitos de m y n elementos, respectivamente, entonces $\mathfrak{M}(A, B)$ es un sistema finito, y la cantidad de sus elementos es $\leq m + n$.

Demostración. Si $B \prec A$, entonces $\mathfrak{M}(A, B) = A$, y la cantidad m de los elementos de este sistema es (por 142) $< m + n$, como se afirmó. Pero si B no es parte de A, y T es el sistema de todos los elementos de B que no están contenidos en A, entonces por 165 su cantidad es $p \leq n$, y puesto que evidentemente se da que

$$\mathfrak{M}(A, B) = \mathfrak{M}(A, T),$$

entonces la cantidad $m + p$ de los elementos de este sistema es por 143 $\leq m + n$, q.e.d.

170. *Teorema.* Todo sistema compuesto de una cantidad n de sistemas finitos es finito.

Demostración por inducción completa (80). Pues

ρ. el teorema es por 8 evidente para $n = 1$.

σ. Si el teorema es válido para un número n, y Σ está compuesto de n' sistemas finitos, entonces sea A uno de estos sistemas y B el sistema compuesto de todos los demás; puesto que su cantidad (por 167) es $= n$, entonces B es, de acuerdo con nuestro supuesto, un sistema finito. Ahora, puesto que evidentemente se da que $\Sigma = \mathfrak{M}(A, B)$, entonces se sigue de aquí y de 169, que Σ es también un sistema finito, q.e.d.

171. *Teorema.* Si ψ es una aplicación desemejante de un sistema finito Σ de n elementos, entonces la cantidad de los elementos de la imagen $\psi(\Sigma)$ es menor que n.

Demostración. Si se escoge de entre todos aquellos elementos de Σ que tienen una y la misma imagen, siempre uno solo de manera arbitraria, entonces el sistema T de todos estos elementos elegidos es claramente una parte propia de Σ, porque ψ es una aplicación desemejante de Σ (26). Al mismo tiempo es manifiesto que la aplicación contenida en ψ (por 21) de esta parte T es una aplicación semejante, y que $\psi(T) = \psi(\Sigma)$, con lo que el sistema $\psi(\Sigma)$ es semejante a la parte propia T de Σ, y de aquí se sigue nuestro teorema por 162 y 165.

172. *Observación final.* Aunque se acaba de demostrar que la cantidad de los elementos de $\psi(\Sigma)$ es menor que la cantidad n de los elementos de Σ, se suele decir en algunas ocasiones, que la cantidad de los elementos de $\psi(\Sigma)$ es $= n$. Evidentemente la palabra cantidad se usa en un sentido diferente al empleado hasta aquí (161); a saber, si α es un elemento de Σ, y α es la cantidad de todos aquellos elementos de Σ que poseen una y la misma imagen $\psi(\alpha)$, entonces se concibe esta última como elemento de $\psi(\Sigma)$ y frecuentemente aun a pesar de todo como representante de α elementos, que al menos por su procedencia pueden ser vistos como diferentes entre sí, y que de acuerdo con esto se cuenta como el a-uplo elemento de $\psi(\Sigma)$. De este modo se llega al concepto, muy útil en muchos casos, de sistemas en los que cada elemento está dotado de un cierto número de frecuencia, que indica cuántas veces debe contarse éste como elemento del sistema. En el caso anterior se

diría, por ejemplo, que n es la cantidad de los elementos contados en este sentido de $\psi(\Sigma)$, mientras que la cantidad m de los elementos realmente diferentes de este sistema coincide con la cantidad de los elementos de T. Semejantes derivaciones del concepto originario de una expresión técnica, que no son otra cosa que ampliaciones del concepto fundamental, ocurren muy frecuentemente en la matemática, pero no es la finalidad de este escrito ocuparse de ello pormenorizadamente.

Explicaciones al presente tratado.

"¿Qué son y para qué sirven los número?" fue innovador en dos direcciones, para la investigación de los fundamentos y para la teoría axiomática de conjuntos. Sobre la significación para la investigación sobre los fundamentos ha aludido de nuevo por primera vez recientemente Hilbert (Math. Ann. 104); un detenido análisis del escrito procedente de E. Zermelo se encuentra en el necrológico de Landau (Gött. Nachr. 1917). Cuán fuertemente la teoría axiomática de conjuntos ha sido influida por Dedekind lo muestra una comparación con los axiomas de Zermelo (Math. Anm. 65), que en parte están tomados directamente de las "definiciones" (§1 del escrito). Que por eso tuvo que postularse el "axioma del infinito", puesto que el intento de demostración de Dedekind (66) reposa en el concepto contradictorio de "cantidad de todo lo pensable", es sabido; asimismo, que en las reflexiones de Dedekind está implicado el axioma de elección (159). También la segunda demostración de Zermelo del teorema de la buena ordenación puede contemplarse como una transposición de la demostración dada aquí de la posibilidad de la inducción completa a la inducción transfinita; pero debería por lo demás ya aquí en los tranfinitos de añadirse el axioma de elección a los demás axiomas implícitamente utilizados por Dedekind. Dedekind podía prescindir de ello para la inducción completa acostumbrada, porque él tenía a su disposición la aplicación detallada en la definición de lo infinito. El teorema de la definición por inducción completa (126) que va más allá de la demostración por inducción completa ha sido agudamente elaborado para lo transfinito por J. v. Neumann (Math. Ann. 99). El teorema encuentra especial aplicación en el álgebra de dominios infinitos, y corresponde a cómo Dedekind obtiene las reglas de cálculo de los números entres gracias a la definición por inducción completa.

Noether.

Was sind und was sollen die Zahlen? R. Dedekind

Trad. e introd. por J. Ferreirós.

Página 8, línea -5. Dice el Sr. Ferreirós: "... La definición de Newton puede servirnos como resumen; en ella se resalta explícitamente la diferencia con respecto a los griegos:

> *Entendemos por número no tanto una multitud de unidades cuanto la razón entre una* cantidad abstracta *cualquiera y otra del mismo género que se toma como unidad.*"

Lo que dijo Newton:

> *By a Number we understand not so much a Multitude of Unities, as the* abstracted Ratio *of any Quantity to another Quantity of the same kind, which we take for Unity.*

No parece necesario, a la vista del texto de Newton, calificar lo incorrectamente calificado

---

Página 12, línea 8. Dice el Sr. Ferreirós: "... los complejos se presentan como pares ordenados de números reales, y las operaciones sobre los complejos se definen gracias a operaciones sobre los números reales que intervienen en el par. Con esto aparece, en 1837, la primera utilización del *método de construcción en aritmética*. Este método, ..., inspiró sin duda a numerosos matemáticos, que trataron de aplicarlo a las restantes extensiones del concepto de número, el más afortunado de los continuadores de Hamilton en esta empresa fue Dedekind."

Reconozco que tengo un conocimiento muy limitado, pero, hasta ahora, nunca había leido nada acerca de un llamado *método de construcción en aritmética*. Parecería más adecuado hablar, en este caso, no del mencionado método, sino de un procedimiento de construcción concreto, para la obtención de los complejos a partir de los reales, ya que los procedimientos establecidos por Dedekind, para la obtención de los reales a partir de los racionales, de los naturales a partir de su "demostración" de la existencia de conjuntos infinitos y de los enteros a partir de los naturales, no son subsumibles bajo el procedimiento de Hamilton. Después de todo, si el método de construcción en cuestión consiste, en definitiva, en generar una cierta entidad (numérica) sujeta a cumplir ciertas condiciones, a partir de algo (numérico) dado que tenga determinadas propiedades, entonces nos podríamos retrotraer, creo, hasta al propio Eudoxio.

Página 19, línea -2. Dice el Sr. Ferreirós: "... Las nuevas nociones abstractas que introdujo (Riemann), como las 'superficies de Riemann' en teoría de funciones complejas, y las 'variedades'de la geometría diferencial, constituyen el modelo al que Dedekind refirió siempre su introducción de nuevos conceptos algebraicos (cuerpo, anillo, módulo, ideal)."

Los conceptos matemáticos introducidos por Riemann requirieron un gran esfuerzo de clarificación, recordemos a H. Weyl con su trabajo sobre las superficies de Riemann, mientras que los propuestos por Dedekind son claros y distintos, por usar terminología cartesiana, desde el principio. Podría decirse

que, por su claridad meridiana y caracter perfeccionista, más bien hubiera sido el modo de hacer de Dedekind modelo para Riemann que no a la inversa, aunque las intuiciones riemannianas no tengan casi parangón en la historia de la matemática.

Página 22, línea 9. Dice el Sr. Ferreirós: "... Ya he aludido al hecho de que las teorías que Dedekind propuso acerca de la fundamentación del sistema numérico se basan en la teoría de conjuntos; casi parece más correcto leer *¿Qué son y para qué sirven los números?*(1888) como un libro sobre teoría de conjuntos, que como un libro acerca de los números naturales."

Es evidente que *¿Qué son y para qué sirven los números?* es, ante todo, un libro sobre los números naturales, pero tratado desde un punto de vista característicamente dedekindiano, i.e., algebraicamente. Porque en tal libro, más que teoría de conjuntos, que la hay, hay álgebra universal, e.g., Dedekind considera álgebras de los tipos (S, φ) y $(S, \varphi, 1)$ formadas por un conjunto S, una operación unaria $\varphi\colon S \longrightarrow S$ y un elemento distinguido $1 \in S$, define, en el punto 44, la subálgebra generada, en un álgebra del tipo (S, φ), por una parte $A \subseteq S$ y establece sus propiedades esenciales:

1. En el punto 48 establece que la subálgebra generada por A está caracterizada como la mínima subálgebra de (S, φ) que contiene a la parte A .
2. En el punto 45 demuestra que el operador de formación de subálgebras es extensivo o inflacionario.
3. A partir de lo establecido en el punto 51 se obtiene, como corolario evidente, que el operador de formación de subálgebras es idempotente.
4. En el punto 54 demuestra que el operador de formación de subálgebras es isótono.
5. En el punto 57 demuestra que, para las álgebras del tipo (S, φ), la operación estructural φ conmuta con el operador de formación de subálgebras.
6. En el punto 59 demuestra, para las álgebras del tipo (S, φ), lo que hoy se conoce como el principio de la demostración por inducción algebraica.
7. En el punto 61 demuestra que el operador de formación de subálgebras conmuta con las uniones de familias arbitrarias no vacías de partes no vacías de S. Este resultado es característico de las álgebras monounarias (S, φ), ya que para las álgebras, no necesariamente monounarias, lo que es cierto es que el operador de formación de subálgebras conmuta con las uniones de familias arbitrarias no vacías dirigidas superiormente de partes del conjunto subyacente del álgebra.
8. En el punto 89 define la relación "$<$" haciendo uso del hecho de que dispone de un álgebra libre.

Además de todo esto, en el punto 126 demuestra lo que hoy conocemos por el principio de la definición por recursión (algebraica) o que el álgebra $(\mathbb{N}, \mathrm{sc}, 1)$ es inicial en una categoría, de álgebras y morfismos, conveniente, y que, en este caso particular, también está en la base de la teoría de las funciones recursivas primitivas; en el punto 131 establece un teorema que (curiosamente) no numera y que dice que dada un álgebra del tipo (S, ω),

con $\omega\colon S \longrightarrow S$, y una parte A de S, la subálgebra de (S, ω) generada por A, A_0, es precisamente $A \cup \bigcup_{n\in\mathbb{N}} \omega^n[A]$, y recomienda que se relean los puntos 57 y 58, seguramente para que nos demos cuenta, ahora que disponemos de los números naturales, de que, por una parte, se puede dar otra demostración del teorema enunciado en el punto 57 y, por otra, que la subálgebra generada por una parte tiene otra descripción más explícita, más constructiva, como la unión de una cadena ascendente de subconjuntos de S, obtenida mediante la aplicación del principio de la definición por recursión, cosa que no podía hacer en el puntro 58, de donde el recurso a la intersección en la definición de la subálgebra generada por un subconjunto, por no disponer, hasta ahí, de los números naturales; en el punto 132 demuestra la unicidad esencial de los sistemas simplemente infinitos, i.e., el isomorfismo entre cierto tipo de álgebras; en el punto 133 tenemos, claramente establecido, el transporte de estructura, i.e., que la estructura es abstracta; en el punto 134 se considera lo que hoy en día se llaman tipos abstractos de datos, etc.

Página 22, línea -3(nota a pié de página). Dice el Sr. Ferreirós: "... Dedekind y Kronecker fueron los primeros en obtener una teoría satisfactoria de la factorización en cualquier *conjunto* de enteros algebraicos."

En lugar de *conjunto* debe decir: "anillo".

Página 22, línea 1. Dice el Sr. Ferreirós: "... Especialmente interesante es que Dedekind presentara un planteamiento abstracto de la noción de grupo..."

Dedekind definió, en el lugar al que se refiere el Sr. Ferreirós, el concepto de grupo *finito*, pero no el de grupo en general.

Página 26, línea 13. Dice el Sr. Ferreirós: "... 'Esbozo de una teoría de las congruencias superiores respecto a un módulo real primo'..."

Podría ser más conveniente decir: 'Esbozo de una teoría de las congruencias superiores respecto a un módulo primo genuino'.

Página 26, línea 13. Dice el Sr. Ferreirós: "... Así, vemos aparecer continuamente subgrupos, subcuerpos, *subideales*, ... y el hecho de que la *intersección de dos grupos*, etc. es de nuevo un grupo ... aparecen sólo la relación de inclusión y las operaciones de unión e intersección, echándose en falta especialmente *operaciones más fuertes* que Cantor empleará, como el producto cartesiano."

Es la primera vez en mi vida que leo el término 'subideal', seguramente se referirá el autor, simplemente, a los ideales de un anillo. Se trata de la intersección de subgrupos de un mismo grupo, no de la intersección de grupos distintos. Desde luego Dedekind trata también de la diferencia de conjuntos, que está al mismo nivel de complejidad que la unión y la intersección. Además considera conjuntos funcionales, e.g., en el punto 131, el de las aplicaciones de un conjunto S en sí mismo, llamado Ω, en el punto 159, los de las aplicaciones inyectivas de un Z_n en un conjunto Σ, que están al mismo nivel de complejidad que los productos cartesianos. Y si no trata, en la obra que nos ocupa, de otras operaciones conjuntistas, aparentemente, es porque

no las necesita para la obtención de sus fines. Dedekind se caracteriza, entre otras cosas, por establecer y usar el mínimo de nociones y construcciones para la obtención de sus fines, y es el caso que los conceptos, construcciones y demostraciones de Dedekind han quedado como modelos de las ciencias exactas (exceptuando la infame "demostración" del punto 66), por no hablar de lo esbozado en sus trabajos, de lo que nada mejor que las palabras de E. Noether: "... ya está en Dedekind".

Página 29, línea 7. Dice el Sr. Ferreirós: "... Demuestra que M' es un grupo, y por lo que sigue queda claro que está considerando la posibilidad de que la aplicación sea no sólo un isomorfismo, sino quizá un *homomorfismo* ..."

Debería el autor calificar al citado homomorfismo de sobreyectivo.

Página 29, línea -9. Dice el Sr. Ferreirós: "... la versión dada por Dedekind al problema de la factorización *ideal* ..."

Debería el autor decir: "... la versión dada por Dedekind al problema de la factorización de los ideales ...".

Página 34, línea 14. Dice el Sr.Ferreirós: "... Era fácil ver que el *mismo método* podía aplicarse para construir los números enteros sobre la base de los naturales, y los racionales sobre la base de los enteros ..."

Aquí el Sr. Ferreirós se esta refiriendo al método empleado por Hamilton en su construcción de los complejos. Es evidente que no se puede aplicar el mismo método para construir los números enteros sobre la base de los naturales, y los racionales sobre la base de los enteros. Porque, como es bien conocido, para obtener los enteros y los racionales no sólo se ha de considerar el producto cartesiano de dos conjuntos convenientes, sino que, además, se ha de pasar al cociente, no siendo este último paso necesario en el caso de Hamilton, aunque si en el de Cauchy y Kronecker para la construcción de los complejos como $R[X]/(X^2+1)$.

Página 34, línea -4. Dice el Sr. Ferreirós: "... Luego se ocupa de los racionales: si a y b designan enteros, definimos los racionales como pares (a, b) tales que ..."

Sería conveniente que el autor especificara que la segunda coordenada ha de ser un entero no nulo.

Página 36, línea -11. Dice el Sr. Ferreirós: "... El tomar como base el dominio de los números racionales con su aritmética, *la construcción de los reales por medio de ciertos objetos compuestos de infinitos elementos*, ..., todos estos son puntos de estrecho contacto entre ambas exposiciones."

Es innegable que hay un estrecho contacto entre dos teorías cuando ambas tratan de lo mismo. Pero el núcleo del asunto es que son *dos* teorías, no que traten de lo mismo. De hecho, los fundamentos de las teorías de Cantor y Dedekind sobre los números reales son radicalmente diferentes. Cantor considera, en primer lugar, las sucesiones fundamentales (de Cauchy), que ya de por sí son objetos de caracter infinitario, y, a continuación, define una

relación de equivalencia sobre el sistema de tales sucesiones, para acabar en un conjunto cociente, en el que cada una de las clases de equivalencia consta de una infinidad de elementos. Por su parte, Dedekind, en su construcción de los reales, no pasa al cociente. De hecho, matemáticamente, el procedimiento de Cantor para la construcción de los reales ha sido más fructífero que el de Dedekind, debido a que está en la base de los procedimientos de complección para los espacios no completos.

El Sr. Ferreirós tiene cierta tendencia, a mi modo de ver no suficientemente justificada, a ver estrechas relaciones entre teorías, por el mero hecho de que hablen o traten sobre lo mismo o cosas similares, cuando en realidad los fundamentos o métodos sobre los que se sustentan dichas teorías son radicalmente distintos y, por lo tanto, son susceptibles de generalizaciones o aplicaciones más o menos fructíferas.

Página 40, línea 5. Dice el Sr. Ferreirós: "... y en el caso de las sucesiones fundamentales se presuponen también ciertas propiedades *topológicas* ..."

Aquí el autor debería referirse a propiedades uniformes, más que a propiedades topológicas.

Página 46, línea 2. Dice el Sr. Ferreirós: "... y todo conjunto infinito puede hacerse corresponder biunívocamente con un *subconjunto* suyo."

Debería calificar el autor al subconjunto de propio o estricto.

Página 52, línea 9. Dice el Sr. Ferreirós: "... El caso es que en la época en que publicó ... tanto Cantor como el *famoso* lógico Frege ..."

Si el autor se refiera a la fama de Frege en el entorno de 1888, hay que dudar, por demasiado conocido, de que tal fuera el caso. Desgraciadamente Frege fué conocido a partir de 1902, a raíz de la paradoja de Russell.

Página 53, línea 18. Dice el Sr. Ferreirós: "... A este respecto hay que decir que aunque propiamente define la inyectividad, *en la práctica considera aplicaciones biyectivas*"

Esa afirmación se dá de bruces contra el propio texto de Dedekind, ya que éste usa las inyectivas cuando procede, e.g., en el §14, punto 159, y las biyectivas cuando lo exige el asunto, e.g., al tratar de la equipotencia entre los conjuntos.

Página 55, línea 12. Dice el Sr. Ferreirós: "... Dedekind dice que el conjunto C es una φ-cadena. Los conjuntos C *isomorfos* a $\aleph$ se caracterizan porque son φ-cadenas para una aplicación φ biyectiva y porque hay un único elemento de C, al que llamamos 1, que no pertenece a $\varphi(C)$."

Para definir las cadenas Dedekind considera, en primer lugar, un par (S, φ) formado por un conjunto S y una endoaplicación φ de S, y, a continuación, dice que una parte K de S es una φ-cadena si $\varphi[K] \subseteq K$, i.e., con la terminología actual, si K es una subálgebra del álgebra monounaria (S, φ). Por otra parte, en la frase citada en lugar de "$\aleph$"debe decir "$\mathbb{N}$" y, además, que las álgebras (C, φ, e) isomorfas a $(\mathbb{N}, \mathrm{sc}, 0)$ (por usar la terminología actual,

Mac Lane, Lawvere, etc.) son precisamente las que cumplen las siguientes condiciones:

1. La aplicación $\varphi\colon C \longrightarrow C$ es inyectiva.
2. $e \notin \mathrm{Im}(\varphi)$.
3. Para cada subconjunto K de C, si $e \in K$ y $\varphi[K] \subseteq K$, entonces $K = C$.

Página 56, línea -9. Dice el Sr. Ferreirós: "...

δ. φ es una aplicación biyectiva.

La aplicación biyectiva φ ..."

Dedekind dice bien *claramente* que se trata de una aplicación inyectiva, jamás de una biyectiva.

Página 57, línea 4. Dice el Sr. Ferreirós: "... cada elemento de $\aleph$ da lugar a una φ-cadena, que es *el conjunto de todos sus sucesores* ..."

Debería especificar el Sr. Ferreirós que es el conjunto de todos sus sucesores incluido el propio elemento. Además, se repite el error tipográfico de usar "$\aleph$"en lugar de "$\mathbb{N}$".

Página 58, línea 2. Dice el Sr. Ferreirós: "... concibiendo las operaciones aritméticas como aplicaciones de $\mathbb{N}$ en $\mathbb{N}$."

Debería decir: "... concibiendo las operaciones aritméticas como aplicaciones de potencias finitas de $\mathbb{N}$ en $\mathbb{N}$."

Página 60, línea 13. Dice el Sr. Ferreirós: "... Adentrarse en el terreno de la lógica, ..., suponía un cierto atrevimiento por parte de Dedekind. ... Ernst Schröder escribió:

> *... cuánto tenía que mejorarse el desarrollo del cálculo lógico para posibilitar el establecimiento de la conexión perdida [entre la lógica y la aritmética] ...*"

Considerando lo que Dedekind hace en su libro se llega a la conclusión de que se adentra, no sólo ni fundamentalmente, en el terreno de la lógica, sino en el del álgebra general y que, con visos de certeza, la conexión perdida entre la lógica y la aritmética es, según Dedekind, lo que hoy llamaríamos, el álgebra universal. Podría decirse, atendiendo al contenido del libro de Dedekind, que entiende por lógica la inferencia lógica, Aristotélica–Booleana, junto a un fragmento del álgebra universal y otro de la teoría de conjuntos.

En la página 67 el Sr. Ferreirós habla, por dos veces, de aplicaciones biyectivas, cuando debería decir inyectivas.

Página 70, línea 9. Dice el Sr. Ferreirós: "... antes de cumplir la respetable *cifra* de 80 años ..."

Creo que los seres humanos cumplimos años, no cifras.

Respecto de la bibliografía proporcionada por el Sr. Ferreirós observamos que, siendo escasa en castellano, la hace más breve de lo que en realidad

es, debería haber citado un notable trabajo sobre Dedekind de Josep Pla i Carrera que lleva por título: "Dedekind y la teoría de conjuntos", publicado en Modern Logic el año 1993, vol. 3, págs 215–305, así como, en italiano, el clásico de Oscar Zariski, a instancia de F. Enriques, o el más reciente, también en italiano, de Francesco Gana titulado: "Scritti sui fondamenti della matematica", publicado por Bibliopolis el año 1982, con el que, por feliz casualidad, el libro del Sr. Ferreirós tiene ciertas notables coincidencias en cuanto a la selección de material y otros asuntos.

Hay muchas más cosas que se podrían decir sobre la introducción del Sr. Ferreirós, pero por ser polémicas y para no cansarle dejo el asunto de la introducción en este punto.

Por lo que respecta a la traducción de "Was sind und was sollen die Zahlen?" podríamos decir que como en todas, algo se perdió en el proceso, e.g., lo que sigue.

Página 111, línea 7. Dice el Sr. Ferreirós: "... Los sistemas R, S se llaman *similares* cuando existe una aplicación φ de S tal que ..."

Falta añadir, respecto de φ, lo que dice Dedekind de ella: que φ es inyectiva (con el lenguaje actual).

Página 111, línea -9. Dice el Sr. Ferreirós: "... Si es una aplicación ..."

Debe decir: "... Si φ es una aplicación ..."

Página 114, línea -18. Dice el Sr. Ferreirós: "... como parte común de los sistemas A, Σ ..."

Debe decir: "... como parte común de los sistemas A_0, Σ ..."

Página 115, demostración del Teorema 63.

Demostración. De $L \subseteq K$, deducimos que $\varphi[L] \subseteq \varphi[K]$, pero $\varphi[K] \subseteq L$, así que $\varphi[L] \subseteq L$, i.e., L es una φ-cadena.

Supongamos que $L \subset K$, que $U_0 \subset K$, siendo $U = K - L$, y que $V = K - U_0$. Entonces $K = U_0 \cup V$ y $L = \varphi[U_0] \cup V$.

Es evidente que $K = U_0 \cup V$, porque $V = K - U_0$.

Para demostrar que $L = \varphi[U_0] \cup V$, establecemos, como lema, que $U_0 = U \cup \varphi[U_0]$. Puesto que $U \subseteq U_0$ y $\varphi[U_0] \subseteq U_0$, tenemos que $U \cup \varphi[U_0] \subseteq U_0$. Para demostrar la inclusión inversa, es suficiente que demostremos que $\varphi[U \cup \varphi[U_0]] \subseteq U \cup \varphi[U_0]$. Ahora bien, $\varphi[U \cup \varphi[U_0]] = \varphi[U] \cup \varphi[\varphi[U_0]]$. Por otra parte, de $U \subseteq U_0$, obtenemos que $\varphi[U] \subseteq \varphi[U_0]$; además, $\varphi[U_0] \subseteq U_0$, luego $\varphi[\varphi[U_0]] \subseteq \varphi[U_0]$, así que $\varphi[U] \cup \varphi[\varphi[U_0]] \subseteq \varphi[U_0]$, luego $\varphi[U] \cup \varphi[\varphi[U_0]] \subseteq U \cup \varphi[U_0]$. Por lo tanto $U_0 \subseteq U \cup \varphi[U_0]$. De donde la igualdad $U_0 = U \cup \varphi[U_0]$.

Demostramos ahora que $L = \varphi[U_0] \cup V$. Ahora bien, de $U_0 \subset K$, obtenemos que $\varphi[U_0] \subseteq \varphi[K]$, pero $\varphi[K] \subseteq L$, así que $\varphi[U_0] \subseteq L$. Por otra parte, a partir de $U \subseteq U_0$ concluimos que $V = K - U_0 \subseteq K - U = K - (K - L) = L$, i.e., que $V \subseteq L$. De modo que $\varphi[U_0] \cup V \subseteq L$. Para inclusión inversa, teniendo en cuenta que K se puede representar como $K = U \cup L$ y como $K = U \cup (\varphi[U_0] \cup V)$, porque $K = U_0 \cup V$ y $U_0 = U \cup \varphi[U_0]$, concluimos que L no puede estar incluido en U, porque $U = K - L$, así que $L \subseteq \varphi[U_0] \cup V$. De donde la igualdad.

Suponiendo ahora que $L = \varphi[K]$, podemos afirmar, por lo anterior, que $\varphi[K] = \varphi[U_0] \cup V$. Pero $K = U_0 \cup V$, así que $\varphi[K] = \varphi[U_0] \cup V$, luego $\varphi[U_0] \cup \varphi[V] = \varphi[U_0] \cup V$. Pero $V \subseteq \varphi[U_0] \cup V$, así que $V \subseteq \varphi[U_0] \cup \varphi[V]$.

Falta demostrar que V no puede estar incluido en $\varphi[U_0]$. Ahora bien, $\varphi[U_0] \subseteq U_0$ y $V = K - U_0$, luego V no puede estar incluido en $\varphi[U_0]$, ya que si lo estuviera, estaría incluido en U_0, lo cual sería absurdo. □

De este teorema se deduce el siguiente Teorema: Si un conjunto M es isomorfo a una de sus partes M', entonces es isomorfo a cualquier otra parte T de M que contenga a M'.

Demostración. Sea f una biyección, arbitraria, pero fija, de M en M', $Q = T - M'$ y $\mathcal{T}_{M',T}$ el conjunto definido como:

$$\mathcal{T}_{M',T} = \{\, A \subseteq M \mid Q \subseteq A \ \ \&\ \ f[A] \subseteq A \,\}.$$

Entonces $M \in \mathcal{T}_{M',T}$, i.e., $\mathcal{T}_{M',T} \neq \varnothing$. Sea $A_0 = \bigcap_{A \in \mathcal{T}_{M',T}} A$. Entonces $Q \subseteq A_0$ y $f[A_0] \subseteq A_0$ (por lo tanto $A_0 \in \mathcal{T}_{M',T}$). Se cumple que $A_0 = Q \cup f[A_0]$. Que $Q \cup f[A_0] \subseteq A_0$ es obvio.

Para demostrar la inclusión inversa, i.e., que $A_0 \subseteq Q \cup f[A_0]$, sea $r \in A_0 - Q$. Supongamos que $r \notin f[A_0]$, entonces $f[A_0] \subseteq A_0 - \{r\}$, luego $f[A_0 - \{r\}] \subseteq A_0 - \{r\}$ (porque $A_0 - \{r\} \subseteq A_0$ y $f[\cdot]$ es isótona). Pero $Q \subseteq A_0 - \{r\}$ (porque $Q \subseteq A_0$ y $r \notin Q$). Así que $A_0 - \{r\} \in \mathcal{T}_{M',T}$, pero $A_0 - \{r\} \subset A_0$, contradicción. Por lo tanto $A_0 = Q \cup f[A_0]$. De donde $T = A_0 \cup (M' - f[A_0])$, ya que $T = Q \cup M'$ y $Q \cup M' = (Q \cup f[A_0]) \cup (M' - f[A_0])$. Pero A_0 es isomorfo a $f[A_0]$, luego T es isomorfo a $f[A_0] \cup (M' - f[A_0])$. Ahora bien, $f[A_0] \cup (M' - f[A_0]) = M'$ y M' es isomorfo a M, así que T es isomorfo a M. □

De este último teorema se deduce el teorema de Cantor-Bernstein, tal como hizo Dedekind.

Página 117, línea 15. Dice el Sr. Ferreirós: "... si a es un elemento de S, y si el conjunto T de todos los elementos de S diferentes de a es finita ..."

Debe decir: "... si a es un elemento de S, y si el conjunto T de todos los elementos de S diferentes de a es finito ..."

Página 128, línea -14. Dice el Sr. Ferreirós: "... Como queda así completamente determinada ..."

Debe decir: "... Como ψ queda así completamente determinada ..."

Página 130, línea -4. Dice el Sr. Ferreirós: "... Consideramos un sistema Ω cuyos elementos toleran una determinada composición tal que de un elemento surge siempre ..."

Debe decir: "... Consideramos un sistema Ω cuyos elementos toleran una determinada composición tal que de un elemento ν surge siempre ..."

Página 134, línea 20. Dice el Sr. Ferreirós: "... 135. *Definición.* Es natural aplicar la definición de una aplicación de la serie ..."

Debe decir: "... 135. *Definición.* Es natural aplicar la definición de una aplicación ψ de la serie ..."

Llega ahora el turno de las Notas del Editor.

En la primera nota de las páginas 181–182 dice el Sr Ferreirós: "... Kronecker estudió en Berlín ... su principal maestro fue E. Kummer(1810–1893) ... No ocupó (Kronecker) una plaza universitaria hasta 1883, tras la muerte de Kummer, pero desde...". Es obvio que la situación descrita es imposible y necesita rectificación.

En la nota número 24 de las páginas 187–188 se dice por tres veces "aplicación biyectiva" cuando debería decir "aplicación inyectiva". Además, en la penúltima línea de la página 187 dice "de un infinitos elementos k", cuando debería decir "de una infinidad de elementos k". Por otra parte, en la página 188, línea 6, dice "... Dedekind postula que el conjunto de aplicaciones de cada Z_n ...", cuando debería decir "... Dedekind postula que el conjunto de las aplicaciones inyectivas de cada Z_n ...".

Puesto que se dice algo, en la misma nota, acerca del uso de alguna forma del axioma de elección en la demostración del Teorema del punto 159 del §14, parece conveniente reconsiderar tal Teorema.

Teorema 0.10. *Si Σ es un sistema infinito, entonces cada uno de los sistemas numéricos Z_n definidos en 98 es fielmente representable en Σ (es decir, es isomorfo a una parte de Σ), y recíprocamente.*

Demostración. Si Σ es un sistema infinito, entonces, por 72, existe ciertamente una parte T de Σ simplemente infinita, y por lo tanto, por 132, isomorfa a la serie numérica $\mathbb{N}$, luego, por 35, cada sistema Z_n, siendo parte de $\mathbb{N}$, es isomorfo a una parte de T y por lo tanto también a una parte de Σ, c.q.d.

La demostración del teorema recíproco, por obvio que pueda parecer, es más compleja. Si cada sistema Z_n es fielmente representable en Σ, a cada número n le corresponde una aplicación inyectiva α_n de Z_n tal que $\alpha_n[Z_n] \subseteq \Sigma$. De la existencia de tal serie de aplicaciones α_n, que consideramos como dada, y sobre la cual no hacemos otras suposiciones,

> ⟦Lo que hace aquí Dedekind es, bajo la hipótesis de que, para cada $n \in \mathbb{N}$, $\mathrm{Mono}(Z_n, \Sigma)$, el conjunto de las aplicaciones inyectivas de Z_n en $\mathbb{N}$, no es vacío, elegir un $(\alpha_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathrm{Mono}(Z_n, \Sigma)$ totalmente arbitrario (**aplicación implícita del axioma de elección numerable, según Zermelo**)⟧

deducimos en primer lugar, con la ayuda del teorema 126, la existencia de una nueva serie de aplicaciones análoga ψ_n dotadas de la propiedad especial de que cada vez que se tenga $m \leq n$, o sea (por 100) cuando $Z_m \subseteq Z_n$, la aplicación ψ_m de Z_m está contenida en la aplicación ψ_n de Z_n, es decir las aplicaciones ψ_m y ψ_n coinciden completamente para todos los números contenidos en Z_m, y por lo tanto siempre se cumple que

$$\psi_m(m) = \psi_n(m).$$

Para aplicar el teorema mencionado (126) con este objetivo, tomemos como Ω el sistema de todas las posibles aplicaciones inyectivas de todos los sistemas Z_n en Σ

> ⟦Así que $\Omega = \bigcup_{n\in\mathbb{N}} \mathrm{Mono}(Z_n, \Sigma)$⟧

y utilicemos las aplicaciones α_n, que están ellas mismas contenidas en Ω, para definir una aplicación θ de Ω en sí mismo. Sea β cualquier elemento de Ω, es decir, por ejemplo, una aplicación inyectiva de un sistema determinado Z_n en Σ; entonces el sistema $\alpha_{n'}[Z_{n'}]$ no puede ser parte de $\beta[Z_n]$, porque en caso contrario $Z_{n'}$ sería isomorfo, por 35, a una parte de Z_n, es decir, por 107, a una parte propia de sí mismo, y por lo tanto resultaría ser un sistema infinito, lo cual entraría en contradicción con el teorema 119; por lo tanto en $Z_{n'}$ hay ciertamente uno o más números p tales que $\alpha_{n'}(p)$ no está contenido en $\beta[Z_n]$; para fijar las ideas, escojamos siempre el mínimo k (96) de los susodichos números p y, dado que, por 108, $Z_{n'}$ está compuesto por Z_n y n', definamos la imagen $\gamma(m) = \beta(m)$ y además $\gamma(n') = \alpha_{n'}(k)$; ahora a esta aplicación γ de $Z_{n'}$ en Σ, que evidentemente es fiel, la consideramos como la imagen $\theta(\beta)$ de la aplicación β, y de este modo queda completamente definida una aplicación θ del sistema Ω en sí mismo.

> ⟦En esta parte Dedekind define explícitamente una aplicación $\theta\colon \Omega \longrightarrow \Omega$, ahora bien, puesto que $\Omega = \bigcup_{n\in\mathbb{N}} \mathrm{Mono}(Z_n, \Sigma)$, siendo la unión disjunta, dar la endoaplicación θ de Ω equivale, por la propiedad universal del coproducto, a dar una familia $(\theta_n)_{n\in\mathbb{N}}$ en la que, para cada $n \in \mathbb{N}$, θ_n es una aplicación de $\mathrm{Mono}(Z_n, \Sigma)$ en Ω, i.e., hay que elegir un $(\theta_n)_{n\in\mathbb{N}}$ de $\prod_{n\in\mathbb{N}} \mathrm{Hom}(\mathrm{Mono}(Z_n, \Sigma), \Omega)$. Pero resulta que, para cualesquiera $n \in \mathbb{N}$ y $\beta \in \mathrm{Mono}(Z_n, \Sigma)$, $\theta_n(\beta)\colon Z_{n'} \longrightarrow \Sigma$ es precisamente la aplicación γ definida por Dedekind. De modo que aquí no se hace uso del axioma de elección, porque las componentes de la familia $(\theta_n)_{n\in\mathbb{N}}$ están definidas explícitamente y, además, uniformemente o naturalmente, i.e., de la misma manera⟧

Una vez determinadas las cosas denominadas Ω y θ en 126, escojamos como elemento de Ω denotado por ω la aplicación dada α_1; de esa manera, por 126, resulta determinada una aplicación ψ de la serie numérica $\mathbb{N}$ en Ω que satisface las condiciones

II. $\psi_1 = \alpha_1$,
III. $\psi_{n'} = \theta(\psi_n)$,

donde la imagen de un número n es indicada por ψ_n en lugar de por $\psi(n)$. Demostramos en primer lugar por inducción completa (80) que ψ_n es una aplicación inyectiva de Z_n en Σ; en efecto,

ρ. por II esto es verdadero para $n = 1$, y
σ. si este enunciado es verdadero para un número n, entonces por III y basándose en la transformación θ de β en γ descrita anteriormente, lo mismo vale también para el sucesor n', c.q.d.

Ahora demostramos, también por inducción completa (80), que para cualquier número m, la propiedad enunciada anteriormente

$$\psi_n(m) = \psi_m(m)$$

pertenece efectivamente a todos los números $n \geq m$, y por lo tanto, por 93 y 74, contenidos en la cadena m_0; en efecto,

ρ. esto es inmediatamente evidente para $n = m$, y

σ. si tal propiedad pertenece a un número n entonces, siempre por III y por la naturaleza misma de θ se sigue que también pertenece al sucesor n', c.q.d.

Una vez establecida esta propiedad particular de la nueva serie de aplicaciones ψ_n, nuestro teorema se demuestra fácilmente. Definimos una aplicación χ de la serie numérica $\mathbb{N}$, haciendo corresponder a cada número n la imagen $\chi(n) = \psi_n(n)$; está claro que, por 21, todas las aplicaciones ψ_n están contenidas en esta aplicación χ. Puesto que ψ_n es una aplicación de Z_n en Σ se sigue sin más que también la serie numérica $\mathbb{N}$ está representada mediante χ en Σ, luego $\chi[\mathbb{N}] \subseteq \Sigma$. Sean ahora m y n números diferentes; en virtud de la simetría es lícito suponer, por 90, que $m < n$; entonces, basándose en lo que precede, tenemos que $\chi(m) = \psi_m(m)$ y $\chi(n) = \psi_n(n)$, pero dado que ψ_n era una aplicación inyectiva de Z_n en Σ, y puesto que m y n son elementos diferentes de Z_n, $\psi_n(m)$ es diferente de $\psi_n(n)$, luego también $\chi(m)$ es diferente de $\chi(n)$, así que χ es una aplicación inyectiva de $\mathbb{N}$. Puesto que además $\mathbb{N}$ es un sistema infinito (71), lo mismo se puede decir, por (67), del sistema $\chi[\mathbb{N}]$ equipotente a él y, por 68, debido a que $\chi[\mathbb{N}]$ es parte de Σ, también Σ es un sistema infinito, c.q.d. □

Para la demostración del teorema precedente puede ser de utilidad la consideración de los siguientes diagramas:

$$\begin{array}{ccc} \mathrm{Mono}(Z_n,\Sigma) & \xrightarrow{\mathrm{in}_n} & \Omega = \bigcup_{n\in\mathbb{N}} \mathrm{Mono}(Z_n,\Sigma) \\ & \searrow^{\theta_n} & \downarrow \theta = [\theta_n]_{n\in\mathbb{N}} \\ & & \Omega = \bigcup_{n\in\mathbb{N}} \mathrm{Mono}(Z_n,\Sigma) \end{array}$$

$$\theta_n \begin{cases} \mathrm{Mono}(Z_n,\Sigma) \longrightarrow \Omega & \\ \qquad \beta \qquad \longmapsto \theta_n(\beta) & \begin{cases} Z_{n'} \longrightarrow \Sigma & \\ \qquad m \quad \longmapsto & \begin{cases} \beta(m), & \text{si } m \in Z_n; \\ \alpha_{n'}(k), & \text{si } m = n', \end{cases} \end{cases} \end{cases}$$

siendo $k = \min\{\, p \in Z_{n'} \mid \alpha_{n'}(p) \notin \beta[Z_n] \,\}$. Observemos que el propio Dedekind, apunta a otras posibles definiciones, e.g., podría haber definido $k = \max\{\, p \in Z_{n'} \mid \alpha_{n'}(p) \notin \beta[Z_n] \,\}$.

$$\begin{array}{ccccc} & & \mathrm{N} & \xleftarrow{\mathrm{sc}} & \mathrm{N} \\ & \overset{\kappa_1}{\nearrow} & \downarrow \psi & & \downarrow \psi \\ 1 & & & & \\ & \underset{\kappa_{\alpha_1}}{\searrow} & & & \\ & & \Omega = \bigcup_{n\in\mathbb{N}} \mathrm{Mono}(Z_n,\Sigma) & \xleftarrow[\theta]{} & \Omega = \bigcup_{n\in\mathbb{N}} \mathrm{Mono}(Z_n,\Sigma) \end{array}$$

en el que κ_1 es la aplicación que al único miembro de 1 le asigna 1, κ_{α_1} la aplicación que al único miembro de 1 le asigna α_1 y $\psi = (\psi_n)_{n\in\mathbb{N}}$.

El Sr. Ferreirós en la página 188, línea 3, dice: "...Por tanto, para considerar χ como algo dado necesitamos apelar al axioma de elección en su versión numerable. ..."

Es evidente que no hay que apelar al axioma de elección numerable ni a ninguna corte suprema para poder afirmar que se dispone de χ, porque la aplicación χ de $\mathbb{N}$ en Σ está definida *explícitamente*, haciendo uso de la familia $(\psi_n)_{n\in\mathbb{N}}$, que fué obtenida, mediante el principio de la definición por recursión, a partir de α_1 y de θ. De hecho χ es la única aplicación de $\mathbb{N}$ en Σ tal que, para cada $n \in \mathbb{N}$, el diagrama:

$$\begin{array}{ccc} \{n\} & \xrightarrow{\mathrm{in}_{\{n\},\mathbb{N}}} & \mathbb{N} = \bigcup_{n\in\mathbb{N}}\{n\} \\ {\scriptstyle \mathrm{in}_{\{n\},Z_n}}\downarrow & & \downarrow{\scriptstyle \chi = \left[\psi_n \circ \mathrm{in}_{\{n\},Z_n}\right]_{n\in\mathbb{N}}} \\ Z_n & \xrightarrow[\psi_n]{} & \Sigma \end{array}$$

conmuta, siendo $\mathrm{in}_{\{n\},Z_n}$ la aplicación que a $n \in \{n\}$ le asigna $n \in Z_n$. No cabe duda de que Dedekind conocía muy bien como definir aplicaciones desde uniones disjuntas de conjuntos hasta un cierto conjunto, cuando por cada una de las componentes se dispone de una aplicación hasta tal conjunto (en el fondo, tal procedimiento está implícito, dos veces, en la demostración del teorema que nos ocupa), no en vano editó y publicó, en particular, el trabajo de Riemann sobre las variedades.

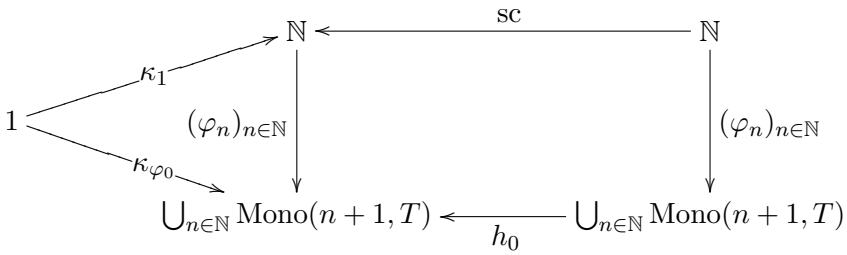
Observemos que si el argumento del Sr. Ferreirós fuera correcto, entonces también se podría decir que θ, por estar en correspondencia con la familia $(\theta_n)_{n\in\mathbb{N}}$, se obtiene haciendo uso del axioma de elección numerable, que no es el caso, debido a que las componentes de $(\theta_n)_{n\in\mathbb{N}}$ tienen una definición explícita y uniforme, como ocurre con χ. Parece ser que el Sr. Ferreirós no toma en consideración que no siempre que hay que elegir hemos de recurrir obligatoriamente al axioma de elección, y desde luego cuando dispongamos de un proceso normado, como los anteriores, nunca.

Cantor, en el trabajo de 1895, traducción al inglés, pág. 105, establece que: Every transfinite aggregate T has parts with the cardinal number $\aleph_0$.

Una demostración del citado teorema puede ser la siguiente. Consideremos, por una parte, la familia de conjuntos $(\mathrm{Mono}(n+1,T))_{n\in\mathbb{N}}$, y, por otra, la familia de aplicaciones de transición $(f_{n,n-1})_{n\in\mathbb{N}-1}$, en la que, para $n \in \mathbb{N}-1$, $f_{n,n-1}$ es la aplicación de $\mathrm{Mono}(n+1,T)$ en $\mathrm{Mono}(n,T)$ obtenida a partir de la inclusión canónica $\mathrm{in}_{n,n+1}$ de n en $n+1$. De modo que $f_{n,n-1}$ asigna a cada aplicación inyectiva φ de $n+1$ en A la aplicación inyectiva $\varphi \circ \mathrm{in}_{n,n+1}$, i.e., la restricción de φ a n. De este modo obtenemos un sistema proyectivo de conjuntos, denotado por $\mathcal{M}(T)$.

Se cumple que cada una de las aplicaciones de transición $f_{n,n-1}$ es sobreyectiva y que cada uno de los conjuntos $\mathrm{Mono}(n+1,T)$ no es vacío. Haciendo uso del axioma de elección, elegimos una familia $(g_{n-1,n})_{n\in\mathbb{N}-1}$ en la que, para $n \in \mathbb{N}-1$, $g_{n-1,n}$ es una aplicación de $\mathrm{Mono}(n,T)$ en $\mathrm{Mono}(n+1,T)$ tal que $f_{n,n-1} \circ g_{n-1,n}$ es la identidad en $\mathrm{Mono}(n,T)$. Entonces se cumple, haciendo uso del principio de la definición por recursión, que, para cada $n \in \mathbb{N}$, la aplicación estructural f_n de $\varprojlim \mathcal{M}(T)$ en $\mathrm{Mono}(n+1,T)$ es sobreyectiva.

Para la aplicación del principio de la definición por recursión en la demostración de que, por ejemplo, f_0 es sobreyectiva consideramos el diagrama



en el que κ_1 es la aplicación que al único miembro de 1 le asigna 1, κ_{φ_0} la aplicación que al único miembro de 1 le asigna φ_0, un elemento arbitrario, pero fijo, de $\mathrm{Mono}(1,T)$ y h_0 la aplicación $[\mathrm{in}_2 \circ g_{0,1}, \mathrm{in}_3 \circ g_{1,2}, \ldots]$. Puesto que, para cada $n \in \mathbb{N}$, se tiene que $\mathrm{Mono}(n+1,T)$ no es vacío, podemos afirmar que $\varprojlim \mathcal{M}(T)$ tampoco es vacío, por un teorema de Bourbaki, luego T tiene partes con el número cardinal $\aleph_0$.

También podría ser de cierto interés poner de relieve que en el punto final del libro de Dedekind, al considerar el concepto de multiplicidad, Dedekind está apuntando hacia lo que hoy en día se denominan *multiconjuntos*, y también a que tales multiconjuntos no cumplen el principio de la extensionalidad (que recoge el hecho de la distinción entre los objetos de un mismo conjunto), que es, junto al principio de la definitud (precisión, no ambigüedad, nitidez), uno de los principios característicos de una de las últimas definiciones clásicas de conjunto propuesta por Cantor, precisamente la que dice: "Por un 'conjunto' entendemos cualquier colección acabada (en un todo) M de objetos definidos y distintos m de nuestra intuición o pensamiento (que serán llamados los 'elementos'de M)".

Para finalizar, y respecto del concepto de "creación" en Dedekind, podría ser interesante señalar que tal término lo usa, en "Continuidad y números irracionales", de un modo que se asemeja a una aplicación del esquema axiomático de reemplazo. Además, hay que poner de manifiesto que el supuesto logicismo de Dedekind se limita, única y exclusivamente, al hecho de que nuestro autor, afirma que la aritmética es "parte de la lógica". Pero lo que está queriendo decir con ello Dedekind es, simplemente, que el concepto de número es independiente de las intuiciones del espacio y del tiempo, en el sentido kantiano. Se es lo que se hace, y Dedekind no propone ningún sistema lógico, al estilo de Frege, logicista confeso y consecuente, como fundamento de la matemática, sino que algebriza la aritmética, en el sentido del álgebra universal e incluso con atisbos del modo de hacer propio de la teoría de categorías.

> It was a commonplace belief among philosophers and mathematicians of the 19th century that the existence of infinite sets could be proved, and in particular the set of natural numbers could be "constructed" out of thin air, "by logic alone." All the proposed "proofs" involved the faulty General Comprehension Principle in some form or other. We know better now: *Logic can codify the valid forms of reasoning but it cannot prove the existence of anything, let alone infinite sets.* By taking account of this fact cleanly and explicitly in the formulation of his axioms, Zermelo made a substantial contribution to the process of purging logic of ontological concerns, a necessary step in the rigurous development of logic as a science in its own right in our century.
>
> *Y. Moschovakis.*

> Brouwer made it clear, as I think beyond any doubt, that there is no evidence supporting the belief in the existential character of the totality of all natural numbers ... The sequence of numbers which grows beyond any stage already reached by passing to the next number, is the manifold of possibilities open towards infinity: it remains forever in the state of creation but is not a closed realm of things existing in themselves. That we blindly converted one into the other is the true source of our difficulties, including the antinomies – a source of more fundamental nature than Russell's vicious principle indicated. Brouwer mathematics, nourished by a belief in the 'absolute' that transcends all possibilities of realization, goes beyond such statements as can claim real meaning and truth founded on evidence.
>
> *H. Weyl.*

En este sección enunciamos el axioma del conjunto infinito, que nos permitirá demostrar la existencia de un álgebra de Dedekind-Peano y, para tales álgebras, obtendremos el principio de la definición por recursión finita, a partir del cual demostraremos que las álgebras de Dedekind-Peano son esencialmente únicas, y que otros principios de definición por recursión más complejos, se pueden obtener a partir del mismo. Además, demostraremos que el conjunto subyacente del álgebra Dedekind-Peano, que será el conjunto de los números naturales, está dotado de una buena ordenación, y que tal ordenación es compatible con las operaciones aritméticas usuales, definidas por recursión, sobre el conjunto de los números naturales.

Los axiomas de la teoría de conjuntos de **ZFSk** hasta ahora enunciados, sólo nos permiten afirmar la existencia de una infinidad de conjuntos distintos, e.g., los conjuntos $\varnothing$, $\{\varnothing\}$, $\{\{\varnothing\}\}$, ..., pero no, y éste será el primer gran salto de lo finito a lo transfinito, la existencia de un conjunto, actualmente, *infinito*. Para poder asegurar la existencia de al menos un conjunto infinito, procedemos axiomáticamente, tal como hizo Zermelo.

0.1. El axioma del conjunto infinito. Antes de enunciar el axioma del conjunto infinito, recordamos que si A es un conjunto, entonces A^+ denota el conjunto sucesor de A, que es $A \cup \{A\}$.

Axioma del conjunto infinito. *Hay al menos un conjunto del cual es miembro el conjunto vacío, y que está cerrado bajo la operación de formación*

del sucesor de un conjunto:

$$\exists A\,(\varnothing \in A \wedge \forall x\,(x \in A \rightarrow x^{+} \in A)).$$

El axioma del conjunto infinito, bajo la forma anterior, se debe a von Neumann; el que propuso Zermelo es:

$$\exists A\,(\varnothing \in A \wedge \forall x\,(x \in A \rightarrow \{x\} \in A)).$$

Obsérvese que lo que diferencia al axioma propuesto por von Neumann del propuesto por Zermelo, reside en la operación de formación del conjunto sucesor, que, en el caso de von Neumann, es la que a un conjunto x la asigna x^{+} y, en el de Zermelo, la que a x le asigna $\{x\}$.

De ahora en adelante usaremos el propuesto por von Neumann.

Antes de proseguir con la obtención de algunas de las consecuencias de la admisión del nuevo axioma, conviene recordar que Dedekind, después de definir a los conjuntos *infinitos* como aquéllos que son isomorfos a un subconjunto estricto de sí mismos, transformando de este modo un teorema de Galileo, según el cual hay tantos números naturales como cuadrados de los mismos, en una definición; propuso, como *teorema*, la existencia de al menos un conjunto infinito. De dicho *teorema* dió la siguiente *demostración*:

> El mundo de mis pensamientos, es decir, la totalidad S de todas las cosas que pueden ser objeto de mi pensamiento es infinito. De hecho, si s indica un elemento de S, el pensamiento s' de que s puede ser objeto de mi pensamiento es él mismo un elemento de S. Si se considera s' como la imagen $\varphi(s)$ del elemento s, entonces la representación φ de S determinada de esa manera tiene la propiedad de que la imagen S' es parte de S; además, S' es parte propia de S, ya que en S hay elementos (e.g., mi propio yo) diferentes de cada pensamiento de la forma s', y por lo tanto no contenido en S'. Por último, está claro que si a y b son elementos distintos de S, entonces las imágenes a' y b' serán diferentes, es decir φ es una representación inyectiva. Por consiguiente, S es infinito.

Sin entrar en los problemas que plantean los aspectos no matemáticos de la anterior *demostración*, cabe señalar que si se admitiera la existencia del conjunto S de todas las cosas que puedan ser objeto del pensamiento (de Dedekind), entonces, ya que cada subconjunto de S, podría ser objeto del pensamiento (de Dedekind), el conjunto $\mathrm{Sub}(S)$, formado por la totalidad de los subconjuntos de S, debería estar incluido en S. Por lo tanto ambos conjuntos deberían ser isomorfos, en virtud del teorema de Cantor-Bernstein, lo cual entraría en contradicción con un teorema de Cantor. Luego, desgraciadamente, no se puede admitir como existente el conjunto de todas las cosas que puedan ser objeto del pensamiento.

Hay que decir, que Peirce también propuso, independientemente de Dedekind, el mismo concepto de infinitud que éste último; y que la *demostración* anterior de Dedekind es similar a una de Bolzano.

0.2. Algebras de Dedekind-Peano. Dedekind, en una carta dirigida a Keferstein, y después de indicarle que su ensayo sobre los números no fué escrito en un día; sino que, más bien, era una síntesis construida después de un prolongado trabajo, basado en un análisis previo de la sucesión de los números naturales tal cual como se presenta, en la experiencia, por así decir, para nuestra consideración; se pregunta por:

> What are the mutually independent fundamental properties of the sequence $\mathbb{N}$, that is, those properties that are not derivable from one another but from which all others follow? And how should we divest these properties of their specifically arithmetic character so that they are subsumed under more general notions and under activities of the understanding *whithout* which no thinking is possible but *with* which a foundation is provided for the reliability and completeness of proofs and for the construction of consistent notions and definitions?

La respuesta a lo anterior viene dada por el concepto de *álgebra de Dedekind-Peano*, de las que a continuación, apoyándonos sobre el axioma del conjunto infinito, demostraremos la existencia, y cuya definición, es la siguiente.

Definición 0.11. Un *álgebra de Dedekind-Peano* es un triplo ordenado $\mathbf{A} = (A, f, e)$ en el que A es un conjunto, f una endoaplicación de A y e un miembro de A, tal que:

1. f es inyectiva.
2. $\mathrm{Im}(f) \cap \{e\} = \varnothing$.
3. $\forall X \subseteq A\,((\, f[X] \subseteq X \wedge e \in X\,) \rightarrow X = A\,)$.

Observemos que la segunda claúsula de la definición anterior afirma simplemente que e no es de la forma $f(a)$, sea cual sea $a \in A$, y que la última cláusula de la misma, dice que la única parte de A que tiene las propiedades de está cerrada bajo f y contener como miembro a e, es la propia A.

Como primer paso hacia la demostración de la existencia de un álgebra de Dedekind-Peano, establecemos el siguiente teorema.

Teorema 0.12. *Hay un único conjunto, el conjunto de los* números naturales*, denotado por* $\mathbb{N}$*, que tiene las siguientes propiedades:*

1. $\varnothing \in \mathbb{N} \wedge \forall n\,(\, n \in \mathbb{N} \rightarrow n^+ \in \mathbb{N}\,)$.
2. $\forall B\,((\, \varnothing \in B \wedge \forall y\,(y \in B \rightarrow y^+ \in B\,)) \rightarrow \mathbb{N} \subseteq B\,)$

Demostración. Existencia. En virtud del axioma del conjunto infinito, existe al menos un conjunto A tal que $\varnothing \in A$ y para cada $x \in A$, $x^+ \in A$. Sea A uno de ellos, arbitrario, pero fijo. Entonces para el conjunto $\mathcal{X}$ definido como:

$$\mathcal{X} = \{\, X \in \mathrm{Sub}(A) \mid \varnothing \in X \wedge \forall x\,(x \in X \rightarrow x^+ \in X)\,\},$$

se cumple que $\mathcal{X} \neq \varnothing$, porque $A \subseteq A$, $\varnothing \in A$ y para cada $x \in A$, $x^+ \in A$. Luego existe el conjunto $\mathbb{N} = \bigcap \mathcal{X}$ y es tal que $\varnothing \in \mathbb{N}$, porque, para cada $X \in \mathcal{X}$, $\varnothing \in X$, y, para cada $x \in \mathbb{N}$, $x^+ \in \mathbb{N}$, ya que, para cada $X \in \mathcal{X}$, $x^+ \in X$.

Ahora demostramos que $\mathbb{N}$ está incluido en cualquier conjunto B que esté cerrado bajo la formación del conjunto sucesor y para el que $\varnothing \in B$. Sea B un tal conjunto, arbitrario, pero fijo. Entonces, ya que $A \cap B \subseteq A$ y $A \cap B$ está cerrado bajo la formación del conjunto sucesor y $\varnothing \in A \cap B$, se cumple que $A \cap B \in \mathcal{X}$, por lo tanto $\mathbb{N} \subseteq A \cap B$, pero $A \cap B \subseteq B$, así que $\mathbb{N} \subseteq B$.

Unicidad. Si $\mathbb{N}'$ tuviera las mismas propiedades que tiene $\mathbb{N}$, entonces $\mathbb{N} \subseteq \mathbb{N}'$ y $\mathbb{N}' \subseteq \mathbb{N}$, luego $\mathbb{N} = \mathbb{N}'$. $\square$

Definición 0.13. Al conjunto vacío, cuando lo consideremos como miembro del conjunto de los números naturales $\mathbb{N}$, lo denotamos por 0. Además, 1 denota al sucesor de 0, i.e., $1 = \{0\}$, 2 al sucesor de 1, i.e., $2 = \{0, 1\}$, ..., 9 al sucesor de 8, i.e., $9 = \{0, 1, \ldots, 8\}$ y 10 al sucesor de 9, i.e., $\{0, 1, \ldots, 9\}$.

Proposición 0.14. *La relación binaria* Sc *sobre* $\mathbb{N}$*, definida como:*

$$\mathrm{Sc} = \{\, (m, n) \in \mathbb{N} \times \mathbb{N} \mid n = m^+ \,\},$$

es una endofunción de $\mathbb{N}$*.*

Demostración. Porque, para cada número natural está unívocamente determinado el conjunto sucesor del mismo y, además, tal conjunto sucesor, en este caso, es un número natural. □

Definición 0.15. Denotamos por sc la endoaplicación de $\mathbb{N}$ cuya función subyacente es Sc y la denominamos la aplicación *sucesor* de $\mathbb{N}$. Además, denotamos el valor de sc en n, para cada $n \in \mathbb{N}$, por n^+ o $n+1$. Por último, denotamos por $\mathbf{N}$ el triplo ordenado $(\mathbb{N}, \mathrm{sc}, 0)$.

Proposición 0.16. *Para cada número natural* $n \in \mathbb{N}$*,* $\mathrm{sc}(n) \neq 0$*, o, lo que es equivalente,* $\{0\} \cap \mathrm{Im}(\mathrm{sc}) = \varnothing$*.*

Demostración. Porque, para cada número natural $n \in \mathbb{N}$, $\mathrm{sc}(n) = n \cup \{n\}$ no es vacío. □

Teorema 0.17 (Principio de la demostración por inducción finita)**.** *Para cada subconjunto* X *de* $\mathbb{N}$*, si* $0 \in X$ *y* $\mathrm{sc}[X] \subseteq X$*, entonces* $X = \mathbb{N}$*.*

Demostración. Sea X un subconjunto de $\mathbb{N}$ tal que $0 \in X$ y $\mathrm{sc}[X] \subseteq X$. Entonces $\mathbb{N} \subseteq X$, ya que $\mathbb{N}$ es el mínimo conjunto con tales propiedades, por lo tanto, ya que por hipótesis $X \subseteq \mathbb{N}$, $X = \mathbb{N}$. □

Proposición 0.18. *El principio de la demostración por inducción finita equivale a que* $\mathrm{Sg}_{\mathbf{N}}(\varnothing) = \mathbb{N}$*, siendo* $\mathrm{Sg}_{\mathbf{N}}(\varnothing)$ *el mínimo subconjunto de* $\mathbb{N}$ *que contiene al vacío, al que pertenece el* 0 *y que está cerrado bajo* sc*, i.e., siendo* $\mathrm{Sg}_{\mathbf{N}}(\varnothing)$ *el conjunto definido como:*

$$\mathrm{Sg}_{\mathbf{N}}(\varnothing) = \bigcap \{\, Y \subseteq \mathbb{N} \mid 0 \in Y \wedge \mathrm{sc}[Y] \subseteq Y \,\}.$$

Demostración. Supongamos el principio de la demostración por inducción finita, i.e., que para cada subconjunto X de $\mathbb{N}$, si $0 \in X$ y $\mathrm{sc}[X] \subseteq X$, entonces $X = \mathbb{N}$. Entonces, por ser $\mathbb{N} \subseteq \mathbb{N}$ y cumplirse que $0 \in \mathbb{N}$ y que $\mathrm{sc}[\mathbb{N}] \subseteq \mathbb{N}$, tenemos que $\mathbb{N}$ pertenece al conjunto $\{\, Y \subseteq \mathbb{N} \mid 0 \in Y \wedge \mathrm{sc}[Y] \subseteq Y \,\}$, luego $\mathrm{Sg}_{\mathbf{N}}(\varnothing) \subseteq \mathbb{N}$. Además, $\mathbb{N} \subseteq \mathrm{Sg}_{\mathbf{N}}(\varnothing)$, porque $0 \in \mathrm{Sg}_{\mathbf{N}}(\varnothing)$, $\mathrm{sc}[\mathrm{Sg}_{\mathbf{N}}(\varnothing)] \subseteq \mathrm{Sg}_{\mathbf{N}}(\varnothing)$ y $\mathbb{N}$ es el mínimo conjunto con tales propiedades. Por lo tanto $\mathrm{Sg}_{\mathbf{N}}(\varnothing) = \mathbb{N}$.

Recíprocamente, supongamos que $\mathrm{Sg}_{\mathbf{N}}(\varnothing) = \mathbb{N}$. Entonces, si un subconjunto X de $\mathbb{N}$ es tal que $0 \in X$ y $\mathrm{sc}[X] \subseteq X$, entonces $X \in \{\, Y \subseteq \mathbb{N} \mid 0 \in Y \wedge \mathrm{sc}[Y] \subseteq Y \,\}$, luego $\mathrm{Sg}_{\mathbf{N}}(\varnothing) \subseteq X$, así que $\mathbb{N} \subseteq X$, pero $X \subseteq \mathbb{N}$, luego $X = \mathbb{N}$. □

A partir del principio de la demostración por inducción finita, se deduce que una condición suficiente para que todos los números naturales tenga una cierta propiedad, es que la tenga el 0, y que cuando un número natural

arbitrario la tenga, también la tenga su sucesor, i.e., si $\varphi(x, t_{[n]})$ es una fórmula, entonces

$$\forall t_0, \ldots, t_{n-1} \, ((\, \varphi(0, t_{[n]}) \wedge \forall x \in \mathbb{N} \, (\, \varphi(x, t_{[n]}) \to \varphi(x^+, t_{[n]})\,) \to \forall x \in \mathbb{N} \, (\, \varphi(x, t_{[n]})\,)).$$

Proposición 0.19. *Si $n \in \mathbb{N} - 1$, entonces hay un $m \in \mathbb{N}$ tal que $n = m^+$, o, lo que es equivalente, $\mathbb{N} - (\{0\} \cup \mathrm{Im}(\mathrm{sc})) = \varnothing$*

Demostración. □

Para demostrar que la aplicación sucesor es inyectiva, definimos a continuación el concepto de conjunto *∈-transitivo*. Además, damos algunas caracterizaciones de dicho concepto y establecemos algunas propiedades de clausura del mismo.

Definición 0.20. Un conjunto A es *∈-transitivo* si para cualesquiera conjuntos x e y, si $y \in x$ y $x \in A$, entonces $y \in A$.

Proposición 0.21. *Sea A un conjunto. Entonces son equivalentes:*

1. *A es ∈-transitivo.*
2. $\bigcup A \subseteq A$.
3. $A \subseteq \mathrm{Sub}(A)$.

Demostración. □

Proposición 0.22.

1. *Si A es ∈-transitivo, entonces A^+ es ∈-transitivo.*
2. *Si A es ∈-transitivo, entonces $\bigcup A$ es ∈-transitivo.*
3. *Si A es tal que todos sus miembros son ∈-transitivos, entonces $\bigcup A$ es ∈-transitivo.*
4. *Si A no es vacío y todos sus miembros son ∈-transitivos, entonces $\bigcap A$ es ∈-transitivo.*

Demostración. □

A continuación, establecemos una caracterización del concepto de conjunto ∈-transitivo, que será especialmente útil en la demostración de que la aplicación sucesor es inyectiva.

Proposición 0.23. *Una condición necesaria y suficiente para que un conjunto A sea ∈-transitivo, es que $\bigcup A^+ = A$*

Demostración. □

Proposición 0.24. *Cualquier número natural es ∈-transitivo.*

Demostración. Demostramos, por inducción, que $T = \{\, n \in \mathbb{N} \mid n \text{ es } \in\text{-transitivo} \,\}$, coincide con el conjunto de los números naturales.

Se cumple que $0 \in T$, porque $\bigcup 0^+ = 0$. Supongamos que $n \in T$, i.e., que n sea ∈-transitivo, o, lo que es equivalente, que $\bigcup n^+ = n$. Entonces

$$\begin{aligned} \bigcup (n^+)^+ &= \bigcup (n^+ \cup \{n^+\}) \\ &= (\bigcup n^+) \cup (\bigcup \{n^+\}) \\ &= n \cup (n \cup \{n\}) \\ &= n^+, \end{aligned}$$

luego n^+ es $\in$-transitivo, i.e., $n^+ \in T$. Por consiguiente $T = \mathbb{N}$.

□

Teorema 0.25. *El triplo ordenado* $(\mathbb{N}, \mathrm{sc}, 0)$ *es un álgebra de Dedekind-Peano.*

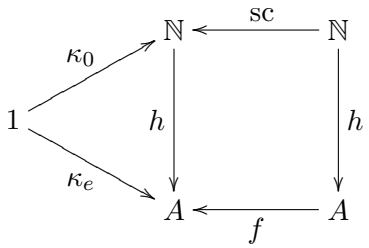
Demostración. □

Proposición 0.26. *El conjunto* $\mathbb{N}$ *es* $\in$*-transitivo.*

Demostración. □

0.3. El principio de la definición por recursión finita. Demostramos a continuación el *principio de la definición por recursión finita*, debido a Dedekind. Este principio de definición nos permitirá demostrar que el álgebra de Dedekind-Peano $(\mathbb{N}, \mathrm{sc}, 0)$ es esencialmente única. También, a partir de dicho principio establecemos otros principios de definición por recursión, que usaremos en la teoría de las funciones recursivas.

Teorema 0.27 (Principio de la definición por recursión finita)**.** *Sea* A *un conjunto,* $e \in A$ *y* $f\colon A \longrightarrow A$ *una endoaplicación de* A*. Entonces se cumple que hay una única aplicación* $h\colon \mathbb{N} \longrightarrow A$ *tal que el diagrama:*



en el que κ_0 *es la aplicación que al único miembro de* 1 *le asigna* 0 *y* κ_e *la aplicación que al único miembro de* 1 *le asigna* e*, conmuta, i.e., tal que:*

1. $h(0) = e$.
2. $\forall n \in \mathbb{N}\,(h(\mathrm{sc}(n)) = f(h(n)))$.

Demostración. Decimos que una función parcial G de $\mathbb{N}$ en A es *aceptable*, respecto de e y $f = (A, F, A)$, si cumple las siguientes condiciones:

1. Si $0 \in \mathrm{Dom}(G)$, entonces $G(0) = e$.
2. Para cada $n \in \mathbb{N}$, si $\mathrm{sc}(n) \in \mathrm{Dom}(G)$, entonces $n \in \mathrm{Dom}(G)$ y $G(\mathrm{sc}(n)) = F(G(n))$.

Sea $\mathcal{G}$ el conjunto de todas las funciones parciales de $\mathbb{N}$ en A que sean aceptables (conjunto obtenido, mediante una aplicación del esquema axiomático de separación, a partir del conjunto de todas las funciones parciales de $\mathbb{N}$ en A). Vamos a demostrar que el conjunto $H = \bigcup \mathcal{G}$ tiene las siguientes propiedades:

1. H es una función parcial de $\mathbb{N}$ en A.
2. H es aceptable.
3. $\mathrm{Dom}(H) = \mathbb{N}$.
4. H es la única función de $\mathbb{N}$ en A tal que
   a) $H(0) = e$.
   b) $\forall n \in \mathbb{N}\,(H(\mathrm{sc}(n)) = F(H(n)))$.

Demostramos en primer lugar que hay a lo sumo una función H de $\mathbb{N}$ en A tal que

- $H(0) = e$.
- $\forall n \in \mathbb{N}\,(H(\mathrm{sc}(n)) = F(H(n)))$.

En efecto, si H' fuera otra función de $\mathbb{N}$ en A que tuviera las mismas propiedades que tiene H, entonces el igualador de H y H', i.e., el conjunto $\mathrm{Eq}(H, H') = \{\, n \in \mathbb{N} \mid H(n) = H'(n) \,\}$, coincidiría con $\mathbb{N}$, ya que, por cumplirse, por una parte, que $0 \in \mathrm{Eq}(H, H')$, debido a que $H(0) = e = H'(0)$, y, por otra, que dado un $n \in \mathbb{N}$, si $n \in \mathrm{Eq}(H, H')$, i.e., si $H(n) = H'(n)$, entonces $\mathrm{sc}(n) \in \mathrm{Eq}(H, H')$, porque

$$\begin{aligned} H(\mathrm{sc}(n)) &= F(H(n)) \text{ (porque } H \text{ tiene tal propiedad)} \\ &= F(H'(n)) \text{ (porque, por hipótesis, } H(n) = H'(n)) \\ &= H'(\mathrm{sc}(n)) \text{ (porque } H' \text{ tiene tal propiedad),} \end{aligned}$$

entonces, en virtud del principio de la demostración por inducción finita, $\mathrm{Eq}(H, H') = \mathbb{N}$, luego, para cada $n \in \mathbb{N}$, $H(n) = H'(n)$, i.e., $H = H'$.

Ahora demostramos que $H = \bigcup \mathcal{G}$ es una función parcial de $\mathbb{N}$ en A.

En efecto, puesto que, para cada $G \in \mathcal{G}$, G es una función parcial de $\mathbb{N}$ en A, $H \subseteq \mathbb{N} \times A$, luego H es una relación de $\mathbb{N}$ en A. Para demostrar que la relación H es una función parcial de $\mathbb{N}$ en A, hay que demostrar que, para cada $n \in \mathbb{N}$ y para cada $y, z \in A$, si $(n, y), (n, z) \in H$, entonces $y = z$. Para ello, es suficiente que demostremos, por inducción, que el conjunto T definido como:

$$T = \{\, n \in \mathbb{N} \mid \forall y, z \in A\,((n, y) \in H \wedge (n, z) \in H \rightarrow y = z) \,\},$$

coincide con $\mathbb{N}$.

Se cumple que $T = \mathbb{N}$, ya que, por una parte, $0 \in T$, porque si $y, z \in A$ son tales que $(0, y) \in H$ y $(0, z) \in H$, entonces, ya que $H = \bigcup \mathcal{G}$, hay un $G_y \in \mathcal{G}$ tal que $(0, y) \in G_y$ y hay un $G_z \in \mathcal{G}$ tal que $(0, z) \in G_z$, luego $0 \in \mathrm{Dom}(G_y)$ y $0 \in \mathrm{Dom}(G_z)$, por lo tanto, ya que G_y y G_z son aceptables, $G_y(0) = e = G_z(0)$, pero $G_y(0) = y$ y $G_z(0) = z$, así que $y = e = z$, por lo tanto $y = z$; y, por otra, dado un $n \in \mathbb{N}$, si $n \in T$, entonces, dados $y, z \in A$ tales que $(\mathrm{sc}(n), y) \in H$ y $(\mathrm{sc}(n), z) \in H$, ya que $H = \bigcup \mathcal{G}$, hay un $G_y \in \mathcal{G}$ tal que $(\mathrm{sc}(n), y) \in G_y$ y hay un $G_z \in \mathcal{G}$ tal que $(\mathrm{sc}(n), z) \in G_z$. Ahora bien, ya que G_y y G_z son aceptables, $n \in \mathrm{Dom}(G_y)$ y $G_y(\mathrm{sc}(n)) = F(G_y(n)) = y$ y $n \in \mathrm{Dom}(G_z)$ y $G_z(\mathrm{sc}(n)) = F(G_z(n)) = z$. Además, se cumple que $(n, G_y(n))$ y $(n, G_z(n)) \in H$, luego, por la hipótesis de inducción, $G_y(n) = G_z(n)$, por lo tanto $F(G_y(n)) = F(G_z(n))$, pero $F(G_y(n)) = y$ y $F(G_z(n)) = z$, así que $y = z$. Podemos afirmar pues que $\mathrm{sc}(n) \in T$. Por consiguiente $\mathbb{N} = T$, i.e., H es una función parcial de $\mathbb{N}$ en A.

Demostramos a continuación que H es aceptable. Si $0 \in \mathrm{Dom}(H)$, entonces, ya que $H = \bigcup \mathcal{G}$, hay un $G \in \mathcal{G}$ tal que $0 \in \mathrm{Dom}(G)$, luego $G(0) = e$, i.e., $(0, e) \in G$, pero $G \subseteq H$, así que $(0, e) \in H$, i.e., $H(0) = e$. Sea $n \in \mathbb{N}$ y supongamos que $\mathrm{sc}(n) \in \mathrm{Dom}(H)$, entonces ya que $H = \bigcup \mathcal{G}$, hay un $G \in \mathcal{G}$ tal que $\mathrm{sc}(n) \in \mathrm{Dom}(G)$, luego $n \in \mathrm{Dom}(G)$ y $G(\mathrm{sc}(n)) = F(G(n))$. De donde, en particular, $n \in \mathrm{Dom}(H)$, porque $\mathrm{Dom}(H) = \bigcup_{G \in \mathcal{G}} \mathrm{Dom}(G)$. Así que

$H(n) = G(n)$ y, ya que $(\mathrm{sc}(n), F(G(n))) \in G$ y $G \subseteq H$, $(\mathrm{sc}(n), F(G(n))) \in H$, i.e., $H(\mathrm{sc}(n)) = F(G(n))$, luego $H(\mathrm{sc}(n)) = F(H(n))$.

Demostramos, por último, que H es una función de $\mathbb{N}$ en A. Para ello es suficiente que demostremos, por inducción, que el conjunto $T = \{\, n \in \mathbb{N} \mid \exists y \in A\, ((n, y) \in H)\,\}$ coincide con $\mathbb{N}$.

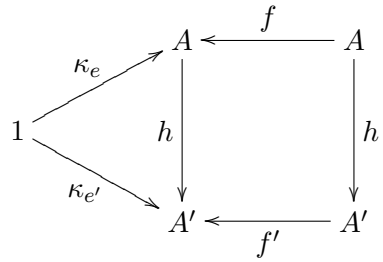
Se cumple que $0 \in T$, porque $\{(0, e)\} \in \mathcal{G}$ y $H = \bigcup \mathcal{G}$. Sea $n \in \mathbb{N}$ y supongamos que $n \in T$. Vamos a demostrar que si $\mathrm{sc}(n) \notin T$, entonces la relación $G = H \cup \{(\mathrm{sc}(n), F(H(n)))\}$ tiene las propiedades de ser una función parcial de $\mathbb{N}$ en A, ser aceptable y contener estrictamente a H, lo cual, junto con lo demostrado hasta ahora para H, constituirá una contradicción.

G es una función parcial de $\mathbb{N}$ en A, porque tanto H como el conjunto $\{(\mathrm{sc}(n), F(H(n)))\}$ lo son y las restricciones de ambas a la intersección de sus dominios de definición (que es el conjunto vacío) coinciden. Además, por definición de G, se cumple que $H \subset G$. Por último, G es aceptable, ya que, por una parte, si $0 \in \mathrm{Dom}(G)$, entonces $0 \in \mathrm{Dom}(H)$, luego $H(0) = e = G(0)$, y, por otra, dado un $m \in \mathbb{N}$, si $\mathrm{sc}(m) \in \mathrm{Dom}(G)$, entonces, puesto que $\mathrm{Dom}(G) = \mathrm{Dom}(H) \cup \{\mathrm{sc}(n)\}$ y $\mathrm{Dom}(H) \cap \{\mathrm{sc}(n)\} = \varnothing$, o bien $\mathrm{sc}(m) \in \mathrm{Dom}(H)$ o bien $\mathrm{sc}(m) = \mathrm{sc}(n)$. Si lo primero, entonces, por ser H aceptable, $m \in \mathrm{Dom}(H)$ y $H(\mathrm{sc}(m)) = F(H(m))$, luego $m \in \mathrm{Dom}(G)$ y $G(\mathrm{sc}(m)) = F(H(m)) = F(G(m))$. Si lo segundo, entonces por ser sc inyectiva, $m = n$, pero $n \in \mathrm{Dom}(H)$, luego $n \in \mathrm{Dom}(G)$ y $G(\mathrm{sc}(m)) = F(H(m)) = F(G(m))$. Pero esto entra en contradicción con la definición de H. Por lo tanto $\mathrm{sc}(n) \in T$ y, en consecuencia, $T = \mathbb{N}$, i.e., $\mathrm{Dom}(H) = \mathbb{N}$.

Luego, tomando como h el triplo ordenado $(\mathbb{N}, H, A)$, obtenemos el teorema. □

Debemos observar que la propiedad establecida en el teorema anterior, para el álgebra de Dedekind-Peano $\mathbf{N} = (\mathbb{N}, \mathrm{sc}, 0)$, no es privativa de ésa álgebra concreta, sino que es compartida por todas las álgebras de Dedekind-Peano.

Si $\mathbf{A} = (A, f, e)$ es un álgebra de Dedekind-Peano, A' un conjunto, $e' \in A'$ y $f' \colon A' \longrightarrow A'$, entonces hay una única aplicación $h \colon A \longrightarrow A'$ tal que el diagrama:



conmuta, siendo κ_e la aplicación que al único miembro de 1 le asigna e y $\kappa_{e'}$ la aplicación que al único miembro de 1 le asigna e'.

Ahora que disponemos del principio de la definición por recursión finita, podemos establecer una versión alternativa, pero equivalente, del axioma de regularidad, y también de la existencia del cierre transitivo de una relación binaria.

Proposición 0.28. *El axioma de regularidad equivale a que no exista ninguna función F cuyo dominio de definición sea $\mathbb{N}$ y tal que, para cada $n \in \mathbb{N}$, $F(n^+) \in F(n)$.*

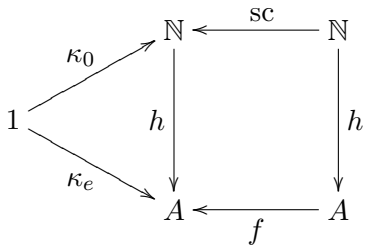
Demostración. □

Proposición 0.29. *Si R es una relación binaria en A, entonces la mínima relación transitiva en A que contiene a R, que es la intersección del conjunto de todas las relaciones transitivas en A que contienen a R, coincide con el* cierre transitivo *de R, denotado por R^{t}, que es:*

$$R^{\mathrm{t}} = \left\{ (a,b) \in A \times A \;\middle|\; \begin{array}{c} \exists m \in \mathbb{N} - 1\, \exists (x_i \mid i \in m^+) \in A^{m^+} \\ (a = x_0 \wedge x_m = b \wedge \forall i \in m\, ((x_i, x_{i^+}) \in R)) \end{array} \right\}.$$

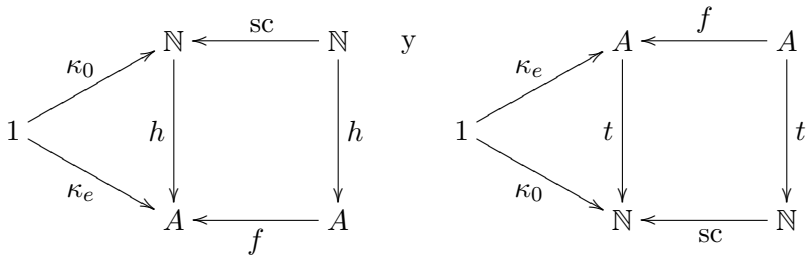
Demostración. □

Proposición 0.30. *Si $\mathbf{A} = (A, f, e)$ es un álgebra de Dedekind-Peano, entonces hay una única aplicación biyectiva $h\colon \mathbb{N} \longrightarrow A$ tal que el diagrama:*

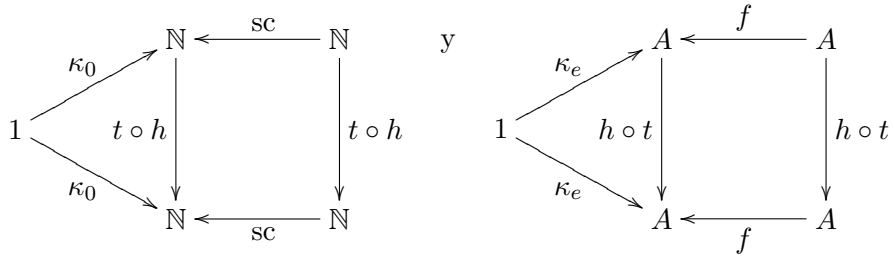


conmuta.

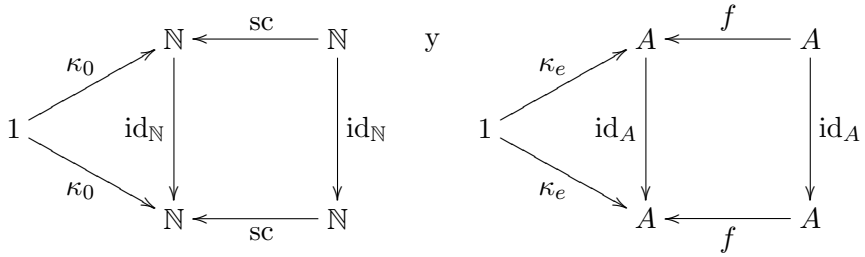
Demostración. Por ser **N** y **A** álgebras de Dedekind-Peano, existe una única aplicación $h\colon \mathbb{N} \longrightarrow A$, así como una única aplicación $t\colon A \longrightarrow \mathbb{N}$, de modo que los diagramas:



conmutan. Luego los diagramas:

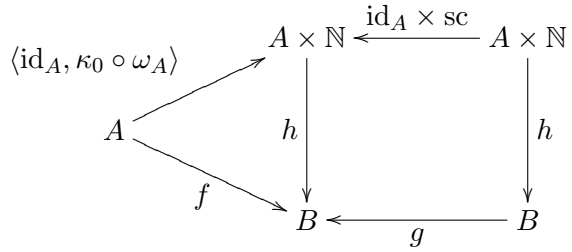


conmutan. Pero los diagramas:



también conmutan. De donde, por unicidad, $t \circ h = \mathrm{id}_{\mathbb{N}}$ y $h \circ t = \mathrm{id}_A$, así que $h\colon \mathbb{N} \longrightarrow A$ es una biyección que cumple las condiciones. □

Proposición 0.31. *Sea $f\colon A \longrightarrow B$ y $g\colon B \longrightarrow B$. Entonces hay una única aplicación $h\colon A \times \mathbb{N} \longrightarrow B$ tal que el diagrama:*



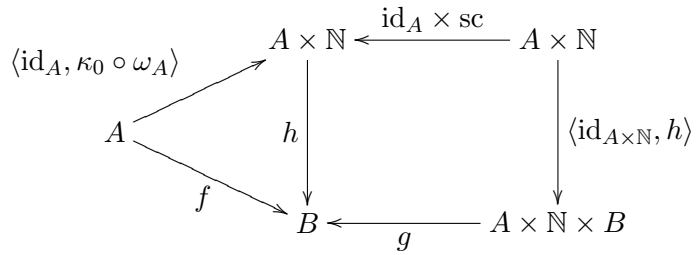
conmuta, i.e., tal que:

1. $\forall a \in A\,(h(a,0) = f(a))$.
2. $\forall a \in A\,\forall n \in \mathbb{N}\,(h(a,n^+) = g(h(a,n)))$.

Demostración. □

En lo que sigue abreviamos por "RPcP" la frase "Recursión primitiva con parámetros", por "RPcPpAP" la frase "Recursión primitiva con parámetros para aplicaciones parciales", por "RPsP" la frase "Recursión primitiva sin parámetros", y por "RPsPpAP" la frase "Recursión primitiva sin parámetros para aplicaciones parciales".

Proposición 0.32 (RPcP)**.** *Sea $f\colon A \longrightarrow B$ y $g\colon A \times \mathbb{N} \times B \longrightarrow B$. Entonces hay una única aplicación $h\colon A \times \mathbb{N} \longrightarrow B$ tal que el diagrama:*



conmuta, i.e., tal que:

1. $\forall a \in A\,(h(a,0) = f(a))$.
2. $\forall a \in A\,\forall n \in \mathbb{N}\,(h(a,n^+) = g(a,n,h(a,n)))$.

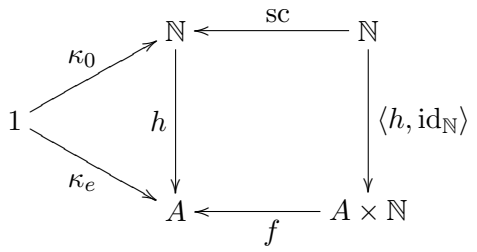
Demostración. □

Proposición 0.33 (RPcPpAP)**.** *Sea $f\colon A \rightarrowtail B$ y $g\colon A \times \mathbb{N} \times B \rightarrowtail B$. Entonces hay una única aplicación parcial $h\colon A \times \mathbb{N} \rightarrowtail B$ tal que:*

1. *Para cada $a \in A$, $(a, 0) \in \mathrm{Dom}(h)$ si y sólo si $a \in \mathrm{Dom}(f)$, y si $(a, 0) \in \mathrm{Dom}(h)$, entonces $h(a, 0) = f(a)$.*
2. *Para cada $a \in A$ y cada $n \in \mathbb{N}$, $(a, n^+) \in \mathrm{Dom}(h)$ si y sólo si $(a, n) \in \mathrm{Dom}(f)$ y $(a, n, h(a, n)) \in \mathrm{Dom}(g)$, y si $(a, n^+) \in \mathrm{Dom}(h)$, entonces $h(a, n^+) = g(a, n, h(a, n))$.*

Demostración. □

Proposición 0.34 (RPsP)**.** *Sea A un conjunto, $e \in A$ y $f\colon A \times \mathbb{N} \rightarrow A$. Entonces hay una única aplicación $h\colon \mathbb{N} \rightarrow A$ tal que el diagrama:*



conmuta, i.e., tal que:

1. $h(0) = e$.
2. $\forall n \in \mathbb{N}\,(h(n^+) = f(h(n), n))$.

Demostración. □

Proposición 0.35 (RPsPpAP)**.** *Sea A un conjunto, $e \in A$ y $f\colon A \times \mathbb{N} \rightarrowtail A$. Entonces hay una única aplicación parcial $h\colon \mathbb{N} \rightarrowtail A$ tal que:*

1. *$0 \in \mathrm{Dom}(h)$ y $h(0) = e$.*
2. *Para cada $n \in \mathbb{N}$, si $n^+ \in \mathrm{Dom}(h)$, entonces $h(n^+) = f(h(n), n))$.*
3. *$\mathrm{Dom}(h) = \mathbb{N}$ o para un $n \in \mathbb{N}$, $\mathrm{Dom}(h) = n^+$ y $f(h(n), n)$ no está definido.*

Demostración. □

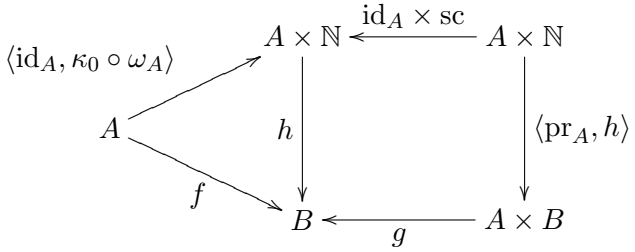
En lo que sigue abreviamos por "PDRCV" la frase "Principio de la definición por recursión de curso de valores".

Proposición 0.36 (PDRCV)**.** *Sea A un conjunto y $f\colon A^\star \rightarrow A$. Entonces hay una única aplicación $h\colon \mathbb{N} \rightarrow A$ tal que, para cada $n \in \mathbb{N}$, $h(n) = f(h{\restriction}n)$.*

Demostración. □

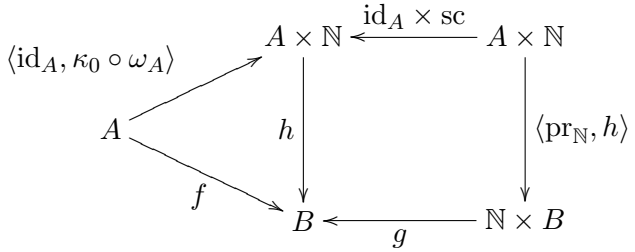
Proposición 0.37.

1. *Sea* $f\colon A \longrightarrow B$ *y* $g\colon A \times B \longrightarrow B$. *Entonces hay una única aplicación* $h\colon A \times \mathbb{N} \longrightarrow B$ *tal que el diagrama:*



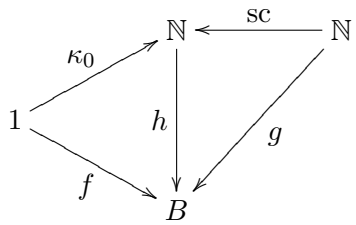
conmuta, i.e., tal que:
a) $\forall a \in A\,(h(a,0) = f(a))$.
b) $\forall a \in A \forall n \in \mathbb{N}\,(h(a,n^+) = g(a,h(a,n)))$.

2. *Sea* $f\colon A \longrightarrow B$ *y* $g\colon \mathbb{N} \times B \longrightarrow B$. *Entonces hay una única aplicación* $h\colon A \times \mathbb{N} \longrightarrow B$ *tal que el diagrama:*



conmuta, i.e., tal que:
a) $\forall a \in A\,(h(a,0) = f(a))$.
b) $\forall a \in A \forall n \in \mathbb{N}\,(h(a,n^+) = g(n,h(a,n)))$.

3. *Sea* $f\colon 1 \longrightarrow B$ *y* $g\colon \mathbb{N} \longrightarrow B$. *Entonces hay una única aplicación* h *de* $\mathbb{N}$ *en* B *tal que el diagrama:*

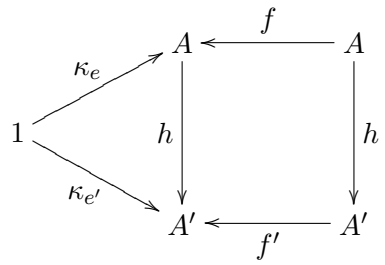


conmuta, i.e., tal que:
a) $(h(0) = f(0))$.
b) $\forall n \in \mathbb{N}\,(h(n^+) = g(n))$.

0.4. Caracterización de Lawvere de las álgebras de Dedekind-Peano.

Vamos a demostrar, en lo que sigue, que una condición necesaria y suficiente para que un triplo ordenado $\mathbf{A} = (A, f, e)$ en el que A es un conjunto, f una endoaplicación de A y e un miembro de A, sea un álgebra de Dedekind-Peano, es que $\mathbf{A}$ tenga la propiedad de la definición por recursión finita, i.e., que si A' es un conjunto, $e' \in A'$ y $f'\colon A' \longrightarrow A'$, entonces exista una única

aplicación $h\colon A \longrightarrow A'$ tal que el diagrama:



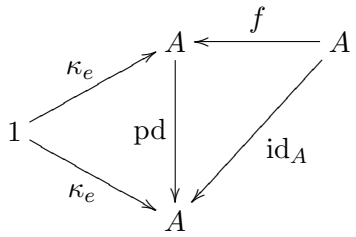
conmute.

De hecho, ya hemos demostrado que la condición es necesaria. Para demostrar la suficiencia hemos de demostrar que si **A** tiene la propiedad de la definición por recursión finita, entonces se cumple que:

- f es inyectiva.
- $\mathrm{Im}(f) \cap \{e\} = \varnothing$.
- $\forall X \subseteq A\,((\, f[X] \subseteq X \wedge e \in X\,) \rightarrow X = A\,)$.

Para ello, establecemos, en primer lugar, la siguiente definición.

Definición 0.38. Si **A** tiene la propiedad de la definición por recursión finita, entonces denotamos por pd a la única endoaplicación de A para la que el diagrama:



conmuta, y la denominamos la aplicación *predecesor*.

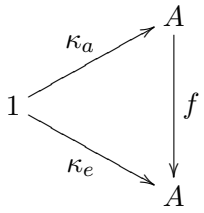
Proposición 0.39. *Si* **A** *tiene la propiedad de la definición por recursión finita, entonces*

1. *La aplicación* $f\colon A \longrightarrow A$ *es inyectiva.*
2. *Para cada* $a \in A$, $f(a) \neq e$, *i.e.,* $\mathrm{Im}(f) \cap \{e\} = \varnothing$.
3. *Para cada* $X \subseteq A$, *si* $f[X] \subseteq X$ *y* $e \in X$, *entonces* $X = A$.

Demostración. Para demostrar que la aplicación $f\colon A \longrightarrow A$ es inyectiva es suficiente que tomemos en consideración que, en la categoría **Set**, las aplicaciones inyectivas son exactamente los monomorfismos, i.e., las aplicaciones cancelables a la izquierda, y que $\mathrm{pd} \circ f = \mathrm{id}_A$.

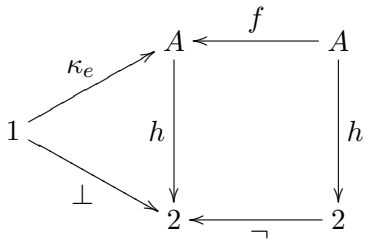
Para demostrar que $\mathrm{Im}(f) \cap \{e\} = \varnothing$, procedemos por reducción al absurdo. Supongamos que exista un $a \in A$ tal que $f(a) = e$, i.e., tal que el

diagrama:



conmute. Entonces $\mathrm{pd} \circ f \circ \kappa_a = \mathrm{pd} \circ \kappa_e$, luego $\mathrm{id}_A \circ \kappa_a = \kappa_e$, i.e., $\kappa_a = \kappa_e$ o, lo que es equivalente, $a = e$, luego $f \circ \kappa_e = f \circ \kappa_a = \kappa_e$.

Ahora bien, para $\mathbf{2} = (2, \bot, \neg)$, siendo $\bot$ la aplicación de 1 en 2 que a 0 le asigna 0 y $\neg$ la endoaplicación de 2 que a 0 le asigna 1 y 1 le asigna 0, tenemos que hay una única aplicación h de A en 2 tal que el diagrama:

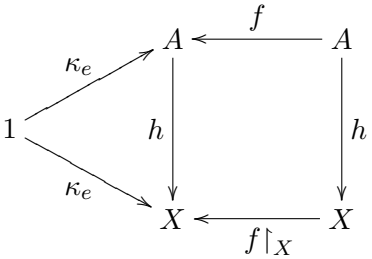


conmuta. Por lo tanto, siendo $\top$ la aplicación de 1 en 2 que a 0 le asigna 1, se cumple que

$$\begin{aligned} \top &= \neg \circ \bot \\ &= h \circ f \circ \kappa_e \\ &= h \circ \kappa_e \\ &= \bot \end{aligned}$$

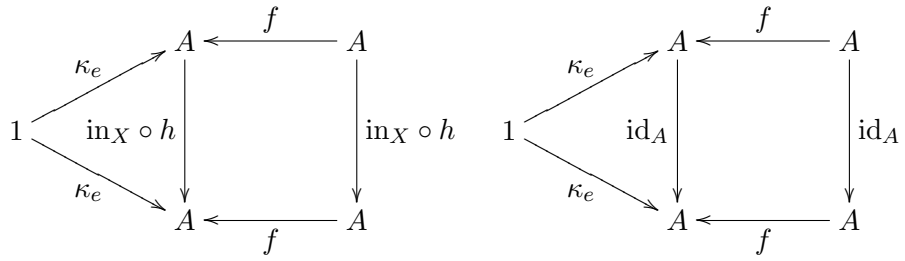
contradicción.

Para demostrar la última parte, es suficiente tomar en consideración que si $X \subseteq A$ es tal que $f[X] \subseteq X$ y $e \in X$, entonces existe una única aplicación $h\colon A \longrightarrow X$ tal que el diagrama:



conmuta.

Ahora bien, los diagramas:



conmutan, luego, por la unicidad, $\mathrm{in}_X \circ h = \mathrm{id}_A$, i.e., in_X es sobreyectiva. Pero como in_X es inyectiva, es, en definitiva, biyectiva. Luego $X = A$. □

Como dice Mac Lane:

> This case illustrates a general point: The axioms needed to describe a Mathematical structure are themselves by no means unique. The recursion theorem is an especially convenient form of axiom; it states that the diagram
>
> $$1 \xrightarrow{\kappa_e} A \xrightarrow{\mathrm{sc}} A$$
>
> is "universal".

0.5. El orden aritmético sobre el conjunto de los números naturales. Nos proponemos demostrar a continuación que el conjunto de los números naturales está dotado de una *buena ordenación*, i.e., de una relación binaria $<$ que cumple las siguientes condiciones:

- $<$ es irreflexiva, i.e., $\forall n \in \mathbb{N}\,(\, n \not< n\,)$.
- $<$ es transitiva, i.e., $\forall m, n, p \in \mathbb{N}\,((\, m < n \wedge n < p\,) \to m < p\,)$.
- $\forall X \subseteq \mathbb{N}\,(\, X \neq \varnothing \to \exists n \in X\,(\,\forall x \in X\,(\, n < x \vee n = x\,)))$.

Para ello, siguiendo a Diener, usaremos, por una parte, el hecho de que la estructura algebraica, dada por la operación unaria sc y la operación ceroaria 0, de que está dotado el conjunto de los números naturales, lo convierte en un álgebra de Dedekind-Peano, y, por otra, que a partir de ello se puede obtener, sobre el conjunto de los números naturales, una relación de orden bien fundamentada y disyuntiva, i.e., en definitiva una buena ordenación sobre $\mathbb{N}$. Pero antes introducimos una serie de nociones y proposiciones relativas a las secciones iniciales de los conjuntos ordenados y las relaciones bien fundamentadas, necesarias para alcanzar el objetivo anterior.

Definición 0.40. Sea A un conjunto y R una relación binaria en A. Decimos que un subconjunto X de A es una *R-sección inicial* de A, si junto a un $x \in X$ contiene al conjunto $\downarrow_R x = \{\, y \in A \mid (y, x) \in R\,\}$ de todos los *R-predecesores* de x, i.e., si

$$\forall x \in X\,(\,\downarrow_R x \subseteq X\,),$$

o, lo que es equivalente, ya que $R^{-1}[X] = \bigcup_{x \in X} \downarrow_R x$, si

$$R^{-1}[X] \subseteq X.$$

Denotamos por $\mathrm{Sec}_R(A)$ el conjunto de todas las R-secciones iniciales de A.

Proposición 0.41. *El conjunto* $\mathrm{Sec}_R(A)$*, de todas las* R*-secciones iniciales de* A*, es un sistema de clausura completamente aditivo sobre* A*, i.e., tiene las siguientes propiedades:*

1. $A \in \mathrm{Sec}_R(A)$.
2. $\forall \mathcal{X} \subseteq \mathrm{Sec}_R(A)\,(\,\mathcal{X} \neq \varnothing \rightarrow \bigcap \mathcal{X} \in \mathrm{Sec}_R(A)\,)$.
3. $\forall \mathcal{X} \subseteq \mathrm{Sec}_R(A)\,(\,\bigcup \mathcal{X} \in \mathrm{Sec}_R(A)\,)$.

Demostración. □

Corolario 0.42. *Sea* A *un conjunto,* R *una relación binaria en* A *y* $X \subseteq A$*. Entonces hay una mínima* R*-sección inicial de* A *que contiene a* X*.*

Demostración. Es suficiente considerar la intersección del conjunto

$$\{\, Y \in \mathrm{Sec}_R(A) \mid X \subseteq Y \,\}.$$

□

Definición 0.43. Sea A un conjunto y R una relación binaria en A. Entonces denotamos por C_R el operador clausura sobre A, canónicamente asociado al sistema de clausura completamente aditivo $\mathrm{Sec}_R(A)$, que asocia a cada subconjunto X de A, $\mathrm{C}_R(X)$, la mínima R-sección inicial de A que contiene a X, a la que denominamos el *cierre inicial* de X relativo a R. En particular, cuando $X = \{x\}$, con $x \in A$, al cierre inicial de $\{x\}$ lo denotamos, para abreviar, por $\mathrm{C}_R(x)$, y lo denominamos también, la R-sección inicial *principal* determinada por x.

Proposición 0.44. *Sea* A *un conjunto y* R *una relación binaria en* A*, entonces el operador* C_R*, definido como:*

$$\mathrm{C}_R \begin{cases} \mathrm{Sub}(A) \longrightarrow \mathrm{Sub}(A) \\ X \quad \longmapsto \bigcap\{\, Y \in \mathrm{Sec}_R(A) \mid X \subseteq Y \,\} \end{cases}$$

tiene las siguientes propiedades:

1. $\mathrm{Im}(\mathrm{C}_R) \subseteq \mathrm{Sec}_R(A)$.
2. $\{\, X \in \mathrm{Sub}(A) \mid X = \mathrm{C}_R(X) \,\} = \mathrm{Sec}_R(A)$.
3. C_R *es extensivo o inflacionario, i.e., para cada* $X \in \mathrm{Sub}(A)$*,* $X \subseteq \mathrm{C}_R(X)$.
4. C_R *es isótono, i.e., para cada* $X, Y \in \mathrm{Sub}(A)$*, si* $X \subseteq Y$*, entonces se cumple que* $\mathrm{C}_R(X) \subseteq \mathrm{C}_R(Y)$.
5. C_R *es idempotente, i.e., para cada* $X \in \mathrm{Sub}(A)$*,* $\mathrm{C}_R(X) = \mathrm{C}_R(\mathrm{C}_R(X))$.
6. C_R *es completamente aditivo, i.e., para cada* $\mathcal{X} \subseteq \mathrm{Sub}(A)$*, se cumple que* $\mathrm{C}_R(\bigcup \mathcal{X}) = \bigcup_{X \in \mathcal{X}} \mathrm{C}_R(X)$.

Proposición 0.45. *Sea* A *un conjunto y* R *una relación binaria en* A*, entonces*

1. $\forall X \subseteq A\,(\mathrm{C}_R(X) = \bigcup_{x \in X} \mathrm{C}_R(x))$.
2. $\forall x \in A\,(\mathrm{C}_R(\downarrow_R x) = \bigcup_{y \in \downarrow_R x} \mathrm{C}_R(y))$.

Proposición 0.46. *Sea* A *un conjunto y* R *una relación binaria en* A*. Si* R *es transitiva, entonces, para cada* $x \in A$*, se cumple que*

$$\mathrm{C}_R(x) = \Downarrow_R x,$$

siendo $\Downarrow_R x = \{\, a \in A \mid (a, x) \in R \vee a = x \,\}$.

Naturalmente, considerando la relación R^{-1}, obtenemos la noción dual de la de R-sección inicial de A, que es la de R-sección final de A, y las propiedades homólogas.

Ahora que disponemos del concepto de cierre inicial, damos una caracterización del cierre transitivo de una relación binaria en un conjunto, especialmente útil para algunas demostraciones posteriores.

Proposición 0.47. *Sea A un conjunto y R una relación binaria en A. Entonces*

$$R^{\mathrm{t}} = \{\, (z,x) \in A \times A \mid \exists y \in A\, (\, (y,x) \in R \wedge z \in \mathrm{C}_R(y)\,)\,\},$$

o, lo que es equivalente

$$R^{\mathrm{t}} = \{\, (z,x) \in A \times A \mid z \in \mathrm{C}_R(\downarrow_R x)\,\}.$$

Demostración. □

Corolario 0.48. *Sea A un conjunto y R una relación binaria en A. Entonces las R-secciones iniciales coinciden con las R^{t}-secciones iniciales y las R-secciones finales con las R^{t}-secciones finales, i.e., para cada subconjunto X de A, $\mathrm{C}_R(X) = \mathrm{C}_{R^{\mathrm{t}}}(X)$ y $\mathrm{C}_{R^{-1}}(X) = \mathrm{C}_{(R^{\mathrm{t}})^{-1}}(X)$.*

Demostración. Demostramos sólo que $\mathrm{C}_R(X) = \mathrm{C}_{R^{\mathrm{t}}}(X)$. Para demostrar que $\mathrm{C}_R(X)$ está incluido en $\mathrm{C}_{R^{\mathrm{t}}}(X)$, es suficiente que demostremos que $\mathrm{C}_{R^{\mathrm{t}}}(X)$ es una R-sección inicial. Ahora bien, si $a \in \mathrm{C}_{R^{\mathrm{t}}}(X)$, entonces $\downarrow_{R^{\mathrm{t}}} a \subseteq \mathrm{C}_{R^{\mathrm{t}}}(X)$, pero $\downarrow_R a \subseteq \downarrow_{R^{\mathrm{t}}} a$, porque si $b \in \downarrow_R a$, entonces, por ser $\downarrow_R a \subseteq \mathrm{C}_R(\downarrow_R a)$, $b \in \mathrm{C}_R(\downarrow_R a)$, luego $(b,a) \in R^{\mathrm{t}}$, i.e., $b \in \downarrow_{R^{\mathrm{t}}} a$.

Del mismo modo, para demostrar que $\mathrm{C}_{R^{\mathrm{t}}}(X) \subseteq \mathrm{C}_R(X)$, es suficiente que demostremos que $\mathrm{C}_R(X)$ es una R^{t}-sección inicial. Ahora bien, si $a \in \mathrm{C}_R(X)$, entonces $\downarrow_R a \subseteq \mathrm{C}_R(X)$, luego $\mathrm{C}_R(\downarrow_R a) \subseteq \mathrm{C}_R(X)$. Además, si $b \in \downarrow_{R^{\mathrm{t}}} a$, entonces $b \in \mathrm{C}_R(\downarrow_R a)$, por lo tanto $b \in \mathrm{C}_R(X)$, así que $\downarrow_{R^{\mathrm{t}}} a \subseteq \mathrm{C}_R(X)$. □

Definición 0.49. Sea A un conjunto, R una relación binaria en A, X un subconjunto de A y $m \in X$. Decimos que m es un *R-minimal* de X si $\downarrow_R m \cap X = \varnothing$. i.e., si no hay ningún $x \in X$ tal que $(x,m) \in R$.

Definición 0.50. Sea A un conjunto y R una relación binaria en A. Decimos que R es una relación *bien fundamentada* sobre A si todo subconjunto no vacío X de A tiene un R-minimal, i.e., si hay un $m \in X$ tal que $\downarrow_R m \cap X = \varnothing$. Además, si $X \subseteq A$, diremos, para abreviar, que R está bien fundamentada sobre X si $R \cap (X \times X)$ lo está sobre X, i.e., si todo subconjunto no vacío Y de X tiene un $R \cap (X \times X)$-minimal.

A continuación establecemos la equivalencia entre el concepto de relación bien fundamentada, y un principio de demostración por inducción.

Proposición 0.51. *Sea A un conjunto y R una relación binaria en A. Entonces una condición necesaria y suficiente para que R esté bien fundamentada sobre A es que, para cada subconjunto X de A, $X = A$, si, para cada $x \in A$, $x \in X$, si $\downarrow_R x \subseteq X$, i.e., R está bien fundamentada si y sólo si*

$$\forall X \subseteq A\, ((\, \forall x \in A\, (\, \downarrow_R x \subseteq X \to x \in X\,)) \to X = A\,)$$

Demostración. La condición es necesaria. Sea X un subconjunto de A tal que para cada $x \in A$, $x \in X$, si $\downarrow_R x \subseteq X$. Si $X \neq A$, entonces $A - X \neq \varnothing$, luego, por la hipótesis, existe un $m \in A - X$ tal que $\downarrow_R m \cap (A - X) = \varnothing$, por lo tanto $\downarrow_R m \subseteq A - (A - X) = X$, así que $m \in X$, contradicción. Por consiguiente $A = X$.

La condición es suficiente. Puesto que la condición

$$\forall X \subseteq A\,((\,\forall x \in A(\downarrow_R x \subseteq X \rightarrow x \in X\,)) \rightarrow X = A\,)$$

equivale a la condición

$$\forall Y \subseteq A\,(\,A - Y \neq \varnothing \rightarrow (\,\exists x \in A\,(\,\downarrow_R x \subseteq X \wedge x \notin Y\,)),$$

si X es un subconjunto no vacío de A, entonces, tomando como subconjunto Y de A, el conjunto $A - X$, y ya que $X = A - (A - X) \neq \varnothing$, existe un $x \in A$ tal que $\downarrow_R x \subseteq A - X$ y $x \notin A - X$, luego hay un $x \in A$ tal que $\downarrow_R x \subseteq A - X$ y $x \in X$, así que hay un $x \in X$ tal que $\downarrow_R x \cap X = \varnothing$. □

Proposición 0.52. *Sea A un conjunto y R una relación binaria en A. Si R está bien fundamentada sobre A, entonces R es irreflexiva.*

Demostración. □

Proposición 0.53. *Sea A un conjunto y R una relación binaria en A. Entonces son equivalentes:*

1. *R está bien fundamentada sobre A.*
2. *R está bien fundamentada sobre cualquier R-sección inicial.*
3. *R está bien fundamentada sobre cualquier R-sección inicial principal.*

Demostración. Nos limitamos a demostrar que de la última condición se deduce la primera.

Supongamos que R esté bien fundamentada sobre cualquier R-sección inicial principal y sea X un subconjunto no vacío de A. Por ser X no vacío, sea $a \in X$, arbitrario, pero fijo. Entonces el conjunto $Y = \mathrm{C}_R(a) \cap X$, que es un subconjunto no vacío de $\mathrm{C}_R(a)$, tiene, por hipótesis, un R-minimal m, i.e., hay un $m \in Y$ tal que $\downarrow_R m \cap Y = \varnothing$. Demostramos ahora que m es un R-minimal de X. En efecto, por ser $Y \subseteq X$, se cumple que $m \in X$. Además, $\downarrow_R m \cap X = \varnothing$, ya que si $\downarrow_R m \cap X \neq \varnothing$, eligiendo un $b \in \downarrow_R m \cap X$, tendríamos que $b \in \mathrm{C}_R(a)$, porque $(b, m) \in R$ y $m \in \mathrm{C}_R(a)$; luego $b \in \downarrow_R m \cap Y$, pero éso es imposible, debido a que $\downarrow_R m \cap Y = \varnothing$. Por lo tanto $\downarrow_R m \cap X = \varnothing$, i.e., X tiene un R-minimal. □

Corolario 0.54. *Sea A un conjunto y R una relación binaria en A. Entonces R está bien fundamentada sobre A si y sólo si R^{t} lo está.*

Proposición 0.55. *La función inyectiva* $\mathrm{Sc} = \{\,(m, n) \in \mathbb{N} \times \mathbb{N} \mid n = m^+\,\}$, *es una relación bien fundamentada sobre* $\mathbb{N}$.

Demostración. En virtud de la prop. 0.53, es suficiente que demostremos que Sc está bien fundamentada sobre cada Sc-sección inicial principal $\mathrm{C}_{\mathrm{Sc}}(n)$; para lo cual, a su vez, es suficiente que demostremos, por inducción finita, que el conjunto T definido como:

$$T = \{\,n \in \mathbb{N} \mid \text{Sc está bien fundamentada sobre } \mathrm{C}_{\mathrm{Sc}}(n)\,\}$$

coincide con $\mathbb{N}$.

Se cumple que $0 \in T$, porque en este caso $\mathrm{C}_{\mathrm{Sc}}(0) = \{0\}$, ya que $\downarrow_{\mathrm{Sc}} 0 = \varnothing$ y la única parte no vacía de $\{0\}$, que es ella misma, tiene a 0 como Sc-minimal. Supongamos que $n \in T$, i.e., que Sc está bien fundamentada sobre $\mathrm{C}_{\mathrm{Sc}}(n)$, entonces, en virtud de las condiciones definitorias del concepto de álgebra de Dedekind-Peano, y por la prop. **??**, tenemos que

$$\mathrm{C}_{\mathrm{Sc}}(n^+) = \{n^+\} \cup \mathrm{C}_{\mathrm{Sc}}(n).$$

Sea X un subconjunto no vacío de $\mathrm{C}_{\mathrm{Sc}}(n^+)$. Si $X \cap \mathrm{C}_{\mathrm{Sc}}(n) = \varnothing$, entonces $X = \{n^+\}$, y n^+ es un Sc-minimal de X. Si $X \cap \mathrm{C}_{\mathrm{Sc}}(n) \neq \varnothing$, entonces, por la hipótesis de inducción, $X \cap \mathrm{C}_{\mathrm{Sc}}(n)$ tiene un Sc-minimal, i.e., hay un $m \in X \cap \mathrm{C}_{\mathrm{Sc}}(n)$ tal que $\downarrow_{\mathrm{Sc}} m \cap (X \cap \mathrm{C}_{\mathrm{Sc}}(n)) = \varnothing$, que es también un Sc-minimal de X, ya que si para algún $x \in X$ se tuviera que $(x, m) \in \mathrm{Sc}$, entonces $x \in \downarrow_{\mathrm{Sc}} m \cap (X \cap \mathrm{C}_{\mathrm{Sc}}(n))$, lo cual es imposible. Por lo tanto $n^+ \in T$. Luego $T = \mathbb{N}$, i.e., Sc está bien fundamentada sobre toda Sc-sección inicial principal $\mathrm{C}_{\mathrm{Sc}}(n)$. Podemos pues afirmar que Sc está bien fundamentada sobre $\mathbb{N}$. □

Corolario 0.56. *El cierre transitivo de* Sc*, denotado en este caso por* $<$ *y denominado el* orden aritmético *sobre* $\mathbb{N}$*, es una relación de orden bien fundamentada sobre* $\mathbb{N}$*.*

Proposición 0.57. *El orden aritmético sobre* $\mathbb{N}$ *es* disyuntivo*, i.e., tiene la siguiente propiedad*

$$\forall m, n \in \mathbb{N}\,(m \neq n \to (m < n \vee n < m))$$

Demostración. Sea $n \in \mathbb{N}$, arbitrario, pero fijo. Demostramos, por inducción sobre m, que el conjunto T definido como:

$$T = \{\, m \in \mathbb{N} \mid m = n \vee m < n \vee n < m \,\},$$

coincide con $\mathbb{N}$.

Se cumple que $0 \in T$, porque al ser $\mathrm{C}_{\mathrm{Sc}^{-1}}(0) = \mathbb{N}$, tenemos que $0 \leq n$. Supongamos que $m \in T$. Si $n \leq m$, entonces de $n \leq m$ y $m < m^+$, concluimos que $n < m^+$. Si $m < n$, entonces hay un $p \in \mathbb{N}$ tal que $p = m^+$ y $n \in \mathrm{C}_{\mathrm{Sc}^{-1}}(p)$, pero $\mathrm{C}_{\mathrm{Sc}^{-1}}(p) = \{p\} \cup \mathrm{C}_{\mathrm{Sc}^{-1}}(\uparrow_{\mathrm{Sc}^{-1}} p)$, luego $m^+ \leq n$, por lo tanto $m^+ \in T$. Así que $T = \mathbb{N}$. □

Corolario 0.58. *El orden aritmético sobre* $\mathbb{N}$ *es una buena ordenación sobre* $\mathbb{N}$*. Luego, para cada* $n \in \mathbb{N}$*,* $<_n = < \cap (n \times n)$*, es una buena ordenación sobre* n*.*

Demostramos a continuación que el orden sobre $\mathbb{N}$ coincide con la restricción de la relación de pertenencia al conjunto $\mathbb{N}$, i.e., con

$$\in_{\mathbb{N}} = \{\, (m, n) \in \mathbb{N} \mid m \in n \,\}.$$

Proposición 0.59. *Se cumple que* $< = \in_{\mathbb{N}}$*.*

Demostración. Para demostrar que $< \subseteq \in_{\mathbb{N}}$, es suficiente que demostremos que $\in_{\mathbb{N}}$ es transitivo y que contiene a Sc, porque $<$ es el cierre transitivo de Sc.

Si $(m, n) \in \mathrm{Sc}$, entonces $n = m^+$, luego $(m, n) \in \in_{\mathbb{N}}$. Además, si $(m, n) \in \in_{\mathbb{N}}$ y $(n, p) \in \in_{\mathbb{N}}$, entonces $m \in n$ y $n \in p$, luego, por ser p $\in$-transitivo, $m \in p$. Por lo tanto $< \subseteq \in_{\mathbb{N}}$.

Para demostrar que $\in_{\mathbb{N}} \subseteq <$, es suficiente que demostremos, por inducción, que el conjunto T definido como:

$$T = \{\, n \in \mathbb{N} \mid \mathrm{C}_{\mathrm{Sc}}(\downarrow_{\mathrm{Sc}} n) = n \,\},$$

coincide con $\mathbb{N}$, ya que, por la prop. 0.47, $m < n$ si y sólo si $m \in \mathrm{C}_{\mathrm{Sc}}(\downarrow_{\mathrm{Sc}} n)$.

Se cumple que $0 \in T$, porque $\mathrm{C}_{\mathrm{Sc}}(\downarrow_{\mathrm{Sc}} 0) = 0$. Supongamos que $n \in T$, entonces

$$\begin{aligned}
\mathrm{C}_{\mathrm{Sc}}(\downarrow_{\mathrm{Sc}} n^+) &= \mathrm{C}_{\mathrm{Sc}}(n) && (\text{porque } \downarrow_{\mathrm{Sc}} n^+ = \{n\}) \\
&= \{n\} \cup \textstyle\bigcup_{m \in \downarrow_{\mathrm{Sc}} n} \mathrm{C}_{\mathrm{Sc}}(m) && (\text{por la prop. } \mathbf{??}) \\
&= \{n\} \cup \mathrm{C}_{\mathrm{Sc}}(\downarrow_{\mathrm{Sc}} n) && (\text{porque } \mathrm{C}_{\mathrm{Sc}} \text{ es comp. aditivo}) \\
&= \{n\} \cup n && (\text{por la hipótesis de inducción}) \\
&= n^+ && (\text{por definición del conjunto sucesor}).
\end{aligned}$$

Por lo tanto $n^+ \in T$. Luego $T = \mathbb{N}$. □

Proposición 0.60. *Para cada $n \in \mathbb{N}$, $\downarrow_< n = n$.*

Demostración. Sea $n \in \mathbb{N}$, entonces

$$\begin{aligned}
\downarrow_< n &= \{\, m \in \mathbb{N} \mid m < n \,\} && (\text{por definición}) \\
&= \{\, m \in \mathbb{N} \mid m \in \mathrm{Sc}(\downarrow_{\mathrm{Sc}} n) \,\} && (\text{por definición}) \\
&= \{\, m \in \mathbb{N} \mid m \in n \,\} && (\text{por la prop. 0.59}) \\
&= n && (\text{por ser } \mathbb{N} \in\text{-transitivo})
\end{aligned}$$

□

Exponemos a continuación otro procedimiento para demostrar que la relación de pertenencia, restringida al conjunto de los números naturales, es una buena ordenación del citado conjunto.

En lo que sigue, convenimos que la relación binaria $<$ sobre el conjunto de los números naturales es $\in_{\mathbb{N}}$.

Proposición 0.61. *La relación $<$ es transitiva.*

Demostración. Demostramos anteriormente que todos los números naturales son $\in$-transitivos, luego si m, n y p lo son y $m < n$ y $n < p$, i.e., $m \in n$ y $n \in p$, entonces $m \in p$, i.e., $m < p$. □

Antes de demostrar que la relación $<$ es irreflexiva, establecemos el siguiente lema.

Lema 0.62. *Sean m, n dos números naturales, entonces son equivalentes:*

1. $m < n$.
2. $m^+ < n^+$.

Demostración. Supongamos que $m^+ < n^+$. Entonces, ya que $n^+ = n \cup \{n\}$, se cumple que $m^+ \in n$ o $m^+ = n$. Puesto que $m \in m^+$, si ocurre que $m^+ \in n$, entonces, por ser $n \in$-transitivo, $m \in n$, y si ocurre que $m^+ = n$, entonces, obviamente, $m \in n$, luego, en cualquier caso, $m < n$.

Para demostrar la recíproca, i.e., que, para cada $m, n \in \mathbb{N}$, si $m < n$, entonces $m^+ < n^+$, procedemos por inducción sobre n, i.e., demostramos, por inducción finita, que el conjunto

$$T = \{\, n \in \mathbb{N} \mid \forall m \in \mathbb{N}\, (m < n \to m^+ < n^+) \,\}$$

coincide con el conjunto de los números naturales.

Se cumple que $0 \in T$, porque el antecedente del condicional

$$m < 0 \to m^+ < 0^+$$

es falso.

Sea $n \in \mathbb{N}$ tal que $n \in T$. Vamos a demostrar que entonces $n^+ \in T$, i.e., que $\forall m \in \mathbb{N}\, (m < n^+ \to m^+ < (n^+)^+)$. Sea $m \in \mathbb{N}$ tal que $m < n^+$. Entonces, ya que $n^+ = n \cup \{n\}$, se cumple que $m \in n$ o $m = n$. Si ocurre que $m \in n$, entonces $m^+ \in n^+ \in (n^+)^+$, luego $m^+ < (n^+)^+$. Si ocurre que $m = n$, entonces $m^+ = n^+ \in (n^+)^+$, luego $m^+ < (n^+)^+$.

Por lo tanto $T = \mathbb{N}$. □

Corolario 0.63. *la relación $<$ es irreflexiva, i.e., para cada $n \in \mathbb{N}$, $n \not< n$.*

Demostración. Sea $T = \{\, n \in \mathbb{N} \mid n \not< n \,\}$.

Se cumple que $0 \in T$, porque $\varnothing \notin \varnothing$.

Sea $n \in \mathbb{N}$ tal que $n \in T$, i.e., tal que $n \not< n$. Entonces, en virtud del lema, $n^+ \not< n^+$, luego $n^+ \in T$. Por lo tanto $T = \mathbb{N}$. □

Corolario 0.64. *El par $(\mathbb{N}, <)$, por ser la relación $<$ irreflexiva y transitiva, es un conjunto ordenado.*

Establecemos a continuación la ley de tricotomía para el conjunto ordenado $(\mathbb{N}, <)$.

Proposición 0.65. *Para cualesquiera números naturales $m, n \in \mathbb{N}$, se cumple que $m < n$ o $m = n$ o $n < m$, pero ni $m < n$ y $m = n$, ni $m < n$ y $n < m$, y tampoco $n < m$ y $m = n$.*

Demostración. No se cumple que $m < n$ y $m = n$, porque si se cumpliera, $<$ no sería irreflexiva. No se cumple que $m < n$ y $n < m$, porque si se cumpliera, entonces, por la transitividad, tendríamos que $n < n$, luego $<$ no sería irreflexiva. No se cumple que $n < m$ y $m = n$, porque si se cumpliera, $<$ no sería irreflexiva.

Para demostrar que, para cualesquiera números naturales $m, n \in \mathbb{N}$, se cumple que $m < n$ o $m = n$ o $n < m$, procedemos por inducción sobre n, i.e., demostramos, por inducción finita, que el conjunto

$$T = \{\, n \in \mathbb{N} \mid \forall m \in \mathbb{N}\, (m < n \vee m = n \vee n < m) \,\}$$

coincide con el conjunto de los números naturales.

Se cumple que $0 \in T$, i.e., que, para cada $m \in \mathbb{N}$, $m = 0$ o $0 < m$. Para ello procedemos por inducción sobre m, i.e., demostramos, por inducción finita, que el conjunto

$$U = \{\, m \in \mathbb{N} \mid m = 0 \vee 0 < m \,\}$$

coincide con el conjunto de los números naturales.

Se cumple que $0 \in U$, porque $0 = 0$.

Supongamos que $m \in U$, i.e., que $m = 0$ o $0 < m$. Si ocurre que $m = 0$, entonces $0 < m^+ = 0^+$, luego $m^+ \in \mathbb{N}$. Si ocurre que $0 < m$, entonces, ya que $m \in m^+$, $0 \in m^+$, luego $m^+ \in \mathbb{N}$.

Por lo tanto $U = \mathbb{N}$. Con lo cual queda demostrado que $0 \in T$.

Sea $n \in \mathbb{N}$ tal que $n \in T$. Si $m < n$, entonces, ya que $n \in n^+$, $m < n^+$. Si $m = n$, entonces $m^+ = n^+$, pero $m \in m^+$, luego $m \in n^+$. Por último, si ocurre que $n < m$, entonces $n^+ < m^+$, luego, ya que $m^+ = m \cup \{m\}$, $n^+ \in m$ o $n^+ = m$. De modo que, en cualquier caso, $n^+ \in T$. Por lo tanto $T = \mathbb{N}$. □

Proposición 0.66. *El conjunto ordenado* $(\mathbb{N}, <)$ *está bien ordenado, i.e., cualquier parte no vacía de* $\mathbb{N}$*, tiene un primer elemento.*

Demostración. En lugar de demostrar que

$$\forall A \subseteq \mathbb{N}\,(A \neq \varnothing \to \exists \min(A)),$$

demostramos que

$$\forall A \subseteq \mathbb{N}\,(\neg(\exists \min(A)) \to A = \varnothing).$$

Sea pués $A \subseteq \mathbb{N}$ sin mínimo, i.e., tal que $\neg(\exists p \in A\, \forall q \in A\,(p \leq q))$, o, lo que es equivalente, tal que $\forall p \in A\, \exists q \in A\,(q < p)$. Vamos a demostrar que $A = \varnothing$, estableciendo, por inducción finita, que el conjunto

$$T = \{\, m \in \mathbb{N} \mid \forall n \in \mathbb{N}\,(n < m \to n \notin A\,\}$$

coincide con el conjunto de los números naturales.

Observemos que si ya estuviera demostrado que $T = \mathbb{N}$, $A = \varnothing$, porque si $A \neq \varnothing$, eligiendo un $p \in A$, tendríamos, por carecer A de mínimo, que existiría un $q \in A$ tal que $q < p$, luego $\neg(\forall m, n \in \mathbb{N}\,(n < m \to n \notin A))$, i.e., $\exists m, n \in \mathbb{N}\,(n < m \ \ \&\ \ n \in A)$, que entraría en contradicción con que $T = \mathbb{N}$.

Se cumple que $0 \in T$, porque en el condicional

$$n < 0 \to n \notin A,$$

el antecedente es falso.

Sea $m \in \mathbb{N}$ tal que $m \in T$. Entonces, dado un $n \in \mathbb{N}$ tal que $n < m^+$, se tiene que $n \in m$ o $n = m$. Si ocurre que $n \in m$, entonces, por la hipótesis de inducción, $n \notin A$, luego $m^+ \in T$. Si ocurre que $n = m$, entonces $m = n \notin A$, porque si $m \in A$, se cumpliría que, para cada $a \in A$, $m \leq a$, ya que, en caso contrario, i.e., si existiera un $a \in A$ tal que $a < m$, entonces $m \notin T$, que entraría en contradicción con que $m \in T$.

Por lo tanto $T = \mathbb{N}$. De donde concluimos que $A = \varnothing$. □

0.6. Principios de demostración por inducción derivados. Para abreviar, denotamos por "PDI" la frase "principio de demostración por inducción".

Proposición 0.67 (PDI de curso de valores)**.** *Sea* X *un subconjunto de* $\mathbb{N}$*. Si, para cada* $n \in \mathbb{N}$*, si cuando* $n \subseteq X$*, entonces* $n \in X$*, entonces* $X = \mathbb{N}$*.*

Demostración. □

Proposición 0.68 (PDI a partir de un número)**.** *Sea* $k \in \mathbb{N}$ *y* $X \subseteq \mathbb{N}$*. Si* $k \in X$ *y para cada* $n \in \mathbb{N}$*, si cuando* $k \leq n$ *y* $n \in X$*, entonces* $n^+ \in X$*, entonces* $\{\, n \in \mathbb{N} \mid k \leq n\,\} \subseteq X$*.*

Demostración. □

Proposición 0.69 (PDI ascendente en un intervalo)**.** *Sean $a, b \in \mathbb{N}$ tales que $a \leq b$ y $X \subseteq \mathbb{N}$. Si $a \in X$ y para cada $n \in \mathbb{N}$, si cuando $a \leq n < b$ y $n \in X$, entonces $n^+ \in X$, entonces $[a, b] = \{ n \in \mathbb{N} \mid a \leq n \wedge n \leq b \} \subseteq X$.*

Demostración. □

Proposición 0.70 (PDI descendente en un intervalo)**.** *Sean $a, b \in \mathbb{N}$ tales que $a \leq b$ y $X \subseteq \mathbb{N}$. Si $b \in X$ y para cada $n \in \mathbb{N}$, si cuando $a \leq n < b$ y $n^+ \in X$, entonces $n \in X$, entonces $[a, b] \subseteq X$.*

Demostración. □

0.7. Caracterización ordinal del conjunto de los números naturales. En la sección anterior caracterizamos al conjunto de los números naturales, dotado de la estructura algebraica, dada por el cero y el sucesor, mediante la propiedad de la definición por recursión. Ahora nos proponemos caracterizar al conjunto de los números naturales, dotado de la estructura ordinal, dada por el orden aritmético, mediante un par de propiedades ordinales adicionales, que tiene el orden sobre el conjunto de los números naturales. Para ello definimos y estudiamos una serie de conceptos, relativos a los conjuntos ordenados, útiles en sí, y algunos de ellos necesarios para establecer la caracterización ordinal antes mencionada.

Definición 0.71. Sea A un conjunto.

1. Un *orden* sobre A es una relación binaria $<$ en A tal que:
   a) $<$ es *irreflexiva*, i.e., $\forall a \in A\, (a \not< a)$.
   b) $<$ es *transitiva*, i.e., $\forall a, b, c \in A\, ((a < b \wedge b < c) \rightarrow a < c)$.
   Denotamos al conjunto de los órdenes sobre A por $\mathrm{Ord}(A)$. Un *conjunto ordenado* es un par ordenado $(A, <)$, abreviado como $\mathbf{A}$, en el que $<\in \mathrm{Ord}(A)$.
2. Un *orden lineal* sobre A es una relación binaria $<$ en A tal que:
   a) $<$ es irreflexiva, i.e., $\forall a \in A\, (a \not< a)$.
   b) $<$ es transitiva, i.e., $\forall a, b, c \in A\, ((a < b \wedge b < c) \rightarrow a < c)$.
   c) $<$ es *disyuntiva*, i.e., $\forall a, b \in A\, (a \neq b \rightarrow (a < b \vee b < a))$.
   Denotamos al conjunto de los órdenes lineales sobre A por $\mathrm{Lo}(A)$. Un *conjunto linealmente ordenado* es un par ordenado $(A, <)$, abreviado como $\mathbf{A}$, en el que $<\in \mathrm{Lo}(A)$.

Sea A un conjunto. Entonces que hay una correspondencia biunívoca entre el conjunto $\mathrm{Ord}(A)$ y el conjunto de las relaciones binarias $\leq$ en A tales que:

1. $\leq$ es reflexiva, i.e., $\Delta_A \subseteq \leq$.
2. $\leq$ es antisimétrica, i.e., $\forall a, b \in A\, ((a \leq b \wedge b \leq a) \rightarrow a = b)$.
3. $\leq$ es transitiva, i.e., $\leq \circ \leq \subseteq \leq$.

Aunque el concepto de orden fué entendido, por parte de su introductor, Hausdorff, en el sentido irreflexivo, en virtud del resultado contenido en el ejercicio anterior, según el cual son indistinguibles las relaciones irreflexivas y transitivas de las refexivas, antisimétricas y transitivas en un mismo conjunto, haremos uso del concepto de orden que más convenga a la situación de que se trate.

Sea A un conjunto. Entonces que hay una correspondencia biunívoca entre el conjunto $\mathrm{Ord}(A)$ y el conjunto de las relaciones binarias $<$ en A tales que:

1. $<$ es asimétrica, i.e., $\forall a, b \in A\,(a < b \to b \not< a)$.
2. $<$ es transitiva, i.e., $< \circ < \subseteq <$.

El conjunto $\mathrm{Ord}(A)$, a su vez, se ordena por extensión, conviniendo que un orden $\leq'$ sobre A extiende a otro orden $\leq$ sobre A, precisamente cuando $\leq \subseteq \leq'$. Esto nos va a permitir caracterizar a los órdenes lineales sobre A como aquellos órdenes sobre A que sean maximales en el conjunto ordenado por extensión $\mathbf{Ord}(A)$.

Proposición 0.72. *Sea A un conjunto y $\leq \in \mathrm{Ord}(A)$. Una condición necesaria y suficiente para que $\leq$ sea un orden lineal sobre A es que $\leq$ sea maximal en $\mathbf{Ord}(A)$.*

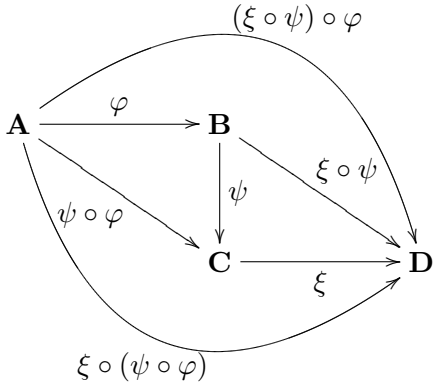
Demostración. □

Definición 0.73. Sean $\mathbf{A}$ y $\mathbf{B}$ dos conjuntos ordenados.

1. Una *aplicación isótona* de $\mathbf{A}$ en $\mathbf{B}$ es un triplo ordenado $(\mathbf{A}, \varphi, \mathbf{B})$, abreviado como φ y denotado por $\varphi\colon \mathbf{A} \longrightarrow \mathbf{B}$, en el que φ es una aplicación de A en B tal que
$$\forall x, y \in A\,(\, x \leq y \to \varphi(x) \leq \varphi(y)\,).$$
2. Una *aplicación antítona* de $\mathbf{A}$ en $\mathbf{B}$ es un triplo ordenado $(\mathbf{A}, \varphi, \mathbf{B})$, abreviado como φ y denotado por $\varphi\colon \mathbf{A} \longrightarrow \mathbf{B}$, en el que φ es una aplicación de A en B tal que
$$\forall x, y \in A\,(\, x \leq y \to \varphi(y) \leq \varphi(x)\,).$$

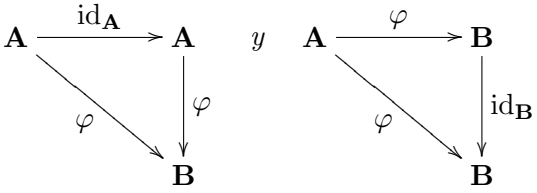
Proposición 0.74. *Sean $\varphi\colon \mathbf{A} \longrightarrow \mathbf{B}$, $\psi\colon \mathbf{B} \longrightarrow \mathbf{C}$ y $\xi\colon \mathbf{C} \longrightarrow \mathbf{D}$ tres aplicaciones isótonas entre conjuntos ordenados. Entonces:*

1. *Siendo $\mathrm{id}_{\mathbf{A}} = (\mathbf{A}, \mathrm{id}_A, \mathbf{A})$, se cumple que $\mathrm{id}_{\mathbf{A}}\colon \mathbf{A} \longrightarrow \mathbf{A}$ es un endomorfismo de $\mathbf{A}$.*
2. *Siendo $\psi \circ \varphi = (\mathbf{A}, \psi \circ \varphi, \mathbf{C})$, se cumple que $\psi \circ \varphi\colon \mathbf{A} \longrightarrow \mathbf{C}$ es una aplicación isótona de $\mathbf{A}$ en $\mathbf{C}$.*
3. (Asociatividad). *El diagrama:*



conmuta.

4. (Neutros). *Los diagramas:*



conmutan.

La composición de dos aplicaciones antítonas es una aplicación isótona, y que la composición de una isótona y una antítona es antítona.

Definición 0.75. Sea $\mathbf{A}$ un conjunto ordenado, $X \subseteq A$ y $a \in A$.

1. Decimos que a que es el *máximo* de $\mathbf{A}$ si, para cada $x \in A$, se cumple que $x \leq a$.
2. Decimos de a es el *mínimo* de $\mathbf{A}$ si, para cada $x \in A$, se cumple que $a \leq x$.
3. Decimos que a es un *minorante* o una *cota inferior* de X en $\mathbf{A}$, y lo denotamos por $a \leq X$, si, para cada $x \in X$, $a \leq x$. Denotamos por $\mathrm{Cinf}_{\mathbf{A}}(X)$ el conjunto de las cotas inferiores de X en $\mathbf{A}$. Además, si $\mathrm{Cinf}_{\mathbf{A}}(X) \neq \varnothing$, entonces decimos que el conjunto X está *acotado inferiormente* en $\mathbf{A}$. Convenimos que $\mathrm{Cinf}_{\mathbf{A}}(\varnothing) = A$.
4. Decimos que a que es un *mayorante* o una *cota superior* de X en $\mathbf{A}$, y lo denotamos por $X \leq a$, si, para cada $x \in X$, $x \leq a$. Denotamos por $\mathrm{Csup}_{\mathbf{A}}(X)$ el conjunto de las cotas superiores de X en $\mathbf{A}$. Además, si $\mathrm{Csup}_{\mathbf{A}}(X) \neq \varnothing$, entonces decimos que el conjunto X está *acotado superiormente* en $\mathbf{A}$. Convenimos que $\mathrm{Csup}_{\mathbf{A}}(\varnothing) = A$.
5. Si X es tal que $\mathrm{Cinf}_{\mathbf{A}}(X) \neq \varnothing$ y $\mathrm{Csup}_{\mathbf{A}}(X) \neq \varnothing$, entonces decimos que X está *acotado* en $\mathbf{A}$.

Un conjunto linealmente ordenado coinciden los conceptos de mínimo y de minimal, así como los de máximo y de maximal

Sea $\mathbf{A}$ un conjunto ordenado y $X \subseteq A$ no vacía. Entonces

1. $\mathrm{Cinf}_{\mathbf{A}}(X) = \bigcap_{x \in X} \Downarrow_{\leq} x$.
2. $\mathrm{Csup}_{\mathbf{A}}(X) = \bigcap_{x \in X} \Uparrow_{\leq} x$.

Definición 0.76. Sea $\mathbf{A}$ un conjunto linealmente ordenado y X una parte de A. Decimos que X es un *intervalo* de $\mathbf{A}$ si, para cada $a \in A$ y cada $x, y \in X$, si $x \leq a \leq y$, entonces $a \in A$.

Proposición 0.77. *Sea* $\mathbf{A}$ *un conjunto linealmente ordenado y* X *una parte de* A*. Entonces* $\widehat{X} = \{\, a \in A \mid \exists x, y \in X\, (\, x \leq a \leq y\,)\,\}$ *es un intervalo de* $\mathbf{A}$ *que contiene a* X *y es el mínimo intervalo de* $\mathbf{A}$ *con dicha propiedad. Por lo tanto* X *es un intervalo exactamente si* $X = \widehat{X}$*.*

Demostración. □

Introducimos a continuación el concepto de *conexión de Galois contravariante*, ya que, como demostraremos en lo que sigue, los operadores $\mathrm{Cinf}_{\mathbf{A}}$ y $\mathrm{Csup}_{\mathbf{A}}$, constituyen un ejemplo de tan importante concepto, introducido por Galois, a principios del XIX, al estudiar la relación existente entre cuerpos y grupos de automorfismos.

Definición 0.78. Una *conexión de Galois contravariante* es un cuádruplo ordenado $(\mathbf{A}, \varphi, \psi, \mathbf{B})$ en el que $\mathbf{A}$ y $\mathbf{B}$ son conjuntos ordenados, φ una aplicación antítona de $\mathbf{A}$ en $\mathbf{B}$ y ψ una aplicación antítona de $\mathbf{B}$ en $\mathbf{A}$ tales que:

1. $\forall a \in A\,(\, a \leq \psi(\varphi(a))\,)$.
2. $\forall b \in B\,(\, b \leq \varphi(\psi(b))\,)$.

Proposición 0.79. *Sea* $\mathbf{A}$ *un conjunto ordenado y* X *e* Y *dos subconjuntos de* A *tales que* $X \subseteq Y$*. Entonces:*

1. $\mathrm{Cinf}_{\mathbf{A}}(X)$ *es una* $\leq$*-sección inicial* A*.*
2. $\mathrm{Csup}_{\mathbf{A}}(X)$ *es una* $\leq$*-sección final de* A*.*
3. $\mathrm{Cinf}_{\mathbf{A}}(Y) \subseteq \mathrm{Cinf}_{\mathbf{A}}(X)$*.*
4. $\mathrm{Csup}_{\mathbf{A}}(Y) \subseteq \mathrm{Csup}_{\mathbf{A}}(X)$*.*
5. $X \subseteq \mathrm{Csup}_{\mathbf{A}}(\mathrm{Cinf}_{\mathbf{A}}(X))$*.*
6. $X \subseteq \mathrm{Cinf}_{\mathbf{A}}(\mathrm{Csup}_{\mathbf{A}}(X))$*.*

Demostración. □

Corolario 0.80. *Si* $\mathbf{A}$ *es un conjunto ordenado, entonces el cuádruplo ordenado* $(\mathrm{Sub}(A), \mathrm{Cinf}_{\mathbf{A}}, \mathrm{Csup}_{\mathbf{A}}, \mathrm{Sub}(A))$ *es una conexión de Galois contravariante.*

Proposición 0.81. *Sea* $\mathbf{A}$ *un conjunto ordenado. Entonces:*

1. *Para cada parte* X *de* A*,* $\mathrm{Cinf}_{\mathbf{A}}(X) = \mathrm{Cinf}_{\mathbf{A}}(\mathrm{Csup}_{\mathbf{A}}(\mathrm{Cinf}_{\mathbf{A}}(X)))$*.*
2. *Para cada parte* X *de* A*,* $\mathrm{Csup}_{\mathbf{A}}(X) = \mathrm{Csup}_{\mathbf{A}}(\mathrm{Cinf}_{\mathbf{A}}(\mathrm{Csup}_{\mathbf{A}}(X)))$*.*
3. $\mathrm{Csup}_{\mathbf{A}} \circ \mathrm{Cinf}_{\mathbf{A}}$ *y* $\mathrm{Cinf}_{\mathbf{A}} \circ \mathrm{Csup}_{\mathbf{A}}$ *son operadores clausura sobre* A*, i.e., ambos son extensivos, isótonos e idempotentes.*
4. *La restricción de* $\mathrm{Cinf}_{\mathbf{A}}$ *al conjunto de los puntos fijos del operador clausura* $\mathrm{Csup}_{\mathbf{A}} \circ \mathrm{Cinf}_{\mathbf{A}}$ *y al conjunto de los puntos fijos del operador clausura* $\mathrm{Cinf}_{\mathbf{A}} \circ \mathrm{Csup}_{\mathbf{A}}$*, determina un antiisomorfismo de* $\mathrm{Im}(\mathrm{Csup}_{\mathbf{A}} \circ \mathrm{Cinf}_{\mathbf{A}})$ *en* $\mathrm{Im}(\mathrm{Cinf}_{\mathbf{A}} \circ \mathrm{Csup}_{\mathbf{A}})$*, cuyo inverso es precisamente el antiisomorfismo de* $\mathrm{Im}(\mathrm{Cinf}_{\mathbf{A}} \circ \mathrm{Csup}_{\mathbf{A}})$ *en* $\mathrm{Im}(\mathrm{Csup}_{\mathbf{A}} \circ \mathrm{Cinf}_{\mathbf{A}})$ *determinado por la restricción de* $\mathrm{Csup}_{\mathbf{A}}$ *al conjunto de los puntos fijos del operador clausura* $\mathrm{Cinf}_{\mathbf{A}} \circ \mathrm{Csup}_{\mathbf{A}}$ *y al conjunto de los puntos fijos del operador clausura* $\mathrm{Csup}_{\mathbf{A}} \circ \mathrm{Cinf}_{\mathbf{A}}$*.*
5. *Para cada subconjunto no vacío* $\mathcal{X}$ *de* $\mathrm{Sub}(A)$*, se cumple que*

$$\mathrm{Cinf}_{\mathbf{A}}(\textstyle\bigcup_{X \in \mathcal{X}} X) = \bigcap_{X \in \mathcal{X}} \mathrm{Cinf}_{\mathbf{A}}(X) \;\; y \;\; \mathrm{Csup}_{\mathbf{A}}(\textstyle\bigcup_{X \in \mathcal{X}} X) = \bigcap_{X \in \mathcal{X}} \mathrm{Csup}_{\mathbf{A}}(X).$$

Demostración. □

Definición 0.82. Sea $\mathbf{A}$ un conjunto ordenado, $X \subseteq A$ y $a \in A$.

1. Decimos que a es el *ínfimo* o el *extremo inferior* de X en $\mathbf{A}$, si cumple las siguientes condiciones:
   a) Para cada $x \in X$, $a \leq x$, i.e., $a \in \mathrm{Cinf}_{\mathbf{A}}(X)$.
   b) Para cada $b \in \mathrm{Cinf}_{\mathbf{A}}(X)$, $b \leq a$.
   Denotamos por $\mathrm{Inf}_{\mathbf{A}}(X)$, o $\mathrm{ínf}_{\mathbf{A}}\, X$, o simplemente por ínf X, el ínfimo de X en $\mathbf{A}$, si tal ínfimo existe.
2. Decimos que a que es el *supremo* o el *extremo superior* de X en $\mathbf{A}$, si cumple las siguientes condiciones:
   a) Para cada $x \in X$, $x \leq a$, i.e., $a \in \mathrm{Csup}_{\mathbf{A}}(X)$.
   b) Para cada $b \in \mathrm{Csup}_{\mathbf{A}}(X)$, $a \leq b$.

Denotamos por $\mathrm{Sup}_{\mathbf{A}}(X)$, o $\bigvee_{\mathbf{A}} X$, o simplemente por $\bigvee X$, el supremo de X en $\mathbf{A}$, si tal supremo existe.

Así pues, el ínfimo de X en $\mathbf{A}$, si existe, es la máxima de las cotas inferiores de X en $\mathbf{A}$. Además, tal ínfimo no pertenece necesariamente a X, pero si perteneciera, entonces sería el mínimo de X. Del mismo modo, el supremo de X en $\mathbf{A}$, caso de existir, es la mínima de las cotas superiores de X en $\mathbf{A}$, y no pertenece necesariamente a X, pero si perteneciera, entonces sería el máximo de X.

Proposición 0.83. *Sea* $\mathbf{A}$ *un conjunto ordenado y* $X \subseteq A$ *tal que existan* $\inf X$ *y* $\bigvee X$*. Entonces:*

1. *Si* $X = \varnothing$*, entonces* $\inf X$ *es el máximo de* $\mathbf{A}$ *y* $\bigvee X$ *el mínimo de* $\mathbf{A}$*.*
2. *Si* $X \neq \varnothing$*, entonces* $\inf X \leq \bigvee X$*.*

Demostración. □

Proposición 0.84. *Sea* $\mathbf{A}$ *un conjunto ordenado y* X *e* Y *dos subconjuntos de* A *tales que existan* $\inf X$*,* $\bigvee X$*,* $\inf Y$ *y* $\bigvee Y$*. Si* $X \subseteq Y$*, entonces* $\inf Y \leq \inf X$ *y* $\bigvee X \leq \bigvee Y$*.*

Demostración. □

Proposición 0.85. *Sea* $\mathbf{A}$ *un conjunto ordenado y* $(x_i)_{i\in i}$ *e* $(y_i)_{i\in I}$ *dos familias en* A *tales que, para cada* $i \in I$*,* $x_i \leq y_i$*. Entonces:*

1. *Si existen* $\bigvee_{i\in I} x_i$ *y* $\bigvee_{i\in I} y_i$*, entonces* $\bigvee_{i\in I} x_i \leq \bigvee_{i\in I} y_i$*.*
2. *Si existen* $\inf_{i\in I} x_i$ *e* $\inf_{i\in I} y_i$*, entonces* $\inf_{i\in I} x_i \leq \inf_{i\in I} y_i$*.*

Demostración. □

Proposición 0.86. *Sea* $\mathbf{A}$ *un conjunto ordenado,* $(x_i)_{i\in I}$ *una familia en* A *y* $(J_l)_{l\in L}$ *una familia de subconjuntos de* I *tal que* $I = \bigcup_{l\in L} J_l$*. Entonces:*

1. *Si para cada* $l \in L$*, existe* $\bigvee_{i\in J_l} x_i$*, entonces existe* $\bigvee_{i\in I} x_i$ *si y sólo si existe* $\bigvee_{l\in L}(\bigvee_{i\in J_l} x_i)$*, y entonces*
$$\bigvee_{i\in I} x_i = \bigvee_{l\in L}(\bigvee_{i\in J_l} x_i).$$
2. *Si para cada* $l \in L$*, existe* $\inf_{i\in J_l} x_i$*, entonces existe* $\inf_{i\in I} x_i$ *si y sólo si existe* $\inf_{l\in L}(\inf_{i\in J_l} x_i)$*, y entonces*
$$\inf_{i\in I} x_i = \inf_{l\in L}(\inf_{i\in J_l} x_i).$$

Demostración. □

Corolario 0.87. *Sea* $\mathbf{A}$ *un conjunto ordenado y* $(x_{i,j})_{(i,j)\in I\times J}$ *una familia en* A*. Entonces:*

1. *Si para cada* $j \in J$*, existe* $\bigvee_{i\in I} x_{i,j}$*, entonces existe* $\bigvee_{(i,j)\in I\times J} x_{i,j}$ *si y sólo si existe* $\bigvee_{j\in J}(\bigvee_{i\in I} x_{i,j})$*, y entonces*
$$\bigvee_{(i,j)\in I\times J} x_{i,j} = \bigvee_{j\in J}(\bigvee_{i\in I} x_{i,j}).$$
2. *Si para cada* $j \in J$*, existe* $\inf_{i\in I} x_{i,j}$*, entonces existe* $\inf_{(i,j)\in I\times J} x_{i,j}$ *si y sólo si existe* $\inf_{j\in J}(\inf_{i\in I} x_{i,j})$*, y entonces*
$$\inf_{(i,j)\in I\times J} x_{i,j} = \inf_{j\in J}(\inf_{i\in I} x_{i,j}).$$

Demostración. □

Proposición 0.88. *Sea* $\mathbf{A}$ *un conjunto ordenado y* X *e* Y *dos subconjuntos de* A *tales que* $X \subseteq Y$*. Entonces:*

1. *Si existen* $\bigvee_{\mathbf{A}} X$ *y* $\bigvee_{\mathbf{Y}} X$*, siendo* $\mathbf{Y} = (Y, \leq \cap (Y \times Y))$*, entonces* $\bigvee_{\mathbf{A}} X \leq \bigvee_{\mathbf{Y}} X$*. Además, si* $\bigvee_{\mathbf{A}} X$ *existe y pertenece a* Y*, entonces* $\bigvee_{\mathbf{Y}} X$ *existe y* $\bigvee_{\mathbf{A}} X = \bigvee_{\mathbf{Y}} X$*.*
2. *Si existen* $\text{ínf}_{\mathbf{A}} X$ *y* $\text{ínf}_{\mathbf{Y}} X$*, entonces* $\text{ínf}_{\mathbf{Y}} X \leq \text{ínf}_{\mathbf{A}} X$*. Además, si* $\text{ínf}_{\mathbf{A}} X$ *existe y pertenece a* Y*, entonces* $\text{ínf}_{\mathbf{Y}} X$ *existe y* $\text{ínf}_{\mathbf{A}} X = \text{ínf}_{\mathbf{Y}} X$*.*

Demostración. □

Proposición 0.89. *Si un conjunto no vacío de números naturales está acotado superiormente, entonces tiene un máximo.*

Demostración. □

Teorema 0.90. *Sea* $\mathbf{A}$ *un conjunto linealmente ordenado no vacío tal que:*

1. $\forall x \in A \, \exists y \in A \, (\, x < y \,)$.
2. $\forall X \subseteq A \, (\, X \neq \varnothing \rightarrow \exists m \in X \, (\, \forall x \in X \, (\, m \leq x \,)))$.
3. $\forall X \subseteq A \, (\text{Csup}_{\mathbf{A}}(X) \neq \varnothing \rightarrow \exists n \in X \, (\forall x \in X \, (x \leq n)))$.

Entonces $\mathbf{A} \cong \mathbf{N}$.

Demostración. □

Definición 0.91. Un conjunto es *finito* si es isomorfo a un número natural. En caso contrario decimos que es *infinito*. Además, si A es un conjunto, $\text{Sub}_{\text{fin}}(A)$ denota el conjunto de los subconjuntos finitos de A.

Lema 0.92. *Para cada número natural* n *se cumple que toda aplicación inyectiva de* n *en sí mismo es sobreyectiva.*

Demostración. La demostración es por inducción. Sea T el subconjunto de $\mathbb{N}$ definido como:

$$T = \left\{ n \in \mathbb{N} \;\middle|\; \forall f \colon n \longrightarrow n \left(\begin{array}{c} \text{si } f \colon n \rightarrowtail n, \\ \text{entonces } f \colon n \twoheadrightarrow n \end{array} \right) \right\}.$$

Se cumple que $0 \in T$, porque la única aplicación de 0 en sí mismo es la aplicación identidad, que es biyectiva.

Sea $n \in \mathbb{N}$ y supongamos que $n \in T$. Queremos demostrar que entonces $n \cup \{n\} \in T$. □

Corolario 0.93 (Dirichlet)**.** *Ningún número natural es isomorfo a un subconjunto estricto de sí mismo.*

Demostración. Si un número natural n fuera isomorfo a un subconjunto estricto X de sí mismo, mediante una biyección $f \colon n \longrightarrow X$, entonces, componiendo f con la inclusión canónica $\text{in}_{X,n}$ de X en n, obtendríamos una aplicación inyectiva $\text{in}_{X,n} \circ f \colon n \rightarrowtail n$, luego tal aplicación debería ser sobreyectiva. Pero la imagen de la aplicación $\text{in}_{X,n} \circ f$ es X que es una parte propia de n. Contradicción. Por lo tanto ningún número natural es isomorfo a un subconjunto estricto de sí mismo. □

Corolario 0.94. *Ningún conjunto finito es isomorfo a un subconjunto estricto de sí mismo.*

Corolario 0.95. *Para cada número natural n se cumple que toda aplicación sobreyectiva de n en sí mismo es inyectiva.*

Demostración. Sea $f\colon n \twoheadrightarrow n$. Entonces f tiene una inversa por la derecha, i.e., existe una aplicación $g\colon n \longrightarrow n$ tal que $f \circ g = \mathrm{id}_n$. Por lo tanto g es inyectiva, luego biyectiva, de donde $f \circ g \circ g^{-1} = g^{-1}$, i.e., $f = g^{-1}$, así que f es biyectiva, luego, en particular, inyectiva. □

Corolario 0.96. *Ningún número natural n es isomorfo a un cociente n/Φ, siendo Φ una relación de equivalencia sobre n tal que $\Phi \neq \Delta_n$.*

Demostración. Si un número natural n fuera isomorfo a un cociente n/Φ, para una relación de equivalencia Φ sobre n tal que $\Phi \neq \Delta_n$, mediante una biyección $f\colon n \longrightarrow n/\Phi$, entonces, componiendo la proyección canónica pr_Φ de n en n/Φ con f^{-1} , obtendríamos una aplicación sobreyectiva $f^{-1} \circ \mathrm{pr}_\Phi\colon n \twoheadrightarrow n$, luego tal aplicación debería ser inyectiva. Pero, por ser $\Phi \neq \Delta_n$, hay dos números naturales $i, j \in n$ tales que $i \neq j$ pero $(i, j) \in \Phi$, luego $[i]_\Phi = [j]_\Phi$, así que $f^{-1}([i]_\Phi) = f^{-1}([j]_\Phi)$. Contradicción. Por lo tanto ningún número natural es isomorfo a un cociente n/Φ, siendo Φ una relación de equivalencia sobre n tal que $\Phi \neq \Delta_n$. □

Corolario 0.97. *Ningún conjunto finito A es isomorfo a un cociente A/Φ, siendo Φ una relación de equivalencia sobre A tal que $\Phi \neq \Delta_A$.*

Proposición 0.98. *Para cada número natural n se cumple que no hay ninguna aplicación inyectiva de $n \cup \{n\}$ en n.*

Demostración. Supongamos que exista una aplicación inyectiva f de $n \cup \{n\}$ en n. Entonces, componiendo f con la inclusión canónica $\mathrm{in}_{n,n\cup\{n\}}$, obtenemos una aplicación inyectiva de $n \cup \{n\}$ en sí mismo. Por lo tanto $\mathrm{in}_{n,n\cup\{n\}} \circ f$ es sobreyectiva, pero la imagen de la aplicación $\mathrm{in}_{n,n\cup\{n\}} \circ f$ es $f[n] \subset n$, luego n no está en tal imagen. Contradicción. Por lo tanto, para cada número natural n se cumple que no hay ninguna aplicación inyectiva de $n \cup \{n\}$ en n. □

Corolario 0.99. *Para cada número natural n se cumple que no hay ninguna aplicación sobreyectiva de n en $n \cup \{n\}$.*

Demostración. Si existiera una aplicación sobreyectiva $f\colon n \twoheadrightarrow n \cup \{n\}$, entonces dicha aplicación tendría una inversa por la derecha, i.e., existiría una aplicación $g\colon n \cup \{n\} \longrightarrow n$ tal que $f \circ g = \mathrm{id}_n$. Por lo tanto g sería una aplicación inyectiva de $n \cup \{n\}$ en n. Contradicción. Por lo tanto, para cada número natural n se cumple que no hay ninguna aplicación sobreyectiva de n en $n \cup \{n\}$. □

Corolario 0.100 (Dedekind)**.**

1. *Cualquier conjunto isomorfo a un subconjunto estricto de sí mismo es infinito.*
2. *El conjunto de los números naturales es infinito.*

Corolario 0.101. *Cualquier conjunto finito es isomorfo a un único número natural. Si A es un conjunto finito, al único número natural isomorfo a A lo denominamos el número cardinal de A y lo denotamos por* $\mathrm{card}(A)$.

Lema 0.102. *Si X es un subconjunto estricto de un número natural n, entonces X es isomorfo a un único número natural $m \in n$.*

Demostración. □

Proposición 0.103. *Cualquier subconjunto de un conjunto finito es finito.*

Proposición 0.104. *Si A es un conjunto finito y F una función, entonces $F[A]$ es finito. Además,* $\mathrm{card}(F[A]) \leq \mathrm{card}(A)$.

Demostración. □

Proposición 0.105. *Si A es un conjunto finito y cada miembro de A es finito, entonces $\bigcup A$ es finito. Además, si* $\mathrm{card}(A) = n$ *y* $A = \{ X_i \mid i \in n \}$, *entonces* $\mathrm{card}(\bigcup A) \leq Sum_{i \in n} \mathrm{card}(X_i)$ *y, si* $X_i \cap X_j = \varnothing$ *cuando* $i \neq j$, *entonces* $\mathrm{card}(\bigcup A) = Sum_{i \in n} \mathrm{card}(X_i)$.

Demostración. □

Proposición 0.106. *Si A es un conjunto finito, entonces* $\mathrm{Sub}(A)$ *es finito. Además, se cumple que*

$$\mathrm{card}(\mathrm{Sub}(A)) = 2^{\mathrm{card}(A)}.$$

Demostración. □

Proposición 0.107. *Si A es un conjunto infinito, entonces, para cada $n \in \mathbb{N}$, hay una aplicación inyectiva de n en A y no hay ningún isomorfismo de n en A.*

Demostración. □

Proposición 0.108. *Si A y B son finitos, entonces $A \times B$ es finito. Además, se cumple que*

$$\mathrm{card}(A \times B) = \mathrm{card}(A) \cdot \mathrm{card}(B).$$

Demostración. □

Proposición 0.109. *Si los conjuntos A y B son finitos, entonces también los conjuntos* $\mathrm{Fnc}(A, B)$, $\mathrm{Pfnc}(A, B)$ *y* $\mathrm{Mfnc}(A, B)$ *son finitos.*

Demostración. □

Definición 0.110. Sea A un conjunto. Decimos de A que es *infinito numerable* si hay un isomorfismo entre A y $\mathbb{N}$. Si tal es el caso, lo denotamos por $\mathrm{card}(A) = \aleph_0$. Por otra parte, decimos de A que es *numerable* si A está dominado por $\mathbb{N}$. Si tal es el caso, lo denotamos por $\mathrm{card}(A) \leq \aleph_0$.

Proposición 0.111. *Cualquier subconjunto infinito de un conjunto infinito numerable es infinito numerable.*

Demostración. □

Corolario 0.112. *Una condición necesaria y suficiente para que un conjunto sea numerable es que sea finito o infinito numerable.*

Proposición 0.113. *Si A es un conjunto infinito numerable y F una función, entonces $F[A]$ es numerable.*

Demostración. □

Proposición 0.114. *El conjunto de los números naturales se puede representar como la unión de un conjunto infinito numerable de conjuntos infinito numerables*

Demostración. □

Usaremos esta últimna proposición en la teoría de la recursión cuando definamos la noción de aplicación de gran amplitud de Kouznetsov.

Proposición 0.115. *La unión de dos conjuntos infinito numerables es un conjunto infinito numerable. Por consiguiente, la unión de un conjunto finito de conjuntos infinito numerables es infinito numerable.*

Demostración. □

Teorema 0.116 (Cantor)**.** *Hay un isomorfismo de* $\mathbb{N} \times \mathbb{N}$ *en* $\mathbb{N}$*.*

Demostración. □

En la teoría de la recursión demostraremos la existencia de aplicaciones recursivas primitivas biyectivas de $\mathbb{N} \times \mathbb{N}$ en $\mathbb{N}$, para las que las dos aplicaciones asociadas a la inversa son recursivas primitivas.

Corolario 0.117. *Si A y B son dos conjuntos infinito numerables, entonces $A \times B$ es infinito numerable. Por consiguiente, para cada número natural no nulo n y cada familia $(A_i \mid i \in n)$, si para cada $i \in n$, A_i es infinito numerable, entonces $\prod_{i\in n} A_i$ es infinito numerable; en particular, si A es infinito numerable, A^n es infinito numerable.*

Proposición 0.118. *Sea $(A_n \mid n \in \mathbb{N})$ una familia de conjuntos tal que, para cada $n \in \mathbb{N}$, $A_n \neq \varnothing$ y A_n es numerable. Entonces $\bigcup_{n\in\mathbb{N}} A_n$ es numerable.*

Demostración. □

Corolario 0.119. *Si A es infinito numerable, entonces $A^\star = \bigcup_{n\in\mathbb{N}} A^n$ es infinito numerable. Por consiguiente, si A es infinito numerable, entonces $\mathrm{Sub}_{\mathrm{fin}}(A)$ es infinito numerable.*

Proposición 0.120. *Sea A un conjunto numerable y R una relación de equivalencia sobre A. Entonces A/R, el conjunto cociente de A entre R, es numerable.*

Demostración. □

Teorema 0.121 (Cantor)**.** *El conjunto de todos los subconjuntos de* $\mathbb{N}$ *es infinito y no es infinito numerable. Por consiguiente, los conjuntos se dividen en tres grupos: Los finitos, los infinito numerables y los innumerables. A los conjuntos de los dos últimos tipos los denominamos conjuntos transfinitos*

Proposición 0.122. *Sea A un conjunto y R una relación binaria en A. Entonces $\mathrm{Pog}(R)$, el preorden generado por R, coincide con $\bigcup_{n\in\mathbb{N}} R^n$, siendo $(R^n \mid n \in \mathbb{N})$ la familia de relaciones definida por recursión como:*

1. $R^0 = \Delta_A$.
2. $R^{n+1} = R \circ R^n$, *para cada* $n \in \mathbb{N}$.

Así pues, para cada $(x, y) \in A \times A$, $(x, y) \in \mathrm{Pog}(R)$ *si y sólo si* $x = y$ *o hay un* $n \in \mathbb{N} - 1$ *y una familia* $(\, a_j \mid j \in n + 1\,)$ *en* A *tal que* $a_0 = x$, $a_n = y$ *y para cada* $j \in n$, $(a_j, a_{j+1}) \in R$.

Por otra parte, $\mathrm{Eqg}(R)$*, la equivalencia generada por* R*, coincide con el conjunto de los pares* $(x, y) \in A \times A$ *tales que* $x = y$ *o hay un* $n \in \mathbb{N} - 1$ *y una familia* $(\, a_j \mid j \in n + 1\,)$ *en* A *tal que* $a_0 = x$, $a_n = y$ *y para cada* $j \in n$, $(a_j, a_{j+1}) \in R \cup R^{-1}$.

1. Algebras heterogéneas relativas a un conjunto de tipos.

En esta sección presentamos, para un conjunto de tipos S, arbitrario pero fijo, los conceptos de S-conjunto heterogéneo y S-aplicación heterogénea entre S-conjuntos heterogéneos, poniendo de relieve que tales entidades constituyen no sólo una categoría, sino un topos, i.e., un lugar matemático, lo suficientemente semejante al mundo conjuntista Cantoriano clásico, como para que en el se pueda desarrollar con toda naturalidad el pensamiento matemático, pero sujeto a la lógica interna del topos. Además, presentamos las nociones y construcciones imprescindibles del álgebra heterogénea que usaremos para definir las diferentes clases de aplicaciones y relaciones recursivas. Las aplicaciones y relaciones mencionadas se pueden definir de multidud de maneras diferentes, desde las máquinas de Turing hasta los algoritmos de Markoff, pasando por el λ-cálculo de Church o la lógica combinatoria de Curry, pero hemos adoptado una presentación algebraica de las mismas por su sencillez y claridad, al menos eso es así para el autor de estas notas.

1.1. La categoría $\mathbf{Set}^S$ de S-conjuntos.

To begin with we define, for a set of sorts, the concept of sorted set, delta of Kronecker, the relation of inclusion between sorted sets, product, coproduct and union of a family of sorted sets, intersection of a nonempty family of sorted sets and sorted mapping between sorted sets.

Definición 1.1. Let S be a set of sorts.

1. A word on S is a mapping $w\colon n \longrightarrow S$, for some $n \in \mathbb{N}$. We denote by $S^\star$ the set of all words on S, i.e., $\bigcup_{n\in\mathbb{N}} S^n$. Moreover, we call the unique mapping $\lambda\colon \varnothing \longrightarrow S$, the empty word on S. The length of w, $|w|$, is the domain of the mapping w.
2. An S-sorted set is a mapping $A = (A_s)_{s\in S}$ from S into $\boldsymbol{\mathcal{U}}$. If A and B are S-sorted sets, then $A \subseteq B$ if, for every $s \in S$, $A_s \subseteq B_s$. El conjunto de los sub-S-conjuntos de A se denota $\mathrm{Sub}(A)$ y cuando se le considera ordenado por $\subseteq_S$ como $\mathbf{Sub}(A)$. Moreover, given a set I and an I-indexed family $(A^i)_{i\in I}$ of S-sorted sets, we denote by $\prod_{i\in I} A^i$ the S-sorted set such that, for every $s \in S$,
$$(\textstyle\prod_{i\in I} A^i)_s = \prod_{i\in I} A^i_s,$$
by $\coprod_{i\in I} A^i$ the S-sorted set such that, for every $s \in S$,
$$(\textstyle\coprod_{i\in I} A^i)_s = \coprod_{i\in I} A^i_s,$$
by $\bigcup_{i\in I} A^i$ the S-sorted set such that, for every $s \in S$,
$$(\textstyle\bigcup_{i\in I} A^i)_s = \bigcup_{i\in I} A^i_s,$$

and if I is nonempty, by $\bigcap_{i\in I} A^i$ the S-sorted set such that, for every $s \in S$,

$$(\bigcap_{i\in I} A^i)_s = \bigcap_{i\in I} A^i_s.$$

3. Una S-relación de un S-conjunto A en otro B es un sub-S-conjunto Φ de $A \times B$. Al conjunto de las S-relaciones de A en B lo denotamos por $\mathrm{Rel}(A, B)$. Si $A = B$, entonces $\mathrm{Rel}(A, B)$ se denota como $\mathrm{Rel}(A)$. La diagonal de A, Δ_A, es la S-relación en A cuya coordenada s-sima es Δ_{A_s}, i.e., la diagonal de A_s. La composición de S-relaciones se realiza coordenada a coordenada, i.e., si Φ es una S-relación de A en B y Ψ lo es de B en C, la composición de Φ y Ψ, $\Psi \circ \Phi$, se define como $\Psi \circ \Phi = (\Psi_s \circ \Phi_s)_{s\in S}$.
4. Una S-función de un S-conjunto A en otro B es una S-relación funcional F de A en B, i.e., una S-relación F de A en B tal que para cada $s \in S$, F_s es una función de A_s en B_s. Al conjunto de las S-funciones de A en B lo denotamos por $\mathrm{Fnc}(A, B)$. La composición de S-funciones, que es un caso particular de la composición de S-relaciones, es una S-función.
5. Una S-aplicación de un S-conjunto A en otro B es un triplo $f = (A, F, B)$ en el que F es una S-función de A en B. Al *conjunto* de las S-aplicaciones de A en B lo denotamos por $\mathrm{Hom}(A, B)$ o por B_A. Las expresiones $f \in \mathrm{Hom}(A, B)$ y $f\colon A \longrightarrow B$ las consideramos sinónimas. La composición de S-aplicaciones es una S-aplicación, como también lo es la identidad.
6. If $w \in S^\star$ and A is an S-sorted set, then A_w is $\prod_{i\in|w|} A_{w_i}$.
7. Given a sort $t \in S$ we call delta of Kronecker in t, the S-sorted set $\delta^t = (\delta^t_s)_{s\in S}$ defined, for every $s \in S$, as:

$$\delta^t_s = \begin{cases} 1, & \text{if } s = t; \\ \varnothing, & \text{otherwise.} \end{cases}$$

For $t \in S$ and a set A, we denote by $\delta^{t,A}$ the S-sorted set defined, for every $s \in S$, as:

$$\delta^{t,A}_s = \begin{cases} A, & \text{if } s = t; \\ \varnothing, & \text{otherwise.} \end{cases}$$

En alguna ocasión, abusando del lenguaje, denotaremos por $\delta^{t,a}$ lo que deberíamos denotar por $\delta^{t,\{a\}}$.

En los conjuntos ordinarios, las aplicaciones de un conjunto A en otro B son, a su vez, un conjunto que coincide con el objeto exponencial de la categoría de conjuntos. En cambio, para un conjunto de tipos S no unitario, las S-aplicaciones de un S-conjunto A en otro B no determinan un S-conjunto sino un conjunto ordinario al que hemos denotado por B_A. Reservamos la notación B^A para cuando introduzcamos el objeto exponencial de la categoría de conjuntos heterogéneos.

Las S-aplicaciones pueden clasificarse con respecto a sus propiedades locales, i.e., su comportamiento en cada coordenada del conjunto de tipos.

Definición 1.2. Sea S un conjunto de tipos, A un S-conjunto y P una propiedad de los conjuntos. Entonces A es localmente P si, para cada $s \in S$,

A_s es P. De igual modo, si $f\colon A \longrightarrow\!\!\!\!\!\rightarrow B$ es una S-aplicación y P una propiedad de las aplicaciones, entonces f es localmente P si, para cada $s \in S$, f_s es P. En particular, un S-conjunto es localmente finito si, para cada $s \in S$, A_s es finito y una S-aplicación es localmente inyectiva (resp., sobreyectiva, biyectiva) cuando la S-función subyacente es, para cada $s \in S$, inyectiva (resp., sobreyectiva, biyectiva).

Los operadores de imagen directa e imagen inversa asociados a una S-aplicación f se definen, igualmente, coordenada a coordenada.

Definición 1.3. Sea $f\colon A \longrightarrow\!\!\!\!\!\rightarrow B$ una S-aplicación:

1. La f-imagen directa (o imagen directa a través de f), es la aplicación definida como:
$$f[\cdot] \begin{cases} \mathrm{Sub}(A) & \longrightarrow \mathrm{Sub}(B) \\ X & \longmapsto (f_s[X_s])_{s\in S} \end{cases}$$
2. La f-imagen inversa(o imagen inversa través de f), es la S-aplicación definida como:
$$f^{-1}[\cdot] \begin{cases} \mathrm{Sub}(B) & \longrightarrow \mathrm{Sub}(A) \\ Y & \longmapsto (f_s^{-1}[Y_s])_{s\in S} \end{cases}$$

Proposición 1.4. *Sea $f\colon A \longrightarrow\!\!\!\!\!\rightarrow B$ una S-aplicación. Entonces*

1. *$f^{-1}[\cdot]$ preserva el orden y conmuta con los operadores $\bigcap$ y $\bigcup$, y también con la diferencia.*
2. *$f[\cdot]$ preserva el orden y conmuta con $\bigcup$ (pero no en general con $\bigcap$, para el que únicamente es cierto, en general, que $f[\bigcap_{F\in\mathcal{F}} F] \subseteq_S \bigcap_{F\in\mathcal{F}} f[F]$.*

A partir de una S-aplicación $f\colon A \longrightarrow\!\!\!\!\!\rightarrow B$ se obtiene un functor
$$f^{-1}[\cdot] \begin{cases} \mathbf{Sub}(B) & \longrightarrow \mathbf{Sub}(A) \\ Y & \longmapsto (\{a \in A_s \mid f_s(a) \in Y_s)\})_{s\in S} \end{cases}$$
la f-imagen inversa, que tiene un adjunto por la izquierda
$$f[\cdot] \begin{cases} \mathbf{Sub}(A) & \longrightarrow \mathbf{Sub}(B) \\ X & \longmapsto (\{b \in B_s \mid \exists x \in X_s\, (f_s(x) = b)\})_{s\in S} \end{cases}$$
la f-imagen directa o existencial, y un adjunto por la derecha
$$f_! \begin{cases} \mathbf{Sub}(A) & \longrightarrow \mathbf{Sub}(B) \\ X & \longmapsto (\{b \in B_s \mid f_s^{-1}[\{b\}] \subseteq X_s\})_{s\in S} \end{cases}$$
la f-imagen universal.

Esto significa que $\forall X \subseteq A$, $\forall Y \subseteq B$
$$f[X] \subseteq Y \text{ exactamente si } X \subseteq f^{-1}[Y] \text{ y}$$
$$f^{-1}[Y] \subseteq X \text{ exactamente si } Y \subseteq f_!(X)$$

Definición 1.5. Sea S un conjunto de tipos.

1. Una S-relación Φ en un S-conjunto A es una S-relación de equivalencia sobre A, si, para cada $s \in S$, Φ_s es una relación de equivalencia sobre A_s. Si $(a, b) \in \Phi_s$, se escribe también $a \equiv b\,(\mathrm{mód.}\,\Phi_s)$ o $a \equiv_{\Phi_s} b$.

   Al conjunto de las S-relaciones de equivalencias sobre un S-conjunto A lo denotamos por $\mathrm{Eqv}(A)$ y por $\mathbf{Eqv}(A)$ cuando lo consideremos

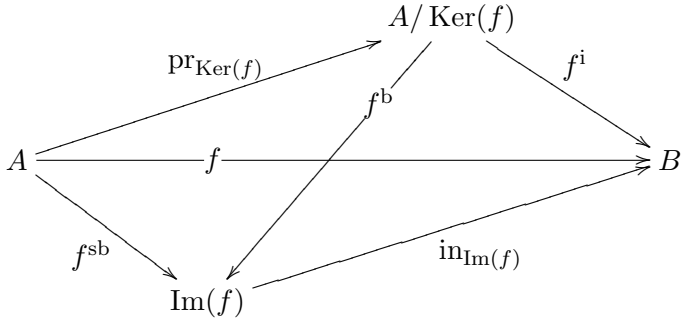
ordenado por la S-inclusión. Lo mismo que en el caso homogéneo, $\mathbf{Eqv}(A)$ es un retículo algebraico y al operador clausura algebraico asociado lo denotamos por Eg_A. Observemos que el operador equivalencia generada se obtiene localmente a través de los operadores equivalencia generada homogéneos, puesto que, para cada S-conjunto A, se cumple que $\mathrm{Eg}_A(\Phi) = (\mathrm{Eq}_{A_s}(\Phi_s))_{s\in S}$.

2. Si $\Phi, \Psi \in \mathrm{Eqv}(A)$ con $\Phi \subseteq_S \Psi$. Entonces el cociente de Ψ entre Φ, Ψ/Φ, es la S-relación de equivalencia $(\Psi_s/\Phi_s)_{s\in S}$ sobre A/Φ cuya coordenada s-sima es
$$\Psi_s/\Phi_s = \{([a]_{\Phi_s}, [b]_{\Phi_s}) \in (A_s/\Phi_s) \mid (a,b) \in \Psi_s\}$$
3. Sea $X \subseteq_S A$ y $\Phi \in \mathrm{Eqv}(A)$. La Φ-saturación de X, $\mathrm{Sat}_\Phi(X)$, es el S-conjunto cuya coordenada s-sima es
$$\mathrm{Sat}_\Phi(X)_s = \{a \in A_s \mid X_s \cap [a]_{\Phi_s} \neq \emptyset\} = \bigcup_{x\in X_s} [x]_{\Phi_s}$$

Los núcleos e imágenes de las S-aplicaciones se definen localmente. La factorización clásica de las aplicaciones es válida también para las S-aplicaciones.

Definición 1.6. Si $f\colon A \longrightarrow B$ es una S-aplicación, el núcleo de f, $\mathrm{Ker}(f)$, es la S-relación de equivalencia sobre A determinada por los núcleos de las aplicaciones subyacentes, i.e., $\mathrm{Ker}(f) = (\mathrm{Ker}(f_s))_{s\in S}$. La imagen de f, $\mathrm{Im}(f)$, es el S-conjunto $(\mathrm{Im}(f_s))_{s\in S}$.

Proposición 1.7. *Si $f\colon A \longrightarrow B$ es una S-aplicación, entonces f se puede factorizar como*



donde todas la S-aplicaciones se definen a partir de las correspondientes en cada coordenada, i.e., para cada $s \in S$, pr_s es la proyección canónica de A_s en $A_s/\mathrm{Ker}(f_s)$, f_s^{b} es el isomorfismo canónico entre $A_s/\mathrm{Ker}(f_s)$ y $\mathrm{Im}(f_s)$, in_s es la inclusión canónica en B_s, f_s^{sb} es la correstricción de f_s a $\mathrm{Im}(f_s)$ y f_s^{i} es la aplicación que a $[a]$ le asigna $f_s(a)$.

La existencia de coordenadas vacías en un S-conjunto es relevante para muchas de las nociones y construcciones que se consideran en este trabajo. Por ello, se introduce la noción de *soporte* de un S-conjunto.

Definición 1.8. Sea A un S-conjunto. El soporte de A, $\mathrm{supp}(A)$, es el conjunto de los $s \in S$ tales que A_s no es vacío, i.e., $\mathrm{supp}(A) = \{s \in S \mid A_s \neq \varnothing\}$.

Para cada conjunto S, el soporte es una función $\mathrm{supp}\colon \boldsymbol{\mathcal{U}}^S \longrightarrow \mathrm{Sub}(S)$. Algunas propiedades de esta se detallan en la siguiente proposición.

Proposición 1.9. *Sean A y B dos S-conjuntos.*

1. *Si $A \subseteq_S B$, entonces* $\mathrm{supp}(A) \subseteq \mathrm{supp}(B)$.
2. $\mathrm{supp}((\varnothing)_{s\in S}) = \varnothing$.
3. *Si $I \neq \varnothing$ y $(A^i)_{i\in I} \in (\boldsymbol{\mathcal{U}}^S)^I$, entonces* $\mathrm{supp}(\bigcup_{i\in I} A^i) = \bigcup_{i\in I} \mathrm{supp}(A^i)$.
4. *Si $I \neq \varnothing$ y $(A^i)_{i\in I} \in (\boldsymbol{\mathcal{U}}^S)^I$, entonces* $\mathrm{supp}(\bigcap_{i\in I} A^i) = \bigcap_{i\in I} \mathrm{supp}(A^i)$.
5. $\mathrm{supp}(A) - \mathrm{supp}(B) \subseteq \mathrm{supp}(A - B)$.
6. $\mathrm{Hom}(A, B) \neq \varnothing$ *si y sólo si* $\mathrm{supp}(A) \subseteq \mathrm{supp}(B)$.

Para los S-conjuntos, la noción de cardinal puede definirse globalmente o relativa a cada coordenada. Desde un punto de vista *interno* a las categorías de S-conjuntos la noción adecuada es la de S-cardinal, entendiendo por tal un S-conjunto en el que todas sus coordenadas son cardinales. Externamente, la cardinalidad del coproducto de un S-conjunto es, a veces, más importante, como cuando se consideran algebras heterogéneas con operaciones finitarias.

Definición 1.10. Sea A un S-conjunto.

1. El S-cardinal de A es el S-conjunto $\mathrm{card}_S(A) = (\mathrm{card}(A_s))_{s\in S}$. Si $\mathfrak{m}$ y $\mathfrak{n}$ son S-cardinales entonces $\mathfrak{m} < \mathfrak{n}$ si, para cada $s \in S$, $\mathfrak{m}_s < \mathfrak{n}_s$. El cardinal de A, $\mathrm{card}(A)$, es el cardinal del conjunto $\coprod A$.
2. A es S-finito (resp., S-infinito, S-infinito numerable, S-numerable), si, para cada $s \in S$, $\mathrm{card}(A_s)$ es finito (resp., infinito, infinito numerable, numerable).
3. A es finito (resp., infinito, infinito numerable, numerable), si $\mathrm{card}(A)$ es finito (resp., infinito, infinito numerable, numerable).

Obsérvese que si A es S-infinito y B es finito, B se puede encajar en A. De hecho, los S-conjuntos S-infinito numerables son los S-conjuntos más pequeños en los que todos los S-conjuntos finitos se pueden encajar.

Si A es un S-conjunto, denotamos mediante $\mathrm{Sub}_{\mathrm{f}}(A)$ el conjunto de los sub-S-conjuntos finitos de A, y, para un cardinal $\mathfrak{m}$,

$$\begin{aligned}
\mathrm{Sub}_{\mathfrak{m}}(A) &= \{X \subseteq_S A \mid \mathrm{card}(\textstyle\coprod X) = \mathfrak{m}\} \\
\mathrm{Sub}_{<\mathfrak{m}}(A) &= \{X \subseteq_S A \mid \mathrm{card}(\textstyle\coprod X) < \mathfrak{m}\} \\
\mathrm{Sub}_{\leq\mathfrak{m}}(A) &= \{X \subseteq_S A \mid \mathrm{card}(\textstyle\coprod X) \leq \mathfrak{m}\}
\end{aligned}$$

Los conjuntos heterogéneos y sus aplicaciones determinan, para un conjunto de tipos fijo, una categoría que, aunque hereda muchas de sus propiedades de la categoría de conjuntos ordinarios, difiere de ésta en aspectos esenciales.

Proposición 1.11. *Los S-conjuntos y las S-aplicaciones, junto con la composición y las identidades, determinan una categoría,* $\mathbf{Set}^S$*, que es, esencialmente, la categoría de functores y transformaciones naturales de S (como categoría discreta) en* **Set**.

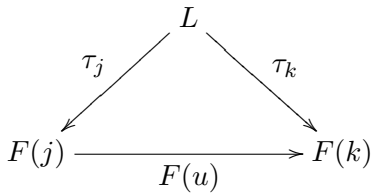
Muchas nociones categoriales en $\mathbf{Set}^S$ pueden obtenerse a partir de las correspondientes en **Set**. Por ejemplo, el objeto final en $\mathbf{Set}^S$ es el S-conjunto $1^S = (1)_{s\in S}$, que en cada coordenada es el objeto final de **Set**. Si A es un S-conjunto, la única S-aplicación de A en 1^S, $!_A$, se obtiene a partir de las

únicas aplicaciones de A_s en el objeto final de **Set**. De hecho, la construcción de límites proyectivos e inductivos en $\mathbf{Set}^S$ es un caso del teorema de los límites con parámetros de [**?**], tal como pone de manifiesto la siguiente proposición.

Proposición 1.12. *La categoría* $\mathbf{Set}^S$ *es completa y cocompleta.*

Demostración. Sea $\mathbf{J}$ una categoría pequeña y $F\colon \mathbf{J} \longrightarrow \mathbf{Set}^S$. Para cada $s \in S$, sea Pr_s el functor de $\mathbf{Set}^S$ en **Set** que a S-conjuntos A y S-aplicaciones f les asigna sus coordenadas s-simas A_s, f_s. Sea F_s la composición de F con Pr_s. Como **Set** es completa F_s tiene un límite proyectivo (L_s, τ_s) con L_s un conjunto y τ_s un cono proyectivo de L_s en F_s. Sea $L = (L_s)_{s\in S}$ y τ el cono proyectivo de L en F definido, para cada objeto $j \in \mathbf{J}$ y cada $s \in S$ como $\tau(j)_s = \tau_s(j)$.

Veamos que el par (L, τ) es un límite proyectivo para F. Sea $u\colon j \longrightarrow k$ un morfismo en $\mathbf{J}$. El triángulo



conmuta, puesto que, para cada $s \in S$, los triángulos correspondientes conmutan, ya que las τ_s son transformaciones naturales. Es un cono proyectivo límite ya que si (M, υ) es otro cono proyectivo, entonces, para cada $s \in S$, hay un único morfismo $\gamma_s\colon M_s \longrightarrow L_s$, porque L_s es un límite proyectivo para cada s. Entonces $\gamma = (\gamma_s)_{s\in S}$ es el único morfismo de M en L que hace conmutativo el triángulo correspondiente.

La existencia de límites inductivos se demuestra del mismo modo. □

Las nociones de morfismos *inyectivos* y *sobreyectivos* en $\mathbf{Set}^S$, definidas a través de los miembros globales, no coinciden, en general, con las nociones *locales* de ambos conceptos. Además, a diferencia de lo que ocurre en **Set**, no todos los morfismos inyectivos son monomorfismos, ni todos los sobreyectivos son epimorfismos.

Definición 1.13. Sea $f\colon A \longrightarrow B$ un morfismo de $\mathbf{Set}^S$. Decimos que f es inyectivo si, para cada $x, y\colon 1^S \longrightarrow A$, si $f \circ x = f \circ y$, entonces $x = y$. Por otra parte, decimos que f es sobreyectivo si, para cada $y\colon 1^S \longrightarrow B$, existe un $x\colon 1^S \longrightarrow A$ tal que $f \circ x = y$.

Proposición 1.14. *Sea S un conjunto de tipos. Entonces, en la categoría* $\mathbf{Set}^S$*, se cumple que*

1. *Sección = loc. sección ⊂ mónica = loc. mónica = loc. inyectiva ⊂ inyectiva.*
2. *Retracción = loc. retracción = loc. épica = loc. sobreyectiva = épica ⊂ sobreyectiva.*

Demostración. Sea $f\colon A \longrightarrow B$ una S aplicación.

1. Puesto que la composición de S-aplicaciones se realiza coordenada a coordenada, f es una sección exactamente si f es localmente una sección.

Si f es mónica entonces, para cada $s \in S$ y cada par de aplicaciones $g, h\colon C \longrightarrow A_s$ se tiene que las únicas S-aplicaciones $\overline{g}, \overline{h}\colon \delta^s(C) \longrightarrow A$, que coinciden en la coordenada s-sima con g y h son tales que $f \circ \overline{g} = f \circ \overline{h}$, luego $\overline{g} = \overline{h}$ y $g = h$, por lo que f es localmente mónica. Recíprocamente, si f es localmente mónica entonces f es mónica.

Toda sección es mónica pero, al igual que en **Set** existen mónicas que no son secciones, e.g., las S-aplicaciones con dominio $0^S = (\emptyset)_{s\in S}$.

Puesto que ser mónica y ser inyectiva coinciden en **Set**, ser localmente mónica y ser localmente inyectiva coinciden en $\mathbf{Set}^S$.

La inyectividad local implica claramente la inyectividad. Sin embargo, la inyectividad no implica la inyectividad local, puesto que cualquier S-aplicación cuyo dominio tenga alguna coordenada vacía es vacuamente inyectivo, aunque no necesariamente localmente inyectivo.

2. Las retracciones coinciden en $\mathbf{Set}^S$ con las S-aplicaciones que son localmente retracciones y por tanto, con las localmente épicas y las localmente sobreyectivas.

Si f es localmente épica, entonces f es épica. Recíprocamente, si f es épica entonces, para cada $s \in S$ y cada par de aplicaciones $g, h\colon B_s \longrightarrow C$, existe un único par de aplicaciones $\overline{g}$ y $\overline{h}$ de B en $\overline{C}$, con $\overline{C}$ el S-conjunto que es 1 en cada coordenada excepto la s-sima en la que $\overline{C}$ es C, que coinciden, respectivamente, en la coordenada s-sima, con g y h. Además, $\overline{g} \circ f = \overline{h} \circ f$ y por tanto, $\overline{g} = \overline{h}$ y $g = h$, por lo que f es localmente épica.

Si f es localmente sobreyectiva entonces es sobreyectiva. Sin embargo, existen S-aplicaciones sobreyectivas que no lo son localmente, e.g., si $S = 2$, la 2-aplicación $(0, !)\colon (1, \emptyset) \longrightarrow (2, \emptyset)$ es vacuamente sobreyectiva, puesto que $(2, \emptyset)$ no tiene miembros globales, aunque no localmente sobreyectivo puesto que su coordenada 0-ésima no es sobreyectiva. □

Puesto que en $\mathbf{Set}^S$ las nociones de épica y retracción coinciden, el axioma de elección es válido en ella.

La categoría de S-conjuntos y S-aplicaciones es un topos, i.e., una categoría cartesiana cerrada con un clasificador de monomorfismos, en tanto que es una categoría de functores sobre un topos. Su estructura es *localmente* como la de conjuntos ordinarios y la proposición 1.12 establece que los límites y colímites se calculan coordenada a coordenada. Esto es cierto también para el cálculo de los exponenciales y el objeto de verdad de $\mathbf{Set}^S$.

En algunos trabajos se definen los S-conjuntos excluyendo la posibilidad de que alguna coordenada sea vacía, lo que destruye obviamente la estructura de topos de las categorías de S-conjuntos, que no son, siquiera, finito cocompletas.

Proposición 1.15. *La categoría* $\mathbf{Set}^S$ *es un topos.*

Demostración. **Set** es un topos, por lo que $\mathbf{Set}^S$, siendo (isomorfa a) una categoría de functores en **Set**, es también un topos (v. [**?**]). □

El exponencial de dos S-conjuntos A y B se denota mediante B^A y es el S-conjunto $(B_s^{A_s})_{s\in S}$, i.e., $(\mathrm{Hom}_{\mathbf{Set}}(A_s, B_s))_{s\in S}$. La función de evaluación, $\mathrm{ev}_{A,B}\colon A \times B^A \longrightarrow A$, es la S-aplicación que en la coordenada s-sima es la

función de evaluación para A_s, B_s en **Set**, i.e., $\mathrm{ev}_{(A,B)_s} = \mathrm{ev}_{A_s,B_s} \colon A_s \times B_s^{A_s} \longrightarrow B_s$.

Si A y B son S-conjuntos, el producto de su exponencial, $\prod_{s\in S} B_s^{A_s}$, es isomorfo al conjunto B_A de las S-aplicaciones de A en B. Este isomorfismo es natural, como pone de manifiesto la siguiente proposición.

Proposición 1.16. *Sea S un conjunto de tipos y* Exp *el functor de* exponenciación *definido como*

$$\begin{array}{ccc} (\mathbf{Set}^S)^{\mathrm{op}} \times \mathbf{Set}^S & \xrightarrow{\mathrm{Exp}} & \mathbf{Set}^S \\ (A,B) & & (B_s^{A_s})_{s\in S} \\ \Big\downarrow{\scriptstyle (f,g)} & \longmapsto & \Big\downarrow{\scriptstyle (g_s \circ \cdot \circ f_s)_{s\in S}} \\ (C,D) & & (D_s^{C_s})_{s\in S} \end{array}$$

Los functores Hom *y* $\prod \circ \mathrm{Exp}$ *son naturalmente isomorfos*

Demostración. El isomorfismo se define, para cada par de S-conjuntos (A,B) como

$$\begin{array}{ccc} \mathrm{Hom}(A,B) & \longrightarrow & \prod_{s\in S} B_s^{A_s} \\ f & \longmapsto & \left\{ \begin{array}{ccc} S & \longrightarrow & \bigcup_{s\in S} B_s^{A_s} \\ s & \longmapsto & \left\{ \begin{array}{ccc} A_s & \longrightarrow & B_s \\ a & \longmapsto & f_s(a) \end{array} \right. \end{array} \right. \end{array}$$

i.e., asociando a f la familia $(f_s)_{s\in S}$ □

El objeto de valores de verdad en $\mathbf{Set}^S$ se denota mediante Ω^S y consiste en el S-conjunto $(2)_{s\in S}$, que en cada coordenada es $2 = \Omega$, el objeto de valores de verdad en **Set**. El clasificador de mónicas es $\top^S = (\top)_{s\in S} \colon 1^S \longrightarrow \Omega^S$, cuya coordenada s-sima, $\top \colon 1 \longrightarrow 2$, es la aplicación que a 0 le asigna 1. El carácter de una S-aplicación mónica $f \colon A \longrightarrow B$ se obtiene entonces a partir de los caracteres de las aplicaciones componentes en **Set**, i.e., $\mathrm{ch}_f = (\mathrm{ch}_{f_s})_{s\in S}$.

Si el conjunto de tipos S no es vacío, el topos $\mathbf{Set}^S$ no es degenerado, i.e., el objeto inicial no es isomorfo a ningún objeto final. Su conjunto de valores de verdad, i.e., el conjunto de los morfismos de 1^S en Ω^S, tiene cardinalidad 2^S. Un S-conjunto es *vacío* si su conjunto de miembros globales lo es. Si $\mathrm{card}(S) \geq 2$, existen en $\mathbf{Set}^S$ objetos que no son cero pero son globalmente vacíos (los S-conjuntos que tienen alguna coordenada vacía). No es, pues, un topos bien punteado puesto que no satisface el principio de extensionalidad: un par de S-aplicaciones distintas cuyo dominio tenga alguna coordenada vacía no pueden distinguirse mediante un S-aplicación desde 1^S. Por consiguiente, 1^S no es un generador y es por ello que conviene introducir las nociones de S-conjunto subfinal y delta de Kronecker, para poder obtener un conjunto de generadores para $\mathbf{Set}^S$.

Definición 1.17.

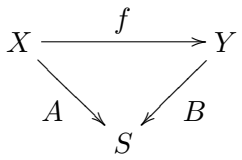
1. Un S-conjunto A es subfinal si $\mathrm{card}(A_s) \leq 1$, para todo $s \in S$.

2. Un miembro parcial de un S-conjunto A es un morfismo desde una delta de Kronecker hasta A, i.e., esencialmente un miembro de una coordenada de A.

En **Set** no existen conjuntos que estén estrictamente entre el objeto inicial y el final, pero en $\mathbf{Set}^S$ existen $2^{\mathrm{card}(S)}$ objetos, salvo isomorfismo, entre el objeto inicial, $0^S = (\varnothing)_{s\in S}$, y el final, 1^S. En general, para un S-conjunto A se cumple que $\mathrm{card}\,(\mathrm{Sub}(A)) = 2^{\sum_{s\in S}\mathrm{card}\,(A_s)}$. El conjunto $\{\delta^s \mid s \in S\}$ es un conjunto de generadores para $\mathbf{Set}^S$ puesto que cualquier par de S-aplicaciones paralelas distintas pueden ser siempre distinguidas haciendo uso de algún morfismo desde un δ^s apropiado. En general, todos los S-conjuntos se pueden representar como coproductos de múltiplos de las deltas de Kronecker, i.e., si A es un S-conjunto, entonces A es naturalmente isomorfo a $\coprod_{s\in S}\mathrm{card}(A_s)\cdot\delta^s$.

En $\mathbf{Set}^S$ se cumple que $[\top,\bot]\colon 1 \amalg 1 \longrightarrow \Omega^S$ es un isomorfismo, por lo que $\mathbf{Set}^S$ es un topos clásico y por consiguiente booleano. Su estructura lógica es, localmente, como la de **Set**. Los morfismos de verdad en $\mathbf{Set}^S$ son, en cada coordenada, los correspondientes en **Set**, e.g., $\wedge^S = (\wedge)_{s\in S}$ y $\neg^S = (\neg)_{s\in S}$. Como consecuencia, las operaciones correspondientes en las álgebras de subobjetos de $\mathbf{Set}^S$ se realizan también coordenada a coordenada y coinciden con las operaciones definidas en **??**. En el álgebra booleana de los subfinales de $\mathbf{Set}^S$, $\mathbf{Sub}(1^S)$, los δ^s son los átomos de la misma y es, esencialmente, el álgebra booleana de los subconjuntos de S, $\mathbf{Sub}(S)$.

Los S-conjuntos pueden ser considerados también como aplicaciones con codominio S, que a cada elemento del dominio de la aplicación le asigna su tipo. Como tales se denominan S-foliaciones y constituyen los objetos de la categoría de cotas inferiores de S en **Set**, $\mathbf{Set}\downarrow S$, i.e., los pares (X, A) en los que X es un conjunto y A una aplicación de X en S, que asigna a cada $x \in X$ su tipo $A(x)$. Las S-aplicaciones de un S-conjunto en otro se corresponden entonces con los morfismos de $\mathbf{Set}\downarrow S$, siendo un morfismo de (X, A) en (Y, B) un triplo $((X, A), f, (Y, B))$ en el que $f\colon X \longrightarrow Y$ tal que el siguiente diagrama conmuta



Proposición 1.18. *Las categorías* $\mathbf{Set}^S$ *y* $\mathbf{Set}\downarrow S$ *son equivalentes.*

Demostración. Sea A un S-conjunto. Sea P^S el functor definido como

$$\begin{array}{ccc} \mathbf{Set}^S & \xrightarrow{\;P^S\;} & \mathbf{Set}\downarrow S \\ A & & (\coprod A, [\kappa_s^A]_{s\in S}) \\ f\downarrow & \longmapsto & \downarrow\coprod f \\ B & & (\coprod B, [\kappa_s^B]_{s\in S}) \end{array}$$

donde κ_s^A es la aplicación constante de A_s en S que asigna a cada miembro de A_s su tipo s y $[\kappa_s^A]_{s\in S}$ la única aplicación de $\coprod A$ en S determinada por la propiedad universal del coproducto, y lo mismo para κ_s^A y $[\kappa_s^A]_{s\in S}$.

Sea Q^S el functor definido como

$$\begin{array}{ccc} \mathbf{Set}\downarrow S & \xrightarrow{\quad Q^S \quad} & \mathbf{Set}^S \\ (X,A) & & (A^{-1}(s))_{s\in S} \\ \Big\downarrow f & \longmapsto & \Big\downarrow (f_s)_{s\in S} \\ (Y,B) & & (B^{-1}(s))_{s\in S} \end{array}$$

donde f_s es la restricción de f al dominio y codominio indicado. Ambos functores son cuasi-inversos, i.e., su composición es naturalmente isomorfa a la identidad, por lo que ambas categorías son equivalentes. □

La categoría $\mathbf{Set}\downarrow S$ es un topos, por el *teorema fundamental de los topoi* (v. [**?**]). La equivalencia con la categoría $\mathbf{Set}^S$ determina morfismos entre ambas categorías que permiten *traducir* la estructura de topos de una categoría hasta la otra, por lo que cualquiera de las dos puede ser utilizada como formalización de los conceptos de conjunto y aplicación heterogénea para un conjunto de tipos S fijo. Sin embargo, algunas construcciones tienen una forma más *natural* en una de las dos, por lo que resulta conveniente considerar directamente algunas de las propiedades del topos $\mathbf{Set}\downarrow S$.

Productos. Sean (X,A) y (Y,B) dos objetos en $\mathbf{Set}\downarrow S$. Su producto es $(X,A)\times(Y,B) = (\mathrm{Pb}(A,B),\mathrm{pr})$, con $\mathrm{Pb}(A,B)$ el producto fibrado en **Set** de A y B, y $\mathrm{p} = A\circ \mathrm{p}_0 = B\circ \mathrm{p}_1$.

$$\begin{array}{ccc} \mathrm{Pb}(A,B) & \xrightarrow{\ \mathrm{p}_1\ } & Y \\ \Big\downarrow \mathrm{p}_0 & \searrow^{\mathrm{p}} & \Big\downarrow B \\ X & \xrightarrow[A]{} & S \end{array}$$

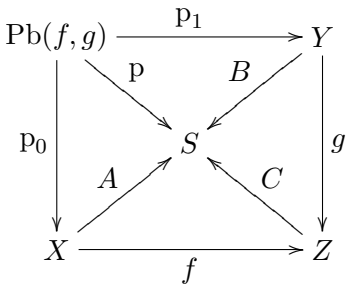
El objeto final es $1^{\downarrow S} = (S, \mathrm{id}_S)$

Igualadores. Sean $f,g\colon (X,A)\longrightarrow(Y,B)$. Su igualador es $\mathrm{eq}(f,g)$ considerado como un morfismo de $\mathrm{Eq}^{\downarrow S}(f,g) = A\circ\mathrm{eq}(f,g)$ en B.

$$\begin{array}{ccccc} \mathrm{Eq}(f,g) & \xrightarrow{\mathrm{eq}(f,g)} & X & \overset{f}{\underset{g}{\rightrightarrows}} & Y \\ & \searrow^{\mathrm{Eq}^{\downarrow S}(f,g)} & \Big\downarrow A & & \swarrow_{B} \\ & & S & & \end{array}$$

Productos fibrados. Sean $f\colon (X,A)\longrightarrow(Z,C)$ y $G\colon (Y,B)\longrightarrow(Z,C)$ dos morfismos en $\mathbf{Set}\downarrow S$. El producto fibrado de f y g, $\mathrm{Pb}^{\downarrow S}(f,g)$, es $(\mathrm{Pb}(f,g),\mathrm{p})$ con $\mathrm{Pb}(f,g)$ el producto fibrado de f y g en **Set** y $\mathrm{p} = C\circ f\circ$

$\mathrm{p}_0 = C \circ g \circ \mathrm{p}_1$ en $\mathbf{Set} \downarrow S$.

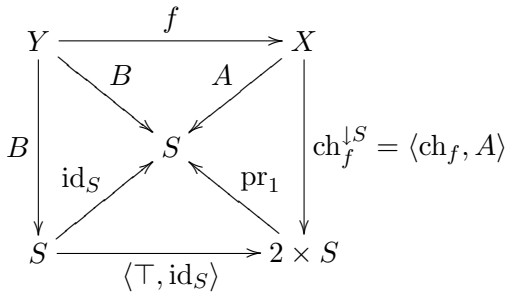


Colímites. El coproducto de (X, A) y (Y, B) es $[A, B]$, la única aplicación de $X \amalg Y$ en S. El objeto inicial es $0^{\downarrow S} = (\emptyset, !_{\emptyset,S})$. El coigualador y la suma amalgamada se obtienen mediante diagramas duales a los del igualador y el producto fibrado.

Exponenciales. Sean (X, A) y (Y, B) dos objetos en $\mathbf{Set} \downarrow S$. Entonces $(Y, B)^{(X,A)} = (\coprod_{s \in S} B^{-1}(s)^{A^{-1}(s)}, \mathrm{pr}_1)$ y la función de evaluación, $\mathrm{ev}_{(X,A),(Y,B)}$ se define como

$$\mathrm{ev}_{(X,A),(Y,B)} \begin{cases} \mathrm{Pb}(A, \mathrm{pr}_1) \longrightarrow Y \\ (x, (f, s)) \longmapsto f(x) \end{cases}$$

Clasificador de subobjetos. El objeto de valores de verdad, $\Omega^{\downarrow S}$, viene dado por $(2 \times S, \mathrm{pr}_1)$, y el clasificador de mónicas es $\top^{\downarrow S} = \langle \top_S, \mathrm{id}_S \rangle$. Si $f \colon (Y, B) \rightarrowtail (X, A)$ entonces $\mathrm{ch}_f^{\downarrow S} = \langle \mathrm{ch}_f, A \rangle$.



Valores de verdad. Por ser $\mathbf{Set} \downarrow S$ un topos, los elementos de Ω^S están en correspondencia biunívoca con $\mathrm{Sub}(1^S)$. Ahora bien, un subobjeto de 1^S es un $f \colon (X, A) \rightarrowtail (S, \mathrm{id}_S)$ tal que $\mathrm{id}_s \circ f = A$, por lo que $f = A$. Así pues, un subobjeto de 1^S se puede identificar con una mónica $f \colon X \rightarrowtail S$, i.e., con un subconjunto de S. Su carácter $\mathrm{ch}_f \colon 1^{\downarrow S} \longrightarrow \Omega^{\downarrow S}$ es $\langle \mathrm{ch}_X, \mathrm{id}_S \rangle$, i.e.,

$$\mathrm{ch}_f(s) = \begin{cases} (1, s) & \text{si } s \in X \\ (0, s) & \text{si } s \notin X \end{cases}$$

El conjunto de valores de verdad de $\mathbf{Set} \downarrow S$ tiene por tanto, cardinalidad 2^S.

Morfismos de verdad. Puesto que $\Omega^{\downarrow S} = (2 \times S, \mathrm{pr}_1)$, la fibra sobre un $s \in S$ es $2 \times \{s\}$, i.e., esencialmente una copia de 2, el objeto de valores de verdad de **Set**. Los morfismos de verdad en $\mathbf{Set} \downarrow S$ consisten en *copias* de los morfismos de verdad correspondientes en **Set** actuando en cada fibra.

Así, por ejemplo,

$$\neg^{\downarrow S} = \langle \neg \circ \mathrm{pr}_0, \mathrm{id}_S \rangle = \begin{cases} 2 \times S \longrightarrow 2 \times S \\ (0,s) \longmapsto (1,s) \\ (1,s) \longmapsto (0,s) \end{cases}$$

y

$$\wedge^{\downarrow S} = \langle \wedge \circ \langle \mathrm{pr}_0 \circ \mathrm{p}_0, \mathrm{pr}_0 \circ \mathrm{p}_1 \rangle, \mathrm{pr}_0 \circ \mathrm{p}_0 \rangle = \begin{cases} (2 \times S) \times_S (2 \times S) \longrightarrow 2 \times S \\ ((x,s),(y,s)) \longmapsto (x \wedge y, s) \end{cases}$$

Por su equivalencia con $\mathbf{Set}^S$, $\mathbf{Set} \downarrow S$ es un topos no degenerado si $S \neq \emptyset$, clásico y booleano, en el que existen objetos no cero pero que son vacíos (los objetos (X, A) en los que A no es una aplicación sobreyectiva) y que, por consiguiente, no está bien punteado.

La equivalencia entre las categorías $\mathbf{Set}^S$ y $\mathbf{Set} \downarrow S$ puede ser considerada también desde otra perspectiva. Ambas categorías son, junto a los functores apropiados, categorías concretas sobre **Set**.

Proposición 1.19. *Sea S un conjunto. Entonces la categoría $\mathbf{Set} \downarrow S$, junto con el functor de olvido*

$$G(f\colon (X,A) \longrightarrow (Y,B)) = f\colon X \longrightarrow Y$$

es una categoría de conjuntos con estructura.

Demostración. Sea $\mathrm{St}(X)$ el conjunto de las aplicaciones A de X en S, y $\mathrm{Ad}((X,A),(Y,B))$ el conjunto de las aplicaciones $f\colon X \longrightarrow Y$ tales que $A = B \circ f$. Entonces $(\mathrm{St}, \mathrm{Ad})$ es un constructo unívocamente transportable, y su categoría asociada es $\mathbf{Set} \downarrow S$. □

La categoría $(\mathbf{Set}^S, \coprod)$ es una categoría concreta (amnéstica y no transportable) sobre **Set**. Por otra parte, $(\mathbf{Set} \downarrow S, G)$, siendo una categoría de conjuntos con estructura, es una categoría concreta y unívocamente transportable. La equivalencia entre ambas es una equivalencia concreta. Puesto que, para cada categoría concreta, existe una categoría concreta unívocamente transportable y una equivalencia concreta hasta ella determinada salvo un isomorfismo concreto (v. [**?**], prop. 5.36), podemos concluir que $(\mathbf{Set} \downarrow S, G)$ es, salvo isomorfismo concreto, la modificación transportable de $(\mathbf{Set}^S, \coprod)$.

Now we define the concept of heterogeneous closure system on an S-sorted set.

Definición 1.20. Let A be an S-sorted set. A heterogeneous closure system, abbreviated to h-closure system, on A is a subset $\mathcal{C}$ of $\mathrm{Sub}(A)$ that satisfies the following conditions

1. $A \in \mathcal{C}$.
2. For every $\mathcal{D} \subseteq \mathcal{C}$, if $\mathcal{D} \neq \varnothing$, then $\bigcap \mathcal{D} \in \mathcal{C}$.

We denote by $\mathrm{Cls}(A)$ the set of the h-closure systems on A.

Proposición 1.21. *Let A be an S-sorted set and $\mathcal{C}$ a* h*-closure system on A. Then $\boldsymbol{\mathcal{C}} = (\mathcal{C}, \subseteq)$ is a complete lattice.*

Demostración. Let $(C^i)_{i\in I}$ be a nonempty family in $\mathcal{C}$. Then the greatest lower bound of $(C^i)_{i\in I}$ is

$$\text{ínf}_{i\in I}C^i = \bigcap_{i\in I}C^i$$

and the least upper bound of the same family is the greatest lower bound of the upper bounds of the S-unión of $(C^i)_{i\in I}$, i.e.,

$$\bigvee_{i\in I}C^i = \bigcap\{T \in \mathcal{C} \mid \bigcup_{i\in I}C^i \subseteq_S T\}$$

In this complete lattice the greatest element is A and the least element $\bigcap\mathcal{C}$. □

Proposición 1.22. *The ordered set* $\mathbf{Cls}(A) = (\mathrm{Cls}(A), \subseteq_S)$ *is a complete lattice.*

Demostración. Let $(\mathcal{C}_i)_{i\in I}$ be a nonempty family in $\mathrm{Cls}(A)$. Then greatest lower bound of $(\mathcal{C}_i)_{i\in I}$ is

$$\text{ínf}_{i\in I}\mathcal{C}_i = \bigcap_{i\in I}\mathcal{C}_i$$

and the least upper bound of the same family is

$$\bigvee_{i\in I}\mathcal{C}_i = \bigcap\{\mathcal{C} \in \mathrm{Cls}(A) \mid \bigcup_{i\in I}\mathcal{C}_i \subseteq \mathcal{C}\}$$

In this complete lattice the greatest element is $\mathrm{Sub}(A)$ and the least element $\{A\}$. □

Definición 1.23. A heterogeneous closure operator, abreviated to h-closure operator, on an S-sorted set A is an operator J on $\mathrm{Sub}(A)$ such that, for every $X, Y \subseteq A$, satisfies:

1. $X \subseteq J(X)$, i.e., J is extensive.
2. If $X \subseteq Y$, then $J(X) \subseteq J(Y)$, i.e., J is isotone.
3. $J(J(X)) = J(X)$, i.e., J is idempotent.

We denote by $\mathrm{Clop}(A)$ the set of the h-closure operators on A and by $\mathbf{Clop}(A)$ the same set but ordered by the relation $\leq$, where, for J and K in $\mathrm{Clop}(A)$, we have that $J \leq K$ if, for every $X \subseteq_S A$, $J(X) \subseteq_S K(X)$. Moreover, we call the fixed points of a h-closure operator J on A, J-closed sets.

La proposición que sigue, así como la observación subsiguiente, serán de utilidad cuando tratemos de extensión de las teorías de Post & Cia.

Proposición 1.24. *Let A be an S-sorted set y J un operador clausura sobre A. Entonces, para cada familia $(X^i)_{i\in I}$ de partes de A, se cumple que*

$$J(\bigcup_{i\in I}X^i) = J(\bigcup_{i\in I}J(X^i)).$$

Además, $J(X \cup Y) = J(X \cup J(Y)) = J(J(X) \cup Y) = J(J(X) \cup J(Y))$.

En el caso heterogéneo, lo mismo que en el homogéneo, para dos partes X, Y de A, si $J(X) \subseteq J(Y)$, entonces $J(X \cup Z) \subseteq J(Y \cup Z)$, para cualquier parte Z de A. Pero observemos que, en el caso heterogéneo, puede existir una parte no vacía y estricta T del conjunto de los tipos S y dos partes X, Y de A, de modo que, para cada $t \in T$, $J(X)_t \subseteq J(Y)_t$, y, a su vez, exista una parte Z de A y un $t \in T$ tal que $J(X \cup Z)_t \nsubseteq J(Y \cup Z)_t$; del mismo modo, puede existir una parte no vacía y estricta T del conjunto de los tipos S y dos partes X, Y de A, tales que, para cada $t \in T$, $J(X)_t = J(Y)_t$, y, a su vez, exista una parte Z de A y un $t \in T$ tal que $J(X \cup Z)_t \neq J(Y \cup Z)_t$.

Proposición 1.25. *The ordered set* $\mathbf{Clop}(A)$ *is a complete lattice.*

Demostración. Let $(J^i)_{i\in I}$ be a nonempty family in $\mathrm{Clop}(A)$. Then the greatest lower bound of $(J^i)_{i\in I}$, $\mathrm{ínf}_{i\in I}\, J^i$, is defined, for every $X \subseteq_S A$, as

$$\mathrm{ínf}_{i\in I} J^i(X) = \bigcap_{i\in I} J^i(X)$$

and the least upper bound of the same family, $\bigvee_{i\in I} J^i$, is

$$\bigvee_{i\in I} J^i = \mathrm{ínf}\left\{J \in \mathrm{Clop}(A) \mid \forall i \in I\,(\, J^i \leq J\,)\right\}$$

The greatest element is the totally inconsistent h-closure operator, κ_A, that, to every $X \subseteq A$, assigns A, and the least the identity on $\mathrm{Sub}(A)$. □

Proposición 1.26. *Let* A *be an* S*-sorted set. Then there exists an anti-isomorphism* Fix *from the ordered set* $\mathbf{Clop}(A)$*, of the* h*-closure operators on* A*, into the ordered set* $\mathbf{Cls}(A)$*, of the* h*-closure systems on* A*.*

Demostración. Veamos, en primer lugar, que si J es un operador clausura heterogéneo, entonces, siendo $\mathrm{Fix}(J) = \{X \subseteq_S A \mid J(X) = X\}$, el conjunto $\mathcal{C}^J = \mathrm{Fix}(J)$ es un sistema de clausura heterogéneo. En efecto, si $(J(X^i))_{i\in I}$ es una familia no vacía en $\mathcal{C}^J$, entonces tenemos que, para cada $i \in I$, se cumple que

$$\bigcap_{i\in I} J(X^i) \subseteq J(X^i)$$

y, por ser $\mathcal{C}^J$ isótono e idempotente,

$$J(\bigcap_{i\in I} J(X^i)) \subseteq J(X^i).$$

Entonces

$$J(\bigcap_{i\in I} J(X^i)) = \bigcap_{i\in I} J(X^i)$$

puesto que J es idempotente, y $\bigcap_{i\in I} J(X^i)$ es un punto fijo de J y, por tanto, pertenece a $\mathcal{C}^J$. Como $J(A) = A$, $\mathrm{Fix}(J)$ es un sistema de clausura.

Por otra parte, si $\mathcal{C}$ es un sistema de clausura heterogéneo, entonces la aplicación $J^{\mathcal{C}}$, definida como:

$$J^{\mathcal{C}} \begin{cases} \mathrm{Sub}(A) \longrightarrow \mathrm{Sub}(A) \\ X \longmapsto \bigcap\{Y \in \mathcal{C} \mid X \subseteq Y\}, \end{cases}$$

es un operador clausura heterogéneo. En efecto, el operador $J^{\mathcal{C}}$ es extensivo, ya que

$$X \subseteq \bigcap\{Y \subseteq A \mid Y \supseteq X\} \subseteq \bigcap\{Y \subseteq \mathcal{C} \mid Y \supseteq X\} = J^{\mathcal{C}}(X),$$

el operador $J^{\mathcal{C}}$ es isótono, ya que si $X \subseteq_S Y$, entonces $\{T \in \mathcal{C} \mid X \subseteq_S T\}$ contiene a $\{T \in \mathcal{C} \mid Y \subseteq_S T\}$, luego $\bigcap\{T \in \mathcal{C} \mid X \subseteq_S T\} \subseteq \bigcap\{T \in \mathcal{C} \mid Y \subseteq_S T\}$, por lo tanto $J^{\mathcal{C}}(X) \subseteq_S J^{\mathcal{C}}(Y)$.

Por último, $J^{\mathcal{C}}$ es idempotente, debido a que por estar $\{T \in \mathcal{C} \mid X \subseteq_S T\}$ incluido en $\{T \in \mathcal{C} \mid J^{\mathcal{C}}(X) \subseteq_S T\}$, se cumple que $\bigcap\{T \in \mathcal{C} \mid X \subseteq_S T\}$ contiene a $\bigcap\{T \in \mathcal{C} \mid J^{\mathcal{C}}(X) \subseteq_S T\}$, luego $J^{\mathcal{C}}(X) = J^{\mathcal{C}}(J^{\mathcal{C}}(X))$.

Las aplicaciones $J \mapsto \mathcal{C}^J$ y $\mathcal{C} \mapsto \mathcal{C}^J$ son inversas una de la otra, y, por tanto, son aplicaciones biyectivas.

Queda por demostrar que las biyecciones son antihomomorfismos, i.e., que invierten el orden. Supongamos que $\mathcal{C} \subseteq \mathcal{D}$. Entonces

$$J^{\mathcal{C}}(X) = \bigcap\{T \in \mathcal{C} \mid T \supseteq X\} \supseteq \bigcap\{T \in \mathcal{D} \mid T \supseteq X\} = J^{\mathcal{D}}(X)$$

luego $J^{\mathcal{C}} \geq J^{\mathcal{D}}$. Supongamos ahora que $J \leq K$. Entonces si $T \in \mathcal{C}_K$, se tiene que $T = K(X)$, para algún $X \subseteq B$. Pero

$$JK(X) \subseteq KK(X) = K(X)$$

luego $T \in \mathcal{C}^J$. □

Comentario. Si $t \in S$ y $a, b \in A_t$, entonces $J(\delta^{t,a}) = J(\delta^{t,b})$ si y sólo si $J(\delta^{t,a})_t = J(\delta^{t,b})_t$. Es evidente que $J(\delta^{t,a}) = J(\delta^{t,b})$ es una condición suficiente para que $J(\delta^{t,a})_t = J(\delta^{t,b})_t$.

Por otra parte, si $J(\delta^{t,a})_t = J(\delta^{t,b})_t$, entonces $J(\delta^{t,a}) = J(\delta^{t,b})$. En efecto, por ser $J(\delta^{t,b})$ el mínimo cerrado que contiene a $\delta^{t,b}$, es suficiente que se demuestre que $J(\delta^{t,a})$ contiene a $\delta^{t,b}$, pero, para $s = t$, eso se cumple por la hipótesis, y, para $s \neq t$, es evidente. Del mismo modo se demuestra la inclusión inversa.

Proposición 1.27. *Sea A un S-conjunto, $J \in \mathrm{Clop}(A)$ y $(X^i)_{i\in I}$ una familia en $\mathrm{Sub}(A)$. Entonces*

$$\textstyle\bigvee_{i\in I}^{\mathrm{Fix}(J)} J(X^i) = J(\bigcup_{i\in I} X^i)$$

Demostración. Si $T \in \mathrm{Fix}(J)$ entonces T contiene a $\bigcup_{i\in I} X^i$ exactamente si T contiene a $\bigcup_{i\in I} J(X^i)$, puesto que para cada cerrado T se tiene que $T \supseteq X$ si y sólo si $T \supseteq J(X)$. Entonces

$$\begin{aligned} J(\textstyle\bigcup_{i\in I} X^i) &= \textstyle\bigcap\{T \in \mathcal{C}^J \mid T \supseteq \bigcup_{i\in I} X^i\} \\ &= \textstyle\bigcap\{T \in \mathcal{C}^J \mid T \supseteq \bigcup_{i\in I} J(X^i)\} \\ &= \textstyle\bigvee_{i\in I}^{\mathcal{C}^J} J(X^i) \end{aligned}$$

□

Para cada conjunto de tipos S, existe una categoría de S-espacios de clausura, cuyos objetos están formados por un S-conjunto y, alternativa pero equivalentemente, un sistema de clausura heterogéneo o un operador clausura heterogéneo, y cuyos morfismos son las S-aplicaciones compatibles con los espacios de clausura respectivos.

Proposición 1.28. *Sea S un conjunto de tipos. Entonces* $\mathbf{ClSp}(S)$*, es la categoría cuyos objetos son pares $(A, \mathcal{C})$, en los que A un S-conjunto y $\mathcal{C} \in \mathrm{Cls}(A)$, y cuyos morfismos de $(A, \mathcal{C})$ en $(B, \mathcal{D})$ son los triplos $((A, \mathcal{C}), f, (B, \mathcal{D}))$, denotados como $f\colon (A, \mathcal{C}) \longrightarrow (B, \mathcal{D})$, en los que f es una S-aplicación de A en B tal que, para cada $D \in \mathcal{D}$, $f^{-1}[D] \in \mathcal{C}$, y con composición e identidades definidas a partir de las de sus S-aplicaciones subyacentes.*

De $\mathbf{ClSp}(S)$ *en* $\mathbf{Set}^S$ *se tiene un functor de olvido,* $G_{\mathbf{ClSp}(S)}$*, definido como:*

$$\begin{array}{ccc} \mathbf{ClSp}(S) & \xrightarrow{G_{\mathbf{ClSp}(S)}} & \mathbf{Set}^S \\ (A,\mathcal{C}) & & A \\ \Big\downarrow f & \longmapsto & \Big\downarrow f \\ (B,\mathcal{D}) & & B \end{array}$$

que es obviamente fiel, por lo que $\mathbf{ClSp}(S)$ *es una categoría concreta sobre* $\mathbf{Set}^S$*.*

Proposición 1.29. *Sea* S *un conjunto de tipos. Entonces* $\mathbf{Clop}(S)$*, es la categoría cuyos objetos son pares* (A,J)*, en los que* A *un* S*-conjunto y* $J \in \mathrm{Clop}(A)$*, y cuyos morfismos de* (A,J) *en* (B,K) *son los triplos* $((A,J),f,(B,K))$*, denotados como* $f\colon (A,J) \longrightarrow (B,K)$*, en los que* f *es una* S*-aplicación de* A *en* B *tal que, para todo* $X \subseteq A$*,* $f[J(X)] \subseteq_S K(f[X])$*, y con composición e identidades definidas a partir de las de sus* S*-aplicaciones subyacentes.*

De $\mathbf{Clop}(S)$ *en* $\mathbf{Set}^S$ *se tiene un functor de olvido* $G_{\mathbf{Clop}(S)}$*, definido similarmente a* $G_{\mathbf{ClSp}(S)}$*, por lo que* $\mathbf{Clop}(S)$ *es también una categoría concreta sobre* $\mathbf{Set}^S$*.*

Proposición 1.30. *Las categorías* $\mathbf{ClSp}(S)$ *y* $\mathbf{Clop}(S)$ *son concretamente isomorfas, a través del functor definido como:*

$$\begin{array}{ccc} \mathbf{Clop}(S) & \longrightarrow & \mathbf{ClSp}(S) \\ (A,J) & & (A,\mathrm{Fix}(J)) \\ \Big\downarrow f & \longmapsto & \Big\downarrow f \\ (B,K) & & (B,\mathrm{Fix}(K)) \end{array}$$

Este resultado justifica que, en lo que sigue, se use aquella de las dos categorías, $\mathbf{Clop}(S)$, o $\mathbf{ClSp}(S)$, que se considere más oportuna para abordar la situación de que se trate. Convenimos que por la categoría de S-espacios de clausura, $\mathbf{ClSp}(S)$, nos referimos indistintamente a cualquiera de las dos categorías $\mathbf{Clop}(S)$, o $\mathbf{ClSp}(S)$.

Cada espacio de clausura ordinario se identifica con un S-espacio de clausura heterogéneo, tomando como conjunto de tipos S cualquier conjunto final.

Podemos inducir un sistema de clausura heterogéneo, de manera optimal, sobre el dominio común de una familia de S-aplicaciones cuando los codominios de las mismas están dotados de sistemas de clausura heterogéneos, y, dualmente, podemos inducir un sistema de clausura heterogéneo, de manera co-optimal, sobre el codominio común de una familia de S-aplicaciones cuando los dominios de las mismas están dotados de sistemas de clausura heterogéneos.

Lema 1.31. *Sea A un S-conjunto, $(A^i,\mathcal{C}^i)_{i\in I}$ una familia de S-espacios de clausura y $f^{\cdot}=(f^i)_{i\in I}$ una familia de S-aplicaciones, en la que, para cada $i\in I$, $f^i\colon A\longrightarrow A^i$. Entonces hay un único sistema de clausura heterogéneo $\mathcal{C}$ sobre A, al que denotamos por $L^{f^{\cdot}}(A^i,\mathcal{C}^i)_{i\in I}$, y denominamos el levantamiento optimal de $(A^i,\mathcal{C}^i)_{i\in I}$ a través de $f^{\cdot}$, tal que:*

1. *Para cada $i\in I$, $f^i\colon (A,L^f(A^i,\mathcal{C}^i)_{i\in I})\longrightarrow(A^i,\mathcal{C}^i)$.*
2. *Dado un S-espacio de clausura $(B,\mathcal{B})$ y $g\colon B\longrightarrow A$, si, para cada $i\in I$, $f^i\circ g\colon (B,\mathcal{B})\longrightarrow(A^i,\mathcal{C}^i)$, entonces $g\colon (B,\mathcal{B})\longrightarrow(A,L^{f^{\cdot}}(A^i,\mathcal{C}^i)_{i\in I})$.*

Además, se cumple que:

1. *Para cada sistema de clausura heterogéneo $\mathcal{C}$ sobre A:*
$$L^{\mathrm{id}_A}(A,\mathcal{C})=\mathcal{C}.$$
2. *Si, para cada $i\in I$, $(A^{i,m},\mathcal{C}^{i,m})_{m\in \mathrm{M}_i}$ es una familia de S-espacios de clausura, $g^{i,\cdot}=(g^{i,m})_{m\in\mathrm{M}_i}$ una familia de S-aplicaciones, en la que, para cada $m\in\mathrm{M}_i$, $g^{i,m}\colon A^i\longrightarrow A^{i,m}$ y $\mathcal{C}^i=L^{g^{i,\cdot}}(A^{i,m},\mathcal{C}^{i,m})_{m\in\mathrm{M}_i}$, entonces*
$$L^{(g^{i,\cdot}\circ f^{\cdot})_{i\in I}}(A^{i,m},\mathcal{C}^{i,m})_{(i,m)\in\coprod_{i\in I}\mathrm{M}_i}=L^{f^{\cdot}}(A^i,\mathcal{C}^i)_{i\in I}.$$

Demostración. Es suficiente que tomemos como $\mathrm{L}^{f^{\cdot}}(A^i,\mathcal{C}^i)_{i\in I}$ el sistema de clausura heterogéneo sobre A generado por $\bigcup_{i\in I}\{\,(f^i)^{-1}[C]\mid C\in\mathcal{C}^i\,\}$. □

Obsérvese que, para cada S-conjunto A, el levantamiento optimal de $(A^i,\mathcal{C}^i)_{i\in\emptyset}$ a través de $f^{\cdot}=(f^i)_{i\in\emptyset}$ es $\{A\}$.

Definición 1.32. Sea $f\colon(A,\mathcal{C})\longrightarrow(B,\mathcal{D})$ un morfismo de S-espacios de clausura. Decimos que f es un morfismo optimal si, para cada S-espacio de clausura $(C,\mathcal{E})$ y cada aplicación $g\colon C\longrightarrow A$, si $f\circ g\colon(C,\mathcal{E})\longrightarrow(B,\mathcal{D})$, entonces $g\colon(C,\mathcal{E})\longrightarrow(A,\mathcal{C})$.

Proposición 1.33. *Sea $f\colon(A,\mathcal{C})\longrightarrow(B,\mathcal{D})$ un morfismo de S-espacios de clausura. Una condición necesaria y suficiente para que f sea un morfismo optimal es que $\mathcal{C}=L^f(B,\mathcal{D})$.*

Proposición 1.34. *Si $f\colon(A,\mathcal{C})\longrightarrow(B,\mathcal{D})$ y $g\colon(B,\mathcal{D})\longrightarrow(C,\mathcal{E})$ son morfismos optimales, entonces $g\circ f\colon(A,\mathcal{C})\longrightarrow(C,\mathcal{E})$ es un morfismo optimal. Además, si $g\circ f\colon(A,\mathcal{C})\longrightarrow(C,\mathcal{E})$ es un morfismo optimal, entonces se cumple que $f\colon(A,\mathcal{C})\longrightarrow(B,\mathcal{D})$ es optimal.*

Lema 1.35. *Sea A un S-conjunto, $(A^i,\mathcal{C}^i)_{i\in I}$ una familia de S-espacios de clausura heterogéneos y $f^{\cdot}=(f^i)_{i\in I}$ una familia de S-aplicaciones, en la que, para cada $i\in I$, $f^i\colon A^i\longrightarrow A$. Entonces hay un único sistema de clausura heterogéneo $\mathcal{C}$ sobre A, al que denotamos por $L_{f^{\cdot}}(A^i,\mathcal{C}^i)_{i\in I}$, y denominamos el levantamiento co-optimal de $(A^i,\mathcal{C}^i)_{i\in I}$ a través de $f^{\cdot}$, tal que:*

1. *Para cada $i\in I$, $f^i\colon(A^i,\mathcal{C}^i)\longrightarrow(A,L_{f^{\cdot}}(A^i,\mathcal{C}^i)_{i\in I})$.*
2. *Dado un S-espacio de clausura $(B,\mathcal{D})$ y $g\colon A\longrightarrow B$, si, para cada $i\in I$, $g\circ f^i\colon(A^i,\mathcal{C}^i)\longrightarrow(B,\mathcal{D})$, entonces $g\colon(A,L_{f^{\cdot}}(A^i,\mathcal{C}^i)_{i\in I})\longrightarrow(B,\mathcal{D})$.*

Además, se cumple que:

1. *Para cada sistema de clausura heterogéneo $\mathcal{C}$ en A:*
$$L_{\mathrm{id}_A}(A,\mathcal{C})=\mathcal{C}.$$

2. *Si, para cada* $i \in I$, $(A^{i,m}, \mathcal{C}^{i,m})_{m\in \mathrm{M}_i}$ *es una familia de* S*-espacios de clausura,* $g^{i,\cdot} = (g^{i,m})_{m\in \mathrm{M}_i}$ *una familia de* S*-aplicaciones, en la que, para cada* $m \in \mathrm{M}_i$, $g^{i,m}\colon A^{i,m} \longrightarrow A^i$ *y* $\mathcal{C}^i = L_{g^i}(A^{i,m}, \mathcal{C}^{i,m})_{m\in \mathrm{M}_i}$, *entonces*

$$L_{(f^\cdot \circ g^{i,\cdot})_{i\in I}}(A^{i,m}, \mathcal{C}^{i,m})_{(i,m)\in \coprod_{i\in I} \mathrm{M}_i} = L_{f^\cdot}(A^i, \mathcal{C}^i)_{i\in I}.$$

Demostración. Es suficiente que tomemos como $\mathrm{L}_{f^\cdot}(A^i, \mathcal{C}^i)_{i\in I}$ el subconjunto de $\mathrm{Sub}(A)$ definido como:

$$\mathrm{L}_{f^\cdot}(A^i, \mathcal{C}^i)_{i\in I} = \{\, C \subseteq A \mid \forall i \in I\, (\, (f^i)^{-1}[C] \in \mathcal{C}^i\,)\,\}.$$

□

Para cada S-conjunto A, el levantamiento co-optimal de $(A^i, \mathcal{C}^i)_{i\in\emptyset}$ a través de $f^\cdot = (f^i)_{i\in\emptyset}$ es $\mathrm{Sub}(A)$.

Corolario 1.36. *El functor de olvido de la categoría* $\mathbf{ClSp}(S)$ *en la categoría* $\mathbf{Set}^S$ *has left and right adjoints.*

Corolario 1.37. *El functor de olvido de la categoría* $\mathbf{ClSp}(S)$ *en la categoría* $\mathbf{Set}^S$ *constucts limits and colimits.*

Definición 1.38. Sea $f\colon (A, \mathcal{C}) \longrightarrow (B, \mathcal{D})$ un morfismo de S-espacios de clausura. Decimos que f es un morfismo co-optimal si, para cada S-espacio de clausura $(C, \mathcal{E})$ y cada aplicación $g\colon B \longrightarrow C$, si $g \circ f\colon (A, \mathcal{C}) \longrightarrow (C, \mathcal{E})$, entonces $g\colon (B, \mathcal{D}) \longrightarrow (C, \mathcal{E})$.

Proposición 1.39. *Sea* $f\colon (A, \mathcal{C}) \longrightarrow (B, \mathcal{D})$ *un morfismo de* S*-espacios de clausura. Una condición necesaria y suficiente para que* f *sea un morfismo co-optimal es que* $\mathcal{D} = L_f(A, \mathcal{C})$.

Proposición 1.40. *Si* $f\colon (A, \mathcal{C}) \longrightarrow (B, \mathcal{D})$ *y* $g\colon (B, \mathcal{D}) \longrightarrow (C, \mathcal{E})$ *son morfismos co-optimales, entonces* $g \circ f\colon (A, \mathcal{C}) \longrightarrow (C, \mathcal{E})$ *es un morfismo co-optimal. Además, si* $g \circ f\colon (A, \mathcal{C}) \longrightarrow (C, \mathcal{E})$ *es un morfismo co-optimal, entonces* $g\colon (B, \mathcal{D}) \longrightarrow (C, \mathcal{E})$ *es co-optimal.*

1.2. S-Signaturas y $\mathbf{\Sigma}$-álgebras heterogéneas.

Definición 1.41. Sea S un conjunto de tipos. Una S-signatura algebraica Σ es un $S^\star \times S$-conjunto $\Sigma = (\Sigma_{w,s})_{(w,s)\in S^\star\times S}$ tal que $\Sigma_{w,s}$ y $\Sigma_{w',s'}$ son disjuntos si $(w, s) \neq (w', s')$.

Si Σ es una S-signatura algebraica y $\sigma \in \Sigma_{w,s}$, para algún par $(w, s) \in S^\star \times S$, entonces decimos que σ es un símbolo de operación de biariedad (w, s) y a las expresiones $\sigma\colon w \longrightarrow s$ y $\sigma \in \Sigma_{w,s}$ las consideramos sinónimas. Además, para cada $w \in S^\star$, a los símbolos de operación pertenecientes al conjunto $\bigcup_{s\in S} \Sigma_{w,s}$, denotado por $\Sigma_{w,\cdot}$, los denominamos símbolos de operación de ariedad w, y, para cada $s \in S$, a los pertenecientes al conjunto $\bigcup_{w\in S^\star} \Sigma_{w,s}$, denotado por $\Sigma_{\cdot,s}$, los denominamos símbolos de operación de coariedad s.

Definición 1.42. Sea $A = (A_s)_{s\in S}$ un S-conjunto y $\mathbf{\Sigma}$ una S-signatura algebraica. Una $\mathbf{\Sigma}$-estructura algebraica F sobre A es una $S^\star \times S$-aplicación de Σ en $\mathrm{Op}^{S^\star\times S}(A) = (\mathbf{Set}(A_w, A_s))_{(w,s)\in S^\star\times S}$. Una $\mathbf{\Sigma}$-álgebra es un par $\mathbf{A} = (A, F)$, en el que A es un S-conjunto y F una $\mathbf{\Sigma}$-estructura algebraica sobre A.

En algunas ocasiones, denotamos a la $\mathbf{\Sigma}$-estructura de una $\mathbf{\Sigma}$-álgebra $\mathbf{A}$ por $F^{\mathbf{A}}$, y a las operaciones que la componen por $F^{\mathbf{A}}_{\sigma}$. Cuando $\sigma\colon \lambda \longrightarrow s$, denotamos mediante $\sigma^{\mathbf{A}}$ al valor de $F^{\mathbf{A}}_{\sigma}\colon 1 \longrightarrow A_s$ para el único miembro de 1.

Definición 1.43.

- Sean $\mathbf{A} = (A, F^{\mathbf{A}})$ y $\mathbf{B} = (B, F^{\mathbf{B}})$ dos $\mathbf{\Sigma}$-álgebras. Un $\mathbf{\Sigma}$-homomorfismo o, simplemente, un homomorfismo, de $\mathbf{A}$ en $\mathbf{B}$ es un triplo ordenado $(\mathbf{A}, f, \mathbf{B})$, denotado por $f\colon \mathbf{A} \longrightarrow \mathbf{B}$, en el que f es una S-aplicación de A en B, tal que para cada $\sigma \in \Sigma$, con $\sigma\colon w \longrightarrow s$, el diagrama

$$\begin{array}{ccc} A_w & \xrightarrow{\quad f_w \quad} & B_w \\ {\scriptstyle F^{\mathbf{A}}_{\sigma}}\downarrow & & \downarrow{\scriptstyle F^{\mathbf{B}}_{\sigma}} \\ A_s & \xrightarrow[\quad f_s \quad]{} & B_s \end{array}$$

  conmuta, i.e., para cada $x \in A_w$, se cumple que

$$f_s(F^{\mathbf{A}}_{\sigma}(x)) = F^{\mathbf{B}}_{\sigma}(f_w(x)).$$

- Sean $f\colon \mathbf{A} \longrightarrow \mathbf{B}$ y $g\colon \mathbf{B} \longrightarrow \mathbf{C}$ dos homomorfismos. Su composición, $g \circ f$, es el triplo $(\mathbf{A}, g \circ f, \mathbf{C})$. Para una $\mathbf{\Sigma}$-álgebra $\mathbf{A}$, el morfismo identidad, $\mathrm{id}_{\mathbf{A}}$, es $(\mathbf{A}, \mathrm{id}_A, \mathbf{A})$, siendo id_A la S-aplicación identidad para A.

A continuación, mostramos algunos ejemplos de álgebras heterogéneas que son de uso frecuente en las matemáticas, aunque, por lo general, con una de las componentes del conjunto heterogéneo subyacente mantenida fija.

Si tomamos como conjunto de tipos S el conjunto $\{\mathsf{e}, \mathsf{v}\}$, en el que e se realizará como un conjunto de escalares, el conjunto subyacente de un anillo, y v como un conjunto de vectores, el conjunto subyacente de un grupo abeliano, como S-signatura la definida como

$$\begin{aligned} \Sigma_{(\mathsf{e},\mathsf{e}),\mathsf{e}} &= \{+_{\mathsf{e}}, \cdot_{\mathsf{e}}\} & \Sigma_{(\mathsf{v},\mathsf{v}),\mathsf{v}} &= \{+_{\mathsf{v}}\} \\ \Sigma_{(\mathsf{e}),\mathsf{e}} &= \{-_{\mathsf{e}}\} & \Sigma_{(\mathsf{v}),\mathsf{v}} &= \{-_{\mathsf{v}}\} \\ \Sigma_{(\lambda),\mathsf{e}} &= \{0_{\mathsf{e}}, 1_{\mathsf{e}}\} & \Sigma_{(\lambda),\mathsf{v}} &= \{0_{\mathsf{v}}\} \\ \Sigma_{(\mathsf{e},\mathsf{v}),\mathsf{v}} &= \{\cdot\} \end{aligned}$$

en la que $+_{\mathsf{e}}, \cdot_{\mathsf{e}}, -_{\mathsf{e}}, 0_{\mathsf{e}}$ y 1_{e} se realizarán como las operaciones estructurales del anillo que se considere, $+_{\mathsf{v}}, -_{\mathsf{v}}$ y 0_{v} como las operaciones estructurales del grupo abeliano que se considere y $\cdot$ como la acción por la izquierda de los escalares sobre los vectores, entonces, por cada anillo $\mathbf{R}$ y cada $\mathbf{R}$-módulo por la izquierda $\mathbf{M}$ obtenemos un álgebra heterogénea, llamado en este caso un módulo. Observemos que los morfismos de un módulo $(\mathbf{R}, \mathbf{M}, \cdot)$ en otro $(\mathbf{R}', \mathbf{M}', \cdot')$ son pares de morfismos, un homomorfismo de anillos $f\colon \mathbf{R} \longrightarrow \mathbf{R}'$ y uno de grupos abelianos $g\colon \mathbf{M} \longrightarrow \mathbf{M}'$, tales que, para cada $r \in R$ y cada $x \in M$, $g(r \cdot x) = f(r) \cdot' g(x)$.

Otros ejemplos de álgebras heterogéneas vienen dados por la noción de autómata, la de $\mathbf{G}$-conjunto, siendo $\mathbf{G}$ un grupo, la de $\mathbf{M}$-conjunto, siendo $\mathbf{M}$ un monoide, la de $\mathbf{K}$-álgebra lineal, con $\mathbf{K}$ un anillo, y, en general, por

cualquier constructo matemático en el que exista, al menos, una acción de un sistema algebraico sobre otro.

Dado un anillo $\mathbf{R}$, también se pueden interpretar los complejos de cadenas de $\mathbf{R}$-módulos por la izquierda, i.e., los pares $((\mathbf{M}_n)_{n\in\mathbb{Z}}, (d_n)_{n\in\mathbb{Z}})$ en los que, para cada $n \in \mathbb{Z}$, $\mathbf{M}_n$ es un $\mathbf{R}$-módulo por la izquierda, y d_{n+1} un morfismo de $\mathbf{R}$-módulos de $\mathbf{M}_{n+1}$ en $\mathbf{M}_n$ tal que $d_n \circ d_{n+1} = 0$, como álgebras heterogéneas para el conjunto de tipos $\mathbb{Z}$ y la $\mathbb{Z}$-signatura algebraica adecuada, y los morfismos de complejos de cadenas de $\mathbf{R}$-módulos por la izquierda como homomorfismos de álgebras heterogéneas. Recordemos que un morfismo de $((\mathbf{M}_n)_{n\in\mathbb{Z}}, (d_n)_{n\in\mathbb{Z}})$ en $((\mathbf{M}'_n)_{n\in\mathbb{Z}}, (d'_n)_{n\in\mathbb{Z}})$ es una $\mathbb{Z}$-familia, $(f_n)_{n\in\mathbb{Z}}$ en la que, para cada $n \in \mathbb{Z}$, f_n es un homomorfismo de $\mathbf{M}_n$ en $\mathbf{M}'_n$ tal que el diagrama:

$$\begin{array}{ccc} \mathbf{M}_{n+1} & \xrightarrow{d_{n+1}} & \mathbf{M}_n \\ \Big\downarrow{\scriptstyle f_{n+1}} & & \Big\downarrow{\scriptstyle f_n} \\ \mathbf{M}'_{n+1} & \xrightarrow[d'_{n+1}]{} & \mathbf{M}'_n \end{array}$$

conmuta.

Proposición 1.44. *Sea $\mathbf{\Sigma}$ una S-signatura algebraica. Las $\mathbf{\Sigma}$-álgebras y los homomorfismos entre ellas forman una categoría, $\mathbf{Alg}(\mathbf{\Sigma})$.*

Al conjunto de los homomorfismos de $\mathbf{A}$ en $\mathbf{B}$ lo denotamos por $\mathrm{Hom}_{\mathbf{\Sigma}}(\mathbf{A}, \mathbf{B})$. Un homomorfismo $f\colon \mathbf{A} \longrightarrow \mathbf{A}$ con el mismo dominio y codominio recibe el nombre de endomorfismo de $\mathbf{A}$, y al monoide de los endomorfismos de $\mathbf{A}$ lo denotamos por $\mathbf{End}_{\mathbf{\Sigma}}(\mathbf{A})$. Un endomorfismo de $\mathbf{A}$ cuya S-aplicación subyacente sea una biyección recibe el nombre de automorfismo y al grupo de los automorfismos de $\mathbf{A}$ lo denotamos por $\mathbf{Aut}_{\mathbf{\Sigma}}(\mathbf{A})$. Los homomorfismos inyectivos (resp., sobreyectivos, biyectivos) entre $\mathbf{\Sigma}$-álgebras son aquellos cuya S-aplicación subyacente es inyectiva (resp., sobreyectiva, biyectiva). Por último, si hay un $\mathbf{\Sigma}$-homomorfismo sobreyectivo de $\mathbf{A}$ en $\mathbf{B}$, diremos que $\mathbf{B}$ es una imagen homomorfa de $\mathbf{A}$.

1.3. Subálgebras heterogéneas.

Los S-subconjuntos del S-conjunto subyacente de un álgebra heterogénea que están cerrados respecto de las operaciones estructurales del álgebra constituyen un sistema de clausura algebraico, lo mismo que en el caso ordinario u homogéneo. Estudiamos a continuación la noción de parte cerrada o subálgebra de un álgebra heterogénea.

En lo que sigue, $\mathbf{\Sigma}$ es una S-signatura algebraica heterogénea arbitraria pero fija.

Definición 1.45. Sea $\mathbf{A} = (A, F^{\mathbf{A}})$ una $\mathbf{\Sigma}$-álgebras y X un S-subconjunto de A, i.e., X es un S-conjunto tal que, para cada $s \in S$, $X_s \subseteq A_s$.

1. Si $\sigma \in \Sigma$, con $\sigma\colon w \longrightarrow s$, decimos de X que está *cerrado bajo la operación* $F^{\mathbf{A}}_{\sigma}\colon A_w \longrightarrow A_s$ si, para cada $a \in X_w$, $F^{\mathbf{A}}_{\sigma}(a) \in X_s$, i.e., si $F^{\mathbf{A}}_{\sigma}[X_w] \subseteq X_s$.

2. Decimos que X es un *cerrado* o una *subálgebra* de $\mathbf{A}$ si, para cada $\sigma \in \Sigma$ con $\sigma\colon w \longrightarrow s$, y cada $a \in X_w$, $F_\sigma^{\mathbf{A}}(a) \in X_s$, i.e., si X está cerrado bajo cada una de las operaciones estructurales de $\mathbf{A}$. Al conjunto de los cerrados de $\mathbf{A}$ lo denotamos por $\mathrm{Cl}(\mathbf{A})$.

Proposición 1.46. *Sea* $\mathbf{A}$ *una* $\mathbf{\Sigma}$*-álgebra. Entonces el conjunto de los cerrados de* $\mathbf{A}$, $\mathrm{Cl}(\mathbf{A})$, *es un sistema de clausura algebraico sobre* A, *i.e., tiene las siguientes propiedades:*

1. $A \in \mathrm{Cl}(\mathbf{A})$.
2. *Si* $\mathcal{X} \subseteq \mathrm{Cl}(\mathbf{A})$ *y* $\mathcal{X} \neq \varnothing$, *entonces* $\bigcap_{X\in\mathcal{X}} X \in \mathrm{Cl}(\mathbf{A})$.
3. *Si* $\mathcal{X} \subseteq \mathrm{Cl}(\mathbf{A})$, $\mathcal{X} \neq \varnothing$ *y si dados* $X, Y \in \mathcal{X}$, *hay un* $Z \in \mathcal{X}$ *tal que* $X \cup Y \subseteq_S Z$, *entonces* $\bigcup_{X\in\mathcal{X}} X \in \mathrm{Cl}(\mathbf{A})$.

Demostración. □

Corolario 1.47. *Sea* $\mathbf{A}$ *una* $\mathbf{\Sigma}$*-álgebra heterogénea. Entonces la endoaplicación* $\mathrm{Sg}_{\mathbf{A}}$ *del conjunto* $\mathrm{Sub}_S(A)$, *de los* S*-subconjuntos de* A, *definida como:*

$$\mathrm{Sg}_{\mathbf{A}} \begin{cases} \mathrm{Sub}_S(A) \longrightarrow \mathrm{Sub}_S(A) \\ X \longmapsto \bigcap\{\, C \in \mathrm{Cl}(\mathbf{A}) \mid X \subseteq_S C \,\} \end{cases}$$

tiene las siguientes propiedades:

1. $\mathrm{Im}(\mathrm{Sg}_{\mathbf{A}}) \subseteq \mathrm{Cl}(\mathbf{A})$.
2. $\{\, X \in \mathrm{Sub}(A) \mid X = \mathrm{Sg}_{\mathbf{A}}(X) \,\} = \mathrm{Cl}(\mathbf{A})$.
3. $\mathrm{Sg}_{\mathbf{A}}$ *es extensiva o inflacionaria, i.e., para cada* $X \in \mathrm{Sub}_S(A)$, $X \subseteq_S \mathrm{Sg}_{\mathbf{A}}(X)$.
4. $\mathrm{Sg}_{\mathbf{A}}$ *es isótona, i.e., para cada* $X, Y \in \mathrm{Sub}_S(A)$, *si* $X \subseteq_S Y$, *entonces se cumple que* $\mathrm{Sg}_{\mathbf{A}}(X) \subseteq_S \mathrm{Sg}_{\mathbf{A}}(Y)$.
5. $\mathrm{Sg}_{\mathbf{A}}$ *es idempotente, i.e., para cada* $X \in \mathrm{Sub}_S(A)$, $\mathrm{Sg}_{\mathbf{A}}(X) = \mathrm{Sg}_{\mathbf{A}}(\mathrm{Sg}_{\mathbf{A}}(X))$.
6. $\mathrm{Sg}_{\mathbf{A}}$ *es algebraica, i.e., para cada* $\mathcal{X} \subseteq \mathrm{Sub}_S(A)$, *si* $\mathcal{X} \neq \varnothing$ *y para cada* $X, Y \in \mathcal{X}$, *existe un* $Z \in \mathcal{X}$ *tal que* $X \cup Y \subseteq_S Z$, *entonces* $\mathrm{Sg}_{\mathbf{A}}(\bigcup \mathcal{X}) = \bigcup_{X\in\mathcal{X}} \mathrm{Sg}_{\mathbf{A}}(X)$.

Por consiguiente, para cada $X \subseteq A$, $\mathrm{Sg}_{\mathbf{A}}(X)$ *es el mínimo cerrado de* $\mathbf{A}$ *que contiene a* X, *y lo denominamos el cerrado de* $\mathbf{A}$ generado *por* X.

Demostración. □

A continuación, introducimos unas nociones que nos permitirán obtener una descripción más constructiva de la subálgebra generada por un S-subconjunto de una $\mathbf{\Sigma}$-álgebra heterogénea.

Definición 1.48. Sea $\mathbf{A} = (A, F)$ una $\mathbf{\Sigma}$-álgebra heterogénea. Entonces:

1. Denotamos por $\mathrm{E}_{\mathbf{A}}$ el operador sobre $\mathrm{Sub}_S(A)$, definido como:

$$\mathrm{E}_{\mathbf{A}} \begin{cases} \mathrm{Sub}_S(A) \longrightarrow \mathrm{Sub}_S(A) \\ X \longmapsto X \cup \big(\bigcup_{\sigma\in\Sigma_{\cdot,s}} F_\sigma[X_{\mathrm{ar}(\sigma)}] \;\big|\; s \in S \big). \end{cases}$$

2. Si $X \subseteq_S A$, entonces denotamos por $(\mathrm{E}_{\mathbf{A}}^n(X) \mid n \in \mathbb{N})$ la familia en $\mathrm{Sub}_S(A)$ definida por recursión como:

$$\mathrm{E}_{\mathbf{A}}^0(X) = X,$$
$$\mathrm{E}_{\mathbf{A}}^{n+1}(X) = \mathrm{E}_{\mathbf{A}}(\mathrm{E}_{\mathbf{A}}^n(X)),\ n \geq 0.$$

Además, convenimos que:

$$\mathrm{E}^{\omega}_{\mathbf{A}}(X) = \bigcup(\mathrm{E}^{n}_{\mathbf{A}}(X) \mid n \in \mathbb{N})$$

Proposición 1.49. *Si* $\mathbf{A}$ *es una* $\mathbf{\Sigma}$*-álgebra y* $X \subseteq_S A$*, entonces* $\mathrm{Sg}_{\mathbf{A}}(X) = \mathrm{E}^{\omega}_{\mathbf{A}}(X)$*.*

Demostración. □

Proposición 1.50. *Si* $\mathbf{A}$ *es una* $\mathbf{\Sigma}$*-álgebra,* $X \subseteq_S A$*,* $s \in S$ *y* $a \in A_s$*, entonces una condición necesaria y suficiente para que* $a \in \mathrm{Sg}_{\mathbf{A}}(X)_s$ *es que exista un* $p \in \mathbb{N} - 1$*, una familia* $(s_i \mid i \in p) \in S^p$*, y una familia* $(a_i \mid i \in p) \in \prod_{i \in p} A_{s_i}$ *tal que* $a = a_{p-1}$ *y para cada* $i \in p$*,* $a_i \in X_{s_i}$*, o* $a_i = \sigma^{\mathbf{A}}$*, para algún* $\sigma\colon \lambda \longrightarrow s_i$*, o* $a_i = F_\sigma(a_{i_\alpha} \mid \alpha \in n)$*, para un* $n \in \mathbb{N} - 1$*, una familia* $(i_\alpha \mid \alpha \in n) \in i^n$ *y un* $\sigma\colon (s_{i_\alpha} \mid \alpha \in n) \longrightarrow s_i$*.*

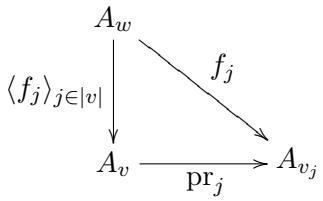
Demostración. □

1.4. Operaciones polinómicas.

A continuación estudiamos aquellas operaciones sobre el conjunto heterogéneo subyacente de una $\mathbf{\Sigma}$-álgebra que se derivan de sus operaciones estructurales. Poteriormente se estudiarán las relaciones de estas operaciones con las operaciones polinómicas formales o términos.

Definición 1.51. Sea $\mathbf{A}$ una $\mathbf{\Sigma}$-álgebra y $w \in S^\star$. La $\mathbf{\Sigma}$-álgebra de las operaciones w-arias sobre $\mathbf{A}$, $\mathbf{Op}_w(\mathbf{A})$, es $\mathbf{A}^{A_w}$, i.e., el producto de $\mathrm{card}(A_w)$-copias de $\mathbf{A}$.

En $\mathbf{Op}_w(\mathbf{A})$, las operaciones estructurales F_σ, con $\sigma\colon v \longrightarrow s$, están definidas para elementos $(f_j)_{j \in |v|}$ de $(A^{A_w})_v = \prod_{j \in |v|} A^{A_w}_{v_j}$. Ahora bien, como A_v es el producto de la familia $(A_{v_j})_{j \in |v|}$, existe, en virtud de la propiedad universal del producto, un único morfismo $\langle f_j \rangle_{j \in |v|}$ de A_w en A_v tal que



conmuta. Entonces

$$F_\sigma \begin{cases} (A^{A_w})_v \longrightarrow A_s^{A_w} \\ (f_j)_{j \in |v|} \longmapsto F_\sigma^{\mathbf{A}} \circ \langle f_j \rangle_{j \in |v|} \end{cases}$$

Definición 1.52. Sea A un S-conjunto y w una palabra sobre S. Entonces

1. Para cada $i \in |w|$, la proyección w-aria, i-ésima para A, $\mathrm{pr}^A_{w,i}$, es la operación definida como:

$$\mathrm{pr}^A_{w,i} \begin{cases} A_w \longrightarrow A_{w(i)} \\ a \longmapsto a_i \end{cases}$$

2. El S-conjunto de las proyecciones w-arias sobre un S-conjunto A es:

$$\mathrm{pr}^A_w = (\{\mathrm{pr}^A_{w,i} \mid w_i = s\})_{s \in S}.$$

Definición 1.53. Sea $\mathbf{A}$ una $\mathbf{\Sigma}$-álgebra y $w \in S^\star$. La $\mathbf{\Sigma}$-álgebra heterogénea de las operaciones polinómicas w-arias u operaciones derivadas w-arias sobre $\mathbf{A}$, $\mathbf{Pol}_w(\mathbf{A})$, es la subálgebra de la $\mathbf{\Sigma}$-álgebra de las operaciones w-arias sobre $\mathbf{A}$, $\mathbf{Op}_w(\mathbf{A})$ generada por pr_w^A.

Proposición 1.54. *Sea $\mathbf{A} = (A, F)$ una $\mathbf{\Sigma}$-álgebra. Entonces, se cumple que, para cada $\sigma \in \Sigma_{w,s}$, $F_\sigma \in \mathrm{Pol}_w(\mathbf{A})_s$.* □

Proposición 1.55. *Sea $\mathbf{A}$ una $\mathbf{\Sigma}$-álgebra, $u, w \in S^\star$, $s \in S$, $P \in \mathrm{Pol}_w(\mathbf{A})_s$ y $Q = (Q_i)_{i\in|w|}$ una familia tal que, para cada $i \in |w|$, $Q_i \in \mathrm{Pol}_u(\mathbf{A})_{w(i)}$. Entonces $P \circ \langle Q_i\rangle_{i\in|w|} \in \mathrm{Pol}_u(\mathbf{A})_s$.*

Demostración. Sea $\mathcal{X}^{w,u}$ el S-conjunto cuya coordenada s-sima es:

$$\mathcal{X}_s^{w,u} = \{P \in \mathrm{Pol}_w(\mathbf{A})_s \mid \forall (Q_i)_{i\in|w|} \in \mathrm{Pol}_u(\mathbf{A})_w,\ f \circ \langle Q_i\rangle_{i\in|w|} \in \mathrm{Pol}_u(\mathbf{A})_s\}$$

En primer lugar, se cumple que el S-conjunto de las proyecciones w-arias sobre A, pr_w^A, está incluido en $\mathcal{X}^{w,u}$ porque, dado un $s \in S$, un $i \in w^{-1}(s)$ y una familia $(Q_i)_{i\in|w|}$ en $\mathrm{Pol}_u(\mathbf{A})_w$,

$$\mathrm{pr}_{w,i}^A \circ \langle Q_i\rangle_{i\in|w|} = Q_i \in \mathrm{Pol}_u(\mathbf{A})_{w(i)}$$

Además, $\mathcal{X}$ es un cerrado de $\mathrm{Pol}_w(\mathbf{A})$, ya que, para cada $\sigma \in \Sigma$, con $\sigma\colon v \longrightarrow s$, y cada $R = (R_i)_{i\in|v|} \in \mathcal{X}_v$, se tiene que $F_\sigma^{\mathbf{Op}_w(\mathbf{A})}(R) \in \mathcal{X}_s$, puesto que dada una familia $(Q_i)_{i\in|w|} \in \mathrm{Pol}_u(\mathbf{A})_w$ se cumple que

$$\begin{aligned} F_\sigma^{\mathbf{Op}_w(\mathbf{A})}(R) \circ \langle Q_i\rangle_{i\in|w|} &= F_\sigma^{\mathbf{A}} \circ \langle R_i\rangle_{i\in|v|} \circ \langle Q_i\rangle_{i\in|w|} \\ &= F_\sigma^{\mathbf{A}} \circ \langle R_i \circ \langle Q_i\rangle_{i\in|w|}\rangle_{i\in|v|} \in \mathrm{Pol}_u(\mathbf{A})_s \end{aligned}$$

□

En la proposición que sigue usamos las operaciones polinómicas para dar otra descripción del operador subálgebra generada.

Proposición 1.56. *Sea $\mathbf{A}$ una $\mathbf{\Sigma}$-álgebra. Entonces se cumple que*

1. *Para cada $w \in S^\star$, cada $a \in A_w$ y cada $s \in S$*

$$\mathrm{Sg}_{\mathbf{A}}((a[w^{-1}[s]])_{s\in S})_s = \{P(a) \mid P \in \mathrm{Pol}_w(\mathbf{A})_s\}.$$

2. *Para cada $X \subseteq A$ y cada $s \in S$ se cumple que*

$$\mathrm{Sg}_{\mathbf{A}}(X)_s = \{P(x) \mid w \in S^\star,\ P \in \mathrm{Pol}_w(\mathbf{A})_s,\ x \in X_w\}$$

□

La siguiente proposición afirma que los cerrados de las $\mathbf{\Sigma}$-álgebras no sólo lo están respecto de las operaciones estructurales, sino respecto de las operaciones polinómicas de las mismas.

Proposición 1.57. *Sea $\mathbf{A}$ una $\mathbf{\Sigma}$-álgebra, X un cerrado de $\mathbf{A}$, $w \in S^\star$, $s \in S$ y $P \in \mathrm{Pol}_w(\mathbf{A})_s$. Entonces, para cada $x \in X_w$, $P(x) \in X_s$.* □

1.5. Álgebras libres.

Demostramos a continuación la existencia de $\mathbf{\Sigma}$-álgebras libres sobre cualquier S-conjunto y se estudia la relación de los *términos* o *símbolos de operación polinómica* con las operaciones polinómicas de una $\mathbf{\Sigma}$-álgebra.

Definición 1.58. De $\mathbf{Alg}(\mathbf{\Sigma})$ en $\mathbf{Set}^S$ existe un functor de olvido $\mathrm{G}_{\mathbf{\Sigma}}$ definido sobre objetos y morfismos como:

$$\mathrm{G}_{\mathbf{\Sigma}}(f\colon \mathbf{A} \longrightarrow \mathbf{B}) = f\colon A \longrightarrow B$$

El functor $\mathrm{G}_{\mathbf{\Sigma}}$ tiene un adjunto por la izquierda, que asigna a cada S-conjunto X, una $\mathbf{\Sigma}$-álgebra libre sobre él. Ésta se obtiene a partir de una cierta $\mathbf{\Sigma}$-álgebra de palabras, como la subálgebra generada por X. En este contexto, es usual referirse a los elementos de X como *variables*.

Definición 1.59. Sea $\mathbf{\Sigma} = (S, \Sigma)$ una signatura algebraica y X un S-conjunto. La $\mathbf{\Sigma}$-álgebra de las palabras sobre X, $\mathrm{W}_{\mathbf{\Sigma}}(X)$, es la definida como:

1. Para cada $s \in S$, $\mathrm{W}_{\mathbf{\Sigma}}(X)_s = (\coprod \Sigma \amalg \coprod X)^\star$, i.e., el conjunto subyacente es, en cada coordenada, el conjunto de las palabras que pueden formarse con símbolos de operación de Σ y variables de X.
2. Para cada $\sigma \in \Sigma$, $\sigma\colon w \longrightarrow s$, la operación estructural F_σ, asociada a σ, es la aplicación de $\mathrm{W}_{\mathbf{\Sigma}}(X)_w$ en $\mathrm{W}_{\mathbf{\Sigma}}(X)_s$, i.e., de $((\coprod \Sigma \amalg \coprod X)^\star)^{|w|}$ en $(\coprod \Sigma \amalg \coprod X)^\star$, que a una palabra de palabras $(P_i)_{i\in|w|}$ le asigna $(\sigma) \curlywedge \curlywedge_{i\in|w|} P_i$, i.e., la concatenación de (la imagen de) σ (bajo las inclusiones canónicas desde Σ hasta $(\coprod \Sigma \amalg \coprod X)^\star$ y de la concatenación de las palabras que componen $(P_i)_{i\in|w|}$.

$$F_\sigma \begin{cases} \mathrm{W}_{\mathbf{\Sigma}}(X)_w \longrightarrow \mathrm{W}_{\mathbf{\Sigma}}(X)_s \\ (P_i)_{i\in|w|} \longmapsto (\sigma) \curlywedge \curlywedge_{i\in|w|} P_i \end{cases}$$

Definición 1.60. La $\mathbf{\Sigma}$-álgebra libre sobre un S-conjunto X, $\mathbf{T}_{\mathbf{\Sigma}}(X)$, es la subálgebra de $\mathrm{W}_{\mathbf{\Sigma}}(X)$ generada por el S-conjunto $(\{(x) \mid x \in X_s\})_{s\in S}$, donde, para cada $s \in S$ y cada $x \in X_s$, (x) es la imagen de x mediante las inclusiones canónicas desde X_s hasta $(\coprod \Sigma \amalg \coprod X)^\star$.

A los elementos de $\mathbf{T}_{\mathbf{\Sigma}}(X)_s$ se les denomina operación polinómicas formales o términos de tipo s con variables en X.

En las figuras siguientes se muestran las inclusiones desde X_s, resp., $\Sigma_{w,s}$, hasta $\mathrm{W}_{\mathbf{\Sigma}}(X)_s$:

$$X_s \xrightarrow{\mathrm{in}_{X_s}} \coprod X \xrightarrow{\mathrm{in}_{\coprod X}} \coprod \Sigma \amalg \coprod X \xrightarrow{\eta_{\coprod \Sigma \amalg \coprod X}} (\coprod \Sigma \amalg \coprod X)^\star$$

$$x \longmapsto (x, s) \longmapsto ((x, s), 1) \longmapsto (((x, s), 1)) \equiv (x)$$

$$\Sigma_{w,s} \xrightarrow{\mathrm{in}_{\Sigma_{w,s}}} \coprod \Sigma \xrightarrow{\mathrm{in}_{\coprod \Sigma}} \coprod \Sigma \amalg \coprod X \xrightarrow{\eta_{\coprod \Sigma \amalg \coprod X}} (\coprod \Sigma \amalg \coprod X)^\star$$

$$\sigma \longmapsto (\sigma, (w, s)) \longmapsto ((\sigma, (w, s)), 0) \longmapsto (((\sigma, (w, s)), 0)) \equiv (\sigma)$$

Proposición 1.61. *Los símbolos de operación polinómica se pueden representar unívocamente como:*

1. (x), *para un único* $s \in S$ *y un único* $x \in X_s$.
2. (σ), *para un único* $s \in S$ *y un único* $\sigma \in \Sigma_{\lambda,s}$.
3. $(\sigma) \curlywedge \curlywedge(P_i)_{i\in|w|}$, *para unos únicos* $w \in S^\star - \{\lambda\}$, $s \in S$, $\sigma \in \Sigma_{w,s}$, *y una única familia* $(P_i)_{i\in|w|}$ *en* $T_{\mathbf{\Sigma}}(X)_w$.

□

Es posible dar otras representaciones de la $\mathbf{\Sigma}$-álgebra libre sobre un S-conjunto, e.g., mediante la noción de árbol etiquetado. Sin embargo, las propiedades esenciales de la $\mathbf{\Sigma}$-álgebra libre sobre un S-conjunto X dependen sólo de su propiedad universal, puesto que esta la determina salvo un único homomorfismo, y no de la forma concreta que se dé de la misma.

Proposición 1.62. *Para cada* S*-conjunto* X*, el par* $(\eta^X, \mathbf{T}_{\mathbf{\Sigma}}(X))$*, en el que* η^X *es la correstricción a* $T_{\mathbf{\Sigma}}(X)$ *de la inclusión canónica de* X *en* $\mathrm{W}_{\mathbf{\Sigma}}(X)$*, es un morfismo universal desde* X *hasta* $\mathrm{G}_{\mathbf{\Sigma}}$*, i.e., dada una* $\mathbf{\Sigma}$*-álgebra* $\mathbf{A}$ *y una* S*-aplicación* $f\colon X \longrightarrow A$*, existe un único homomorfismo de* $\mathbf{\Sigma}$*-álgebras* $f^\sharp\colon \mathbf{T}_{\mathbf{\Sigma}}(X) \longrightarrow \mathbf{A}$ *que extiende* f*, i.e., tal que el siguiente diagrama conmuta:*

$$\begin{array}{ccc} X & \xrightarrow{\eta^X} & T_{\mathbf{\Sigma}}(X) \\ & \searrow^{f} & \downarrow{\scriptstyle f^\sharp} \\ & & A \end{array}$$

Demostración. En la coordenada s-sima, la aplicación $f^\sharp_s\colon \mathrm{T}_{\mathbf{\Sigma}}(X)_s \longrightarrow A_s$ se define, por recursión, como:

$$P \longmapsto \begin{cases} f_s(x), & \text{si } P = (x); \\ \sigma^{\mathbf{A}}, & \text{si } P = (\sigma); \\ F^{\mathbf{A}}_\sigma(f^\sharp_{w(0)}(P_0), \ldots, f^\sharp_{w(|w|-1)}(P_{|w|-1})), & \text{si } P = (\sigma) \curlywedge \curlywedge(P_i)_{i\in|w|}. \end{cases}$$

□

Siguiendo la práctica habitual, los términos, $F^{\mathbf{T}_{\mathbf{\Sigma}}(X)}_\sigma(P_i \mid i \in |w|)$ se denotan como $\sigma(P_0, \ldots, P_{|w|-1})$. Asimismo, si no hay ambigüedad, los términos (x) y (σ) se denotan simplemente como x y σ.

Corolario 1.63. *El functor* $\mathbf{T}_{\mathbf{\Sigma}}$ *es adjunto por la izquierda del functor de olvido* $\mathrm{G}_{\mathbf{\Sigma}}$.

$$\mathbf{Alg}(\mathbf{\Sigma}) \underset{\mathbf{T}_{\mathbf{\Sigma}}}{\overset{\mathrm{G}_{\mathbf{\Sigma}}}{\underset{\longleftarrow}{\overset{\longrightarrow}{\top}}}} \mathbf{Set}$$

Proposición 1.64. *Cada* $\mathbf{\Sigma}$*-álgebra* $\mathbf{A}$ *es isomorfa a un cociente de una* $\mathbf{\Sigma}$*-álgebra libre sobre un* S*-conjunto.* □

Demostración. Sea $\mathbf{A}$ una $\mathbf{\Sigma}$-álgebra. Entonces la extensión canónica de la identidad en A, $\mathrm{id}^\sharp_{\mathbf{A}}$, es un epimorfismo y $\mathbf{T}_{\mathbf{\Sigma}}(A)/\operatorname{Ker}(\mathrm{id}^\sharp_{\mathbf{A}})$ es isomorfa a $\mathbf{A}$. □

1.6. Operaciones polinómicas formales y operaciones polinómicas.

Las operaciones polinómicas sobre una $\mathbf{\Sigma}$-álgebra $\mathbf{A}$ se pueden caracterizar como las realizaciones de las operaciones polinómicas formales. Estos son los miembros de una cierta $\mathbf{\Sigma}$-álgebra libre sobre un S-conjunto de variables asociado a la ariedad de las operaciones.

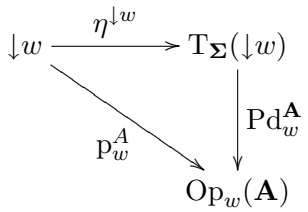
Para el estudio de las operaciones polinómica formales es necesario asociar a cada palabra sobre S un S-conjunto de *variables*.

Definición 1.65. Sea $w \in S^\star$. Entonces $\downarrow w$ es el S-conjunto

$$\downarrow w = (w^{-1}[s])_{s\in S}$$

Si A un S-conjunto y w es una palabra sobre S, entonces los conjuntos $A_{\downarrow w}$ y A_w son naturalmente isomorfos. En lo que sigue, si no hay ambigüedad, no distinguiremos notacionalmente entre las S-aplicaciones de $A_{\downarrow w}$ y los elementos de A_w.

Las operaciones polinómicas w-arias sobre un álgebra pueden definirse mediante los símbolos de operación polinómica w-arios. Para ello, se hace uso del hecho de que dada una $\mathbf{\Sigma}$-álgebra $\mathbf{A}$ y un $w \in S^\star$, existe un único homomorfismo $\mathrm{Pd}_w^{\mathbf{A}} \colon \mathbf{T}_{\mathbf{\Sigma}}(\downarrow w) \longrightarrow \mathbf{Op}_w(\mathbf{A})$ tal que el diagrama



conmuta, siendo p_w^A la S-aplicación definida, para cada $s \in S$ y para cada $i \in \downarrow w_s$, como $\mathrm{p}_{w,s}^A(i) = \mathrm{pr}_{w,i}^A$.

Definición 1.66. Sea $\mathbf{A}$ una $\mathbf{\Sigma}$-álgebra, $w \in S^\star$, $s \in S$ y $P \in \mathrm{T}_{\mathbf{\Sigma}}(\downarrow w)_s$. Entonces a $\mathrm{Pd}_{w,s}^{\mathbf{A}}(P)$ se le denomina el polinomio (w,s)-ario determinado por P en $\mathbf{A}$ y se le denota por $P^{\mathbf{A}}$.

Proposición 1.67. *Sea $\mathbf{A}$ una $\mathbf{\Sigma}$-álgebra y $w \in S^\star$. La $\mathbf{\Sigma}$-álgebra heterogénea de las operaciones polinómicas w-arias sobre $\mathbf{A}$, $\mathbf{Pol}_w(\mathbf{A})$, coincide con la subálgebra de $\mathbf{Op}_w(\mathbf{A})$ canónicamente asociada a la imagen de $\mathrm{T}_{\mathbf{\Sigma}}(\downarrow w)$ mediante $\mathrm{Pd}_w^{\mathbf{A}}$, i.e., $\mathrm{Pol}_w(\mathbf{A}) = \mathrm{Pd}_w^{\mathbf{A}}[\mathbf{T}_{\mathbf{\Sigma}}(\downarrow w)]$.* □

Demostración. Puesto que $\mathrm{pr}_w^A \subseteq \mathrm{Pd}_w^{\mathbf{A}}[\mathrm{T}_{\mathbf{\Sigma}}(\downarrow w)]$, $\mathrm{Sg}_{\mathbf{Op}_w(\mathbf{A})}(\mathrm{pr}_w^A) \subseteq \mathrm{Pd}_w^{\mathbf{A}}[\mathrm{T}_{\mathbf{\Sigma}}(\downarrow w)]$.

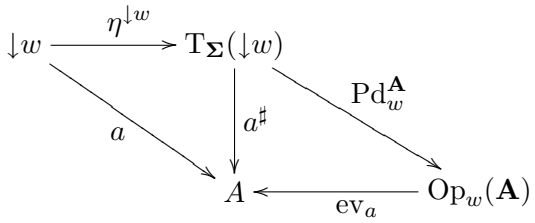
Recíprocamente,

$$\begin{aligned}
\mathrm{Pd}_w^{\mathbf{A}}[\mathrm{T}_{\mathbf{\Sigma}}(\downarrow w)] &= \mathrm{Pd}_w^{\mathbf{A}}[\mathrm{Sg}_{\mathbf{T}_{\mathbf{\Sigma}}(\downarrow w)}(\eta^{\downarrow w}[\downarrow w])] \\
&= \mathrm{Sg}_{\mathbf{Op}_w(\mathbf{A})}(\mathrm{Pd}_w^{\mathbf{A}}[\eta^{\downarrow w}[\downarrow w]]) \\
&= \mathrm{Sg}_{\mathbf{Op}_w(\mathbf{A})}(\mathrm{p}_w^A[\downarrow w]) \\
&= \mathrm{Sg}_{\mathbf{Op}_w(\mathbf{A})}(\mathrm{pr}_w^A) \\
&= \mathrm{Pol}_w^{\mathbf{A}}
\end{aligned}$$

□

Proposición 1.68 (Ley de reciprocidad)**.** *Sea* $\mathbf{A}$ *una* $\mathbf{\Sigma}$*-álgebra,* P *un polinomio formal en* $\mathrm{T}_{\mathbf{\Sigma}}(\downarrow w)_s$ *y* $a\colon \downarrow w \longrightarrow A$*. Entonces* $a^\sharp_s(P) = P^{\mathbf{A}}(a)$*.*

Demostración. El diagrama



conmuta, siendo ev_a el homomorfismo de evaluación definido, en la coordenada s-sima, como

$$(\mathrm{ev}_a)_s(f\colon A_w \longrightarrow A_s) = f(a)$$

luego, para cada $P \in \mathrm{T}_{\mathbf{\Sigma}}(\downarrow w)_s$, se cumple que:

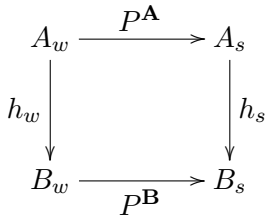
$$a^\sharp_s(P) = (\mathrm{ev}_a)_s \circ \mathrm{Pd}^A_{w,s}(P) = (\mathrm{ev}_a)_s(P^{\mathbf{A}}) = P^{\mathbf{A}}(a)$$

□

Proposición 1.69. *La restricción a* $\mathbf{Pol}_w(\mathbf{A})$ *de* $\mathrm{Pd}^{\mathbf{A}}_w$ *es un homomorfismo sobreyectivo, por lo que* $\mathbf{T}_{\mathbf{\Sigma}}(\downarrow w)/\operatorname{Ker}(\mathrm{Pd}^{\mathbf{A}}_w)$ *es isomorfa a* $\mathbf{Pol}_w(\mathbf{A})$*.* □

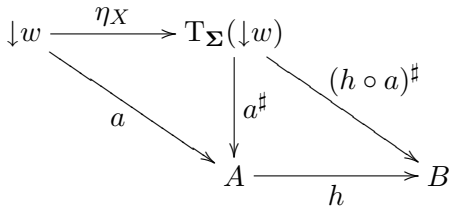
Las operaciones polinómicas w-arias se comportan, respecto de los homomorfismos, como las operaciones estructurales de las álgebras.

Proposición 1.70. *Sea* $\mathbf{\Sigma}$ *un signatura algebraica y* $h\colon \mathbf{A} \longrightarrow \mathbf{B}$ *un homomorfismo de* $\mathbf{\Sigma}$*-álgebras. Entonces para cada* $w \in S^\star$*,* $s \in S$ *y* $P \in \mathrm{T}_{\mathbf{\Sigma}}(\downarrow w)_s$ *el diagrama*



conmuta.

Demostración. El diagrama



conmuta, por lo que

$$h_s \circ P^{\mathbf{A}}(a) = h_s \circ a^\sharp_s(P) = (h \circ a)^\sharp_s(P) = P^{\mathbf{B}}(h \circ a) = P^{\mathbf{B}}(h_w(a))$$

□

1.7. Aplicaciones recursivas primitivas.

> Tarski has stressed in his lecture (and I think justly) the great importance of the concept of general recursiveness (or Turing computability). It seems to me that this importance is largely due to the fact that with this concept one has for the first time succeeded in giving an absolute definition of an interesting epistemological notion, i.e., one not depending on the formalism chosen. In all other cases treated previously, such as demonstrability or definability, one has been able to define them only relative to a given language, and for each individual language it is clear that the one thus obtained is not the one looked for. For the concept of computability, however, although it is merely a special kind of demonstrability or decidability, the situation is different. By a kind of miracle it is not necessary to distinguish orders, and the diagonal procedure does not lead outside the defined notion.
>
> *K. Gödel.*

> En mathématiques, il est d'usage d'entendre par "algorithme" une prescription précise, définissant un processus de calcul, conduisant à partir de points de départ qui varient au résultat cherché.
>
> *A.A. Markov.*

La teoría de la recursión se ocupa del *estudio y clasificación de las relaciones y funciones computables* y tuvo su origen en algunas de las nociones y construcciones que introdujo Gödel en su trabajo sobre la incompletud. Además, la teoría de la recursión, junto con la teoría de autómatas, lenguajes y máquinas, es el *fundamento de la informática teórica* y esta, a su vez, de la industria de los ordenadores.

Desde tiempo inmemorial se sabe que cierta clase de *problemas*, e.g., la determinación del máximo común divisor de dos números enteros, mediante el algoritmo de Euclides, la determinación de los números primos, mediante la criba de Eratóstenes, o la determinación de si una ecuación $a_nX^n + \ldots + a_1X + a_0 = 0$, con coeficientes enteros, tiene soluciones enteras, son *algorítmicamente solubles*, i.e., hay algoritmos o procedimientos mecánicos que permiten obtener la solución del problema en cuestión (para el último, las soluciones enteras han de ser divisores de a_0). De manera que hasta principios del presente siglo se daba por hecho que existían algoritmos y que el único problema residía en determinarlos. Así pues, si lo que se desea es determinar un algoritmo, no hay ninguna necesidad de definir la clase de todos los algoritmos; eso sólo es necesario si se pretende demostrar que algún *problema no es algorítmicamente soluble*. i.e., que para dicho problema no hay ningún algoritmo que lo resuelva.

Ejemplos de problemas matemáticos algorítmicamente insolubles vienen dados por:

1. El problema de las ecuaciones diofánticas (que es el problema décimo de la lista de veintitrés que propuso Hilbert en 1900:
   > Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.*").

   Resuelto por Matijasevich.

2. El problema de las palabras para los semigrupos finitamente presentados (problema de Thue). Resuelto, independientemente, por Post y Markoff.
3. El problema de las palabras para los grupos finitamente presentados (problema de Dehn & Thue). Resuelto, independientemente, por Novikoff, Boone y Britton.
4. El problema del homeomorfismo para las n-variedades ($4 \leq n$).

Es posible que el primero en afirmar la *no existencia de un algoritmo* fuera Tietze en 1908, quién dijo de los grupos de presentación finita:

> "la cuestión acerca de cuando dos grupos son isomorfos no es soluble en general."

Pero parece ser que fue, por una parte, el *problema de la decidibilidad de la lógica de predicados*, planteado por Hilbert y Ackermann en su libro sobre lógica, publicado en 1928, y, por otra, el asunto de la *solubilidad de todo problema matemático*, lo que indujo, en aras a resolverlos, a diversos investigadores a partir de 1930, y entre los que cabe mencionar a Gödel, Church y Turing, a proponer diversas *formalizaciones del concepto informal de función mecánicamente computable*. Debido a que de todas esas formalizaciones, y de otras, propuestas por Kleene, Post y Markov, se demostró que eran dos a dos equivalentes, se propuso la hipótesis, conocida como *Hipótesis de Church-Turing-Post-Kleene*, que afirma la coincidencia entre el concepto informal de *función parcial mecánica o algorítmicamente computable*, y el concepto formal de *aplicación parcial recursiva*. Naturalmente, esa hipótesis, de caracter similar a otras hipótesis propuestas en las ciencias empíricas, no es demostrable, y su fundamento último reside en las equivalencias antes mencionadas.

Definimos y estudiamos en esta sección las aplicaciones y relaciones recursivas primitivas, lo cual nos permitirá, en particular, dotar al conjunto de los números naturales de una estructura algebraica, i.e., de unas operaciones finitarias (la adición y la multiplicación, entre otras), que como puso de manifiesto Dedekind, son definibles por recursión y sus propiedades demostrables por inducción, lo mismo que ocurre con casi todas las operaciones aritméticas usuales, y, que de hecho, tienen la propiedad de caer bajo el concepto de aplicación recursiva primitiva, estando, además, tales operaciones finitarias sujetas a cumplir ciertas condiciones, expresadas ecuacional o implicacionalmente, y de modo que tal estructura sea compatible con la buena ordenación de que está dotado el conjunto de los números naturales.

Conviene también señalar que el conjunto de las aplicaciones recursivas primitivas, considerado por primera vez por Gödel, es una de las clases de aplicaciones numéricas (con argumentos y valores, números naturales), junto al de las aplicaciones recursivas (generales) y al de las aplicaciones parciales recursivas, que se considera está constituido por aplicaciones que son mecánicamente computables (si no se toman en consideración las limitaciones espacio-temporales, o si no se las identifica con las aplicaciones que sean pragmáticamente computables), pace Blum, Shub and Smale.

Puesto que el conjunto de las aplicaciones recursivas primitivas será la unión de la mínima subálgebra heterogénea de una determinada álgebra

heterogénea, definimos en primer lugar la signatura algebraica heterogénea del álgebra heterogénea en cuestión.

Definición 1.71. Denotamos por $\mathbf{\Sigma}^{\mathrm{rp}}$ la $\mathbb{N}$-signatura algebraica heterogénea, para las aplicaciones recursivas primitivas, cuya coordenada (w,n)-sima, con $(w,n) \in \mathbb{N}^\star \times \mathbb{N}$, es la definida como:

$$\Sigma^{\mathrm{rp}}_{w,n} = \begin{cases} \{\kappa_{0,0}\}, & \text{si } w = \lambda \text{ y } n = 0; \\ \{\mathrm{sc}\} \cup \{\mathrm{pr}_{1,0}\}, & \text{si } w = \lambda \text{ y } n = 1; \\ \{\, \mathrm{pr}_{n,i} \mid i \in n \,\}, & \text{si } w = \lambda \text{ y } n \geq 2; \\ \{\Omega^{m,n}_{\mathrm{C}}\}, & \text{si } w = (m) \curlywedge (n \mid i \in m) \text{ y } m \geq 1; \\ \{\Omega^{m}_{\mathrm{R}}\}, & \text{si } w = (m) \curlywedge (m+2) \text{ y } n = m+1; \\ \varnothing, & \text{en cualquier otro caso.} \end{cases}$$

Definición 1.72. Denotamos por $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$ la $\mathbf{\Sigma}^{\mathrm{rp}}$-álgebra heterogénea cuyo $\mathbb{N}$-conjunto subyacente, $\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$, es $(\mathrm{Hom}(\mathbb{N}^n, \mathbb{N}))_{n \in \mathbb{N}}$, de modo que la coordenada n-sima es el conjunto de las aplicaciones de $\mathbb{N}^n$ en $\mathbb{N}$, y en la que las operaciones estructurales son:

1. $\kappa_{0,0}$, la aplicación constante 0-aria determinada por 0, que es la aplicación de $\mathbb{N}^0$ en $\mathbb{N}$, que al único miembro de $\mathbb{N}^0$ le asigna como valor 0.
2. sc, la aplicación sucesor.
3. $\mathrm{pr}_{1,0}$, la aplicación identidad de $\mathbb{N}$.
4. Para cada $n \geq 2$ y cada $i \in n$, $\mathrm{pr}_{n,i}$, la proyección canónica i-ésima de $\mathbb{N}^n$ en $\mathbb{N}$.
5. Para cada $m \in \mathbb{N} - 1$ y cada $n \in \mathbb{N}$, $\Omega^{m,n}_{\mathrm{C}}$, el operador de composición (generalizada) de ariedad $(m) \curlywedge (n \mid i \in m)$ y coariedad n, que es la aplicación de $\mathrm{Hom}(\mathbb{N}^m, \mathbb{N}) \times (\mathrm{Hom}(\mathbb{N}^n, \mathbb{N}))^m$ en $\mathrm{Hom}(\mathbb{N}^n, \mathbb{N})$ que a un par $(f, (g_i \mid i \in m))$ del primero le asigna como valor la aplicación $\Omega^{m,n}_{\mathrm{C}}(f, (g_i \mid i \in m))$ de $\mathbb{N}^n$ en $\mathbb{N}$ obtenida componiendo $\langle g_i \mid i \in m \rangle$ y f.
6. Para cada $m \in \mathbb{N}$, Ω^{m}_{R}, el operador de recursión primitiva de ariedad $(m) \curlywedge (m+2)$ y coariedad $m+1$, que es la aplicación de $\mathrm{Hom}(\mathbb{N}^m, \mathbb{N}) \times \mathrm{Hom}(\mathbb{N}^{m+2}, \mathbb{N})$ en $\mathrm{Hom}(\mathbb{N}^{m+1}, \mathbb{N})$ que a un par (f, g) del primero le asigna como valor la aplicación $\Omega^{m}_{\mathrm{R}}(f, g)$ de $\mathbb{N}^{m+1}$ en $\mathbb{N}$ obtenida de f y g por recursión primitiva.

En la definición anterior, en virtud del isomorfismo natural que existe entre ambos, hemos identificado el conjunto $\mathrm{Hom}(\mathbb{N}^1, \mathbb{N})$ con el conjunto $\mathrm{End}(\mathbb{N})$, de las endoaplicaciones de $\mathbb{N}$. Además, para simplificar la notación, hemos identificado los símbolos de operación heterogéneos con sus realizaciones en el $\mathbb{N}$-conjunto $(\mathrm{Hom}(\mathbb{N}^n, \mathbb{N}) \mid n \in \mathbb{N})$.

Puesto que disponemos del concepto de subálgebra de un álgebra heterogénea, para la $\mathbf{\Sigma}^{\mathrm{rp}}$-álgebra heterogénea $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$, un $\mathbb{N}$-subconjunto $\mathcal{F} = (\mathcal{F}_n)_{n \in \mathbb{N}}$ del $\mathbb{N}$-conjunto subyacente $\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$ de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$, será una subálgebra precisamente cuando cumpla las siguientes condiciones:

- $\kappa_{0,0} \in \mathcal{F}_0$.
- $\mathrm{sc} \in \mathcal{F}_1$.
- $\mathrm{pr}_{1,0} \in \mathcal{F}_1$.

- Para cada $n \geq 2$ y cada $i \in n$, $\mathrm{pr}_{n,i} \in \mathcal{F}_n$.
- Para cada $m \in \mathbb{N} - 1$, cada $n \in \mathbb{N}$, cada $f \in \mathcal{F}_m$ y cada $(g_i \mid i \in m) \in (\mathcal{F}_n)^m$, $\Omega_{\mathrm{C}}^{m,n}(f, (g_i \mid i \in m)) \in \mathcal{F}_n$.
- Para cada $m \in \mathbb{N}$, cada $f \in \mathcal{F}_m$ y cada $g \in \mathcal{F}_{m+2}$, $\Omega_{\mathrm{R}}^{m}(f, g) \in \mathcal{F}_{m+1}$.

Debido a que lo que es cierto para todas las álgebras heterogéneas, lo es de las de una signatura determinada, tenemos las siguientes proposiciones.

Proposición 1.73.

1. $(\mathrm{Hom}(\mathbb{N}^n, \mathbb{N}))_{n\in\mathbb{N}}$ *es una subálgebra de* $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$.
2. *Si* $(\mathcal{F}^i)_{i\in I}$ *es una familia no vacía de subálgebras de* $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$, *entonces* $\bigcap_{i\in I} \mathcal{F}^i$ *es una subálgebra de* $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$.
3. *Si* $(\mathcal{F}^i)_{i\in I}$ *es una familia no vacía de subálgebras de* $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$, *y si dados* $i, j \in I$, *hay un* $k \in I$ *tal que* $\mathcal{F}^i \cup \mathcal{F}^j \subseteq_{\mathbb{N}} \mathcal{F}^k$, *entonces* $\bigcup_{i\in I} \mathcal{F}^i$ *es una subálgebra de* $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$.

Corolario 1.74. *Para la* $\mathbf{\Sigma}^{\mathrm{rp}}$*-álgebra heterogénea* $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$, *se cumple que la endoaplicación* $\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}$ *del conjunto* $\mathrm{Sub}_{\mathbb{N}}(\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N}))$, *de los* $\mathbb{N}$*-subconjuntos de* $\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$, *definida como:*

$$\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})} \begin{cases} \mathrm{Sub}_{\mathbb{N}}(\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})) \longrightarrow \mathrm{Sub}_{\mathbb{N}}(\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})) \\ \mathcal{F} \qquad\qquad\quad \longmapsto \bigcap\{\, \mathcal{C} \in \mathrm{S}(\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})) \mid \mathcal{F} \subseteq_{\mathbb{N}} \mathcal{C} \,\} \end{cases}$$

tiene las siguientes propiedades:

1. $\mathrm{Im}(\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}) \subseteq \mathrm{Cl}(\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N}))$.
2. $\{\, \mathcal{X} \in \mathrm{Sub}_{\mathbb{N}}(\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})) \mid \mathcal{X} = \mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}(\mathcal{X}) \,\} = \mathrm{Cl}(\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N}))$.
3. $\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}$ *es extensiva, i.e., para cada* $\mathcal{X} \in \mathrm{Sub}_{\mathbb{N}}(\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N}))$, *se cumple que* $\mathcal{X} \subseteq_{\mathbb{N}} \mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}(\mathcal{X})$.
4. $\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}$ *es isótona, i.e., para cada* $\mathcal{X}, \mathcal{Y} \in \mathrm{Sub}_{\mathbb{N}}(\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N}))$, *si* $\mathcal{X} \subseteq_{\mathbb{N}} \mathcal{Y}$, *entonces* $\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}(\mathcal{X}) \subseteq_{\mathbb{N}} \mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}(\mathcal{Y})$.
5. $\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}$ *es idempotente, i.e., para cada* $\mathcal{X} \in \mathrm{Sub}_{\mathbb{N}}(\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N}))$, *se cumple que* $\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}(\mathcal{X}) = \mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}(\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}(\mathcal{X}))$.
6. $\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}$ *es algebraica, i.e., para cada familia no vacía* $(\mathcal{X}^i)_{i\in I}$ *en* $\mathrm{Sub}_{\mathbb{N}}(\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N}))$, *si para cada* $i, j \in I$, *existe un* $k \in I$ *tal que* $\mathcal{X}^i \cup \mathcal{X}^j \subseteq_{\mathbb{N}} \mathcal{X}^k$, *entonces* $\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}(\bigcup_{i\in I} \mathcal{X}^i) = \bigcup_{i\in I} \mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}(\mathcal{X}^i)$.

Por consiguiente, para cada $\mathcal{X} \subseteq \mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$, $\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}(\mathcal{X})$, *al que también denotamos por* $\overline{\mathcal{X}}$, *es el mínimo cerrado de* $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$ *que contiene a* $\mathcal{X}$, *y lo denominamos el cerrado de* $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$ generado *por* $\mathcal{X}$.

Demostración. □

Observemos que la propiedad de algebricidad del operador $\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}$ equivale a que, para cada $\mathcal{X} \subseteq_{\mathbb{N}} \mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$, se cumpla que:

$$\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}(\mathcal{X}) = \bigcup_{\mathcal{F}\in\mathrm{Sub}_{\mathrm{fin}}(\mathcal{X})} \mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}(\mathcal{F}),$$

siendo $\mathrm{Sub}_{\mathrm{fin}}(\mathcal{X})$ el conjunto formado por los $\mathbb{N}$-subconjuntos $\mathcal{F}$ de $\mathcal{X}$ tales que el soporte de $\mathcal{F}$, i.e., el conjunto $\mathrm{supp}(\mathcal{F}) = \{\, n \in \mathbb{N} \mid \mathcal{F}_n \neq \varnothing \,\}$, es finito y, además, para cada $n \in \mathrm{supp}(\mathcal{F})$, $\mathcal{F}_n$ es finito.

Definición 1.75. Sea $\mathcal{F} = (\mathcal{F}_n)_{n\in\mathbb{N}}$ un $\mathbb{N}$-subconjunto finito de $\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$. Entonces a las aplicaciones pertenecientes a la unión de la subálgebra heterogénea de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$ generada por tal $\mathbb{N}$-subconjunto finito, las denominamos aplicaciones *recursivas primitivas relativas a* $\mathcal{F}$, o aplicaciones $\mathcal{F}$-*recursivas primitivas*, y al conjunto de todas ellas lo denotamos por $\mathrm{ARP}(\mathcal{F})$.

En particular, el conjunto de las aplicaciones *recursivas primitivas*, denotado por ARP, es la unión de la subálgebra heterogénea de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$ generada por el $\mathbb{N}$-conjunto $(\varnothing)_{n\in\mathbb{N}}$ (cuyas coordenadas son todas vacías).

No perdemos generalidad, si en lugar de definir el conjunto de las aplicaciones recursivas primitivas respecto de un $\mathbb{N}$-subconjunto finito de $\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$, lo definimos respecto de una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$, ya que, debido a que el operador $\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}$ es idempotente, para cada $\mathbb{N}$-subconjunto finito $\mathcal{F}$ de $\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$, se cumple que:

$$\mathrm{ARP}(\mathcal{F}) = \mathrm{ARP}(\overline{\mathcal{F}}).$$

Además, si $\mathcal{F}$ es una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$, entonces $\mathrm{ARP}(\mathcal{F})$ es, simplemente, $\bigcup_{n\in\mathbb{N}} \mathcal{F}_n$.

Como consecuencia inmediata de las propiedades del operador $\mathrm{Sg}_{\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})}$, tenemos, por una parte, que para cada $\mathbb{N}$-subconjunto finito $\mathcal{F}$ de $\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$, $\mathrm{ARP} \subseteq \mathrm{ARP}(\mathcal{F})$, i.e., que toda aplicación recursiva primitiva es una aplicación $\mathcal{F}$-recursiva primitiva y, por otra, que si $\mathcal{F}$, $\mathcal{G}$ y $\mathcal{H}$ son tres $\mathbb{N}$-subconjuntos finitos de $\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$ tales que $\mathcal{F} \subseteq \mathcal{G} \subseteq \mathcal{H}$, y, además, toda aplicación de $\bigcup_{n\in\mathbb{N}} \mathcal{F}_n$ es $\mathcal{G}$-recursiva primitiva y toda aplicación de $\bigcup_{n\in\mathbb{N}} \mathcal{G}_n$ es $\mathcal{H}$-recursiva primitiva, entonces toda aplicación de $\bigcup_{n\in\mathbb{N}} \mathcal{F}_n$ es $\mathcal{H}$-recursiva primitiva.

Proposición 1.76. *Sea* $\mathcal{F} = (\mathcal{F}_n)_{n\in\mathbb{N}}$ *un* $\mathbb{N}$*-subconjunto finito de* $\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$ *y* $f \in \bigcup_{n\in\mathbb{N}} \mathrm{Hom}(\mathbb{N}^n, \mathbb{N})$. *Entonces una condición necesaria y suficiente para que* $f \in \mathrm{ARP}(\mathcal{F})$ *es que exista una sucesión de formación para* f *relativa a* $\mathbf{\Sigma}^{\mathrm{rp}}$ *y* $\mathcal{F}$, *i.e., que exista un* $p \in \mathbb{N} - 1$, *y una familia* $(f_i)_{i\in p}$ *en* $\bigcup_{n\in\mathbb{N}} \mathrm{Hom}(\mathbb{N}^n, \mathbb{N})$ *tal que* $f = f_{p-1}$ *y, para cada* $i \in p$, *se cumpla que:*

1. $f_i \in \mathcal{F}_n$, *para algún* $n \in \mathbb{N}$, *o*
2. $f_i = \kappa_{0,0}$, *o*
3. $f_i = \mathrm{sc}$, *o*
4. $f_i = \mathrm{pr}_{1,0}$, *o*
5. $f_i = \mathrm{pr}_{n,j}$, *para algún* $n \geq 2$ *y algún* $j \in n$, *o*
6. f_i *es* $m+1$*-aria y* $f_i = \Omega^m_{\mathrm{R}}(f_j, f_k)$, *para un* j *y un* $k \in i$ *tales que* f_j *sea* m*-aria y* f_k *sea* $m+2$*-aria, o*
7. f_i *es* n*-aria y* $f_i = \Omega^{m,n}_{\mathrm{C}}(f_j, (f_{k_\alpha} \mid \alpha \in m))$, *para un* $m \in \mathbb{N} - 1$, *un* $j \in i$ *y una familia* $(k_\alpha \mid \alpha \in m) \in i^m$ *tal que* f_j *sea* m*-aria y, para cada* $\alpha \in m$, f_{k_α} *sea* n*-aria.*

Demostración. Sea $\mathcal{L}$ el $\mathbb{N}$-subconjunto de $\mathrm{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$ cuya coordenada n-sima, $\mathcal{L}_n$, consta de todas las aplicaciones $f \in \mathrm{Hom}(\mathbb{N}^n, \mathbb{N})$ para las que

existe una sucesión de formación relativa a $\mathbf{\Sigma}^{\mathrm{rp}}$ y $\mathcal{F}$. Puesto que $\mathrm{ARP}(\mathcal{F})$ es la unión de $\overline{\mathcal{F}}$, i.e., la unión del mínimo cerrado de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\star}, \mathbb{N})$ que contiene a $\mathcal{F}$, para demostrar que $\mathrm{ARP}(\mathcal{F}) \subseteq \bigcup_{n\in\mathbb{N}} \mathcal{L}_n$, será suficiente que demostremos que $\mathcal{L}$ es un cerrado de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\star}, \mathbb{N})$ y que contiene a $\mathcal{F}$.

Se cumple que $\mathcal{F} \subseteq_{\mathbb{N}} \mathcal{L}$, porque, dado un $n \in \mathbb{N}$ y un $f \in \mathcal{F}_n$, la familia $(f_i)_{i\in 1}$ con $f_0 = f$, es una sucesión de formación para f. Es evidente que $\kappa_{0,0} \in \mathcal{L}_0$, que sc y $\mathrm{pr}_{1,0} \in \mathcal{L}_1$ y que, para cada $n \geq 2$ y cada $j \in n$, $\mathrm{pr}_{n,j} \in \mathcal{L}_n$. Además, dado un $m \in \mathbb{N} - 1$, un $n \in \mathbb{N}$, un $f \in \mathcal{L}_m$ y una m-familia $(g_j)_{j\in m}$ en $\mathcal{L}_n$, en virtud de la definición de $\mathcal{L}$, tenemos que hay una sucesión de formación $(f_i)_{i\in n_f}$ para f y, para cada $j \in m$, hay una sucesión de formación $(f_{j,i})_{i\in n_j}$ para g_j. Situación que resumimos, parcialmente, mediante la matriz:

$$\begin{pmatrix} f_0 & f_1 & \cdots & f_{n_f-1} = f \\ f_{0,0} & f_{0,1} & \cdots & f_{0,n_0-1} = g_0 \\ f_{1,0} & f_{1,1} & \cdots & f_{1,n_1-1} = g_1 \\ \vdots & \vdots & \ddots & \vdots \\ f_{m-1,0} & f_{m-1,1} & \cdots & f_{m-1,n_{m-1}-1} = g_{m-1} \end{pmatrix}$$

Luego para $n = n_f + \left(\sum_{j\in m} n_j\right) + 1$ y tomando como $(h_i)_{i\in n}$ la familia cuyo último término es $\Omega_{\mathrm{C}}^{m,n}(f, (g_j \mid j \in m))$ y siendo los otros términos los formado por los de la matriz, recorridos de izquierda a derecha y de arriba abajo, se cumple que $(h_i)_{i\in n}$ es una sucesión de formación para $\Omega_{\mathrm{C}}^{m,n}(f, (g_j \mid j \in m))$, luego $\Omega_{\mathrm{C}}^{m,n}(f, (g_j \mid j \in m)) \in \mathcal{L}_n$. Del mismo modo se demuestra que $\mathcal{L}$ está cerrado bajo Ω_{R}^{m}. Por consiguiente $\mathcal{L}$ es un cerrado de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\star}, \mathbb{N})$. De todo ello concluimos que $\mathrm{ARP}(\mathcal{F}) \subseteq \bigcup_{n\in\mathbb{N}} \mathcal{L}_n$.

Demostramos ahora que $\bigcup_{n\in\mathbb{N}} \mathcal{L}_n \subseteq \mathrm{ARP}(\mathcal{F})$. Sea $n \in \mathbb{N}$ y $f \in \mathcal{L}_n$. Entonces, por definición, hay un $p \in \mathbb{N}-1$ y una familia $(f_i)_{i\in p}$ en $\bigcup_{n\in\mathbb{N}} \mathrm{Hom}(\mathbb{N}^n, \mathbb{N})$ tal que $f = f_{p-1}$ y, para cada $i \in p$, se cumple que $f_i \in \mathcal{F}_n$, para algún $n \in \mathbb{N}$, o $f_i = \kappa_{0,0}$, o $f_i = \mathrm{sc}$, o $f_i = \mathrm{pr}_{1,0}$, o $f_i = \mathrm{pr}_{n,j}$, para algún $n \geq 2$ y algún $j \in n$, o f_i es $m+1$-aria y $f_i = \Omega_{\mathrm{R}}^{m}(f_j, f_k)$, para un j y un $k \in i$ tales que f_j sea m-aria y f_k sea $m+2$-aria, o f_i es n-aria y $f_i = \Omega_{\mathrm{C}}^{m,n}(f_j, (f_{k_\alpha} \mid \alpha \in m))$, para un $m \in \mathbb{N} - 1$, un $j \in i$ y una familia $(k_\alpha)_{\alpha\in m} \in i^m$ tal que f_j sea m-aria y, para cada $\alpha \in m$, f_{k_α} sea n-aria.

Demostramos que $f = f_{p-1} \in \mathrm{ARP}(\mathcal{F})$, por inducción sobre $i \in p$. Para $i = 0$, $f_0 \in \mathrm{ARP}(\mathcal{F})$, porque, en este caso, f_0 o bien pertenece a $\mathcal{F}_n$, para algún $n \in \mathbb{N}$, o bien es de la forma $\kappa_{0,0}$, o sc, o $\mathrm{pr}_{1,0}$, o $\mathrm{pr}_{n,j}$, para algún $n \geq 2$ y algún $j \in n$ y entonces $f_0 \in \mathrm{ARP}(\mathcal{F})$, porque $\mathrm{ARP}(\mathcal{F})$ es la unión del mínimo cerrado de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\star}, \mathbb{N})$ que contiene a $\mathcal{F}$. Sea $k \in p$ y supongamos que $\forall i \in k$, $f_i \in \mathrm{ARP}(\mathcal{F})$. Entonces, por definición, $f_k \in \mathcal{F}_n$, para algún $n \in \mathbb{N}$, o $f_k = \kappa_{0,0}$, o $f_k = \mathrm{sc}$, o $f_k = \mathrm{pr}_{1,0}$, o $f_k = \mathrm{pr}_{n,j}$, para algún $n \geq 2$ y algún $j \in n$, o f_k es $m+1$-aria y $f_k = \Omega_{\mathrm{R}}^{m}(f_u, f_v)$, para un u y un $v \in k$ tales que f_u sea m-aria y f_v sea $m+2$-aria, o f_k es n-aria y $f_k = \Omega_{\mathrm{C}}^{m,n}(f_j, (f_{k_\alpha} \mid \alpha \in m))$, para un $m \in \mathbb{N} - 1$, un $j \in k$ y una familia $(k_\alpha)_{\alpha\in m} \in k^m$ tal que f_j sea m-aria y, para cada $\alpha \in m$, f_{k_α} sea n-aria. Es evidente que en los cinco primeros casos $f_k \in \mathrm{ARP}(\mathcal{F})$. En los dos últimos casos también $f_k \in \mathrm{ARP}(\mathcal{F})$, porque al ser, por hipótesis, $f_0, \ldots, f_{k-1} \in \mathrm{ARP}(\mathcal{F})$, también f_u, f_v y $f_{k_0}, \ldots, f_{k_{m-1}} \in \mathrm{ARP}(\mathcal{F})$, luego,

ya que $\mathrm{ARP}(\mathcal{F})$ es la unión del mínimo cerrado de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$ que contiene a $\mathcal{F}$, $f_k = \Omega^m_{\mathrm{R}}(f_u, f_v) \in \mathrm{ARP}(\mathcal{F})$ y $f_k = \Omega^{m,n}_{\mathrm{C}}(f_j, (f_{k_\alpha} \mid \alpha \in m)) \in \mathrm{ARP}(\mathcal{F})$. Así que, para cada $k \in p$, $f_k \in \mathrm{ARP}(\mathcal{F})$, luego, para $k = p - 1$, $f = f_{p-1} \in \mathrm{ARP}(\mathcal{F})$. Por lo tanto $\bigcup_{n\in\mathbb{N}} \mathcal{L}_n \subseteq \mathrm{ARP}(\mathcal{F})$. □

Corolario 1.77. *Sea $f \in \bigcup_{n\in\mathbb{N}} \mathrm{Hom}(\mathbb{N}^n, \mathbb{N})$. Entonces una condición necesaria y suficiente para que $f \in \mathrm{ARP}$ es que exista un $p \in \mathbb{N} - 1$, y una familia $(f_i)_{i\in p}$ en $\bigcup_{n\in\mathbb{N}} \mathrm{Hom}(\mathbb{N}^n, \mathbb{N})$ tal que $f = f_{p-1}$ y, para cada $i \in p$, se cumpla que:*

1. *$f_i = \kappa_{0,0}$, o*
2. *$f_i = \mathrm{sc}$, o*
3. *$f_i = \mathrm{pr}_{1,0}$, o*
4. *$f_i = \mathrm{pr}_{n,j}$, para algún $n \geq 2$ y algún $j \in n$, o*
5. *f_i es $m+1$-aria y $f_i = \Omega^m_{\mathrm{R}}(f_j, f_k)$, para un j y un $k \in i$ tales que f_j sea m-aria y f_k sea $m+2$-aria, o*
6. *f_i es n-aria y $f_i = \Omega^{m,n}_{\mathrm{C}}(f_j, (f_{k_\alpha} \mid \alpha \in m))$, para un $m \in \mathbb{N} - 1$, un $j \in i$ y una familia $(k_\alpha \mid \alpha \in m) \in i^m$ tal que f_j sea m-aria y, para cada $\alpha \in p$, f_{k_α} sea n-aria.*

Corolario 1.78. *El conjunto de las aplicaciones recursivas primitivas es infinito numerable. Por consiguiente, la mayoría de las aplicaciones numericas no son recursivas primitivas.*

Corolario 1.79. *El conjunto de las aplicaciones recursivas primitivas ceroarias es infinito numerable. Además, hay ninguna aplicación recursiva primitiva unaria $g\colon \mathbb{N} \longrightarrow \mathbb{N}$ tal que, para cada $n \in \mathbb{N}$, $g(n) = f_n$, siendo $\{ f_n \mid n \in \mathbb{N} \}$ la imagen de un isomorfismo entre $\mathbb{N}$ y el conjunto de las aplicaciones recursivas primitivas ceroarias.*

Corolario 1.80. *El conjunto de las aplicaciones recursivas primitivas unarias es infinito numerable. Además, no hay ninguna aplicación recursiva primitiva $g\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$ tal que, para cada $n \in \mathbb{N}$, $g(n, -) = f_n$, siendo $\{ f_n \mid n \in \mathbb{N} \}$ la imagen de un isomorfismo entre $\mathbb{N}$ y el conjunto de las aplicaciones recursivas primitivas unarias.*

Demostración. Hay al menos $\aleph_0$ de ellas, porque $\mathrm{id}_{\mathbb{N}}$, sc, sc^2,..., sc^n, ..., son todas recursivas primitivas y dos a dos distintas. hay a lo sumo $\aleph_0$ de ellas, porque son parte de las aplicaciones recursivas primitivas, de las que hay una infinidad numerable.

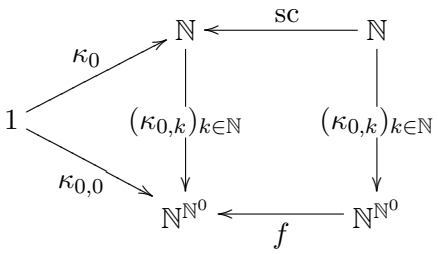
Supongamos que exista una aplicación recursiva primitiva $g\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$ tal que, para cada $n \in \mathbb{N}$, $g(n, -) = f_n$. Entonces la endoaplicación $f = \mathrm{sc} \circ g \circ \langle \mathrm{id}_{\mathbb{N}}, \mathrm{id}_{\mathbb{N}} \rangle$ de $\mathbb{N}$, que a un $n \in \mathbb{N}$ le asigna $g(n, n) + 1$, es recursiva primitiva. Por lo tanto, hay un $n \in \mathbb{N}$, para el que $f = f_n$, así que $f(n) = f_n(n) = g(n, n)$ y $f(n) = g(n, n) + 1$, que es absurdo. □

La segunda parte del corolario anterior se puede generalizar de modo que, para cada número natural $n \geq 1$, no hay ninguna aplicación recursiva primitiva $g\colon \mathbb{N}^{1+n} \longrightarrow \mathbb{N}$ tal que, para cada $x \in \mathbb{N}$, $g(x, -) = f_x$, siendo $\{ f_x \mid x \in \mathbb{N} \}$ la imagen de un isomorfismo entre $\mathbb{N}$ y el conjunto de las aplicaciones recursivas primitivas n-arias. Porque si existiera una aplicación recursiva primitiva $g\colon \mathbb{N}^{1+n} \longrightarrow \mathbb{N}$ tal que, para cada $x \in \mathbb{N}$, $g(x, -) = f_x$,

entonces la aplicación $f = \mathrm{sc} \circ g \circ \langle \mathrm{pr}_{n,0}, \mathrm{pr}_{n,0}, \mathrm{pr}_{n,1}, \ldots, \mathrm{pr}_{n,n-1} \rangle$ de $\mathbb{N}^n$ en $\mathbb{N}$, que a un $(y_j)_{j\in n} \in \mathbb{N}^n$ le asigna $g(y_0, y_0, y_1, \ldots, y_{n-1}) + 1$, es recursiva primitiva. Por lo tanto, hay un $x \in \mathbb{N}$, para el que $f = f_x$, así que, para $(y_j)_{j\in n} = (x)_{j\in n}$, $f(x, \ldots, x) = f_x(x, \ldots, x) = g(x, x, \ldots, x)$ y $f(x, \ldots, x) = g(x, x, \ldots, x) + 1$, que es absurdo.

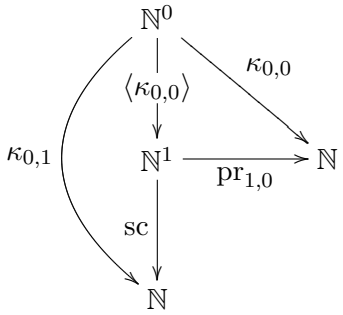
1.8. Algunas aplicaciones recursivas primitivas.

Proposición 1.81. *La familia de aplicaciones $(\kappa_{0,k})_{k\in\mathbb{N}}$, que es la única aplicación de $\mathbb{N}$ en $\mathbb{N}^{\mathbb{N}^0}$ tal que el diagrama:*

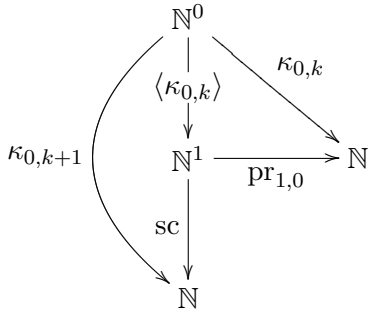


conmuta, siendo f la endoaplicación de $\mathbb{N}^{\mathbb{N}^0}$ que a una aplicación t de $\mathbb{N}^0$ en $\mathbb{N}$ le asigna $\mathrm{sc} \circ \langle t \rangle$, es tal que, para cada $k \in \mathbb{N}$, $\kappa_{0,k}$ es recursiva primitiva.

Demostración. Desde luego $\kappa_{0,0}$ es recursiva primitiva. Por otra parte, la aplicación constante $\kappa_{0,1} \colon \mathbb{N}^0 \longrightarrow \mathbb{N}$, que al único miembro de $\mathbb{N}^0$ le asigna 1, es recursiva primitiva, porque $\kappa_{0,1} = \Omega_{\mathrm{C}}^{1,0}(\mathrm{sc}, (\kappa_{0,0}))$, i.e., $\kappa_{0,1}$ es la composición de $\langle \kappa_{0,0} \rangle$ y sc, o diagramáticamente:



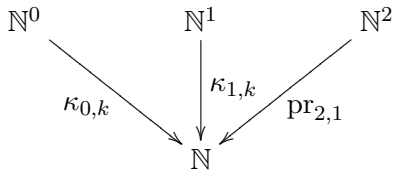
Supongamos que la aplicación constante $\kappa_{0,k} \colon \mathbb{N}^0 \longrightarrow \mathbb{N}$, que al único miembro de $\mathbb{N}^0$ le asigna k, para $k \geq 0$ sea recursiva primitiva. Entonces la aplicación constante $\kappa_{0,k+1} \colon \mathbb{N}^0 \longrightarrow \mathbb{N}$, que al único miembro de $\mathbb{N}^0$ le asigna $k + 1$, es recursiva primitiva, porque $\kappa_{0,k+1} = \Omega_{\mathrm{C}}^{1,0}(\mathrm{sc}, (\kappa_{0,k}))$, i.e., $\kappa_{0,1}$ es la composición de $\langle \kappa_{0,k} \rangle$ y sc, o diagramáticamente:



□

Proposición 1.82. *Para cada $k \in \mathbb{N}$, la aplicación constante $\kappa_{1,k}\colon \mathbb{N}^1 \longrightarrow \mathbb{N}$, que a cualquier miembro de $\mathbb{N}^1$ le asigna k, es recursiva primitiva.*

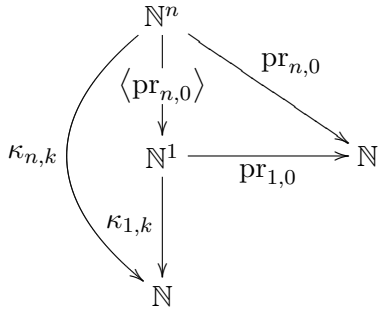
Demostración. Lo es porque $\kappa_{1,k} = \Omega^0_{\mathrm{R}}(\kappa_{0,k}, \mathrm{pr}_{2,1})$, o diagramáticamente:



□

Corolario 1.83. *Para cada $n \geq 2$ y cada $k \in \mathbb{N}$, la aplicación constante $\kappa_{n,k}\colon \mathbb{N}^n \longrightarrow \mathbb{N}$, que a cualquier miembro de $\mathbb{N}^n$ le asigna k, es recursiva primitiva.*

Demostración. Porque $\kappa_{n,k} = \Omega^{1,n}_{\mathrm{C}}(\kappa_{1,k}, (\mathrm{pr}_{n,0}))$, i.e., $\kappa_{n,k}$ es la composición de $\langle \mathrm{pr}_{n,0} \rangle$ y $\kappa_{1,k}$, o diagramáticamente:



□

Con esto queda demostrado que todas las aplicaciones constantes son recursivas primitivas. Ahora bien, si, e.g., respecto de la conjetura de Goldbach, según la cual *cualquier número natural par distinto del* 2 *es la suma de dos números primos*, que todavía no ha sido demostrada, a pesar de que su verdad parece indudable, definimos la endoaplicación f de $\mathbb{N}$ como:

$$f \begin{cases} \mathbb{N} \longrightarrow \mathbb{N} \\ x \longmapsto f(x) = \begin{cases} 1, & \text{si la conjetura es verdadera;} \\ 0, & \text{si la conjetura es falsa,} \end{cases} \end{cases}$$

entonces, en virtud del principio del tercio excluso, f es una aplicación constante (sí, pero ¿cual de ellas?), luego recursiva primitiva. Estamos ante un caso en el que disponemos, por una parte, de un conjunto, el de las aplicaciones recursivas primitivas, exactamente definido y, por otra, de una aplicación, la f, también perfectamente definida, y, en virtud de un principio lógico, está *determinada* la pertenencia al conjunto en cuestión de la aplicación, en este caso, positivamente. Sin embargo, dado el estado actual del conocimiento matemático, no está deductivamente *decidida* tal pertenencia. Esto proyecta sombras de duda acerca de la legitimidad del uso indiscriminado en las matemáticas de las definiciones no efectivas de entidades matemáticas. Al respecto dice N. Cuesta:

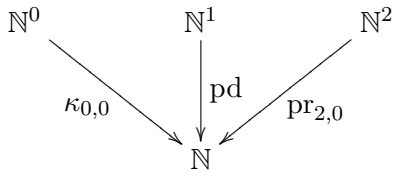
> Difícil es también dar un criterio para discernir las definiciones efectivas de las aparentes. No todos los matemáticos convendrán con Hilbert en que está bien definido el número real, cuyo desarrollo diádico sea
>
> $$0'[2^{\sqrt{2}}][3^{\sqrt{3}}][4^{\sqrt{4}}]\dots$$
>
> y donde $[n^{\sqrt{n}}]$ vale 0, 1, según que, respectivamente, $n^{\sqrt{n}}$ sea racional o irracional.

Proposición 1.84. *La aplicación* $\mathrm{pd}\colon \mathbb{N}^1 \longrightarrow \mathbb{N}$*, de formación del* predecesor *de un número natural, definida como:*

$$\mathrm{pd}\begin{cases} \mathbb{N}^1 \longrightarrow \mathbb{N} \\ x \longmapsto \mathrm{pd}(x) = \begin{cases} 0, & si\ x = 0; \\ y, & si\ x = \mathrm{sc}(y), \end{cases} \end{cases}$$

es recursiva primitiva.

Demostración. Lo es porque $\mathrm{pd} = \Omega^0_{\mathrm{R}}(\kappa_{0,0}, \mathrm{pr}_{2,0})$, o diagramáticamente:



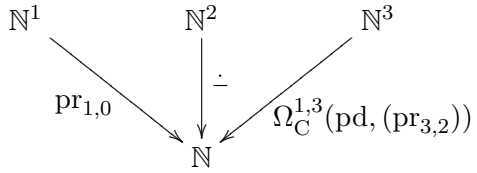
□

Proposición 1.85. *La* diferencia modificada $\dot{-}\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$*, definida como:*

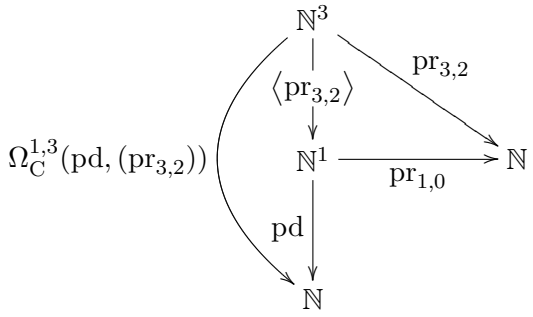
$$\begin{cases} x \dot{-} 0 = x, \\ x \dot{-} \mathrm{sc}(y) = \mathrm{pd}(x \dot{-} y), \quad si\ y \geq 0, \end{cases}$$

es recursiva primitiva.

Demostración. Lo es porque $\dot{-} = \Omega^1_{\mathrm{R}}(\mathrm{pr}_{1,0}, \Omega^{1,3}_{\mathrm{C}}(\mathrm{pd}, (\mathrm{pr}_{3,2})))$, o diagramáticamente:



siendo $\Omega_{\mathrm{C}}^{1,3}(\mathrm{pd}, (\mathrm{pr}_{3,2}))$ la aplicación de $\mathbb{N}^3$ en $\mathbb{N}$ obtenida como:



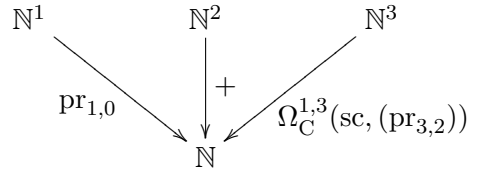
□

Proposición 1.86. *La suma* $+\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$*, definida como:*

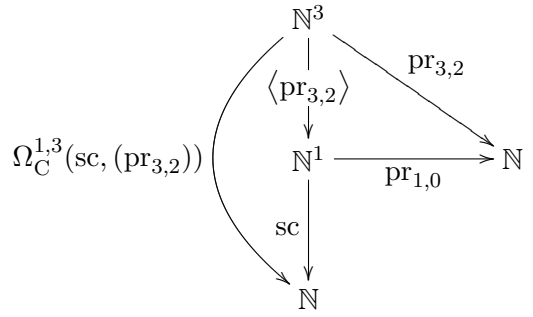
$$\begin{cases} x + 0 = x, \\ x + \mathrm{sc}(y) = \mathrm{sc}(x + y), \quad \textit{si } y \geq 0, \end{cases}$$

es recursiva primitiva.

Demostración. Lo es porque $+ = \Omega_{\mathrm{R}}^{1}(\mathrm{pr}_{1,0}, \Omega_{\mathrm{C}}^{1,3}(\mathrm{sc}, (\mathrm{pr}_{3,2})))$, o diagramáticamente:



siendo $\Omega_{\mathrm{C}}^{1,3}(\mathrm{sc}, (\mathrm{pr}_{3,2}))$ la aplicación de $\mathbb{N}^3$ en $\mathbb{N}$ obtenida como:



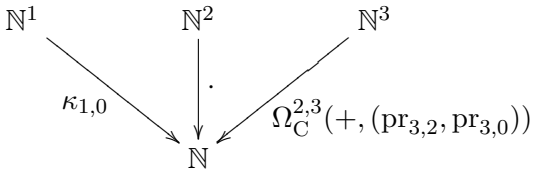
□

Proposición 1.87. *El producto* $\cdot\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$*, definido como:*

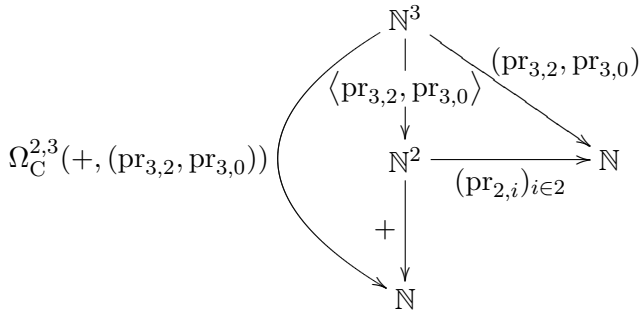
$$\begin{cases} x \cdot 0 = 0, \\ x \cdot \mathrm{sc}(y) = x \cdot y + x, \quad \textit{si } y \geq 0, \end{cases}$$

es una aplicación recursiva primitiva.

Demostración. Lo es porque $\cdot = \Omega^1_{\mathrm{R}}(\kappa_{1,0}, \Omega^{2,3}_{\mathrm{C}}(+, (\mathrm{pr}_{3,2}, \mathrm{pr}_{3,0})))$, o diagramáticamente:



siendo $\Omega^{2,3}_{\mathrm{C}}(+, (\mathrm{pr}_{3,2}, \mathrm{pr}_{3,0}))$ la aplicación de $\mathbb{N}^3$ en $\mathbb{N}$ obtenida como:



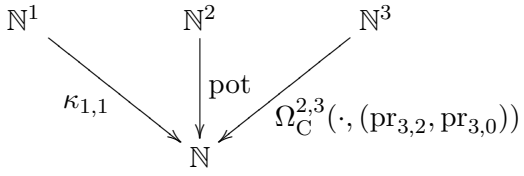
□

Proposición 1.88. *La* potenciación pot$\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$*, definida como:*

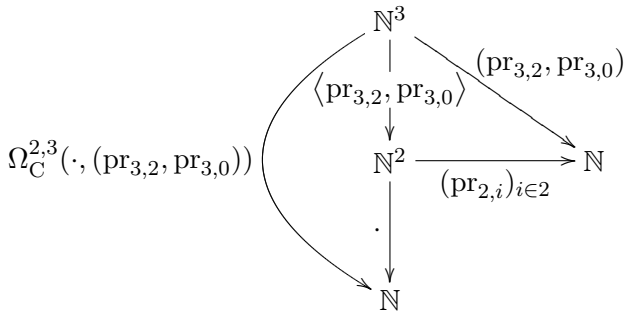
$$\begin{cases} x^0 = 1, \\ x^{\mathrm{sc}(y)} = x^y \cdot x, \quad \textit{si } y \geq 0, \end{cases}$$

es una aplicación recursiva primitiva.

Demostración. Lo es porque pot $= \Omega^1_{\mathrm{R}}(\kappa_{1,1}, \Omega^{2,3}_{\mathrm{C}}(\cdot, (\mathrm{pr}_{3,2}, \mathrm{pr}_{3,0})))$, i.e., se cumple que:



siendo $\Omega^{2,3}_{\mathrm{C}}(\cdot, (\mathrm{pr}_{3,2}, \mathrm{pr}_{3,0}))$ la aplicación de $\mathbb{N}^3$ en $\mathbb{N}$ obtenida como:



□

Proposición 1.89. *Para cada $n \geq 1$ y cada $i \in n$, la aplicación $\mathrm{sc}_{n,i}$ de $\mathbb{N}^n$ en $\mathbb{N}$ que a un $x \in \mathbb{N}^n$ le asigna $\mathrm{sc}(x_i)$, es recursiva primitiva.*

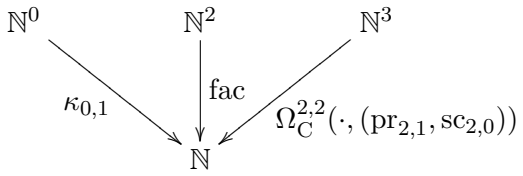
Demostración. Lo es porque $\mathrm{sc}_{n,i} = \Omega_{\mathrm{C}}^{1,n}(\mathrm{sc}, (\mathrm{pr}_{n,i}))$. □

Proposición 1.90. *La aplicación* factorial $\mathrm{fac}\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$*, definida como:*

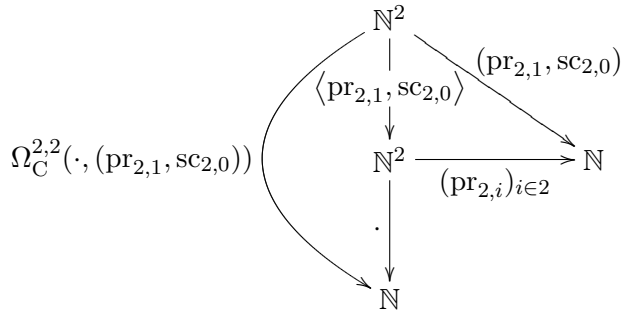
$$\begin{cases} 0! = 1, \\ \mathrm{sc}(y)! = y! \cdot \mathrm{sc}(y), \quad \textit{si } y \geq 0, \end{cases}$$

es una aplicación recursiva primitiva.

Demostración. Lo es porque $\mathrm{fac} = \Omega_{\mathrm{R}}^{0}(\kappa_{0,1}, \Omega_{\mathrm{C}}^{2,2}(\cdot, (\mathrm{pr}_{2,1}, \mathrm{sc}_{2,0})))$, i.e., se cumple que:



siendo $\Omega_{\mathrm{C}}^{2,2}(\cdot, (\mathrm{pr}_{2,1}, \mathrm{sc}_{2,0}))$ la aplicación de $\mathbb{N}^2$ en $\mathbb{N}$ obtenida como:



□

1.9. Relaciones recursivas primitivas.

Ahora que ya disponemos del concepto de aplicación recursiva primitiva y del de aplicación recursiva primitiva relativa a una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\bullet}, \mathbb{N})$, definimos la noción de relación recursiva primitiva y de relación recursiva primitiva relativa a una subálgebra

heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\bullet}, \mathbb{N})$, a través de la aplicación característica de la relación, demostramos que, para cada $n \in \mathbb{N}$, el conjunto de las relaciones recursivas primitivas es un álgebra Booleana que contiene a las relaciones n-arias finitas (y, por lo tanto a las cofinitas) y caracterizamos a las relaciones recursivas primitivas mediante las fibras o conjuntos de nivel de las aplicaciones recursivas primitivas.

Además, demostramos que el sistema de las relaciones recursivas primitivas está cerrado bajo el operador mixto de composición (generalizada), cilindrificaciones, concatenación, los operadores relacionales de cuantificación universal y existencial limitadas, así como que los operadores mixtos de minimización limitada transforman relaciones recursivas primitivas en aplicaciones recursivas primitivas y que un nuevo operador mixto de definición por casos, transforma aplicaciones recursivas primitivas y relaciones recursivas primitivas en aplicaciones recursivas primitivas.

Por otra parte, demostramos que las relaciones recursivas primitivas se conservan bajo las imágenes inversas mediante la aplicación determinada por una familia de aplicaciones recursivas primitivas, que la función subyacente de una aplicación recursiva primitiva es una relación recursiva primitiva y que las fibras de una aplicación recursiva primitiva son relaciones recursivas primitivas.

Por último, demostramos la existencia de situaciones de Cantor recursivas primitivas y de representaciones isomorfas recursivas primitivas entre $\mathbb{N}$ y $\mathbb{N}^{\star}$.

En la definición que sigue, para una relación n-aria R sobre $\mathbb{N}$, convenimos que ch_R, la aplicación característica de R, denota la aplicación de $\mathbb{N}^n$ en $\mathbb{N}$ definida como:

$$\mathrm{ch}_R \begin{cases} \mathbb{N}^n & \longrightarrow \mathbb{N} \\ (x_i \mid i \in n) & \longmapsto \mathrm{ch}_R(x_i \mid i \in n) = \begin{cases} 1, & \text{si } (x_i \mid i \in n) \in R; \\ 0, & \text{en caso contrario.} \end{cases} \end{cases}$$

De modo que ch_R es la composición de $\chi_R \colon \mathbb{N}^n \longrightarrow 2$, el caracter de R, e $\mathrm{in}_2 \colon 2 \longrightarrow \mathbb{N}$, la inclusión canónica de 2 en $\mathbb{N}$.

Definición 1.91. Sea $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\bullet}, \mathbb{N})$ y $R \subseteq \mathbb{N}^n$, i.e., una relación n-aria sobre $\mathbb{N}$. Decimos que R es una relación *recursiva primitiva relativa a* $\mathcal{F}$, o que es una relación *$\mathcal{F}$-recursiva primitiva* si su aplicación característica $\mathrm{ch}_R \in \mathrm{ARP}(\mathcal{F})$. Al conjunto de las relaciones $\mathcal{F}$-recursivas primitivas lo denotamos por $\mathrm{RRP}(\mathcal{F})$.

En particular, decimos que R es una relación *recursiva primitiva* si $\mathrm{ch}_R \in \mathrm{ARP}$. Al conjunto de las relaciones recursivas primitivas lo denotamos por RRP.

Si $\mathcal{F}$ y $\mathcal{G}$ son dos subálgebras heterogéneas finitamente generadas de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\bullet}, \mathbb{N})$ tales que $\mathcal{F} \subseteq \mathcal{G}$ y $R \subseteq \mathbb{N}^n$ es una relación $\mathcal{F}$-recursiva primitiva, entonces R es $\mathcal{G}$-recursiva primitiva. Por consiguiente, para cada subálgebra heterogénea finitamente generada $\mathcal{F}$ de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\bullet}, \mathbb{N})$, se cumple que $\mathrm{RRP} \subseteq \mathrm{RRP}(\mathcal{F})$, i.e., que toda relación recursiva primitiva es $\mathcal{F}$-recursiva primitiva.

Proposición 1.92. *Para cada $n \in \mathbb{N}-1$, el conjunto de las relaciones recursivas primitivas n-arias es infinito numerable. Por consiguiente, la mayoría de las relaciones en $\mathbb{N}$ no son recursivas primitivas.*

Demostración. □

Lema 1.93. *Sea $m \in \mathbb{N}-1$, $n \in \mathbb{N}$, $(f_i)_{i\in m}$ una familia de aplicaciones en la que, para cada $i \in m$, $f_i\colon \mathbb{N}^n \longrightarrow \mathbb{N}$ y Q una relación m-aria en $\mathbb{N}$. Entonces hay una única relación n-aria, obtenida de $f_i\colon \mathbb{N}^n \longrightarrow \mathbb{N}$ y Q por* composición generalizada*, a la que denotamos por $\Pi_{\mathrm{C}}^{m,n}(Q,(f_i)_{i\in m})$, tal que, para cada $x \in \mathbb{N}^n$, una condición necesaria y suficiente para que $x \in \Pi_{\mathrm{C}}^{m,n}(Q,(f_i)_{i\in m})$ es que $(f_i(x) \mid i \in m) \in Q$.*

Demostración. $\Pi_{\mathrm{C}}^{m,n}(Q,(f_i)_{i\in m})$ es $\langle f_i\rangle_{i\in m}^{-1}[Q]$ □

Proposición 1.94. *Sea $m \in \mathbb{N}-1$, $n \in \mathbb{N}$, $(f_i)_{i\in m}$ una familia de aplicaciones en la que, para cada $i \in m$, $f_i\colon \mathbb{N}^n \longrightarrow \mathbb{N}$, Q una relación m-aria y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})$. Si, para cada $i \in m$, f_i es $\mathcal{F}$-recursiva primitiva y Q es una relación $\mathcal{F}$-recursiva primitiva, entonces la relación n-aria $\Pi_{\mathrm{C}}^{m,n}(Q,(f_i)_{i\in m})$ en $\mathbb{N}$ es $\mathcal{F}$-recursiva primitiva.*

Demostración. Porque $\mathrm{ch}_{\Pi_{\mathrm{C}}^{m,n}(Q,(f_i)_{i\in m})} = \Omega_{\mathrm{C}}^{m,n}(\mathrm{ch}_Q,(f_i)_{i\in m})$. □

Corolario 1.95. *Sea $m \in \mathbb{N}-1$, $n \in \mathbb{N}$, $(f_i)_{i\in m}$ una familia de aplicaciones en la que, para cada $i \in m$, $f_i\colon \mathbb{N}^n \longrightarrow \mathbb{N}$, Q una relación m-aria. Si, para cada $i \in m$, f_i es una aplicación recursiva primitiva y Q una relación recursiva primitiva, entonces la relación n-aria $\Pi_{\mathrm{C}}^{m,n}(Q,(f_i \mid i \in m))$ en $\mathbb{N}$ es recursiva primitiva.*

Proposición 1.96. *Sea $n \in \mathbb{N}$, R una relación n-aria en $\mathbb{N}$ y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})$. Si R es $\mathcal{F}$-recursiva primitiva, entonces la* negación *de R, a la que denotamos por $\mathrm{Ng}^n(R)$ y que es la relación n-aria $\mathbb{N}^n - R$ en $\mathbb{N}$, es $\mathcal{F}$-recursiva primitiva.*

Demostración. Porque $\mathrm{ch}_{\mathrm{Ng}^n(R)} = 1 \dot{-} \mathrm{ch}_R$. □

Corolario 1.97. *Sea $n \in \mathbb{N}$ y R una relación n-aria en $\mathbb{N}$. Si R es recursiva primitiva, entonces la relación n-aria $\mathrm{Ng}^n(R)$ en $\mathbb{N}$ es recursiva primitiva.*

Proposición 1.98. *Sea $n \in \mathbb{N}$, P y Q dos relaciones n-arias en $\mathbb{N}$ y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet,\mathbb{N})$. Si P y Q son $\mathcal{F}$-recursivas primitivas, entonces la* conjunción *de P y Q, a la que denotamos por $\mathrm{Cj}^n(P,Q)$ y que es la relación n-aria $P \cap Q$ en $\mathbb{N}$, es $\mathcal{F}$-recursiva primitiva.*

Demostración. □

Corolario 1.99. *Sea $n \in \mathbb{N}$ y P y Q dos relaciones n-arias en $\mathbb{N}$. Si P y Q son recursivas primitivas, entonces la relación n-aria $\mathrm{Cj}^n(P,Q)$ en $\mathbb{N}$ es recursiva primitiva.*

Definición 1.100. Sean m, $n \in \mathbb{N}$ y $\varphi\colon m \longrightarrow n$. Entonces denotamos por Rl^φ la aplicación de $\mathrm{Sub}(\mathbb{N}^m)$ en $\mathrm{Sub}(\mathbb{N}^n)$ que a una relación m-aria R en $\mathbb{N}$ le asigna la relación n-aria $\mathrm{Rl}^\varphi(R)$ en $\mathbb{N}$ definida como:

$$\mathrm{Rl}^\varphi(R) = \{\, x \in \mathbb{N}^n \mid (x_{\varphi(i)} \mid i \in m) \in R \,\}.$$

Además, si φ es inyectiva (resp., sobreyectiva, biyectiva) a los operadores relacionales del tipo Rl^{φ} los denominamos *operadores de expansión* o de *adjunción de variables ficticias* (resp., de *contracción* o de *identificación de variables*, de *permutación de las variables*).

Proposición 1.101. *Sean m, n y $t \in \mathbb{N}$ tales que $t > m, n$, $\alpha\colon m \rightarrowtail t$, $\beta\colon n \rightarrowtail t$, P una relación m-aria en $\mathbb{N}$, Q una relación n-aria en $\mathbb{N}$ y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\bullet}, \mathbb{N})$. Si P y Q son $\mathcal{F}$-recursivas primitivas, entonces la* conjunción generalizada *de P y Q relativa a (α, β, t), a la que denotamos por $\mathrm{Cj}^{m,n}_{\alpha,\beta,t}(P, Q)$ y que es la relación t-aria $\mathrm{Rl}^{\alpha}(P) \cap \mathrm{Rl}^{\beta}(Q)$ en $\mathbb{N}$ es $\mathcal{F}$-recursiva primitiva.*

Demostración. □

Corolario 1.102. *Sean m, n y $t \in \mathbb{N}$ tales que $t > m, n$, $\alpha\colon m \rightarrowtail t$, $\beta\colon n \rightarrowtail t$, P una relación m-aria en $\mathbb{N}$, Q una relación n-aria en $\mathbb{N}$. Si P y Q son recursivas primitivas, entonces la relación t-aria $\mathrm{Cj}^{m,n}_{\alpha,\beta,t}(P, Q)$ en $\mathbb{N}$ es recursiva primitiva.*

Proposición 1.103. *Sea $n \in \mathbb{N}$, P y Q dos relaciones n-arias en $\mathbb{N}$ y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\bullet}, \mathbb{N})$. Si P y Q son $\mathcal{F}$-recursivas primitivas, entonces la* disyunción *de P y Q, a la que denotamos por $\mathrm{Dj}^{n}(P, Q)$ y que es la relación n-aria $P \cup Q$ en $\mathbb{N}$ es $\mathcal{F}$-recursiva primitiva.*

Demostración. □

Corolario 1.104. *Sea $n \in \mathbb{N}$ y P y Q dos relaciones n-arias en $\mathbb{N}$. Si P y Q son recursivas primitivas, entonces la relación n-aria $\mathrm{Dj}^{n}(P, Q)$ en $\mathbb{N}$ es recursiva primitiva.*

Proposición 1.105. *Sean m, n y $t \in \mathbb{N}$ tales que $t > m, n$, $\alpha\colon m \rightarrowtail t$, $\beta\colon n \rightarrowtail t$, P una relación m-aria en $\mathbb{N}$, Q una relación n-aria en $\mathbb{N}$ y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\bullet}, \mathbb{N})$. Si P y Q son $\mathcal{F}$-recursivas primitivas, entonces la* disyunción generalizada *de P y Q relativa a (α, β, t), a la que denotamos por $\mathrm{Dj}^{m,n}_{\alpha,\beta,t}(P, Q)$ y que es la relación t-aria $\mathrm{Rl}^{\alpha}(P) \cup \mathrm{Rl}^{\beta}(Q)$ en $\mathbb{N}$ es $\mathcal{F}$-recursiva primitiva.*

Demostración. □

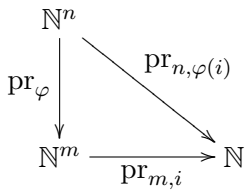
Corolario 1.106. *Sean m, n y $t \in \mathbb{N}$ tales que $t > m, n$, $\alpha\colon m \rightarrowtail t$, $\beta\colon n \rightarrowtail t$, P una relación m-aria en $\mathbb{N}$, Q una relación n-aria en $\mathbb{N}$. Si P y Q son recursivas primitivas, entonces la relación t-aria $\mathrm{Dj}^{m,n}_{\alpha,\beta,t}(P, Q)$ en $\mathbb{N}$ es recursiva primitiva.*

Proposición 1.107. *Sea $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\bullet}, \mathbb{N})$ y $n \in \mathbb{N}$. Entonces el conjunto de las relaciones n-arias en $\mathbb{N}$ $\mathcal{F}$-recursivas primitivas es una subálgebra Booleana del álgebra Booleana $\mathrm{Sub}(\mathbb{N}^{n})$. Además, $\mathrm{Sub}_{\mathrm{fin}}(\mathbb{N}^{n})$ está incluido en tal subálgebra Booleana.*

Demostración. □

Corolario 1.108. *Sea $n \in \mathbb{N}$. Entonces el conjunto de las relaciones n-arias en $\mathbb{N}$ recursivas primitivas es una subálgebra Booleana del álgebra Booleana $\mathrm{Sub}(\mathbb{N}^{n})$. Además, $\mathrm{Sub}_{\mathrm{fin}}(\mathbb{N}^{n})$ está incluido en tal subálgebra Booleana.*

Definición 1.109. Sean m, $n \in \mathbb{N}$ y $\varphi\colon m \longrightarrow n$. Entonces denotamos por pr_φ la única aplicación de $\mathbb{N}^n$ en $\mathbb{N}^m$ tal que, para cada $i \in m$, el diagrama:



conmuta. De modo que pr_φ asigna a cada $x \in \mathbb{N}^n$, la m-tupla $(x_{\varphi(i)})_{i\in m}$.

Proposición 1.110. *Sean q, $r \in \mathbb{N}$ y φ una aplicación estrictamente creciente de q en $r+q$. Entonces hay una única aplicación estrictamente creciente φ^{c}, la* complementaria *de φ, de r en $r+q$ tal que:*

1. $\mathrm{Im}(\varphi) \cap \mathrm{Im}(\varphi^{\mathrm{c}}) = \varnothing$.
2. $\mathrm{Im}(\varphi) \cup \mathrm{Im}(\varphi^{\mathrm{c}}) = r+q$.

Demostración. □

Definición 1.111. Sean q, $r \in \mathbb{N}$, φ una aplicación estrictamente creciente de q en $r+q$ y L una relación r-aria en $\mathbb{N}$. Entonces el *cilindro en $\mathbb{N}^{r+q}$ elevado sobre L a lo largo de los ejes φ*, al que denotamos por $\mathrm{Cyl}_\varphi(L)$, es la imagen inversa de L bajo $\mathrm{pr}_{\varphi^{\mathrm{c}}}$. De modo que:

$$\mathrm{Cyl}_\varphi(L) = \{\, x \in \mathbb{N}^{r+q} \mid (x_{\varphi^{\mathrm{c}}(j)} \mid j \in r) \in L \,\}$$

Proposición 1.112. *Sean q, $r \in \mathbb{N}$, φ una aplicación estrictamente creciente de q en $r+q$, L una relación r-aria en $\mathbb{N}$ y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$. Si L es $\mathcal{F}$-recursiva primitiva, entonces la relación $r+q$-aria $\mathrm{Cyl}_\varphi(L)$ en $\mathbb{N}$ (el cilindro en $\mathbb{N}^{r+q}$ elevado sobre L a lo largo de los ejes φ), es $\mathcal{F}$-recursiva primitiva.*

Demostración. □

Corolario 1.113. *Sean q, $r \in \mathbb{N}$, φ una aplicación estrictamente creciente de q en $r+q$ y L una relación r-aria en $\mathbb{N}$. Si L es recursiva primitiva, entonces la relación $r+q$-aria $\mathrm{Cyl}_\varphi(L)$ en $\mathbb{N}$ (el cilindro en $\mathbb{N}^{r+q}$ elevado sobre L a lo largo de los ejes φ), es recursiva primitiva.*

Proposición 1.114. *Sean m, $n \in \mathbb{N}$, L una relación m-aria en $\mathbb{N}$, M una relación n-aria en $\mathbb{N}$ y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$. Si L y M son $\mathcal{F}$-recursivas primitivas, entonces la concatenación de L y M, $L \curlywedge M$, que es una relación $m+n$-aria en $\mathbb{N}$, es $\mathcal{F}$-recursiva primitiva.*

Demostración. □

Corolario 1.115. *Sean m, $n \in \mathbb{N}$, L una relación m-aria en $\mathbb{N}$ y M una relación n-aria en $\mathbb{N}$. Si L y M son recursivas primitivas, entonces la concatenación de L y M, $L \curlywedge M$, que es una relación $m+n$-aria en $\mathbb{N}$, es recursiva primitiva.*

En lo que sigue convenimos en denotar por Γ_f la función subyacente de una aplicación numérica $f\colon \mathbb{N}^n \longrightarrow \mathbb{N}$, de modo que

$$\Gamma_f = \{\, (x, f(x)) \mid x \in \mathbb{N}^n \,\} = \mathrm{Im}(\langle \mathrm{id}_{\mathbb{N}^n}, f\rangle).$$

Proposición 1.116. *Sea $\mathcal{F} = (\mathcal{F}_n \mid n \in \mathbb{N})$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$ y $f\colon \mathbb{N}^n \longrightarrow \mathbb{N}$. Si f es $\mathcal{F}$-recursiva primitiva, entonces Γ_f, la función subyacente de f, que es un subconjunto de $\mathbb{N}^{n+1}$, es $\mathcal{F}$-recursiva primitiva.*

Demostración. □

Corolario 1.117. *Sea $f \in \mathrm{Hom}(\mathbb{N}^n, \mathbb{N})$. Si f es recursiva primitiva, entonces Γ_f, la función subyacente de f, es recursiva primitiva.*

Hay aplicaciones numéricas cuya función subyacente es una relación recursiva primitiva, pero que no son recursivas primitivas.

Proposición 1.118. *Sea $m \in \mathbb{N}$, $n \in \mathbb{N}-1$, $(f_i)_{i\in n}$ una familia de aplicaciones en la que, para cada $i \in n$, $f_i\colon \mathbb{N}^m \longrightarrow \mathbb{N}$ y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$. Si, para cada $i \in n$, f_i es $\mathcal{F}$-recursiva primitiva, entonces $\Gamma_{\langle f_i\rangle_{i\in n}}$ es $\mathcal{F}$-recursiva primitiva.*

Demostración. □

Corolario 1.119. *Sea $m \in \mathbb{N}$, $n \in \mathbb{N} - 1$ y $(f_i)_{i\in n}$ una familia de aplicaciones en la que, para cada $i \in n$, $f_i\colon \mathbb{N}^m \longrightarrow \mathbb{N}$. Si, para cada $i \in n$, f_i es recursiva primitiva, entonces $\Gamma_{\langle f_i\rangle_{i\in n}}$ es recursiva primitiva.*

Proposición 1.120. *Sea $f\colon \mathbb{N}^n \longrightarrow \mathbb{N}$, $a \in \mathbb{N}$ y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$. Si f es $\mathcal{F}$-recursiva primitiva, entonces $f^{-1}[\{a\}]$, la fibra de f en a, es $\mathcal{F}$-recursiva primitiva.*

Demostración. □

Corolario 1.121. *Sea $f\colon \mathbb{N}^n \longrightarrow \mathbb{N}$, $a \in \mathbb{N}$. Si f es recursiva primitiva, entonces $f^{-1}[\{a\}]$, la fibra de f en a, es recursiva primitiva.*

Proposición 1.122. *Sea $L \subseteq \mathbb{N}^n$ y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$. Entonces una condición necesaria y suficiente para que L sea $\mathcal{F}$-recursiva primitiva es que exista una aplicación $f\colon \mathbb{N}^n \longrightarrow \mathbb{N}$ tal que f sea $\mathcal{F}$-recursiva primitiva y L sea la fibra de f en un $a \in \mathbb{N}$.*

Demostración. □

Corolario 1.123. *Sea $L \subseteq \mathbb{N}^n$. Entonces una condición necesaria y suficiente para que L sea recursiva primitiva es que exista una aplicación $f\colon \mathbb{N}^n \longrightarrow \mathbb{N}$ tal que f sea sea recursiva primitiva y L sea la fibra de f en un $a \in \mathbb{N}$.*

Proposición 1.124. *Sean m, $n \in \mathbb{N}$, $(f_i \mid i \in m)$ una familia de aplicaciones en la que, para cada $i \in m$, $f_i\colon \mathbb{N}^n \longrightarrow \mathbb{N}$ y $(R_i \mid i \in m)$ una familia de relaciones n-arias tal que, para cada i, $j \in m$, si $i \neq j$, entonces $R_i \cap R_j = \varnothing$ y $\bigcup_{i\in m} R_i = \mathbb{N}^n$. Entonces hay una única aplicación n-aria $\Omega^{m,n}_{\mathrm{DC}}((f_i \mid i \in m), (R_i \mid i \in m))$,* definida por casos *a partir de $(f_i \mid i \in m)$ y $(R_i \mid i \in m)$, tal que, para cada $x \in \mathbb{N}^n$,*

$$\Omega^{m,n}_{\mathrm{DC}}((f_i)_{i\in m}, (R_i)_{i\in m})(x) = f_i(x),$$

siendo i el único miembro de m tal que $x \in R_i$.

Demostración. □

Proposición 1.125. *Sean m, $n \in \mathbb{N}$, $(f_i)_{i\in m}$ una familia de aplicaciones en la que, para cada $i \in m$, $f_i\colon \mathbb{N}^n \longrightarrow \mathbb{N}$, $(R_i)_{i\in m}$ una familia de relaciones n-arias tal que, para cada i, $j \in m$, si $i \neq j$, entonces $R_i \cap R_j = \varnothing$ y $\bigcup_{i\in m} R_i = \mathbb{N}^n$ y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$. Si, para cada $i \in m$, f_i es $\mathcal{F}$-recursiva primitiva y R_i es $\mathcal{F}$-recursiva primitiva, entonces $\Omega^{m,n}_{\mathrm{DC}}((f_i)_{i\in m}, (R_i)_{i\in m}) \in \mathcal{F}_n$.*

Demostración. Porque $\Omega^{m,n}_{\mathrm{DC}}((f_i)_{i\in m}, (R_i)_{i\in m}) = f_0 \cdot \mathrm{ch}_{R_0} + \ldots + f_{m-1} \cdot \mathrm{ch}_{R_{m-1}}$. □

Corolario 1.126. *Sean m, $n \in \mathbb{N}$, $(f_i)_{i\in m}$ una familia de aplicaciones en la que, para cada $i \in m$, $f_i\colon \mathbb{N}^n \longrightarrow \mathbb{N}$ y $(R_i)_{i\in m}$ una familia de relaciones n-arias tal que, para cada i, $j \in m$, si $i \neq j$, entonces $R_i \cap R_j = \varnothing$ y $\bigcup_{i\in m} R_i = \mathbb{N}^n$. Si, para cada $i \in m$, f_i es recursiva primitiva y R_i es recursiva primitiva, entonces $\Omega^{m,n}_{\mathrm{DC}}((f_i)_{i\in m}, (R_i)_{i\in m})$ es recursiva primitiva.*

La recursividad primitiva de las relaciones no se conserva, en general, bajo la formación de imágenes directas.

Definición 1.127. Sea $n \in \mathbb{N}$ y $f\colon \mathbb{N}^{n+1} \longrightarrow \mathbb{N}$, entonces:

1. $\sum^{n+1}_{<}(f)$ denota la aplicación de $\mathbb{N}^{n+1}$ en $\mathbb{N}$ definida como:
$$\sum\nolimits^{n+1}_{<}(f) \begin{cases} \mathbb{N}^{n+1} \longrightarrow \mathbb{N} \\ (x, y) \longmapsto \sum(f(x, z) \mid z < y). \end{cases}$$
2. $\sum^{n+1}_{\leq}(f)$ denota la aplicación de $\mathbb{N}^{n+1}$ en $\mathbb{N}$ definida como:
$$\sum\nolimits^{n+1}_{\leq}(f) \begin{cases} \mathbb{N}^{n+1} \longrightarrow \mathbb{N} \\ (x, y) \longmapsto \sum(f(x, z) \mid z \leq y). \end{cases}$$
3. $\prod^{n+1}_{<}(f)$ denota la aplicación de $\mathbb{N}^{n+1}$ en $\mathbb{N}$ definida como:
$$\prod\nolimits^{n+1}_{<}(f) \begin{cases} \mathbb{N}^{n+1} \longrightarrow \mathbb{N} \\ (x, y) \longmapsto \prod(f(x, z) \mid z < y). \end{cases}$$
4. $\prod^{n+1}_{\leq}(f)$ denota la aplicación de $\mathbb{N}^{n+1}$ en $\mathbb{N}$ definida como:
$$\prod\nolimits^{n+1}_{\leq}(f) \begin{cases} \mathbb{N}^{n+1} \longrightarrow \mathbb{N} \\ (x, y) \longmapsto \prod(f(x, z) \mid z \leq y). \end{cases}$$

Proposición 1.128. *Sean $n \in \mathbb{N}$, $f\colon \mathbb{N}^{n+1} \longrightarrow \mathbb{N}$, y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$. Si f es $\mathcal{F}$-recursiva primitiva, entonces $\sum^{n+1}_{<}(f)$, $\sum^{n+1}_{\leq}(f)$, $\prod^{n+1}_{<}(f)$ y $\prod^{n+1}_{\leq}(f)$ son $\mathcal{F}$-recursivas primitivas.*

Demostración. □

Corolario 1.129. *Sean $n \in \mathbb{N}$ y $f\colon \mathbb{N}^{n+1} \longrightarrow \mathbb{N}$. Si f es recursiva primitiva, entonces $\sum^{n+1}_{<}(f)$, $\sum^{n+1}_{\leq}(f)$, $\prod^{n+1}_{<}(f)$ y $\prod^{n+1}_{\leq}(f)$ son recursivas primitivas.*

Definición 1.130. Sea $n \in \mathbb{N}$, entonces:

1. $\exists_<^{n+1}$, el *operador de cuantificación existencial limitado estricto*, es la endoaplicación de $\mathrm{Sub}(\mathbb{N}^{n+1})$ que a una relación $n+1$-aria R en $\mathbb{N}$ le asigna la relación $n+1$-aria
$$\exists_<^{n+1}(R) = \{\, (x,y) \in \mathbb{N}^{n+1} \mid \exists z < y\, ((x,z) \in R) \,\}.$$
2. $\exists_\leq^{n+1}$, el *operador de cuantificación existencial limitado amplio*, es la endoaplicación de $\mathrm{Sub}(\mathbb{N}^{n+1})$ que a una relación $n+1$-aria R en $\mathbb{N}$ le asigna la relación $n+1$-aria
$$\exists_\leq^{n+1}(R) = \{\, (x,y) \in \mathbb{N}^{n+1} \mid \exists z \leq y\, ((x,z) \in R) \,\}.$$
3. $\forall_<^{n+1}$, el *operador de cuantificación universal limitado estricto*, es la endoaplicación de $\mathrm{Sub}(\mathbb{N}^{n+1})$ que a una relación $n+1$-aria R en $\mathbb{N}$ le asigna la relación $n+1$-aria
$$\forall_<^{n+1}(R) = \{\, (x,y) \in \mathbb{N}^{n+1} \mid \forall z < y\, ((x,z) \in R) \,\}.$$
4. $\forall_\leq^{n+1}$, el *operador de cuantificación universal limitado amplio*, es la endoaplicación de $\mathrm{Sub}(\mathbb{N}^{n+1})$ que a una relación $n+1$-aria R en $\mathbb{N}$ le asigna la relación $n+1$-aria
$$\forall_\leq^{n+1}(R) = \{\, (x,y) \in \mathbb{N}^{n+1} \mid \forall z \leq y\, ((x,z) \in R) \,\}.$$

Proposición 1.131. *Sean $n \in \mathbb{N}$, $R \subseteq \mathbb{N}^{n+1}$, y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$. Si R es $\mathcal{F}$-recursiva primitiva, entonces $\exists_<^{n+1}(R)$, $\exists_\leq^{n+1}(R)$, $\forall_<^{n+1}(R)$ y $\forall_\leq^{n+1}(R)$ son $\mathcal{F}$-recursivas primitivas.*

Demostración. □

Corolario 1.132. *Sean $n \in \mathbb{N}$ y $R \subseteq \mathbb{N}^{n+1}$. Si R es recursiva primitiva, entonces $\exists_<^{n+1}(R)$, $\exists_\leq^{n+1}(R)$, $\forall_<^{n+1}(R)$ y $\forall_\leq^{n+1}(R)$ son recursivas primitivas.*

Definición 1.133. Sea $n \in \mathbb{N}$, entonces:

1. $\mu_<^{n+1}$, el *operador de minimización limitado estricto*, es la aplicación de $\mathrm{Sub}(\mathbb{N}^{n+1})$ en $\mathrm{Hom}(\mathbb{N}^{n+1}, \mathbb{N})$ que a una relación $n+1$-aria R en $\mathbb{N}$ le asigna la aplicación
$$\mu_<^{n+1}(R) \begin{cases} \mathbb{N}^{n+1} \longrightarrow \mathbb{N} \\ (x,y) \longmapsto \begin{cases} \min\{\, z < y \mid (x,z) \in R \,\}, & \text{si } \exists z < y\, ((x,z) \in R); \\ 0, & \text{en caso contrario.} \end{cases} \end{cases}$$
2. $\mu_\leq^{n+1}$, el *operador de minimización limitado amplio*, es la aplicación de $\mathrm{Sub}(\mathbb{N}^{n+1})$ en $\mathrm{Hom}(\mathbb{N}^{n+1}, \mathbb{N})$ que a una relación $n+1$-aria R en $\mathbb{N}$ le asigna la aplicación
$$\mu_\leq^{n+1}(R) \begin{cases} \mathbb{N}^{n+1} \longrightarrow \mathbb{N} \\ (x,y) \longmapsto \begin{cases} \min\{\, z \leq y \mid (x,z) \in R \,\}, & \text{si } \exists z \leq y\, ((x,z) \in R); \\ 0, & \text{en caso contrario.} \end{cases} \end{cases}$$

Proposición 1.134. *Sean $n \in \mathbb{N}$, $R \subseteq \mathbb{N}^{n+1}$, y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^\bullet, \mathbb{N})$. Si R es $\mathcal{F}$-recursiva primitiva, entonces $\mu_<^{n+1}(R)$ y $\mu_\leq^{n+1}(R)$ son $\mathcal{F}$-recursivas primitivas.*

Demostración. □

Corolario 1.135. *Sean $n \in \mathbb{N}$ y $R \subseteq \mathbb{N}^{n+1}$. Si R es recursiva primitiva, entonces $\mu^{n+1}_{<}(R)$ y $\mu^{n+1}_{\leq}(R)$ son recursivas primitivas.*

Proposición 1.136. *Sean $n \in \mathbb{N}$, $f\colon \mathbb{N}^n \longrightarrow \mathbb{N}$, y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\bullet}, \mathbb{N})$. Si Γ_f es $\mathcal{F}$-recursiva primitiva y hay una aplicación $\mathcal{F}$-recursiva primitiva $g\colon \mathbb{N}^n \longrightarrow \mathbb{N}$ tal que, para cada $x \in \mathbb{N}^n$, $f(x) \leq g(x)$, entonces f es $\mathcal{F}$-recursiva primitiva.*

Demostración. □

Corolario 1.137. *Sean $n \in \mathbb{N}$ y $f\colon \mathbb{N}^n \longrightarrow \mathbb{N}$. Si Γ_f es recursiva primitiva y hay una aplicación recursiva primitiva $g\colon \mathbb{N}^n \longrightarrow \mathbb{N}$ tal que, para cada $x \in \mathbb{N}^n$, $f(x) \leq g(x)$, entonces f es recursiva primitiva.*

Definición 1.138. Sea $f\colon \mathbb{N} \longrightarrow \mathbb{N}$ y $L \subseteq \mathbb{N}$. Decimos de f que es una *enumeración* de L si $\mathrm{Im}(f) = L$.

Definición 1.139 (Kouznetsov)**.** Sea $f\colon \mathbb{N} \longrightarrow \mathbb{N}$ y L un subconjunto infinito de $\mathbb{N}$. Decimos que f es una *enumeración directa* de L si $\mathrm{Im}(f) = L$ y, además, f es *extensiva*, i.e., para cada $n \in \mathbb{N}$, $n \leq f(n)$.

Proposición 1.140. *Sea L un subconjunto infinito de $\mathbb{N}$, $f\colon \mathbb{N} \longrightarrow \mathbb{N}$ una enumeración directa de L y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\bullet}, \mathbb{N})$. Si f es $\mathcal{F}$-recursiva primitiva, entonces L es $\mathcal{F}$-recursiva primitiva.*

Demostración. □

Corolario 1.141. *Sea L un subconjunto infinito de $\mathbb{N}$ y $f\colon \mathbb{N} \longrightarrow \mathbb{N}$ una enumeración directa de L. Si f es recursiva primitiva, entonces L es recursiva primitiva.*

Definición 1.142. Sean $n \in \mathbb{N} - 1$, $L \subseteq \mathbb{N}^{n+1}$ y $(x, y) \in \mathbb{N}^{n+1}$. Decimos que (x, y) es un *punto inferior* de L (a lo largo del último eje) si $(x, y) \in L$ y, para cada $z \in \mathbb{N}$, si $z < y$, entonces $(x, z) \notin L$. Al conjunto de los puntos inferiores de L lo denotamos por $\mathrm{Inf}^{n+1}(L)$.

Proposición 1.143. *Sean $n \in \mathbb{N} - 1$, $L \subseteq \mathbb{N}^{n+1}$ y $\mathcal{F}$ una subálgebra heterogénea finitamente generada de $\mathbf{H}^{\mathrm{rp}}(\mathbb{N}^{\bullet}, \mathbb{N})$. Si L es $\mathcal{F}$-recursiva primitiva, entonces $\mathrm{Inf}^{n+1}(L)$ es $\mathcal{F}$-recursiva primitiva.*

Demostración. □

Corolario 1.144. *Sean $n \in \mathbb{N} - 1$ y $L \subseteq \mathbb{N}^{n+1}$. Si L es recursiva primitiva, entonces $\mathrm{Inf}^{n+1}(L)$ es recursiva primitiva.*

El conjunto de los números naturales se puede representar como la unión de una infinidad numerable de conjuntos infinito numerables y dos a dos disjuntos, e.g., para la familia $(X_n \mid n \in \mathbb{N})$ de subconjuntos de $\mathbb{N}$ definida como:

$$X_n = \begin{cases} \{0\} \cup \{\, 2k+1 \mid k \in \mathbb{N}\}, & \text{si } n = 0; \\ \{\, 2^n m \mid m \in X_0 - \{0\}\,\}, & \text{si } n \geq 1, \end{cases}$$

se cumple que $\mathbb{N} = \bigcup_{n \in \mathbb{N}} X_n$, que los conjuntos X_n son dos a dos disjuntos y que cada uno de ellos es infinito numerable.

Se cumple que $X_0 \cap X_n = \varnothing$, si $n \geq 1$, porque $0 \notin X_n$ y porque los elementos de X_n son todos pares, ya que empiezan por 2^n, siendo $n \geq 1$. Además, $X_m \cap X_n = \varnothing$, si $m, n \geq 1$ y $m \neq n$, porque, suponiendo que $m < n$, entonces hay un $p \geq 1$ tal que $m + p = n$. Por lo tanto, si $a \in X_m \cap X_n$, $a = 2^m \cdot x$ y $a = 2^n \cdot y$, con x e y impares, luego $2^m \cdot x = 2^m \cdot 2^n \cdot y$, de donde $x = 2^p \cdot y$, pero x es impar y $2^p \cdot y$ es par, que es una contradicción.

Definición 1.145. Sea f es una endoaplicación de $\mathbb{N}$. Decimos que f es una aplicación de *gran amplitud* si para cada $n \in \mathbb{N}$, hay un $M \subseteq \mathbb{N}$ tal que $\operatorname{card}(M) = \aleph_0$ y para cada $m \in M$, $f(m) = n$.

Puesto que $\mathbb{N} = \bigcup_{n \in \mathbb{N}} X_n$, siendo los conjuntos X_n infinito numerables y dos a dos disjuntos, la endoaplicación f de $\mathbb{N}$ que a un $x \in \mathbb{N}$ le asigna el único $n \in \mathbb{N}$ tal que $x \in X_n$, es una aplicación de gran amplitud.

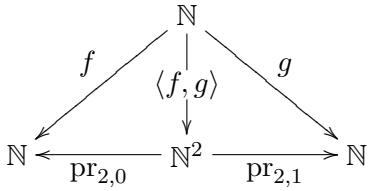
Proposición 1.146. *Sea f es una endoaplicación de $\mathbb{N}$. Entonces son equivalentes:*

1. *f es una aplicación de gran amplitud.*
2. *Para cada $n \in \mathbb{N}$, $\operatorname{card}(f^{-1}[\{n\}]) = \aleph_0$.*
3. *Hay una relación de equivalencia Φ sobre $\mathbb{N}$ tal que, para cada $n \in \mathbb{N}$, $\operatorname{card}([n]_\Phi) = \aleph_0$.*

Demostración. □

Proposición 1.147. *Sean $f, g \colon \mathbb{N} \longrightarrow \mathbb{N}$ dos aplicaciones tales que la aplicación $\langle f, g \rangle : \mathbb{N} \longrightarrow \mathbb{N}^2$ sea sobreyectiva. Entonces f y g son aplicaciones de gran amplitud, i.e., son sobreyectivas y con todas las fibras infinitas.*

Demostración. Recordemos que $\langle f, g \rangle$ es la única aplicación de $\mathbb{N}$ en $\mathbb{N}^2$ tal que el diagrama:



conmuta. Puesto que $\mathrm{pr}_{2,0}$ y $\mathrm{pr}_{2,1}$ son sobreyectivas, f y g también lo son.

Nos limitamos a demostrar que f tiene todas las fibras infinitas, debido a que el argumento para demostrar lo mismo de g, es idéntico. Supongamos que no sea ese el caso, i.e., que exista un $n \in \mathbb{N}$ tal que $f^{-1}[n] = \{ x_{n,0}, \ldots, x_{n,p-1} \}$, con $p > 0$. Entonces, para cada $i \in p$, $\langle f, g \rangle (x_{n,i}) = (n, g(x_{n,i}))$. Veamos que hay un $(x, y) \in \mathbb{N}^2$ tal que, para cada $k \in \mathbb{N}$, $\langle f, g \rangle (k) \neq (x, y)$. En efecto, sea y un número natural distinto de $g(x_{n,\alpha})$, para cada $i \in p$, entonces para $(x, y) = (n, y)$, tenemos que, para cada $k \in \mathbb{N}$, $\langle f, g \rangle (k) \neq (n, y)$, porque si, para algún $k \in \mathbb{N}$, tuviéramos que $\langle f, g \rangle (k) = (n, y)$, entonces, por ser $\langle f, g \rangle (k) = (f(k), g(k))$, tendríamos que $f(k) = n$ y $g(k) = y$, luego, de $f(k) = n$, que k debería ser igual a uno de entre los elementos de $f^{-1}[n]$, por ejemplo a $x_{n,i}$, y entonces que $g(x_{n,i}) = y$, pero eso es imposible, ya que, para cada $i \in p$, $g(x_{n,i}) \neq y$. □

Corolario 1.148. *Sea $m \in \mathbb{N}$ tal que $m \geq 2$ y $(f_i)_{i \in m}$ una familia de aplicaciones tal que, para cada $i \in m$, f_i sea una endoaplicación de $\mathbb{N}$. Si*

$\langle f_i \rangle_{i\in m} : \mathbb{N} \longrightarrow \mathbb{N}^m$ es sobreyectiva, entonces, para cada $i \in m$, f_i es una aplicación de gran amplitud.

Demostración. □

Teorema 1.149 (Kouznetsov)**.** *Si f es una endoaplicación de $\mathbb{N}$ de gran amplitud, entonces existe una endoaplicación g de $\mathbb{N}$ tal que $\langle f, g\rangle$ es un isomorfismo de $\mathbb{N}$ en $\mathbb{N}^2$. Además, en virtud de la proposición anterior, g es una aplicación de gran amplitud.*

Demostración. Sea $n \in \mathbb{N}$, arbitrario pero fijo. Puesto que f es una endoaplicación de gran amplitud, la fibra de f en n, que es un conjunto infinito numerable, se puede representar, supuesta elejida una biyección de $\mathbb{N}$ en tal fibra, como $f^{-1}[n] = \{\, x_{n,i} \mid i \in \mathbb{N}\}$. Sea entonces g_n la aplicación de $f^{-1}[n]$ en $\mathbb{N}$ definida como $g(x_{n,i}) = i$, para cada $i \in \mathbb{N}$. Puesto que $\mathbb{N} = \bigcup_{n\in\mathbb{N}} f^{-1}[n]$, o gráficamente:

$$\mathbb{N} = \begin{pmatrix} x_{0,0}, & x_{0,1}, & x_{0,2}, & \dots, & x_{0,i}, \dots \\ x_{1,0}, & x_{1,1}, & x_{1,2}, & \dots, & x_{1,i}, \dots \\ \dots, & \dots, & \dots, & \dots, & \dots, \dots \\ x_{n,0}, & x_{n,1}, & x_{n,2}, & \dots, & x_{n,i}, \dots \\ \dots, & \dots, & \dots, & \dots, & \dots, \dots \end{pmatrix}$$

y dos filas distintas son disjuntas, definimos la endoaplicación g de $\mathbb{N}$ como la única para la que cada uno de los diagramas:

$$\begin{array}{ccc} f^{-1}[n] & \xrightarrow{\mathrm{in}_n} & \bigcup_{n\in\mathbb{N}} f^{-1}[n] \\ & \searrow^{g_n} & \downarrow g \\ & & \mathbb{N} \end{array}$$

conmuta. Es evidente que entonces $\langle f, g\rangle$ es biyectiva. □

Proposición 1.150. *Si f es una endoaplicación de $\mathbb{N}$ recursiva primitiva y de gran amplitud, entonces hay una endoaplicación g de $\mathbb{N}$ recursiva primitiva tal que $\langle f, g\rangle$ es una biyección de $\mathbb{N}$ en $\mathbb{N}^2$.*

Demostración. □

Proposición 1.151. *Sea $m \geq 1$. Entonces hay situaciones de Cantor para m que son recursivas primitivas, i.e., hay un par ordenado $(\gamma^m, (\gamma^m_j)_{j\in m})$ en el que γ^m es una aplicación recursiva primitiva de $\mathbb{N}^m$ en $\mathbb{N}$ y, para cada $j \in m$, γ^m_j una endoaplicación recursiva primitiva de $\mathbb{N}$ tal que:*

1. $\gamma^m \circ \langle \gamma^m_j \rangle_{j\in m} = \mathrm{id}_{\mathbb{N}}$.
2. $\langle \gamma^m_j \rangle_{j\in m} \circ \gamma^m = \mathrm{id}_{\mathbb{N}^m}$.

Además, hay situaciones de Cantor para m recursivas primitivas $(\gamma^m, (\gamma^m_j)_{j\in m})$ tales que:

1. *Para cada $j \in m$ y para cada $n \in \mathbb{N}$, $\gamma^m_j(n) \leq n$.*
2. *Hay una aplicación recursiva primitiva $\pi\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$ tal que, para cada $x \in \mathbb{N}$ y cada $y \in \mathbb{N}$, si, para cada $j \in m$, $x_j \leq y$, entonces $\gamma^m(x) \leq \pi(y, m)$.*

Demostración. □

Proposición 1.152. *Sea $m \geq 1$. Si tanto $(\gamma^m, (\gamma_j^m)_{j\in m})$ como $(\overline{\gamma}^m, (\overline{\gamma}_j^m)_{j\in m})$ son situaciones de Cantor para m recursivas primitivas, entonces hay una endoaplicación recursiva primitiva η de $\mathbb{N}$ tal que $\eta \circ \gamma^m = \overline{\gamma}^m$.*

Demostración. □

Proposición 1.153. *Hay una biyección (natural) entre el conjunto de las aplicaciones ξ de $\mathbb{N} - 1$ en $\mathbb{N}^\star - \{\lambda\}$ y el conjunto de los pares ordenados (ξ_0, ξ_1) en los que ξ_0 es una endoaplicación parcial de $\mathbb{N}$ tal que $\mathrm{Dom}(\xi_0) = \mathbb{N} - 1$ y, para cada $t \in \mathrm{Dom}(\xi_0)$, $\xi_0(t) \geq 1$ y ξ_1 una aplicación parcial de $\mathbb{N}^2$ en $\mathbb{N}$ tal que $\mathrm{Dom}(\xi_1) = \bigcup_{t\in\mathbb{N}-1}\{t\} \times \xi_0(t)$. Por consiguiente hay una biyección (natural) entre el conjunto de las aplicaciones ξ de $\mathbb{N}$ en $\mathbb{N}^\star$ tales que $\xi(0) = \lambda$ y el mismo conjunto de pares ordenados de aplicaciones parciales.*

Demostración. □

Definición 1.154. Sea ξ una aplicación de $\mathbb{N}$ en $\mathbb{N}^\star$ tal que $\xi(0) = \lambda$. Decimos que ξ es una *representación recursiva primitiva de $\mathbb{N}$ en $\mathbb{N}^\star$* si el par ordenado (ξ_0, ξ_1), que le corresponde, en virtud de la biyección (natural) anterior, es tal que hay un par ordenado $(\overline{\xi}_0, \overline{\xi}_1)$ de aplicaciones recursivas primitivas, con $\overline{\xi}_0 \colon \mathbb{N} \longrightarrow \mathbb{N}$ y $\overline{\xi}_1 \colon \mathbb{N}^2 \longrightarrow \mathbb{N}$, para el que se cumple que:

1. Para cada $t \in \mathbb{N}$, $\overline{\xi}_0(t) = \xi_0(t)$.
2. Para cada $t \in \mathbb{N} - 1$ y cada $j \in \xi_0(t)$, $\overline{\xi}_1(t, j) = \xi_1(t, j)$

Proposición 1.155. *Hay una biyección (natural) entre el conjunto de las biyecciones η de $\mathbb{N}^\star$ en $\mathbb{N}$ tales que $\eta(\lambda) = 0$ y el conjunto de los pares ordenados (η_0, η_1) en los que η_0 es una endoaplicación inyectiva de $\mathbb{N}$ tal que, para cada $x \in \mathbb{N}$, $\eta_0(x) \neq 0$ y η_1 una aplicación sobreyectiva de $\mathbb{N}^2$ en $\mathbb{N}$ tal que, para cada $x, y \in \mathbb{N}$, $\eta_1(x, y) = 0$ si y sólo si $x = 0$ e $y = 0$.*

Demostración. □

Definición 1.156. Sea η una aplicación de $\mathbb{N}^\star$ en $\mathbb{N}$ tal que $\eta(\lambda) = 0$. Decimos que η es una *representación recursiva primitiva de $\mathbb{N}^\star$ en $\mathbb{N}$* si el par ordenado (η_0, η_1), que le corresponde, en virtud de la biyección (natural) anterior, es tal que η_0 y η_1 son aplicaciones recursivas primitivas.

Definición 1.157. Sea ξ una aplicación de $\mathbb{N}$ en $\mathbb{N}^\star$ y η una aplicación de $\mathbb{N}^\star$ en $\mathbb{N}$. Decimos que (ξ, η) es una *representación isomorfa recursiva primitiva entre $\mathbb{N}$ y $\mathbb{N}^\star$* si $\eta \circ \xi = \mathrm{id}_{\mathbb{N}}$, $\xi \circ \eta = \mathrm{id}_{\mathbb{N}^\star}$, ξ es una representación recursiva primitiva de $\mathbb{N}$ en $\mathbb{N}^\star$ y η una representación recursiva primitiva de $\mathbb{N}^\star$ en $\mathbb{N}$.

Proposición 1.158. *Hay una representación isomorfa recursiva primitiva entre $\mathbb{N}$ y $\mathbb{N}^\star$.*

Demostración. □