Carlos Ivorra Castillo

SUPERFICIES ARITMÉTICAS

CON APLICACIONES A LA TEORÍA DE CURVAS ELÍPTICAS

Rideo hominem unius libri

Índice General

Introducción **ix**

1 Anillos excelentes 1

Capítulo I: Preliminares **3**
1.1 La descomposición primaria 3
1.2 El teorema chino del resto 8
1.3 Anillos íntegramente cerrados 9
1.4 Módulos fielmente planos 15
1.5 Conjuntos constructibles 17

Capítulo II: Anillos locales completos **23**
2.1 Suavidad formal 23
2.2 Los teoremas de estructura 30
2.3 El criterio jacobiano de Nagata 37
2.4 Suavidad formal y formas diferenciales 48

Capítulo III: Anillos excelentes **53**
3.1 Anillos universalmente catenarios 53
3.2 Anillos de Nagata 59
3.3 Las propiedades J 68
3.4 Homomorfismos suaves 75
3.5 La propiedad G 80
3.6 Anillos y esquemas excelentes 87

2 Superficies aritméticas 93

Capítulo IV: Preliminares **95**
4.1 Curvas planas 95
4.2 Divisores 100
4.3 Cónicas 109
4.4 Curvas elípticas 119

Capítulo V: Superficies fibradas **125**
5.1 Modelos de curvas 125
5.2 Explosiones 135
5.3 La geometría de las superficies fibradas 154
5.4 Un ejemplo de desingularización 159

Capítulo VI: Superficies regulares **169**
6.1 Intersecciones de curvas 169
6.2 Aplicaciones birracionales 182
6.3 Resolución de singularidades 190

Capítulo VII: Superficies minimales **201**
7.1 Equivalencia birracional de superficies 202
7.2 Superficies relativamente minimales 204
7.3 Superficies minimales 217
7.4 Desingularizaciones minimales 220
7.5 La estructura de grupo de una curva elíptica 223

Capítulo VIII: Modelos de curvas elípticas **231**
8.1 Modelos de Weierstrass 231
8.2 El modelo regular minimal 245
8.3 El modelo de Weierstrass minimal 251
8.4 Reducción de curvas elípticas 258
8.5 Reducción del modelo regular minimal 260

Capítulo IX: El algoritmo de Tate **271**
9.1 Descripción del algoritmo 271
9.2 Inicio de la prueba 274
9.3 Conclusión del paso 2 279
9.4 Los pasos intermedios 283
9.5 Conclusión del paso 7 287
9.6 Los pasos finales 291
9.7 El caso $\operatorname{car} k > 3$ 300
9.8 Reducción y cambios de base 303

Capítulo X: El modelo de Néron **311**
10.1 El esquema de componentes conexas 311
10.2 Cambios de base planos 321
10.3 Esquemas de grupos 326
10.4 El modelo de Néron 333
10.5 Propiedades del modelo de Néron 344

3 Aplicaciones 353

Capítulo XI: Caracteres de grupos 355
11.1 Representaciones lineales de grupos 357
11.2 Caracteres 362
11.3 Caracteres complejos 369
11.4 Caracteres inducidos 374
11.5 El teorema de Brauer 380
11.6 Caracteres en grupos cociente 386
11.7 Complementos 387

Capítulo XII: Curvas de Tate 393
12.1 Curvas elípticas complejas 394
12.2 La curva de Tate 399
12.3 La suprayectividad de la aplicación de Tate 406
12.4 Curvas con reducción multiplicativa 410

Capítulo XIII: Subgrupos de torsión 419
13.1 Preliminares sobre cuerpos métricos 420
13.2 Módulos de Tate 426
13.3 El criterio de Néron-Ogg-Shafarevich 430
13.4 El carácter de Artin 436
13.5 El invariante de Swan 444
13.6 El conductor de una curva elíptica 451

Bibliografía 453

Índice de Materias 454

Introducción

El propósito de este libro es profundizar en el estudio de las curvas elípticas a través de lo que podríamos considerar una generalización de la noción de reducción. Recordemos que una *curva elíptica* E/K sobre un cuerpo K es una curva proyectiva regular de género 1 definida sobre K en la que hemos seleccionado un punto racional $O \in E(K)$. Es conocido que toda curva elíptica es isomorfa a una cúbica dada por una *ecuación de Weierstrass:*

$$Y^2 + a_1XY + a_3Y^2 = X^3 + a_2X^2 + a_4X + a_6,$$

para ciertos $a_i \in K$, de modo que el punto racional prefijado O se corresponde con el único punto infinito de esta curva, a saber, el punto de coordenadas homogéneas $O = [0, 1, 0]$.

En este libro estudiaremos el caso en que K es el cuerpo de cocientes de un dominio de Dedekind D. (El ejemplo básico es $\mathbb{Q}$ como cuerpo de cocientes de $\mathbb{Z}$.) Entonces es posible elegir la ecuación de Weierstrass de modo que tenga sus coeficientes en D y, para cada ideal primo (no nulo) $\mathfrak{p}$ de D, podemos considerar su *reducción* módulo $\mathfrak{p}$, es decir, la ecuación de Weierstrass cuyos coeficientes son las clases de los coeficientes a_i en el cuerpo de restos $k = D/\mathfrak{p}$.

La reducción de una curva elíptica ya no tiene por qué ser una curva elíptica. Ello se debe a que puede tener un punto singular. En general, cada ecuación de Weierstrass tiene asociado un *discriminante* $\Delta \in K$ (que depende polinómicamente de los coeficientes a_i, por lo que estará en D si éstos están), de modo que la curva definida por la ecuación es regular (y automáticamente elíptica) si y sólo si $\Delta \neq 0$. El discriminante de la reducción de E módulo un primo $\mathfrak{p}$ es la clase de Δ módulo $\mathfrak{p}$, por lo que la reducción será una curva elíptica si y sólo si $\mathfrak{p} \nmid \Delta$.

Esto nos permite ya distinguir clases de curvas elípticas según su comportamiento ante la reducción módulo un primo $\mathfrak{p}$: una curva elíptica puede tener *buena* o *mala reducción* módulo $\mathfrak{p}$, según que la reducción sea o no elíptica.[1] Entre las curvas con mala reducción se pueden dividir en varias clases atendiendo al punto singular de la reducción. (Sólo puede haber uno.) La mala reducción es *multiplicativa* si el punto singular es un *nodo,* es decir, que tiene dos tangentes distintas o, equivalentemente, si al considerar la regularización de la curva le

[1] En realidad esto ha de matizarse, porque una misma curva elíptica puede describirse con ecuaciones de Weierstrass distintas, y puede ocurrir que una tenga buena reducción y otra tenga mala reducción en un mismo primo.

aparecen dos antiimágenes distintas. Si, por el contrario, el punto singular es una *cúspide,* es decir, que tiene una única tangente y una única antiimagen en la regularización, decimos que la mala reducción es *aditiva.* A su vez, todavía es posible distinguir entre curvas con mala reducción multiplicativa *racional* o *irracional* (distinción que no vamos a explicar aquí).

Con esto termina la clasificación de las reducciones de una curva elíptica que proporciona la teoría elemental. Como decíamos, nuestro propósito es llevar esta clasificación mucho más lejos. El lector que esté familiarizado con la utilidad del concepto de reducción y de la distinción entre los distintos tipos de reducciones a la hora de comprender el comportamiento de las curvas elípticas, se podrá hacer una primera idea del potencial que ofrece avanzar en esta dirección.

La idea básica que vamos a explotar es la siguiente: en principio, una ecuación de Weierstrass define un esquema proyectivo

$$C = \mathrm{Proy}(K[X,Y,Z]/(F)),$$

donde F es la homogeneización de la ecuación de Weierstrass. Enfocar de este modo el estudio de la curva definida por la ecuación —en términos de la teoría de esquemas— puede ser más o menos provechoso, pero, en último extremo, el estudio del esquema C/K es equivalente al estudio de la curva E/K en términos clásicos, es decir, concebida como un subconjunto cerrado del plano proyectivo $\mathrm{P}^2(\bar{K})$, donde $\bar{K}$ es la clausura algebraica de K. La idea que realmente aporta algo nuevo es considerar el esquema W

$$W = \mathrm{Proy}(D[X,Y,Z]/(F)).$$

Si $S = \mathrm{Esp}\, D$, el homomorfismo natural $D \longrightarrow D[X,Y,Z]/(F)$ induce un homomorfismo de esquemas $W \longrightarrow S$. Los puntos de S son el punto genérico η (el ideal nulo de D) y tantos puntos cerrados como ideales primos (no nulos) tiene D. Como $k(\eta) = D_0 = K$, resulta que la *fibra genérica* de W es

$$W_\eta = \mathrm{Proy}(K[X,Y,Z]/(F)),$$

es decir, la curva elíptica definida por la ecuación de Weierstrass, mientras que si $\mathfrak{p} \in D$ es un primo no nulo, entonces $k(\mathfrak{p}) = D_\mathfrak{p}/\mathfrak{p} = D/\mathfrak{p}$ es el cuerpo de restos módulo $\mathfrak{p}$, y la fibra correspondiente es

$$W_\mathfrak{p} = \mathrm{Proy}(k(\mathfrak{p})[X,Y,Z]/(F)),$$

la reducción de la ecuación de Weierstrass módulo $\mathfrak{p}$.

El esquema W es un ejemplo de lo que llamaremos una *superficie fibrada,* uno de los conceptos básicos que vamos a estudiar en este libro. Notemos que el nombre de "superficie" le conviene en cuanto que es un esquema de dimensión 2, aunque es más bien lo que podríamos llamar un haz de curvas. Más concretamente, es lo que llamaremos un *modelo de Weierstrass* de la curva elíptica dada (el modelo de Weierstrass asociado a la ecuación dada). Vemos que reúne en un único objeto geométrico la curva y sus reducciones, pero no se trata de una mera "catalogación" de las reducciones, sino que al relacionarlas

de este modo podemos distinguir diferencias más sutiles entre los tipos de mala reducción. En realidad, no tiene interés relacionar reducciones de una misma ecuación módulo primos diferentes, por lo que, a la hora de estudiar la reducción $W_\mathfrak{p}$, podemos sustituir D por la localización $D_\mathfrak{p}$ sin alterar la fibra $W_\mathfrak{p}$. Así el esquema $S = \operatorname{Esp} D_\mathfrak{p}$ tiene sólo dos puntos, el punto genérico η y el punto cerrado $\mathfrak{p}$, y tenemos una superficie fibrada W que tiene únicamente dos fibras.

Si la reducción módulo $\mathfrak{p}$ es mala, ahora puede ocurrir que el punto singular de $W_\mathfrak{p}$ sea también singular como punto de W o que, por el contrario, sea regular. En el primer caso es posible construir una *desingularización* de W, es decir, una superficie fibrada regular X/S, cuya fibra genérica sigue siendo la misma (la curva elíptica dada), junto con un homomorfismo birracional $X \longrightarrow W$.

En principio, hay muchas superficies fibradas regulares no isomorfas cuya fibra genérica sea una curva elíptica dada, pero, de entre todas ellas, es posible seleccionar una de forma canónica, la que llamaremos el *modelo regular minimal* de la curva elíptica. Si X/S es dicho modelo regular minimal, la fibra cerrada $X_\mathfrak{p}$ puede variar entre un número finito de posibilidades, que suponen una clasificación mucho más fina de los tipos de reducción módulo $\mathfrak{p}$ de la curva.

Del proceso que acabamos de esbozar y que conduce al modelo regular minimal de una curva elíptica, el paso más delicado es —con diferencia— el problema de *desingularizar* una superficie fibrada dada. Es bien conocido que toda curva proyectiva es birracionalmente equivalente a una curva proyectiva regular, pero el análogo en dimensiones superiores es un problema muy complejo del que se conocen diversos resultados parciales. En este libro aceptaremos sin demostración un teorema de Lipman (teorema 6.31) sobre desingularización de superficies excelentes, a partir del cual demostraremos los resultados específicos de desingularización que vamos a necesitar. El mero enunciado del teorema requiere conocer el concepto de *anillo excelente,* el cual determina una familia de anillos noetherianos que incluye a las álgebras finitamente generadas sobre un cuerpo y comparte con ellas algunas propiedades fundamentales. Se trata de un concepto técnico muy sofisticado del álgebra conmutativa. Por ello, este libro está estructurado del modo siguiente:

En una primera parte, que incluye los tres primeros capítulos, exponemos la teoría de los anillos excelentes. Más concretamente, el primer capítulo recoge algunos preliminares de álgebra conmutativa de carácter más elemental, en el segundo capítulo exponemos algunos requisitos más profundos, y en el tercero presentamos las distintas propiedades que componen la definición de los anillos excelentes, que son finalmente introducidos y estudiados en la última sección.

La segunda parte, hasta el capítulo VIII, desarrolla la teoría que hemos esbozado en esta introducción, de forma que el lector que esté dispuesto a aceptar sin prueba no sólo el teorema de Lipman, sino todo lo concerniente a la existencia de desingularizaciones (esencialmente, los teoremas 6.34 y 6.35), puede empezar directamente por el capítulo IV, salvo que necesitará unos pocos preliminares de álgebra conmutativa incluidos en la primera parte, a saber, la sección 3.1 sobre anillos universalmente catenarios (que es independiente de todo lo anterior) y

unos pocos resultados elementales del capítulo I (que puede consultar a medida que vayan siendo necesarios).

Excepto el teorema de Lipman, todos los resultados de este libro están demostrados a partir de resultados anteriores o de resultados demostrados en otros de mis libros, citados entre corchetes con los convenios siguientes:

[N]	*Teoría de números*
[CE]	*Curvas elípticas*
[AC]	*Álgebra conmutativa*
[E]	*Esquemas*

Queda claro, pues, que el lector deberá tener una buena base de álgebra conmutativa y teoría de esquemas, así como algunos conocimientos sobre curvas elípticas. Las referencias a [N] se reducen a las propiedades básicas de los dominios de Dedekind.

En el capítulo IX presentamos un algoritmo debido a Tate que permite calcular explícitamente las fibras cerradas del modelo regular minimal de una curva elíptica a partir de cualquiera de sus ecuaciones de Weierstrass. En el capítulo X estudiamos la posibilidad de extender al modelo regular minimal la estructura de variedad abeliana de una curva elíptica. La respuesta es negativa, pero sucede que sí que es posible dotar de estructura de grupo al abierto de puntos suaves del modelo regular minimal. Este abierto recibe el nombre de *modelo de Néron* de la curva elíptica, y puede caracterizarse por una propiedad universal de extensión de homomorfismos.

Los últimos capítulos del libro se agrupan en una tercera parte de aplicaciones a las curvas elípticas de la teoría desarrollada previamente. Básicamente, esta tercera parte contiene lo necesario para definir y demostrar las propiedades básicas del conductor de una curva elíptica, un concepto demasiado técnico para tratar de explicarlo aquí, pero que ocupa, sin lugar a dudas, un lugar destacado en la teoría. Este objetivo requiere algunos resultados de la teoría de caracteres de grupos finitos, y por ello dedicamos el capítulo XI a exponer los preliminares necesarios y poco más.

En el capítulo XII exponemos la teoría de Tate sobre curvas elípticas con reducción multiplicativa sobre cuerpos métricos discretos y completos. Muchas demostraciones sobre curvas elípticas requieren distinguir el caso de curvas con *buena reducción potencial* (es decir, curvas que pasan a tener buena reducción tras una extensión del cuerpo base) y curvas con *reducción multiplicativa potencial* (ídem, pero con reducción multiplicativa en vez de con buena reducción). La teoría de Tate resulta ser una herramienta muy valiosa en el segundo caso.

Finalmente, en el capítulo XIII estudiamos la acción del grupo de Galois absoluto $G(\bar{K}/K)$ (donde $\bar{K}$ es una clausura algebraica de K) sobre los grupos $E[m]$ de puntos de torsión de una curva elíptica E/K, lo cual nos lleva al concepto de conductor. Además de los resultados sobre teoría de caracteres grupos expuesta en el capítulo XI, esto requiere, conocer también la teoría de ramificación en cuerpos métricos discretos y completos, desarrollada en el capítulo X

de mi libro sobre *Teoría de cuerpos de clases,* citado como [CC]. Esta teoría aparece en [CC] como requisito previo, de modo que los resultados que necesitamos son independientes de la teoría de cuerpos de clases propiamente dicha.

Como ya hice en mi libro sobre la teoría de *Esquemas,* debo acabar esta introducción reiterando mi más sincera gratitud al profesor Qing Liu por la correspondencia que ha mantenido conmigo mientras redactaba este libro, y que ha sido fundamental en mi estudio de las superficies aritméticas.

Primera parte

Anillos excelentes

Capítulo I

Preliminares

En este primer capítulo presentamos algunos resultados variados de álgebra conmutativa de carácter más elemental que los que veremos en los capítulos siguientes.

1.1 La descomposición primaria

Vamos a probar aquí el que fue uno de los primeros resultados relevantes del álgebra conmutativa abstracta, debido a Emmy Noether. Se trata de un teorema de descomposición de ideales en anillos noetherianos que generaliza a la factorización ideal de los dominios de Dedekind. Por conveniencia lo formularemos en un contexto ligeramente más general, no en anillos sino en módulos.

Definición 1.1 Sea A un anillo noetheriano y M un A-módulo. Diremos que un submódulo N es *primario* si el cociente M/N tiene un único primo asociado $\mathfrak{p}$, en cuyo caso diremos también que N es $\mathfrak{p}$-*primario.*

En [AC 4.43] definimos un ideal primario en un anillo A como un ideal $\mathfrak{q}$ tal que todos los divisores de cero en $A/\mathfrak{q}$ son nilpotentes. Observemos que esta definición coincide con la que hemos dado aquí en el caso $M = A$.

En efecto: un ideal $\mathfrak{q}$ es $\mathfrak{p}$-primario si y sólo si $A/\mathfrak{q}$ tiene a $\mathfrak{p}$ como único primo asociado, luego $\mathfrak{p} = \operatorname{rad}\mathfrak{q}$ y todos los divisores de cero de $A/\mathfrak{q}$ son nilpotentes. Recíprocamente, si todos los divisores de cero de $A/\mathfrak{q}$ son nilpotentes, la unión de todos los primos asociados de $A/\mathfrak{q}$ (es decir, el conjunto de los divisores de cero) coincide con la intersección de todos ellos (el conjunto de los elementos nilpotentes), lo cual sólo puede ocurrir si $A/\mathfrak{q}$ tiene un único primo asociado. ∎

Teorema 1.2 *Si A es un anillo noetheriano, M es un A-módulo y $\mathfrak{p}$ es un ideal primo de A, la intersección de un número finito de submódulos $\mathfrak{p}$-primarios de M es también $\mathfrak{p}$-primaria.*

DEMOSTRACIÓN: Basta probarlo para dos submódulos, digamos N_1 y N_2. Para ello, consideramos el monomorfismo natural

$$M/(N_1 \cap N_2) \longrightarrow (M/N_1) \oplus (M/N_2)$$

y aplicamos los teoremas [AC 3.47] y [AC 3.48]:

$$\varnothing \neq \mathrm{As}(M/(N_1 \cap N_2)) \subset \mathrm{As}(M/N_1) \cup \mathrm{As}(M/N_2) = \{\mathfrak{p}\}.$$

■

Definición 1.3 Sea A un anillo noetheriano, M un A-módulo y N un submódulo. Una *descomposición primaria* de N es un conjunto de submódulos primarios $N_1, \ldots, N_r$ tales que $N = N_1 \cap \cdots \cap N_r$. La descomposición es *reducida* si ninguno de los N_i puede omitirse y, si N_i es $\mathfrak{p}_i$-primario, entonces los primos $\mathfrak{p}_i$ son distintos dos a dos.

Es claro que toda descomposición primaria puede simplificarse hasta otra reducida. (Basta sustituir todos los submódulos con el mismo primo asociado por su intersección, y luego eliminar alguno de los submódulos si es redundante.)

Evidentemente, el hecho principal que vamos a probar es la existencia de descomposiciones primarias, pero antes obtendremos algunos resultados sobre unicidad.

Teorema 1.4 *Sea A un anillo noetheriano, sea M un A-módulo, sea N un submódulo y sea $N = N_1 \cap \cdots \cap N_r$ una descomposición primaria reducida, donde N_i es un submódulo $\mathfrak{p}_i$-primario. Entonces* $\mathrm{As}(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

DEMOSTRACIÓN: Tenemos un monomorfismo natural

$$M/N \longrightarrow (M/N_1) \oplus \cdots \oplus (M/N_r),$$

del que se sigue que $\mathrm{As}(M/N) \subset \bigcup_i \mathrm{As}(M/N_i) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. Recíprocamente, $(N_2 \cap \cdots \cap N_r)/N$ es isomorfo a un submódulo (no nulo) de M/N_1, luego su único primo asociado es $\mathfrak{p}_1$. Como $(N_2 \cap \cdots \cap N_r)/N$ es un submódulo de M/N, resulta que $\mathfrak{p}_1 \in \mathrm{As}(M/N)$. Lo mismo vale para los demás $\mathfrak{p}_i$. ■

Teorema 1.5 *Sea A un anillo noetheriano, sea M un A-módulo, sea N un submódulo $\mathfrak{p}$-primario y sea $\mathfrak{p}'$ un ideal primo de A. Entonces:*

a) Si $\mathfrak{p} \not\subset \mathfrak{p}'$, se cumple que $N_{\mathfrak{p}'} = M_{\mathfrak{p}'}$.

b) Si $\mathfrak{p} \subset \mathfrak{p}'$, entonces $N = M \cap N_{\mathfrak{p}'}$.

DEMOSTRACIÓN: a) Tenemos que $M_{\mathfrak{p}'}/N_{\mathfrak{p}'} = (M/N)_{\mathfrak{p}'}$ y [AC 3.50] implica que los primos asociados del cociente son las localizaciones de los primos de $\mathrm{As}(M/N)$ contenidos en $\mathfrak{p}'$, o sea, ninguno, luego $M_{\mathfrak{p}'}/N_{\mathfrak{p}'} = 0$ por [AC 3.48].

b) La conclusión $N = M \cap N_{\mathfrak{p}'}$ hay que entenderla, con más precisión, como que N es la antiimagen de $N_{\mathfrak{p}'}$ por el homomorfismo natural $M \longrightarrow M_{\mathfrak{p}'}$. Esto se cumple si el homomorfismo natural $M/N \longrightarrow (M/N)_{\mathfrak{p}'} = M_{\mathfrak{p}'}/N_{\mathfrak{p}'}$ es inyectivo.

Si $x \in M/N$ no nulo tiene imagen nula, existe un $s \in A \setminus \mathfrak{p}'$ tal que $sx = 0$, pero el submódulo $\langle x\rangle \subset M/N$ no tiene más primo asociado que $\mathfrak{p}$, luego existe un $a \in A$ tal que $\mathrm{An}(ax) = \mathfrak{p}$, luego $s \in \mathfrak{p} \subset \mathfrak{p}'$, lo cual es absurdo. ∎

Teorema 1.6 *Sea A un anillo noetheriano, M un A-módulo y N un submódulo que admita una descomposición primaria reducida $N = N_1 \cap \cdots \cap N_r$. Si N_i es $\mathfrak{p}_i$-primario y $\mathfrak{p}_i$ es minimal en $\mathrm{As}(M/N)$, entonces $N_i = M \cap N_{\mathfrak{p}_i}$.*

Demostración: Tenemos que si $j \neq i$ entonces $\mathfrak{p}_j \not\subset \mathfrak{p}_i$, por lo que el teorema anterior nos da que $N_{j,\mathfrak{p}_i} = M_{\mathfrak{p}_i}$, mientras que $N_i = M \cap N_{i,\mathfrak{p}_i}$.

Si $x \in N_i$, entonces, para todo $j \neq i$, su imagen $x/1 \in M_{\mathfrak{p}_i}$ puede expresarse como $x/1 = x_j/s_j$, con $x_j \in N_j$. Esto nos da un $s'_j \in A \setminus \mathfrak{p}_i$ tal que $s'_j x \in N_j$. Multiplicándolos todos obtenemos un $s \in A \setminus \mathfrak{p}_i$ tal que $sx \in N$, así pues, $x/1 = sx/s \in N_{\mathfrak{p}_i}$. Esto prueba que $N_i \subset M \cap N_{\mathfrak{p}_i} \subset M \cap N_{i,\mathfrak{p}_i} = N_i$. ∎

Así pues, si los primos asociados de M/N coinciden con los minimales, la descomposición primaria de N (si existe) en única. Veamos finalmente la existencia:

Teorema 1.7 *Si A es un anillo noetheriano y M un A-módulo finitamente generado, todo submódulo de M tiene una descomposición primaria.*

Demostración: Si N es un submódulo de M, basta probar que el submódulo nulo de M/N tiene una descomposición primaria o, equivalentemente, podemos suponer que $N = 0$.

Para cada $\mathfrak{p} \in \mathrm{As}(M)$, consideramos el conjunto $\mathcal{C}$ de los submódulos $N \subset M$ tales que $\mathfrak{p} \notin \mathrm{As}(N)$. Es no vacío, pues $0 \in \mathcal{C}$, y toda cadena respecto de la inclusión tiene un maximal, ya que, por definición de asociado, todo primo asociado de una unión es asociado de uno de los módulos que la componen. Por el lema de Zorn, existe un submódulo $N_{\mathfrak{p}} \in \mathcal{C}$ maximal respecto de la inclusión.

Como $\mathfrak{p}$ es asociado de M y no de $N_{\mathfrak{p}}$, ha de ser $N_{\mathfrak{p}} \neq M$. Por otra parte, si $M/N_{\mathfrak{p}}$ tuviera un primo asociado $\mathfrak{p}' \neq \mathfrak{p}$, entonces $M/N_{\mathfrak{p}}$ contendría un submódulo $N'/N_{\mathfrak{p}} \cong A/\mathfrak{p}'$, con lo que los primos asociados de N' estarían entre los de N y $\mathfrak{p}'$, luego $N' \in \mathcal{C}$ contradiría la maximalidad de N. Esto implica que $N_{\mathfrak{p}}$ es $\mathfrak{p}$-primario.

Finalmente, un primo asociado de $\bigcap_{\mathfrak{p}} N_{\mathfrak{p}}$ ha de ser asociado de todos los $N_{\mathfrak{p}}$, luego ha de ser distinto de todos los $\mathfrak{p}$ posibles. Por consiguiente, la intersección, al no tener asociados, ha de ser nula. ∎

Veamos ahora algunas aplicaciones de la descomposición primaria:

Teorema 1.8 *Sea $\phi : A \longrightarrow B$ un homomorfismo de anillos noetherianos y M un B-módulo. Sea $f : \mathrm{Esp}\, B \longrightarrow \mathrm{Esp}\, A$ el homomorfismo de esquemas asociado. Entonces, $\mathrm{As}_A(M) = f[\mathrm{As}_B(M)]$.*

DEMOSTRACIÓN: Sea $\mathfrak{P} \in \mathrm{As}_B(M)$. Entonces existe un $x \in M$ tal que $\mathfrak{P} = \mathrm{An}_B(x)$. Como $\mathrm{An}_A(x) = \mathrm{An}_B(x) \cap A = \mathfrak{P} \cap A = f(P)$, vemos que $f(P) \in \mathrm{As}_A(M)$.

Tomemos ahora $\mathfrak{p} \in \mathrm{As}_A(M)$ y sea $x \in M$ tal que $\mathfrak{p} = \mathrm{An}_A(x)$. Llamemos $I = \mathrm{An}_B(x)$ y consideremos una descomposición primaria reducida

$$I = \mathfrak{Q}_1 \cap \cdots \cap \mathfrak{Q}_r,$$

donde cada ideal $\mathfrak{Q}_i$ es $\mathfrak{P}_i$-primario. Como M contiene al submódulo $Bx \cong B/I$, tenemos que todos los primos $\mathfrak{P}_i$ son primos asociados de M. Basta probar que $\mathfrak{p} = \mathfrak{P}_i \cap A$, para cierto i. Sabemos que $I \cap A = \mathfrak{p}$, luego $\mathfrak{p} \subset \mathfrak{P}_i \cap A$ para todo i. Si en ningún caso se diera la igualdad, podríamos tomar $a_i \in \mathfrak{P}_i \cap A$, $a_i \notin \mathfrak{p}$. Para todo m suficientemente grande, se cumple $a_i^m \in \mathfrak{Q}_i$, luego llegamos a que $a = a_1^m \cdots a_r^m \in I \cap A = \mathfrak{p}$, lo cual es imposible. ∎

Teorema 1.9 (Bourbaki) *Sea $\phi : A \longrightarrow B$ un homomorfismo de anillos noetherianos, sea E un A-módulo y F un B-módulo que sea plano como A-módulo. Sea $f : \mathrm{Esp}\, B \longrightarrow \mathrm{Esp}\, A$ el homomorfismo de esquemas asociado a ϕ. Entonces:*

a) Para todo ideal primo $\mathfrak{p}$ de A, se cumple que

$$f[\mathrm{As}_B(F/\mathfrak{p}F)] = \mathrm{As}_A(F/\mathfrak{p}F) = \begin{cases} \{\mathfrak{p}\} & \text{si } F/\mathfrak{p}F \neq 0, \\ \varnothing & \text{si } F/\mathfrak{p}F = 0. \end{cases}$$

b) $\mathrm{As}_B(E \otimes_A F) = \bigcup_{\mathfrak{p} \in \mathrm{As}(E)} \mathrm{As}_B(F/\mathfrak{p}F)$.

DEMOSTRACIÓN: a) Observamos que $F/\mathfrak{p}F \cong F \otimes_A (A/\mathfrak{p})$ es plano sobre $A/\mathfrak{p}$, que es un dominio íntegro, luego $F/\mathfrak{p}F$ es un $A/\mathfrak{p}$-módulo libre de torsión. (La multiplicación por un elemento de $A/\mathfrak{p}$ es inyectiva y sigue siéndolo tras el cambio de base.) Esto significa que los únicos elementos de A que anulan a los elementos no nulos de $F/\mathfrak{p}F$ (si los hay) son los de $\mathfrak{p}$, luego, si hay tales elementos, $\mathfrak{p}$ es el único primo asociado.

b) Si $\mathfrak{p} \in \mathrm{As}(E)$, entonces E contiene un submódulo isomorfo a $A/\mathfrak{p}$, luego $E \otimes_A F$ contiene un submódulo isomorfo a $(A/\mathfrak{p}) \otimes_A F = F/\mathfrak{p}F$. Por consiguiente, $\mathrm{As}_B(F/\mathfrak{p}F) \subset \mathrm{As}_B(E \otimes_A F)$. Esto nos da una inclusión.

Para probar la inclusión contraria supongamos primeramente que E es un A-módulo finitamente generado con un único primo asociado $\mathfrak{p}$.

Sea $\mathfrak{P} \in \mathrm{As}_B(E \otimes_A F)$. Vamos a probar que $\mathfrak{P} \cap A = \mathfrak{p}$. Si $e \in E$ es no nulo, entonces $\mathrm{As}(eE) = \mathfrak{p}$, y $eE \cong A/\mathrm{An}(e)$, luego este anillo tiene a $\mathfrak{p}/\mathrm{An}(e)$ como único primo asociado. Esto implica que todo $a \in \mathfrak{p}$ es nilpotente en $A/\mathrm{An}(e)$, es decir, que existe un $n \geq 1$ tal que $a^n e = 0$.

Tomemos ahora $x \in E \otimes_A F$ tal que $\mathrm{An}(x) = \mathfrak{P}$. Descomponiendo x en suma de tensores $e \otimes f$, vemos que para cada $a \in \mathfrak{p}$ existe un n suficientemente grande tal que $a^n x = 0$, luego $a^n \in \mathfrak{P}$, luego $a \in \mathfrak{P}$. Así pues, $\mathfrak{p} \subset \mathfrak{P} \cap A$.

Por otra parte, hemos visto que los anuladores de los elementos de E están todos contenidos en $\mathfrak{p}$, luego si $a \in A \setminus \mathfrak{p}$, la multiplicación por a es inyectiva en E. Como F es plano sobre A, también lo es en $E \otimes_A F$, luego $a \notin \mathfrak{P}$. Esto nos da la igualdad $\mathfrak{p} = \mathfrak{P} \cap A$.

Tomemos ahora $e_1 \in E$ tal que $E_1 = e_1 E \cong A/\mathfrak{p}_1$ (donde $\mathfrak{p}_1 = \mathfrak{p}$). Si $E_1 \neq E$, podemos tomar igualmente un submódulo $E_2/E_1 \subset E/E_1$ tal que $E_2/E_1 \cong A/\mathfrak{p}_2$. Como A es noetheriano, el proceso ha de terminar, con lo que obtenemos una serie

$$0 = E_0 \subset E_1 \subset \cdots \subset E_r = E$$

tal que cada factor $E_i/E_{i-1} \cong A/\mathfrak{p}_i$, para cierto primo $\mathfrak{p}_i$ de A. Entonces

$$0 = E_0 \otimes_A F \subset E_1 \otimes_A F \subset \cdots \subset E_r \otimes_A F = E \otimes_A F$$

cumple que

$$(E_i \otimes_A F)/(E_{i-1} \otimes_A F) \cong (A/\mathfrak{p}_i) \otimes_A F \cong F/\mathfrak{p}_i F,$$

luego $\mathrm{As}_B(E \otimes_A F) \subset \bigcup_i \mathrm{As}_B(F/\mathfrak{p}_i F)$. Si $\mathfrak{P} \in \mathrm{As}_B(F/\mathfrak{p}_i F)$, por a) sabemos que $\mathfrak{P} \cap A = \mathfrak{p}_i$ y, por lo que hemos probado antes, si $\mathfrak{p}_i \neq \mathfrak{p}$ no puede ser $\mathfrak{P} \in \mathrm{As}_B(E \otimes_A F)$. Así pues, $\mathrm{As}_B(E \otimes_A F) \subset \mathrm{As}_B(F/\mathfrak{p}F)$, que es lo que queríamos probar.

Ahora supongamos únicamente que E es un A-módulo finitamente generado. En tal caso podemos considerar una descomposición primaria reducida del submódulo trivial $0 = E_1 \cap \cdots \cap E_r$. Así, E es isomorfo a un submódulo de $(E/E_1) \oplus \cdots \oplus (E/E_r)$ y $E \otimes_A F$ es isomorfo a un submódulo de

$$(E/E_1) \otimes_A F \oplus \cdots \oplus (E/E_r) \otimes_A F,$$

luego

$$\mathrm{As}_B(E \otimes_A F) \subset \bigcup_i \mathrm{As}_B((E/E_i) \otimes_A F) = \bigcup_i \mathrm{As}_B(F/\mathfrak{p}_i F),$$

donde la última igualdad se sigue del caso anterior aplicado a los módulos E/E_i.

En el caso general podemos descomponer $E = \bigcup_{i \in I} E_i$ como unión de submódulos finitamente generados.

Por definición de primo asociado, es claro que $\mathrm{As}_A(E)$ es la unión de los conjuntos $\mathrm{As}_A(E_i)$, y $\mathrm{As}_B(E \otimes_A F)$ es la unión de los conjuntos $\mathrm{As}_B(E_i \otimes_A F)$. Esto reduce el problema al caso ya probado. ∎

Combinando los apartados a) y b) del teorema anterior vemos además que

$$f[\mathrm{As}_B(E \otimes_A F)] = \{\mathfrak{p} \in \mathrm{As}(E) \mid \mathfrak{p}F \neq F\}.$$

Si F es fielmente plano sobre A (ver el teorema 1.22 más abajo), tenemos simplemente que $f[\mathrm{As}_B(E \otimes_A F)] = \mathrm{As}(E)$.

Conviene destacar algunos casos particulares. Por ejemplo, si $F = B$, es decir, si suponemos que B es una A-álgebra plana y que E es un A-módulo arbitrario, tenemos que

$$\mathrm{As}_B(E \otimes_A B) = \bigcup_{\mathfrak{p} \in \mathrm{As}(E)} \mathrm{As}_B(B/\mathfrak{p}B),$$

y si hacemos, además, $E = A$, la fórmula se reduce a

$$\mathrm{As}(B) = \bigcup_{\mathfrak{p} \in \mathrm{As}(A)} \mathrm{As}_B(B/\mathfrak{p}B).$$

1.2 El teorema chino del resto

Vamos a extraer algunas consecuencias de la versión más general del teorema chino del resto.

Definición 1.10 Diremos que dos ideales I, J de un anillo A son *primos entre sí* si $I + J = 1$.

Observemos que si I, J son primos entre sí, entonces $IJ = I \cap J$, pues

$$I \cap J = (I \cap J)(I + J) \subset IJ \subset I \cap J.$$

Otro hecho elemental es que Si I es primo con J y con J', también lo es con JJ', pues

$$1 = (I + J)(I + J') \subset I + JJ' \subset 1.$$

Teorema 1.11 (Teorema chino del resto) *Si A es un anillo, $I_1, \ldots, I_n$ son ideales primos entre sí dos a dos y llamamos $I = I_1 \cdots I_n$, entonces*

$$A/I \cong (A/I_1) \oplus \cdots \oplus (A/I_n).$$

Demostración: Llamamos $I_i^* = \prod_{j \neq i} I_j = \bigcap_{j \neq i} I_j$, de modo que $I_i + I_i^* = 1$. Así, existe un $a_i \in A$ tal que $a_i \equiv 1$ (mód I_i), $a_i \equiv 0$ (mód I_j), para $j \neq i$. Es claro entonces que el monomorfismo natural $A/I \longrightarrow (A/I_1) \oplus \cdots \oplus (A/I_n)$ es suprayectivo, pues una antiimagen de $([b_1], \ldots, [b_n])$ es $[a_1 b_1 + \cdots + a_n b_n]$. ∎

Como primera aplicación vamos a probar un teorema de estructura para las compleciones de los anillos semilocales:

Definición 1.12 Un anillo A es *semilocal* si tiene un número finito de ideales maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. Cuando hablemos de la compleción $\hat{A}$ de un anillo semilocal, se entenderá que nos referimos a su compleción respecto del ideal $I = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$.

Los anillos semilocales aparecen de forma natural como extensiones enteras (en particular, finitas) de anillos locales (por [AC 3.63]).

Notemos que los ideales $\mathfrak{m}_i$ son primos entre sí dos a dos, luego lo mismo sucede con los ideales $\mathfrak{m}_i^r$. Por el teorema chino del resto,

$$A/I^r \cong (A/\mathfrak{m}_1^r) \oplus \cdots \oplus (A/\mathfrak{m}_n^r).$$

Los isomorfismos son canónicos, por lo que al tomar límites inversos vemos que

$$\hat{A} = \hat{A}_1 \oplus \cdots \oplus \hat{A}_n,$$

donde $\hat{A} = \varprojlim_r (A/I^r)$ es la compleción de A (respecto de la topología I-ádica) y $\hat{A}_i = \varprojlim_r (A/\mathfrak{m}_i^r)$ es la compleción respecto a la topología $\mathfrak{m}_i$-ádica.

En particular, todo anillo semilocal completo es suma directa de anillos locales completos. ∎

Veamos ahora una segunda aplicación:

Teorema 1.13 *Sea A un anillo reducido con un número finito de primos minimales, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Sea $F(A)$ el anillo completo de cocientes de A, es decir, su localización respecto del conjunto de los elementos que no son divisores de cero. Entonces $F(A) \cong K_1 \oplus \cdots \oplus K_r$, donde K_i es el cuerpo de cocientes de $A/\mathfrak{p}_i$.*

Demostración: Según [AC 3.43], tenemos que el conjunto S de los elementos de A que no son divisores de cero es $S = A \setminus (\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r)$. Por lo tanto, los únicos ideales primos de $F(A)$ son los ideales $S^{-1}\mathfrak{p}_1, \ldots, S^{-1}\mathfrak{p}_r$, que son a la vez maximales y minimales. Además, $F(A)$ también es reducido, luego se cumple que $S^{-1}\mathfrak{p}_1 \cap \cdots \cap S^{-1}\mathfrak{p}_r = 0$. Por el teorema chino del resto, tenemos que

$$F(A) = S^{-1}A \cong S^{-1}A/S^{-1}\mathfrak{p}_1 \oplus \cdots \oplus S^{-1}A/S^{-1}\mathfrak{p}_r.$$

Ahora observamos que $S^{-1}A/S^{-1}\mathfrak{p}_i \cong S_i'^{-1}(A/\mathfrak{p}_i)$, donde S_i' es la imagen de S en $A/\mathfrak{p}_i$, pero $S^{-1}A/S^{-1}\mathfrak{p}_i$ es un cuerpo, y la única localización de $A/\mathfrak{p}_i$ que es un cuerpo es K_i. ∎

1.3 Anillos íntegramente cerrados

Aquí probaremos algunos resultados sobre anillos íntegramente cerrados. En la prueba del primero de ellos usaremos el concepto siguiente: Si A es un dominio íntegro y K su cuerpo de cocientes, diremos que un elemento $\alpha \in K$ es *casi entero* sobre A si existe un $a \in A$ no nulo tal que $a\alpha^n \in A$ para todo $n \geq 1$.

Notemos que si α es entero sobre A, entonces es casi entero, ya que el A-módulo $A[\alpha]$ es finitamente generado, y basta tomar como a un denominador común de los generadores, de modo que $A[\alpha] \subset Aa^{-1}$, luego $aA[\alpha] \subset A$. El recíproco es cierto si A es noetheriano, ya que entonces tenemos igualmente la inclusión $A[\alpha] \subset Aa^{-1}$ y el A-módulo Aa^{-1} es finitamente generado, luego $A[\alpha]$ también.

Teorema 1.14 *Si A es un anillo íntegramente cerrado, entonces $A[X]$ también lo es.*

DEMOSTRACIÓN: Sea K el cuerpo de cocientes de A. Entonces, el cuerpo de cocientes de $A[X]$ es el mismo que el de $K[X]$, pero éste es íntegramente cerrado, ya que tiene factorización única. Así pues, todo elemento de dicho cuerpo de cocientes entero sobre $A[X]$ pertenece a $K[X]$. Por lo tanto, es de la forma $\alpha = p(X)/a$, donde $p(X) \in A[X]$, $a \in A$. Pongamos que α satisface una ecuación de la forma

$$\alpha^n + f_1(X)\alpha^{n-1} + \cdots + f_n(X) = 0,$$

donde $f_i(X) \in A[X]$. Sea A_0 la $\mathbb{Z}$-álgebra generada por a y los coeficientes de $p(X)$ y de los $f_i(X)$. Así, A_0 es una $\mathbb{Z}$-álgebra finitamente generada, luego es un anillo noetheriano, tenemos que α es entero sobre $A_0[X]$ y basta probar que $\alpha \in A[X]$. Equivalentemente, podemos suponer que A es noetheriano.

Como α es, en particular, casi entero sobre $A[X]$, existe un polinomio

$$g(X) = b_m X^m + b_{m-1}X^{m-1} + \cdots + b_s X^s,$$

con $b_i \in A$, $b_m, b_s \neq 0$, tal que $g(X)\alpha^n \in A[X]$ para todo $n \geq 0$. Pongamos que

$$\alpha = \alpha_s X^s + \alpha_{s-1}X^{s-1} + \cdots + \alpha_t X^t \in K[X],$$

donde $\alpha_s, \alpha_t \neq 0$. Entonces $\alpha_t^n b_s \in A$ para todo $n \geq 1$, luego α_t es casi entero (y, por consiguiente, entero) sobre A, lo que a su vez implica que $\alpha_t \in A$. Ahora observamos que $\alpha - \alpha_t X^t$ también es entero sobre $A[X]$, luego podemos razonar similarmente y concluir que $\alpha_{t-1} \in A$, hasta llegar a que $\alpha \in A[X]$. ∎

Ahora probaremos una caracterización de los anillos íntegramente cerrados debida a Krull. Conviene dar nombre a las propiedades que involucra:

Definición 1.15 Sea A un anillo noetheriano. Para cada $k \geq 0$, definimos las propiedades siguientes:

(R_k) Si $\mathfrak{p} \in \operatorname{Esp} A$ y $\operatorname{alt}\mathfrak{p} \leq k$, entonces $A_\mathfrak{p}$ es regular.

(S_k) Para cada $\mathfrak{p} \in \operatorname{Esp} A$, se cumple que $\operatorname{pr} A_\mathfrak{p} \geq \min\{k, \operatorname{alt}\mathfrak{p}\}$.

Obviamente, $R_{k+1} \Rightarrow R_k \Rightarrow S_k$ y $S_{k+1} \Rightarrow S_k$. Vamos a analizar con más detalle las propiedades S_k para los primeros valores de k:

- *La propiedad S_0 es trivial.*
- *La propiedad S_1 equivale a que todos los primos asociados de A sean minimales.*

  En efecto, observemos, en general, que un primo $\mathfrak{p}$ es asociado de A si y sólo si $\mathfrak{p}A_\mathfrak{p}$ es asociado de $A_\mathfrak{p}$. (Se cumple que $\mathfrak{p}A_\mathfrak{p} = \operatorname{An}(a/s)$ si y sólo si $\mathfrak{p}A_\mathfrak{p} = \operatorname{An}(a/1)$ si y sólo si $\mathfrak{p} = \operatorname{An}(a)$.)

Si A cumple S_1 y $\mathfrak{p}$ es un primo asociado, entonces $\operatorname{pr} A_\mathfrak{p} = 0$. La propiedad S_1 implica entonces que $\operatorname{alt}\mathfrak{p} = 0$, es decir, que $\mathfrak{p}$ es un primo minimal. Recíprocamente, si $\operatorname{alt}\mathfrak{p} \geq 1$, entonces no es un primo minimal, luego no es asociado, luego $\mathfrak{p}A_\mathfrak{p}$ tampoco lo es. Si éste sólo contuviera divisores de cero, debería estar contenido en un primo asociado, lo cual es imposible porque es maximal. Así pues, $\operatorname{pr} A_\mathfrak{p} \geq 1$.

- *La propiedad S_2 equivale a que tanto A como los anillos A/aA, donde $a \in A$ no es un divisor de cero, cumplan la propiedad S_1.*

  En efecto, si A cumple S_2 y a no es un divisor de cero, entonces A/aA cumple S_1, ya que si $\operatorname{alt}(\mathfrak{p}/aA) \geq 1$, existe un primo minimal $\mathfrak{q}$ de a tal que $(a) \subset \mathfrak{q} \subsetneq \mathfrak{p}$, y el teorema de los ideales principales [AC 5.2] nos da que $\operatorname{alt}\mathfrak{q} = 1$, luego $\operatorname{alt}\mathfrak{p} \geq 2$, luego $\operatorname{pr} A_\mathfrak{p} \geq 2$, luego $\operatorname{pr}(A/aA)_{\mathfrak{p}/aA} \geq 1$. Recíprocamente, si A y todos los anillos A/aA cumplen S_1, entonces A cumple S_2, ya que si $\operatorname{alt}\mathfrak{p} \geq 2$, entonces existe un $a \in \mathfrak{p}$ que no es un divisor de cero (de lo contrario, $\mathfrak{p}$ estaría contenido en un primo asociado que, por S_1, sería minimal, lo cual es imposible). Por el teorema de los ideales principales, $\mathfrak{p}$ no puede ser un primo minimal de a, luego $\operatorname{alt}(\mathfrak{p}/aA) \geq 1$, luego $\operatorname{pr}(A_\mathfrak{p}/aA_\mathfrak{p}) \geq 1$, luego $\operatorname{pr} A_\mathfrak{p} \geq 2$.

Estas propiedades caracterizan algunos conceptos del álgebra conmutativa. Por ejemplo, un anillo A cumple R_k para todo k si y sólo si es regular, mientras que A cumple S_k para todo k si y sólo si, para todo $\mathfrak{p} \in \operatorname{Esp} A$, se cumple que $\operatorname{pr} A_\mathfrak{p} \geq \operatorname{alt}\mathfrak{p} = \dim A_\mathfrak{p}$, es decir, si, para todo $\mathfrak{p} \in \operatorname{Esp} A$, la localización $A_\mathfrak{p}$ es un anillo de Cohen-Macaulay (en cuyo caso se dice que A es un anillo de Cohen-Macaulay). Veamos otro caso de interés:

Teorema 1.16 *Un anillo es reducido si y sólo si cumple R_0 y S_1.*

Demostración: Si A es reducido, entonces cumple S_1 por [AC 3.52]. Para probar que cumple R_0 tomamos un $\mathfrak{p} \in \operatorname{Esp} A$ de altura 0, es decir, un primo minimal, y hemos de ver que $A_\mathfrak{p}$ es regular. Ahora bien, $A_\mathfrak{p}$ es reducido por [E 2.23], luego su único ideal primo ha de ser nulo, luego es un cuerpo, luego es regular.

Supongamos ahora que A cumple R_0 y S_1. Si $a \in A$ es nilpotente (no nulo), entonces $\operatorname{As}(\langle a\rangle) \subset \operatorname{As}(A)$, luego existe un $\mathfrak{p} \in \operatorname{As}(A)$ (es decir, un primo minimal, por la propiedad S_0) tal que $\mathfrak{p} = \operatorname{An}(ba)$, para cierto $b \in A$. Esto implica que $ba/1 \in A_\mathfrak{p}$ es no nulo y obviamente es nilpotente, luego $A_\mathfrak{p}$ no es regular (no es un dominio íntegro), en contradicción con la propiedad R_0. ∎

La propiedad más interesante caracterizada en términos de las propiedades R_k y S_k es la de ser íntegramente cerrado, aunque conviene generalizar el concepto para no restringirlo a dominios íntegros:

Definición 1.17 Un anillo A es *normal* si para todo $\mathfrak{p} \in \operatorname{Esp} A$ el anillo $A_\mathfrak{p}$ es (un dominio íntegro) íntegramente cerrado.

Claramente, un dominio íntegro es normal si y sólo si es íntegramente cerrado. El teorema siguiente fue demostrado por Krull en el caso de dominios íntegros:

Teorema 1.18 (Serre) *Un anillo es normal si y sólo si cumple las propiedades R_1 y S_2.*

Demostración: Es claro que un anillo A cumple las propiedades R_k o S_k si y sólo si las cumple $A_\mathfrak{p}$ para todo $\mathfrak{p} \in \operatorname{Esp} A$, luego basta probar que un anillo local A es un dominio íntegro íntegramente cerrado si y sólo si cumple las propiedades R_1 y S_2.

Supongamos primeramente que A es íntegramente cerrado. Si $\operatorname{alt}\mathfrak{p} \leq 1$, entonces $A_\mathfrak{p}$ es íntegramente cerrado y tiene dimensión ≤ 1. O bien es un cuerpo (trivialmente regular) o bien $\operatorname{alt}\mathfrak{p} = 1$, en cuyo caso $A_\mathfrak{p}$ es regular por [E 7.20]. Así pues, A cumple R_1. Más aún, es evidente que $\operatorname{pr}(A_\mathfrak{p}) = 1$, luego $\mathfrak{p}$ también cumple S_2. Falta probar S_2 para ideales $\mathfrak{p}$ de altura ≥ 2. Podemos cambiar A por $A_\mathfrak{p}$ y suponer que A es un anillo local de dimensión ≥ 2, y hemos de probar que $\operatorname{pr}(A) \geq 2$. Supongamos, por el contrario, que $\operatorname{pr}(A) \leq 1$.

Tomemos $a \in \mathfrak{p}$ no nulo. Entonces $\mathfrak{p}/aA$ sólo contiene divisores de cero de A/aA, luego es un primo asociado (pues es maximal y está contenido en un primo asociado). Esto significa que existe un $b \in A \setminus aA$ tal que $b\mathfrak{p} \subset aA$.

Vamos a usar el teorema [E 7.4]. Si $\mathfrak{q}$ es un ideal primo de altura 1, está estrictamente contenido en $\mathfrak{p}$, ya que $\mathfrak{p}$ es el ideal maximal de A y tiene altura ≥ 2. Por consiguiente, podemos tomar un $c \in \mathfrak{p} \setminus \mathfrak{q}$, de modo que $bc \in b\mathfrak{p} \subset aA$, luego $b/a \in A_\mathfrak{q}$. Como esto vale para todo $\mathfrak{q}$, el teorema [E 7.4] nos da que $b/a \in A$, luego $b \in aA$, contradicción.

Supongamos ahora que A cumple las propiedades R_1 y S_2. En particular cumple R_0 y S_1, luego es reducido. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ los primos minimales de A, sea $A_i = A/\mathfrak{p}_i$, sea K_i el cuerpo de cocientes de A_i y sea $F(A)$ el anillo completo de fracciones de A. Según 1.13 tenemos que $F(A) = K_1 \oplus \cdots \oplus K_r$. Notemos que A es un subanillo de $F(A)$. Vamos a probar que A es íntegramente cerrado en $F(A)$.

Si $a/s \in F(A)$ cumple

$$(a/s)^n + c_1(a/s)^{n-1} + \cdots + c_n = 0,$$

con $c_i \in A$, escrito de otra forma es

$$a^n + c_1 a^{n-1} s + \cdots + c_n s^n = 0.$$

Sea $\mathfrak{P} \in \operatorname{Esp} A$ un primo de altura 1. Por R_1 sabemos que $A_\mathfrak{P}$ es regular, luego es un dominio íntegro íntegramente cerrado. Reinterpretando la ecuación anterior en $A_\mathfrak{P}$ y teniendo en cuenta que $s/1 \neq 0$, podemos volver a la ecuación primera y concluir que $a/s \in A_\mathfrak{P}$ o, equivalentemente, que $a \in sA_\mathfrak{P}$.

El teorema de los ideales principales [AC 5.2] nos da que todos los primos minimales de s tienen altura 1. Si los llamamos $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$, la propiedad S_2

nos dice que son todos los primos asociados de A/sA, luego la descomposición primaria de sA es de la forma

$$sA = \mathfrak{Q}_1 \cap \cdots \cap \mathfrak{Q}_r,$$

donde $\mathfrak{Q}_i$ es $\mathfrak{P}_i$-primario y, por 1.6, tenemos que $a \in sA_{\mathfrak{P}_i} \cap A = \mathfrak{Q}_i$. Así pues, $s \in sA$, luego $a/s \in A$, como queríamos probar.

En particular, la "base canónica" $e_1, \ldots, e_r \in F(A)$ cumple que $e_i^2 - e_i = 0$, que es una relación de integridad, luego $e_i \in A$. Esto implica que $r = 1$, ya que si $r > 1$, las relaciones $e_i e_j = 0$ (para $i \neq j$) implican que los e_i no son unidades, luego todos ellos pertenecen al ideal maximal de A, lo cual es imposible porque suman 1.

Como A es reducido, ha de ser $\mathfrak{p}_1 = 0$, luego A es un dominio íntegro con cuerpo de fracciones $F(A)$ y, según hemos probado, es íntegramente cerrado. ∎

Veamos un par de aplicaciones:

Teorema 1.19 *Sea A un dominio íntegro noetheriano y supongamos que existe un $f \in A$ no nulo tal que A_f es íntegramente cerrado. Entonces el conjunto de los puntos normales de* $\operatorname{Esp} A$ *es abierto.*

Demostración: Consideremos el conjunto (finito) E formado por los primos $\mathfrak{q} \in \operatorname{As}_A(A/fA)$ tales que, o bien $\operatorname{alt}\mathfrak{q} > 1$, o bien $\operatorname{alt}\mathfrak{q} = 1$ y $A_\mathfrak{q}$ no es regular. Basta probar que el conjunto de los puntos normales de $\operatorname{Esp} A$ es el complementario del cerrado

$$\bigcup_{\mathfrak{q} \in E} V(\mathfrak{q}).$$

Observemos en primer lugar que si un primo $\mathfrak{p}$ cumple que $f \notin \mathfrak{p}$, entonces $A_\mathfrak{p}$ es íntegramente cerrado, ya que es una localización de A_f. También es obvio que f pertenece a todos los elementos de E, ya que anula a A/fA.

Supongamos que $\mathfrak{p} \in V(\mathfrak{q})$, para cierto $\mathfrak{q} \in E$, es decir, que $\mathfrak{q} \subset \mathfrak{p}$, y veamos que $A_\mathfrak{p}$ no puede ser íntegramente cerrado. Si lo fuera, por la propiedad R_1, vemos que $\mathfrak{q}$ no puede tener altura 1. Tenemos, pues, que $\operatorname{alt}\mathfrak{q} \geq 2$, luego la propiedad S_2 nos da que $\operatorname{pr} A_\mathfrak{q} \geq 2$. Esto implica que existe $g \in \mathfrak{q}$ tal que f, g es una sucesión regular o, lo que es lo mismo, que g no es un divisor de cero de A/fA, lo cual contradice a que $\mathfrak{q}$ sea un primo asociado del cociente.

Supongamos ahora que $A_\mathfrak{p}$ no es íntegramente cerrado y veamos que contiene un elemento de E. Ha de fallar la propiedad R_1 o la propiedad S_2. Si falla R_1, existe un ideal $\mathfrak{q} \subset \mathfrak{p}$ de altura ≤ 1 tal que $A_\mathfrak{q}$ no es regular. No puede ser $\mathfrak{q} = 0$, ya que A_0 es un cuerpo y sí que es regular, luego $\operatorname{alt}\mathfrak{q} = 1$. El teorema [E 7.20] nos da que $A_\mathfrak{q}$ tampoco es íntegramente cerrado, luego $f \in \mathfrak{q}$ y, por su altura, $\mathfrak{q}$ es un primo minimal de A/fA, luego es también un primo asociado, de modo que $\mathfrak{q} \in E$.

Supongamos ahora que $A_\mathfrak{p}$ no cumple la propiedad S_2, es decir, que existe un primo $\mathfrak{q} \subset \mathfrak{p}$ tal que $\operatorname{pr}\mathfrak{q} < \min(2, \operatorname{alt}\mathfrak{q})$. Obviamente, $\operatorname{alt}\mathfrak{q}$ no puede ser 0, ni

tampoco 1, ya que entonces $\operatorname{pr}\mathfrak{q} = 0$, luego $\mathfrak{q} = 0$ y $\operatorname{alt}\mathfrak{q} = 0$. Por consiguiente, $\operatorname{alt}\mathfrak{q} > 1$ y $\operatorname{pr}\mathfrak{q} = 1$. Notemos que $A_\mathfrak{q}$ no es íntegramente cerrado, ya que el ideal $\mathfrak{q}$ incumple también la propiedad S_2 visto como ideal de $A_\mathfrak{q}$, luego $f \in \mathfrak{q}$ y todos los elementos de $\mathfrak{q}$ son divisores de cero en A/fA, de donde se sigue que $\mathfrak{q}$ es asociado del cociente, luego $\mathfrak{q} \in E$. ∎

En otras palabras, el teorema afirma que si $\operatorname{Esp} A$ contiene un abierto formado por puntos normales, entonces el conjunto de los puntos normales es abierto.

Teorema 1.20 *Sea $f : X \longrightarrow Y$ un homomorfismo suave de un esquema conexo X en un esquema normal localmente noetheriano Y. Entonces X también es normal.*

Demostración: Más en general, vamos a probar que, sin la hipótesis de conexión, el esquema X tiene componentes conexas normales. Para ello basta probar que todo $x \in X$ tiene un entorno normal. Tomando un entorno afín de $y = f(x)$, podemos suponer que $Y = \operatorname{Esp} A$ es afín. También podemos sustituir X por un entorno afín de x según el teorema [E A33], lo que nos da un homomorfismo llano $g : X \longrightarrow A^n_Y$. Como, por 1.14, tenemos que $A[X_1, \ldots, X_n]$ es íntegramente cerrado, esto nos reduce el problema al caso en que f es llano, es decir, al caso en que sus fibras tienen dimensión 0.

Basta probar que $\mathcal{O}_X(X)$ cumple las propiedades R_1 y S_2. Para probar la primera tomamos un punto $x \in X$ tal que $\dim \mathcal{O}_{X,x} = 1$ y hemos de ver que es regular. El teorema [E 4.52] nos da que $\dim \mathcal{O}_{X,x} = \dim \mathcal{O}_{Y,y}$, luego, como Y es normal, tenemos que $\mathcal{O}_{Y,y}$ es regular. Su ideal maximal es, pues, principal, y lo mismo sucede con el ideal maximal de $\mathcal{O}_{X,x}$, debido a que es no ramificado sobre $\mathcal{O}_{Y,y}$. Esto implica que $\mathcal{O}_{X,x}$ también es regular, y así $\mathcal{O}_X(X)$ cumple R_1.

Para probar S_2 podemos tomar un punto $x \in X$ con $\dim \mathcal{O}_{X,x} \geq 2$, con lo que también $\dim \mathcal{O}_{Y,y} \geq 2$ y, como $\mathcal{O}_Y(Y)$ cumple S_2, existe una sucesión regular (a, b) en $\mathfrak{m}_y\mathcal{O}_{Y,y}$. Basta probar que su imagen es regular en $\mathcal{O}_{X,x}$.

Observemos que, por hipótesis, $\mathcal{O}_{X,x}$ es plano sobre $\mathcal{O}_{Y,y}$. Esto implica a su vez que $\mathcal{O}_{X,x}/(a)$ es plano sobre $\mathcal{O}_{Y,y}/(a)$. En efecto, se deduce de la propia definición teniendo en cuenta que, si M es un $\mathcal{O}_{Y,y}/(a)$-módulo, entonces

$$M \otimes_{\mathcal{O}_{Y,y}/(a)} (\mathcal{O}_{X,x}/(a)) \cong M \otimes_{\mathcal{O}_{Y,y}} \mathcal{O}_{X,x}$$

como $\mathcal{O}_{Y,y}/(a)$-módulos.

Como a no es un divisor de cero en $\mathcal{O}_{Y,y}$, la multiplicación por a es inyectiva y, como $\mathcal{O}_{X,x}$ es plano sobre $\mathcal{O}_{Y,y}$, la multiplicación por a también es inyectiva en $\mathcal{O}_{X,x}$, luego a no es un divisor de cero en $\mathcal{O}_{X,x}$.

Similarmente, tenemos que b no es un divisor de cero en $\mathcal{O}_{Y,y}/(a)$, luego b no es un divisor de cero en $\mathcal{O}_{X,x}/(a)$, luego (a, b) es una sucesión regular en $\mathcal{O}_{X,x}$, lo que prueba que $\mathcal{O}_X(X)$ cumple S_2. ∎

1.4 Módulos fielmente planos

Definición 1.21 Si A es un anillo y M un A-módulo, diremos que M es *fielmente plano* si, para toda sucesión de A-módulos

$$0 \longrightarrow P \longrightarrow Q \longrightarrow R \longrightarrow 0,$$

la sucesión es exacta si y sólo si lo es la sucesión

$$0 \longrightarrow P \otimes_A M \longrightarrow Q \otimes_A M \longrightarrow R \otimes_A M \longrightarrow 0,$$

Obviamente, los A-módulos fielmente planos, son planos. Veamos algunas caracterizaciones:

Teorema 1.22 *Sea A un anillo y M un A-módulo. Las afirmaciones siguientes son equivalentes:*

a) M es fielmente plano.

b) M es plano y, para todo A-módulo $N \neq 0$, se cumple que $M \otimes_A N \neq 0$.

c) M es plano y, para todo ideal maximal $\mathfrak{m}$ de A, se cumple que $\mathfrak{m}M \neq M$.

Demostración: a) $\Rightarrow$ b) Si $M \otimes_A N = 0$, consideramos la sucesión de A-módulos $0 \longrightarrow N \longrightarrow 0$. Como $0 \longrightarrow M \otimes_A N \longrightarrow 0$ es exacta, también lo es la original, luego $N = 0$.

b) $\Rightarrow$ c) Como $A/\mathfrak{m} \neq 0$, también $(A/\mathfrak{m}) \otimes_A M = M/\mathfrak{m}M \neq 0$.

c) $\Rightarrow$ b) Tomemos $x \in N$ no nulo y sea I el núcleo del homomorfismo $A \longrightarrow N$ dado por $a \mapsto ax$. Así $A/I \cong Ax$, luego $I \neq A$. Sea $\mathfrak{m}$ un ideal maximal de A que contenga a I. Entonces $IM \subset \mathfrak{m}M \subsetneq M$ y $(A/I) \otimes_A M \cong M/IM \neq 0$. Como M es plano, el homomorfismo $(A/I) \otimes_A M \longrightarrow N \otimes_A M$ es inyectivo, luego $N \otimes_A N \neq 0$.

b) $\Rightarrow$ a) Consideremos una sucesión de A-módulos $P \xrightarrow{f} Q \xrightarrow{g} R$ que multiplicada por $\otimes_A M$ sea exacta. Como M es plano, el funtor $\otimes_A M$ es exacto, lo que implica que $\operatorname{Im}(f \circ g) \otimes_A M = \operatorname{Im}(f_M \circ g_M) = 0$ (se ve en la prueba de [AC 1.37]). Por hipótesis $\operatorname{Im}(f \circ g) = 0$, es decir, $f \circ g = 0$. El mismo teorema muestra ahora que $(\operatorname{N} g/\operatorname{Im} f) \otimes_A M = \operatorname{N} g_M/\operatorname{Im} f_M = 0$ y, de nuevo por hipótesis, $\operatorname{N} g/\operatorname{Im} f = 0$, es decir, la sucesión es exacta. ∎

Notemos que la prueba del teorema anterior muestra que si M es un A-módulo fielmente plano, entonces cumple la definición para sucesiones arbitrarias, no necesariamente de la forma $0 \longrightarrow P \longrightarrow Q \longrightarrow R \longrightarrow 0$, cosa que también puede probarse directamente sin dificultad.

Ahora también es evidente que si $A \longrightarrow B$ es un homomorfismo plano entre anillos locales (entendiendo que envía el ideal maximal de A dentro del ideal maximal de B), entonces es fielmente plano.

Otras propiedades sencillas son las siguientes:

- Si M es un B-módulo fielmente plano y B es una A-álgebra fielmente plana, entonces M es un A-módulo fielmente plano.
- Si M es un A-módulo fielmente plano y B es una A-álgebra arbitraria, entonces $M \otimes_A B$ es un B-módulo fielmente plano.
- Si B es una A-álgebra y M es un B-módulo fielmente plano que también es fielmente plano como A-módulo, entonces B es también un A-módulo fielmente plano.

Teorema 1.23 *Sea A un anillo y B una A-álgebra fielmente plana. Entonces:*

a) Para todo A-módulo N, el homomorfismo natural $N \longrightarrow N \otimes_A B$ es inyectivo. En particular, el homomorfismo natural $A \longrightarrow B$ es inyectivo y podemos considerar a A como subanillo de B.

b) Para cada ideal I de A, se cumple que $IB \cap A = I$.

c) El homomorfismo de esquemas $\operatorname{Esp} B \longrightarrow \operatorname{Esp} A$ es suprayectivo.

DEMOSTRACIÓN: a) Tomemos $x \in N$ no nulo. Como B es plano, la inclusión $Ax \longrightarrow N$ da lugar a un monomorfismo $Ax \otimes_A B \longrightarrow N \otimes_A B$, por lo que $x \otimes 1 \neq 0$.

b) Tenemos que $B \otimes_A (A/I) = B/IB$ es fielmente plano sobre A/I, luego, por el apartado anterior, el homomorfismo $A/I \longrightarrow B/IB$ es inyectivo, lo que significa precisamente que $IB \cap A = I$.

c) Tomemos un ideal $\mathfrak{p} \in \operatorname{Esp} A$. Como B es fielmente plano sobre A, también $B_\mathfrak{p} = B \otimes_A A_\mathfrak{p}$ es fielmente plano sobre $A_\mathfrak{p}$, lo que implica que $\mathfrak{p}B_\mathfrak{p} \neq B_\mathfrak{p}$. Sea $\mathfrak{m}$ un ideal maximal de $B_\mathfrak{p}$ que contenga a $\mathfrak{p}B_\mathfrak{p}$. Entonces, $\mathfrak{p}A_\mathfrak{p} \subset \mathfrak{m} \cap A_\mathfrak{p}$, luego $\mathfrak{p}A_\mathfrak{p} = \mathfrak{m} \cap A_\mathfrak{p}$, ya que $\mathfrak{p}A_\mathfrak{p}$ es el ideal maximal de $A_\mathfrak{p}$. Si llamamos $\mathfrak{P} = \mathfrak{m} \cap B$, vemos que $\mathfrak{P} \cap A = (\mathfrak{m} \cap B) \cap A = \mathfrak{m} \cap A = (\mathfrak{m} \cap A_\mathfrak{p}) \cap A = \mathfrak{p}A_\mathfrak{p} \cap A = \mathfrak{p}$. ∎

En realidad, la suprayectividad del homomorfismo de esquemas es una caracterización:

Teorema 1.24 *Sea A un anillo y B una A-álgebra. Las afirmaciones siguientes son equivalentes:*

a) B es fielmente plano sobre A.

b) B es plano sobre A y el homomorfismo de esquemas $\operatorname{Esp} B \longrightarrow \operatorname{Esp} A$ es suprayectivo.

c) B es plano sobre A y para todo ideal maximal $\mathfrak{m}$ de A existe un ideal maximal $\mathfrak{m}'$ de B tal que $\mathfrak{m}' \cap A = \mathfrak{m}$.

DEMOSTRACIÓN: a) ⇒ b) está probado en el teorema anterior.

b) ⇒ c) En principio tenemos un ideal primo $\mathfrak{p}$ de B tal que $\mathfrak{p} \cap A = \mathfrak{m}$, pero si $\mathfrak{m}'$ es un ideal maximal de B que contenga a $\mathfrak{p}$, tenemos que $\mathfrak{m} \subset \mathfrak{m}' \cap A$, y se ha de dar la igualdad porque $\mathfrak{m}$ es maximal.

c) ⇒ a) La existencia de $\mathfrak{m}'$ implica que $\mathfrak{m}B \neq B$, luego B es fielmente plano sobre A. ∎

1.5 Conjuntos constructibles

En esta sección demostraremos algunos resultados topológicos sobre homomorfismos de esquemas, todos ellos basados en la noción de conjunto constructible que definimos a continuación:

Definición 1.25 Si X es un espacio topológico, un subconjunto $E \subset X$ es *constructible* si es de la forma

$$E = \bigcup_{i=1}^{n} (U_i \cap C_i),$$

donde los conjuntos $U_i \subset X$ son abiertos y los $C_i \subset X$ cerrados.

Es evidente que el complementario, una unión finita y una intersección finita de conjuntos constructibles es constructible. Equivalentemente, la familia de todos los subconjuntos constructibles de X es el álgebra de Boole generada por los abiertos de X. También es evidente que la antiimagen de un conjunto constructible por una aplicación continua es constructible.

Usaremos a menudo el teorema siguiente:

Teorema 1.26 *Si X es un espacio topológico noetheriano y $E \subset X$, las afirmaciones siguientes son equivalentes:*

a) E es constructible.

b) Para todo cerrado irreducible $T \subset X$, o bien $E \cap T$ contiene un abierto no vacío de T, o bien $E \cap T$ es diseminado en T, es decir, su clausura tiene interior vacío.

Demostración: Si E es constructible, entonces $E \cap T$ es constructible en T, luego podemos suponer que $X = T$ es irreducible. Expresemos E según la definición de conjunto constructible. Podemos suponer que $U_i \cap C_i \neq \varnothing$ para todo i. Si uno de los C_i contiene a U_i, entonces E contiene el abierto no vacío U_i. En caso contrario, los abiertos $U_i \setminus (U_i \cap C_i)$ son no vacíos. Como X es irreducible, su intersección también es no vacía, y es un abierto $V \subset X \setminus E$. Así, $\overline{E} \subset X \setminus V$, luego $\overline{E}$ no puede contener ningún abierto no vacío, ya que dicho abierto no cortaría a V.

Vamos a probar el recíproco por inducción noetheriana, es decir, probaremos que todos los subconjuntos cerrados de X cumplen el teorema. Si no fuera así, podríamos encontrar un cerrado X_0 que no cumple el teorema pero tal que todo cerrado estrictamente contenido en X_0 sí que lo cumple. Equivalentemente, podemos suponer que todo cerrado estrictamente contenido en X cumple el teorema y probar que X también lo cumple.

Sea, pues, $E \subset X$ un subconjunto que cumpla b). Si $Y \subsetneq X$ es cerrado, tenemos que $E \cap Y$ cumple b) para Y, luego, por hipótesis de inducción $E \cap Y$ es constructible en Y (luego también en X).

Si X es reducible, digamos $X = X_1 \cup X_2$, donde X_1 y X_2 son cerrados estrictamente contenidos en X, entonces tenemos que $E = (E \cap X_1) \cup (E \cap X_2)$ es constructible.

Supongamos, pues, que X es irreducible. En tal caso podemos aplicar b) a $T = X$, y tenemos dos posibilidades: o bien E contiene un abierto no vacío U, en cuyo caso $E = U \cup (E \cap (X \setminus U))$ es constructible por la hipótesis de inducción aplicada al cerrado $X \setminus U$, o bien $E \subset \overline{E} \subsetneq X$, en cuyo caso E es constructible por la hipótesis de inducción aplicada a $\overline{E}$. ∎

Una forma de probar que un conjunto es abierto es demostrar primero que es constructible y luego aplicar el teorema siguiente:

Teorema 1.27 *Sea X un esquema noetheriano y $E \subset X$ un subconjunto constructible. Entonces E es abierto si y sólo si es estable por generalización, es decir, si cuando contiene un punto contiene a todas sus generalizaciones.*

Demostración: Es obvio que los abiertos son estables por generalización. Supongamos ahora que E tiene esta propiedad. Como en el teorema anterior, razonamos por inducción noetheriana. Si $Y \subsetneq X$ es cerrado, es obvio que $E \cap Y$ es constructible en Y y estable por generalización, luego $E \cap Y$ es abierto en Y.

Si X es reducible, digamos $X = X_1 \cup X_2$, con X_1, X_2 cerrados estrictamente contenidos en X, entonces

$$X \setminus E = ((X \setminus E) \cap X_1) \cup ((X \setminus E) \cap X_2)$$

es cerrado en X por hipótesis de inducción, luego E es abierto. Si X es irreducible, podemos suponer que $E \neq \varnothing$, en cuyo caso E contiene al punto genérico de X, es decir, es denso. El teorema 1.26 implica entonces que E contiene un abierto no vacío U, con lo que $E = U \cap ((X \setminus U) \cap E)$ es abierto por hipótesis de inducción. ∎

Ahora nos hace falta un resultado técnico:

Teorema 1.28 *Sea $X = \operatorname{Esp} B$ un esquema afín noetheriano y sea E un subconjunto constructible de X. Entonces existe una B-álgebra B' finitamente generada tal que la imagen del homomorfismo $\operatorname{Esp} B' \longrightarrow X$ es exactamente E.*

Demostración: Supongamos en primer lugar que $E = U \cap C$, donde C es cerrado y U es un abierto principal, $U = D(b)$, con $b \in B$. Pongamos que $C = V(I)$, donde I es un ideal de B. Sea $B' = (B/I)_{\bar{b}}$. Claramente B' está generada sobre B por $1/\bar{b}$, y es inmediato que cumple el teorema.

En el caso general, podemos expresar E como unión finita de conjuntos $U_i \cap C_i$, para $i = 1, \ldots, m$, donde los abiertos U_i son principales. Sea B'_i una B-álgebra que cumpla el teorema para $U_i \cap C_i$ y sea $B' = B'_1 \oplus \cdots \oplus B'_m$, de modo que $\operatorname{Esp} B'$ puede verse como la unión disjunta de los esquemas $\operatorname{Esp} B'_i$, y nuevamente es obvia la conclusión. ∎

Finalmente podemos probar el resultado fundamental:

Teorema 1.29 (Chevaley) *Sea $f : X \longrightarrow Y$ un homomorfismo de tipo finito entre esquemas noetherianos. Si $E \subset X$ es un conjunto constructible, entonces $f[E]$ es constructible.*

DEMOSTRACIÓN: Podemos cubrir Y por un número finito de abiertos afines U, y basta probar que $f[E] \cap U = f[E \cap f^{-1}[U]]$ es constructible. Puesto que $E \cap f^{-1}[U]$ es constructible, no perdemos generalidad si suponemos que $Y = \operatorname{Esp} A$ es afín. Similarmente, podemos cubrir X por un número finito de abiertos afines V, y basta probar que cada $f[E \cap V]$ es constructible. Equivalentemente, podemos suponer que $X = \operatorname{Esp} B$ también es afín.

Supongamos en primer lugar que $E = X$ y veamos que $f[X]$ es constructible mediante el teorema 1.26. Sea T un cerrado irreducible en Y, que será de la forma $T = V(\mathfrak{p}) = \operatorname{Esp}(A/\mathfrak{p})$, para cierto $\mathfrak{p} \in \operatorname{Esp} A$. Suponemos que $f[X] \cap T$ no es diseminado en T (es decir, que es denso) y hemos de probar que contiene un abierto no vacío de T.

Sean $A' = A/\mathfrak{p}$, $B' = B/\mathfrak{p}B$. Así, el homomorfismo $\phi : A' \longrightarrow B'$ se corresponde con la restricción $f^{-1}[T] \longrightarrow T$, que es densa. Notemos que ϕ es inyectivo, ya que si I es su núcleo, entonces $f[X] \cap T \subset V(I)$, luego ha de ser $V(I) = \operatorname{Esp} A'$ y, en particular, I contiene al ideal nulo. Ahora es claro que basta demostrar lo siguiente:

Si A es un dominio íntegro noetheriano y B es un anillo que contiene a A y es finitamente generado como A-álgebra, la imagen del homomorfismo natural $f : \operatorname{Esp} B \longrightarrow \operatorname{Esp} A$ contiene un abierto no vacío.

Pongamos que $B = A[x_1, \ldots, x_n]$ y digamos que $x_1, \ldots, x_r$ son algebraicamente independientes, mientras que los demás x_i son algebraicos sobre el álgebra $A^* = A[x_1, \ldots, x_r]$. Entonces, cada x_i con $i > r$ cumple una ecuación de la forma

$$g_{i0}(x)x_i^{d_i} + g_{i1}(x)x_i^{d_i-1} + \cdots = 0,$$

donde los $g_{ij}(x) \in A[x_1, \ldots, x_r]$ son polinomios y $g_{i0}(x) \neq 0$. Podemos suponer que $r < n$, ya que en caso contrario f sería claramente suprayectivo. Sea

$$g(x) = \prod_{i=r+1}^{n} g_{i0}(x),$$

que es un polinomio no nulo. Sea $a \in A$ uno de sus coeficientes no nulos. Vamos a probar que el abierto principal $D(a)$ está contenido en la imagen de f. Sea $\mathfrak{p} \in \operatorname{Esp} A$ tal que $a \notin \mathfrak{p}$ y sea $\mathfrak{p}^* = \mathfrak{p}A^*$ (el conjunto de los polinomios con coeficientes en $\mathfrak{p}$). Entonces $g \notin \mathfrak{p}^*$, luego $B_{\mathfrak{p}^*}$ es una extensión entera de $A^*_{\mathfrak{p}^*}$ (pues en las relaciones polinómicas de los x_i podemos dividir entre el coeficiente director).

Por [AC 3.63] existe un primo $\mathfrak{P}$ de $B_{\mathfrak{p}^*}$ cuya imagen en $A^*_{\mathfrak{p}^*}$ es $\mathfrak{p}^*A^*_{\mathfrak{p}^*}$. Así,

$$\mathfrak{P} \cap A = \mathfrak{P} \cap A^*_{\mathfrak{p}^*} \cap A = \mathfrak{p}^*A^*_{\mathfrak{p}^*} \cap A^* \cap A = \mathfrak{p}^*A^* \cap A = \mathfrak{p},$$

luego $\mathfrak{p} = (\mathfrak{P} \cap B) \cap A = f(\mathfrak{P} \cap B)$.

Esto acaba la prueba de que $f[X]$ es constructible. Si $E \subset X$ es un conjunto constructible arbitrario, el teorema anterior nos da un homomorfismo de tipo finito $X' \longrightarrow X$ cuya imagen es E, luego la imagen de la composición $X' \longrightarrow Y$ es $f[E]$, que resulta ser constructible por la parte ya probada. ∎

Para homomorfismos planos la situación es más simple:

Teorema 1.30 *Todo homomorfismo plano de tipo finito entre esquemas localmente noetherianos es abierto.*

Demostración: Sea $f : X \longrightarrow Y$ en las condiciones del enunciado y sea $U \subset X$ un abierto. Si $V \subset Y$ es un abierto noetheriano, basta probar que el conjunto $f[U] \cap V = f[U \cap f^{-1}[V]]$ es abierto, luego podemos suponer que Y es afín y noetheriano. Similarmente, descomponiendo U en unión de abiertos afines, podemos suponer que $U = X$ es afín. Por el teorema anterior sabemos que $f[X]$ es constructible, y por 1.27 basta probar que es estable por generalización.

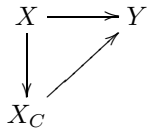
Equivalentemente, tenemos un homomorfismo plano de tipo finito $A \longrightarrow B$ entre anillos noetherianos y queremos probar que si $\mathfrak{P} \in \operatorname{Esp} B$ y $\mathfrak{q} \in \operatorname{Esp} A$ cumplen $\mathfrak{q} \subset \mathfrak{p} = \mathfrak{P} \cap A$, entonces existe un $\mathfrak{Q} \in \operatorname{Esp} B$ tal que $\mathfrak{Q} \subset \mathfrak{P}$ y $\mathfrak{q} = \mathfrak{Q} \cap A$.

Podemos cambiar A y B por $A_\mathfrak{p}$ y $B_\mathfrak{P}$ o, equivalentemente, suponer que A y B son anillos locales. Entonces B es fielmente plano sobre A, y basta tener el cuenta el teorema 1.24. ∎

Veamos ahora qué podemos decir si eliminamos la condición de finitud. Nos restringiremos al caso de esquemas afines:

Teorema 1.31 *Sea $f : X \longrightarrow Y$ un homomorfismo de un esquema afín X en un esquema afín noetheriano Y. Entonces $f[X]$ es intersección de una familia de conjuntos constructibles de Y.*

Demostración: Sea $X = \operatorname{Esp} B$, $Y = \operatorname{Esp} A$. Sea $\mathcal{F}$ la familia de las subálgebras de B que son finitamente generadas sobre A. Para cada $C \in \mathcal{F}$, sea $X_C = \operatorname{Esp} C$ y sea $g_C : X_C \longrightarrow Y$ el homomorfismo natural. Por el teorema 1.29, tenemos que $g_C[X_C]$ es constructible en Y. Los diagramas conmutativos



muestran que

$$f[X] \subset \bigcap_{C \in \mathcal{F}} g_C[X_C].$$

Vamos a probar que se da la igualdad. Para ello tomamos un $\mathfrak{p} \in Y \setminus f[X]$. Esto significa que la fibra de $\mathfrak{p}$ es vacía o, equivalentemente, que $B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} = 0$, o

también que $\mathfrak{p}B_\mathfrak{p} = B_\mathfrak{p}$. A su vez, esto significa que podemos expresar

$$1 = \sum_{i=1}^{n} \pi_i(b_i/s),$$

donde $\pi_i \in \mathfrak{p}$, $b_i \in B$, $s \in A \setminus \mathfrak{p}$. La igualdad es en $B_\mathfrak{p}$, lo que significa, explícitamente, que existe un $s' \in A \setminus \mathfrak{p}$ tal que, en B,

$$s'(\sum_{i=1}^{n} \pi_i b_i - s) = 0.$$

Tomemos $C \in \mathcal{F}$ que contenga a los b_i. Entonces, deshaciendo los pasos anteriores llegamos a que $\mathfrak{p}(B_C)_\mathfrak{p} = (B_C)_\mathfrak{p}$ o, lo que es lo mismo, a que la fibra de $\mathfrak{p}$ respecto a g_C es vacía o, también, a que $\mathfrak{p} \in Y \setminus g_C[X_C]$. ∎

Vamos a combinar el teorema anterior con el siguiente:

Teorema 1.32 *Sea X un esquema afín noetheriano y E una intersección de subconjuntos constructibles de X. Si E es estable por especialización (es decir, cuando contiene a un punto, contiene a todas sus especializaciones), entonces E es cerrado.*

Demostración: Pongamos que $E = \bigcap_{i\in I} E_i$, donde cada $E_i \subset X$ es constructible.

Sea W una componente irreducible de $\overline{E}$ y $\xi \in W$ su punto genérico. Entonces $W \cap E$ es denso en W. En efecto, un abierto no vacío en W es de la forma $U \cap W$, donde U es abierto en X. Si V es el complemento en X de las demás componentes irreducibles de $\overline{E}$, entonces $V \cap W \neq \varnothing$, y, como W es irreducible, $U \cap V \cap W \neq \varnothing$. Claramente, entonces, $U \cap V \cap E \neq \varnothing$, y cualquier punto en esta intersección está en $U \cap W \cap E \neq \varnothing$.

Por consiguiente, $W \cap E_i$ también es denso en W. Por 1.26, vemos que $W \cap E_i$ contiene un abierto en W no vacío, luego $\xi \in E_i$. Como esto es cierto para todo i, resulta que $\xi \in E$. Pero todos los puntos de W son especializaciones de ξ, luego $W \subset E$. Como esto es cierto para todas las componentes irreducibles W, concluimos que $E = \overline{E}$. ∎

Ahora podemos probar un último teorema sobre los homomorfismos fielmente planos:

Teorema 1.33 *Sea A un anillo noetheriano, B una A-álgebra, $X = \operatorname{Esp} B$, $Y = \operatorname{Esp} A$ y $f : X \longrightarrow Y$ el homomorfismo natural. Si B es fielmente plano sobre A, entonces un conjunto $C \subset Y$ es cerrado en Y si y sólo si $f^{-1}[C]$ es cerrado en X.*

Demostración: Supongamos que $f^{-1}[C]$ es cerrado en X. Esto significa que $f^{-1}[C] = V(I)$, donde I es un ideal de B. Sabemos que f es suprayectivo por 1.24, luego $C = f[f^{-1}[C]]$. Aplicamos 1.31 al homomorfismo asociado a la composición $A \longrightarrow B \longrightarrow B/I$, que nos da que C es intersección de conjuntos

constructibles. Por el teorema anterior, basta probar que C es cerrado por especializaciones.

Tomemos, pues, $\mathfrak{p}_1,\ \mathfrak{p}_2 \in Y,\ \mathfrak{p}_2 \subset \mathfrak{p}_1,\ \mathfrak{p}_2 \in C$. Hemos de probar que $\mathfrak{p}_1 \in C$. Podemos tomar $\mathfrak{P}_1 \in X$ tal que $f(\mathfrak{P}_1) = \mathfrak{p}_1$. El homomorfismo natural $A_{\mathfrak{p}_1} \longrightarrow B_{\mathfrak{P}_1}$ es plano, luego fielmente plano, luego el homomorfismo $\operatorname{Esp} B_{\mathfrak{P}_1} \longrightarrow \operatorname{Esp} A_{\mathfrak{p}_1}$ es suprayectivo, luego existe un ideal $\mathfrak{P}_2 \in X$ tal que $\mathfrak{P}_2 \subset \mathfrak{P}_1$, $f(\mathfrak{P}_2) = \mathfrak{p}_2$. Como $\mathfrak{P}_2 \in f^{-1}[C]$ y este conjunto es cerrado, también $\mathfrak{P}_1 \in f^{-1}[C]$, luego $\mathfrak{p}_1 \in C$. ∎

Notemos que, bajo las hipótesis del teorema anterior, se cumple igualmente que un conjunto $U \subset Y$ es abierto si y sólo si $f^{-1}[U]$ es abierto en X. Esto significa que la topología de Y es la topología cociente inducida por f desde X.

Capítulo II

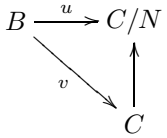
Anillos locales completos

Dedicamos este segundo capítulo a demostrar algunos resultados sobre anillos locales completos respecto a la topología $\mathfrak{m}$-ádica determinada por su ideal maximal. Recordemos que, en general, [AC 4.2 y 4.8] si A es un anillo, I es un ideal de A y M es un A-módulo, la topología I-ádica en M es la única topología en M compatible con la estructura de A-módulo (es decir, que hace continuas a las operaciones de M) y que tiene a los submódulos I^nM como base de entornos de 0. Según [AC 4.21], si M es finitamente generado e I está contenido en todos los ideales maximales de A (en particular, si A es local e I es su ideal maximal) entonces la topología I-ádica en M es de Hausdorff.

2.1 Suavidad formal

La suavidad formal es un concepto técnico debido a Grothendieck que nos permitirá demostrar fácilmente algunos teoremas de estructura sobre anillos locales completos debidos a Cohen, así como otras propiedades de interés de este tipo de anillos.

Definición 2.1 Sea A un anillo, B una A-álgebra e I un ideal de B. Diremos que B es I-*suave* sobre A si para toda A-álgebra C, todo ideal N de C tal que $N^2 = 0$ y todo A-homomorfismo $u : B \longrightarrow C/N$ tal que $u[I^n] = 0$ para cierto $n \geq 1$ (es decir, que sea continuo cuando en B consideramos la topología I-ádica y en C/N la topología discreta), existe un A-homomorfismo v que hace conmutativo el diagrama



Diremos que v es una *elevación* de u. Si cada u tiene una única elevación v diremos que B es I-*llano* sobre A.

Notemos que la elevación v es necesariamente continua, ya que si $u[I^n] = 0$, entonces $v[I^n] \subset N$, luego $v[I^{2n}] \subset N^2 = 0$.

La condición $N^2 = 0$ en la definición anterior supone la reducción al caso más simple de la propiedad que realmente tiene interés, y que viene dada por el teorema siguiente:

Teorema 2.2 *Sea A un anillo, B una A-álgebra, I un ideal de B, C una A-álgebra completa y de Hausdorff para la topología N-ádica y $u : B \longrightarrow C/N$ un homomorfismo continuo (considerando en B la topología I-ádica y en C/N la topología discreta). Entonces u tiene una elevación $v : B \longrightarrow C$.*

Demostración: Podemos considerar a C/N como cociente de C/N^2 sobre el ideal $N' = N/N^2$, para el que se cumple $N'^2 = 0$. La definición anterior nos da una elevación (continua) $u_2 : B \longrightarrow C/N^2$. Nuevamente, podemos considerar C/N^2 como cociente de C/N^3 respecto al ideal $N'' = N^2/N^3$, que también cumple $N''^2 = 0$, lo que nos da una elevación $u_3 : B \longrightarrow C/N^3$. Procediendo de este modo, obtenemos homomorfismos continuos u_i que a su vez determinan un homomorfismo (claramente continuo) $v : B \longrightarrow \varprojlim_i C/N^i = \hat{C} = C$ que cumple el teorema. ∎

Notemos que la hipótesis de que C tenga la propiedad de Hausdorff respecto de la topología N-ádica se usa al final de la prueba, al identificar a C con su compleción $\hat{C}$.

Veamos ahora algunas propiedades elementales de la suavidad formal:

Teorema 2.3 *Sean $A \xrightarrow{g} B \xrightarrow{g'} B'$ homomorfismos de anillos de modo que g' sea continuo para la topología I-ádica de B y la topología I'-ádica de B'. Si B es I-suave (resp. llano) sobre A y B' es I'-suave (resp. llano) sobre B, entonces B' es I'-suave (resp. llano) sobre A.*

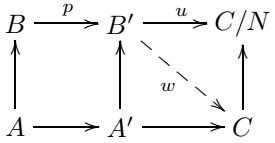
Demostración: Consideremos el diagrama siguiente, donde u, C y N están en las condiciones de la definición de anillo I'-suave sobre A:

$$\begin{array}{ccc} B' & \xrightarrow{u} & C/N \\ {\scriptstyle g'}\uparrow & \overset{v}{\searrow} & \uparrow \\ B & \xrightarrow[w]{} & C \end{array}$$

Como $g' \circ u$ es un A-homomorfismo continuo, se eleva a un A-homomorfismo w que hace conmutativo el diagrama. Éste convierte a C en una B-álgebra y a u en un B-homomorfismo. Usando que B' es I'-suave sobre B, obtenemos un B-homomorfismo v que hace conmutativo el diagrama, el cual prueba que B' es también I'-suave sobre A. La versión para anillos llanos se obtiene sin dificultad. ∎

Teorema 2.4 *Sea A un anillo, sean B y A' dos A-álgebras y sea $B' = B \otimes_A A'$. Si B es I-suave (resp. llano) sobre A, entonces B' es IB'-suave (resp. llano) sobre A'.*

DEMOSTRACIÓN: Tenemos el diagrama siguiente:



donde $u[(IB')^n] = 0$, con lo que $(pu)[I^n] = 0$. Esto implica que pu se eleva a un A-homomorfismo $v : B \longrightarrow C$. Éste induce a su vez un A'-homomorfismo $w : B' \longrightarrow C$, y es fácil ver que es una elevación de u. Las unicidades para el caso de anillos llanos son inmediatas. ∎

Veamos algunos ejemplos de suavidad formal. En primer lugar, es inmediato que un anillo de polinomios $A[X_1, \ldots, X_n]$ es 0-suave sobre A. Otro caso elemental es el siguiente:

Teorema 2.5 *Sea A un anillo y $S \subset A$ un subconjunto multiplicativo. Entonces $S^{-1}A$ es 0-llano sobre A.*

DEMOSTRACIÓN: Si tenemos un A-homomorfismo $u : S^{-1}A \longrightarrow C/N$ en las condiciones de la definición, para cada $s \in S$ necesariamente $u(s) = [s]$ (identificando $s = s \cdot 1 \in C$), y $[s]$ es una unidad en C/N. Esto implica que s es una unidad en C, ya que en caso contrario existiría un ideal primo $\mathfrak{P}$ de C tal que $s \in C$, pero, como N es nilpotente, sería $N \subset \mathfrak{P}$, y entonces $[s] \in \mathfrak{P}/N$ no podría ser una unidad.

El hecho de que los elementos de S sean unidades de C implica que existe un único A-homomorfismo $v : S^{-1}A \longrightarrow C$, que claramente es la única elevación posible de u. ∎

Teorema 2.6 *Sea B un anillo local, sea $\mathfrak{m}$ su ideal maximal y sea $\hat{B}$ su compleción. Entonces B es $\mathfrak{m}$-suave (resp. $\mathfrak{m}$-llano) sobre un anillo A si y sólo si $\hat{B}$ es $\hat{\mathfrak{m}}$-suave (resp. $\hat{\mathfrak{m}}$-llano) sobre A.*

DEMOSTRACIÓN: La clave está en que todo homomorfismo $u : B \longrightarrow C/N$ tal que $u[\mathfrak{m}^n] = 0$ se extiende a un único homomorfismo $\hat{u} : \hat{B} \longrightarrow C/N$, a saber, el inducido por los homomorfismos $u_r : B/\mathfrak{m}^r \longrightarrow C/N$, para $r \geq n$. (En términos topológicos, como C/N es un anillo topológico discreto, es completo, y todo homomorfismo continuo de B en C/N se extiende a la compleción de B.) La extensión cumple además que $\hat{u}[\hat{\mathfrak{m}}^n] = 0$.

Así, si $\hat{B}$ es $\hat{\mathfrak{m}}$ suave (resp. llano) sobre A, el homomorfismo $\hat{u}$ se eleva a un (único) A-homomorfismo $\hat{v} : \hat{B} \longrightarrow C$, que a su vez se restringe a un único A-homomorfismo $v : B \longrightarrow C$, que es una elevación de u, luego B es $\mathfrak{m}$-suave (resp. llano) sobre A.

Recíprocamente, si B es $\mathfrak{m}$-suave (resp. llano) sobre A, un homomorfismo $\hat{u} : \hat{B} \longrightarrow C/N$ se restringe a un homomorfismo $u : B \longrightarrow C/N$, que se eleva a un (único) homomorfismo $v : B \longrightarrow C$, que se extiende a un único homomorfismo $\hat{v} : \hat{B} \longrightarrow C$ que eleva a $\hat{u}$. Así pues, $\hat{B}$ es $\hat{\mathfrak{m}}$-llano (resp. suave) sobre A. ∎

En particular, como A es obviamente $\mathfrak{m}$-llano sobre A, el teorema anterior implica que $\hat{A}$ es $\hat{\mathfrak{m}}$-llano sobre A.

Teorema 2.7 *Sea K/k una extensión de cuerpos.*

a) Si es algebraica separable, entonces K es 0-llano sobre k.

b) Si es separablemente generada, entonces K es 0-suave sobre k.

Demostración: a) Sea C una k-álgebra, $N \subset C$ un ideal tal que $N^2 = 0$ y $u : K \longrightarrow C/N$ un k-homomorfismo. Consideremos una extensión finita intermedia $k \subset L \subset K$. Por el teorema del elemento primitivo, será de la forma $L = k(\alpha)$. Sea $f(X) \in k[X]$ el polinomio mínimo de α. La separabilidad nos da que $f'(\alpha) \neq 0$. Sea $y \in C$ un representante de $u(\alpha)$. Así,

$$[f(y)] = f(u(\alpha)) = u(f(\alpha)) = 0,$$

luego $f(y) \in N$. Como $N^2 = 0$, para todo $n \in N$ tenemos que

$$f(y + n) = f(y) + f'(y)n.$$

(La igualdad es k-lineal en f, luego basta probarla para $f = X^i$.) Pero $f'(\alpha)$ es una unidad en K, luego $u(f'(\alpha)) = [f'(y)]$ es una unidad en C/N, de donde se sigue que $f'(y)$ es una unidad en C. (Por el mismo argumento empleado en la prueba del teorema anterior.) Tomemos entonces $n = -f(y)/f'(y) \in N$. De este modo, $f(y + n) = 0$. Cambiando y por $y + n$ tenemos que $f(y) = 0$. Ahora podemos definir $v_L : L = k[X]/(f(X)) \longrightarrow C$ mediante $v_L(\alpha) = y$, que claramente es una elevación de $u|_L$.

Observemos que la elevación v_L es única, ya que, si tuviéramos dos, cumplirían que $v_1(\alpha) = v_2(\alpha) + n$, con $n \in$ y $f(v_1(\alpha)) = f(v_2(\alpha)) = 0$, luego $f'(v_1(\alpha))n = 0$ y, según hemos visto, $f'(v_1(\alpha))$ sería una unidad en C, luego $n = 0$, luego $v_1(\alpha) = v_2(\alpha)$, luego $v_1 = v_2$.

Esta unicidad permite extender todas las elevaciones v_L hasta un (único) k-homomorfismo $v : K \longrightarrow C$, que es una elevación de u.

b) La hipótesis significa que K es separable sobre una extensión puramente trascendente $k(X)$ de k (donde X es un conjunto de indeterminadas). Por 2.3 y el apartado anterior, podemos suponer que $K = k(X)$. La 0-suavidad se sigue inmediatamente de la definición: si tenemos un homomorfismo $u : K \longrightarrow C/N$, tomamos un conjunto $Y \subset C$ cuyas clases módulo N sean las imágenes por u de las indeterminadas de X. Existe un k-homomorfismo de anillos $v_0 : k[X] \longrightarrow C$ que biyecta X con Y, de modo que compuesto con $C \longrightarrow C/N$ es la restricción de u. Los elementos de $v_0[k[X]]$ son unidades en C/N (porque están en el cuerpo $u[K]$), luego también son unidades en C. Esto permite extender v_0 a un monomorfismo $v : K \longrightarrow C$ que obviamente eleva a u. ∎

Para obtener otros ejemplos de suavidad formal vamos a necesitar varios resultados previos. El primero es elemental:

Teorema 2.8 *Sea A un anillo noetheriano local cuyo ideal maximal sea nilpotente. Entonces un A-módulo es plano si y sólo si es libre.*

DEMOSTRACIÓN: En general, todo módulo libre es plano. Supongamos ahora que M es un A-módulo plano, sea $\mathfrak{m}$ el ideal maximal de A y sea $k = A/\mathfrak{m}$ el cuerpo de restos. Tomemos un conjunto $B \subset M$ tal que las imágenes de B en $M/\mathfrak{m}M = M \otimes_A k$ sean una k-base y vamos a probar que B es una A-base de M. Sea N el submódulo generado por B. Tenemos que $M = N + \mathfrak{m}M$, luego

$$M/N = \mathfrak{m}(M/N) = \mathfrak{m}^2(M/N) = \mathfrak{m}^3(M/N) = \cdots$$

Como $\mathfrak{m}$ es nilpotente, concluimos que $M/N = 0$, luego B es un sistema generador de M.

Ahora basta demostrar que si $m_1, \ldots, m_n \in M$ son k-linealmente independientes en $M/\mathfrak{m}M$, entonces son también A-linealmente independientes. Razonamos por inducción sobre n. Si $n = 1$, suponemos que $am_1 = 0$ y hemos de probar que $a = 0$.

Sea $K \subset A$ el núcleo del homomorfismo $A \longrightarrow A$ dado por la multiplicación por a. La sucesión exacta $K \longrightarrow A \xrightarrow{a} A$ da lugar a otra sucesión exacta

$$K \otimes_A M \longrightarrow M \xrightarrow{a} M.$$

Como x_1 está en el núcleo de la multiplicación por a, podemos expresarlo como $x_1 = b_1y_1 + \cdots + b_ry_r$, donde $b_i \in A$ y $ab_i = 0$. Como x_1 no es nulo en $M/\mathfrak{m}M$, no todos los b_i están en $\mathfrak{m}$, es decir, algún b_i es una unidad, luego $a = 0$.

Supongamos ahora que $a_1x_1 + \cdots + a_nx_n = 0$, con $n > 1$. Razonamos igualmente, pero ahora partiendo del homomorfismo $A^n \longrightarrow A$ determinado por $(b_1, \ldots, b_n) \mapsto a_1b_1 + \cdots + a_nb_n$. Ahora tenemos una sucesión exacta

$$K \otimes_A M \longrightarrow M^n \longrightarrow M$$

y $(x_1, \ldots, x_n)$ está en el núcleo del segundo homomorfismo, luego

$$x_i = \sum_j b_{ij}y_{ij}, \quad \sum_i a_ib_{ij} = 0.$$

Como $x_n \notin \mathfrak{m}M$, ha de ser $b_{nj} \notin \mathfrak{m}$ para algún j. Así, b_{nj} es una unidad, lo que nos permite expresar a_n como combinación lineal de los otros a_i, digamos $a_n = c_1a_1 + \cdots + c_{n-1}a_{n-1}$. Sustituyendo en la combinación lineal original, resulta que

$$a_1(x_1 + c_1x_n) + \cdots + a_{n-1}(x_{n-1} + c_{n-1}x_n) = 0$$

Es claro que los elementos $x_i + c_ix_n$ son k-linealmente independientes en $M/\mathfrak{m}M$, luego, por hipótesis de inducción, concluimos que $a_1 = \cdots = a_{n-1} = 0$, de donde también $a_n = 0$, ya que es combinación lineal de los a_i. ∎

Seguidamente probamos algunos resultados sobre la cohomología de las extensiones de anillos:

Definición 2.9 Sea A un anillo, B una A-álgebra, I un ideal de B y N un B-módulo tal que $I^nN = 0$ para cierto $n > 0$. Un 2-*cociclo continuo simétrico* es una aplicación A-bilineal simétrica $f : B \times B \longrightarrow N$ que cumpla las condiciones siguientes:

a) Para todos los $x, y, z \in B$, se cumple la relación

$$xf(y,z) - f(xy,z) + f(x,yz) - f(x,y)z = 0.$$

b) Existe un $m \geq n$ tal que $f(x,y) = 0$ cuando $x \in I^m$ o $y \in I^m$.

Vamos a ver que un cociclo en estas condiciones nos permite definir lo que se llama una *extensión* de N por B. Definimos $\tau = f(1,1)$, con lo que la propiedad a) nos da que $x\tau = f(x,1)$ para todo $x \in B$. Consideramos el A-módulo $C = (B/I^m) \oplus N$, y definimos en él el producto dado por

$$(\bar{x}, \xi)(\bar{y}, \eta) = (\bar{x}\bar{y}, x\eta + y\xi - f(x,y)).$$

Una comprobación rutinaria muestra que C es así un anillo conmutativo con unidad $(1, \tau)$ y que N es un ideal que cumple $N^2 = 0$ y $C/N \cong B/I^m$. La aplicación $A \longrightarrow C$ dada por $a \mapsto (\bar{a}, a\tau)$ es un homomorfismo de anillos y el diagrama siguiente es conmutativo:

$$\begin{array}{ccc} B & \xrightarrow{u} & C/N \\ \uparrow & & \uparrow \\ A & \longrightarrow & C \end{array}$$

Diremos que el cociclo f *se escinde* si existe un A-homomorfismo $g : B \longrightarrow N$ tal que $f = \partial g$, donde

$$(\partial g)(x,y) = xg(y) - g(xy) + g(x)y.$$

Ésta es la condición necesaria y suficiente para u se eleve a un A-homomorfismo $v : B \longrightarrow C$. En efecto, si existe g, basta definir $v(x) = (\bar{x}, g(x))$. Recíprocamente, si existe v, basta llamar g a la composición de v con la proyección en la segunda componente.

Teorema 2.10 *Sea A un anillo, B una A-álgebra e I un ideal de B.*

a) Si B es I-suave sobre A, entonces todo 2-cociclo continuo simétrico se escinde.

b) Si B/I^n es un A-módulo proyectivo para infinitos valores de n y todo 2-cociclo continuo simétrico se escinde, entonces B es I-suave sobre A.

DEMOSTRACIÓN: El apartado a) es consecuencia inmediata de la discusión previa al teorema. Veamos b). Para ello suponemos un diagrama conmutativo

$$\begin{array}{ccc} B & \xrightarrow{u} & C/N \\ \uparrow & & \uparrow \\ A & \longrightarrow & C \end{array}$$

en el que $u[I^n] = 0$ y $N^2 = 0$. El ideal N puede verse como C/N-módulo y, a través de u, como B-módulo tal que $I^n N = 0$. Cambiando n por un natural mayor, podemos suponer que B/I^n es un A-módulo proyectivo. Por definición, esto significa que el homomorfismo $B/I^n \longrightarrow C/N$ se eleva a un homomorfismo de A-módulos $B/I^n \longrightarrow C$ o, equivalentemente, que existe un homomorfismo de A-módulos $\lambda : B \longrightarrow C$ que induce a u y cumple además que $\lambda[I^n] = 0$. Sólo hemos de probar que podemos exigir que λ sea un homomorfismo de anillos.

Para cada $x, y \in B$, definimos $f(x, y) = \lambda(xy) - \lambda(x)\lambda(y)$. Puesto que λ induce un homomorfismo de anillos módulo N, se cumple que $f(x, y) \in N$. Así, $f : B \times B \longrightarrow N$ es una forma A-bilineal simétrica. Observemos que λ convierte a C en un B-módulo con el producto dado por $x\xi = \lambda(x)\xi$. Puesto que N es un ideal de B, también es un B-submódulo. Con esto es inmediato comprobar que f es un 2-cociclo continuo simétrico.

Por hipótesis, existe un A-homomorfismo $g : B \longrightarrow N$ tal que

$$\lambda(xy) - \lambda(x)\lambda(y) = f(x, y) = xg(y) - g(xy) + g(x)y.$$

Por consiguiente, llamando $v = \lambda + g$, tenemos que

$$v(xy) = \lambda(x)\lambda(y) + \lambda(x)g(y) + \lambda(y)g(x) = v(x)v(y),$$

(puesto que $g(x)g(y) \in N^2 = 0$).

Esto prueba que g es un homomorfismo de A-álgebras, y obviamente eleva a u, al igual que λ. ∎

Esto es todo lo que necesitamos para probar el teorema siguiente:

Teorema 2.11 *Sea A un anillo local, sea $\mathfrak{m}$ su ideal maximal y $k = A/\mathfrak{m}$ su cuerpo de restos. Si B es una A-álgebra plana y $B \otimes_A k$ es 0-suave sobre k, entonces B es $\mathfrak{m}B$-suave sobre A.*

DEMOSTRACIÓN: Basta probar que $B/\mathfrak{m}^n B$ es 0-suave sobre $A/\mathfrak{m}^n$ para todo $n > 0$. En efecto, en tal caso, dado un A-homomorfismo $u : B \longrightarrow C/N$ tal que $u[\mathfrak{m}^n B] = 0$, tenemos que $\mathfrak{m}^n(C/N) = 0$, luego $\mathfrak{m}^n C \subset N$, con lo que $\mathfrak{m}^{2n} C \subset N^2 = 0$. Cambiando n por $2n$ podemos suponer que $\mathfrak{m}^n C = 0$, con lo que C es una $A/\mathfrak{m}^n$-álgebra. Por otra parte, u induce un $A/\mathfrak{m}^n$-homomorfismo $\bar{u} : B/\mathfrak{m}^n B \longrightarrow C/N$. Si $B/\mathfrak{m}^n B$ es 0-suave, entonces $\bar{u}$ se eleva a un $A/\mathfrak{m}^n$-homomorfismo $\bar{v} : B/\mathfrak{m}^n B \longrightarrow C$. El homomorfismo $v : B \longrightarrow C$ deducido de $\bar{v}$ es una elevación de u.

Notemos ahora que $B/\mathfrak{m}^n B = B \otimes_A (A/\mathfrak{m}^n)$ es plano sobre $A/\mathfrak{m}^n$, así como que $(B/\mathfrak{m}^n B) \otimes_{A/\mathfrak{m}^n} k \cong B \otimes_A k$, luego podemos sustituir ambos anillos por los cocientes y suponer que $\mathfrak{m}^n = 0$. El teorema 2.8 nos da entonces que B es un A-módulo libre, luego es proyectivo, y también lo es $B/\mathfrak{m}^n B$ para todo n suficientemente grande (ya que $\mathfrak{m}^n = 0$). Esto nos sitúa en las hipótesis del teorema anterior, luego basta probar que todo 2-cociclo continuo simétrico se escinde.

Tomemos, pues, $f : B \times B \longrightarrow N$, donde $\mathfrak{m}^i N = 0$. Supongamos en primer lugar que $\mathfrak{m}N = 0$. Entonces, llamando $B_0 = B/\mathfrak{m}B = B \otimes_A k$, tenemos que N es un B_0-módulo, y f induce una aplicación bilineal $f_0 : B_0 \times B_0 \longrightarrow N$, que claramente es un 2-cociclo continuo simétrico. Como B_0 es 0-suave sobre k, el teorema anterior nos da que f_0 se escinde, es decir, que existe un k-homomorfismo $g_0 : B_0 \longrightarrow N$ tal que $f_0 = \partial g_0$. Si definimos $g(x) = g_0(\bar{x})$, tenemos un A-homomorfismo $g : B \longrightarrow N$ tal que $f = \partial g$.

En el caso general, sea $f_1 : B \times B \longrightarrow N/\mathfrak{m}N$ la composición de f con el epimorfismo natural $N \longrightarrow N/\mathfrak{m}N$. Es claro que se trata de un 2-cociclo continuo simétrico, y se escinde por el caso anterior. Así pues, $f_1 = \partial \bar{g}_1$, para cierto A-homomorfismo $\bar{g}_1 : B \longrightarrow N/\mathfrak{m}N$. Como B es proyectivo sobre A, existe un A-homomorfismo $g_1 : B \longrightarrow N$ que induce a $\bar{g}_1$ módulo N. Entonces $f_2 = f_1 - \partial g_1$ es un 2-cociclo continuo simétrico con valores en $\mathfrak{m}N$.

Repitiendo la construcción obtenemos $g_2 : B \longrightarrow \mathfrak{m}N$ tal que el cociclo $f_3 = f_1 - \partial(g_1 + g_2)$ toma valores en $\mathfrak{m}^2 N$. Como $\mathfrak{m}$ es nilpotente, tras un número finito de pasos, llegamos a que $f = \partial(g_1 + \cdots + g_n)$. ∎

2.2 Los teoremas de estructura

Aquí vamos a aplicar los resultados de la sección anterior para demostrar ciertos teoremas de estructura para anillos locales completos. En general, si A es un anillo local y k es su cuerpo de restos, podemos distinguir cuatro casos:

I) $\operatorname{car} A = \operatorname{car} k = 0$.

II) $\operatorname{car} A = \operatorname{car} k = p$, para cierto primo p.

III) $\operatorname{car} A = 0$, $\operatorname{car} k = p$, para cierto primo p.

IV) $\operatorname{car} A = p^n$, $\operatorname{car} k = p$, para cierto primo p y cierto $n > 1$.

En los dos primeros casos diremos que el anillo A es *equicaracterístico*. El caso IV es el más complicado y no nos va a interesar. Notemos que no puede darse si, por ejemplo, A es un dominio íntegro.

Por ejemplo, si $A = k[[X_1, \ldots, X_n]]$ es un anillo de series formales de potencias sobre un cuerpo k, entonces su cuerpo de restos es k, luego es un anillo local completo equicaracterístico. Veremos que, recíprocamente, los anillos locales completos equicaracterísticos están cerca de ser anillos de series formales de potencias. La parte delicada de la prueba consiste en demostrar que tienen cuerpos de coeficientes, en el sentido de la definición siguiente:

Definición 2.12 Sea A un anillo local equicaracterístico y k su cuerpo de restos. Un *cuerpo de coeficientes* de A es un subcuerpo K de A tal que el epimorfismo canónico $A \longrightarrow k$ se restringe a un isomorfismo $K \longrightarrow k$.

Teorema 2.13 *Todo anillo local completo equicaracterístico tiene un cuerpo de coeficientes.*

DEMOSTRACIÓN: Sea A un anillo local completo equicaracterístico, sea $\mathfrak{m}$ su ideal maximal y sea $k = A/\mathfrak{m}$ su cuerpo de restos. Si $\operatorname{car} A = 0$, entonces A contiene a $\mathbb{Z}$ y $\mathbb{Z} \cap \mathfrak{m} = 0$ o, de lo contrario, k tendría característica prima. Por consiguiente A contiene a $\mathbb{Q}$. Tanto en este caso como si A tiene característica prima, tenemos que A contiene un cuerpo perfecto k_0, y k puede verse como una extensión de k_0 a través del epimorfismo natural $A \longrightarrow k$. Por [GA 1.32], dicha extensión es separablemente generada, es decir, tiene una base de trascendencia $S \subset k$ tal que $k/k_0(S)$ es algebraica separable. Sea $S' \subset A$ un conjunto de representantes de los elementos de S. Es claro entonces que $k_0[S'] \cap \mathfrak{m} = 0$, luego A contiene un cuerpo $K = k_0(S)$ cuya imagen en k es $k_0(S)$.

Por 2.7 sabemos que k/K es 0-llano y, por 2.2, la identidad $k \longrightarrow A/\mathfrak{m}$ da lugar a un K-homomorfismo continuo $k \longrightarrow A$ cuya imagen es un cuerpo de coeficientes de A. ∎

Si A es un anillo local en el caso III) de la división que hemos hecho al principio de la sección, entonces A contiene a $\mathbb{Z}$ y su ideal maximal $\mathfrak{m}$ contiene al primo p. Vamos a empezar estudiando el caso más sencillo:

Definición 2.14 Diremos que un anillo de valoración discreta A de característica 0 es un *p-anillo* si su ideal maximal está generado por el primo $p \in \mathbb{Z}$.

Si K es un cuerpo de característica prima p, existe un p-anillo cuyo cuerpo de restos es isomorfo a K. Esto resulta de aplicar el teorema siguiente a $A = \mathbb{Z}_p$.

Teorema 2.15 *Sea A un anillo de valoración discreta, sea $\mathfrak{m} = (\pi)$ su ideal maximal, sea k su cuerpo de restos y K una extensión de k. Entonces existe un anillo de valoración discreta B que contiene a A, cuyo ideal maximal está generado también por π y cuyo cuerpo de restos es isomorfo a K.*

DEMOSTRACIÓN: Sea S una base de trascendencia de K sobre k y sea $k_1 = k(S)$. Sea $A' = A[X]$ un anillo de polinomios, donde X es un conjunto de indeterminadas en biyección con S. Podemos definir una valoración en A' asignando a cada polinomio el mínimo de los valores de sus coeficientes no nulos (respecto de la valoración de A). Su anillo de enteros es $A_1 = A'_{\pi A'}$, que es, por lo tanto, un anillo de valoración discreta. Además $A_1/\pi A_1 \cong k_1$.

Esto nos permite reducir el problema al caso en que el cuerpo K es algebraico sobre k. Fijamos una clausura algebraica L del cuerpo de cocientes de A. Aplicamos el lema de Zorn al conjunto de todos los pares (B, ϕ), donde $A \subset B \subset L$, B es un anillo de valoración discreta en el que π es primo y $\phi : B \longrightarrow K$ es un A-homomorfismo cuyo núcleo es el ideal generado por π en B. Consideramos el orden dado por $(B, \phi) \leq (B', \phi')$ si $B \subset B'$ y $\phi'|_B = \phi$.

Si tenemos una cadena de tales pares, es obvio que la unión de sus anillos es un subanillo B de L, que los homomorfismos se extienden a un homomorfismo $\phi : B \longrightarrow K$ con núcleo πB, y que las valoraciones en cada anillo se extienden a una valoración en B con primo π respecto a la que B es el anillo de enteros. Así pues, (B, ϕ) es una cota superior de la cadena. Por consiguiente, existe un par maximal (B, ϕ), y hemos de probar que la imagen de ϕ es todo K.

Dicha imagen es un cuerpo $K_0 \cong B/\pi B$. Si $K_0 \subsetneq K$ podemos tomar un $\alpha \in K \setminus K_0$. Su polinomio mínimo sobre K_0 será la imagen de un polinomio mónico $f(X) \in B[X]$. Obviamente, $f(X)$ ha de ser irreducible en $B[X]$, luego también en $B_0[X]$ (donde B_0 es el cuerpo de cocientes de B). Sea α' una raíz de $f(X)$ en L y sea $B' = B[\alpha'] \cong B[X]/(f)$. Es claro que ϕ se extiende a un homomorfismo $\phi' : B' \longrightarrow K$ tal que $\phi'(\alpha') = \alpha$. Además

$$B'/\pi B' \cong B[X]/(\pi, f) \cong K_0[X]/(f) \cong K_0[\alpha].$$

En particular, $\pi B'$ es un ideal maximal. Como B' es entero sobre B, tenemos que todo ideal maximal de B' contiene a π (teorema [AC 3.63]), luego $\pi B'$ es el único ideal maximal de B'. En definitiva, B' es un anillo noetheriano local cuyo ideal maximal es principal. Esto implica que B' es un anillo de valoración discreta, ya que todo elemento no nulo de B' puede escribirse como $\epsilon\pi^n$, donde ϵ es una unidad, luego B' es el anillo de enteros de la valoración asociada al primo π. Con esto tenemos probado que (B', ϕ') contradice la maximalidad de (B, ϕ).

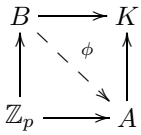
Concluimos que $B/\pi B \cong K$, luego B cumple el teorema. ∎

Ahora usamos la noción de suavidad formal para probar un teorema de existencia de homomorfismos:

Teorema 2.16 *Sea B un p-anillo y A un anillo completo local. Para cada monomorfismo $\phi_0 : k \longrightarrow K$ entre sus cuerpos de restos respectivos, existe un homomorfismo $\phi : B \longrightarrow A$ que induce a ϕ_0.*

Demostración: Sea $k_0 \subset k$ el cuerpo primo. Como K ha de tener característica p, vemos que el ideal maximal de A, llamémoslo $\mathfrak{m}$, contiene a p, y no puede contener a ningún otro primo. Por consiguiente, el homomorfismo natural $\mathbb{Z} \longrightarrow A$ se extiende a un homomorfismo local $\mathbb{Z}_p \longrightarrow A$.

Por otra parte, $B \otimes_{\mathbb{Z}_p} k_0 = B/pB = k$ es una extensión separablemente generada de k_0 (porque k_0 es perfecto, de nuevo por [GA 1.32]), luego es 0-suave sobre k_0, por el teorema 2.7. Además, B es un $\mathbb{Z}_p$-módulo libre de torsión, luego es plano (Teorema [AC A8]). El teorema 2.11 nos da que B es pB-suave sobre $\mathbb{Z}_p$ y el teorema 2.2 nos da un A-homomorfismo ϕ que hace conmutativo el diagrama siguiente:



La flecha horizontal superior es la composición $B \longrightarrow k \xrightarrow{\phi_0} K$, luego ϕ cumple lo pedido. ∎

De aquí se deduce un teorema de unicidad sobre p-anillos:

Teorema 2.17 *Para cada cuerpo k de característica prima p, existe (salvo isomorfismo) un único p-anillo completo local que tiene a k por cuerpo de restos.*

Demostración: Ya hemos visto (por el teorema 2.15) que existe un p-anillo cuyo cuerpo de restos es isomorfo a k. Su compleción será un p-anillo completo local con el mismo cuerpo de restos. Falta probar la unicidad. Supongamos que B y B' cumplen ambos estas condiciones. El teorema anterior nos da un homomorfismo $\phi : B \longrightarrow B'$ que induce la identidad entre los cuerpos de restos.

Claramente $\phi(p) = p$, y $B' = \phi[B] + pB'$. Así, todo elemento $x \in B'$ puede expresarse como

$$x = \phi(b_0) + px_1 = \phi(b_0 + pb_1) + p^2x_2 = \phi(b_0 + pb_1 + p^2b_2) + p^3x_3 = \cdots$$

En definitiva, si llamamos

$$y_n = \sum_{i=0}^{n} b_i p^i, \quad y = \sum_{i=0}^{\infty} b_i p^i \in B,$$

tenemos que $x - \phi(y) = x - \phi(y_n) - \phi(y - y_n) \in p^{n+1}B'$, para todo n, luego $x = \phi(y)$. Por consiguiente, ϕ es suprayectivo. Entonces, su núcleo ha de ser un ideal primo, pero, ciertamente, no es pB, luego ha de ser 0, lo que nos da que ϕ es un isomorfismo. ∎

Es obvio que un anillo local no equicaracterístico no puede tener un cuerpo de coeficientes, pero ahora es fácil probar que sí tiene un anillo de coeficientes en el sentido de la definición siguiente:

Definición 2.18 Sea A un anillo completo local de característica 0 cuyo cuerpo de restos tenga característica prima p, sea $\mathfrak{m}$ su ideal maximal. Un *anillo de coeficientes* de A es un anillo noetheriano local completo $A_0 \subset A$, cuyo ideal maximal es pA_0 y tal que $A = A_0 + \mathfrak{m}$ o, equivalentemente, $k = A/\mathfrak{m} \cong A_0/pA_0$.

Teorema 2.19 *Si A es un anillo completo local de característica 0 cuyo cuerpo de restos tiene característica prima, entonces tiene un anillo de coeficientes que es un anillo de valoración discreta completo.*

Demostración: Por el teorema anterior existe un p-anillo completo A_0 cuyo cuerpo de restos es el de A. Por 2.16 existe un homomorfismo $\phi : A_0 \longrightarrow A$ que induce un isomorfismo entre los cuerpos de restos. Se cumple que ϕ es inyectivo, pues los únicos ideales no nulos de A_0 son los de la forma p^nA_0 y ninguno de ellos está contenido en el núcleo (porque A tiene característica 0). Obviamente, A_0 cumple lo pedido. ∎

Notemos que si consideramos a los cuerpos como 0-anillos, entonces un cuerpo de coeficientes en el sentido de la definición 2.12 puede considerarse un anillo de coeficientes en el sentido de 2.18.

Para llegar a los teoremas de estructura necesitamos un último resultado técnico elemental sobre anillos completos:

Teorema 2.20 *Sea A un anillo, I un ideal y M un A-módulo. Supongamos que A es completo con la topología I-ádica y que la topología I-ádica en M es de Hausdorff. Si M/IM está generado sobre A/I por $\bar{\omega}_1, \ldots, \bar{\omega}_n$, para ciertos $\omega_1, \ldots, \omega_n \in M$, entonces éstos son un generador de M sobre A.*

DEMOSTRACIÓN: Sea $N \subset M$ el submódulo generado por $\omega_1, \ldots, \omega_n$. Tenemos que $M = N + IM$. Así, todo $\xi \in M$ puede expresarse como

$$\xi = a_1\omega_1 + \cdots + a_n\omega_n + \xi_1, \quad \xi_1 \in IM.$$

A su vez, $\xi_1 = a_{11}\omega_1 + \cdots + a_{n1}\omega_n + \xi_2$, donde $a_{i1} \in I$, $\xi_2 \in I^2M$. De nuevo, $\xi_2 = a_{12}\omega_1 + \cdots + a_{n2}\omega_n + \xi_3$, donde $a_{i2} \in I^2$, $\xi_3 \in I^3M$. De este modo obtenemos expresiones de la forma

$$\xi = (a_1 + a_{11} + \cdots + a_{1m})\omega_1 + \cdots + (a_n + a_{n1} + \cdots + a_{nm})\omega_n + \xi_{m+1},$$

donde $a_{ij} \in I^j$, $\xi_{m+1} \in I^{m+1}M$. Sea $b_i = \sum_j a_{ij} \in A$, de modo que

$$\xi - b_1\omega_1 - \cdots - b_n\omega_n \in \bigcap_m I^m M = 0.$$

Así pues, $\xi \in N$. ∎

Teorema 2.21 *Sea A un anillo noetheriano local completo. En el caso en que no sea equicaracterístico, supongamos además que A es un dominio íntegro. Entonces A contiene un subanillo A' local, regular y completo, con el mismo cuerpo de restos, de modo que A es una A'-álgebra finita.*

DEMOSTRACIÓN: Sea $\mathfrak{m}$ el ideal maximal de A y $k = A/\mathfrak{m}$ su cuerpo de restos. Vamos a tratar simultáneamente el caso en que $\operatorname{car} A = \operatorname{car} k$ (caso 1) y el caso en que A es un dominio íntegro de característica 0 y k es un cuerpo de característica prima p (caso 2).

Sea A_0 un anillo de coeficientes de A, entendiendo que es un cuerpo en el caso 1 (teorema 2.13) y un anillo de valoración discreta completo en el caso 2.

En el caso 2 tenemos que $\dim A/pA < \dim A$, luego el teorema [A 5.18] nos da un sistema de parámetros $y_1, \ldots, y_n$ de A tal que $y_1 = p$. En el caso 1 tomamos un sistema de parámetros arbitrario $y_1, \ldots, y_n$. Notemos que $n = \dim A$.

Sea $A_0[[Y]]$ el anillo de las series formales de potencias con coeficientes en A_0 e indeterminadas $Y_1, \ldots, Y_n$ en el caso 1 o $Y_2, \ldots, Y_n$ en el caso 2. Podemos definir un A_0-homomorfismo de anillos $\phi : A_0[[Y]] \longrightarrow A$ mediante $Y_i \mapsto y_i$. En el caso 2 convenimos en llamar $Y_1 = p \in A_0$, de modo que también se cumple $\phi(Y_1) = y_1$. Sea $A' \subset A$ la imagen de ϕ, sea $\mathfrak{m}' = (y_1, \ldots, y_n)_{A'}$ y sea $\mathfrak{m}_0 = (Y_1, \ldots, Y_n)_{A_0[[Y]]}$.

Observemos que $\mathfrak{m}'$ está formado por las series de potencias en $y_1, \ldots, y_n$ con término independiente nulo en el caso 1 o por las series de potencias en

$y_2, \ldots, y_n$ con término independiente múltiplo de p en el caso 2. En ambos casos, los elementos de A' que no están en $\mathfrak{m}'$ son unidades, pues son series de potencias cuyo término independiente es una unidad de A_0. Por lo tanto, $\mathfrak{m}'$ es el único ideal maximal de A'. Claramente, A' es un anillo noetheriano local completo. Tenemos monomorfismos

$$k = A_0[[Y]]/\mathfrak{m}_0 \longrightarrow A'/\mathfrak{m}' \longrightarrow A/\mathfrak{m} = k.$$

(El segundo es inyectivo porque si una serie de potencias en $y_1, \ldots, y_n$ con coeficientes en A_0 está en $\mathfrak{m}$, necesariamente su término independiente está en $\mathfrak{m} \cap A_0 \subset \mathfrak{m}'$.) Así pues, $A'/\mathfrak{m}' = A/\mathfrak{m}$.

Si M es un A-módulo de longitud finita, sus factores de composición son A-módulos isomorfos a $A/\mathfrak{m}$, luego también son A'-módulos isomorfos a $A'/\mathfrak{m}'$ y toda serie de composición de M como A-módulo es también una serie de composición de M como A'-módulo, luego $l_A(M) = l_{A'}(M)$.

Como $\mathfrak{m}'A$ es un ideal $\mathfrak{m}$-primario, el anillo $A/\mathfrak{m}'A$ tiene dimensión 0, luego tiene longitud finita como A-módulo y, según acabamos de observar, también como A'-módulo, y también como $A'/\mathfrak{m}'$-módulo. En particular, es un A-módulo finitamente generado. Según el teorema [AC 4.21] la topología $\mathfrak{m}'$-ádica en A es de Hausdorff. Esto nos permite aplicar el teorema 2.20, según el cual A es un A'-módulo finitamente generado (es decir, una A'-álgebra finita).

Por [AC 3.68] concluimos que $\dim A' = \dim A = n$. Por otra parte, $A_0[Y]$ es un dominio íntegro de dimensión n (por [AC 4.57] y [AC 4.63]). Si el epimorfismo $\phi : A_0[[Y]] \longrightarrow A'$ no fuera inyectivo, su núcleo sería un ideal primo no nulo, luego sería $\dim A' < n$. Así pues, $A' \cong A_0[[Y]]$, lo que implica que A' es regular (por [AC 5.11] y [AC 5.65]). ∎

Notemos que, según hemos visto en la prueba, el anillo A' es, concretamente, un anillo de series formales de potencias sobre un anillo de coeficientes de A. También podemos expresar los anillos locales completos como cocientes de anillos de series formales de potencias:

Teorema 2.22 *Sea A un anillo local completo. En el caso en que no sea equicaracterístico, supongamos además que A es un dominio íntegro. Sea A_0 un anillo de coeficientes de A. Si el ideal maximal de A es finitamente generado, digamos $\mathfrak{m} = (x_1, \ldots, x_n)$, entonces tenemos un epimorfismo natural $A_0[[X_1, \ldots, X_n]] \longrightarrow A$. En particular A es noetheriano.*

Demostración: Como en la prueba del teorema anterior, entendemos que A_0 es un cuerpo en el caso equicaracterístico. Basta observar que todo $a \in A$ puede expresarse como serie de potencias en $x_1, \ldots, x_n$ y coeficientes en A_0. En efecto, por definición de anillo de coeficientes, podemos tomar un $a_0 \in A_0$ tal que $a \equiv a_0$ (mód $\mathfrak{m}$). Así

$$a - a_0 = \sum_{i=1}^{n} c_i x_i, \qquad c_i \in A.$$

A su vez, $c_i = a_i + b_i$, para un $a_i^1 \in A_0$ y un $b_i^1 \in \mathfrak{m}$. Por consiguiente,

$$a - a_0 - \sum_{i=1}^{n} a_i x_i = \sum_{i,j=1}^{n} c_{ij} x_i x_j, \qquad c_{ij} \in A.$$

Ahora podemos descomponer $c_{ij} = a_{ij} + b_{ij}$, con $a_{ij} \in A_0$ y $b_{ij} \in \mathfrak{m}$. Procediendo de este modo, vamos obteniendo formas $F_m \in A_0[X_1, \dots, X_n]$ y $G_m \in A[X_1, \dots, X_n]$ de grado m tales que

$$a - \sum_{m=0}^{r} F_m(x_1, \dots, x_n) = G_{r+1}(x_1, \dots, x_n) \in \mathfrak{m}^{r+1}.$$

Es claro entonces que $a = \sum_{m=0}^{\infty} F_m(x_1, \dots, x_n)$. ∎

Notemos que si A es equicaracterístico y regular, podemos suponer que n es la dimensión de A, con lo que, considerando las dimensiones, vemos que el epimorfismo del teorema anterior ha de ser, de hecho, un isomorfismo, tal y como se prueba en [AC 5.12].

Como última aplicación de la existencia de cuerpos de coeficientes demostraremos una relación entre la suavidad formal y la regularidad:

Teorema 2.23 *Sea A un anillo noetheriano local que contenga un cuerpo k_0, sea $\mathfrak{m}$ su ideal maximal y $k = A/\mathfrak{m}$ el cuerpo de restos. Si A es $\mathfrak{m}$ suave sobre k_0, entonces A es regular. El recíproco es cierto si la extensión k/k_0 es separablemente generada.*

Demostración: Sea $\hat{A}$ la compleción de A respecto de la topología $\mathfrak{m}$-ádica. Notemos que $\hat{A}$ es plano sobre A y, según la observación tras el teorema 2.6, sabemos que $\hat{A}$ es $\hat{\mathfrak{m}}$-suave sobre A. Por transitividad y el teorema [AC 5.11] podemos suponer que A es completo.

Es claro que A es equicaracterístico, luego podemos identificar a k con un subcuerpo de A. Consideremos ahora el cuerpo primo $k_0' \subset k \cap k_0$. Como k_0' es perfecto, la extensión k_0/k_0' es separablemente generada, luego k_0 es 0-suave sobre k_0' por el teorema 2.7. Por transitividad, tenemos que A también es $\mathfrak{m}$-suave sobre k_0', luego podemos suponer que k_0 es perfecto y que está contenido en k.

Sea $x_1, \dots, x_n$ un generador minimal de $\mathfrak{m}$. Observemos que $1, x_1, \dots, x_n$ forman una k-base de $A/\mathfrak{m}^2$, ya que si $a_0 + a_1 x_1 + \cdots + a_n x_n \in \mathfrak{m}^2$ con $a_i \in k$, entonces $a_0 \in k \cap \mathfrak{m} = 0$ y tenemos $a_1 x_1 + \cdots + a_n x_n = 0$ en $\mathfrak{m}/\mathfrak{m}^2$, luego todos los a_i son nulos, ya que los x_i son k-una base de $\mathfrak{m}/\mathfrak{m}^2$. Esto hace que el epimorfismo de k-álgebras

$$k[X_1, \dots, X_n]/(X_1, \dots, X_n)^2 \longrightarrow A/\mathfrak{m}^2$$

haga corresponder dos k-bases, luego es un isomorfismo. Por lo tanto, podemos definir un homomorfismo de k-álgebras

$$A \longrightarrow A/\mathfrak{m}^2 \longrightarrow k[X_1, \dots, X_n]/(X_1, \dots, X_n)^2 \longrightarrow k[[X_1, \dots, X_n]]/\mathfrak{m}'^2,$$

donde $\mathfrak{m}' = (X_1, \ldots, X_n)$. Por hipótesis, este homomorfismo se eleva a un homomorfismo $\phi : A \longrightarrow k[[X_1, \ldots, X_n]]$. Podemos aplicar el teorema 2.20 con $I = \mathfrak{m}$ y $M = k[[X_1, \ldots, X_n]]$ con la estructura de A-módulo dada por ϕ.

Notemos que $\phi(x_i) \equiv X_i$ (mód $\mathfrak{m}'^2$), luego por [AC 4.52] concluimos que las series formales $\phi(x_i)$ generan $\mathfrak{m}'$, lo que a su vez significa que la topología $\mathfrak{m}$-ádica en $k[[X_1, \ldots, X_n]]$ es la topología $\mathfrak{m}'$-ádica. Además, $M/\mathfrak{m}M = k$ está generado por 1 como k-espacio vectorial, luego también M está generado por 1, luego ϕ es suprayectivo.

Esto implica que $\dim A \geq n$, luego A es regular.

Supongamos ahora que A es regular y que la extensión k/k_0 es separablemente generada. Por el teorema 2.6, basta probar que $\hat{A}$ es $\hat{\mathfrak{m}}$-suave sobre k_0. Como $\hat{A}$ sigue siendo regular (teorema [AC 5.11]) podemos suponer que A es completo. Ahora bien, según la observación tras el teorema 2.22, sabemos que $A = k[[X_1, \ldots, X_n]]$, que es $\mathfrak{m}$-suave sobre k por ser la compleción de una localización de un anillo de polinomios. Por último, el teorema 2.7 nos da que k es 0-suave sobre k_0, luego por transitividad A es $\mathfrak{m}$-suave sobre k_0. ∎

2.3 El criterio jacobiano de Nagata

En esta sección demostraremos un teorema similar a [AC 5.73] para anillos de series formales de potencias sobre un cuerpo en lugar de anillos de polinomios. Esto nos permitirá demostrar a su vez un análogo de [AC 5.74], que es el resultado que necesitaremos más adelante. En realidad nos va a interesar únicamente el caso de cuerpos de característica prima, aunque para situar en su contexto el primer concepto que vamos a discutir empezaremos demostrando un resultado en característica 0:

Teorema 2.24 *Sea K/k una extensión de cuerpos de característica 0, consideremos un conjunto $B \subset K$ y sea $dB = \{db \mid b \in B\} \subset \Omega^1_{K/k}$.*

a) B es algebraicamente independiente sobre k si y sólo si $d|_B$ es inyectiva y dB es K-linealmente independiente.

b) B es una base de trascendencia de K/k si y sólo si $d|_B$ es inyectiva y dB es una K-base de $\Omega^1_{K/k}$.

Demostración: Supongamos en primer lugar que B es una base de trascendencia de K/k y sea $L = k(B)$. Si V es un L-espacio vectorial, es claro que toda aplicación $i : B \longrightarrow V$ se extiende de forma única a una k-derivación $D : L \longrightarrow V$ dada por

$$D(a) = \sum_i \left.\frac{\partial F}{\partial X_i}\right|_{(b_1,\ldots,b_n)} i(b_i),$$

donde $F \in k[X_1, \ldots, X_n]$ y $a = F(b_1, \ldots, b_n)$. Según el teorema [E 7.31] existe una única aplicación L-lineal $\phi : \Omega^1_{L/k} \longrightarrow V$ tal que $D = d \circ \phi$. En particular,

$\phi(db) = i(b)$, para todo $b \in B$. Para que esto sea posible (para cualquier elección de i) es necesario que $d|_B$ sea inyectiva. Además tenemos que cualquier aplicación $dB \longrightarrow V$ se extiende a una única aplicación lineal sobre $\Omega^1_{L/k}$, lo cual sólo es posible si dB es una L-base de $\Omega^1_{L/k}$.

Si $L \subset L' \subset K$ y L'/L es una extensión finita, el teorema [E 7.38] nos da que el homomorfismo natural $\Omega^1_{L/k} \otimes_L L' \longrightarrow \Omega^1_{L'/k}$ es un isomorfismo.

Las k-derivaciones $d_{L'} : L' \longrightarrow \Omega^1_{L'/k} \longrightarrow \Omega^1_{L/k} \otimes_L L' \longrightarrow \Omega^1_{L/k} \otimes_L K$ se extienden a una k-derivación $d_K : K \longrightarrow \Omega^1_{K/k} \otimes_L K$.

Por otra parte, una k-derivación $D : K \longrightarrow V$ está completamente determinada por sus restricciones $D_{L'} : L' \longrightarrow V$, donde L' recorre las extensiones finitas de L. Cada una de ellas es una k-derivación que determina una aplicación L'-lineal $\phi_{L'} : \Omega^1_{L'/k} \longrightarrow V$. A su vez, las aplicaciones $\psi_{L'} : \Omega^1_{L/k} \otimes_L L' \longrightarrow V$ determinan una aplicación K-lineal $\psi : \Omega^1_{L/k} \otimes_L K \longrightarrow V$ tal que $D = d_K \circ \psi$. Esto significa que $\Omega^1_{L/k} \otimes_L K$ y d_K cumplen la propiedad universal del teorema [E 7.31], de donde se sigue que $\Omega^1_{K/k} \cong \Omega^1_{L/k} \otimes_L K$, así como que $d|_B$ es inyectiva y dB es una K-base de $\Omega^1_{K/k}$.

Como todo conjunto algebraicamente independiente B se extiende a una base de trascendencia, concluimos también que dB es, en este caso, K-linealmente independiente.

Recíprocamente, si $d|_B$ es inyectiva y dB es K-linealmente independiente, entonces B ha de ser algebraicamente independiente. En caso contrario existirían $b_1, \ldots, b_n \in B$ distintos dos a dos y un polinomio $F \in k[X_1, \ldots, X_n]$ no nulo tal que $F(b_1, \ldots, b_n) = 0$. Podemos tomar F de grado mínimo. Entonces

$$0 = d0 = \sum_i \left.\frac{\partial F}{\partial X_i}\right|_{(b_1,\ldots,b_n)} db_i,$$

donde las derivadas no son nulas porque tienen grado menor que F (y aquí usamos que los cuerpos tienen característica 0), lo que nos lleva a que los db_i no son linealmente independientes.

Si dB es una K-base de $\Omega^1_{K/k}$, tenemos que B es algebraicamente independiente, luego está contenido en una base de trascendencia B', luego $d|_{B'}$ es inyectiva y dB' es una K-base de $\Omega^1_{K/k}$, luego $dB = dB'$, luego $B = B'$. ∎

Para extensiones de cuerpos de característica prima p, la condición necesaria y suficiente para que dB sea una base de $\Omega^1_{K/k}$ no es que B sea una base de trascendencia de K/k, sino que sea una p-base, en el sentido de la definición siguiente:

Definición 2.25 Sea K/k una extensión de cuerpos de característica prima p. Un conjunto $B \subset K$ es *p-independiente* sobre k si los monomios $b_1^{e_1} \cdots b_n^{e_n}$, donde $b_1, \ldots, b_n \in B$ son distintos dos a dos y $0 \le e_i < p$, son linealmente independientes sobre kK^p. (Notemos que los elementos de k son algebraicos sobre K^p, de donde se sigue que $kK^p = k[K^p] = K^p[k]$ es un cuerpo.)

Diremos que B es una *p-base* de K sobre k si es p-independiente y además $K = kK^p[B]$, es decir, si todo elemento de K se expresa de forma única como un polinomio con coeficientes en kK^p, cuyos monomios tienen grado menor que p en cada variable, evaluado en elementos de B. (A tales polinomios los llamaremos polinomios *reducidos*.)

Es claro que un conjunto $B \subset K$ es p-independiente si y sólo si lo son todos sus subconjuntos finitos. Si B es finito, entonces es p-independiente si y sólo si $|kK^p[B] : kK^p| = p^{|B|}$ (ya que los $p^{|B|}$ monomios reducidos en $b_1, \ldots, b_n$ son, en cualquier caso, un generador de $kK^p[B]$ sobre kK^p).

Notemos también que una p-base es un sistema p-independiente maximal respecto de la inclusión, ya que si B es p-independiente pero $kK^p[B] \subsetneq K$, entonces cualquier $b \in K \setminus kK^p[B]$ cumple que las potencias $1, b, b^2, \ldots, b^{p-1}$ son linealmente independientes sobre $kK^p[B]$, luego (por la prueba del teorema de transitividad de grados) los monomios reducidos en $B \cup \{p\}$ son linealmente independientes sobre kK^p. Así pues, $B \cup \{b\}$ es también p-independiente. El lema de Zorn implica entonces que todo sistema p-independiente puede extenderse hasta una p-base.

Ahora ya podemos demostrar el análogo del teorema 2.24:

Teorema 2.26 *Sea K/k una extensión de cuerpos de característica prima p, sea $B \subset K$ y sea $dB = \{db \mid b \in B\} \subset \Omega^1_{K/k}$.*

a) B es p-independiente sobre k si y sólo si $d|_B$ es inyectiva y dB es K-linealmente independiente.

b) B es una p-base si y sólo si $d|_B$ es inyectiva y dB es una K-base de $\Omega^1_{K/k}$.

Demostración: Supongamos en primer lugar que B es una p-base de K sobre k. Si V es un K-espacio vectorial, toda aplicación $i : B \longrightarrow V$ se extiende de forma única a una k-derivación $D : K \longrightarrow V$ mediante

$$D(a) = \sum_i \left.\frac{\partial F}{\partial X_i}\right|_{(b_1,\ldots,b_n)} i(b_i),$$

donde $F \in kK^p[X_1, \ldots, X_n]$ es un polinomio reducido y $a = F(b_1, \ldots, b_n)$.

En efecto, notemos que todo monomio puede expresarse en la forma

$$F = \alpha X_1^{r_1 p} \cdots X_n^{r_n p} G,$$

donde $\alpha \in kK^p$ y G es un monomio reducido. Si $F^* = \alpha b_1^{r_1 p} \cdots b_n^{r_n p} G$, tenemos que $F(b_1, \ldots, b_n) = F^*(b_1, \ldots, b_n)$ y

$$\left.\frac{\partial F}{\partial X_i}\right|_{(b_1,\ldots,b_n)} = \left.\frac{\partial F^*}{\partial X_i}\right|_{(b_1,\ldots,b_n)}.$$

Esto implica que la fórmula que define a D vale para cualquier monomio F, no necesariamente reducido y, por linealidad, para cualquier polinomio F, no necesariamente reducido. De aquí se sigue que D es ciertamente una derivación.

Al igual que en la prueba de 2.24, esto implica que $d|_B$ es inyectiva y que dB es una K-base de $\Omega^1_{K/k}$.

Si B es p-independiente, se extiende a una p-base B', luego $dB \subset dB'$ es K-linealmente independiente.

Si B no es p-independiente pero $d|_B$ es inyectiva, B tiene un subconjunto finito que no es p-independiente. Esto significa que existe un polinomio reducido $F \in kK^p[X_1, \dots, X_n]$ no nulo tal que $F(b_1, \dots, b_n) = 0$, para ciertos elementos $b_1, \dots, b_n \in B$ distintos dos a dos. Podemos elegirlo de grado mínimo. Entonces

$$0 = d0 = \sum_i \left.\frac{\partial F}{\partial X_i}\right|_{(b_1,\dots,b_n)} db_i,$$

donde las derivadas no son idénticamente nulas porque F es reducido, y no se anulan en $(b_1, \dots, b_n)$ por la minimalidad de F. Esto significa que $db_1, \dots, db_n$ no son linealmente independientes.

Así termina la prueba de a). Para terminar la prueba de b) suponemos que $d|_B$ es inyectiva y que dB es una K-base de $\Omega^1_{K/k}$. Por a) sabemos que B es p-independiente, luego está contenido en una p-base B'. Entonces, $d|_{B'}$ es inyectiva, $dB \subset dB'$ y dB' es K-linealmente independiente, luego $dB = dB'$, luego $B = B'$. ∎

Definición 2.27 Sea A un anillo, sean $x_1, \dots, x_r \in A$ y consideremos derivaciones $D_1, \dots, D_s \in \mathrm{Der}(A) = \mathrm{Der}_{\mathbb{Z}}(A, A)$. Llamaremos *matriz jacobiana* asociada a estos elementos a la matriz $J(x_1, \dots, x_r; D_1, \dots, D_s) = (D_i x_j)_{i,j}$. Si $\mathfrak{P}$ es un ideal de A, llamaremos $J(x_1, \dots, x_r; D_1, \dots, D_s)(\mathfrak{P})$ a la matriz formada por las clases módulo $\mathfrak{P}$ de los coeficientes de la matriz jacobiana. Si $\mathfrak{P}$ es un ideal primo y contiene a $x_1, \dots, x_r$, entonces el rango de esta matriz sólo depende del ideal $I = (x_1, \dots, x_r)$, por lo que lo representaremos por $\operatorname{rang} J(I; D_1, \dots, D_s)$.

(Nos referimos al rango de la matriz considerada como matriz con coeficientes en el cuerpo de cocientes de $A/\mathfrak{P}$. Más en general, si A es un dominio íntegro con cuerpo de cocientes K y M es un A-módulo, llamaremos *rango* de M a la dimensión de $M \otimes_A K$.)

En efecto, si $y_1, \dots, y_t$ es otro generador de I, tenemos que

$$y_l = \sum_j a_j x_j, \qquad D_i y_l = \sum_j (a_j D_i x_j + x_j D_i a_j) \equiv \sum_j a_j D_i x_j \ (\text{mód } \mathfrak{P}),$$

luego

$$\begin{aligned}\operatorname{rang} J(x_1, \dots, x_r; D_1, \dots, D_s) &= \operatorname{rang} J(x_1, \dots, x_r, y_1, \dots, y_t; D_1, \dots, D_s)\\ &= \operatorname{rang} J(y_1, \dots, y_t; D_1, \dots, D_s).\end{aligned}$$

Si $\Delta \subset \mathrm{Der}(A)$, definimos $\operatorname{rang} J(I; \Delta)(\mathfrak{P})$ como el máximo de los rangos $\operatorname{rang} J(I; D_1, \dots, D_s)(\mathfrak{P})$, donde las derivaciones $D_1, \dots, D_s$ recorren los subconjuntos finitos de Δ.

Observemos que, en realidad, si $I_{\mathfrak{P}} = (x_1, \ldots, x_r)A_{\mathfrak{P}}$, entonces

$$\operatorname{rang} J(I;\Delta)(\mathfrak{P}) = \operatorname{rang} J(x_1, \ldots, x_r;\Delta)(\mathfrak{P}).$$

En efecto, si $y \in I$, tenemos que

$$sy = \sum_j a_j x_j, \qquad a_j \in A,\ s \in A \setminus \mathfrak{P}.$$

luego si $D_i \in \Delta$, se cumple que,

$$sD_i y \equiv \sum_j a_j D_i x_j \ (\text{mód } \mathfrak{P}), \qquad s \not\equiv 0 \ (\text{mód } \mathfrak{P}),$$

por lo que $\operatorname{rang} J(x_1, \ldots, x_r;\Delta)(\mathfrak{P}) = \operatorname{rang} J(x_1, \ldots, x_r, y;\Delta)(\mathfrak{P})$. ∎

El teorema siguiente nos da una condición suficiente para que un punto de un espectro $\operatorname{Esp}(A/I)$, donde A es un anillo regular, sea también regular:

Teorema 2.28 *Sea A un anillo regular, I un ideal de A y $\mathfrak{P} \in \operatorname{Esp} A$ tal que $I \subset \mathfrak{P}$. Sea $r = \operatorname{alt} I_{\mathfrak{P}}$ y $\Delta \subset \operatorname{Der}(A)$. Entonces:*

a) $\operatorname{rang} J(I;\Delta)(\mathfrak{P}) \leq r$.

b) Si $\operatorname{rang} J(f_1, \ldots, f_r;\Delta)(\mathfrak{P}) = r$ *para ciertos* $f_1, \ldots, f_r \in I$, *entonces* $I_{\mathfrak{P}} = (f_1, \ldots, f_r)_{\mathfrak{P}}$ *y* $A_{\mathfrak{P}}/I_{\mathfrak{P}}$ *es regular.*

Demostración: Sea $\mathfrak{Q}$ un ideal primo tal que $I \subset \mathfrak{Q} \subset \mathfrak{P}$ y $\operatorname{alt}\mathfrak{Q} = r$. Entonces, considerando determinantes vemos que

$$\operatorname{rang} J(I;\Delta)(\mathfrak{P}) \leq \operatorname{rang} J(I;\Delta)(\mathfrak{Q}).$$

Tenemos que $A_{\mathfrak{Q}}$ es un anillo local regular de dimensión r, luego existen $g_1, \ldots, g_r \in \mathfrak{Q}$ tales que $\mathfrak{Q}A_{\mathfrak{Q}} = (g_1, \ldots, g_r)_{\mathfrak{Q}}$. Así, todo $f \in I$ satisface una relación de la forma $sf = \sum_i a_i g_i$, con $a_i \in A$, $s \in A \setminus \mathfrak{Q}$.

Si $D \in \Delta$, tenemos que

$$sDf \equiv \sum_i a_i D g_i \ (\text{mód } \mathfrak{Q}),$$

lo que significa que la fila de la matriz $J(I;\Delta)(\mathfrak{Q})$ correspondiente a f es combinación lineal de las filas correspondientes a $g_1, \ldots, g_r$, luego $\operatorname{rang} J(I;\Delta)(\mathfrak{Q}) \leq r$.

b) Sea $\mathfrak{m} = \mathfrak{P}A_{\mathfrak{P}}$, el ideal maximal de $A_{\mathfrak{P}}$. Vamos a probar que las clases de $f_1, \ldots, f_r$ en $\mathfrak{m}/\mathfrak{m}^2$ son linealmente independientes módulo $\mathfrak{m}$. Para ello suponemos que

$$a_1 f_1 + \cdots + a_r f_r \in \mathfrak{m}^2, \qquad a_i \in A_{\mathfrak{P}},$$

y hemos de probar que $a_i \in \mathfrak{m}$. Multiplicando por un elemento adecuado de $A \setminus \mathfrak{P}$ podemos suponer que $a_i \in A$, con lo que la combinación lineal está, de

hecho, en $\mathfrak{P}^2$. Por hipótesis, existen $D_1, \dots, D_n \in \Delta$ tales que la matriz $(D_i f_j)$ tiene determinante no nulo módulo $\mathfrak{P}$. Como

$$a_1 D_i f_1 + \cdots + a_r D_i f_r \equiv 0 \text{ (mód } \mathfrak{P}),$$

ha de ser $a_j \in \mathfrak{P}$ para todo j.

Por consiguiente, $f_1, \dots, f_r$ se extienden a un sistema regular de parámetros de $A_\mathfrak{P}$ (teorema [AC 4.52]) y el teorema [AC 5.26] nos da que $(f_1, \dots, f_r)_\mathfrak{P}$ es un ideal primo de altura r, luego ha de ser $IA_\mathfrak{P}$ (pues existe un primo $\mathfrak{Q}$ de altura r tal que $(f_1, \dots, f_r)_\mathfrak{P} \subset I_\mathfrak{P} \subset \mathfrak{Q}A_\mathfrak{P}$). El cociente $A_\mathfrak{P}/I_\mathfrak{P}$ es regular por [AC 5.19]. ∎

Bajo ciertas condiciones, tenemos una condición necesaria y suficiente:

Teorema 2.29 *Sea A un anillo regular, sea $\mathfrak{P} \in \operatorname{Esp} A$ y $\Delta \subset \operatorname{Der}(A)$. Las afirmaciones siguientes son equivalentes:*

a) $\operatorname{rang} J(\mathfrak{P}; \Delta)(\mathfrak{P}) = \operatorname{alt} \mathfrak{P}$.

b) Para cada primo $\mathfrak{Q} \subset \mathfrak{P}$, el cociente $A_\mathfrak{P}/\mathfrak{Q}A_\mathfrak{P}$ es regular si y sólo si $\operatorname{rang} J(\mathfrak{Q}; \Delta)(\mathfrak{P}) = \operatorname{alt} \mathfrak{Q}$.

Demostración: a) es el caso particular $\mathfrak{Q} = \mathfrak{P}$ de b). Suponiendo a), si $\operatorname{rang} J(\mathfrak{Q}; \Delta)(\mathfrak{P}) = \operatorname{alt} \mathfrak{Q}$, tenemos que $A_\mathfrak{P}/\mathfrak{Q}A_\mathfrak{P}$ es regular por el teorema anterior aplicado a $I = \mathfrak{Q}$.

Recíprocamente, si el cociente es regular, [AC 5.19] nos da que existen $f_1, \dots, f_r \in \mathfrak{P}$, tales que $\mathfrak{P}A_\mathfrak{P} = (f_1, \dots, f_r)A_\mathfrak{P}$ y $\mathfrak{Q}A_\mathfrak{P} = (f_1, \dots, f_s)A_\mathfrak{P}$, donde $r = \operatorname{alt} \mathfrak{P}$, $s = \operatorname{alt} \mathfrak{Q}$. Por a), tenemos que $\operatorname{rang} J(f_1, \dots, f_r; \Delta)(\mathfrak{P}) = r$, luego

$$\operatorname{rang} J(\mathfrak{Q}; \Delta)(\mathfrak{P}) = \operatorname{rang} J(f_1, \dots, f_s; \Delta)(\mathfrak{P}) = s.$$

∎

Vamos a probar que la condición a) del teorema anterior se cumple para todo $\mathfrak{P}$ cuando A es un anillo de series formales de potencias. Para ello necesitamos varios resultados previos.

Teorema 2.30 *Sea K/k una extensión de cuerpos de característica prima p y sea $\mathcal{F}$ una familia de cuerpos intermedios tal que la intersección de dos cualesquiera de ellos contenga a un tercero. Las afirmaciones siguientes son equivalentes:*

a) $\bigcap_{L \in \mathcal{F}} LK^p = kK^p$.

b) La aplicación natural $\Omega^1_{K/k} \longrightarrow \varprojlim_{L \in \mathcal{F}} \Omega^1_{K/L}$ es inyectiva.

c) Para cada $B \subset K$ finito y p-independiente sobre k, existe un $L \in \mathcal{F}$ tal que B es p-independiente sobre L.

d) Existe una p-base B de K sobre k tal que para cada subconjunto finito de B existe un $L \in \mathcal{F}$ sobre el que es p-independiente.

DEMOSTRACIÓN: Observemos que si $k \subset L \subset L' \subset K$, tenemos aplicaciones K-lineales naturales $\Omega^1_{K/L} \longrightarrow \Omega^1_{K/L'}$, determinados por que $db \mapsto db$. Más concretamente, se trata del homomorfismo dado por el teorema [E 7.31] a partir de la L-derivación $d : K \longrightarrow \Omega^1_{K/L'}$.

Estos homomorfismos convierten a $\{\Omega^1_{K/L}\}_{L\in\mathcal{F}}$ en un sistema inverso (en un sentido que generaliza de forma obvia a la definición [AC 4.4]). Por el mismo motivo tenemos aplicaciones K-lineales $\Omega^1_{K/k} \longrightarrow \Omega^1_{K/L}$, que inducen un homomorfismo natural $\Omega^1_{K/k} \longrightarrow \varprojlim_{L\in\mathcal{F}} \Omega^1_{K/L}$.

a) $\Rightarrow$ c) Sean $v_1, \dots, v_n$ los monomios reducidos en los elementos de B, que, por hipótesis, son linealmente independientes sobre kK^p. Podemos tomar un $L \in \mathcal{F}$ tal que el rango de dichos monomios sobre L sea máximo. Si este rango es $r < n$, entonces tenemos r monomios L-independientes, digamos $v_1, \dots, v_r$, pero $v_n = c_1v_1 + \cdots + c_rv_r$, con $c_i \in L$. Por la independencia sobre kK^p, para algún índice, por ejemplo $i = 1$, se cumple que $c_1 \notin kK^p$. Por a) tenemos que $c_1 \notin L'$, para cierto $L' \in \mathcal{F}$ que podemos tomar contenido en L. Entonces $v_1, \dots, v_r, v_n$ son L'-independientes, pues $v_1, \dots, v_r$ lo son por ser L-independientes, luego, si fueran L'-dependientes, v_n debería ser combinación lineal de los otros, pero, por la unicidad de las coordenadas, la primera debería ser c_1, lo cual es imposible. Esto contradice la maximalidad del rango.

c) $\Rightarrow$ d) es trivial. (Sirve cualquier p-base.)

d) $\Rightarrow$ b) Sea $\omega \in \Omega^1_{K/k}$ no nulo. Como dB es una K-base, podemos expresarlo como $\omega = c_1db_1 + \cdots + c_ndb_n$, para ciertos $b_i \in B$ y $c_i \in K$. Por d), existe un $L \in \mathcal{F}$ tal que $b_1, \dots, b_n$ son p-independientes sobre L. Por consiguiente, $db_1, \dots, db_n$ son linealmente independientes en $\Omega^1_{K/L}$, luego la imagen de ω en $\Omega^1_{K/L}$ es no nula, al igual que su imagen en el límite inverso.

b) $\Rightarrow$ a) Si $a \in K\backslash kK^p$, entonces es p-independiente sobre k, luego $da \in \Omega^1_{K/k}$ es no nulo. Por b), existe un $L \in \mathcal{F}$ tal que $da \in \Omega^1_{K/L}$ también es nulo, lo que implica que $a \notin LK^p$. ∎

Teorema 2.31 *Sean K/k y $\mathcal{F}$ como en el teorema anterior y sea E/K una extensión finitamente generada. Si $\bigcap_{L\in\mathcal{F}} LK^p = kK^p$, entonces $\bigcap_{L\in\mathcal{F}} LE^p = kE^p$.*

DEMOSTRACIÓN: La extensión E/K puede descomponerse en un número finito de extensiones simples, por lo que no perdemos generalidad si suponemos que $E = K(a)$. Distinguiremos varios casos:

1) Si a es trascendente sobre K, entonces

$$\bigcap_{L\in\mathcal{F}} LE^p = \bigcap_{L\in\mathcal{F}} LK^p(a^p) = kK^p(a^p) = kE^p.$$

(El paso no trivial es la segunda igualdad: notemos que un elemento de $LK^p(a^p)$ es de la forma $b = F(a^p)$, para un cierto $F \in LK^p[X]$ unívocamente determinado. Si b está en la intersección, entonces $F \in kK^p[X]$, luego $b \in kK^p(a^p)$.)

2) Supongamos ahora que a es algebraico separable sobre K. Entonces, según [E 7.38] tenemos que $\Omega^1_{K/k} \otimes_K E \cong \Omega^1_{E/k}$, por lo que una p-base de K/k es también una p-base de E/k y basta usar el apartado d) del teorema anterior.

3) Ahora supongamos que a es puramente inseparable sobre K. Descomponiendo la extensión E/K en más extensiones simples, podemos suponer que $a^p = b \in K$. Entonces $E = K[X]/(X^p - b)$ y [E 7.34] nos da que

$$\Omega^1_{E/k} \cong (\Omega^1_{K[X]/k} \otimes_{K[X]} E)/\langle db \otimes 1\rangle .$$

Por otra parte, la prueba del teorema [E 7.37] aplicado a $I = 0$ nos da un isomorfismo

$$\Omega^1_{K[X]/k} \cong (\Omega^1_{K/k} \otimes_K K[X]) \oplus \Omega^1_{K[X]/K}.$$

Más explícitamente, es $\Omega^1_{K[X]/k} \cong (\Omega^1_{K/k} \otimes_K K[X]) \oplus \langle dX\rangle_{K[X]}$. Por consiguiente,

$$\Omega^1_{K[X]/k} \otimes_{K[X]} E \cong (\Omega^1_{K/k} \otimes_K E) \oplus \langle 1 \otimes da\rangle_E ,$$

y a su vez,

$$\Omega^1_{E/k} \cong \big((\Omega^1_{K/k}/\langle db\rangle) \otimes_K E\big) \oplus \langle da\rangle .$$

Lo mismo es válido para cualquier $L \in \mathcal{F}$ en lugar de k, es decir:

$$\Omega^1_{E/L} \cong \big((\Omega^1_{K/L}/\langle db\rangle) \otimes_K E\big) \oplus \langle da\rangle .$$

Si $db \neq 0$, entonces $b \notin kK^p$, por lo que es p-independiente y podemos extenderlo hasta una p-base de K sobre k, digamos $\{b\} \cup B$. Así, $\{db\} \cup dB$ es una K-base de $\Omega^1_{K/k}$, luego $\{da\} \cup dB$ es una E-base de $\Omega^1_{E/k}$, luego $\{a\} \cup B$ es una p-base de E sobre k.

Más aún, podemos suponer que B resulta de eliminar un elemento adecuado de una p-base de K sobre k que cumpla la propiedad d) del teorema anterior. Entonces, si $b, b_1, \ldots, b_n$ son p-independientes en K sobre un $L \in \mathcal{F}$, tenemos que $a, b_1, \ldots, b_n$ son p-independientes en E sobre L.

Si $db = 0$ tomamos como B cualquier p-base de K sobre k que cumpla la citada propiedad d) y tenemos igualmente que $\{a\} \cup B$ es una p-base de E sobre k que cumple dicha propiedad para E. ∎

Teorema 2.32 *Sea K un cuerpo de característica prima p, sea $\mathcal{F}$ una familia de subcuerpos tal que la intersección de dos cualesquiera de ellos contenga a un tercero. Supongamos además que para todo $L \in \mathcal{F}$ se cumple $|K : L| < \infty$, así como que $\bigcap_{L\in\mathcal{F}} L = K^p$. Sea E/K una extensión finita. Entonces existe un $L \in \mathcal{F}$ tal que, para todo subcuerpo $K' \subset L$ que cumpla $|K : K'| < \infty$, tenemos que $\dim_E \Omega^1_{E/K'} = \dim_K \Omega^1_{K/K'}$.*

Demostración: Sea $K = K_0 \subset K_1 \subset \cdots \subset K_t = E$ una cadena de cuerpos intermedios de modo que $K_i = K_{i-1}(a_i)$, donde x_i es separable sobre K_{i-1} o bien $a_i^p \in K_{i-1}$. El teorema anterior aplicado a $k = K^p$ nos da que

$\bigcap_{L\in\mathcal{F}} LK_i^p = K_i^p$. Esto hace que baste probar el teorema para cada una de las extensiones K_i/K_{i-1}, ya que en tal caso podemos tomar un mismo $L \in \mathcal{F}$ que sirva para todos los tramos, y así, si $K' \subset L$, $|K : K'| < \infty$, también $K' \subset LK_i^p$, $|K_i; K'| < \infty$, luego

$$\dim_E \Omega^1_{E/K'} = \dim_{K_{t-1}} \Omega^1_{K_{t-1}/K'} = \cdots = \dim_K \Omega^1_{K/K'}.$$

Equivalentemente, podemos suponer que $E = K(a)$. Si a es separable, según [E 7.38] tenemos que $\Omega^1_{E/K'} = \Omega^1_{K/K'} \otimes_K E$, y el resultado es cierto para cualquier L.

Supongamos ahora que $a^p = b \in K$, pero que $b \notin K^p$. Entonces existe un $L \in \mathcal{F}$ tal que $b \notin L$. Si $K' \subset L$ cumple $|K : K'| < \infty$, al igual que en la prueba del teorema anterior vemos que

$$\Omega^1_{E/K'} \cong \left((\Omega^1_{K/K'}/\langle db\rangle) \otimes_K E\right) \oplus \langle da\rangle .$$

Como $K'K^p \subset L$, tenemos que $b \notin K'K^p$, luego es p-independiente sobre K', luego $db \neq 0$, lo que implica la igualdad de las dimensiones. ∎

Teorema 2.33 *Sea k un cuerpo de característica p, sea $R = k[[X_1, \ldots, X_n]]$, sea $\mathfrak{P} \in \operatorname{Esp} R$ y sea $A = R/\mathfrak{P}$. Sea $\mathcal{F}$ una familia de subcuerpos de k tal que la intersección de dos cualesquiera de ellos contenga a un tercero. Supongamos además que $|k : L| < \infty$ para todo $L \in \mathcal{F}$ y que $\bigcap_{L\in\mathcal{F}} L = k^p$. Entonces existe un $L \in \mathcal{F}$ tal que para todo cuerpo intermedio $k^p \subset k' \subset L$ tal que $|k : k'| < \infty$, se cumple que*

$$\operatorname{rang}_A \operatorname{Der}_{k'} A = \dim A + \dim_k \operatorname{Der}_{k'} k.$$

Demostración: Sea $n = \dim A$ y sea $x_1, \ldots, x_n$ un sistema de parámetros de A. En la prueba del teorema 2.21 hemos visto que si $B = k[[x_1, \ldots, x_n]]$, entonces B es isomorfo a $k[[X_1, \ldots, X_n]]$ y que A es una B-álgebra finita.

Tomemos un cuerpo intermedio $k^p \subset k' \subset k$ tal que $|k : k'| < \infty$. Entonces $|k : k'| = p^r$. Si $u_1, \ldots, u_r$ es una p-base de k sobre k', entonces

$$\operatorname{Der}_{k'} k = \operatorname{Hom}_k(\Omega^1_{k/k'}, k),$$

luego $\dim_k \operatorname{Der}_{k'} k = \dim_k \Omega^1_{k/k'} = r$.

Si $C = k'[[x_1^p, \ldots, x_n^p]]$, entonces B es un C-módulo libre con base el conjunto de los monomios reducidos en $u_1, \ldots, u_r, x_1, \ldots, x_n$.

El mismo argumento empleado en la prueba del teorema 2.26 prueba entonces que $\Omega^1_{B/C}$ es un B-módulo libre de base $du_1, \ldots, du_r, dx_1, \ldots, dx_n$. Concretamente, si $\mathcal{B} = \{u_1, \ldots, u_r, x_1, \ldots, x_n\}$ y V es un B-módulo, cada aplicación $i : \mathcal{B} \longrightarrow V$ se extiende de forma única a una C-derivación $D : B \longrightarrow V$ dada por

$$D(a) = \sum_i i(u_i) \left.\frac{\partial F}{\partial X_i}\right|_{(u_1,\ldots,u_r,x_1,\ldots,x_n)} + \sum_i i(x_i) \left.\frac{\partial F}{\partial Y_i}\right|_{(u_1,\ldots,u_r,x_1,\ldots,x_n)},$$

donde $F \in C[X_1, \ldots, X_r, Y_1, \ldots, Y_n]$ es un polinomio reducido y

$$a = F(u_1, \ldots, u_r, x_1, \ldots, x_n).$$

De aquí obtenemos un único homomorfismo de B-módulos $\phi : \Omega^1_{B/C} \longrightarrow V$ que cumple $\phi(du_i) = i(u_i)$, $\phi(dx_i) = i(x_i)$. Esto sólo puede ocurrir si $\Omega^1_{B/C}$ es un B-módulo libre con la base indicada.

Notemos ahora que toda derivación $D : B \longrightarrow B$ es continua, ya que, claramente, $D[\mathfrak{m}_B^m] \subset \mathfrak{m}_B^{m-1}$, luego las derivaciones atraviesan las sumas infinitas y, por consiguiente, toda $D \in \mathrm{Der}_{k'}(B)$ se anula en C. Así pues,

$$\mathrm{Der}_{k'} B = \mathrm{Der}_C B = \mathrm{Hom}_B(\Omega^1_{B/C}, B).$$

Como $\Omega^1_{B/C}$ es un B-módulo libre de rango $r + n$, lo mismo le sucede al B-módulo de homomorfismos en B, luego concluimos que

$$\mathrm{rang}\, \mathrm{Der}_{k'} B = \mathrm{rang}_B \Omega^1_{B/C} = n + r = \dim A + \dim_k \mathrm{Der}_{k'} k,$$

luego se cumple el teorema cuando $A = B$.

Como antes, tenemos que

$$\mathrm{Der}_{k'} A = \mathrm{Der}_C A = \mathrm{Hom}_A(\Omega^1_{A/C}, A).$$

Como A es un C-módulo finitamente generado, se cumple que $\Omega^1_{A/C}$ es un A-módulo finitamente generado ([E 7.35]). Por lo tanto, si $K' \subset K \subset E$ son los cuerpos de cocientes respectivos de $C \subset B \subset A$,

$$\mathrm{Der}_{k'} A \otimes_A E = \mathrm{Hom}_A(\Omega^1_{A/C}, A) \otimes_A E$$

$$\cong \mathrm{Hom}_E(\Omega^1_{A/C} \otimes_A E, E) \cong \mathrm{Hom}_E(\Omega^1_{E/K'}, E)$$

(El primer isomorfismo es una relación natural entre módulos de homomorfismos y productos tensoriales que sólo usa que $\Omega^1_{A/C}$ es un A-módulo finitamente generado; el segundo isomorfismo se sigue de [E 7.34 c)], que nos da el isomorfismo $\Omega^1_{A/C} \otimes_A E \cong \Omega^1_{E/C}$, junto con [E 7.34 b)] y [E 7.33], que nos dan que $\Omega^1_{E/C} \cong \Omega^1_{E/K'}$.) Así pues,

$$\mathrm{rang}_A \mathrm{Der}_{k'} A = \dim_E(\mathrm{Der}_{k'} A \otimes_A E) = \dim_K \Omega^1_{E/K'}.$$

Por el caso $A = B$, que hemos probado antes, todo se reduce a demostrar que $\dim_K \Omega^1_{E/K'} = \mathrm{rang}_B \Omega^1_{B/C}$ o, por el mismo argumento anterior, que

$$\dim_K \Omega^1_{E/K'} = \dim_F \Omega^1_{K/K'}.$$

Más concretamente, recordemos que K' es el cuerpo de cocientes del anillo $C = k'[[x_1^p, \ldots, x_n^p]]$ y hay que probar esto para todo k' contenido en un cierto $L \in \mathcal{F}$ tal que $|k : k'| < \infty$.

Para cada $L \in \mathcal{F}$, sea F_L el cuerpo de cocientes de $C_L = L[[x_1^p, \ldots, x_n^p]]$. Como B es un C_L-módulo finitamente generado, es entero sobre C_L y, como éste es íntegramente cerrado (por ser regular) resulta que $B \cap F_L = C_L$.

Si $a \in \bigcap_{L\in\mathcal{F}} F_L \subset K$, podemos expresarlo en la forma $a = u/v$, con u, $v \in B$. Multiplicando por v^{p-1} podemos suponer que $v \in B^p \subset F_L$. Entonces $u \in B \cap F_L = C_L$ para todo $L \in \mathcal{F}$, luego $u \in \bigcap_{L\in\mathcal{F}} C_L = B^p$. Esto prueba que

$$\bigcap_{L\in\mathcal{F}} F_L = K^p.$$

Ahora basta aplicar el teorema anterior, ya que si $k' \subset L$ cumple $|k : k'| < \infty$, entonces $K' \subset F_L$ cumple $|K : K'| < \infty$. ∎

Ahora ya podemos probar el resultado que perseguíamos:

Teorema 2.34 (Nagata) *Sea k un cuerpo de característica prima p, sea $R = k[[X_1, \ldots, X_n]]$ y sea $\mathfrak{P} \in \operatorname{Esp} R$. Entonces* $\operatorname{rang} J(\mathfrak{P}; \operatorname{Der}(R))(\mathfrak{P}) = \operatorname{alt} \mathfrak{P}$.

Demostración: Sea $A = R/\mathfrak{P}$ y $s = \dim A$. Fijemos una p-base de k sobre k^p y sea $\mathcal{F}$ la familia de cuerpos intermedios que resultan de adjuntar a k^p todos los elementos de la p-base salvo un número finito de ellos. Es claro que estamos en las condiciones del teorema anterior, por lo que existe un cuerpo $k^p \subset k' \subset k$ tal que $|k : k'| < \infty$ y

$$\operatorname{rang}_A \operatorname{Der}_{k'} A = s + r,$$

donde $r = \dim_k \operatorname{Der}_{k'} k$ y, según hemos visto en la prueba, cumple también que $|k : k'| = p^r$.

Por otra parte, en la prueba del teorema anterior, particularizada para $\mathfrak{p} = 0$ (es decir, para $A = R$), muestra que si $u_1, \ldots, u_r$ es una p-base de k sobre k' y llamamos $u_{r+i} = X_i$, entonces cada aplicación $\{u_1, \ldots, u_{r+n}\} \longrightarrow A$ se extiende a una única k'-derivación de R en A. Llamamos $D_i : R \longrightarrow A$ a la única derivación que cumple

$$D_i u_j = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Es claro entonces que $D_1, \ldots, D_{r+n}$ son una A-base de $\operatorname{Der}_{k'}(R, A)$. Sea ahora $D \in \operatorname{Der}_{k'}(A)$ y sea $c_i = D(\phi(u_i)) \in A$. Sea $D_0 = \sum c_i D_i \in \operatorname{Der}_{k'}(R, A)$, de modo que $D = D_0 \circ \phi$. Vemos así que D está completamente determinada por los c_i. Por otra parte, para que unos $(c_1, \ldots, c_{r+n}) \in A^{r+n}$ determinen una derivación D, es necesario y suficiente que cumplan las ecuaciones lineales

$$\sum_{i=1}^{r+n} c_i D_i(f) = 0, \qquad f \in \mathfrak{P}.$$

Es claro entonces que

$$\operatorname{rang} \operatorname{Der}_{k'}(A) = r + n - \operatorname{rang} J(\mathfrak{P}, D_1, \ldots, D_{r+n})(\mathfrak{P}).$$

Por consiguiente,

$$\operatorname{rang} J(\mathfrak{P}, D_1, \ldots, D_{r+n})(\mathfrak{P}) = n - s = \operatorname{alt} \mathfrak{P},$$

por [AC 5.44], ya que R es un anillo local regular, luego es de Cohen-Macaulay. Esto implica que $\operatorname{rang} J(\mathfrak{P}, \operatorname{Der} R)(\mathfrak{P}) \geq \operatorname{alt} \mathfrak{P}$, y la otra desigualdad se cumple por 2.28. ∎

Combinando esto con 2.29, tenemos finalmente:

Teorema 2.35 *Sea k un cuerpo de característica prima, $R = k[[X_1, \ldots, X_n]]$ y $A = R/I$, donde I es un ideal de R. Entonces, el conjunto de los puntos regulares de* $\operatorname{Esp} A$ *es abierto.*

Demostración: Sea $\mathfrak{p} = \mathfrak{P}/I$ un punto regular de $\operatorname{Esp} A$. Entonces, en particular, $A_\mathfrak{p} = R_\mathfrak{P}/I_\mathfrak{P}$ es un dominio íntegro, luego $I_\mathfrak{P} = \mathfrak{Q}R_\mathfrak{P}$, para un cierto $\mathfrak{Q} \in \operatorname{Esp} R$, $\mathfrak{Q} \subset \mathfrak{P}$. El teorema 2.29, junto con el teorema anterior, implica que $\operatorname{rang} J(\mathfrak{Q}; \operatorname{Der} R)(\mathfrak{P}) = \operatorname{alt} \mathfrak{Q} = \operatorname{alt} I_\mathfrak{Q}$.

Sea $r = \operatorname{alt} I_\mathfrak{Q}$. Entonces existen $f_1, \ldots, f_r \in I$ tales que $I_\mathfrak{P} = (f_1, \ldots, f_r)_\mathfrak{P}$. Podemos tomar $g \in R \setminus \mathfrak{P}$ tal que $I_g = (f_1, \ldots, f_r)_g$. Sean $D_1, \ldots, D_r \in \operatorname{Der} R$ tales que $h = \det(D_i f_j) \notin \mathfrak{P}$. Así, si $\mathfrak{p}' = \mathfrak{P}'/I \in \operatorname{Esp} A$ cumple que $gh \notin \mathfrak{P}'$, entonces $I_{\mathfrak{P}'} = (f_1, \ldots, f_r)_{\mathfrak{P}'}$ y $\operatorname{rang} J(I, \operatorname{Der} R)(\mathfrak{P}') = r$. El teorema 2.28 implica entonces que $A_{\mathfrak{p}'}$ es regular. Así pues, el conjunto de los puntos regulares de $\operatorname{Esp} A$ contiene al abierto principal $D(gh)$, que es un entorno de $\mathfrak{p}$. ∎

2.4 Suavidad formal y formas diferenciales

Para terminar el capítulo demostraremos una caracterización de la suavidad formal en términos de los espacios de formas diferenciales. Necesitamos varios resultados previos, el primero de los cuales requiere un concepto auxiliar:

Definición 2.36 Sean $k \longrightarrow A \longrightarrow B$ homomorfismos de anillos y sea I un ideal en B. Diremos que B es *I-suave* sobre A con respecto a k si para toda A-álgebra C, todo ideal N de C tal que $N^2 = 0$ y todo A-homomorfismo $u : B \longrightarrow C/N$ que cumpla $u[I^n] = 0$ para cierto $n \geq 1$, si u se eleva a un k-homomorfismo $v' : B \longrightarrow C$, entonces también puede elevarse a un A-homomorfismo $v : B \longrightarrow C$.

Teorema 2.37 *Sean $k \longrightarrow A \longrightarrow B$ homomorfismos de anillos y sea I un ideal de B. Las afirmaciones siguientes son equivalentes:*

a) B es I-suave sobre A con respecto a k.

b) Si N es un B-módulo tal que $I^n N = 0$ para cierto $n \geq 1$, entonces la aplicación natural $\operatorname{Der}_k(B, N) \longrightarrow \operatorname{Der}_k(A, N)$ es suprayectiva.

c) Para cada $n \geq 1$, la aplicación $\Omega^1_{A/k} \otimes_A (B/I^n) \longrightarrow \Omega^1_{B/k} \otimes_B (B/I^n)$ tiene una inversa por la derecha.

DEMOSTRACIÓN: Llamemos $k \xrightarrow{f} A \xrightarrow{g} B$ a los homomorfismos dados.

a) $\Rightarrow$ b) Sea $C = (B/I^n) * N$ la extensión construida tras la definición 2.9 a partir del cociclo nulo. Sea $u : B \longrightarrow B/I^n = C/N$ el homomorfismo natural. Dada $D \in \mathrm{Der}_k(A, N)$, definimos $\lambda : A \longrightarrow C$ mediante $\lambda(a) = (u(g(a)), D(a))$. Claramente es un homomorfismo, que nos permite considerar a C como A-álgebra. Por otra parte, $v' : B \longrightarrow C$ dado por $v'(b) = (u(b), 0)$ es un k-homomorfismo que eleva a u. Por hipótesis, existe también un A-homomorfismo $v : B \longrightarrow C$ que eleva a u. Necesariamente, será de la forma $v(b) = (u(b), D'(b))$, donde $D' \in \mathrm{Der}_k(B, N)$. Que v sea un A-homomorfismo significa que $gv = \lambda$, luego $gD' = D$, luego se cumple b).

b) $\Rightarrow$ a) Supongamos dado un diagrama conmutativo

$$\begin{array}{ccccc} & & B & \xrightarrow{u} & C/N \\ & & {\scriptstyle g}\uparrow & & \uparrow{\scriptstyle j} \\ k & \xrightarrow[f]{} & A & \xrightarrow[\lambda]{} & C \end{array}$$

según exige la definición de I-suavidad relativa a k. Supongamos que existe un k-homomorfismo $v' : B \longrightarrow C$ que eleva a u. Que eleve a u significa que $v'j = u$, y que sea un k-homomorfismo significa que $fgv' = f\lambda$. Entonces $D = \lambda - gv' \in \mathrm{Der}_k(A, N)$. En efecto, tenemos que $Dj = \lambda j - gu = 0$, luego D toma imágenes en N. Además, multiplicando

$$v'(g(a)) = \lambda(a) - D(a) \qquad \text{por} \qquad v'(g(a')) = \lambda(a') - D(a')$$

y teniendo en cuenta que $D(a)D(a') \in N^2 = 0$, vemos que

$$v'(g(aa')) = \lambda(aa') - \lambda(a)D(a') - \lambda(a')D(a),$$

luego $D(aa') = aD(a') + a'D(a)$. Por último, $fD = 0$, luego D es una k-derivación.

Consideramos a N como B-módulo a través de v'. Si $u[I^n] = 0$, entonces $v'[I^n] \subset N$, luego $I^n N \subset N^2 = 0$. Por hipótesis, existe $D' \in \mathrm{Der}_k(B, N)$ tal que $D = gD'$. Llamamos $v = v' + D'$. Claramente,

$$v(b)v(b') = v'(bb') + v'(b)D'(b') + v'(b')D'(b) = v'(bb') + D'(bb') = v(bb'),$$

luego v es un homomorfismo. Además,

$$vj = v'j + D'j = u \qquad \text{y} \qquad gv = gv' + gD' = gv' + D = \lambda,$$

luego v es una elevación de u y un A-homomorfismo.

b) $\Leftrightarrow$ c) Observemos, en general, que una condición necesaria y suficiente para que un homomorfismo de A-módulos $\alpha : M \longrightarrow N$ tenga inverso por la derecha (es decir, que exista un $\beta : N \longrightarrow M$ tal que $\alpha\beta = 1$) es que para todo A-módulo P, el homomorfismo $\mathrm{Hom}_A(M, P) \longrightarrow \mathrm{Hom}_A(N, P)$ sea suprayectivo.

En nuestro caso, c) equivale a que para todo B-módulo N tal que $I^n B = 0$, el homomorfismo natural

$$\mathrm{Hom}_{B/I^n}(\Omega^1_{B/k} \otimes_B (B/I^n), N) \longrightarrow \mathrm{Hom}_{B/I^n}(\Omega^1_{A/k} \otimes_A (B/I^n), N)$$

sea suprayectivo. A través de dos isomorfismos canónicos, este homomorfismo se corresponde con

$$\mathrm{Hom}_B(\Omega^1_{B/k}, N) \longrightarrow \mathrm{Hom}_A(\Omega^1_{A/k}, N),$$

que a su vez se corresponde con

$$\mathrm{Der}_k(B, N) \longrightarrow \mathrm{Der}_k(A, N),$$

luego, ciertamente, b) es equivalente a c). ∎

Teorema 2.38 *Sea A un anillo, B una A-álgebra e I un ideal de B. Si B es I-suave sobre A, entonces $\Omega^1_{B/A} \otimes_B (B/I)$ es un B/I-módulo proyectivo.*

Demostración: Hemos de probar que si $\phi : L \longrightarrow M$ es un epimorfismo de B/I-módulos, entonces el homomorfismo

$$\mathrm{Hom}_{B/I}(\Omega^1_{B/A} \otimes_B (B/I), L) \longrightarrow \mathrm{Hom}_{B/I}(\Omega^1_{B/A} \otimes_B (B/I), M)$$

también es suprayectivo. A través de isomorfismos canónicos, este homomorfismo se corresponde con

$$\mathrm{Hom}_B(\Omega^1_{B/A}, L) \longrightarrow \mathrm{Hom}_B(\Omega^1_{B/A}, M),$$

y éste a su vez con $\mathrm{Der}_A(B, L) \longrightarrow \mathrm{Der}_A(B, M)$.

Sea $C = (B/I) * L$ la extensión construida tras la definición 2.9 a partir del cociclo nulo, y sea $N \subset L$ el núcleo de ϕ. Podemos considerar tanto a N como a L como ideales de C, de modo que $L^2 = 0$ y, por consiguiente, también $N^2 = 0$. Además $C/L = B/I$, mientras que $C/N = (B/I) * M$.

Para cada $D \in \mathrm{Der}_A(B, M)$, tenemos un A-homomorfismo $u : B \longrightarrow C/N$ dado por $u(b) = (\bar{b}, D(b))$. Por hipótesis podemos elevarlo a un A-homomorfismo $v : B \longrightarrow C$, que será de la forma $v(b) = (b, D'(b))$, donde $D' \in \mathrm{Der}_A(B, L)$ es una antiimagen de D. ∎

Teorema 2.39 *Sea B un anillo, e I un ideal nilpotente. Sea $u : L \longrightarrow M$ un homomorfismo de B-módulos, donde M es proyectivo. Entonces u tiene inverso por la derecha si y sólo si lo tiene $\bar{u} : L/IL \longrightarrow M/IM$.*

Demostración: Una implicación es trivial. Si $\bar{v} : M/IM \longrightarrow L/IL$ es un inverso por la derecha de $\bar{u}$, como M es proyectivo, existe un homomorfismo v que hace conmutativo el diagrama siguiente:

$$\begin{array}{ccc} M & \xrightarrow{v} & L \\ \downarrow & & \downarrow \\ M/IM & \xrightarrow[\bar{v}]{} & L/IL \end{array}$$

Llamemos $w = uv : L \longrightarrow L$. Así w induce la identidad en L/IL, lo que implica que $L = w[L] + IL$. Por lo tanto,

$$L/w[L] = I(L/w[L]) = I^2(L/w[L]) = \cdots$$

Como I es nilpotente, concluimos que w es suprayectivo. Por otra parte, si $x \in \mathrm{N}\, w$, entonces $0 = w(x) \equiv x \pmod{I}L$, luego $x \in IL$. Por lo tanto, $x = \sum a_i y_i$, con $a_i \in I$, $y_i \in L$. De aquí,

$$0 = w(x) = \sum a_i w(y_i) \equiv \sum a_i y_i \pmod{I^2 L},$$

luego $x \in I^2 L$. Prosiguiendo de este modo concluimos que $x \in I^n L = 0$. Así pues, w es un automorfismo de L y vw^{-1} es un inverso por la derecha de u, ya que $uvw^{-1} = ww^{-1} = 1$. ∎

Finalmente podemos probar:

Teorema 2.40 *Sean $k \longrightarrow A \longrightarrow B$ homomorfismos de anillos y sea I un ideal de B tal que B sea I-suave sobre k. Entonces B es I-suave sobre A si y sólo si el homomorfismo natural $\Omega^1_{A/k} \otimes_A (B/I) \longrightarrow \Omega^1_{B/k} \otimes_B (B/I)$ tiene inverso por la derecha.*

Demostración: Si B es I suave sobre A, entonces también es I suave sobre A con respecto a k, luego basta aplicar el teorema 2.37. Recíprocamente, si $n \geq 1$, llamemos $B_n = B/I^n$. Como la I-suavidad es lo mismo que la I^n-suavidad, el teorema 2.38 nos da que $\Omega^1_{B/k} \otimes_B B_n$ es un B_n-módulo proyectivo. Sea $I_n = I/I^n$, de modo que I_n es nilpotente y $B_n/I_n = B/I$. Más aún,

$$(\Omega^1_{A/k} \otimes_A B_n)/I_n(\Omega^1_{A/k} \otimes_A B_n) \cong \Omega^1_{A/k} \otimes_A (B/I),$$

e igualmente con B en lugar de A. El teorema anterior nos da entonces que el homomorfismo

$$\Omega^1_{B/k} \otimes_B B_n \longrightarrow \Omega^1_{A/k} \otimes_A B_n$$

tiene inverso por la derecha, luego el teorema 2.37 implica que B es I-suave sobre A con respecto a k. Como también es I-suave sobre k, concluimos que es I-suave sobre A. ∎

En realidad nos interesará la siguiente consecuencia inmediata:

Teorema 2.41 *Sea A un anillo local regular que contenga un cuerpo k_0, sea $\mathfrak{m}$ su ideal maximal y $k = A/\mathfrak{m}$ su cuerpo de restos. Entonces A es $\mathfrak{m}$-suave sobre k_0 si y sólo si el homomorfismo $\Omega^1_{k_0/\mathbb{Z}} \otimes_{k_0} k \longrightarrow \Omega^1_{A/\mathbb{Z}} \otimes_A k$ es inyectivo.*

Demostración: Sea $k' \subset k_0$ el cuerpo primo. Entonces A es $\mathfrak{m}$-suave sobre k' por el teorema 2.23. Basta aplicar el teorema anterior a $k' \longrightarrow k_0 \longrightarrow A$. (Notemos que $\Omega^1_{k_0/\mathbb{Z}} = \Omega^1_{k_0/k'}$, e igualmente con A en lugar de k_0.) ∎

Capítulo III

Anillos excelentes

La clase de los anillos excelentes contiene a la de las álgebras de tipo finito sobre un cuerpo y conserva sus propiedades más importantes; pero es mucho más extensa, hasta el punto de que contiene casi todos los anillos que aparecen de forma natural en geometría algebraica, en especial los anillos noetherianos locales completos. La definición es un tanto técnica, y dedicaremos secciones sucesivas a describir las propiedades que aparecen en ella y otras relacionadas.

3.1 Anillos universalmente catenarios

La propiedad que estudiamos aquí está relacionada con el comportamiento de la dimensión de Krull:

Definición 3.1 Un anillo noetheriano A es *catenario* si para toda terna de ideales primos $\mathfrak{q} \subset \mathfrak{p} \subset \mathfrak{m}$ se cumple la igualdad

$$\operatorname{alt}(\mathfrak{m}/\mathfrak{q}) = \operatorname{alt}(\mathfrak{m}/\mathfrak{p}) + \operatorname{alt}(\mathfrak{p}/\mathfrak{q}).$$

Diremos que A es *universalmente catenario* si toda A-álgebra finitamente generada es catenaria. (Y, en tal caso, es obvio que, de hecho, es universalmente catenaria.)

Recordemos que, por definición, $\operatorname{alt}(\mathfrak{m}/\mathfrak{q})$ es el máximo de las longitudes n de las cadenas de ideales primos

$$\mathfrak{q} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{m}.$$

Se cumple que un anillo noetheriano A es catenario si y sólo si toda cadena maximal que una $\mathfrak{q}$ con $\mathfrak{m}$ tiene longitud $n = \operatorname{alt}(\mathfrak{m}/\mathfrak{q})$. En efecto, si A es catenario y la cadena anterior es maximal, entonces

$$\operatorname{alt}(\mathfrak{m}/\mathfrak{q}) = \operatorname{alt}(\mathfrak{p}_1/\mathfrak{p}_0) + \cdots + \operatorname{alt}(\mathfrak{p}_n/\mathfrak{p}_{n-1}),$$

pero es obvio que $\operatorname{alt}(\mathfrak{p}_i/\mathfrak{p}_{i-1}) = 1$, luego $\operatorname{alt}(\mathfrak{m}/\mathfrak{n}) = n$. Recíprocamente, dados ideales $\mathfrak{q} \subset \mathfrak{p} \subset \mathfrak{m}$, tomamos cadenas maximales que unan $\mathfrak{q}$ con $\mathfrak{p}$ y $\mathfrak{p}$ con $\mathfrak{m}$,

cuyas longitudes serán $\operatorname{alt}(\mathfrak{p}/\mathfrak{q})$ y $\operatorname{alt}(\mathfrak{m}/\mathfrak{p})$, respectivamente. La unión de ambas cadenas será una cadena maximal que une $\mathfrak{q}$ con $\mathfrak{m}$, luego su longitud será $\operatorname{alt}(\mathfrak{m}/\mathfrak{q}) = \operatorname{alt}(\mathfrak{m}/\mathfrak{p}) + \operatorname{alt}(\mathfrak{p}/\mathfrak{q})$. ∎

Teorema 3.2 *Sea A un anillo noetheriano.*

a) A es universalmente catenario si y sólo si $A[X_1, \ldots, X_n]$ es catenario para todo $n \geq 1$.

b) Toda localización y todo cociente de un anillo (universalmente) catenario es (universalmente) catenario.

c) A es (universalmente) catenario si y sólo si $A_\mathfrak{p}$ es (universalmente) catenario, para todo ideal maximal $\mathfrak{p}$ de A.

Demostración: Es evidente que las localizaciones y los cocientes de los anillos catenarios son catenarios, de donde se sigue a). Veamos que esto implica la parte de b) para anillos universalmente catenarios.

En efecto, si A es universalmente catenario y $S \subset A$ es un conjunto multiplicativo, entonces $(S^{-1}A)[X_1, \ldots, X_n] = S^{-1}(A[X_1, \ldots, X_n])$, luego es catenario. Similarmente, si I es un ideal de A, entonces

$$(A/I)[X_1, \ldots, X_n] = A[X_1, \ldots, X_n]/I[X_1, \ldots, X_n],$$

luego es catenario.

Una implicación de c) es un caso particular de b). También es claro que si $A_\mathfrak{p}$ es catenario para todo ideal maximal $\mathfrak{p}$, entonces A es catenario. (Para comprobar la definición para tres primos $\mathfrak{p} \subset \mathfrak{q} \subset \mathfrak{m}$ localizamos A respecto de un ideal maximal que contenga a $\mathfrak{m}$.)

Supongamos ahora que $A_\mathfrak{p}$ es universalmente catenario, para todo ideal maximal $\mathfrak{p}$, y hemos de probar que $A[X_1, \ldots, X_n]$ es catenario, para lo cual a su vez basta probar que lo es $A[X_1, \ldots, X_n]_\mathfrak{P}$, para un ideal maximal $\mathfrak{P}$. Tomamos $\mathfrak{p} = A \cap \mathfrak{P}$, que es un ideal maximal de A, ya que si $a \in A \setminus \mathfrak{p}$, entonces a es una unidad módulo $\mathfrak{P}$, luego existe un polinomio F tal que $aF - 1 \in \mathfrak{P}$, luego $aF(0) - 1 \in \mathfrak{p}$, luego a es una unidad módulo $\mathfrak{p}$.

Es claro que $A[X_1, \ldots, X_n]_\mathfrak{P} = A_\mathfrak{p}[X_1, \ldots, X_n]_{\mathfrak{P}'}$, donde $\mathfrak{P}' = \mathfrak{P}_\mathfrak{p}$, y este anillo es catenario por ser una localización de una $A_\mathfrak{p}$-álgebra finitamente generada. ∎

Si A es un dominio íntegro catenario, aplicando la definición para $\mathfrak{q} = 0$ obtenemos la relación

$$\operatorname{alt}\mathfrak{m} = \operatorname{alt}(\mathfrak{m}/\mathfrak{p}) + \operatorname{alt}\mathfrak{p}$$

y, recíprocamente, esta relación (para todo par de ideales primos $\mathfrak{p} \subset \mathfrak{m}$) implica que A es catenario, aunque no sea un dominio íntegro.

El ejemplo más importante de anillos universalmente catenarios es el siguiente:

Teorema 3.3 *Toda álgebra afín sobre un cuerpo es universalmente catenaria.*

DEMOSTRACIÓN: Puesto que toda álgebra afín es un cociente de un anillo de polinomios, basta probar que el anillo $A = k[X_1, \ldots, X_n]$ es catenario. Si $\mathfrak{q} \subset \mathfrak{p}$ son dos ideales primos, entonces $A/\mathfrak{q}$ es una k-álgebra afín íntegra, luego [AC 3.75] nos da que

$$\dim A/\mathfrak{q} = \operatorname{alt}(\mathfrak{p}/\mathfrak{q}) + \dim A/\mathfrak{p}.$$

Por el mismo teorema aplicado a A vemos que

$$\dim A = \operatorname{alt}\mathfrak{p} + \dim A/\mathfrak{p}, \quad \dim A = \operatorname{alt}\mathfrak{q} + \dim A/\mathfrak{q},$$

y así concluimos que $\operatorname{alt}\mathfrak{p} = \operatorname{alt}(\mathfrak{p}/\mathfrak{q}) + \operatorname{alt}\mathfrak{q}$. ∎

Otra familia notable de anillos catenarios es la de los anillos locales regulares. Más en general:

Teorema 3.4 *Todo anillo local de Cohen-Macaulay es catenario.*

DEMOSTRACIÓN: Sea A un anillo local de Cohen-Macaulay y sea $\mathfrak{p}$ un ideal primo de A. Por el teorema [AC 5.44] tenemos que

$$\dim A = \operatorname{alt}\mathfrak{p} + \dim(A/\mathfrak{p}).$$

Si $\mathfrak{p} \subset \mathfrak{q}$ es otro ideal primo, el teorema [AC 5.43] implica que $A_\mathfrak{q}$ también es un anillo local de Cohen-Macaulay, y la igualdad precedente aplicada a $A_\mathfrak{q}$ es

$$\dim A_\mathfrak{q} = \operatorname{alt}(\mathfrak{p}A_\mathfrak{q}) + \dim(A_\mathfrak{q}/\mathfrak{p}A_\mathfrak{q}),$$

que equivale a $\operatorname{alt}\mathfrak{q} = \operatorname{alt}\mathfrak{p} + \operatorname{alt}(\mathfrak{q}/\mathfrak{p})$. ∎

Pasamos ahora a la propiedad correspondiente en esquemas:

Definición 3.5 Diremos que un esquema localmente noetheriano X es *(universalmente) catenario* si los anillos $\mathcal{O}_{X,P}$ son (universalmente) catenarios, para todo punto $P \in X$.

Es claro que X es (universalmente) catenario si y sólo si, para cada abierto afín $U \subset X$, el anillo $\mathcal{O}_X(U)$ es (universalmente) catenario o, también, si X puede cubrirse por abiertos afines U con esta propiedad. En particular, un anillo A es (universalmente) catenario si y sólo si lo es el esquema $\operatorname{Esp} A$.

Por otra parte, observemos que X es universalmente catenario si y sólo si el producto $A^n_X = A^n_\mathbb{Z} \times_\mathbb{Z} X$ es catenario. En efecto, basta tener en cuenta que, si $U \subset X$ recorre los abiertos afines de X, los abiertos A^n_U cubren A^n_X y se cumple que $\mathcal{O}_{A^n_X}(A^n_U) = \mathcal{O}_X(U)[X_1, \ldots, X_n]$.

Un esquema localmente noetheriano X es catenario si y sólo si para toda terna de cerrados irreducibles no vacíos $W \subset Y \subset Z \subset X$ se cumple que

$$\operatorname{codim}_Z(W) = \operatorname{codim}_Z(Y) + \operatorname{codim}_Y(W).$$

En efecto, si P es el punto genérico de W, entonces W, Y, Z se corresponden con tres ideales primos de $\mathcal{O}_{X,P}$, de modo que la igualdad anterior equivale a la igualdad que define a los anillos catenarios.

El teorema siguiente es una mera reformulación de 3.3:

Teorema 3.6 *Todo conjunto algebraico sobre un cuerpo es universalmente catenario.*

Por otra parte:

Teorema 3.7 *Todo esquema regular localmente noetheriano es universalmente catenario.*

Demostración: Sea X un esquema regular localmente noetheriano. Como $A^n_{\mathbb{Z}}$ es suave sobre $\mathbb{Z}$, tenemos que A^n_X es suave sobre X, luego [E 7.50] implica que A^n_X también es regular, luego es catenario, pues los anillos locales regulares son catenarios. ∎

Terminamos la sección con algunas consecuencias sobre la dimensión de Krull:

Teorema 3.8 *Sea $f : X \longrightarrow Y$ un homomorfismo denso localmente de tipo finito entre esquemas íntegros localmente noetherianos, sea $x \in X$ y llamemos $y = f(x)$. Entonces*

$$\dim \mathcal{O}_{X,x} + \text{grad.tr.}_{k(y)} k(x) \leq \dim \mathcal{O}_{Y,y} + \text{grad.tr.}_{K(Y)} K(X),$$

y si Y es universalmente catenario se cumple la igualdad.

Demostración: No perdemos generalidad si suponemos que $X = \operatorname{Esp} B$ e $Y = \operatorname{Esp} A$ son afines noetherianos y que f es de tipo finito, con lo que se corresponde con un homomorfismo de anillos $A \longrightarrow B$ que convierte a B en una A-álgebra finitamente generada. Que f sea denso se traduce en que el punto genérico de X se corresponde con el punto genérico de Y, luego $A \longrightarrow B$ es un monomorfismo de anillos. Pongamos que $B = A[b_1, \ldots, b_n]$. Los puntos x e y se identifican con ideales primos $\mathfrak{P}$ y $\mathfrak{p}$ de B y A tales que $\mathfrak{p} = \mathfrak{P} \cap A$. En estos términos, el teorema equivale a que

$$\dim B_{\mathfrak{P}} - \dim A_{\mathfrak{p}} \leq \text{grad.tr.}_{A_0} B_0 - \text{grad.tr.}_{k(\mathfrak{p})} k(\mathfrak{P}),$$

y se cumple la igualdad si A es universalmente catenario. (Notemos que las localizaciones A_0 y B_0 son los respectivos cuerpos de fracciones.) Consideremos las A-álgebras $B_i = A[b_1, \ldots, b_i]$ con los ideales $\mathfrak{P}_i = \mathfrak{P} \cap B_i$. Si A es universalmente catenario, todos los B_i lo son. Cada extensión $B_i \subset B_{i+1}$ cumple las mismas hipótesis que la extensión $A \subset B$. Si probamos la fórmula para cada una de ellas, tenemos que

$$\dim B_{i+1\mathfrak{P}_{i+1}} - \dim B_{i\mathfrak{P}_i} \leq \text{grad.tr.}_{B_{i+1,0}} B_{i,0} - \text{grad.tr.}_{k(\mathfrak{P}_i)} k(\mathfrak{P}_{i+1})$$

(con igualdad si A es universalmente catenario). Sumando todas las desigualdades (o igualdades) obtenemos la correspondiente a $A \subset B$. Equivalentemente, podemos suponer que $n = 1$ o, lo que es lo mismo, que $B = A[b]$.

Cambiando A por $A_\mathfrak{p}$ y B por $B_\mathfrak{p} = A_\mathfrak{p}[b]$ no se modifican ni las localizaciones ni los grados de trascendencia que aparecen en la desigualdad. Además, si A es universalmente catenario también lo es $A_\mathfrak{p}$. Equivalentemente, podemos suponer que A es un anillo local y que $\mathfrak{p}$ es su ideal maximal. Llamemos $k = k(\mathfrak{p}) = A/\mathfrak{p}$ y sea $B = A[b] = A[X]/I$, donde I es un ideal primo de $A[X]$.

Si $I = 0$, entonces $B = A[X]$, $\text{grad.tr.}_{A_0} B_0 = 1$ y $B/\mathfrak{p}B = k[X]$ tiene dimensión 1, luego

$$\text{alt}(\mathfrak{P}/\mathfrak{p}B) = \begin{cases} 1 & \text{si } \mathfrak{p}B \subsetneq \mathfrak{P}, \\ 0 & \text{si } \mathfrak{p}B = \mathfrak{P}. \end{cases}$$

En el primer caso $\mathfrak{P}' = \mathfrak{P}/\mathfrak{p}B$ es un ideal maximal de $k[X]$, luego $\mathfrak{P}$ es un ideal maximal de B, luego $k(\mathfrak{P}) = B/\mathfrak{P}$ es una extensión finita de k, pues $\mathfrak{P}'$ es un punto cerrado del conjunto algebraico $\operatorname{Esp} k[X]$, y esto implica que $k(\mathfrak{P}') = k(\mathfrak{P})$ es una extensión finita de k. Por consiguiente, $\text{grad.tr.}_k k(\mathfrak{P}) = 0$. En el segundo caso $k(\mathfrak{P}) \cong k(X)$, luego $\text{grad.tr.}_k k(\mathfrak{P}) = 1$. En ambos casos concluimos que

$$\text{alt}(\mathfrak{P}/\mathfrak{p}B) = 1 - \text{grad.tr.}_k k(\mathfrak{P}) = \text{grad.tr.}_{A_0} B_0 - \text{grad.tr.}_k k(\mathfrak{P}).$$

Por otra parte, B es un A-módulo libre, luego es plano, luego podemos aplicar el teorema [E 4.52], que en términos de anillos afirma que

$$\text{alt}(\mathfrak{P}/\mathfrak{p}B) = \dim B_\mathfrak{P} - \dim A_\mathfrak{p}.$$

(Observemos que la fibra de $\mathfrak{p}$ es $B \otimes_A (A/\mathfrak{p}) \cong B/\mathfrak{p}B$ y que $\mathfrak{P}$ se corresponde en este anillo con $\mathfrak{P}/\mathfrak{p}B$.) Uniendo las dos igualdades obtenemos que la fórmula del enunciado se cumple con igualdad.

Supongamos ahora que $I \neq 0$. Entonces b es raíz de cualquier polinomio no nulo de I, por lo que es algebraico sobre k, y esto hace que $\text{grad.tr.}_{A_0} B_0 = 0$. Sea $\mathfrak{P} = \mathfrak{P}^*/I$. Como $A \longrightarrow A[X]/I$ es inyectiva, tenemos que $A \cap I = 0$, luego $\operatorname{alt} I = \operatorname{alt} I A_0[X]$, pues $A_0[X] = S^{-1}A[X]$, donde $S = A \setminus \{0\}$, y los ideales primos de este anillo se corresponden con los ideales de $A[X]$ disjuntos con S. Así pues,

$$\operatorname{alt} I = \operatorname{alt} I A_0[X] \leq \dim A_0[X] = 1$$

y, puesto que $I \neq 0$, ha de ser $\operatorname{alt} I = 1$. Por consiguiente,

$$\operatorname{alt} \mathfrak{P} \leq \operatorname{alt} \mathfrak{P}^* - \operatorname{alt} I = \operatorname{alt} \mathfrak{P}^* - 1,$$

y si A es universalmente catenario, entonces $A[X]$ es catenario y tenemos la igualdad.

Por otra parte, es claro que $\mathfrak{P}^* \cap A = \mathfrak{p}$, así como que $k(\mathfrak{P}^*) = k(\mathfrak{P})$, por lo que podemos aplicar el caso $I = 0$, ya probado, a la extensión $A \subset A[X]$ y el ideal $\mathfrak{P}^*$. Esto nos da la igualdad

$$\operatorname{alt} \mathfrak{P}^* - \operatorname{alt} \mathfrak{p} = 1 - \text{grad.tr.}_{k(\mathfrak{p})} k(\mathfrak{P}).$$

Combinando ambas resulta

$$\operatorname{alt}\mathfrak{P} - \operatorname{alt}\mathfrak{p} \leq -\text{grad.tr.}_{k(\mathfrak{p})}k(\mathfrak{P}),$$

y si A es universalmente catenario se cumple la igualdad. Es claro que esto equivale a la fórmula del enunciado. ∎

Como consecuencia obtenemos la siguiente generalización de [E 4.53]:

Teorema 3.9 *Sea $f : X \longrightarrow Y$ un homomorfismo plano, suprayectivo y de tipo finito entre esquemas íntegros noetherianos, y supongamos además que Y es universalmente catenario. Entonces, para todo $y \in Y$, la fibra X_y tiene todas sus componentes irreducibles de la misma dimensión, y ésta es igual a*

$$\dim X_y = \dim X - \dim Y.$$

Demostración: La fibra X_y es un conjunto algebraico sobre $k(y)$, luego contiene un punto cerrado $x \in X_y$. Entonces $k(x)$ es una extensión finita de $k(y)$. Según el teorema anterior:

$$\dim \mathcal{O}_{X,x} - \dim \mathcal{O}_{Y,y} = d,$$

donde $d = \text{grad.tr.}_{K(Y)}K(X)$ no depende de x ni de y. El teorema [E 4.52] nos da que $\dim \mathcal{O}_{X_y,x} = d$, para todo punto cerrado $x \in X_y$, lo que implica que todas las componentes irreducibles de X_y tienen la misma dimensión d.

Si ahora tomamos como $y \in Y$ un punto cerrado, entonces $\dim \mathcal{O}_{Y,y} = \dim Y$ y, como la fibra X_y es cerrada en X, el punto x también es cerrado en X, luego $\dim \mathcal{O}_{X,x} = \dim X$, de donde se sigue que $d = \dim X - \dim Y$. ∎

Ahora podemos demostrar otro hecho destacable:

Teorema 3.10 *Sea $f : X \longrightarrow Y$ un homomorfismo propio y birracional entre esquemas íntegros localmente noetherianos. Entonces* $\dim X = \dim Y$.

Demostración: Para todo $x \in X$, llamando $y = f(x)$, tenemos que

$$\dim \mathcal{O}_{X,x} \leq \dim \mathcal{O}_{Y,y} + \text{grad.tr.}_{K(Y)}K(X) - \text{grad.tr.}_{k(y)}k(x) \leq \dim \mathcal{O}_{Y,y}$$

porque $K(X) = K(Y)$. Si en X podemos formar una cadena creciente de $n+1$ cerrados irreducibles, cualquier x que pertenezca al primero de ellos cumple $\dim \mathcal{O}_{X,x} \geq n$, luego existe un $y \in Y$ tal que $\dim Y \geq \dim \mathcal{O}_{Y,y} \geq n$, luego $\dim X \leq \dim Y$ (entendiendo que si X tiene dimensión infinita, lo mismo le sucede a Y).

Ahora vamos a probar la desigualdad opuesta, $\dim X \geq \dim Y$. Basta probar que si $U \subset Y$ es un abierto noetheriano, entonces $\dim U \leq \dim X$, pues la dimensión de Y es el supremo de las dimensiones de los abiertos U. (Ver la prueba de [E 3.22].) Como $\dim X \geq \dim f^{-1}[U]$, basta probar el teorema para la restricción $f^{-1}[U] \longrightarrow U$ o, equivalentemente, podemos suponer que X e Y son noetherianos. (notemos que $f^{-1}[U]$ es noetheriano porque f es de tipo finito.)

En general, la desigualdad $\dim X \geq \dim Y$ es válida para cualquier aplicación continua, cerrada y suprayectiva entre espacios topológicos noetherianos. En efecto, si X tiene dimensión infinita no hay nada que probar. En caso contrario, razonamos por inducción sobre la dimensión de X.

Supongamos que $\dim X = n$ y que el resultado es cierto para espacios de dimensión menor que n. Sea $X = X_1 \cup \cdots \cup X_m$ la descomposición de X en componentes irreducibles. Entonces,

$$Y = f[X_1] \cup \cdots \cup f[X_m]$$

es una descomposición de Y en cerrados irreducibles (aunque puede que alguno sea redundante, por estar contenido en la unión de los otros). Basta probar que $\dim X_i \geq \dim f[X_i]$, pues entonces

$$\dim X = \max_i \dim X_i \geq \max_i \dim f[X_i] = \dim Y.$$

Como la restricción $f|_{X_i} : X_i \longrightarrow f[X_i]$ cumple las mismas hipótesis que f, concluimos que no perdemos generalidad si suponemos que X es irreducible. (En principio, puede ser $\dim X_i < n$, pero entonces tenemos la desigualdad por hipótesis de inducción. Así pues, mantenemos la hipótesis de que $\dim X = n$.) Si X es irreducible, también lo es Y. Si $\dim Y = 0$ no hay nada que probar. Sea, pues,

$$Y_0 \subsetneq Y_1 \subsetneq \cdots \subsetneq Y_m = Y$$

una cadena de cerrados irreducibles en Y, con $m \geq 1$. Entonces $f^{-1}[Y_{m-1}] \subsetneq X$ es cerrado y obviamente $\dim f^{-1}[Y_{m-1}] < n$, luego, por hipótesis de inducción $m - 1 \leq \dim Y_{m-1} < n$, luego $m \leq n$. Esto prueba que $\dim Y \leq n$. ∎

3.2 Anillos de Nagata

Ahora nos ocupamos de una propiedad relacionada con las clausuras enteras (en términos de anillos) o con las normalizaciones (en términos de esquemas).

Definición 3.11 Sea A un dominio íntegro noetheriano y K su cuerpo de cocientes. Diremos que A cumple la propiedad N_1 si la clausura entera de A en K es un A-módulo finitamente generado. Diremos que A cumple la propiedad N_2 si, para toda extensión finita L de K, la clausura entera de A en L es un A-módulo finitamente generado. Diremos que un anillo noetheriano B es un *anillo de Nagata* si, para todo ideal primo $\mathfrak{p}$ de B, el dominio íntegro $B/\mathfrak{p}$ tiene la propiedad N_2.

Estas propiedades se conservan por localización. Para probarlo, conviene observar un hecho elemental:

Teorema 3.12 *Sea A un dominio íntegro, sea K su cuerpo de cocientes, sea L/K una extensión finita, sea B la clausura entera de A en L y sea $S \subset A$ un conjunto multiplicativo. Entonces, la clausura entera de $S^{-1}A$ en L es $S^{-1}B$.*

DEMOSTRACIÓN: Si $x \in L$ es entero sobre $S^{-1}A$, entonces satisface una ecuación de la forma

$$x^n + \frac{a_1}{s}x^{n-1} + \frac{a_2}{s}x^{n-2} + \cdots + \frac{a_0}{s} = 0,$$

de donde se sigue que $s^n x \in B$, luego $x \in S^{-1}B$. El recíproco se prueba análogamente. ∎

Con esto podemos probar:

Teorema 3.13 *Toda localización de un anillo con la propiedad N_1, N_2 o de Nagata cumple la misma propiedad.*

DEMOSTRACIÓN: Sea A un dominio íntegro y $S \subset A$ un subconjunto multiplicativo. Sea K el cuerpo de cocientes de A, sea L/K una extensión finita y B la clausura entera de A en L. Según el teorema anterior, la clausura entera de $S^{-1}A$ en L es $S^{-1}B$, por lo que si A es N_2 (o es N_1 y tomamos $L = K$), sabemos que B es un A-módulo finitamente generado, luego $S^{-1}B$ es un $S^{-1}A$-módulo finitamente generado, lo que prueba que $S^{-1}A$ tiene la propiedad N_2 (o N_1).

Supongamos ahora que A es un anillo de Nagata (no necesariamente un dominio íntegro). Un ideal primo de $S^{-1}A$ es de la forma $S^{-1}\mathfrak{p}$, donde $\mathfrak{p}$ es un primo de A disjunto con S. Entonces, $S^{-1}A/S^{-1}\mathfrak{p} = S'^{-1}(A/\mathfrak{p})$, donde $S' \subset A/\mathfrak{p}$ está formado por las clases de los elementos de S. Como $A/\mathfrak{p}$ tiene la propiedad N_2, por la parte ya probada, lo mismo vale para $S^{-1}A/S^{-1}\mathfrak{p}$, luego $S^{-1}A$ también es un anillo de Nagata. ∎

El teorema siguiente muestra que la distancia entre las propiedades N_1 y N_2 es menor de lo que parece:

Teorema 3.14 *Sea A un dominio íntegro noetheriano íntegramente cerrado y K su cuerpo de cocientes, sea L una extensión finita separable de K y sea B la clausura entera de A en L. Entonces B es un A-módulo finitamente generado.*

DEMOSTRACIÓN: Como A es noetheriano, podemos sustituir L por una extensión finita separable, y suponer que la extensión L/K es finita de Galois. Fijemos una K-base $\omega_1, \ldots, \omega_n$ de L y sea $\omega_1^*, \ldots, \omega_n^*$ su base dual, es decir, la que cumple que $\mathrm{Tr}_K^L(\omega_i\omega_j^*) = \delta_{ij}$. (Existe porque, al ser la extensión separable, la forma bilineal definida por la traza es regular.[1]) Multiplicando los ω_i^* por un elemento adecuado de A (lo que exige dividir cada ω_i por el mismo elemento, para que las bases sigan siendo duales), podemos exigir que cada ω_i^* sea entero sobre A.

Así, todo $\alpha \in B$ se expresa como combinación lineal $\alpha = \alpha_1\omega_1 + \cdots + \alpha_n\omega_n$ donde $\alpha_i = \mathrm{Tr}_K^L(\alpha\omega_i^*) \in K$ es entero sobre A, luego $\alpha_i \in A$. Esto significa que B es un submódulo del A-módulo generado por $\omega_1, \ldots, \omega_n$, luego B es un A-módulo finitamente generado. ∎

Como consecuencia inmediata:

[1] Ver el teorema 10.29 de mi libro de Álgebra.

Teorema 3.15 *Un dominio íntegro noetheriano de característica* 0 *tiene la propiedad* N_2 *si y sólo si tiene la propiedad* N_1.

DEMOSTRACIÓN: Sea A un dominio íntegro noetheriano de característica 0 y sea K su cuerpo de cocientes. Si tiene la propiedad N_1 y L es una extensión finita de K, entonces la clausura entera B de A en L es finitamente generada sobre la clausura entera en K (por el teorema anterior) y ésta es finitamente generada sobre A (por la propiedad N_1), luego B es un A-módulo finitamente generado. ∎

En característica prima, la propiedad N_2 se reduce al caso de extensiones puramente inseparables:

Teorema 3.16 *Sea A un dominio íntegro noetheriano y K su cuerpo de cocientes. Entonces A tiene la propiedad N_2 si y sólo si para toda extensión finita puramente inseparable L/K se cumple que la clausura entera de A en L es un A-módulo finitamente generado.*

DEMOSTRACIÓN: Basta tener en cuenta que toda extensión finita puede descomponerse en una extensión puramente inseparable seguida de una extensión separable. ∎

El teorema siguiente nos permitirá probar que los anillos locales completos son anillos de Nagata:

Teorema 3.17 (Tate) *Sea A un dominio íntegro noetheriano íntegramente cerrado y sea $x \in A$ un elemento no nulo tal que $\mathfrak{p} = Ax$ es un ideal primo. Supongamos que A es completo con la topología $\mathfrak{p}$-ádica y que $A/\mathfrak{p}$ es N_2. Entonces A es N_2.*

DEMOSTRACIÓN: Por el teorema 3.15, podemos suponer que A tiene característica prima p. Sea K el cuerpo de cocientes de A, sea L/K una extensión finita puramente inseparable y sea B la clausura entera de A en L. Sea $e = p^f$ tal que $L^e \subset K$. Hemos de probar que B es un A-módulo finitamente generado. Como A es noetheriano, podemos sustituir L por una extensión, lo que nos permite suponer que existe $y \in L$ tal que $x = y^e$. Como A es íntegramente cerrado, resulta que $B = \{b \in L \mid b^e \in A\}$. En particular, $y \in B$.

Vamos a probar que B es un A-módulo finitamente generado mediante el teorema 2.20. Tenemos que A es completo con la topología $\mathfrak{p}$-ádica, luego nos falta probar que la topología $\mathfrak{p}$-ádica en B es de Hausdorff y que $B/\mathfrak{p}B$ es un $A/\mathfrak{p}$-módulo finitamente generado.

Tomemos un ideal primo $\mathfrak{P}$ de B tal que $\mathfrak{P} \cap A = \mathfrak{p}$. Entonces

$$\mathfrak{P} = \{b \in B \mid b^e \in \mathfrak{p}\} = yB.$$

(Si $u \in \mathfrak{P}$, entonces $u^e = y^e a$, luego $(u/y)^e \in A$, luego $b = u/y \in B$, luego $u \in yB$.) Por lo tanto, $\mathfrak{p}B = xB = (yB)^e = \mathfrak{P}^e$.

Así, $A_\mathfrak{p}$ y $B_\mathfrak{P}$ son dominios íntegros noetherianos locales cuyos ideales maximales son principales y no nulos. Esto implica que son anillos de valoración discreta (pues, por ejemplo, todo elemento de A es de la forma ϵx^n, donde ϵ es una unidad).

Observemos que $|k(\mathfrak{P}) : k(\mathfrak{p})| \leq |L : K|$. Esto es un caso particular de la conocida fórmula $n = ef$, pero podemos dar una prueba elemental: basta ver que si $\omega_1, \ldots, \omega_f \in B_\mathfrak{P}$ son linealmente independientes en $k(\mathfrak{P})$ sobre $k(\mathfrak{p})$, entonces son linealmente independientes sobre K. En caso contrario, tendríamos una combinación lineal $\alpha_1\omega_1 + \cdots + \alpha_f\omega_f = 0$, con $\alpha_i \in K$. Multiplicando por la potencia adecuada de x podemos exigir que $\alpha_i \in A_\mathfrak{p}$ para todo i y que al menos uno de ellos sea una unidad. Pero entonces, al tomar clases módulo $\mathfrak{P}$ tendríamos una combinación lineal no trivial de los ω_i igualada a 0.

Es claro que $B/\mathfrak{P}$ está contenido en la clausura entera de $A/\mathfrak{p}$ en $k(\mathfrak{P})$, luego, por hipótesis, $B/\mathfrak{P}$ es un $A/\mathfrak{p}$-módulo finitamente generado. Así, la serie

$$0 = \mathfrak{P}^e/\mathfrak{P}^e \subset \mathfrak{P}^{e-1}/\mathfrak{P}^e \subset \cdots \subset \mathfrak{P}/\mathfrak{P}^e \subset B/\mathfrak{P}^e$$

muestra que $B/\mathfrak{P}^e = B/\mathfrak{p}B$ también es un $A/\mathfrak{p}$-módulo finitamente generado, ya que todos los factores $\mathfrak{P}^i/\mathfrak{P}^{i+1} \cong B/\mathfrak{P}$ son finitamente generados.

Por otra parte, de la relación $\mathfrak{p}B = \mathfrak{P}^e$ se sigue que la topología $\mathfrak{p}$-ádica en B es la misma que la topología $\mathfrak{P}$-ádica. Sólo nos falta probar que es de Hausdorff. Ahora bien, es claro que $y^n B_\mathfrak{P} \cap B = y^n B$, luego

$$\bigcap_{n\geq 1} \mathfrak{P}^n = \bigcap_{n\geq 1} y^n B \subset \bigcap_{n\geq 1} y^n B_\mathfrak{P} = 0,$$

puesto que $B_\mathfrak{P}$ es un anillo local y su topología $\mathfrak{P}$-ádica es de Hausdorff. ∎

Teorema 3.18 (Nagata) *Todo anillo noetheriano local y completo es un anillo de Nagata.*

Demostración: Sea A un anillo noetheriano local y completo. Si $\mathfrak{p}$ es un ideal primo, entonces $A/\mathfrak{p}$ también es un anillo noetheriano local y completo, luego basta probar que todo dominio íntegro noetheriano local y completo tiene la propiedad N_2.

Por el teorema 2.21, tenemos que A contiene un subanillo noetheriano regular y completo A' tal que A es un A'-módulo finitamente generado, luego podemos suponer que A es regular. (Notemos que A es entero sobre A', por lo que la clausura entera de A en una extensión finita de su cuerpo de cocientes coincide con la clausura entera de A'.) Más concretamente, según la observación posterior al teorema, podemos suponer que $A = A_0[[X_1, \ldots, X_n]]$, donde A_0 es un cuerpo o bien un anillo de valoración discreta completo. Probaremos el teorema por inducción sobre n.

Si $n = 0$, entonces $A = A_0$. Si es un cuerpo, entonces tiene trivialmente la propiedad N_2. Si es un anillo de valoración discreta, aplicamos el teorema

anterior tomando como $\mathfrak{p}$ su ideal maximal. Tenemos que $A/\mathfrak{p}$ es un cuerpo, luego cumple N_2, y concluimos que A también cumple N_2.

Si el resultado es cierto para $n-1$, aplicamos el teorema anterior al ideal primo $\mathfrak{p} = (X_n)$. Así $A/\mathfrak{p} \cong A_0[[X_1, \dots, X_{n-1}]]$ tiene la propiedad N_2 por hipótesis de inducción y $A = A_0[[X_1, \dots, X_{n-1}]][[X_n]]$ es completo con la topología $\mathfrak{p}$-ádica, luego A cumple la propiedad N_2. ∎

Ahora necesitamos estudiar una propiedad intermedia entre la propiedad de Nagata y la propiedad N_1 para anillos locales. Por razones técnicas conviene definirla para anillos semilocales:

Definición 3.19 Diremos que un anillo semilocal A es *analíticamente no ramificado* si su compleción $\hat{A}$ es reducida. Un ideal primo $\mathfrak{p}$ de A es *analíticamente no ramificado* si la compleción $\widehat{A/\mathfrak{p}} = (A/\mathfrak{p}) \otimes_A \hat{A} = \hat{A}/\mathfrak{p}\hat{A}$ es reducida.

Teorema 3.20 *Todo dominio íntegro noetheriano local analíticamente no ramificado tiene la propiedad N_1.*

Demostración: Sea A un dominio íntegro noetheriano local analíticamente no ramificado y sean $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ los primos minimales de $\hat{A}$. El teorema 1.13 nos da que el anillo completo de cocientes de $\hat{A}$ es $C = K_1 \oplus \cdots \oplus K_r$, donde K_i es el cuerpo de cocientes de $\hat{A}/\mathfrak{P}_i$. Es claro entonces que la clausura entera de $\hat{A}$ en C es la suma directa de las clausuras enteras de cada $\hat{A}/\mathfrak{P}_i$ en K_i. Como $\hat{A}/\mathfrak{P}_i$ es un dominio íntegro local y completo, es un anillo de Nagata, y en particular tiene la propiedad N_1, luego su clausura entera es finitamente generada. Así pues, podemos concluir que la clausura entera de $\hat{A}$ en C es un $\hat{A}$-módulo finitamente generado.

Sea K el cuerpo de cocientes de A y B la clausura entera de A en K. Como $\hat{A}$ es plano sobre A, tenemos que $B \otimes_A \hat{A} \subset K \otimes_A \hat{A} \subset C$, y todos los elementos de $B \otimes_A \hat{A}$ son enteros sobre $\hat{A}$, luego $B \otimes_A \hat{A}$ puede considerarse como submódulo de la clausura entera de $\hat{A}$ en C, luego es un $\hat{A}$-módulo finitamente generado.

Sean $b_1, \dots, b_n \in B$ un generador de $B \otimes_A \hat{A}$ sobre $\hat{A}$ y sea $B' = \langle b_1, \dots, b_n \rangle_A$. Entonces $(B/B') \otimes_A \hat{A} = 0$ y, como $\hat{A}$ es fielmente plano sobre A, esto implica que $B = B'$, es decir, que B es un A-módulo finitamente generado. ∎

El teorema siguiente nos permitirá probar que los dominios íntegros locales de Nagata son analíticamente no ramificados:

Teorema 3.21 *Sea A un dominio íntegro noetheriano semilocal y sea $x \in A$ un elemento no nulo que pertenezca a todos los ideales maximales. Supongamos además que todos los primos asociados de A/xA son minimales y (como primos de A) son regulares y analíticamente no ramificados. Entonces A es analíticamente no ramificado.*

Demostración: Sean $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ los primos minimales (o asociados) de A/xA. Por hipótesis, $\hat{A}/\mathfrak{p}_i\hat{A}$ es reducido, luego sus primos asociados son también minimales y, si los llamamos $\mathfrak{P}_{i,1}, \dots, \mathfrak{P}_{i,n_i}$, se cumple que

$$\mathfrak{p}_i\hat{A} = \bigcap_j \mathfrak{P}_{i,j}.$$

Por el teorema de los ideales principales [AC 5.2], los primos $\mathfrak{p}_i$ tienen altura 1, luego los anillos $A_{\mathfrak{p}_i}$ son anillos locales regulares y de dimensión 1. En particular son dominios de Dedekind locales, es decir, anillos de valoración discreta.[2] Sea $\pi_i \in A$ tal que $\mathfrak{p}_i A_{\mathfrak{p}_i} = \pi_i A_{\mathfrak{p}_i}$. Entonces $\mathfrak{P}_{ij}\hat{A}_{\mathfrak{P}_{ij}}$ es el único primo minimal de $\mathfrak{p}_i\hat{A}_{\mathfrak{P}_{ij}}$, luego $\mathfrak{P}_{ij}\hat{A}_{\mathfrak{P}_{ij}} = \mathfrak{p}_i\hat{A}_{\mathfrak{P}_{ij}} = \pi_i\hat{A}_{\mathfrak{P}_{ij}}$.

Como $\hat{A}_{\mathfrak{P}_{ij}}$ es plano sobre $\hat{A}$ y $\hat{A}$ es plano sobre A, resulta que π no es un divisor de cero en $\hat{A}_{\mathfrak{P}_{ij}}$ (la multiplicación por π es inyectiva y sigue siéndolo tras el cambio de base). De nuevo por el teorema de los ideales principales, concluimos que $\hat{A}_{\mathfrak{P}_{ij}}$ tiene dimensión 1, luego es regular. En particular es un dominio íntegro, por lo que si llamamos $\mathfrak{Q}_{ij}$ al núcleo del homomorfismo natural $\hat{A} \longrightarrow \hat{A}_{\mathfrak{P}_{ij}}$, vemos que se trata de un ideal primo. Para probar que $\hat{A}$ es reducido basta ver que $N = \bigcap_{i,j} \mathfrak{Q}_{ij} = 0$.

La fórmula del teorema 1.9 (ver también las observaciones posteriores) nos da que

$$\mathrm{As}(\hat{A}/x\hat{A}) = \bigcup_{\mathfrak{p}\in \mathrm{As}(A)} \mathrm{As}_{\hat{A}}(\hat{A}/\mathfrak{p}\hat{A}),$$

es decir, que los primos asociados de $\hat{A}/x\hat{A}$ son exactamente los $\mathfrak{P}_{ij}$. Tomando una descomposición primaria de 0 en este anillo, podemos expresar

$$x\hat{A} = \bigcap_{i,j} I_{ij},$$

donde cada I_{ij} es un ideal $\mathfrak{P}_{ij}$-primario. Según el teorema 1.5, tenemos que $I_{ij} = \hat{A} \cap \hat{A}_{\mathfrak{P}_{ij}}$, luego $\mathfrak{Q}_{ij} \subset I_{ij}$, luego $N \subset x\hat{A}$. Por otra parte, x no es un divisor de cero en A (porque es un dominio íntegro), luego tampoco lo es de $\hat{A}$, luego no pertenece a ningún $\mathfrak{Q}_{ij}$. Por consiguiente, si $n \in N$, será de la forma $n = xa$, luego $xa \in \mathfrak{Q}_{ij}$, luego $a \in \mathfrak{Q}_{ij}$, luego $a \in N$. Así pues, $N = xN$. El lema de Nakayama [AC 4.51] implica que $N = 0$. (Aquí usamos la hipótesis de que x pertenece a todos los ideales maximales de A, luego también a todos los de $\hat{A}$.) ∎

Teorema 3.22 *Todo dominio íntegro semilocal que sea un anillo de Nagata es analíticamente no ramificado.*

Demostración: Sea A un anillo que cumpla las hipótesis. Razonaremos por inducción sobre $\dim A$. Si $\dim A = 0$ entonces A es un cuerpo y el teorema es trivial.

Sea B la clausura entera de A en su cuerpo de cocientes. Por hipótesis, B es un A-módulo finitamente generado, luego también es un anillo de Nagata. Sea I la intersección de los ideales maximales de A y J la intersección de los ideales maximales de B. Observemos que si $\mathfrak{P}$ es un ideal primo de B tal que $IB \subset \mathfrak{P}$, entonces $I \subset \mathfrak{P} \cap A$, luego $\mathfrak{P} \cap A$ ha de ser uno de los ideales maximales de A, luego $\mathfrak{P}$ ha de ser uno de los ideales maximales de B (por [AC 3.63]). Así pues,

[2] Para más detalles sobre los dominios de Dedekind ver el principio de la sección 5.1

$J = \operatorname{rad} IB$, luego existe un $n \geq 1$ tal que $J^n \subset IB \subset J$. Esto implica que la topología I-ádica en B coincide con la J-ádica, luego podemos considerar a $\hat{A}$ como subanillo de $\hat{B}$.

Si probamos que $\hat{B}$ es reducido, también lo será $\hat{A}$. Equivalentemente, no perdemos generalidad si suponemos que A es íntegramente cerrado. Notemos también que, según [AC 3.68], $\dim B = \dim A$, luego al cambiar A por B mantenemos la hipótesis de inducción, según la cual el teorema es cierto para anillos de dimensión menor que la de A.

Notemos que $I \neq 0$ (o de lo contrario $\dim A = 0$), por lo que podemos tomar un $x \in I$ no nulo. Basta probar que cumple las hipótesis del teorema anterior. Por el teorema 1.18, tenemos que A cumple la propiedad S_2, luego los primos asociados de A/xA son minimales. Además, tienen altura 1 por el teorema de los ideales principales [AC 5.2], luego la propiedad R_1 nos da que son regulares. Por último, si $\mathfrak{p}$ es uno de ellos, tenemos que $A/\mathfrak{p}$ es un dominio íntegro semilocal de Nagata tal que $\dim(A/\mathfrak{p}) < \dim A$, luego $\mathfrak{p}$ es analíticamente no ramificado por hipótesis de inducción. ∎

Veamos un último resultado técnico que necesitamos para probar el resultado principal sobre los anillos de Nagata:

Teorema 3.23 *Sea A un dominio íntegro noetheriano y K su cuerpo de cocientes. Supongamos que existe un $f \in A$ no nulo tal que A_f es íntegramente cerrado y que $A_\mathfrak{p}$ tiene la propiedad N_1 para todo ideal maximal $\mathfrak{p}$ de A. Entonces A tiene también la propiedad N_1.*

Demostración: Representaremos con el signo $'$ las clausuras enteras. Si $\mathfrak{p}$ es un ideal maximal, tenemos que $(A_\mathfrak{p})' = A'_\mathfrak{p}$ es un $A_\mathfrak{p}$-módulo finitamente generado. Sea $\omega_1, \ldots, \omega_n \in A'$ un sistema generador. Llamemos $C^\mathfrak{p} = A[\omega_1, \ldots, \omega_n]$, que es un A-módulo finitamente generado (ya que los ω_i son enteros sobre A), luego es noetheriano.

Llamemos $X = \operatorname{Esp} A$ y $X^\mathfrak{p} = \operatorname{Esp} C^\mathfrak{p}$. Notemos que $(C^\mathfrak{p})_f = A_f$ es íntegramente cerrado, luego el teorema 1.19 nos da que el conjunto $F_\mathfrak{p} \subset X^\mathfrak{p}$ formado por los puntos que no son normales es cerrado en $X^\mathfrak{p}$. Como el homomorfismo $\pi_\mathfrak{p} : X^\mathfrak{p} \longrightarrow X$ es finito, se cumple que $\pi_\mathfrak{p}[F_\mathfrak{p}]$ es cerrado en X.

Veamos ahora que $\mathfrak{p} \notin \pi_\mathfrak{p}[F_\mathfrak{p}]$. En efecto, si $\mathfrak{P} \in X^\mathfrak{p}$ cumple que $\mathfrak{P} \cap A = \mathfrak{p}$, entonces $C^\mathfrak{p} \subset (C^\mathfrak{p})_\mathfrak{p} \subset (C^\mathfrak{p})_\mathfrak{P}$ y $(C^\mathfrak{p})_\mathfrak{p} = (A_\mathfrak{p})'$ es íntegramente cerrado. Por consiguiente, $(C^\mathfrak{p})_\mathfrak{P}$ es una localización de un anillo íntegramente cerrado, luego es también íntegramente cerrado, y así $\mathfrak{P} \notin F_\mathfrak{p}$. Por consiguiente, el conjunto

$$F = \bigcap_\mathfrak{p} \pi_\mathfrak{p}[F_\mathfrak{p}],$$

donde $\mathfrak{p}$ recorre los ideales maximales de A, es un cerrado en X que no contiene a ningún punto cerrado. Por [E 3.1] ha de ser $F = \varnothing$. Aquí hemos usado que F es cuasicompacto por ser cerrado en X, que es cuasicompacto por ser afín. La cuasicompacidad de X nos da también que existe un número finito de ideales maximales $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ tales que

$$\bigcap_{i=1}^n \pi_{\mathfrak{p}_i}[F_{\mathfrak{p}_i}] = \varnothing.$$

Sea $C = A[C^{\mathfrak{p}_1}, \ldots, C^{\mathfrak{p}_n}]$, que es un A-módulo finitamente generado. Vamos a ver que $C_{\mathfrak{Q}}$ es íntegramente cerrado, para todo $\mathfrak{Q} \in \operatorname{Esp} C$. Esto se debe a que $\mathfrak{Q} \cap A \notin \pi_{\mathfrak{p}_i}[F_{\mathfrak{p}_i}]$ para algún i, luego $\mathfrak{q} = \mathfrak{Q} \cap C^{\mathfrak{p}_i}$ es normal en $X_{\mathfrak{p}_i}$, es decir, que $(C^{\mathfrak{p}_i})_{\mathfrak{q}}$ es íntegramente cerrado, y $A \subset (C^{\mathfrak{p}_i})_{\mathfrak{q}} \subset C_{\mathfrak{Q}}$. Como C es entero sobre A, ha de ser $C \subset (C^{\mathfrak{p}_i})_{\mathfrak{q}} \subset C_{\mathfrak{Q}}$, luego $C_{\mathfrak{Q}} = (C^{\mathfrak{p}_i})_{\mathfrak{q}}$ es íntegramente cerrado.

Así pues, el esquema $\operatorname{Esp} C$ es normal, luego C es íntegramente cerrado, luego $A' = C$ es un A-módulo finitamente generado. ∎

Finalmente podemos probar:

Teorema 3.24 (Nagata) *Si A es un anillo de Nagata y B es una A-álgebra finitamente generada, entonces B es también un anillo de Nagata.*

Demostración: Es obvio que todo cociente de un anillo de Nagata es también un anillo de Nagata, luego podemos cambiar A por su imagen en B y suponer que $A \subset B$. Entonces $B = A[x_1, \ldots, x_n]$, para ciertos $x_i \in B$. Razonando inductivamente, basta considerar el caso en que $B = A[x]$.

Consideremos un primo $\mathfrak{P} \in \operatorname{Esp} B$ y llamemos $\mathfrak{p} = A \cap \mathfrak{p}$. Entonces, es claro que $B/\mathfrak{P} = (A/\mathfrak{p})[\bar{x}]$, donde $A/\mathfrak{p}$ es un dominio íntegro de Nagata y lo que tenemos que probar es que $B/\mathfrak{P}$ tiene la propiedad N_2. En definitiva, hemos de probar lo siguiente:

> *Si $B = A[x]$ es un dominio íntegro y A es un anillo de Nagata, entonces B tiene la propiedad N_2.*

Sea K el cuerpo de cocientes de A y sea $\overline{A}$ la clausura entera de A en K, que es un A-módulo finitamente generado. Sea $\overline{B}$ la adjunción a B de un generador de $\overline{A}$ sobre A, de modo que $\overline{B} = \overline{A}[x]$. Es fácil ver que $\overline{A}$ también es un anillo de Nagata. (En general, es fácil ver que toda álgebra finita sobre un anillo de Nagata es un anillo de Nagata.) Como $\overline{B}$ es una extensión entera de $\overline{B}$, la clausura entera de $\overline{B}$ en cualquier extensión finita del cuerpo de cocientes de B es la misma que la de B, por lo que basta probar que $\overline{B}$ tiene la propiedad N_2. En definitiva, podemos reemplazar A por $\overline{A}$ y suponer que A es íntegramente cerrado.

Supongamos en primer lugar que x es trascendente sobre K, con lo que B es también íntegramente cerrado por 1.14. Si B tiene característica 0, entonces basta probar que tiene la propiedad N_1 por el teorema 3.15, lo cual es trivial.

Si B tiene característica prima p, basta considerar una extensión finita puramente inseparable $L = K(x, \alpha_1, \ldots, \alpha_n)$ de $K(x)$. Sea $m = p^e$ tal que $\alpha_i^m \in K(x)$ para todo i. Es claro que existe una extensión finita puramente inseparable K'/K tal que $\alpha_i \in K'(x^{1/m})$. Sea $\overline{A}$ la clausura entera de A en K' y $\overline{B}$ la clausura entera de B en L. Así $\overline{A}[x^{1/m}]$ es íntegramente cerrado por el teorema 1.14, luego $B = A[x] \subset \overline{B} \subset \overline{A}[x^{1/m}]$. Como A tiene la propiedad N_2, tenemos que $\overline{A}$ es un A-módulo finitamente generado, luego $\overline{A}[x^{1/m}]$ es un B-módulo finitamente generado, luego $\overline{B}$ también lo es.

A partir de aquí podemos suponer que x es algebraico sobre K, con lo que el cuerpo de cocientes de B es una extensión finita de K. Si L es, a su vez, una

extensión finita de dicho cuerpo de cocientes, también es finita la extensión L/K. Como antes, llamamos $\overline{A}$ y $\overline{B}$ a las clausuras enteras de A y B en L. Sabemos que $\overline{A}$ es un A-módulo finitamente generado, luego $\overline{A}[x]$ es un B-módulo finitamente generado, lo que a su vez implica que $B = A[x] \subset \overline{A}[x] \subset \overline{B}$.

Basta probar que $\overline{B}$ es finitamente generado sobre $\overline{A}[x]$. Ahora bien, $\overline{A}$ es un anillo de Nagata porque es un A-módulo finitamente generado y A es un anillo de Nagata, luego podemos cambiar A por $\overline{A}$ y B por $\overline{A}[x]$ (y K por L), con lo que todo se reduce a probar lo siguiente:

> *Si A es un dominio íntegro de Nagata íntegramente cerrado, K es su cuerpo de cocientes y $x \in K$, entonces el anillo $B = A[x]$ tiene la propiedad N_1.*

Sea $x = b/a$, con $a, b \in A$. Entonces $B_a = B[1/a] = A[1/a]$ es íntegramente cerrado, ya que es una localización de A. Por el teorema 3.23 basta probar que $B_{\mathfrak{P}}$ tiene la propiedad N_1 para todo ideal maximal $\mathfrak{P}$ de B.

Llamemos $\mathfrak{p} = \mathfrak{P} \cap A$. Como $B/\mathfrak{P} = (A/\mathfrak{p})[\bar{x}]$ es un cuerpo, $\bar{x}$ es algebraico sobre (el cuerpo de cocientes de) $A/\mathfrak{p}$, luego existe un polinomio $f(X) \in A[X]$ tal que $f(x) \in \mathfrak{P}$. Podemos suponer que el coeficiente director c de $f(X)$ cumple $c \notin \mathfrak{p}$. Entonces $B_{\mathfrak{P}} = (B_c)_{\mathfrak{P}_c}$, y los anillos A_c y B_c cumplen las mismas hipótesis que A y B. Así pues, no perdemos generalidad si suponemos que c es una unidad de A o, equivalentemente, que $f(X)$ es mónico.

Sea K' la adjunción a K de las raíces de $f(X)$, sea A' la clausura entera de A en K' (que contiene a dichas raíces) y sea $B' = A'[x]$.

Como A es un anillo de Nagata, tenemos que A' es un A-módulo finitamente generado, luego A' es un dominio íntegro de Nagata íntegramente cerrado y B' es un B-módulo finitamente generado. Sea $\mathfrak{P}'$ cualquier ideal maximal de B' tal que $\mathfrak{P}' \cap B = \mathfrak{P}$ (existe por [AC 3.63]). Si $B'_{\mathfrak{P}'}$ tiene la propiedad N_1 para todo $\mathfrak{P}'$, lo mismo le sucede a $B'_{\mathfrak{P}}$ por 3.23 (notemos que $(B'_{\mathfrak{P}})_a$ es una localización de $B'_A = A'_a$, luego es íntegramente cerrado). A su vez, si $B'_{\mathfrak{P}}$ es N_1, lo mismo le sucede a $B_{\mathfrak{P}}$, ya que la clausura entera de $B_{\mathfrak{P}}$ está contenida en la de $B'_{\mathfrak{P}}$, que es finitamente generada sobre $B'_{\mathfrak{P}}$ y éste es finitamente generado sobre $B_{\mathfrak{P}}$.

En resumen, podemos cambiar A por A', etc., por lo que podemos suponer que $f(X)$ tiene todas sus raíces en K (luego, de hecho, en A) y, en particular, que $x \equiv c \pmod{\mathfrak{P}}$, donde c es una de dichas raíces. Como B no se altera si cambiamos x por $x - c$, podemos suponer que $x \in \mathfrak{P}$.

Sea Q el núcleo del homomorfismo $A[X] \longrightarrow A[x] = B$ dado por $X \mapsto x$. Vamos a probar que Q está generado por los polinomios $aX - b$ tales que $x = b/a$. En efecto, si $F(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in Q$, entonces $b = a_0x$ es entero sobre A, luego $b \in A$ porque A es íntegramente cerrado. Consecuentemente, $F(X) - (a_0X - b)X^{n-1} \in Q$, y basta razonar por inducción sobre el grado de F.

Sea I el ideal generado por todos los $b \in A$ tales que $x = b/a$, es decir, $I = xA \cap A$. Es claro entonces que $XA[X] + Q = XA[X] + I$, luego

$$B/xB \cong A[X]/(XA[X] + Q) = A[X]/(XA[X] + I) \cong A/I.$$

Vamos a aplicar el teorema 3.21 al anillo $B_{\mathfrak{P}}$, lo que nos dará que es analíticamente no ramificado y, por 3.20 tendrá la propiedad N_1, tal y como queremos probar. Hemos de ver que los primos asociados de $B_{\mathfrak{P}}/xB_{\mathfrak{P}}$ son minimales y que, como primos de $B_{\mathfrak{P}}$, son regulares y analíticamente no ramificados.

Por [E 7.4], sabemos que $A = \bigcap_{\mathfrak{q}} A_{\mathfrak{q}}$, donde $\mathfrak{q}$ recorre los ideales primos de altura 1. Es claro entonces que $xA = \bigcap_{\mathfrak{q}} xA_{\mathfrak{q}}$, luego $I = xA \cap A = \bigcap_{\mathfrak{q}}(xA_{\mathfrak{q}} \cap A)$.

Ahora bien, si $x \notin \mathfrak{q}A_{\mathfrak{q}}$, entonces $xA_{\mathfrak{q}} = A_{\mathfrak{q}}$ y $xA_{\mathfrak{q}} \cap A = A$, luego en realidad

$$I = \bigcap_{i=1}^{s} (xA_{\mathfrak{q}_i} \cap A),$$

donde $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ son los primos de altura 1 tales que $x \in \mathfrak{q}_i A_{\mathfrak{q}_i}$.

Los primos asociados de $B_{\mathfrak{P}}/xB_{\mathfrak{P}} = (B/xB)_{\mathfrak{P}} \cong (A/I)_{\mathfrak{P}}$ son parte de los primos asociados de A/I. Vamos a ver que todos ellos son minimales. Si $I \subset \mathfrak{q} \subset A$ es un primo asociado de A/I y $u \in \mathfrak{q}$, entonces u es un divisor de cero de A/I, luego existe un $v \in A \setminus I$ tal que $uv \in I$. Existe un i tal que $v \notin xA_{\mathfrak{q}_i}$, pero $uv \in xA_{\mathfrak{q}_i}$, luego u es un divisor de cero de $A_{\mathfrak{q}_i}/xA_{\mathfrak{q}_i}$. En particular, u no es una unidad, luego $u \in \mathfrak{q}_i A_{\mathfrak{q}_i} \cap A = \mathfrak{q}_i$.

Con esto hemos probado que $\mathfrak{q} \subset \mathfrak{q}_1 \cup \cdots \cup \mathfrak{q}_s$ y, por [AC 3.51], de hecho $\mathfrak{q} \subset \mathfrak{q}_i$ para un i. Como $\mathfrak{q}_i$ tiene altura 1 y (salvo en el caso trivial $x = 0$) se cumple que $I \neq 0$, ha de ser $\mathfrak{q} = \mathfrak{q}_i$, un primo minimal de I.

Consideremos ahora un primo minimal $\mathfrak{p}$ de $B_{\mathfrak{P}}/xB_{\mathfrak{P}}$. Hemos de probar que $(B_{\mathfrak{P}})_{\mathfrak{p}} = B_{\mathfrak{p}'}$ es regular, donde $\mathfrak{p}' = \mathfrak{p} \cap B$. Tenemos que $\mathfrak{p}'$ es un primo minimal de B/xB, que se corresponde con un primo minimal de A/I, concretamente con $\mathfrak{q} = \mathfrak{p}' \cap A$. El primo $\mathfrak{q}$ es uno de los $\mathfrak{q}_i$ que hemos considerado antes, luego $x \in \mathfrak{q}A_{\mathfrak{q}}$, de donde se sigue inmediatamente que $B_{\mathfrak{p}'} = A_{\mathfrak{q}}$. Ahora basta tener en cuenta que $A_{\mathfrak{q}}$ es regular porque A es íntegramente cerrado y $\mathfrak{q}$ tiene altura 1. (Es la propiedad R_1 del teorema 1.18.)

Finalmente, $B_{\mathfrak{P}}/\mathfrak{p} = (B/\mathfrak{p}')_{\mathfrak{P}}$ y $B/\mathfrak{p}' \cong A/\mathfrak{q}$. El cociente $A/\mathfrak{q}$ es obviamente un anillo de Nagata y, por 3.13, también lo es $B_{\mathfrak{P}}/\mathfrak{p}$, luego por 3.22 es analíticamente no ramificado. ∎

3.3 Las propiedades J

Las propiedades de esta sección tienen que ver con la existencia de puntos regulares en un esquema (o de ideales primos con localización regular en un anillo). Empezamos demostrando un resultado que usaremos en varias ocasiones:

Teorema 3.25 *Sea $\phi : A \longrightarrow B$ un homomorfismo plano entre anillos locales. Si B es regular, entonces A también lo es.*

Demostración: Si k es el cuerpo de restos de A, se cumple que

$$\mathrm{Tor}_q^A(k,k) \otimes_A B \cong \mathrm{Tor}_q^B(k \otimes_A B, k \otimes_A B).$$

En efecto, si partimos de una resolución libre de k, digamos:

$$\cdots \longrightarrow L_1 \longrightarrow L_0 \longrightarrow k \longrightarrow 0,$$

entonces

$$\cdots \longrightarrow L_1 \otimes_A B \longrightarrow L_0 \otimes_A B \longrightarrow k \otimes_A B \longrightarrow 0$$

es una resolución libre de $k \otimes_A B$. Teniendo en cuenta que

$$(L_i \otimes_A B) \otimes_B (k \otimes_A B) \cong L_i \otimes_A (k \otimes_A B),$$

resulta que los B-módulos $\mathrm{Tor}_q^B(k \otimes_A B, k \otimes_A B)$ son los grupos de cohomología del complejo

$$\cdots \longrightarrow (L_{i+1} \otimes_A k) \otimes_A B \longrightarrow (L_i \otimes_A k) \otimes_A B \longrightarrow \cdots$$

y el teorema [AC 1.37] nos da el isomorfismo indicado. Según los teoremas [AC 5.55] y [AC 5.51], concluimos que $\mathrm{Tor}_q^A(k,k) \otimes_A B = 0$ para $q > \dim B$. Como B es fielmente plano sobre A, concluimos que $\mathrm{Tor}_q^A(k,k) = 0$, luego, según [AC 5.51] resulta que $\mathrm{dp}\, k \leq \dim B$ y [AC 5.61] nos permite concluir que A es regular. ∎

Si X es un esquema, representaremos por $\mathrm{Reg}\, X$ el conjunto de los puntos regulares de X. Vamos a enunciar unas condiciones técnicas para que $\mathrm{Reg}\, X$ sea abierto en X.

Teorema 3.26 *Sea A un anillo noetheriano y $X = \mathrm{Esp}\, A$. Para que el conjunto de puntos regulares de X sea abierto*

a) es necesario y suficiente que, para cada punto $\mathfrak{p} \in \mathrm{Reg}\, X$, el conjunto $\mathrm{Reg}\, X$ contenga un abierto no vacío de $V(\mathfrak{p})$.

b) es suficiente que, para cada punto $\mathfrak{p} \in \mathrm{Reg}\, X$, el conjunto $\mathrm{Reg}\, V(\mathfrak{p})$ contenga un abierto no vacío.

Demostración: a) es el teorema [AC A19], ya que la primera propiedad de dicho teorema es trivial en este contexto, pues las localizaciones de anillos regulares son regulares. Basta probar que b) ⇒ a).

Sea $\mathfrak{p} \in \mathrm{Reg}\, X$ y sea $a_1, \ldots, a_r \in \mathfrak{p}$ un sistema regular de parámetros de $A_\mathfrak{p}$. Sea $I = (a_1, \ldots, a_r)$ Como $IA_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$, existe un $f \in A \setminus \mathfrak{p}$ tal que $IA_f = \mathfrak{p}A_f$.

Tenemos que $U = D(f)$ es un entorno de $\mathfrak{p}$. Como $V(\mathfrak{p}) = \mathrm{Esp}(A/\mathfrak{p})$ es un esquema íntegro, el abierto $U \cap V(\mathfrak{p})$ cortará al abierto no vacío de puntos regulares que existe por hipótesis y, por otra parte, basta probar que U contiene un abierto no vacío de $U \cap V(\mathfrak{p})$. Así pues, podemos sustituir A por A_f, lo que equivale a suponer que $I = \mathfrak{p}$.

Basta probar que si $\mathfrak{q} \in \mathrm{Reg}(V(\mathfrak{p}))$, entonces $\mathfrak{q} \in \mathrm{Reg}\, X$. Tenemos que el anillo $(A/\mathfrak{p})_\mathfrak{q} = A_\mathfrak{q}/\mathfrak{p}A_\mathfrak{q}$ es regular, es decir, que $\mathfrak{q}A_\mathfrak{q}/\mathfrak{p}A_\mathfrak{q}$ admite un generador con $d = \dim(A_\mathfrak{q}/\mathfrak{p}A_\mathfrak{q})$ elementos.

Por otra parte, $\mathfrak{p}A_\mathfrak{q}$ está generado por una sucesión regular (en $A_\mathfrak{p}$, luego también en $A_\mathfrak{q}$) de r elementos, luego $\dim A_\mathfrak{q} = d + r$. Puesto que, obviamente, $\mathfrak{q}A_\mathfrak{q}$ admite un generador con $d + r$ elementos, concluimos que $A_\mathfrak{q}$ es regular. ∎

Ahora conviene introducir algunos nombres:

Definición 3.27 Sea A un anillo noetheriano. Diremos que A cumple la propiedad J_0 si $\operatorname{Esp} A$ contiene un abierto no vacío de puntos regulares, y diremos que cumple la propiedad J_1 si el conjunto de puntos regulares en $\operatorname{Esp} A$ es abierto (tal vez vacío).

Notemos que si A es un dominio íntegro, entonces el ideal nulo es siempre regular en $\operatorname{Esp} A$, luego todo dominio íntegro J_1 es también J_0.

En realidad, la propiedad que nos va a interesar es la propiedad J_2 que introduciremos enseguida, pero antes conviene demostrar un par de teoremas técnicos:

Teorema 3.28 *Sean $A \subset B$ dominios íntegros y $K \subset K'$ sus cuerpos de cocientes. Supongamos que B es un A-módulo finitamente generado, que A es regular y que la extensión K'/K es separablemente generada. Entonces B tiene la propiedad J_0.*

Demostración: Sea $t_1, \ldots, t_n \in B$ una base de trascendencia de K' sobre K tal que K' es separable sobre $K_1 = K(t_1, \ldots, t_n)$. Como A es regular, también lo es $A_1 = A[t_1, \ldots, t_n]$, luego podemos cambiar A por A_1 y suponer que la extensión K'/K es finita separable. Sea $\omega_1, \ldots, \omega_r \in B$ una K-base de K', que podemos suponer entera sobre A. Como B está finitamente generada sobre A, existe un $s \in A$ no nulo tal que todos los elementos de B tienen coordenadas en A_s. Más aún, todos los elementos de B_s tendrán coordenadas en A_s y, como $A_s \subset B_s$, el recíproco es obvio. Por lo tanto, cambiando A y B por A_s y B_s, podemos suponer que B es un A-módulo libre y, en particular, plano.

Si demostramos que la fibra genérica del homomorfismo $\operatorname{Esp} B \longrightarrow \operatorname{Esp} A$ es suave, el teorema [E A34] nos da que $\operatorname{Esp} B$ contiene un abierto no vacío formado por puntos llanos, cuya imagen será abierta por 1.30 y, aplicando [E 7.50] a la restricción a este abierto, concluimos que $\operatorname{Esp} B$ contiene un abierto de puntos regulares, tal y como queremos demostrar.

La fibra genérica es $\operatorname{Esp}(B \otimes_A K)$, que es un conjunto algebraico finito, porque, al ser B un A-módulo finitamente generado, el homomorfismo es finito. Si $\overline{K}$ es la clausura algebraica de K, también será un conjunto algebraico finito el cambio de base $\operatorname{Esp}(B \otimes_A \overline{K})$, luego será regular si es reducido (pues en tal caso será una suma directa de cuerpos).

Como $\overline{K}$ es plano sobre K y éste a su vez lo es sobre A (por ser una localización), la inclusión $B \longrightarrow K'$ induce un monomorfismo $B \otimes_A \overline{K} \longrightarrow K' \otimes_A \overline{K}$. Basta probar, pues, que $K' \otimes_A \overline{K} = K' \otimes_K \overline{K}$ es reducido. Ahora bien, podemos

ver a $\operatorname{Esp} K'$ como un conjunto algebraico sobre K y basta aplicar [E 3.57], ya que la extensión K'/K es separable. ∎

Teorema 3.29 *Si K'/K es una extensión de cuerpos finitamente generada, existe una extensión finita puramente inseparable K_1/K tal que la extensión $K'K_1/K_1$ es separablemente generada.*

Demostración: Consideremos un generador finito $K' = K(S)$ y llamemos $B = K[S]$, de modo que K' es el cuerpo de cocientes de B. Sea $\overline{K}$ una clausura algebraica de K. Vamos a estudiar $B \otimes_K \overline{K}$. Llamemos R' a su radical.

Como el anillo es noetheriano, R' estará generado por un número finito de elementos, cada uno de los cuales será a su vez suma de un número finito de elementos de la forma $b \otimes \alpha$, con $b \in B$ y $\alpha \in \overline{K}$. Sea $R \subset B$ el ideal generado por los elementos b y K_0 una extensión finita de K que contenga a los elementos α. Podemos identificar a $B \otimes_K K_0$ con un subanillo de $B \otimes_K \overline{K}$. Los generadores de R' pueden verse también como elementos de $B \otimes_K K_0$ o, más concretamente, del ideal $R \otimes_K K_0$.

Es claro que $R \otimes_K K_0 = R' \cap (B \otimes_K K_0)$, y esto implica que $R \otimes_K K_0$ es el radical de $B \otimes_K K_0$. Por otra parte,

$$R' = R \otimes_K \overline{K} = (R \otimes_K K_0) \otimes_{K_0} \overline{K}, \quad B \otimes_K \overline{K} = (B \otimes_K K_0) \otimes_{K_0} \overline{K},$$

de donde

$$(B \otimes_K \overline{K})/R' \cong ((B \otimes_K K_0)/(R \otimes_K K_0)) \otimes_{K_0} \overline{K},$$

es decir, $(B \otimes_K \overline{K})_{red} \cong (B \otimes_K K_0)_{red} \otimes_{K_0} \overline{K}$. En términos de $X = \operatorname{Esp} B$, lo que hemos probado es que $(X_{K_0})_{red}$ es geométricamente reducido.

Llamemos ahora K_1 a la clausura puramente inseparable de K en K_0, de modo que tenemos extensiones finitas $K \subset K_1 \subset K_0$, donde la primera es puramente inseparable y la segunda es separable. Se cumple que

$$(X_{K_1})_{red} \otimes_{K_1} \operatorname{Esp} K_0 \cong (X_{K_0})_{red}.$$

En efecto, el esquema $\operatorname{Esp} K_0$ es un conjunto algebraico sobre K_1 geométricamente reducido por [E 3.64], luego el miembro izquierdo es reducido por [E 3.57]. Por otra parte, tenemos inmersiones cerradas naturales de ambos esquemas en X_{K_0}, y las dos son homeomorfismos, luego ambos esquemas son isomorfos a la única estructura de subesquema cerrado reducido de X_{K_0}. Esto implica que $(X_{K_1})_{red}$ también es geométricamente reducido. Tenemos inmersiones cerradas

$$(X_{K_1})_{red} \longrightarrow X_{K_1} \longrightarrow X.$$

La primera es ciertamente un homeomorfismo, y la segunda también, ya que K_1/K es puramente inseparable (de nuevo por [E 3.57]). Como X es íntegro, concluimos que $(X_{K_1})_{red}$ es irreducible, luego también es íntegro.

Llamamos ahora $B_1 = (B \otimes_K K_1)_{red}$, que, según acabamos de ver, es un dominio íntegro. Por el teorema [E 3.64], su cuerpo de fracciones, digamos K_1',

es separablemente generado sobre K_1. La inclusión $B \subset B \otimes_K K_1$ induce una inclusión $B \subset B_1$ que a su vez induce una inclusión $K' \subset K_1'$, luego también $K'K_1 \subset K_1'$. Por [E 3.64] aplicado a $\operatorname{Esp} K_1'$ tenemos que $K_1' \otimes_{K_1} \overline{K}$ es reducido, y la inclusión $K'K_1 \otimes_{K_1} \overline{K} \subset K_1' \otimes_{K_1} \overline{K}$ implica que $K'K_1 \otimes_{K_1} \overline{K}$ también lo es, luego, por el mismo teorema, la extensión $K'K_1/K_1'$ es separablemente generada. ∎

Diremos que A cumple la propiedad J_2 si satisface las propiedades del teorema siguiente:

Teorema 3.30 (Nagata) *Si A es un anillo noetheriano, las propiedades siguientes son equivalentes:*

a) Toda A-álgebra finitamente generada cumple la propiedad J_1.

b) Toda A-álgebra finita (como A-módulo) cumple la propiedad J_1.

c) Para todo $\mathfrak{p} \in \operatorname{Esp} A$ y toda extensión finita puramente inseparable K' de $k(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$, existe una A-álgebra finita A' tal que $A/\mathfrak{p} \subset A' \subset K'$, cuyo cuerpo de cocientes es K' y que cumple la propiedad J_0.

Demostración: Es obvio que a) ⇒ b), así como que b) ⇒ c), sin más que observar que $k(\mathfrak{p})$ es el cuerpo de cocientes de $A/\mathfrak{p}$, que $K' = k(\mathfrak{p})[\alpha_1, \ldots, \alpha_n]$, que los α_i se pueden tomar enteros sobre $k(\mathfrak{p})$ y así $A' = (A/\mathfrak{p})[\alpha_1, \ldots, \alpha_n]$ cumple lo pedido.

Veamos que c) ⇒ a). En primer lugar consideremos un primo $\mathfrak{p}$ una A-álgebra A' que cumplan c). Sea $\omega_1, \ldots, \omega_n \in A'$ una $k(\mathfrak{p})$-base de K'. Existe un $f \in A/\mathfrak{p}$ no nulo tal que $\omega_1, \ldots, \omega_n$ es una base de A'_f sobre $(A/\mathfrak{p})_f$. Así, A'_f es libre sobre $(A/\mathfrak{p})_f$ y, en particular, plano. Si $\mathfrak{Q}$ es un primo en A'_f y $\mathfrak{q} = \mathfrak{Q} \cap (A/\mathfrak{p})_f$, entonces $A'_\mathfrak{Q}$ es plano sobre $(A/\mathfrak{p})_\mathfrak{q}$, y el teorema 3.25 nos da que $(A/\mathfrak{p})_\mathfrak{q}$ es regular.

El homomorfismo $\operatorname{Esp} A'_f \longrightarrow \operatorname{Esp}(A/\mathfrak{p})_f$ es finito, luego es cerrado. Sabemos que el primer esquema contiene un abierto U formado por puntos regulares. Por 1.30 tenemos que su imagen es abierta en $\operatorname{Esp}(A/\mathfrak{p})_f$, luego también en $\operatorname{Esp}(A/\mathfrak{p})$, y acabamos de probar que dicha imagen está formada por puntos regulares. En definitiva, tenemos que $A/\mathfrak{p}$ cumple la propiedad J_0.

Más aún, hemos probado que para cada primo $\mathfrak{p} \in \operatorname{Esp} A$, el cerrado $V(\mathfrak{p})$ contiene un abierto no vacío formado por puntos regulares. Según el teorema 3.26 b), esto implica que A tiene la propiedad J_1, al igual que todos los anillos $A/\mathfrak{p}$ (aplicando el teorema a los primos que contienen a $\mathfrak{p}$).

También por dicho teorema, basta probar que si $\mathfrak{P}$ es un ideal primo de B, entonces el anillo $B/\mathfrak{P}$ tiene la propiedad J_0. Ahora bien, llamando $\mathfrak{p}$ a la antiimagen de $\mathfrak{p}$ en A, tenemos que $B/\mathfrak{P}$ es un dominio íntegro finitamente generado sobre $A/\mathfrak{p}$. Por lo tanto, basta probar lo siguiente:

Si B es un dominio íntegro que contiene a un anillo cociente $A/\mathfrak{p}$, para cierto $\mathfrak{p} \in \operatorname{Esp} A$, y es finitamente generado sobre $A/\mathfrak{p}$, entonces tiene la propiedad J_0.

Ahora bien, $A/\mathfrak{p}$ también cumple la propiedad c), luego en el enunciado anterior podemos cambiar $A/\mathfrak{p}$ por A y suponer que $A \subset B$ es un dominio íntegro. Más aún, hemos probado que $\operatorname{Esp} A$ contiene un abierto de puntos regulares, que podemos tomar principal, digamos de la forma $\operatorname{Esp} A_f$, para un $f \in A$. Entonces $A_f \subset B_f$ y, si probamos que B_f cumple J_0, lo mismo valdrá para A_f. Más aún, A_f también cumple la propiedad c), luego no perdemos generalidad si suponemos además que A es regular.

Así pues, tenemos una extensión de dominios íntegros $A \subset B$ que es finitamente generada, A es regular, cumple c) y queremos probar que B es J_0. Sean $K \subset K'$ los cuerpos de cocientes de A y B.

Por el teorema anterior existe una extensión finita puramente inseparable K_1/K tal que $K_1' = K'K_1$ es separablemente generado sobre K_1. La propiedad c) nos da que K_1 contiene una A-álgebra finita A_1 tal que $\operatorname{Esp} A_1$ contiene un abierto no vacío de puntos regulares.

Sea B_1' la imagen del homomorfismo $B \otimes_A A_1 \longrightarrow K_1'$. Entonces B_1' es una A_1-álgebra finitamente generada, una B-álgebra finita, un dominio íntegro y su cuerpo de fracciones es K_1'.

El teorema 3.28 aplicado a los anillos A_1 y B_1' nos da que $\operatorname{Esp} B_1'$ contiene un abierto no vacío de puntos regulares. El mismo razonamiento aplicado en la prueba de dicho teorema a los anillos A y B nos permite ahora sustituir B y B_1' por abiertos adecuados para que B_1' sea un B-módulo libre y, en particular, plano. (Notemos que, al ser B_1' un dominio íntegro, el abierto que tomamos corta necesariamente al abierto de puntos regulares, luego no perdemos esta propiedad.) El teorema 3.25 nos da que las imágenes de los puntos regulares de $\operatorname{Esp} B_1'$ por el homomorfismo $\operatorname{Esp} B_1' \longrightarrow \operatorname{Esp} B$ son regulares, y 1.30 nos da que $\operatorname{Esp} B$ contiene un abierto no vacío de puntos regulares. ∎

Veamos algunas propiedades elementales de los anillos J_2:

Teorema 3.31 *Sea A un anillo con la propiedad J_2. Entonces:*

a) A tiene la propiedad J_1, es decir, el conjunto de los puntos regulares de $\operatorname{Esp} A$ es abierto.

b) Toda A-álgebra finitamente generada tiene la propiedad J_2.

c) Toda localización de A tiene la propiedad J_2.

Demostración: a) y b) son consecuencias inmediatas de la propiedad a) del teorema anterior, mientras que c) es consecuencia de la propiedad c) del mismo teorema. En efecto, si $S \subset A$ es un conjunto multiplicativo, un primo de $S^{-1}A$ es de la forma $S^{-1}\mathfrak{p}$, donde $\mathfrak{p}$ es un primo de A disjunto con S. Entonces

$$S^{-1}A_{S^{-1}\mathfrak{p}} = A_{\mathfrak{p}}, \quad S^{-1}A/S^{-1}\mathfrak{p} = S^{-1}(A/\mathfrak{p}), \quad k(S^{-1}\mathfrak{p}) = k(\mathfrak{p}).$$

Si K' es una extensión puramente inseparable de $k(\mathfrak{p})$ y A' es la extensión de $A/\mathfrak{p}$ que cumple la propiedad c), entonces $S^{-1}A'$ es una extensión finita de

$S^{-1}A/S^{-1}\mathfrak{p}$ y $\operatorname{Esp} S^{-1}A'$ tiene un abierto no vacío de puntos regulares por el teorema 3.25, ya que el homomorfismo $\operatorname{Esp} S^{-1}A' \longrightarrow \operatorname{Esp} A'$ es plano. ∎

Para el próximo teorema necesitamos la siguiente observación elemental: Si A y B son dos anillos, entonces el esquema $X = \operatorname{Esp}(A \oplus B)$ es la unión disjunta de dos abiertos isomorfos a $\operatorname{Esp} A$ y $\operatorname{Esp} B$.

En efecto, basta observar que los cerrados $U_A = V(0 \oplus B)$ y $U_B = V(A \oplus 0)$ están formados por los ideales primos de $A \oplus B$ que contienen a $(0,1)$ y $(1,0)$, respectivamente. Como $(1,0) + (0,1)$ es la identidad de $A \oplus B$, vemos que $U_A \cap U_B = \varnothing$ y, como $(1,0)(0,1) = (0,0)$, resulta que $X = U_A \cup U_B$, luego U_A y U_B son también abiertos. Es claro que $U_A \cong \operatorname{Esp} A$ y $U_B \cong \operatorname{Esp} B$. ∎

Teorema 3.32 *Todo anillo noetheriano local y completo tiene la propiedad J_2.*

Demostración: Sea A un anillo noetheriano local y completo. Basta probar que toda A-álgebra finita B tiene la propiedad J_1. Tenemos un homomorfismo $A \longrightarrow B$. Cambiando A por el cociente sobre el núcleo, podemos suponer que B es una extensión de A. Por [AC 3.63 y 3.64] tenemos que B tiene un número finito de ideales maximales, $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. Si $\mathfrak{m}$ es el ideal maximal de A, su fibra es $\operatorname{Esp}(B/\mathfrak{m}B)$, luego $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ son los únicos ideales primos por encima de $\mathfrak{m}B$, luego $\mathfrak{m}' = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$ es el radical de $\mathfrak{m}B$. Por lo tanto, existe un $r \geq 1$ tal que $\mathfrak{m}'^r \subset \mathfrak{m}B$, luego la topología $\mathfrak{m}'$-ádica en B coincide con la topología $\mathfrak{m}$-ádica, que es completa.

Según hemos probado tras 1.12, se cumple que $B = \hat{B} = \hat{B}_1 \oplus \cdots \oplus \hat{B}_n$, donde $\hat{B}_i$ es la compleción de B respecto de la topología $\mathfrak{m}_i$-ádica. Por la observación previa a este teorema, $\operatorname{Esp} B$ es unión disjunta de abiertos isomorfos a $\operatorname{Esp} \hat{B}_i$, para $i = 1, \ldots, n$, luego B tiene la propiedad J_1 si y sólo si la tiene cada $\hat{B}_i$. En definitiva, basta probar que todo anillo noetheriano local y completo tiene la propiedad J_1.

Vamos a aplicar el criterio 3.26 b). Sea A un anillo noetheriano local y completo y consideremos un ideal primo $\mathfrak{p}$. Hemos de probar que $\operatorname{Esp}(A/\mathfrak{p})$ contiene un abierto no vacío de puntos regulares. Ahora bien, $A/\mathfrak{p}$ también es un anillo noetheriano local y completo, luego podemos suponer que A es un dominio íntegro y sólo hemos de probar que $\operatorname{Esp} A$ contiene un abierto no vacío de puntos regulares.

Por el teorema 2.21, sabemos que A es finito sobre una subálgebra regular A'. Si A tiene característica 0, la extensión de sus cuerpos de cocientes será separablemente generada, luego podemos aplicar el teorema 3.28 para concluir que $\operatorname{Esp} A$ tiene un abierto no vacío de puntos regulares.

Si A tiene característica prima, entonces es equicaracterístico, y el teorema 2.22 nos da un epimorfismo $K[[X_1, \ldots, X_n]] \longrightarrow A$. Finalmente basta aplicar el teorema 2.35. ∎

En particular, todo cuerpo k tiene la propiedad J_2, luego toda k-álgebra afín tiene la propiedad J_1, luego su conjunto de puntos regulares es abierto. Es fácil ver que si es reducida entonces dicho conjunto es no vacío, lo cual generaliza al teorema [E 7.21].

3.4 Homomorfismos suaves

De acuerdo con [E 7.49], podríamos decir que un homomorfismo de anillos $A \longrightarrow B$ es "suave" si es plano, convierte a B en una A-álgebra finitamente generada y, para cada $\mathfrak{p} \in \operatorname{Esp} A$, la fibra $B \otimes_A k(\mathfrak{p})$ es una $k(\mathfrak{p})$-álgebra afín geométricamente regular. Sin embargo, necesitamos generalizar estos conceptos (tanto la suavidad como la regularidad geométrica) eliminando la condición de finitud, y a ello dedicamos esta sección.

Definición 3.33 Sea A un anillo noetheriano y $k \subset A$ un subcuerpo. Diremos que A es *geométricamente regular* sobre k si $A \otimes_k K$ es regular, para toda extensión finita K/k.

Observemos que si A es una k-álgebra de tipo finito, entonces $\operatorname{Esp} A$ es un conjunto algebraico afín geométricamente regular en el sentido de la definición [E 7.23], pero la definición anterior no requiere la hipótesis de finitud.

Por definición, $A \otimes_k K$ es regular si y sólo si lo es $(A \otimes_k K)_{\mathfrak{P}}$, para cada ideal maximal $\mathfrak{P}$. Observemos que $A \otimes_k K$ es una A-álgebra finita, luego entera, luego $\mathfrak{p} = A \cap \mathfrak{P}$ es un ideal maximal de A, por [AC 3.63] (y todo ideal maximal $\mathfrak{p}$ de A es de la forma $\mathfrak{p} = A \cap \mathfrak{P}$). Además, es claro que $(A \otimes_k K)_{\mathfrak{P}} = (A_{\mathfrak{p}} \otimes_k K)_{\mathfrak{P}'}$, donde $\mathfrak{P}' = \mathfrak{P}_{\mathfrak{p}}$. Todo lo dicho vale igual para ideales primos en lugar de maximales, luego hemos probado lo siguiente:

Teorema 3.34 *Sea A un anillo y $k \subset A$ un subcuerpo. Las afirmaciones siguientes son equivalentes:*

a) A es geométricamente regular sobre k.

b) $A_{\mathfrak{p}}$ es geométricamente regular sobre k, para todo ideal primo $\mathfrak{p}$ de A.

c) $A_{\mathfrak{p}}$ es geométricamente regular sobre k, para todo ideal maximal $\mathfrak{p}$ de A.

El concepto de suavidad formal nos ayudará también a estudiar la regularidad geométrica debido al resultado siguiente:

Teorema 3.35 *Sea A un anillo noetheriano local que contenga un cuerpo k_0. Sea $\mathfrak{m}$ su ideal maximal y $k = A/\mathfrak{m}$ su cuerpo de restos. Si A es $\mathfrak{m}$-suave sobre k_0, entonces A es geométricamente regular sobre k_0.*

Demostración: Sea K/k_0 una extensión finita. Entonces $A' = A \otimes_k K$ es $\mathfrak{m}A'$-suave sobre K por cambio de base. Sea $\mathfrak{n}$ un ideal maximal de A'. Como A' es un A-módulo finitamente generado, es entero sobre A, y [AC 3.63] implica que $\mathfrak{m}A' \subset \mathfrak{n}$. Por consiguiente, si llamamos $A'' = A'_{\mathfrak{n}}$ y $\mathfrak{m}'' = \mathfrak{n}A''$, tenemos que el homomorfismo $A' \longrightarrow A''$ es continuo para las topologías $\mathfrak{m}A'$-ádica y $\mathfrak{m}''$-ádica.

Por otro lado, el teorema 2.5 implica que A'' es 0-llano sobre A', luego en particular es $\mathfrak{m}''$-llano. Por transitividad concluimos que A'' es $\mathfrak{m}''$-suave sobre K. Ahora bien, A'' es un anillo noetheriano local que contiene a K, luego, por

el teorema 2.23, sabemos que es regular. Como esto es válido para todo ideal maximal $\mathfrak{n}$ de A', hemos probado que A' es regular. ∎

Puede probarse que el recíproco también es cierto, pero es más complicado y no nos va a hacer falta. De momento podemos demostrar lo siguiente:

Teorema 3.36 *Si A es un anillo noetheriano regular y $k \subset A$ es un subcuerpo perfecto, entonces A es geométricamente regular sobre k.*

DEMOSTRACIÓN: Si $\mathfrak{p}$ es un ideal primo de A, tenemos que $A_\mathfrak{p}$ es regular y $k(\mathfrak{p})$ es separablemente generado sobre k, luego $A_\mathfrak{p}$ es $\mathfrak{p}$-suave sobre k por 2.23, luego es geométricamente regular por el teorema anterior. Como esto es cierto para todo primo $\mathfrak{p}$, concluimos que A es geométricamente regular sobre k. ∎

Definición 3.37 Diremos que un homomorfismo de anillos $\phi : A \longrightarrow B$ es *suave* si es plano y, para cada $\mathfrak{p} \in \operatorname{Esp} A$, la fibra $B \otimes_A k(\mathfrak{p})$ es geométricamente regular sobre $k(\mathfrak{p})$.

Tal y como hemos indicado, al comparar con [E 7.49] debemos tener presente que no exigimos que B sea una A-álgebra finitamente generada.

Teorema 3.38 *Si $\phi : A \longrightarrow B$ es un homomorfismo suave de anillos, un ideal $\mathfrak{p} \in \operatorname{Esp} B$ es regular si y sólo si lo es $\mathfrak{P} = \phi^{-1}[\mathfrak{P}] \in \operatorname{Esp} A$.*

DEMOSTRACIÓN: El homomorfismo $\phi_\mathfrak{P} : A_\mathfrak{P} \longrightarrow B_\mathfrak{p}$ es plano. Además, la fibra de $\mathfrak{p}$ respecto a él es la misma que la fibra respecto de ϕ, que es geométricamente regular y, en particular, regular.

En estas condiciones, hemos de probar que $A_\mathfrak{P}$ es regular si y sólo si lo es $B_\mathfrak{p}$. Una implicación es el teorema 3.25. Supongamos ahora que $A_\mathfrak{P}$ es regular. El teorema [E 4.52] nos da la relación $\dim B_\mathfrak{p} = \dim A_\mathfrak{P} + \dim B_\mathfrak{p}/\mathfrak{P}B_\mathfrak{p}$. La conclusión es inmediata: Como $A_\mathfrak{P}$ es regular, el ideal $\mathfrak{P}$ está generado por $\dim A_\mathfrak{P}$ elementos, que también generan $\mathfrak{P}B_\mathfrak{p}$ y, unidos a un generador de $\mathfrak{p}/\mathfrak{P}B_\mathfrak{p}$ con $\dim B_\mathfrak{p}/\mathfrak{P}B_\mathfrak{p}$ elementos (que existe porque $B_\mathfrak{p}/\mathfrak{P}B_\mathfrak{p}$ es regular), nos da un generador de $\mathfrak{p}$ con $\dim B_\mathfrak{p}$ elementos, luego $B_\mathfrak{p}$ es regular. ∎

Teorema 3.39 *Sean $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ homomorfismos de anillos.*

a) Si ϕ y ψ son suaves, entonces $\phi \circ \psi$ también lo es.

b) Si $\phi \circ \psi$ es suave y ψ es fielmente plano, entonces ϕ es regular.

DEMOSTRACIÓN: a) Sabemos que $\phi \circ \psi$ es plano. Sea $\mathfrak{p} \in \operatorname{Esp} A$ y L una extensión finita de $k(\mathfrak{p})$. Hemos de probar que el anillo $C \otimes_A L$ es regular.

Como ϕ es suave, tenemos que el anillo $B \otimes_A L$ es regular. Por el teorema anterior, basta probar que $\psi \otimes 1 : B \otimes_A L \longrightarrow C \otimes_A L$ es suave.

Ciertamente, es plano. Si $\mathfrak{P} \in \operatorname{Esp}(B \otimes_A L)$ y F es una extensión finita de $k(\mathfrak{P})$ (en particular, una extensión de L), entonces $(C \otimes_A L) \otimes_{B \otimes_A L} F \cong C \otimes_B F$,

luego hemos de ver que este anillo es regular. Si $\mathfrak{Q} = \mathfrak{P} \cap B$, por la regularidad de ψ, basta probar que F es una extensión finita de $k(\mathfrak{Q})$, lo cual se debe a que la extensión $k(\mathfrak{Q})/k(\mathfrak{P})$ es finita, ya que $B \otimes_A L$ es un B-módulo finitamente generado.

b) Se cumple que B es plano sobre A, porque si $M \longrightarrow N$ es un monomorfismo de A-módulos, también lo es $M \otimes_A B \otimes_B C \longrightarrow N \otimes_A B \otimes_B C$, porque C es plano sobre A, luego también $M \otimes_A B \longrightarrow N \otimes_A B$, porque C es fielmente plano sobre B.

Tomemos nuevamente un $\mathfrak{p} \in \operatorname{Esp} A$ y una extensión finita L de $k(\mathfrak{p})$. Como antes, tenemos que $B \otimes_A L \longrightarrow C \otimes_A L$ es suave, pero ahora sabemos que $C \otimes_A L$ es regular y queremos probar que $B \otimes_A L$ también lo es. Nuevamente, esto es consecuencia del teorema anterior, aunque ahora necesitamos también 1.24. ∎

Teorema 3.40 *Si $A \longrightarrow B$ es un homomorfismo suave de anillos y A' es una A-álgebra finitamente generada, entonces $A' \longrightarrow B \otimes_A A'$ también es suave.*

Demostración: Sea $\mathfrak{P}' \in \operatorname{Esp} A'$ y $\mathfrak{P} = \mathfrak{P}' \cap A$. Sea $k = k(\mathfrak{P})$ y $K = k(\mathfrak{P}')$. El homomorfismo $A' \longrightarrow B \otimes_A A'$ es plano por cambio de base. Hemos de probar que la fibra de $\mathfrak{P}'$ es geométricamente regular o, lo que es lo mismo, que si L es una extensión finita de K, el anillo

$$B \otimes_A A' \otimes_{A'} K \otimes_K L = B \otimes_K L = (B \otimes_A k) \otimes_k L$$

es regular. Como K es finitamente generado sobre k, lo mismo le sucede a L. Por 3.29 existe una extensión finita puramente inseparable k'/k tal que $L' = Lk'$ es separablemente generada sobre k'.

Observemos que $(B \otimes_A A') \otimes_{A'} L' = ((B \otimes_A A') \otimes_{A'} L) \otimes_L L'$ es fielmente plano sobre $(B \otimes_A A') \otimes_{A'} L$ (por que L' es plano sobre L). Si probamos que $(B \otimes_A A') \otimes_{A'} L'$ es regular, el teorema 3.25 (aplicado a las localizaciones del homomorfismo natural entre ambos, que induce una aplicación suprayectiva entre sus espectros) nos da que $(B \otimes_A A') \otimes_{A'} L$ también es regular, que es lo que queremos probar.

Por hipótesis, $T = B \otimes_A k'$ es regular. Por otra parte, se cumple que

$$(B \otimes_A A') \otimes_{A'} L' = B \otimes_A L' = (B \otimes_A k') \otimes_{k'} L' = T \otimes_{k'} L'.$$

Basta probar que el homomorfismo $T \longrightarrow T \otimes_{k'} L'$ es suave, ya que entonces $T \otimes_{k'} L'$ será regular por el teorema anterior. Esto se reduce a probar que las fibras $k(\mathfrak{p}) \otimes_T T \otimes_{k'} L'$ (para $\mathfrak{p} \in \operatorname{Esp} T$) son geométricamente regulares o, lo que es lo mismo, que si E es una extensión finita de $k(\mathfrak{p})$, entonces $E \otimes_{k'} L'$ es regular. Sea $k' \subset F \subset L'$, donde $F = k'(X_1, \ldots, X_n)$ es una extensión puramente trascendente de k' tal que L'/F sea finita separable. Tenemos un monomorfismo

$$E \otimes_{k'} F \longrightarrow E(X_1, \ldots, X_n)$$

cuya imagen está formada por las fracciones con denominador en $k'[X_1,\dots,X_n]$, luego $E\otimes_{k'} F$ es isomorfo a una localización de $E[X_1,\dots,X_n]$, luego es un dominio íntegro regular.

Como $E\otimes_{k'} L' = E\otimes_{k'} F\otimes_F L'$, basta probar que si A es una F-álgebra regular, y L'/F es una extensión finita separable, entonces $A\otimes_F L'$ es regular. Por el teorema anterior, basta probar que el homomorfismo $A\longrightarrow A\otimes_F L'$ es suave, para lo cual, a su vez, basta probar que si E es una extensión de F, entonces $E\otimes_F L'$ es regular.

Ahora bien, $\operatorname{Esp} L'$ es un conjunto algebraico geométricamente regular sobre F por el teorema [E 7.24], luego $E\otimes_F L'$ es regular por el teorema [E 7.29]. ∎

Como consecuencia obtenemos:

Teorema 3.41 *Si $f : A\longrightarrow B$ es un homomorfismo fielmente plano y suave entre anillos noetherianos y B tiene la propiedad J_2, entonces A también la tiene.*

Demostración: Llamemos $X = \operatorname{Esp} B$, $Y = \operatorname{Esp} A$ y consideremos el homomorfismo de esquemas $\phi : X\longrightarrow Y$ asociado a f. Por el teorema 3.38 sabemos que $\phi^{-1}[\operatorname{Reg} Y] = \operatorname{Reg} X$. El teorema 1.33 implica que $\operatorname{Reg} X$ es abierto en X si y sólo si $\operatorname{Reg} Y$ es abierto en Y, es decir, que B tiene la propiedad J_1 si y sólo si la tiene A. Si B tiene la propiedad J_2, el teorema anterior implica que A también la tiene. ∎

Los homomorfismos suaves conservan más propiedades. Para mostrar más ejemplos necesitamos el teorema siguiente:

Teorema 3.42 *Sea $f : A\longrightarrow B$ un homomorfismo plano entre anillos locales y sea $\mathfrak{m}$ el ideal maximal de A. Entonces*

$$\operatorname{pr}(B) = \operatorname{pr}(A) + \operatorname{pr}(B/\mathfrak{m}B).$$

Demostración: Sea $\mathfrak{n}$ el ideal maximal de B. Consideremos una sucesión regular maximal $x_1,\dots,x_r\in\mathfrak{m}$ y una sucesión $B/\mathfrak{m}B$-regular maximal $y_1,\dots,y_s\in\mathfrak{n}$. Llamemos x'_i a la imagen de x_i en B y probemos que $x'_1,\dots,x'_r,y_1,\dots,y_s\in\mathfrak{n}$ es una sucesión regular maximal de B.

Como la multiplicación por x_1 es un monomorfismo $A\longrightarrow A$ y B es plano sobre A, la multiplicación por x'_1 es un monomorfismo $B\longrightarrow B$, luego x'_1 es regular en B. Ahora tenemos en cuenta que x_2 no es un divisor de cero de A/x_1A y concluimos que x'_2 no es un divisor de cero de $A/x_1A\otimes_A B\cong B/x'_1B$, luego x'_1,x'_2 es también una sucesión regular. Procediendo de este modo, llegamos a que $x'_1,\dots,x'_r$ es una sucesión regular.

Llamemos $A_r = A/(x_1,\dots,x_r)$. Entonces $\mathfrak{m}\in\operatorname{As}_A(A_r)$ y

$$A_r\otimes_A B\cong B/(x'_1,\dots,x'_r).$$

El teorema [AC A.15] nos da que y_1 es regular en B y que B/y_1B es plano sobre A, luego la sucesión exacta

$$0\longrightarrow B\xrightarrow{y_1} B\longrightarrow B/y_1B\longrightarrow 0$$

nos da (por [AC A.3]) una sucesión exacta

$$0 \longrightarrow A_r \otimes_A B \longrightarrow A_r \otimes_A B \longrightarrow A_r \otimes_A (B/y_1B) \longrightarrow 0.$$

Esto prueba que la sucesión $x_1', \ldots, x_r', y_1$ es regular. Ahora aplicamos [AC A.15] a y_2 y al anillo B/y_1B, ya que

$$(B/y_1B) \,/\, \mathfrak{m}(B/y_1B) \cong B/(\mathfrak{m} + (y_1))B \cong (B/\mathfrak{m}B) \,/\, y_1(B/\mathfrak{m}B),$$

y sabemos que y_2 no es un divisor de cero del último cociente. Concluimos que y_2 es regular en B/y_1B y que $B/(y_1, y_2)B$ es plano sobre A, de donde, razonando como antes, concluimos que $x_1', \ldots, x_r', y_1, y_2$ es una sucesión regular. Tras un número finito de pasos, llegamos a que $x_1', \ldots, x_r', y_1, \ldots, y_s$ es regular. Falta probar que es una sucesión maximal o, lo que es lo mismo, que si llamamos $B_s = B/(y_1, \ldots, y_s)$, el cociente

$$B/(x_1', \ldots, x_r', y_1, \ldots, y_s) \cong A_r \otimes_A B_s$$

tiene profundidad 0 o, lo que es lo mismo, que $\mathfrak{n} \in \operatorname{As}(A_r \otimes_A B_s)$. Ahora bien, esto es consecuencia inmediata de 1.9, que nos da la fórmula

$$\operatorname{As}_B(A_r \otimes_A B_s) = \bigcup_{\mathfrak{p} \in \operatorname{As}(A_r)} \operatorname{As}_B(B_s/\mathfrak{p}B_s)$$

y, ciertamente, $\mathfrak{n} \in \operatorname{As}_B(B_s/\mathfrak{m}B_s)$. ∎

Teorema 3.43 *Sea $f : A \longrightarrow B$ un homomorfismo fielmente plano y suave entre anillos noetherianos. Entonces A cumple la propiedad R_i o S_i de* 1.15 *si y sólo si la cumple B.*

Demostración: Sea $\mathfrak{p} \in \operatorname{Esp} A$ y tomemos $\mathfrak{P} \in \operatorname{Esp} B$ minimal entre los primos que cumplen $\mathfrak{P} \cap A = \mathfrak{p}$. Sea $k = k(\mathfrak{p})$. Entonces, la fibra de $\mathfrak{p}A_\mathfrak{p}$ respecto del homomorfismo $A_\mathfrak{p} \longrightarrow B_\mathfrak{P}$ contiene únicamente al ideal $\mathfrak{P}B_\mathfrak{P}$, es decir, que $B_\mathfrak{P} \otimes_A k$ sólo tiene un ideal primo, por lo que $\dim(B_\mathfrak{P} \otimes_A k) = \operatorname{pr}(B_\mathfrak{P} \otimes_A k) = 0$. El teorema [E 4.52] nos da que $\dim B_\mathfrak{P} = \dim A_\mathfrak{p}$, y el teorema anterior nos da que $\operatorname{pr} B_\mathfrak{P} = \operatorname{pr} A_\mathfrak{p}$.

Si B cumple la propiedad S_i, entonces

$$\operatorname{pr} A_\mathfrak{p} = \operatorname{pr} B_\mathfrak{P} \geq \text{mín}\{i, \dim B_\mathfrak{P}\} = \text{mín}\{i, \dim A_\mathfrak{p}\},$$

luego A también cumple S_i.

Si B cumple la propiedad R_i y suponemos que $\dim A_\mathfrak{p} \leq i$, entonces también $\dim B_\mathfrak{P} \leq i$, luego $B_\mathfrak{P}$ es regular, y $A_\mathfrak{p}$ también lo es por 3.38. Así pues, A también cumple R_i. Observemos que en estas implicaciones no hemos usado la suavidad de f.

Supongamos ahora que A cumple S_i. Sea $\mathfrak{P} \in \operatorname{Esp} B$ y llamemos $\mathfrak{p} = \mathfrak{P} \cap A$, $k = k(\mathfrak{p})$. Sabemos que la fibra $B \otimes_A k \cong B_\mathfrak{P} \otimes_{A_\mathfrak{p}} k$ es regular, luego también cumple la propiedad S_k. Por el teorema anterior,

$$\begin{aligned}\operatorname{pr} B_\mathfrak{P} &= \operatorname{pr} A_\mathfrak{p} + \operatorname{pr}(B_\mathfrak{P} \otimes_{A_\mathfrak{p}} k) \geq \text{mín}\{i, \dim A_\mathfrak{p}\} + \text{mín}\{i, \dim(B_\mathfrak{P} \otimes_{A_\mathfrak{p}} k)\} \\ &\geq \text{mín}\{i, \dim A_\mathfrak{p} + \dim(B_\mathfrak{P} \otimes_{A_\mathfrak{p}} k)\} = \text{mín}\{i, \dim B_\mathfrak{P}\},\end{aligned}$$

donde hemos aplicado nuevamente el teorema [E 4.52].

Si A cumple R_i y $\dim B_{\mathfrak{P}} \leq i$, entonces $\dim A_{\mathfrak{p}} \leq \dim B_{\mathfrak{P}} \leq i$ (porque $f_{\mathfrak{P}}$ es suprayectivo), luego $A_{\mathfrak{p}}$ es regular y $B_{\mathfrak{P}}$ también lo es por 3.38. Por consiguiente, B también cumple R_i. ∎

En particular, los teoremas 1.16 y 1.18 nos dan que, en las condiciones del teorema anterior, A es reducido o normal si y sólo si lo es B.

3.5 La propiedad G

Nos ocupamos ahora de la tercera y última propiedad que define a los anillos excelentes, debida a Grothendieck.

Definición 3.44 Diremos que un anillo noetheriano A tiene la *propiedad G* si, para cada ideal primo $\mathfrak{p}$ de A, el homomorfismo natural $\phi_{\mathfrak{p}} : A_{\mathfrak{p}} \longrightarrow \hat{A}_{\mathfrak{p}}$ (de $A_{\mathfrak{p}}$ en su compleción) es suave. Notemos que $\phi_{\mathfrak{p}}$ siempre es plano, luego lo que exige realmente la propiedad G es que sus fibras sean geométricamente regulares.

Los homomorfismos $\phi_{\mathfrak{p}}$ no son, en general, finitamente generados, y ésta es la razón por la que en la sección anterior hemos tenido que generalizar la suavidad al caso de homomorfismos que no sean necesariamente finitamente generados.

Teorema 3.45 *Si un anillo A tiene la propiedad G, también la tiene toda localización y todo cociente de A.*

Demostración: Sea $S \subset A$ un subconjunto multiplicativo. Un ideal primo de $S^{-1}A$ es de la forma $S^{-1}\mathfrak{p}$, donde $\mathfrak{p}$ es un ideal primo disjunto con S, y $S^{-1}A_{S^{-1}\mathfrak{p}} = A_{\mathfrak{p}}$. La conclusión es inmediata.

Si I es un ideal de A, todo primo de $\bar{A} = A/I$ es de la forma $\bar{\mathfrak{p}} = \mathfrak{p}/I$, donde $\mathfrak{p}$ es un primo de A, y $\bar{A}_{\bar{\mathfrak{p}}} = A_{\mathfrak{p}}/I_{\mathfrak{p}}$. Notemos que, por [AC 4.17], la compleción de $\bar{A}_{\bar{\mathfrak{p}}}$ es $\hat{A}_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \bar{A}_{\bar{\mathfrak{p}}}$. Hemos de estudiar las fibras del homomorfismo natural $\bar{A}_{\bar{\mathfrak{p}}} \longrightarrow \hat{A}_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \bar{A}_{\bar{\mathfrak{p}}}$. Para ello, tomamos un primo de $\bar{A}_{\bar{\mathfrak{p}}}$, que será de la forma $\bar{\mathfrak{q}} = \mathfrak{q}A_{\mathfrak{p}}/I_{\mathfrak{p}}$, donde $I \subset \mathfrak{q} \subset \mathfrak{p}$. Su fibra es

$$\hat{A}_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \bar{A}_{\bar{\mathfrak{p}}} \otimes_{\bar{A}_{\bar{\mathfrak{p}}}} k(\bar{\mathfrak{q}}) = \hat{A}_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} k(\bar{\mathfrak{q}}) = \hat{A}_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} k(\mathfrak{q}),$$

donde hemos usado que

$$k(\bar{\mathfrak{q}}) = (A_{\mathfrak{p}}/I_{\mathfrak{p}})_{\mathfrak{q}A_{\mathfrak{p}}/I_{\mathfrak{p}}} \,/\, (\mathfrak{q}A_{\mathfrak{p}}/I_{\mathfrak{p}})(A_{\mathfrak{p}}/I_{\mathfrak{p}})_{\mathfrak{q}A_{\mathfrak{p}}/I_{\mathfrak{p}}}$$

$$\cong (A_{\mathfrak{q}}/I_{\mathfrak{q}}) \,/\, (\mathfrak{q}A_{\mathfrak{q}}/I_{\mathfrak{q}}) \cong A_{\mathfrak{q}}/\mathfrak{q}A_{\mathfrak{q}} = k(\mathfrak{q}).$$

Así pues, la fibra de $\bar{\mathfrak{q}}$ coincide con la fibra de $\mathfrak{q}A_{\mathfrak{p}}$ respecto al homomorfismo $A_{\mathfrak{p}} \longrightarrow \hat{A}_{\mathfrak{p}}$, que, por hipótesis, es geométricamente regular sobre $k(\mathfrak{q})$. ∎

Ahora es inmediato que un anillo noetheriano A tiene la propiedad G si y sólo si la tienen todas sus localizaciones $A_{\mathfrak{p}}$, donde $\mathfrak{p}$ recorre los ideales primos de A. Más aún, basta con que esto se cumpla para los ideales maximales, ya que, si $\mathfrak{p} \subset \mathfrak{m}$, entonces $A_{\mathfrak{p}}$ es una localización de $A_{\mathfrak{m}}$.

Similarmente, la prueba del teorema anterior muestra que si A/I tiene la propiedad G para todo ideal I de A, entonces A tiene la propiedad G. Más aún, basta con que esto suceda para todo ideal primo.

Teorema 3.46 *Si un anillo noetheriano local tiene la propiedad G, también tiene la propiedad J_2.*

DEMOSTRACIÓN: Si A es un anillo local con la propiedad G, el homomorfismo $A \longrightarrow \hat{A}$ es suave y fielmente plano, y $\hat{A}$ tiene la propiedad J_2 por 3.32, luego basta aplicar el teorema 3.41. ∎

Teorema 3.47 *Si $\phi : A \longrightarrow B$ es un homomorfismo de anillos suave y fielmente plano y B tiene la propiedad G, entonces A también la tiene.*

DEMOSTRACIÓN: Si $\mathfrak{p} \in \operatorname{Esp} A$, el teorema 1.24 nos da un $\mathfrak{P} \in \operatorname{Esp} B$ tal que $\phi^{-1}[\mathfrak{P}] = \mathfrak{p}$. Consideremos el diagrama conmutativo

$$\begin{array}{ccc} \hat{A}_{\mathfrak{p}} & \xrightarrow{\hat{\phi}_{\mathfrak{p}}} & \hat{B}_{\mathfrak{P}} \\ {\scriptstyle\alpha}\uparrow & & \uparrow{\scriptstyle\beta} \\ A_{\mathfrak{p}} & \xrightarrow[\phi_{\mathfrak{p}}]{} & B_{\mathfrak{P}} \end{array}$$

Por hipótesis, β es suave, y es fácil ver que $\phi_{\mathfrak{p}}$ también lo es por serlo ϕ. Por otra parte, $\hat{\phi}_{\mathfrak{p}}$ es plano. Esto es consecuencia del teorema [AC A.14]: como $\hat{B}_{\mathfrak{P}}$ es plano sobre $A_{\mathfrak{p}}$, llamando $\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}$, tenemos que $\mathfrak{m} \otimes_{A_{\mathfrak{p}}} \hat{B}_{\mathfrak{P}} \cong \mathfrak{m}\hat{B}_{\mathfrak{P}} = \hat{\mathfrak{m}}\hat{B}_{\mathfrak{P}}$, pero, según [AC 4.18],

$$\mathfrak{m} \otimes_{A_{\mathfrak{p}}} \hat{B}_{\mathfrak{P}} \cong \mathfrak{m} \otimes_{A_{\mathfrak{p}}} \hat{A}_{\mathfrak{p}} \otimes_{\hat{A}_{\mathfrak{p}}} \hat{B}_{\mathfrak{P}} \cong \hat{\mathfrak{m}} \otimes_{\hat{A}_{\mathfrak{p}}} \hat{B}_{\mathfrak{P}},$$

luego también $\hat{\mathfrak{m}} \otimes_{\hat{A}_{\mathfrak{p}}} \hat{B}_{\mathfrak{P}} \cong \hat{\mathfrak{m}}\hat{B}_{\mathfrak{P}}$, y el isomorfismo es el natural. Aplicando de nuevo [AC A.14] concluimos que $\hat{B}_{\mathfrak{P}}$ es plano sobre $\hat{A}_{\mathfrak{p}}$, tal y como hemos afirmado.

Como los anillos son locales, $\hat{\phi}_{\mathfrak{p}}$ es, de hecho, fielmente plano. Ahora basta aplicar el teorema 3.39, según el cual $\alpha \circ \hat{\phi}_{\mathfrak{p}} = \phi_{\mathfrak{p}} \circ \beta$ es suave, luego también lo es α. Esto prueba que A tiene la propiedad G. ∎

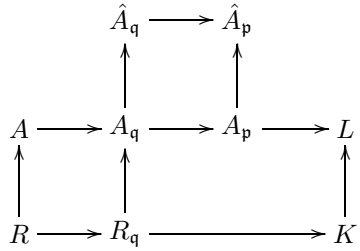
Como todas las propiedades que estamos estudiando, la propiedad G la cumplen los anillos locales completos:

Teorema 3.48 *Todo anillo noetheriano local y completo tiene la propiedad G.*

DEMOSTRACIÓN: Sea A un anillo noetheriano local y completo y tomemos $\mathfrak{p} \in \operatorname{Esp} A$. Hemos de probar que el homomorfismo $A_{\mathfrak{p}} \longrightarrow \hat{A}_{\mathfrak{p}}$ es suave. Para ello tomamos un primo $\mathfrak{p}'$ de $A_{\mathfrak{p}}$ y hemos de probar que la fibra de $\mathfrak{p}'$ es geométricamente regular sobre $k(\mathfrak{p}')$.

Notemos que $\mathfrak{p}' = \mathfrak{q}A_\mathfrak{p}$, donde $\mathfrak{q} \subset \mathfrak{p}$ es un primo de A. En la prueba del teorema 3.45 (tomando $I = \mathfrak{q}$) hemos visto que, si $\bar{A} = A/\mathfrak{q}$ y $\bar{\mathfrak{p}} = \mathfrak{p}/\mathfrak{q}$, la fibra de $\mathfrak{p}'$ coincide con la fibra de 0 respecto al homomorfismo de $\bar{A}_{\bar{\mathfrak{p}}}$ en su compleción. Como $\bar{A}$ también es un anillo noetheriano completo, no perdemos generalidad si suponemos que A es un dominio íntegro y que $\mathfrak{p}' = 0$. En definitiva, si llamamos L al cuerpo de cocientes de A, lo que hemos de probar es que $\hat{A}_\mathfrak{p} \otimes_{A_\mathfrak{p}} L$ es geométricamente regular sobre L.

Según el teorema 2.21, tenemos que A contiene un anillo local regular y completo R tal que A es una R-álgebra finita. Sea $\mathfrak{q} = \mathfrak{p} \cap R$. Consideremos la localización $A_\mathfrak{q} = A \otimes_R R_\mathfrak{q}$. Por el [AC 3.63 y 3.64] vemos que $A_\mathfrak{q}$ tiene un número finito de ideales maximales (en correspondencia con los ideales maximales de A cuya antiimagen en R es $\mathfrak{q}$, uno de los cuales es $\mathfrak{p}$) y $A_\mathfrak{p}$ es la localización de $A_\mathfrak{q}$ respecto de uno de ellos. El mismo argumento empleado en la prueba del teorema 3.32 muestra que $\hat{A}_\mathfrak{p}$ es un sumando directo de la compleción $\hat{A}_\mathfrak{q} = \hat{R}_\mathfrak{q} \otimes_{R_\mathfrak{q}} A_\mathfrak{q}$. Si llamamos K al cuerpo de cocientes de R, la situación es la siguiente:



Ahora observamos que $\hat{A}_\mathfrak{p} \otimes_{A_\mathfrak{p}} L = \hat{A}_\mathfrak{p} \otimes_{A_\mathfrak{q}} L$ (porque, en $\hat{A}_\mathfrak{p} \otimes_{A_\mathfrak{q}} L$ se cumple que $a(a'/s) \otimes b = a(a'/s) \otimes (s/s)b = a \otimes (a'/s)b$, para todo $a'/s \in A_\mathfrak{p}$). Por lo tanto, es un sumando directo de $\hat{A}_\mathfrak{q} \otimes_{A_\mathfrak{q}} L = \hat{R}_\mathfrak{q} \otimes_{R_\mathfrak{q}} L = (\hat{R}_\mathfrak{q} \otimes_{R_\mathfrak{q}} K) \otimes_K L$.

Por consiguiente, si probamos que $\hat{R}_\mathfrak{q} \otimes_{R_\mathfrak{q}} K$ es geométricamente regular sobre K, tendremos que $\hat{A}_\mathfrak{q} \otimes_{A_\mathfrak{q}} L$ será geométricamente regular sobre L, y lo mismo valdrá para $\hat{A}_\mathfrak{p} \otimes_{A_\mathfrak{p}} L$.

Equivalentemente, cambiando A por R, podemos suponer que A es un anillo local regular y completo, con lo que también son regulares $A_\mathfrak{p}$, $\hat{A}_\mathfrak{p}$ y $\hat{A}_\mathfrak{p} \otimes_{A_\mathfrak{p}} L$ (el tercero por ser una localización del segundo). Si L tiene característica 0, entonces $\hat{A}_\mathfrak{p} \otimes_{A_\mathfrak{p}} L$ es geométricamente regular sobre L por el teorema 3.36. Así pues, en adelante podemos suponer que L tiene característica prima p. Por la observación tras 2.22, tenemos que $A = k[[X_1, \ldots, X_n]]$.

Recordemos que queremos probar que $\hat{A}_\mathfrak{p} \otimes_{A_\mathfrak{p}} L$ es geométricamente regular sobre L, para lo cual basta probar que lo son sus localizaciones en cada uno de sus primos $\mathfrak{P}$. Como se trata de la fibra del homomorfismo $A_\mathfrak{p} \longrightarrow \hat{A}_\mathfrak{p}$, el primo $\mathfrak{P}$ puede identificarse con un primo $\mathfrak{P} \in \operatorname{Esp} \hat{A}_\mathfrak{p}$ tal que $\mathfrak{P} \cap A_\mathfrak{p} = 0$. Más aún, por [E 3.47] resulta que, a través de dicha identificación, la localización en $\mathfrak{P}$ es isomorfa a $(\hat{A}_\mathfrak{p})_\mathfrak{P}$. Basta probar, pues, que este anillo es geométricamente regular sobre L.

Fijemos un generador de k/k^p y llamemos $\mathcal{F}$ a la familia de todos los cuerpos intermedios $k^p \subset F \subset k$ que resultan de adjuntar a k^p todos los elementos del generador salvo un número finito de ellos. Así, los índices $|k : F|$ son finitos y

$$\bigcap_{F\in\mathcal{F}} F = k^p.$$

Para cada $F \in \mathcal{F}$, llamemos $A_F = F[[X_1^p, \ldots, X_n^p]]$ y sea $L_F \subset L$ su cuerpo de cocientes. Tenemos que A es un A_F-módulo finitamente generado, luego la extensión A/A_F es entera. Además A_F es íntegramente cerrado, porque es regular, luego $A \cap L_F = A_F$.

Si $a \in \bigcap_{F\in\mathcal{F}} L_F \subset L$, podemos expresarlo en la forma $a = u/v$, para ciertos u, $v \in A$. Multiplicando por v^{p-1} podemos suponer que $v \in A^p \subset L_F$. Entonces $u \in A \cap L_F = A_F$ para todo $F \in \mathcal{F}$, luego $u \in \bigcap_{F\in\mathcal{F}} A_F = A^p$. Esto prueba que

$$\bigcap_{F\in\mathcal{F}} L_F = L^p.$$

Llamemos $\mathfrak{p}_F = \mathfrak{p} \cap A_F$. Del hecho de que $A^p \subset A_F \subset A$ se sigue que $A_\mathfrak{p} = A \otimes_{A_F} A_{F,\mathfrak{p}_F}$, pues $s \in A_F \backslash \mathfrak{p}_F$, entonces $s \in A \backslash \mathfrak{p}$ o, de lo contrario, $s^p \in \mathfrak{p}_F$ y también $s \in \mathfrak{p}_F$. Esto permite definir un homomorfismo $A \otimes_{A_F} A_{F,\mathfrak{p}_F} \longrightarrow A_\mathfrak{p}$, que claramente es un isomorfismo.

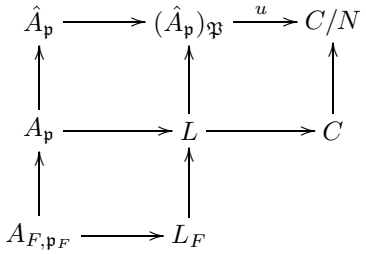
Como A es un A_F-módulo finitamente generado, $A_\mathfrak{p}$ es también un $A_{F,\mathfrak{p}_F}$-módulo finitamente generado. Más aún, es claro que, a través del isomorfismo anterior, $\mathfrak{p}_F A_\mathfrak{p} = \mathfrak{p}$, es decir, la topología $\mathfrak{p}$-ádica en $A_\mathfrak{p}$ coincide con la topología $\mathfrak{p}_F$-ádica al considerarlo como $A_{F,\mathfrak{p}_F}$-módulo. Esto nos da a su vez la identificación $\hat{A}_\mathfrak{p} = A_\mathfrak{p} \otimes_{A_{F,\mathfrak{p}_F}} \hat{A}_{F,\mathfrak{p}_F}$.

Vamos a probar que $\hat{A}_\mathfrak{p}$ es 0-suave sobre $A_\mathfrak{p}$ con respecto a $A_{F,\mathfrak{p}_F}$. Para ello consideramos un diagrama conmutativo

$$\begin{array}{ccccc}
\hat{A}_{F,\mathfrak{p}_F} & \longrightarrow & \hat{A}_\mathfrak{p} & \xrightarrow{u} & C/N \\
\uparrow & & \uparrow & & \uparrow \\
A_{F,\mathfrak{p}_F} & \longrightarrow & A_\mathfrak{p} & \xrightarrow[u']{} & C
\end{array}$$

donde C es un anillo y N un ideal tal que $N^2 = 0$. Suponemos que u se eleva a un $A_{F,\mathfrak{p}_F}$-homomorfismo de álgebras $v' : \hat{A}_\mathfrak{p} \longrightarrow C$. Llamamos $w = v'|_{\hat{A}_{F,\mathfrak{p}_F}}$ y $v = u' \otimes w : \hat{A}_\mathfrak{p} = A_\mathfrak{p} \otimes_{A_{F,\mathfrak{p}_F}} \hat{A}_{F,\mathfrak{p}_F} \longrightarrow C$. Es fácil ver que v eleva a u y es un $A_\mathfrak{p}$-homomorfismo.

De aquí se sigue a su vez que $(\hat{A}_\mathfrak{p})_\mathfrak{P}$ es 0-suave sobre L con respecto a L_F. En efecto, basta considerar el diagrama siguiente:



Si u se levanta a un L_F-homomorfismo $v' : (\hat{A}_\mathfrak{p})_\mathfrak{P} \longrightarrow C$, la restricción de v' a $\hat{A}_\mathfrak{p}$ es un $A_{F,\mathfrak{p}_F}$-homomorfismo que levanta a la restricción de u. Según hemos visto, la restricción de u se levanta entonces a un $A_\mathfrak{p}$-homomorfismo $v'' : \hat{A}_\mathfrak{p} \longrightarrow C$. Las imágenes por u de los elementos de $\hat{A}_\mathfrak{p} \setminus \mathfrak{P}$ son unidades de C/N, luego las imágenes por v'' de dichos elementos son unidades en C (véase la prueba de 2.5). Esto implica que v'' se extiende a un L-homomorfismo $v : (\hat{A}_\mathfrak{p})_\mathfrak{P} \longrightarrow C$ que eleva a u.

Vamos a llamar $E = (\hat{A}_\mathfrak{p})_\mathfrak{P}$, que es un anillo local con ideal maximal $\mathfrak{P}$. Al ser 0-suave, también es $\mathfrak{P}$-suave sobre L con respecto a L_F. Según 2.37, esto implica que el homomorfismo

$$\Omega^1_{L/L_F} \otimes_L (E/\mathfrak{P}) \longrightarrow \Omega^1_{E/L_F} \otimes_E (E/\mathfrak{P})$$

tiene inverso por la derecha y, en particular, es inyectivo. Por otra parte, el teorema 2.30 aplicado a la extensión L/L^p nos da que el homomorfismo

$$\Omega^1_{L/\mathbb{Z}} \longrightarrow \varprojlim_{F\in\mathfrak{F}} \Omega^1_{L/F}$$

también es inyectivo (notemos que $\Omega^1_{L/L^p} = \Omega^1_{L/\mathbb{Z}}$), y lo mismo vale para

$$\Omega^1_{L/\mathbb{Z}} \otimes_L (E/\mathfrak{P}) \longrightarrow \varprojlim_{F\in\mathfrak{F}} (\Omega^1_{L/F} \otimes_L (E/\mathfrak{P})).$$

Por último, el diagrama conmutativo:

$$\begin{array}{ccc} \Omega^1_{L/\mathbb{Z}} \otimes_L (E/\mathfrak{P}) & \longrightarrow & \Omega^1_{E/\mathbb{Z}} \otimes_E (E/\mathfrak{P}) \\ \downarrow & & \downarrow \\ \varprojlim_{F\in\mathfrak{F}} (\Omega^1_{L/L_F} \otimes_L (E/\mathfrak{P})) & \longrightarrow & \varprojlim_{F\in\mathfrak{F}} (\Omega^1_{E/L_F} \otimes_E (E/\mathfrak{P})) \end{array}$$

nos da que el homomorfismo $\Omega^1_{L/\mathbb{Z}} \otimes_L (E/\mathfrak{P}) \longrightarrow \Omega^1_{E/\mathbb{Z}} \otimes_E (E/\mathfrak{P})$ es inyectivo. Así pues, el teorema 2.41 implica que E es $\mathfrak{P}$-suave sobre L y 3.35 nos permite concluir que es geométricamente regular sobre L. ∎

Combinando los dos últimos teoremas, obtenemos una condición caracterización débil de la propiedad G:

Teorema 3.49 *Si A es un anillo noetheriano y para todo ideal maximal $\mathfrak{m}$ de A el homomorfismo $A_\mathfrak{m} \longrightarrow \hat{A}_\mathfrak{m}$ es suave, entonces A tiene la propiedad G.*

DEMOSTRACIÓN: Por el teorema anterior, $\hat{A}_\mathfrak{m}$ tiene la propiedad G, y por el teorema 3.47 también la tiene $A_\mathfrak{m}$. Como esto vale para todo ideal maximal de A, las observaciones tras el teorema 3.45 implican que A tiene la propiedad G. ∎

Ahora necesitamos un último resultado técnico:

Teorema 3.50 *Sea A un anillo noetheriano y $X = \operatorname{Esp} A$. Si $Z \subset X$ es la intersección de un abierto con un cerrado y $Z \neq \varnothing$, entonces existe un $\mathfrak{p} \in Z$ tal que $\dim A/\mathfrak{p} \leq 1$.*

DEMOSTRACIÓN: Podemos suponer que $Z = D(f) \cap V(\mathfrak{P})$, donde $f \in A \setminus \mathfrak{P}$. Entonces Z es isomorfo a $\operatorname{Esp}((A/\mathfrak{P})_{\bar{f}})$, donde $\bar{f}$ es la clase de f módulo $\mathfrak{P}$. Sea $\mathfrak{m}$ un ideal maximal de $(A/\mathfrak{P})_{\bar{f}}$ y sea $\mathfrak{p}$ su imagen en A. Entonces $\mathfrak{m} = (\mathfrak{p}/\mathfrak{P})_{\bar{f}}$, con lo que es evidente que $\mathfrak{p} \in Z$. Por otra parte, es fácil ver que, si g es la clase de f módulo $\mathfrak{p}$, entonces

$$(A/\mathfrak{p})_g \cong A_f/\mathfrak{p}A_f \cong (A/\mathfrak{P})_{\bar{f}} \,/\, \mathfrak{m}$$

es un cuerpo. Esto significa que g está contenido en todos los ideales no nulos del dominio íntegro $D = A/\mathfrak{p}$. En particular, los primos minimales de g son todos los primos de altura 1 de D, que, en particular, son un número finito.

Si $\mathfrak{p}'$ es cualquier ideal primo de D y $d \in \mathfrak{p}'$ no es nulo, entonces d pertenece a cualquiera de sus primos minimales, que, por el teorema de los ideales principales [AC 5.2], tiene altura 1. Así pues, $\mathfrak{p}'$ está contenido en la unión de los primos minimales de g y por [AC 3.51] es uno de ellos. Así pues $\operatorname{alt}\mathfrak{p}' \leq 1$. Esto prueba que $\dim D \leq 1$. ∎

Teorema 3.51 *Si un anillo A tiene la propiedad G y B es una A-álgebra finitamente generada, entonces B tiene también la propiedad G.*

DEMOSTRACIÓN: No perdemos generalidad si suponemos que $B = A[t]$. Tomamos un ideal maximal $\mathfrak{P}$ de B y hemos de probar que el homomorfismo $B_\mathfrak{P} \longrightarrow \hat{B}_\mathfrak{P}$ es suave. Sea $\mathfrak{m} = \mathfrak{P} \cap A$. Como $B_\mathfrak{P}$ es la localización de $A_\mathfrak{m}[t]$ respecto de un ideal maximal y $A_\mathfrak{m}$ también tiene la propiedad G, no perdemos generalidad si suponemos que A es un anillo local y que $\mathfrak{m}$ es su ideal maximal.

El teorema 3.40 nos da que el homomorfismo natural $B \longrightarrow B' = B \otimes_A \hat{A}$ es suave, y claramente es fielmente plano, por lo que podemos tomar un ideal maximal $\mathfrak{P}'$ de B' cuya antiimagen en B sea $\mathfrak{P}$. La prueba de 3.47 muestra que si $B'_{\mathfrak{P}'} \longrightarrow \hat{B}'_{\mathfrak{P}'}$ es suave, también lo es $B_\mathfrak{P} \longrightarrow \hat{B}_\mathfrak{P}$. Como $B' = \hat{A}[t]$, podemos suponer que A es un anillo local completo.

Llamemos $C = B_\mathfrak{P}$. Hemos de probar que $C \longrightarrow \hat{C}$ es suave. Para ello tomamos un primo $\mathfrak{p} \in \operatorname{Esp} C$ y una extensión finita L de $k(\mathfrak{p})$. Hemos de probar que $\hat{C} \otimes_C L$ es regular. Como $k(\mathfrak{P})$ es el cuerpo de cocientes de $C/\mathfrak{p}$,

podemos tomar una $k(\mathfrak{p})$-base de L formada por elementos enteros sobre $C/\mathfrak{p}$. Sea $D \subset L$ la adjunción a $C/\mathfrak{p}$ de dicha base, con lo que D es una C-álgebra finita y L es su cuerpo de cocientes. Así, podemos ver a $\hat{C} \otimes_C L$ como la fibra genérica del homomorfismo $D \longrightarrow \hat{C} \otimes_C D = \hat{D}$. Teniendo en cuenta el teorema [E 3.47], basta probar que si $\mathfrak{Q} \in \operatorname{Esp} \hat{D}$ cumple $\mathfrak{Q} \cap D = 0$, entonces $\hat{D}_{\mathfrak{Q}}$ es regular.

En definitiva, tenemos los anillos siguientes:

$$A \longrightarrow B = A[t] \longrightarrow C = B_{\mathfrak{P}} \longrightarrow D \longrightarrow \hat{D} \longrightarrow \hat{D}_{\mathfrak{Q}}.$$

Observemos que D es un dominio íntegro, por lo que el núcleo N del homomorfismo $C \longrightarrow D$ es un ideal primo. Podemos cambiar A por $A/(A \cap N)$, B por $B/(B \cap N)$ y $\mathfrak{P}$ por $\mathfrak{P}/N$, con lo que A sigue siendo un anillo local completo, sólo que ahora es además un dominio íntegro.

Notemos que, como D es una extensión finita de C, se trata de un anillo semilocal, y la fibra de $\mathfrak{P}$ respecto al homomorfismo $C \longrightarrow D$ es $D/\mathfrak{P}D$. Por lo tanto, si I es la intersección de los ideales maximales de D, resulta que $I/\mathfrak{P}D$ es el radical de $D/\mathfrak{P}D$, luego existe un $n \geq 1$ tal que $I^n \subset \mathfrak{P}D \subset I$, luego la topología I-ádica en D coincide con la $\mathfrak{P}$-ádica, luego $\hat{D}$ es la compleción de D en el sentido usual para anillos semilocales.

Sean $X = \operatorname{Esp} D$, $X' = \operatorname{Esp} \hat{D}$ y $f : X' \longrightarrow X$ el homomorfismo natural. Basta probar que $f^{-1}[\operatorname{Reg}(X)] \subset \operatorname{Reg}(X')$, pues, como D es íntegro, tenemos que $f(\mathfrak{Q}) = 0 \in \operatorname{Reg}(X)$, y lo que queremos probar es que $\mathfrak{Q} \in \operatorname{Reg}(X')$.

Sabemos que A es J_2 por el teorema 3.32, luego también lo son B, C y D. En particular D es J_1, es decir, $\operatorname{Reg}(X)$ es abierto en X. Por otra parte, $\operatorname{Reg}(X')$ es abierto en X' de nuevo por 3.32.

Supongamos que $f^{-1}[\operatorname{Reg}(X)] \setminus \operatorname{Reg}(X') \neq \varnothing$ y vamos a llegar a una contradicción. Por el teorema anterior existe un primo $\mathfrak{p}' \in f^{-1}[\operatorname{Reg}(X)] \setminus \operatorname{Reg}(X')$ tal que $\dim \hat{D}/\mathfrak{p}' \leq 1$.

No puede suceder que el ideal $\mathfrak{p}'$ sea maximal en $\hat{D}$, ya que entonces tendríamos que $I \subset \mathfrak{p}' \cap D = f(\mathfrak{p}')$, luego $f(\mathfrak{p}')$ sería un ideal maximal de D. Si los ideales maximales de D son $\mathfrak{m}_1 = f(\mathfrak{p}'), \mathfrak{m}_2, \ldots, \mathfrak{m}_r$, según hemos visto tras la definición 1.12, $\hat{D} = \hat{D}_{\mathfrak{m}_1} \oplus \cdots \oplus \hat{D}_{\mathfrak{m}_r}$. Por la observación previa a 3.32, resulta que $\operatorname{Esp} \hat{D}$ es unión disjunta de abiertos isomorfos a los espectros de los anillos $\hat{D}_{\mathfrak{m}_i}$, y es fácil ver que, a través de estos isomorfismos, $\hat{D}_{\mathfrak{p}'} = \hat{D}_{\mathfrak{m}_1}$ (o, con más precisión: $(\hat{D})_{\mathfrak{p}'} = \widehat{D_{\mathfrak{m}_1}}$). Pero esto es contradictorio, pues tenemos que $D_{\mathfrak{m}_1}$ es regular, luego también lo es su compleción, y por otra parte tenemos que $\hat{D}_{\mathfrak{p}'}$ no es regular.

Así pues, podemos concluir que $\dim \hat{D}/\mathfrak{p}' = 1$. Llamemos $\mathfrak{p} = \mathfrak{p}' \cap D$. Estamos suponiendo que $D_{\mathfrak{p}}$ es regular pero $\hat{D}_{\mathfrak{p}'}$ no.

El homomorfismo $D_{\mathfrak{p}} \longrightarrow \hat{D}_{\mathfrak{p}'}$ es plano. Si la fibra $\hat{D}_{\mathfrak{p}'}/\mathfrak{p}\hat{D}_{\mathfrak{p}'}$ fuera regular, el mismo argumento empleado en la prueba de 3.38 nos daría que $\hat{D}_{\mathfrak{p}'}$ es regular. Así pues, $\hat{D}_{\mathfrak{p}'}/\mathfrak{p}\hat{D}_{\mathfrak{p}'} \cong (\hat{D}/\mathfrak{p}\hat{D})_{\mathfrak{p}'/\mathfrak{p}\hat{D}}$ no es regular.

Esto nos permite cambiar D por $D/\mathfrak{p}$ (luego $\hat{D}$ por $\hat{D}/\mathfrak{p}\hat{D}$, C por $C/(\mathfrak{p}\cap C)$, etc.) y suponer que $\mathfrak{p} = 0$. De este modo tenemos las inclusiones:

$$A \longrightarrow B = A[t] \longrightarrow C = B_{\mathfrak{P}} \longrightarrow D \longrightarrow \hat{D}/\mathfrak{p}',$$

donde A es un anillo local completo y D es una C-álgebra finita.

Llamemos $E = \hat{D}/\mathfrak{p}'$ y sea J la intersección de los ideales maximales de E. Recordemos que I es la intersección de los ideales maximales de D y que $\mathfrak{m}$ es el ideal maximal de A.

Como $C/\mathfrak{P}C \cong B/\mathfrak{P} = (A/\mathfrak{m})[\bar{t}]$ es un cuerpo, tenemos que $\bar{t}$ es algebraico, luego la extensión $k(\mathfrak{P})/k(\mathfrak{m})$ es finita. Como D es finito sobre C, también $D/I \cong \hat{D}/\hat{I}$ tiene dimensión finita sobre $k(\mathfrak{P})$, luego sobre $k(\mathfrak{m})$. El epimorfismo $\hat{D}/\hat{I} \longrightarrow E/J$, nos da que E/J es un $k(\mathfrak{p})$-espacio vectorial de dimensión finita. Si J^n admite un sistema generador con g elementos, tenemos una aplicación $k(\mathfrak{m})$-lineal suprayectiva $(E/J)^e \longrightarrow J^n/J^{n+1}$, lo que nos da que todos los cocientes J^n/J^{n+1} tienen dimensión finita, y lo mismo vale para E/J^n.

Vamos a probar que A es un cuerpo. En caso contrario, $\mathfrak{m} \neq 0$, luego también $\mathfrak{m}E \neq 0$. Como $\dim E = 1$, los primos minimales de $\mathfrak{m}E$ son ideales maximales, luego, $J \subset \operatorname{rad}(\mathfrak{m}E)$, con lo que existe un $n \geq 1$ tal que $J^n \subset \mathfrak{m}E$ y el epimorfismo $E/J^n \longrightarrow E/\mathfrak{m}E$ nos da que $E/\mathfrak{m}E$ es un $k(\mathfrak{m})$-espacio vectorial de dimensión finita. El teorema 2.20 nos da que E es un A-módulo finitamente generado. (Notemos que $\mathfrak{m}E \subset J$ y como, por [AC 4.21], la topología J-ádica es de Hausdorff, lo mismo vale para la topología $\mathfrak{m}$-ádica en E.)

Como A es noetheriano y $D \subset E$, resulta que D también es un A-módulo finitamente generado. Esto implica que la topología I-ádica en D coincide con la topología $\mathfrak{m}$-ádica. Por consiguiente, $\hat{D} = D \otimes_A \hat{A} = D$, luego $\mathfrak{p}' = 0$, y esto es una contradicción, ya que $\mathfrak{p}'$ no es regular.

Tenemos, pues, que A es un cuerpo, luego $\dim B \leq 1$ por [AC 4.63], luego $\dim C \leq 1$ y $\dim D \leq 1$ porque es finito sobre C (teorema [AC 3.68]). El teorema [AC 4.57], junto con las observaciones tras 1.12 nos dan que $\dim \hat{D} = 1$. Como $\mathfrak{p}'$ no es un ideal maximal, ha de ser un primo minimal. Ahora bien, A es un anillo de Nagata por 3.18, B también lo es por 3.24, C también lo es por 3.13 y D lo es también por 3.24. El teorema 3.22 nos da que $\hat{D}$ es reducido, luego $\hat{D}_{\mathfrak{p}'}$ es regular por 1.16, contradicción ∎

3.6 Anillos y esquemas excelentes

Finalmente, vamos a recoger en una definición todas las propiedades que hemos estudiado en las secciones precedentes:

Definición 3.52 Un anillo noetheriano A es *excelente* si cumple las tres propiedades siguientes:

a) es universalmente catenario,

b) tiene la propiedad J_2,

c) tiene la propiedad G.

Muchas de las propiedades de los anillos excelentes dependen únicamente de las propiedades b) y c), por lo que es conveniente llamar anillos *cuasiexcelentes* a los anillos noetherianos que cumplen estas dos propiedades, aunque no sean universalmente catenarios.

Las propiedades básicas de los anillos excelentes son consecuencias inmediatas de los teoremas que ya hemos probado. De ellas se desprende que todos la inmensa mayoría de los anillos que aparecen de forma natural en geometría algebraica son excelentes:

Teorema 3.53 *Se cumplen los hechos siguientes:*

a) Toda localización de un anillo (cuasi)excelente es también (cuasi)excelente.

b) Toda álgebra finitamente generada sobre un anillo (cuasi)excelente es también (cuasi)excelente.

c) Un anillo A es (cuasi)excelente si y sólo si lo es A/I, para todo ideal I de A, si y sólo si lo es $A/\mathfrak{P}$, para todo $\mathfrak{P} \in \operatorname{Esp} A$.

d) Todo anillo noetheriano semilocal y completo (en particular, todo cuerpo) es excelente.

e) Un anillo noetheriano local es cuasiexcelente si y sólo si tiene la propiedad G.

Demostración: a) Es consecuencia de 3.2, 3.31 y 3.45.

b) Por 3.1, 3.31 y 3.51.

c) Basta probar la equivalencia para ideales primos, pues implica trivialmente la equivalencia para ideales cualesquiera. La equivalencia es cierta para la propiedad de ser universalmente catenario, lo cual se sigue inmediatamente de la definición. Para la propiedad J_2 basta tener en cuenta la equivalencia c) en el teorema 3.30, ya que si $\mathfrak{p}/\mathfrak{P} \in \operatorname{Esp}(A/\mathfrak{P})$, entonces

$$k(\mathfrak{p}/\mathfrak{P}) = (A/\mathfrak{P})_{\mathfrak{p}/\mathfrak{P}} \,/\, (\mathfrak{p}/\mathfrak{P})(A/\mathfrak{P})_{\mathfrak{p}/\mathfrak{P}}$$

$$= (A_{\mathfrak{p}}/\mathfrak{P}A_{\mathfrak{p}}) \,/\, (\mathfrak{p}A_{\mathfrak{p}}/\mathfrak{P}A_{\mathfrak{p}}) = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} = k(\mathfrak{p}),$$

y $(A/\mathfrak{P})/(\mathfrak{p}/\mathfrak{P}) \cong A/\mathfrak{p}$, de donde se sigue que el ideal $\mathfrak{p}/\mathfrak{P}$ cumple dicha propiedad c) para $A/\mathfrak{p}$ si y sólo si la cumple $\mathfrak{p}$ para A.

Para la propiedad G basta tener en cuenta el teorema 3.45 y las observaciones posteriores.

d) Veamos en primer lugar que si A es un anillo noetheriano local y completo, entonces es excelente. Teniendo en cuenta los teoremas 3.32 y 3.48, sólo nos falta probar que A es universalmente catenario. Por el apartado c) que acabamos de

probar, basta probar que $A/\mathfrak{p}$ es universalmente catenario para todo $\mathfrak{p} \in \operatorname{Esp} A$. Como $A/\mathfrak{p}$ también es un anillo noetheriano local y completo, no perdemos generalidad si suponemos que A es un dominio íntegro. Entonces, el teorema 2.21 nos da que A es finito sobre un anillo regular, que es universalmente catenario por 3.7, luego A también es universalmente catenario.

En general, si A es semilocal, por las observaciones tras 1.12 sabemos que $A = A_1 \oplus \cdots \oplus A_n$, donde cada A_i es un anillo noetheriano local y completo (la compleción de A respecto a uno de sus ideales maximales). En particular, los A_i son anillos excelentes. Por la observación previa a 3.32, sabemos que $\operatorname{Esp} A$ es unión disjunta de abiertos isomorfos a $\operatorname{Esp} A_i$, luego la localización de A respecto a un ideal primo coincide con la localización de un A_i respecto a uno de sus ideales primos. El teorema 3.2 y la observación tras 3.45 implican que A es universalmente catenario y tiene la propiedad G. Respecto a la propiedad J_2, puesto que toda A-álgebra finita es también un anillo noetheriano semilocal y completo, basta probar que A cumple la propiedad J_1, pero es obvio que si $\operatorname{Reg}(A_i)$ es abierto en $\operatorname{Esp} A_i$, también $\operatorname{Reg}(A)$ es abierto en $\operatorname{Esp} A$.

e) Por el teorema 3.46. ∎

Un caso particular de la propiedad c) es que un anillo A es (cuasi)excelente si y sólo si lo es A_{red}.

Como ya se ha podido apreciar en las demostraciones precedentes, la propiedad de ser universalmente catenario y la propiedad G son locales, en el sentido de que A las cumple si y sólo si las cumplen las localizaciones $A_{\mathfrak{p}}$, para todo $\mathfrak{p} \in \operatorname{Esp} A$ (o incluso para todo ideal maximal de A), mientras que la propiedad J_2 es global, ya que se cumple localmente siempre que A tiene la propiedad G y eso no implica necesariamente que la cumpla A.

La propiedad de Nagata no interviene en la definición de los anillos excelentes porque es consecuencia de las otras:

Teorema 3.54 *Todo anillo cuasiexcelente es un anillo de Nagata.*

DEMOSTRACIÓN: Sea A un anillo cuasiexcelente y $\mathfrak{p} \in \operatorname{Esp} A$, sea K el cuerpo de cocientes de $A/\mathfrak{p}$, L una extensión finita de K y B la clausura entera de A en L. Hemos de probar que B es un A-módulo finitamente generado. Podemos tomar una K-base de L formada por elementos enteros sobre $A/\mathfrak{p}$. Al adjuntarlos a $A/\mathfrak{p}$ obtenemos una A-álgebra finitamente generada A' cuyo cuerpo de cocientes es L. Como A' también es un anillo cuasiexcelente, basta probar que todo dominio íntegro cuasiexcelente tiene la propiedad N_1.

Sabemos que $\operatorname{Reg}(A)$ es abierto en $\operatorname{Esp} A$, y además es no vacío porque contiene al ideal nulo, luego $\operatorname{Esp} A$ contiene, en particular, un abierto no vacío de puntos normales, que podemos tomar de la forma $\operatorname{Esp} A_f$, para cierto $f \in A$. En particular, el esquema $\operatorname{Esp} A_f$ es normal, luego A_f es íntegramente cerrado. El teorema 3.23 nos reduce el problema a demostrar que $A_{\mathfrak{m}}$ tiene la propiedad N_1 para todo ideal maximal $\mathfrak{m}$ de A.

Ahora bien, tenemos que el homomorfismo $A_{\mathfrak{m}} \longrightarrow \hat{A}_{\mathfrak{m}}$ es suave y fielmente plano, y $A_{\mathfrak{m}}$ es reducido, luego las observaciones tras 3.43 nos dan que $\hat{A}_{\mathfrak{m}}$

también es reducido, es decir, que $A_{\mathfrak{m}}$ es analíticamente no ramificado, luego tiene la propiedad N_1 por 3.20. ∎

Veamos un último ejemplo de anillos excelentes, que conecta la teoría con la geometría aritmética:

Teorema 3.55 *Todo dominio de Dedekind de característica* 0 *es excelente.*

Demostración: Sea D un dominio de Dedekind de característica 0 y sea K su cuerpo de cocientes. Si $\mathfrak{p} \in \operatorname{Esp} D$, entonces $D_{\mathfrak{p}}$ es regular,[3] luego es universalmente catenario por 3.7. Por consiguiente, 3.2 implica que D es universalmente catenario.

Para demostrar que D tiene la propiedad G basta considerar un ideal maximal $\mathfrak{p} \in \operatorname{Esp} D$ y probar que el homomorfismo $A_{\mathfrak{p}} \longrightarrow \hat{A}_{\mathfrak{p}}$ es suave. Sabemos que $A_{\mathfrak{p}}$ es un anillo de valoración discreta de característica 0, luego tenemos únicamente dos fibras. Una es la del ideal maximal, que se corresponde con el anillo

$$\hat{A}_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} (A_{\mathfrak{p}}/\mathfrak{p}) \cong \hat{A}_{\mathfrak{p}}/\mathfrak{p}\hat{A}_{\mathfrak{p}} = k(\mathfrak{p}).$$

Obviamente, $k(\mathfrak{p})$ es geométricamente regular sobre sí mismo. La otra fibra es la fibra genérica, correspondiente al anillo $\hat{K} = \hat{A}_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} K$, que no es sino el cuerpo de cocientes de $\hat{A}_{\mathfrak{p}}$, ya que se trata de una localización de este anillo en la que el generador de su único ideal maximal pasa a ser una unidad. Como K es perfecto, el teorema 3.36 nos da que $\hat{K}$ es geométricamente regular sobre K. Esto prueba que D tiene la propiedad G.

Para probar que D cumple la propiedad J_2 usaremos la caracterización c) del teorema 3.30. Tomamos un primo $\mathfrak{p} \in \operatorname{Esp} D$ y una extensión finita puramente inseparable K' de $k(\mathfrak{p})$.

Si $\mathfrak{p} = 0$ entonces ha de ser $K' = k(\mathfrak{p}) = K$ y basta tomar $D' = D \subset K'$, de forma que D', al ser regular, cumple la propiedad J_0.

La otra posibilidad es que $\mathfrak{p}$ sea un ideal maximal, en cuyo caso, $D/\mathfrak{p} = k(\mathfrak{p})$, con lo que basta tomar como D' la adjunción a $k(\mathfrak{p})$ de una base de K' formada por elementos enteros sobre D. Así, D' es una D-álgebra finita y, como también es un álgebra (íntegra) finitamente generada sobre un cuerpo, es excelente y tiene la propiedad J_0. ∎

Definición 3.56 Un esquema X es *excelente* si admite un cubrimiento por abiertos afines U_i tales que los anillos $\mathcal{O}_X(U_i)$ son excelentes.

Notemos también que, por definición, los esquemas excelentes son localmente noetherianos. El teorema siguiente muestra que si la definición se cumple con un cubrimiento abierto, se cumple con cualquier otro (que esté formado por abiertos afines noetherianos).

Teorema 3.57 *Si X es un esquema excelente y $U \subset X$ es un abierto afín, entonces el anillo $\mathcal{O}_X(U)$ es excelente.*

[3]Para más detalles sobre los dominios de Dedekind ver el principio de la sección 5.1

DEMOSTRACIÓN: Sea U_i un cubrimiento de X según la definición de esquema excelente. Para cada $x \in U$ existe un índice i tal que $x \in U \cap U_i$, luego existe un $f \in \mathcal{O}_X(U_i)$ tal que $x \in V = D(f) \subset U \cap U_i$, así, $\mathcal{O}_X(V) = \mathcal{O}_X(U_i)_f$ es un anillo excelente. Esto prueba que U es también un esquema excelente. Equivalentemente, podemos suponer que $X = U = \operatorname{Esp} A$, y hemos de probar que A es excelente.

Ciertamente, A es universalmente catenario y tiene la propiedad G, ya que ambas propiedades son locales. Falta probar que tiene la propiedad J_2. Para ello consideramos una A-álgebra B finitamente generada, y hemos de probar que tiene la propiedad J_1.

Sea $Y = \operatorname{Esp} B$. Tenemos un homomorfismo $f : Y \longrightarrow X$ de tipo finito. Para cada $y \in Y$, podemos tomar un abierto afín $y \in V_y \subset f^{-1}[U_i]$, para cierto índice i, luego Y admite un cubrimiento por abiertos afines V tales que cada $\mathcal{O}_Y(V)$ es un álgebra de tipo finito sobre un anillo $\mathcal{O}_X(U_i)$, luego los anillos $\mathcal{O}_Y(V)$ son excelentes. Esto prueba que Y es un anillo afín noetheriano y excelente, luego, cambiando X por Y, basta probar que A tiene la propiedad J_1, es decir, que el conjunto de puntos regulares de X es abierto.

Ahora bien, el conjunto de puntos regulares de X es la unión de los conjuntos de puntos regulares de los U_i, que son abiertos porque los anillos $\mathcal{O}_X(U_i)$ son excelentes. ∎

En particular, un anillo A es excelente si y sólo si el esquema $\operatorname{Esp} A$ es excelente. Ahora ya es inmediato el teorema siguiente:

Teorema 3.58 *Si X es un esquema excelente, también lo es todo abierto, todo cerrado y todo esquema de tipo finito sobre X. Además, si X es íntegro, su normalización $\pi : X' \longrightarrow X$ en cualquier extensión finita de $K(X)$ es un homomorfismo finito.*

También es evidente que, en un esquema excelente reducido, el conjunto de los puntos regulares es abierto.

Segunda parte

Superficies aritméticas

Capítulo IV

Preliminares

4.1 Curvas planas

Aquí vamos a mostrar la relación entre el tratamiento clásico de las variedades algebraicas, que es el utilizado en [CE], con el tratamiento moderno en términos de la teoría de esquemas expuesta en [E]. El lector debería tener claro que ambos son equivalentes, pero aquí se trata de explicitar esa equivalencia de cara a tratar con ejemplos concretos. Por ello nos limitaremos al caso más simple, que es el único en el que nos será útil comparar ambos planteamientos, a saber, el de las curvas planas. Todos los hechos que aquí enunciamos sin demostración, o incluso que empleamos tácitamente, son hechos con los que el lector deberá estar familiarizado, todos los cuales han sido tratados convenientemente en [AC] o [E].

A lo largo de toda esta sección K será un cuerpo arbitrario, $\bar{K}$ será su clausura algebraica y $F(X,Y,Z) \in K[X,Y,Z]$ será un polinomio homogéneo no constante.

Recordemos que, en términos clásicos, el *conjunto algebraico proyectivo* C/K definido por F es el conjunto $V(F)$ formado por todos los puntos del plano proyectivo $\mathrm{P}^2(\bar{K})$ cuyas coordenadas homogéneas cumplen $F(X,Y,Z) = 0$. Decimos que es un conjunto *"definido sobre K"* para expresar que la ecuación que lo define tiene sus coeficientes en K. Los puntos de C que admiten un sistema de coordenadas homogéneas en K^3 se llaman *puntos racionales* de C/K.

A la hora de estudiar propiedades locales de los puntos de C, podemos restringirnos a un abierto afín deshomogeneizando la ecuación. Más detalladamente, todo punto de $\mathrm{P}^2(\bar{K})$ tiene al menos una coordenada no nula. Supongamos, por ejemplo, que queremos estudiar un punto que cumple $Z \neq 0$. Entonces podemos identificar el plano afín $A^2(\bar{K})$ con el abierto $D(Z) \subset \mathrm{P}^2(\bar{K})$ formado por los puntos cuya tercera coordenada homogénea es no nula. Concretamente, la identificación es

$$(x,y) \mapsto (x,y,1), \qquad (x,y,z) \mapsto (x/z, y/z).$$

Una vez fijada la identificación $A^2(\bar{K}) = D(Z)$, es costumbre llamar "puntos finitos" a los puntos de $A^2(\bar{K})$ y "puntos infinitos" a los de la "recta del infinito" $V(Z)$, aunque hemos de tener presente que podríamos haber elegido cualquier recta de $\mathrm{P}^2(\bar{K})$ como "recta del infinito", a la hora de identificar $A^2(\bar{K})$ con un abierto afín en $\mathrm{P}^2(\bar{K})$.

El abierto afín $U = C \cap A^2(\bar{K})$, es decir, el abierto de los puntos finitos de C, es el conjunto $U = V(f)$ formado por los puntos de $A^2(\bar{K})$ que cumplen la ecuación $f(X, Y) = 0$, donde $f(X, Y) = F(X, Y, 1)$ es la deshomogeneización de F respecto de Z. Los puntos racionales de U son los puntos de U cuyas coordenadas (afines) son racionales.

En términos de la teoría de esquemas, el *conjunto algebraico proyectivo* C/K definido por F es el esquema

$$C = \mathrm{Proy}(K[X, Y, Z]/(F)).$$

Ahora, el hecho de que C *"está definido sobre* K*"* significa que el homomorfismo natural $K \longrightarrow K[X, Y, Z]/(F)$ induce un homomorfismo de esquemas $C \longrightarrow \mathrm{Esp}\, K$ al que llamamos *homomorfismo estructural* de C/K.

Los puntos de C son ahora los ideales primos homogéneos (es decir, generados por un conjunto de polinomios homogéneos) de $K[x, y, z] = K[X, Y, Z]/(F)$ distintos de $M = (x, y, z)$. (Notemos que, por ser homogéneo, todo $\mathfrak{p} \in C$ cumple $\mathfrak{p} \subsetneq (x, y, z)$.) Los puntos *cerrados* de C son los ideales "maximales" en el sentido de que no están estrictamente contenidos en otro ideal de C.

Según acabamos de indicar, un punto de C no puede contener a x, y, z. Si, por ejemplo, no contiene a z, esto significa, por definición, que pertenece al abierto afín $U = D(z)$, que se identifica de forma natural con

$$U = \mathrm{Esp}\, K[\bar{x}, \bar{y}],$$

donde $K[\bar{x}, \bar{y}] = K[x, y, z]_{(z)}$ es el anillo de cocientes de grado 0 en la localización $K[x, y, z]_z$, cuyos generadores son $\bar{x} = x/z$, $\bar{y} = y/z$. La inmersión abierta $U \longrightarrow C$ está inducida por el homomorfismo

$$\phi : K[x, y, z] \longrightarrow K[\bar{x}, \bar{y}]$$

dado por $x \mapsto \bar{x}$, $y \mapsto \bar{y}$, $z \mapsto 1$. En la práctica, basta tener en cuenta que

$$K[\bar{x}, \bar{y}] \cong K[X, Y]/(f),$$

donde f es la deshomogeneización de F respecto de Z. Como aquí sólo vamos a trabajar explícitamente con los puntos de C identificándolos con puntos de U, a partir de aquí escribiremos x e y en lugar de $\bar{x}$ y $\bar{y}$ e identificaremos $K[x, y] = K[X, Y]/(f)$. Los puntos de U son los ideales primos de $K[x, y]$, que son de la forma $\mathfrak{p} = \mathfrak{P}/(f)$, donde $\mathfrak{P}$ es un ideal primo de $K[X, Y]$ que contiene a f. Los puntos cerrados de U son los ideales maximales de $K[x, y]$, que se corresponden con los ideales maximales de $K[X, Y]$ que contienen a f.

De este modo, el esquema U es el análogo abstracto del conjunto $U \subset A^2(\bar{K})$ en sentido clásico. Para relacionar ambos conjuntos observamos en primer lugar que cada punto racional $(a,b) \in U \subset A^2(\bar{K})$ determina un punto cerrado de C, a saber, el ideal $\mathfrak{p} = (x-a, y-b)$. Notemos que $\mathfrak{p}$ es un ideal maximal, porque $K[x,y]/\mathfrak{p} \cong K$. De hecho, esto significa que $\mathfrak{p}$ es un punto racional de U en el sentido de la teoría de esquemas.

En efecto, por definición, $\mathfrak{p} \in U$ es un *punto racional* si

$$k(\mathfrak{p}) = \mathcal{O}_{U,\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}} = K,$$

donde $\mathcal{O}_{U,\mathfrak{p}} = K[x,y]_{\mathfrak{p}}$, pero entonces existen $(a,b) \in K^2$ tales que $x-a \in \mathfrak{m}_{\mathfrak{p}}$, $y-b \in \mathfrak{m}_{\mathfrak{p}}$, pero esto implica que $x-a,\ y-b \in \mathfrak{p}$, luego $\mathfrak{p} = (x-a, y-b)$. Recíprocamente, si $\mathfrak{p}$ es un ideal maximal de $K[x,y]$, se cumple que

$$k(\mathfrak{p}) \cong K[x,y]/\mathfrak{p}.$$

(Más en general: si $\mathfrak{p}$ es un ideal primo arbitrario, el miembro izquierdo es el cuerpo de cocientes del miembro derecho), luego si $\mathfrak{p}$ cumple $K[x,y]/\mathfrak{p} \cong K$, entonces es racional. Con esto hemos probado que la aplicación

$$(a,b) \mapsto (x-a, y-b)$$

biyecta los puntos $(a,b) \in K^2$ que cumplen la ecuación $f(X,Y) = 0$ con los puntos racionales del esquema afín U. Los demás puntos que cumplen la ecuación se corresponden con los demás puntos cerrados de U, pero no de forma biyectiva. Para entender la situación consideramos la extensión de constantes

$$U_{\bar{K}} = \operatorname{Esp} \bar{K}[x,y] = \operatorname{Esp}(\bar{K}[X,Y]/(f)).$$

Se trata del esquema análogo a U que resulta de cambiar K por $\bar{K}$. Como K era un cuerpo arbitrario, todo lo que hemos visto para U vale también para el esquema $U_{\bar{K}}$. La diferencia es que, por una parte, todos los puntos del conjunto algebraico U (en sentido clásico) son trivialmente racionales respecto de $\bar{K}$ y, por otra parte, los puntos cerrados del esquema $U_{\bar{K}}$ coinciden con los puntos racionales. Esto es porque, en general, si $\mathfrak{p}$ es un punto cerrado, la extensión de cuerpos $k(\mathfrak{p})/K$ es finita, luego, para el caso de $\bar{K}$, ha de ser trivial.

Por consiguiente, tenemos que los puntos de $U \subset A^2(\bar{K})$, es decir, los puntos de $A^2(\bar{K})$ que cumplen la ecuación $f(X,Y) = 0$, se corresponden biunívocamente con los puntos cerrados de $U_{\bar{K}}$.

Por otra parte, los puntos de $U_{\bar{K}}$ se relacionan con los de U a través de la proyección $p : U_{\bar{K}} \longrightarrow U$ inducida por el homomorfismo natural

$$\phi : K[x,y] \longrightarrow \bar{K}[x,y]$$

inducido por la inclusión $K[X,Y] \subset \bar{K}[X,Y]$. (Concretamente, $p(\mathfrak{p}) = \phi^{-1}[\mathfrak{p}]$.) Esta aplicación es finita y suprayectiva, pero no inyectiva, y transforma puntos cerrados en puntos cerrados, por lo que cada punto cerrado de U se corresponde con un número finito de puntos cerrados de $U_{\bar{K}}$.

Conviene observar que, más en general, tenemos definida $p : C_{\bar{K}} \longrightarrow C$, de modo que $U_{\bar{K}} = p^{-1}[U]$ y la proyección sobre $U_{\bar{K}}$ que estamos considerando es la restricción de la proyección sobre $C_{\bar{K}}$.

Observemos ahora que cada punto racional de C tiene una única antiimagen en $C_{\bar{K}}$. En efecto, como $U_{\bar{K}} = p^{-1}[U]$, podemos trabajar con U y $U_{\bar{K}}$. Según hemos visto, un punto racional de U es de la forma $\mathfrak{p} = (x-a, y-b) \subset K[x,y]$, para ciertos $a, b \in K$, y su única antiimagen en $U_{\bar{K}}$ es $\mathfrak{p}' = (x-a, y-b) \subset \bar{K}[x,y]$. En efecto, tenemos que $\mathfrak{p} \subset \phi^{-1}[\mathfrak{p}']$, luego $\mathfrak{p} = \phi^{-1}[\mathfrak{p}'] = p(\mathfrak{p}')$. Por otra parte, si $p(\mathfrak{q}) = \mathfrak{p}$, entonces $x-a$, $y-b \in \mathfrak{q}$, luego ha de ser $\mathfrak{q} = \mathfrak{p}'$.

De este modo, si identificamos cada punto racional de U con su única antiimagen en $U_{\bar{K}}$, tenemos que la biyección entre los puntos de U en sentido clásico y los puntos cerrados de $U_{\bar{K}}$ como esquema extiende a la biyección entre los puntos racionales de U en sentido clásico y los puntos racionales de U como esquema.

Ejemplo Consideremos el caso concreto en el que $U/\mathbb{R}$ es el esquema afín (o el conjunto algebraico afín en sentido clásico) definido por la ecuación $X^2+Y^2 = 1$.

El punto racional $(1,0) \in U$ se corresponde con el ideal $(x-1, y)$, mientras que el par de puntos conjugados $(2, \pm\sqrt{3}\,i)$ se corresponde con los ideales

$$\mathfrak{p}_1 = (x-2, y+\sqrt{3}\,i), \qquad \mathfrak{p}_2 = (x-2, y-\sqrt{3}\,i)$$

de $U_{\mathbb{C}}$, los cuales se corresponden ambos con el punto cerrado $\mathfrak{p} = (x-2, y^2+3)$ de U. En efecto, $\mathfrak{p}$ es un ideal maximal de $k[x,y]$, pues $k[x,y]/\mathfrak{p} \cong \mathbb{C}$ y, como $y^2+3 = (y+\sqrt{3}\,i)(y-\sqrt{3}\,i) \in \mathfrak{p}_i$, tenemos que $\mathfrak{p} \subset p(\mathfrak{p}_i)$, luego, por la maximalidad, $p(\mathfrak{p}_i) = \mathfrak{p}$. Recíprocamente, un ideal $\mathfrak{q} \in U_{\mathbb{C}}$ tal que $p(\mathfrak{q}) = \mathfrak{p}$ ha de contener a $x-2$ y a $(y+\sqrt{3}\,i)(y-\sqrt{3}\,i)$ luego, al ser primo, ha de contener a uno de los dos elementos $y \pm \sqrt{3}\,i$, luego ha de ser $\mathfrak{q} = \mathfrak{p}_i$, para un i. ∎

Volviendo al esquema proyectivo C/K, sus puntos no cerrados se corresponden con los factores irreducibles del polinomio F. Observemos que son todos homogéneos, porque si $f = f_1^{r_1} \cdots f_n^{r_n}$ es la descomposición de f en factores irreducibles en $K[X,Y]$ y llamamos f_i^* a la homogeneización de f_i respecto de Z, ésta es irreducible en $K[X,Y,Z]$ y $F = f_1^{*r_1} \cdots f_n^{*r_n} Z^{r_{n+1}}$ (con $r_{n+1} \geq 0$) es la descomposición de F en factores irreducibles en $K[X,Y,Z]$. Llamemos $F_i = f_i^*$ y $F_{n+1} = Z$ si es que $r_{n+1} > 0$. Así, $F = F_1^{r_1} \cdots F_m^{r_m}$, donde cada F_i es un polinomio homogéneo irreducible (y m es n o $n+1$).

El ideal $\mathfrak{p}_i = (F_i)/(F) = (F_i(x,y,z))$ es un ideal primo de $K[x,y,z]$ y, como todo punto de C contiene a $f(x,y,z)$, también ha de contener a uno de los $\mathfrak{p}_i$. Por consiguiente, si $\Gamma_i = V(\mathfrak{p}_i)$ es el conjunto de puntos de C que contienen a $\mathfrak{p}_i$, tenemos que

$$C = \Gamma_1 \cup \cdots \cup \Gamma_m$$

es la descomposición de C en componentes irreducibles. Los puntos de Γ_i se corresponden con los ideales homogéneos de $K[X,Y,Z]$ que contienen a F_i, luego

podemos identificar a Γ_i con el esquema proyectivo íntegro

$$\Gamma_i = \mathrm{Proy}(K[X,Y,Z]/(F_i)).$$

Tenemos, pues, que los puntos $\mathfrak{p}_i$ son los puntos genéricos de las componentes irreducibles de C, es decir, los puntos cuasigenéricos de C.

Cada componente Γ_i corta a $D(z)$ salvo si $F_i = Z$. Excluyendo este caso, las intersecciones $\Gamma_i \cap D(z)$ son las componentes irreducibles de U. Más concretamente, si $\mathfrak{p}_i = (f_i^*(x,y,z))$, entonces, a través de la inmersión abierta $U \longrightarrow C$, el punto $\mathfrak{p}_i$ se corresponde con $\mathfrak{p}_i = (f_i(x,y))$ y $\Gamma_i \cap D(z) = V(\mathfrak{p}_i)$, entendido ahora como el conjunto de puntos de U que contienen a $\mathfrak{p}_i$. Así pues, la descomposición en componentes irreducibles de U es

$$U = \Gamma_1 \cup \cdots \cup \Gamma_n,$$

donde Γ_i se identifica con el esquema afín íntegro $\Gamma_i = \mathrm{Esp}(K[X,Y]/(f_i))$. Las álgebras $K[X,Y]/(f_i)$ tienen todas dimensión 1 (por ejemplo, por [AC 4.58], teniendo en cuenta que $K[X,Y]$ tiene dimensión 2). Por lo tanto, sus únicos ideales primos aparte del ideal nulo (que se corresponde con el ideal $\mathfrak{p}_i$ de U) son maximales, y se corresponden con puntos cerrados de U.

Así pues, los únicos puntos de U son los puntos cerrados y sus puntos cuasigenéricos, y lo mismo vale para C. Incidentalmente, esto prueba que C tiene dimensión 1 (y, más precisamente, que todas las componentes irreducibles de C tienen dimensión 1), lo cual es, por otra parte, una consecuencia general del hecho de que C es una hipersuperficie.

En todo este libro, llamaremos *curva* a cualquier conjunto algebraico (es decir, un esquema de tipo finito sobre un cuerpo) cuyas componentes irreducibles tienen todas dimensión 1, sin exigir que sea reducido o irreducible.

En estos términos, C es una curva proyectiva y U es una curva afín.

Observemos que, términos clásicos, no hay diferencia entre el conjunto algebraico proyectivo definido por las ecuaciones

$$F_1^{r_1} \cdots F_m^{r_m} = 0 \quad \text{y} \quad F_1 \cdots F_m = 0,$$

mientras que los esquemas

$$\mathrm{Proy}(K[X,Y,Z]/(F_1^{r_1} \cdots F_m^{r_m})) \quad \text{y} \quad \mathrm{Proy}(K[X,Y,Z]/(F_1 \cdots F_m))$$

no son isomorfos (salvo en el caso obvio en que todos los exponentes son 1). Por ello, cuando hablemos de "la curva definida por la ecuación $F = 0$", entendida como un esquema, deberemos tener presente que, en realidad, nos referimos a la curva definida por el polinomio F, y no por ningún otro polinomio que dé lugar a una ecuación equivalente, por ejemplo, alterando los exponentes de sus factores irreducibles.

Lo que sucede es que, en la curva definida por $F_1^{r_1}\cdots F_m^{r_m}$, la componente irreducible Γ_i tiene multiplicidad r_i, pero dejamos para la sección 4.2 la discusión del concepto de multiplicidad de una componente irreducible, pues es más conveniente hacerlo en términos de divisores.

El teorema [AC 5.73] conecta la noción clásica de regularidad con el concepto abstracto definido en [AC]. Vamos a particularizarlo al caso de curvas planas:

Teorema 4.1 (Criterio jacobiano para curvas planas) *Sea K un cuerpo algebraicamente cerrado, sea $U = \operatorname{Esp} A$, donde $A = K[X,Y]/(f)$, para cierto polinomio $f \in K[X,Y]$ no constante. Sea $\mathfrak{p} = \mathfrak{P}/(f)$ un punto cerrado de U, donde $\mathfrak{P} = (X-a, Y-b)$ es un ideal maximal de $K[X,Y]$. Entonces, el punto $\mathfrak{p}$ es regular en U si y sólo si alguna de las derivadas*

$$\left.\frac{\partial f}{\partial X}\right|_{(a,b)}, \quad \left.\frac{\partial f}{\partial X}\right|_{(a,b)}$$

es no nula.

En efecto, basta observar que a y b son los valores definidos como $(\xi_1,\ldots,\xi_n)$ antes de [AC 5.73], con lo que la matriz $J(\mathfrak{p})$ definida allí es el vector formado por las dos derivadas del enunciado. Por otra parte, es claro que $\dim \mathcal{O}_{U,\mathfrak{p}} = 1$, luego, por la primera nota posterior a [AC 5.73], la regularidad de $\mathfrak{p}$ equivale a que este vector tenga rango 1, es decir, a que alguna de las dos derivadas no sea nula.

Para referencias posteriores, enunciamos como teorema la fórmula deducida en la nota tras el teorema [E 3.34]:

Teorema 4.2 *Si C/K es una curva proyectiva plana de grado d, su género aritmético es*

$$p_a = \binom{d-1}{2} = \frac{(d-1)(d-2)}{2}.$$

4.2 Divisores

En esta sección recogeremos algunos resultados sobre divisores en esquemas contenidos explícita o implícitamente en [E] junto con alguno nuevo.

Recordemos ([E 8.20]) que un divisor de Cartier D en un esquema localmente noetheriano X está determinado por una familia de pares (U_i, f_i), donde los abiertos U_i son un cubrimiento de X y cada f_i es un cociente de elementos regulares de $\mathcal{O}_X(U_i)$ (que cumplen una condición de compatibilidad). El divisor D es entero si los f_i son elementos regulares de $\mathcal{O}_X(U_i)$. El conjunto $\operatorname{Div}_c(X)$ formado por los divisores de Cartier de X tiene una estructura natural de grupo abeliano.

Cada divisor de Cartier tiene asignado un haz coherente $\mathcal{O}_X(D^{-1})$ (definición [E 8.27]) determinado por que $\mathcal{O}_X(D^{-1})|_{U_i} = f_i\mathcal{O}_X(U_i)$. Si D es entero,

entonces $\mathcal{O}_X(D^{-1})$ es un haz coherente de ideales de $\mathcal{O}_X$, luego, según el teorema [E 5.10], determina un subesquema cerrado de X, que representaremos por $(D, \mathcal{O}_D)$.

Notemos que D, considerado como subconjunto de X, está formado por los puntos $P \in X$ tales que $\mathcal{O}_X(D^{-1})_P \neq \mathcal{O}_{X,P}$, lo que equivale a que f_{iP} no sea una unidad en $\mathcal{O}_{X,P}$ (donde i es un índice tal que $P \in U_i$), y esto equivale a que P pertenezca al soporte de D, considerado como divisor (definición [E 8.22]). El haz $\mathcal{O}_D$ está determinado por que, para cada abierto afín $U \subset X$, tenemos que $\mathcal{O}_D(U \cap D) = \mathcal{O}_X(U)/\mathcal{O}_X(D^{-1})(U)$. En particular, si $P \in D$, se cumple que $\mathcal{O}_{D,P} = \mathcal{O}_{X,P}/\mathcal{O}_X(D^{-1})_P$.

Ejemplo Las curvas planas son un caso particular de la situación que acabamos de describir. En efecto, en el caso afín tomamos $X = A^2_K = \operatorname{Esp} K[X,Y]$. Cada $f \in K[X,Y]$ puede identificarse con el divisor de Cartier D determinado por un único abierto $U = X$ y $f \in \mathcal{O}_X(X)$. El haz coherente asociado es $\mathcal{O}_X(D^{-1}) = f\mathcal{O}_X(X) = (f)$, y el esquema que determina es

$$D = \operatorname{Esp}(K[X,Y]/(f)),$$

es decir, la curva plana determinada por f.

En el caso proyectivo partimos de $X = \mathrm{P}^2_K = \operatorname{Proy}(K[X,Y,Z])$. Cada polinomio homogéneo $F \in K[X,Y,Z]$, de grado n, determina un divisor de Cartier entero D tomando como abiertos $U_1 = D(X)$, $U_2 = D(Y)$, $U_3 = D(Z)$ y, en cada uno de ellos, $f_1 = F/X^n$, $f_2 = F/Y^n$, $f_3 = F/Z^n$.

Recordemos que, por ejemplo, $\mathcal{O}_X(U_1) = K[X,Y,Z]_{(X)}$ es el anillo de los cocientes de grado 0 en la localización $K[X,Y,Z]_X$. Este anillo es isomorfo a $K[Y,Z]$ y, a través del isomorfismo, f_1 se corresponde con la deshomogeneización de F respecto de la variable X. Lo mismo vale para los otros dos abiertos.

Los tres pares (U_i, f_i) determinan ciertamente un divisor de Cartier porque, por ejemplo, $f_1/f_2 = (Y/X)^n$ es una unidad en $\mathcal{O}_X(U_1 \cap U_2)$, pues, a través de la identificación $\mathcal{O}_X(U_1) \cong K[Y,Z]$, tenemos que U_1 se identifica con $\operatorname{Esp} K[Y,Z]$ y $U_1 \cap U_2$ se identifica con el abierto principal $D(Y)$, luego $\mathcal{O}_X(U_1 \cap U_2)$ se identifica con la localización $K[Y,Z]_Y$, y f_1/f_2 es claramente una unidad de este anillo.

Ahora, el haz $\mathcal{O}_X(D^{-1})$ está determinado por que $\mathcal{O}_X(D^{-1})|_{U_i} = (f_i)$, luego $D \cap U_i$ es la curva afín definida por el polinomio f_i. Más precisamente, si llamamos $Y = \operatorname{Proy}(K[X,Y,Z]/(F))$, tenemos inmersiones cerradas

$$i : D \longrightarrow \mathrm{P}^2_K, \qquad j : Y \longrightarrow \mathrm{P}^2_K,$$

de modo que $D \cap U_i \cong Y \cap U_i$, y es fácil ver que los isomorfismos coinciden en las intersecciones, de modo que determinan un isomorfismo $D \cong Y$. ∎

En el teorema siguiente recogemos algunas propiedades de la estructura de esquema de un divisor.

Teorema 4.3 *Sea X un esquema irreducible localmente noetheriano y sea $D \in \operatorname{Div}_c(X)$ un divisor entero no trivial, considerado como subesquema cerrado de X.*

a) Las componentes irreducibles de D tienen codimensión 1 en X.

b) La inmersión $i : D \longrightarrow X$ es regular.

c) Si X es regular, entonces D es un esquema de Cohen-Macaulay, es decir, que los anillos $\mathcal{O}_{D,P}$ son de Cohen-Macaulay. En particular, los únicos puntos asociados de D (definición [E 3.18]*) son sus puntos cuasigenéricos.*

d) La misma conclusión es válida si X es normal y $\dim X \leq 2$.

DEMOSTRACIÓN: Hemos visto que D, como conjunto, coincide con el soporte de D como divisor, luego a) es el teorema [E 8.29].

b) Para todo $P \in D$, el núcleo de $\mathcal{O}_{X,P} \longrightarrow \mathcal{O}_{D,P}$ es $\mathcal{O}_X(D^{-1})_P$, que está generado por un elemento regular de $\mathcal{O}_{X,P}$, luego, por definición, la inmersión cerrada es regular.

c) Las inmersiones regulares son localmente intersecciones completas, luego el teorema [E 7.68] implica que D es un esquema de Cohen-Macaulay. El teorema [AC 5.38] implica que los puntos asociados de D coinciden con sus puntos cuasigenéricos.

d) Si $P \in D$, entonces $\mathcal{O}_{X,P}$ es un dominio íntegramente cerrado de dimensión ≤ 2. Por el teorema 1.18 tiene la propiedad S_2, luego es un anillo de Cohen-Macaulay y, por [AC 5.37], también lo es $\mathcal{O}_{D,P}$. ∎

Observemos que, en las condiciones del teorema anterior, si $D \mid E$ son dos divisores enteros, tenemos que $E = DF$, para un tercer divisor entero F, luego

$$\mathcal{O}_X(E^{-1}) \cong \mathcal{O}_X(D^{-1}) \otimes_{\mathcal{O}_X} \mathcal{O}_X(F^{-1}) \cong \mathcal{O}_X(D^{-1})\mathcal{O}_X(F^{-1}) \subset \mathcal{O}_X(D^{-1})$$

(El último isomorfismo se sigue fácilmente de que los haces de ideales son localmente libres de rango 1.) Esto implica a su vez que existe una inmersión cerrada natural $i : D \longrightarrow E$.

Los puntos (o, equivalentemente, los subespacios cerrados irreducibles) de codimensión 1 en X se llaman divisores primos de X, y los productos formales de divisores primos con exponentes enteros se llaman divisores de Weil de X. Si $P \in X$ es un divisor primo, está definido ([E 8.26]) un homomorfismo de grupos $v_P : \mathrm{Div}_c(X) \longrightarrow \mathbb{Z}$ tal que, si D es un divisor entero,

$$v_P(D) = l(\mathcal{O}_{X,P}/\mathcal{O}_X(D^{-1})_P).$$

Más concretamente, si (U_i, f_i) es uno de los pares que definen al divisor D tal que $P \in U_i$, con lo que $f_i \in \mathcal{O}_X(U_i)$ (porque D es entero) y $f_{i,P} \in \mathcal{O}_{X,P}$, podemos escribir

$$v_P(D) = l(\mathcal{O}_{X,P}/(f_{i,P})).$$

Las observaciones posteriores a [E 8.26] muestran cómo calcular esta longitud cuando X es noetheriano y normal. En tal caso, $\mathcal{O}_{X,P}$ es un anillo de valoración discreta, $\mathfrak{m}_P = (\pi)$, para cierto primo π, y $v_P(D) = v_\pi(f_{i,P})$ no es sino el exponente de π en $f_{i,P}$. (En realidad, no es necesario que X sea normal, sino

que basta con que sea normal en codimensión 1, es decir, que los puntos de codimensión 1 sean normales.)

De aquí se sigue que si X es noetheriano y normal en codimensión 1, entonces $v_P(D) = 0$ excepto si $P \in D$, en cuyo caso P es un punto cuasigenérico de D como subesquema de X. Más en general, aunque X no sea normal o D no sea entero, se cumple que $v_P(D) = 0$ salvo para un número finito de divisores primos, por lo que los homomorfismos v_P determinan un homomorfismo $\mathrm{Div}_c(X) \longrightarrow \mathrm{Div}(X)$ entre el grupo de los divisores de Cartier y el grupo de los divisores de Weil de X. Si además X es regular, entonces es un isomorfismo.

Para referencias posteriores recogemos en un teorema parte de la discusión precedente:

Teorema 4.4 *Si X es un esquema noetheriano y normal en codimensión 1, cada divisor de Cartier D puede identificarse con un divisor de Weil, de modo que si P es un divisor primo su exponente en D es $v_P(D) = v_P(D_P)$, donde v_P es la valoración del anillo de valoración discreta $\mathcal{O}_{X,P}$ y D_P es la localización a P de cualquier función que defina al divisor D en un entorno de P. Si D es entero podemos considerar a D como subesquema cerrado de X, y $v_P(D)$ es entonces la multiplicidad de P como componente irreducible de D.*

Ejemplo Si $X = \mathrm{P}^2_K$, los divisores primos de X se corresponden biunívocamente con los ideales principales (F), donde $F \in K[X,Y,Z]$ es un polinomio homogéneo irreducible. Cada cada polinomio homogéneo se descompone en producto de factores irreducibles, los cuales son también homogéneos, digamos $F = F_1^{r_1} \cdots F_m^{r_m}$, con lo que podemos asociar a F el divisor de Weil entero

$$D = (F_1)^{r_1} \cdots (F_m)^{r_m}.$$

Es claro que todo divisor de Weil entero es de esta forma, y que dos polinomios homogéneos F y G determinan el mismo divisor de Weil si y sólo si se diferencian en una unidad, es decir, si $(F) = (G)$. Así pues, los divisores de Weil enteros de P^2_K se corresponden biunívocamente con los ideales principales homogéneos de $K[X,Y,Z]$. Por otra parte, en el ejemplo precedente habíamos asignado un divisor de Cartier entero a cada polinomio homogéneo F. Vamos a probar ahora que uno y otro se corresponden a través del isomorfismo natural entre los divisores de Cartier y los divisores de Weil de P^2_K.

En efecto, llamemos D al divisor de Cartier asociado al polinomio homogéneo $F = F_1^{r_1} \cdots F_m^{r_m}$. Hemos visto que, como esquema, se corresponde con

$$D = \mathrm{Proy}(K[X,Y,Z]/(F)),$$

luego los únicos divisores de Weil P para los que $v_P(D) \neq 0$ son los puntos cuasigenéricos de esta curva plana, que, según hemos visto, son los ideales primos $(F_i)/(F)$. Vistos como puntos de X, son los ideales primos $P_i = (F_i)$.

Notemos que $v_{P_i}(D)$ depende únicamente de $\mathcal{O}_{X,P_i}$, luego, para calcularlo, podemos restringirnos a un entorno afín de P_i. Si suponemos, por ejemplo,

que $F_i \neq Z$, podemos restringirnos al abierto principal $D(Z) = A^2_K$. Sabemos que $D \cap Z$ es la curva plana en A^2_K determinada por la deshomogeneización $f(X,Y) = F(X,Y,1)$ o, también, el divisor de Cartier asociado a f en A^2_K.

La descomposición de f en factores irreducibles en $K[X,Y]$ es $f = f_1^{r_1} \cdots f_n^{r_n}$, donde $n = m$ si Z no aparecía entre los factores irreducibles de F o bien $n = m-1$ si $F_m = Z$. En cualquier caso, el divisor primo P_i, como punto de A^2_K, es $P_i = (f_i)$. Ahora basta observar que, en $\mathcal{O}_{X,P_i} = K[X,Y]_{f_i}$, se cumple que $\mathfrak{m}_{P_i} = (f_i)$, luego $v_{P_i}(D) = v_{f_i}(f) = r_i$.

Así pues, el divisor de Weil asociado al divisor de Cartier D asociado a F resulta ser $D = (F_1)^{r_1} \cdots (F_m)^{r_m}$. También hemos probado el resultado análogo para divisores de A^2_K. ∎

El ejemplo anterior muestra cómo los exponentes los factores irreducibles de un polinomio están determinados por el divisor asociado al polinomio, aunque en realidad hemos probado que, de hecho, están determinados por la estructura de esquema asociada al divisor. La mejor forma de explicitarlo es a través de la noción de multiplicidad de una componente irreducible:

Definición 4.5 Si X es un esquema y Γ es una componente irreducible con punto genérico ξ, el anillo $\mathcal{O}_{X,\xi}$ tiene dimensión 0, luego tiene longitud finita, y dicha longitud se llama la *multiplicidad* de Γ en X.

Si D es un divisor de Cartier entero en un esquema noetheriano y normal X y P es el punto genérico de una componente irreducible Γ de D, considerado como subesquema cerrado de D, entonces la multiplicidad de Γ en D es

$$l(\mathcal{O}_{D,P}) = l(\mathcal{O}_{X,P}/\mathcal{O}_X(D^{-1})_P) = v_P(D).$$

Vemos, pues, que el divisor de Weil asociado a D está completamente determinado por la estructura de esquema de D (pues el exponente en D de cada divisor primo es su multiplicidad en D como esquema).

Teorema 4.6 *Sea X un esquema regular y D un divisor de Cartier (considerado como subesquema cerrado de X). Un punto $x \in D$ cumple que $\mathcal{O}_{D,x}$ es reducido si y sólo si pertenece únicamente a componentes irreducibles de multiplicidad 1 en D. En particular, D es reducido si y sólo si todas sus componentes irreducibles tienen multiplicidad 1.*

Demostración: Pongamos que D está definido por $f \in \mathcal{O}_{X,x}$ en un entorno de x, de modo que $\mathcal{O}_{D,x} = \mathcal{O}_{X,x}/(f)$.

Como $\mathcal{O}_{X,x}$ es un dominio de factorización única, podemos descomponer $f = \epsilon\pi_1^{r_1} \cdots \pi_m^{r_m}$, donde los $\pi_i \in \mathcal{O}_{X,x}$ son primos no asociados dos a dos y ϵ es una unidad. Podemos tomar un entorno afín U de x tal que f, ϵ y π_i sean localizaciones de funciones de $\mathcal{O}_X(U)$ y de modo que la factorización de f sea válida también en $\mathcal{O}_X(U)$. Sea $\mathfrak{q}$ el ideal primo de $\mathcal{O}_X(U)$ que se corresponde con x.

Los ideales $\mathfrak{p}_i = (\pi_i) \subset \mathcal{O}_{X,x}$ son los primos minimales de f, y se corresponden con los primos minimales de f en $\mathcal{O}_X(U)$ contenidos en $\mathfrak{q}$, los cuales, a su

vez, se corresponden con los primos minimales de $\mathcal{O}_X(U)/(f) = \mathcal{O}_D(U \cap D)$ contenidos en $\mathfrak{q}/(f)$, que son los puntos genéricos de las componentes irreducibles de D que contienen a x. Así pues, la multiplicidad de cada una de esas componentes es $v_{\pi_i}(f) = r_i$. Así pues, las componentes irreducibles tienen multiplicidad 1 si y sólo si f es libre de cuadrados en $\mathcal{O}_{X,x}$, lo cual equivale claramente a que $\mathcal{O}_{D,x}$ sea reducido. ∎

Observemos que, en este teorema, la hipótesis de que las componentes irreducibles de D tengan multiplicidad 1 equivale a que el divisor de Weil asociado a D sea libre de cuadrados. En particular, la estructura de esquema asociada al divisor de Cartier asociada a un divisor primo es la estructura de subesquema cerrado reducido.

Nota Una consecuencia útil del teorema anterior es la siguiente: manteniendo las mismas hipótesis, sea Γ una componente conexa de D con multiplicidad 1. Sea $i : \Gamma \longrightarrow D$ la inmersión cerrada correspondiente a la estructura de subesquema cerrado reducido, sea $U \subset D$ el complementario de la unión de las componentes irreducibles de D distintas de Γ y sea $\Gamma_0 = i^{-1}[U]$, es decir, el abierto que resulta de quitarle a Γ los puntos donde corta a otras componentes. La restricción $i|_{\Gamma_0} : \Gamma_0 \longrightarrow U$ es también una inmersión cerrada, pero ahora es biyectiva y ambos esquemas son reducidos. Por la unicidad de la estructura de subesquema cerrado reducido, ha de ser un isomorfismo y, como aplicación $i|_{\Gamma_0} : \Gamma_0 \longrightarrow D$ es una inmersión abierta. De este modo, los puntos de Γ_0, como puntos de D, no sólo son reducidos, sino que tienen todas las propiedades locales que tengan como puntos de Γ con la estructura de subesquema cerrado reducido. ∎

Ejemplo Consideremos la curva plana $D = \mathrm{Esp}(K[X,Y]/(XY^2))$. Claramente tiene dos componentes irreducibles, Γ_1 y Γ_2, correspondientes a los ideales primos (x) e (y), respectivamente. La primera tiene multiplicidad 1 y la segunda multiplicidad 2. Sus estructuras de subesquema cerrado reducido son, respectivamente, $\mathrm{Esp}(K[X,Y]/(X))$ y $\mathrm{Esp}(K[X,Y]/(Y))$, con las cuales ambas son isomorfas a A^1_K y se cortan en el punto $\mathfrak{p} = (x,y)$. En particular, con dicha estructura, ambas componentes irreducibles son geométricamente regulares. Sin embargo, su situación en D es muy distinta. Por la observación precedente, los puntos de Γ_1 distintos de $\mathfrak{p}$ son geométricamente regulares en D, mientras que los puntos de Γ_2 no son siquiera regulares, pues sus anillos locales $\mathcal{O}_{D,x}$ no son reducidos. ∎

Si X/k es una curva (un conjunto algebraico de dimensión 1 sobre un cuerpo k) entonces los divisores primos de X son los puntos cerrados, luego está definido su grado $\mathrm{grad}_k P = |k(P) : k|$. Este grado se extiende de forma obvia a un homomorfismo $\mathrm{grad}_k : \mathrm{Div}(X) \longrightarrow \mathbb{Z}$ y, en particular, podemos definir el grado de un divisor de Cartier como

$$\mathrm{grad}_k D = \sum_P v_P(D)\,\mathrm{grad}_k P,$$

donde P recorre los puntos cerrados de X.

Recordemos ahora que, para toda curva proyectiva E sobre un cuerpo k y todo haz coherente $\mathcal{M}$ sobre E tenemos definida [E 6.31] la característica de Euler $\chi_k(\mathcal{M})$. Cuando el haz coherente es de la forma $\mathcal{M} = \mathcal{O}_E(D)$, para cierto $D \in \mathrm{Div}_c(E)$, el teorema [E 10.11] nos da la relación

$$\mathrm{grad}_k(D) = \chi_k(\mathcal{O}_E(D)) - \chi_k(\mathcal{O}_E).$$

Esto nos lleva a la definición siguiente:

Definición 4.7 Si E/k es una curva proyectiva, definimos el *grado (de un haz)* de un haz inversible $\mathcal{L}$ en E como

$$\mathrm{grad}_k \mathcal{L} = \chi_k(\mathcal{L}) - \chi_k(\mathcal{O}_E).$$

En estos términos acabamos de probar que, para todo divisor $D \in \mathrm{Div}_c(E)$, se cumple que $\mathrm{grad}_k(\mathcal{O}_E(D)) = \mathrm{grad}_k(D)$. Más aún, el teorema [E 8.34] nos garantiza que $D \mapsto \mathcal{O}_E(D)$ induce un isomorfismo $\mathrm{Cl}_c(E) \cong \mathrm{Pic}(E)$, luego el grado $\mathrm{grad} : \mathrm{Pic}(E) \longrightarrow \mathbb{Z}$ es un homomorfismo de grupos.

En [E 10.24] demostramos que, en una curva proyectiva X, un divisor D es amplio si y sólo si $\mathrm{grad}\, D > 0$, pero bajo el supuesto de que X sea geométricamente regular y geométricamente conexa. Ahora vamos a probar que dichas hipótesis no son necesarias:

Teorema 4.8 *Sea X/k una curva proyectiva íntegra y $D \in \mathrm{Div}_c(X)$. Entonces D es amplio si y sólo si* $\mathrm{grad}\, D > 0$.

Demostración: El teorema [E 10.16] nos da que si $\mathrm{grad}\, D < 0$ entonces $\mathcal{O}_X(D^n)(X) = 0$, luego $\mathcal{O}_X(D^n)$ no puede tener un generador global, luego D no puede ser amplio. Si $\mathrm{grad}\, D = 0$ y $\mathcal{O}_X(D^n)$ es muy amplio, entonces, por [E 10.16 c)], $\mathcal{O}_X(D^n) \cong \mathcal{O}_X$, pero $\mathcal{O}_X$ no puede ser muy amplio, ya que $K = \mathcal{O}_X(X)$ es un cuerpo, por [E 4.26] y tendríamos una inmersión cerrada $X \longrightarrow \mathrm{P}^0_K = \mathrm{Esp}\, K$, lo cual es imposible. Así pues, para que D sea amplio es necesario que $\mathrm{grad}\, D > 0$.

Supongamos ahora que $\mathrm{grad}\, D > 0$ y sea $E \in \mathrm{Div}_c(X)$ un divisor amplio. El teorema [E 10.11], junto con las definiciones de la característica de Euler y de la dimensión de un divisor, nos da que

$$\dim(D^n/E) \geq \mathrm{grad}(D^n/E) + \chi(\mathcal{O}_X),$$

luego, si n es suficientemente grande, tenemos que $\dim(D^n/E) \neq 0$. Tomamos un $f \in \mathcal{O}_X(D^n/E)(X)$ no nulo, de modo que $(f)D^n/E$ es entero. Queremos probar que $\mathcal{O}_X(D^n)$ tiene un generador global, pero este haz es el mismo que $\mathcal{O}_X((f)D^n)$, luego podemos sustituir D por $(f)D^n$ y suponer que $E \mid D$. Fijemos, de nuevo, un $n \geq 1$, de modo que $E^n \mid D^n$, y sea $F = D^n/E^n$, que es un divisor entero.

El teorema [E 10.10] nos da una sucesión exacta

$$0 \longrightarrow \mathcal{O}_X(E^n) \longrightarrow \mathcal{O}_X(D^n) \longrightarrow i^*\mathcal{O}_F \longrightarrow 0,$$

donde $i : F \longrightarrow X$ es la inmersión cerrada canónica. Consideremos ahora en X un haz coherente $\mathcal{F}$ arbitrario, que nos da una sucesión exacta

$$\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_X(E^n) \xrightarrow{\alpha} \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_X(D^n) \longrightarrow \mathcal{F} \otimes_{\mathcal{O}_X} i^*\mathcal{O}_F \longrightarrow 0.$$

De ella deducimos a su vez las sucesiones exactas de cohomología

$$H^1(X, \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_X(E^n)) \longrightarrow H^1(X, \operatorname{Im}\alpha) \longrightarrow H^2(X, \mathrm{N}(\alpha)),$$

$$H^1(X, \operatorname{Im}\alpha) \longrightarrow H^1(X, \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_X(D^n)) \longrightarrow H^1(X, \mathcal{F} \otimes_{\mathcal{O}_X} i^*\mathcal{O}_F).$$

Ahora bien, como X tiene dimensión 1, sabemos que $H^2(X, \mathrm{N}(\alpha)) = 0$ y, por otra parte, $\mathcal{F}\otimes_{\mathcal{O}_X} i^*\mathcal{O}_F$ se anula en $X\backslash F$, luego también $H^1(X, \mathcal{F}\otimes_{\mathcal{O}_X} i^*\mathcal{O}_F) = 0$. En efecto, basta calcular este grupo mediante la cohomología de Čech asociada a un cubrimiento afín formado por un abierto afín de X que contenga a F (teorema [E 4.37]) y abiertos afines disjuntos con F.

Por el teorema [E 6.25] sabemos que $H^1(X, \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_X(E^n)) = 0$ para todo n suficientemente grande, luego las sucesiones exactas precedentes nos dan que también $H^1(X, \mathcal{F}\otimes_{\mathcal{O}_X} \mathcal{O}_X(D^n)) = 0$, luego, por el mismo teorema, el haz $\mathcal{O}_X(D)$ es amplio. ∎

Para terminar, demostramos otro resultado que no está probado en [E], el cual se basa en un resultado técnico de álgebra conmutativa:

Definición 4.9 Sea A un anillo, M un A-módulo y $a \in A$. Consideramos el submódulo $M[a] = \{m \in M \mid am = 0\}$. Si M/aM y $M[a]$ tienen longitud finita, definimos

$$e_A(a, M) = l_A(M/aM) - l_A(M[a]).$$

Teorema 4.10 *Sea A un anillo y $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ una sucesión exacta de A-módulos. Si $e_A(a, M')$ y $e_A(a, M'')$ son finitos, también lo es $e_A(a, M)$, y además $e_A(a, M) = e_A(a, M') + e_A(a, M'')$.*

Demostración: Sea $N = (aM \cap M')/aM'$, que es un submódulo de M'/aM', luego tiene longitud finita. Es fácil definir de forma natural sucesiones exactas

$$0 \longrightarrow N \longrightarrow M'/aM' \longrightarrow M/aM \longrightarrow M''/aM'' \longrightarrow 0,$$

$$0 \longrightarrow M'[a] \longrightarrow M[a] \longrightarrow M''[a] \longrightarrow N \longrightarrow 0.$$

Por ejemplo, para definir el epimorfismo δ de la segunda sucesión, llamando α y β a los homomorfismos de la sucesión exacta dada en el enunciado, tomamos $m'' \in M''[a]$, tomamos $m \in M$ tal que $\beta(m) = m''$, con lo que $am \in M'$. Tomamos $\delta(m'') = [am] \in N$. Es fácil ver que no depende de la elección de m.

Las sucesiones anteriores implican que M/aM y $M[a]$ tienen longitud finita, pues todos los demás módulos tienen longitud finita. Además,

$$l_A(N) - l_A(M'/aM') + l_A(M/aM) - l_A(M''/aM'') = 0,$$

$$l_A(M'[a]) - l_A(M[a]) + l_A(M''[a]) - l_A(N) = 0.$$

Sumando ambas ecuaciones obtenemos la ecuación del enunciado. ∎

Teorema 4.11 *Sea X/k una curva, sean $\Gamma_1,\dots,\Gamma_r$ sus componentes irreducibles, consideradas como subesquemas cerrados con la estructura reducida y sean $m_1,\dots,m_r$ sus multiplicidades. Entonces, si $\mathcal{L}\in \mathrm{Pic}(X)$, se cumple que*

$$\mathrm{grad}_k\,\mathcal{L} = \sum_i m_i\,\mathrm{grad}_k\,\mathcal{L}|_{\Gamma_i},$$

donde $\mathcal{L}|_{\Gamma_i}$ es la imagen inversa de $\mathcal{L}$ por la inmersión cerrada $\Gamma_i\longrightarrow X$.

Demostración: Por [E 8.34] podemos suponer que $\mathcal{L}=\mathcal{O}_X(D)$, para cierto $D\in \mathrm{Div}_c(X)$. Si llamamos ξ_i al punto genérico de Γ_i, la fórmula que hemos de probar puede escribirse en la forma

$$\mathrm{grad}_k\,D = \sum_i l(\mathcal{O}_{X,\xi_i})\,\mathrm{grad}_k\,D|_{\Gamma_i}.$$

Como todo divisor es cociente de dos divisores enteros (teorema [E 10.7]) podemos suponer que D es entero. Por definición,

$$\mathrm{grad}_k\,D = \sum_P v_P(D)\ \mathrm{grad}_k\,P,$$

donde P recorre los puntos cerrados de X o, equivalentemente, el conjunto finito de puntos que forman el soporte de D. Si P es uno de estos puntos, sea $A=\mathcal{O}_{X,P}$ y sea $a\in A$ un generador de $\mathcal{O}_X(D^{-1})_P$, que es un elemento regular de A. Así

$$v_P(D) = l_A(A/aA).$$

Pongamos que P pertenece a las componentes irreducibles $\Gamma_1,\dots,\Gamma_s$. Éstas se corresponden con los primos minimales de A. Llamémoslos $\mathfrak{p}_1,\dots,\mathfrak{p}_s$. Observemos que $\mathcal{O}_{\Gamma_i}(D|_{\Gamma_i}^{-1})_P = (a,\mathfrak{p}_i)/\mathfrak{p}_i$, luego $v_P(D|_{\Gamma_i}) = l_{A/\mathfrak{p}_i}(A/(a,\mathfrak{p}_i))$. Basta probar que

$$l_A(A/aA) = \sum_i l_{A_{\mathfrak{p}_i}}(A_{\mathfrak{p}_i})\,l_{A/\mathfrak{p}_i}(A/(a,\mathfrak{p}_i)).$$

Como a es regular, se cumple que $A[a]=0$, luego el miembro izquierdo es $e_A(a,A)$. Vamos a probar, más en general, que si M es un A-módulo finitamente generado, se cumple que

$$e_A(a,M) = \sum_i l_{A_{\mathfrak{p}_i}}(M_{\mathfrak{p}_i})\,l_{A/\mathfrak{p}_i}(A/(a,\mathfrak{p}_i)).$$

Podemos suponer que $M\neq 0$. Tomamos un primo $\mathfrak{q}_1$ asociado a M, de modo que M tiene un submódulo M_1 isomorfo a $A/\mathfrak{p}_1$. Si $M_1\subsetneq M$, podemos tomar un primo $\mathfrak{q}_2$ asociado a M/M_1, lo que nos da un submódulo M_2 tal que M_2/M_1 es isomorfo a $A/\mathfrak{q}_2$. Como A es noetheriano, la sucesión $0\subsetneq M_1\subsetneq M_2\subsetneq\cdots$ tiene que terminar en M.

Supongamos demostrada la fórmula para módulos de la forma $A/\mathfrak{q}$. Entonces consideramos la sucesión exacta

$$0\longrightarrow M_1\longrightarrow M_2\longrightarrow M_2/M_1\longrightarrow 0.$$

La fórmula se cumple para M_1 y M_2/M_2, y $l_{A/\mathfrak{p}_i}(-)$ cumple la misma relación que en el teorema anterior hemos probado para $e_A(a,-)$. De estos hechos se sigue fácilmente que la fórmula es válida para M_2. Entonces, la sucesión exacta

$$0 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow M_3/M_2 \longrightarrow 0$$

nos da que también se cumple para M_3 y, tras un número finito de pasos, llegamos a que se cumple para M.

Supongamos, pues, que $M = A/\mathfrak{q}$. Si $\mathfrak{q}$ es el ideal maximal, entonces tenemos que $M_{\mathfrak{p}_i} = 0$, y también $e_A(a,M) = 0$ (notemos que $a \in \mathfrak{q}$ porque P está en el soporte de D).

Si $\mathfrak{q}$ no es el ideal maximal, ha de ser uno de los primos minimales $\mathfrak{p}_j$. Entonces $M_{\mathfrak{p}_i} = 0$ para $i \neq j$ y $M_{\mathfrak{p}_j}$ es el cuerpo de cocientes de $A/\mathfrak{p}_j$, que tiene longitud 1. Así pues, la fórmula se reduce a

$$e_A(a, A/\mathfrak{p}_j) = l_{A/\mathfrak{p}_j}(A/(a,\mathfrak{p}_j)),$$

y esto es cierto, pues, por una parte, $(A/\mathfrak{p}_j)[a] = 0$, ya que $a \notin \mathfrak{p}_j$ (a es regular), y por otra parte $a(A/\mathfrak{p}_j) = (a,\mathfrak{p}_j)/\mathfrak{p}_j$. ∎

4.3 Cónicas

La aplicación principal de las técnicas que expondremos en los capítulos siguientes será el estudio de las curvas elípticas, que son una familia de cúbicas planas. Ahora vamos a estudiar las curvas planas cuadráticas, es decir, las cónicas. Aquí entenderemos por *cónica* cualquier curva proyectiva plana de grado 2 sobre un cuerpo K, es decir, definida por una ecuación de la forma

$$aX^2 + bY^2 + cZ^2 + dXY + eXZ + fYZ = 0,$$

con $a,b,c,d,e,f \in K$ no todos nulos. En particular, no exigimos que el polinomio sea irreducible.

El teorema 4.2 nos da que las cónicas tienen género $p_a = 0$, y el teorema [E 10.23] nos da lo siguiente:

Teorema 4.12 *Toda cónica regular C/K con un punto racional es isomorfa a la recta proyectiva P^1_K.*

Los polinomios homogéneos de grado 2 se llaman también formas cuadráticas, y es conocido[1] que toda forma cuadrática sobre un cuerpo K de característica $\neq 2$ se transforma con un cambio de variables lineal en otra de la forma $aX^2 + bY^2 + cZ^2$. Con esto podemos describir las cónicas sobre cuerpos de característica distinta de 2:

[1] Teorema 8.3 de mi *Teoría de Números*. La hipótesis car $k \neq 2$ se supone desde el principio del capítulo.

Teorema 4.13 *Si K es un cuerpo tal que $\operatorname{car} K \neq 2$, toda cónica C/K es isomorfa a otra definida por una ecuación de la forma*

$$aX^2 + bY^2 + cZ^2 = 0,$$

con a, b, $c \in K$ no todos nulos. Además:

a) C/K es geométricamente regular si y sólo si $abc \neq 0$. En tal caso también es geométricamente íntegra.

b) Si (exactamente) dos de los coeficientes a, b, c son no nulos, C/K es geométricamente reducible y geométricamente reducida, y tiene un único punto geométricamente singular, que, de hecho, es singular y racional.

c) Si sólo uno de los coeficientes es no nulo, entonces C es una recta doble, con lo que es geométricamente irreducible pero no es reducida en ningún punto y, en particular, no tiene puntos regulares.

Demostración: Acabamos de explicar que C/K se transforma en una cónica definida por una ecuación como la del enunciado mediante un cambio de variables lineal (que, en abstracto, corresponde a un isomorfismo).

a) Supongamos que C/K es geométricamente singular, es decir, que la extensión de constantes $C_{\bar{K}}$ tiene un punto singular, donde $\bar{K}$ es la clausura algebraica de K. No perdemos generalidad si suponemos que dicho punto singular está en el abierto afín $U = V(z)$, que es la curva definida por la ecuación

$$aX^2 + bY^2 + c = 0.$$

Un punto cualquiera de U es un ideal de la forma $(x-u, y-v)$, para ciertos u, $v \in \bar{K}$ tales que $au^2 + bv^2 + c = 0$. Si es singular, el criterio jacobiano nos da que (u, v) cumple las ecuaciones $2au = 2bv = 0$, luego $u = v = 0$, pero entonces (u, v) no cumple la ecuación de la cónica. Así pues, $C_{\bar{K}}$ es regular y C es geométricamente regular.

Por otra parte es geométricamente íntegra, ya que $C_{\bar{K}}$ es una cónica regular con un punto racional, luego, por el teorema anterior, $C_{\bar{K}} \cong \mathrm{P}^1_{\bar{K}}$ es una curva íntegra.

Los apartados b) y c) implican el recíproco de a).

b) Si, por ejemplo, $c = 0$ y $ab \neq 0$, entonces la ecuación (homogénea) de la cónica se reduce a

$$aX^2 + bY^2 = (\sqrt{a}\,X + \sqrt{-b}\,Y)(\sqrt{a}\,X - \sqrt{-b}\,Y) = 0.$$

La hipótesis de que $\operatorname{car} K \neq 2$ implica que los dos factores son distintos, luego $C_{\bar{K}}$ es reducida y tiene dos componentes irreducibles, que son dos rectas isomorfas a $\mathrm{P}^1_{\bar{K}}$. Por consiguiente, $C_{\bar{K}}$ es reducida (pero no irreducible) y todos sus puntos son regulares salvo el punto de intersección de las rectas, que es el ideal homogéneo (x, y). La proyección de este punto en C es el punto racional $(x, y) \in C$, que es, pues, el único punto geométricamente singular de C. De

hecho, es singular, puesto que, si fuera regular, el teorema anterior nos daría que $C \cong \mathrm{P}^1_K$, pero entonces sería geométricamente regular.

El apartado c) es inmediato. ∎

En característica 2, para obtener un resultado análogo añadiremos la hipótesis de que el cuerpo sea perfecto:

Teorema 4.14 *Si K es un cuerpo perfecto de característica 2, toda cónica C/K es isomorfa a otra definida por una ecuación de la forma*

$$aX^2 + bY^2 + cZ^2 + dXY = 0,$$

con a, b, c, $d \in K$ no todos nulos. Además:

a) Si c y d son no nulos, la ecuación se puede transformar hasta $Z^2+XY = 0$, con lo que C/K es geométricamente regular y tiene un punto racional. Por consiguiente, $C \cong \mathrm{P}^1_K$.

b) Si $d \neq 0$ y $c = 0$, entonces C/K es geométricamente reducible y geométricamente reducida. Tiene un único punto geométricamente singular que, de hecho, es singular y racional.

c) Si $d = 0$, un cambio de variables lineal transforma C/K en la cónica dada por la ecuación $X^2 = 0$, luego es una recta doble, geométricamente irreducible pero no reducida, con lo que no tiene puntos regulares.

Demostración: En principio, C/K está definida por una ecuación de la forma

$$aX^2 + bY^2 + cZ^2 + dXY + eXZ + fYZ = 0.$$

Si $d = e = f = 0$, ya tiene la forma exigida por el enunciado. En caso contrario, no perdemos generalidad si suponemos que $d \neq 0$. Dividiendo la ecuación entre d podemos suponer que $d = 1$.

El cambio de variables $X = X' + fZ$, $Y = Y' + eZ$ transforma la ecuación en

$$aX^2 + bY^2 + (c + af^2 + be^2 + ef)Z^2 + XY = 0,$$

que tiene la forma indicada.

Supongamos, pues, que C/K está definida por la ecuación

$$aX^2 + bY^2 + cZ^2 + dXY = 0.$$

Hemos probado que si $d \neq 0$ podemos exigir, de hecho, que $d = 1$. Si además $c \neq 0$, el cambio $Z' = \sqrt{c}\,Z$ hace que también $c = 1$, y el cambio $Z = Z'+\sqrt{a}X+\sqrt{b}Y$ reduce la ecuación a $XY+Z^2 = 0$, que es geométricamente regular por el criterio jacobiano y, obviamente, tiene el punto racional $[1, 1, 1]$. Esto prueba a).

Bajo las hipótesis de b), la ecuación se reduce a $aX^2 + XY + bY^2 = 0$. El polinomio se descompone (en una clausura algebraica de K) en producto de

dos factores irreducibles distintos, que definen dos rectas isomorfas a $\mathrm{P}^1_{\bar{K}}$ que se cortan en el punto racional $[0,0,1]$. Desde aquí se llega a la conclusión igual que en el apartado análogo del teorema anterior.

Por último, si $d = 0$, no perdemos generalidad si suponemos que $a \neq 0$. El cambio de variables $X' = \sqrt{a}\,X$ hace que $a = 1$. Llamando $b' = \sqrt{b}$, $c' = \sqrt{c}$, la ecuación puede escribirse como $(X + b'Y + c'Z)^2 = 0$, y el cambio de variables $X' = X + b'Y + c'Z$ la transforma en $X^2 = 0$, con lo que tenemos c). ∎

Ahora vamos a caracterizar intrínsecamente las cónicas, es decir, mediante propiedades geométricas de una curva que no hagan referencia a las ecuaciones que la definen.

Recordemos que el género aritmético de una curva C/K es

$$p_a(C) = 1 - \dim_K H^0(C, \mathcal{O}_C) + \dim_K H^1(C, \mathcal{O}_C).$$

Si C/K es geométricamente íntegra, el teorema [E 4.26] reduce la expresión a $p_a(C) = \dim_K H^1(C, \mathcal{O}_X) \geq 0$, pero en general el género de una curva podría incluso ser negativo (pero no el de una hipersuperficie de P^2_K, por el teorema 4.2).

Ahora bien, una cónica C/K puede pasar a tener género negativo si la consideramos sobre "el cuerpo equivocado". En efecto, supongamos que K/k es una extensión de cuerpos de grado n. Podemos considerar a C definida sobre k tomando como homomorfismo estructural la composición

$$C \longrightarrow \mathrm{Esp}\, K \longrightarrow \mathrm{Esp}\, k.$$

Con esto no estamos alterando el esquema C, luego los grupos $H^0(C, \mathcal{O}_C)$ y $H^1(C, \mathcal{O}_C)$ siguen siendo los mismos. No obstante, su dimensión sobre k no es la misma que sobre K, por lo que el género de C/k es

$$p_a(C) = 1 - \dim_k H^0(C, \mathcal{O}_C) + \dim_k H^1(C, \mathcal{O}_C)$$

$$= 1 - n \dim_K H^0(C, \mathcal{O}_C) + n \dim_K H^1(C, \mathcal{O}_C) = -(n-1) \leq 0,$$

donde hemos usado que el género de C/K es 0.

En particular, si la extensión K/k no es trivial, vemos que C/k no es una cónica, puesto que tiene género negativo. (La definición de cónica es relativa al cuerpo: una curva es una cónica sobre K si es isomorfa a una hipersuperficie de grado 2 en P^2_K.) En el supuesto de que la ecuación F que define a C/K tenga sus coeficientes en k, es importante no confundir la curva C/k con la cónica definida sobre k por la misma ecuación. La primera es el mismo esquema

$$C = \mathrm{Proy}(K[X,Y,Z]/(F))$$

(con otro homomorfismo estructural), mientras que la segunda es el esquema

$$C' = \mathrm{Proy}(k[X,Y,Z]/(F)),$$

que, obviamente, también es una cónica.

Ejemplo Vamos a estudiar con más detenimiento el fenómeno que acabamos de señalar. Para ello consideremos un conjunto algebraico proyectivo arbitrario X/k, sea k'/k una extensión finita de cuerpos que, por simplicidad supondremos finita y separable, de modo que $k' = k(\alpha)$, para cierto $\alpha \in k'$. Llamemos

$$X^* = X_{k'} = X \times_k \operatorname{Esp} k'.$$

De este modo, X^* es un conjunto algebraico sobre k' definido por ecuaciones con coeficientes en k. Ahora vamos a considerar el esquema X^*/k, que, según veremos, no es el mismo que X/k. Vamos a calcular

$$X^*_{k'} = X \times_k \operatorname{Esp} k' \times_k \operatorname{Esp} k' = X \times_k \operatorname{Esp}(k' \otimes_k k').$$

Si $p(X)$ es el polinomio mínimo de α en $k[X]$, tenemos que $k' = k[X]/(p)$, luego

$$k' \otimes_k k' = k'[X]/(p).$$

Sea $p(X) = (X - \alpha)p_2(X) \cdots p_n(X)$ la descomposición de $p(X)$ en factores irreducibles de $k'[X]$. Entonces,

$$\operatorname{Esp}(k' \otimes_k k') = P_1 \cup \cdots \cup P_n$$

donde cada P_i es un abierto $P_i \cong \operatorname{Esp} k_i$, donde $k_i = k'[X]/(p_i(X))$. Por consiguiente,

$$X^*_{k'} = X_{k_1} \cup \cdots \cup X_{k_n}.$$

El caso más simple se da cuando X/k es geométricamente irreducible y la extensión k'/k es finita de Galois, de modo que $p(X)$ tiene sus raíces en k', con lo que $k_i = k'$. Entonces vemos que X^*/k ya no es geométricamente irreducible, ni geométricamente conexo, sino que $X^*_{k'}$ es unión de n componentes irreducibles disjuntas, todas ellas isomorfas a $X_{k'}$.

En particular, si X/k es una cónica geométricamente irreducible y k'/k es finita de Galois no trivial, entonces X^*/k' también es una cónica geométricamente irreducible, pero X^*/k no puede ser una cónica, ya que las cónicas son geométricamente conexas. ∎

Probamos ahora un resultado técnico que vamos a necesitar:

Teorema 4.15 *Sea X/A un esquema proyectivo sobre un anillo noetheriano A tal que las fibras de los puntos de* $\operatorname{Esp} A$ *tengan dimensión ≤ 1 y $H^1(X, \mathcal{O}_X) = 0$. Si $\mathcal{F}$, $\mathcal{G}$ son dos haces coherentes en X con generadores globales, entonces, el homomorfismo*

$$\phi : \mathcal{F}(X) \otimes_A \mathcal{G}(X) \longrightarrow (\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G})(X)$$

es suprayectivo.

Demostración: Como $\mathcal{F}(X)$ y $\mathcal{G}(X)$ son A-módulos finitamente generados, tenemos sucesiones exactas

$$0 \longrightarrow \mathcal{N}_1 \longrightarrow \mathcal{O}_X^p \xrightarrow{\alpha} \mathcal{F} \longrightarrow 0, \qquad 0 \longrightarrow \mathcal{N}_2 \longrightarrow \mathcal{O}_X^q \xrightarrow{\beta} \mathcal{G} \longrightarrow 0,$$

de donde obtenemos una sucesión exacta

$$H^0(X, \mathcal{O}_U^p) \longrightarrow H^0(X, \mathcal{F}) \longrightarrow H^1(X, \mathcal{N}_1) \longrightarrow H^1(X, \mathcal{O}_X) = 0.$$

Podemos elegir α y p de modo que el homomorfismo de la izquierda sea suprayectivo, con lo que $H^1(X, \mathcal{N}_1) = 0$, e igualmente $H^1(X, \mathcal{N}_2) = 0$.

Por otra parte, es fácil construir un isomorfismo natural

$$(\mathcal{O}_X^p \otimes_{\mathcal{O}_X} \mathcal{O}_X^q)/\big((\mathcal{N}_1 \otimes_{\mathcal{O}_X} \mathcal{O}_X^q) + (\mathcal{O}_X^p \otimes_{\mathcal{O}_X} \mathcal{N}_1)\big) \cong \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}.$$

Si llamamos $\mathcal{N}$ al denominador del primer miembro, tenemos sucesiones exactas

$$0 \longrightarrow \mathcal{N} \longrightarrow \mathcal{O}_X^p \otimes_{\mathcal{O}_X} \mathcal{O}_X^q \longrightarrow \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G} \longrightarrow 0$$

y

$$0 \longrightarrow \mathcal{N}' \longrightarrow (\mathcal{N}_1 \otimes_{\mathcal{O}_X} \mathcal{O}_X^q) \oplus (\mathcal{O}_X^p \otimes_{\mathcal{O}_X} \mathcal{N}_1) \longrightarrow \mathcal{N} \longrightarrow 0.$$

Por la hipótesis sobre las fibras del homomorfismo estructural, el teorema [E A15] nos da que el grupo de cohomología de orden 2 de cualquier haz coherente en X es nulo. Por lo tanto tenemos una sucesión exacta

$$H^1(X, (\mathcal{N}_1 \otimes_{\mathcal{O}_X} \mathcal{O}_X^q) \oplus (\mathcal{O}_X^p \otimes_{\mathcal{O}_X} \mathcal{N}_1)) \longrightarrow H^1(X, \mathcal{N}) \longrightarrow 0.$$

El primer haz es simplemente $\mathcal{N}_1^q \oplus \mathcal{N}_2^p$, donde los exponentes indican suma directa, y es claro que $H^1(X, \mathcal{N}_1^q \oplus \mathcal{N}_2^p) = 0$. Por consiguiente, también tenemos que $H^1(X, \mathcal{N}) = 0$. Así pues, el homomorfismo

$$H^0(X, \mathcal{O}_X^p \otimes_{\mathcal{O}_X} \mathcal{O}_X^q) \longrightarrow H^0(\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G})$$

es suprayectivo. Notemos ahora que

$$H^0(X, \mathcal{O}_X^p) \otimes_A H^0(X, \mathcal{O}_X^q) \cong H^0(X, \mathcal{O}_X)^p \otimes_A H^0(X, \mathcal{O}_X)^q$$

$$\cong H^0(X, \mathcal{O}_X)^{pq} \cong H^0(X, \mathcal{O}_X^{pq}) \cong H^0(X, \mathcal{O}_X^p \otimes_{\mathcal{O}_X} \mathcal{O}_X^q).$$

Finalmente, basta considerar el diagrama conmutativo

$$\begin{array}{ccc} H^0(X, \mathcal{O}_X^p) \otimes_A H^0(X, \mathcal{O}_X^q) & \longrightarrow & H^0(X, \mathcal{F}) \otimes_A H^0(X, \mathcal{G}) \\ \cong\downarrow & & \downarrow\phi \\ H^0(X, \mathcal{O}_X^p \otimes_{\mathcal{O}_X} \mathcal{O}_X^q) & \longrightarrow & H^0(X, \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}) \end{array}$$

del que deducimos que ϕ es suprayectivo. ∎

Finalmente probamos la caracterización intrínseca de las cónicas:

Teorema 4.16 *Sea C/k una curva íntegra proyectiva que sea localmente una intersección completa. Supongamos que $p_a(C) \leq 0$ y sea $K = H^0(C, \mathcal{O}_C)$. Entonces podemos considerar a C como curva definida sobre K de modo que C/K es una cónica.*

DEMOSTRACIÓN: Observemos que K es un cuerpo por [E 4.26], más aún, es una extensión finita de k. Las restricciones $K = \mathcal{O}_C(C) \longrightarrow \mathcal{O}_C(U)$, para cada abierto U de C, convierten a $\mathcal{O}_C$ en un haz de K-álgebras, lo cual determina un homomorfismo $C \longrightarrow \operatorname{Esp} K$ definido sobre k. Como C/k es proyectivo, también lo es C/K. Según la definición del género aritmético:

$$\begin{aligned} p_a(C) &= 1 - \dim_k H^0(C, \mathcal{O}_C) + \dim_k H^1(C, \mathcal{O}_C) \\ &= 1 - |K : k| + |K : k| \dim_K H^1(C, \mathcal{O}_C). \end{aligned}$$

Es claro entonces que la hipótesis $p_a(C) \leq 0$ equivale a que $H^1(C, \mathcal{O}_C) = 0$. Cambiando k por K podemos suponer que $K = k$, con lo que $p_a(C) = 0$.

Si $\omega_{C/k}$ es el haz canónico, se cumple que $\operatorname{grad} \omega_{C/k} = 2(p_a - 1) = -2$, luego $\dim_k H^0(C, \omega^*_{C/k}) = 3$. (Ver los resultados tras el teorema de Riemann-Roch [E 10.20].) Vamos a probar que el haz $\omega^*_{C/k}$ es muy amplio.

Sea $D \in \operatorname{Div}_c(C)$ tal que $\omega^*_{C/k} \cong \mathcal{O}_C(D)$. Teniendo en cuenta [E 8.30], podemos tomarlo entero, ya que basta sustituirlo por $(f)D$, con $f \in \mathcal{O}_C(D)(C)$ no nulo.

Notemos que los anillos de $\mathcal{L} = \mathcal{O}_C(D)$ son subanillos de $K(C)$, y todos ellos contienen a k. En particular, si $x \in C$ no pertenece al soporte de D, se cumple que $\mathcal{L}_x = \mathcal{O}_{C,x}$ y $1 \in \mathcal{L}(C)$ es un generador global de $\mathcal{L}$ en x. Vamos a probar que $\mathcal{L}$ también tiene generadores globales para los puntos del soporte de D, es decir, que $\mathcal{L}$ tiene un generador global.

Representaremos por $k(x)$ al haz rascacielos en C que en cada entorno U de x está definido como el $\mathcal{O}_C(U)$-módulo $k(x)$, que es obviamente un $\mathcal{O}_C$-módulo. El haz $\mathcal{L} \otimes_{\mathcal{O}_C} k(x)$ es también un haz rascacielos, que en los entornos de x viene dado por $\mathcal{L}_x/\mathfrak{m}_x\mathcal{L}_x$. Tenemos una sucesión exacta

$$0 \longrightarrow \mathcal{I}\mathcal{L} \longrightarrow \mathcal{L} \longrightarrow \mathcal{L} \otimes_{\mathcal{O}_C} k(x) \longrightarrow 0,$$

donde $\mathcal{I}$ es el haz de ideales de $\mathcal{O}_C$ asociado al subesquema cerrado reducido x. Vamos a probar que $H^1(C, \mathcal{I}\mathcal{L}) = 0$. Esto implicará que el homomorfismo natural $\mathcal{L}(C) \longrightarrow \mathcal{L}_x/\mathfrak{m}_x\mathcal{L}_x$ es suprayectivo. Más aún, si llamamos I al $\mathcal{O}_{C,x}$-módulo generado por la imagen del homomorfismo natural $\mathcal{L}(C) \longrightarrow \mathcal{L}_x$, tenemos una sucesión exacta

$$I \otimes_{\mathcal{O}_{C,x}} k(x) \longrightarrow \mathcal{L}_x \otimes_{\mathcal{O}_{C,x}} k(x) \longrightarrow (\mathcal{L}_x/I) \otimes_{\mathcal{O}_{C,x}} k(x) \longrightarrow 0.$$

El primer homomorfismo es suprayectivo, luego $(\mathcal{L}_x/I) \otimes_{\mathcal{O}_{C,x}} k(x) = 0$, y el lema de Nakayama implica entonces que $I = \mathcal{L}_x$. Por lo tanto, C tiene un generador global en x.

Para probar que, en efecto, $H^1(C, \mathcal{I}\mathcal{L}) = 0$, consideramos la sucesión exacta

$$0 \longrightarrow \mathcal{O}_C(D^{-1}) \longrightarrow \mathcal{I} \longrightarrow \mathcal{F} \longrightarrow 0,$$

donde $\mathcal{F}$ tiene su soporte contenido en D. Como $\mathcal{L}$ es localmente libre, al multiplicar por $\otimes_{\mathcal{O}_C}\mathcal{L}$, seguimos teniendo una sucesión exacta:

$$0 \longrightarrow \mathcal{O}_C \longrightarrow \mathcal{I}\mathcal{L} \longrightarrow \mathcal{F} \otimes_{\mathcal{O}_C} \mathcal{L} \longrightarrow 0.$$

(El isomorfismo $\mathfrak{I}\mathfrak{L} \cong \mathfrak{I} \otimes_{\mathcal{O}_C} \mathfrak{L}$ es también una consecuencia inmediata de que $\mathfrak{L}$ es localmente libre de rango 1.)

El haz $\mathcal{N} = \mathcal{F} \otimes_{\mathcal{O}_C} \mathfrak{L}$ tiene también su soporte contenido en D, y claramente cumple que $\mathcal{O}_C(D^{-1})\mathcal{N} = 0$, luego por [AC B6] tenemos que $\mathcal{N} = i_* i^* \mathcal{N}$, donde $i : D \longrightarrow C$ es la inmersión cerrada natural. Por consiguiente, tenemos que $H^1(C, \mathcal{N}) = H^1(D, i^*\mathcal{N}) = 0$, ya que D tiene dimensión 0. Esto nos da la sucesión exacta de cohomología:

$$0 = H^1(C, \mathcal{O}_C) \longrightarrow H^1(C, \mathfrak{I}\mathfrak{L}) \longrightarrow 0,$$

que nos da $H^1(C, \mathfrak{I}\mathfrak{L}) = 0$ y, en definitiva, que $\mathfrak{L}$ tiene un generador global.

En particular, una k-base de $\mathfrak{L}(C)$ es un generador global de $\mathfrak{L}$, luego podemos considerar su homomorfismo asociado $\phi : C \longrightarrow \mathrm{P}^2_k$. Vamos a probar que es una inmersión cerrada.

Llamemos $U \subset C$ al complementario del soporte de D y para cada $n \geq 1$, sea $L(D^n) = \mathcal{O}_C(D^n)(C)$. Notemos que $L(D^n) \subset \mathcal{O}_C(U)$. En efecto, un elemento $h \in L(D^n)$ es un elemento $h \in K(C)^*$ tal que $(h)D^n \geq 1$. Si $x \in U$ y f representa al divisor D en un entorno de x, tenemos que $f_x \in \mathcal{O}^*_{C,x}$, así como que $h_x f_x^n \in \mathcal{O}_{C,x}$, luego también $h_x \in \mathcal{O}_{C,x}$, lo que prueba que $h \in \mathcal{O}_C(U)$. Más aún, se cumple que

$$\mathcal{O}_C(U) = \bigcup_{n \geq 1} L(D^n).$$

En efecto, si $h \in \mathcal{O}_C(U)$ y $x \in C \setminus U$, entonces $h_x = a/b$, con $a, b \in \mathcal{O}_{C,x}$. El anillo $\mathcal{O}_{C,x}/b\mathcal{O}_{C,x}$ tiene dimensión 0, luego su ideal maximal es su único ideal primo, luego sus elementos son nilpotentes. Si f es un representante de D en un entorno de x, tenemos que f_x pertenece a dicho ideal maximal luego $f_x^n \in b\mathcal{O}_{C,x}$, para todo n suficientemente grande, luego $h_x f_x^n \in \mathcal{O}_{C,x}$. Obviamente, el mismo n sirve para todos los puntos de un entorno de x, luego por compacidad existe un n que vale para todo x (y esto es trivialmente cierto si $x \in U$). Por consiguiente, $(h)D^n \geq 1$ y $h \in L(D^n)$.

Aplicando a C/k el teorema 4.15 obtenemos que el homomorfismo natural

$$L(D) \otimes_k \overset{n}{\cdots} \otimes_k L(D) \longrightarrow L(D^n)$$

es suprayectivo, para todo $n \geq 1$.

Si, como base de $L(D)$, tomamos una de la forma $1, s, t$, entonces, por definición, $U = C_1$, y ϕ se restringe al homomorfismo $U \longrightarrow A^2_k$ asociado al homomorfismo $k[X, Y] \longrightarrow \mathcal{O}_C(U)$ dado por $X \mapsto s$, $Y \mapsto t$. Según los resultados precedentes, es un epimorfismo, luego $\phi|_U$ es una inmersión cerrada.

A través del isomorfismo $\omega^*_{C/k} \cong \mathcal{O}_C(D)$, lo que hemos probado es que existe una base de $\omega^*_{C/k}(C)$ cuyo homomorfismo asociado $C \longrightarrow \mathrm{P}^2_k$ se restringe a una inmersión cerrada $U \longrightarrow A^2_k$. Si $x \in C \setminus U$, como $\mathcal{O}_C(D)$ tiene un generador global, existe un $f \in L(D)$ tal que $f_x \mathcal{O}_{C,x} = \mathcal{O}_C(D)_x$, luego x no está en el soporte de $D' = (f)D$. Por consiguiente, trabajando con D' en lugar de con D, obtenemos otra base de $\omega^*_{C/k}(C)$ que define un homomorfismo que es una

inmersión cerrada en un entorno de x. Los homomorfismos asociados a dos bases de $\omega^*_{C/k}$ se diferencian en un automorfismo de P^2_k, luego también ϕ ha de ser una inmersión cerrada en un entorno de x. En definitiva, concluimos que ϕ es una inmersión cerrada.

Ahora podemos considerar a C/k como una hipersuperficie de P^2_k, luego es de la forma $\operatorname{Proy} k[X,Y,Z]/(F)$, para un cierto polinomio homogéneo F de grado d. Por el teorema 4.2 tenemos que

$$0 = p_a(C) = \frac{(d-1)(d-2)}{2},$$

luego $d \leq 2$. Si $d = 2$ tenemos que C/k es una cónica, mientras que si $d = 1$ entonces $C \cong \mathrm{P}^1_k$, y también es isomorfo a una cónica. ∎

Observemos que en la prueba del teorema anterior hemos visto que toda cónica posee un divisor entero D de grado 2. Podemos extraer más consecuencias de este teorema, pero para ello necesitamos un resultado general sobre normalizaciones de curvas:

Teorema 4.17 *Sea $\pi : C' \longrightarrow C$ la normalización de una curva íntegra proyectiva C/k. Para cada punto $P \in C$ existe un número natural δ_P tal que $\delta_P = 0$ si y sólo si P es regular en C y*

$$p_a(C) = p_a(C') + \sum_{P \in C} |k(P) : k|\, \delta_P.$$

Demostración: Como el homomorfismo π es birracional, podemos identificar $K = k(C') = k(C)$ y considerar a todos los anillos de $\mathcal{O}_{C'}$ y $\mathcal{O}_C$ como subanillos de K, de modo que los homomorfismos naturales se corresponden con inclusiones. Tenemos entonces una sucesión exacta

$$0 \longrightarrow \mathcal{O}_C \longrightarrow \pi_*\mathcal{O}_{C'} \longrightarrow \mathcal{F} \longrightarrow 0,$$

de modo que, para cada punto $P \in C$, se cumple que $\mathcal{F}_P = \pi_*\mathcal{O}_{C',P}/\mathcal{O}_{C,P}$. Los dos primeros haces de la sucesión son coherentes, luego $\mathcal{F}$ también lo es.

Notemos que $\pi_*\mathcal{O}_{C',P}$ es la clausura entera de $\mathcal{O}_{C,P}$, por lo que $\mathcal{F}_P = 0$ si y sólo si P es normal o, equivalentemente, regular en C. El hecho de que el soporte de $\mathcal{F}$ sea finito implica que $H^1(C,\mathcal{F}) = 0$. Así:

$$\chi(\mathcal{F}) = \dim_k H^0(C,\mathcal{F}) = \sum_P \dim_k \mathcal{F}_P$$

(donde P recorre los puntos singulares de C). En particular, resulta que la longitud $\delta_P = l_{\mathcal{O}_{C,P}}\mathcal{F}_P$ es finita, ya que los $\mathcal{O}_{C,P}$-submódulos de $\mathcal{F}_P$ son k-espacios vectoriales. Más precisamente, los $\mathcal{O}_{C,P}$-módulos simples son isomorfos a $k(P)$, luego $\dim_k \mathcal{F}_P = |k(P) : k|\, \delta_P$.

Por la aditividad de la característica de Euler, $\chi(\pi_*\mathcal{O}_{C'}) = \chi(\mathcal{O}_C) + \chi(\mathcal{F})$. Como π es finito, el teorema [E A10] nos da que $\chi(\pi_*\mathcal{O}_{C'}) = \chi(\mathcal{O}_{C'})$. En definitiva, tenemos que

$$p_a(C) = 1 - \chi(\mathcal{O}_C) = 1 - \chi(\mathcal{O}_{C'}) + \chi(\mathcal{F}) = p_a(C') + \sum_{P \in C} |k(P) : k|\, \delta_P.$$

∎

Teorema 4.18 *Si C/k es una cónica íntegra, entonces el homomorfismo*

$$\mathrm{grad} : \mathrm{Pic}(C) \longrightarrow \mathbb{Z}$$

es inyectivo. Si es suprayectivo, entonces $C \cong \mathrm{P}^1_k$. En caso contrario, C tiene a lo sumo un punto singular, necesariamente racional y, si es así, su normalización es isomorfa a $\mathrm{P}^1_{k'}$, donde k'/k es una extensión cuadrática.

Demostración: Si $\mathcal{L} \in \mathrm{Pic}(C)$ tiene grado 0, entonces $\mathcal{L}(C) \neq 0$ por el ejemplo tras la definición [E 10.21], luego $\mathcal{L} \cong \mathcal{O}_C$ por [E 10.16 c)]. Esto prueba que el homomorfismo dado por el grado es inyectivo. Su imagen será de la forma $d\mathbb{Z}$, para cierto $d \geq 1$. En la prueba del teorema 4.16 hemos visto que C/k tiene un divisor entero de grado 2, luego ha de ser $d = 1, 2$.

Consideremos la normalización $\pi : C' \longrightarrow C$. El teorema [E 10.9] nos da que C'/k tiene también un divisor entero de grado d, que podemos identificar con un divisor de Weil, que será de la forma $D = P^2$, donde $P \in C'$ es un punto racional, o bien de la forma $D = P$, donde $\mathrm{grad}_k P = 1, 2$.

Por el teorema anterior, como $p_a(C) = 0$, resulta que $p_a(C') \leq 0$, luego el teorema 4.16 implica que C'/k' es una cónica, donde $k' = H^0(C', \mathcal{O}_{C'})$ es una extensión de k. Ahora bien, es claro que $k \subset k' \subset k(P)$, luego $|k' : k| \leq 2$. Más aún, en la prueba de 4.16 hemos visto también que $H^1(C', \mathcal{O}_{C'}) = 0$, luego

$$p_a(C') = 1 - |k' : k|.$$

Si $d = 1$, entonces $D = P$ es un punto racional, luego $k' = k$ y $p_a(C') = 0$. El teorema anterior implica entonces que C es regular y tiene un divisor de grado 1, luego el teorema [E 10.22] (junto con el ejemplo previo) implica que $C \cong \mathrm{P}^1_k$.

Recíprocamente, si C no es regular, entonces $p_a(C') = -1$, y la fórmula del teorema anterior nos da que C/k tiene un único punto singular, que además es racional. Por otra parte, la extensión k'/k es cuadrática y

$$\mathrm{grad}_{k'} D = \frac{1}{2} \mathrm{grad}_k D = 1,$$

luego $C' \cong \mathrm{P}^1_{k'}$, por el mismo argumento anterior. ∎

En particular tenemos un refinamiento de 4.12:

Teorema 4.19 *Toda cónica íntegra C/k con un punto racional regular es isomorfa a P^1_k.*

Demostración: Basta observar que un punto racional regular P define un divisor de Cartier de grado 1. En efecto, basta considerar un entorno afín regular U de P, donde P, como divisor de Weil, se identifica con un divisor de Cartier de U de grado 1. Restringiendo U, podemos suponer que el divisor es principal, es decir, que está determinado por un único par (U, f), para cierta $f \in \mathcal{O}_C(U)$. Entonces, los pares (U, f) y $(C \setminus \{P\}, 1)$ definen un divisor de Cartier en C cuyo divisor de Weil asociado es P. Claramente, su grado sigue siendo 1. ∎

4.4 Curvas elípticas

Recordamos ahora las propiedades básicas de las curvas elípticas expuestas en el capítulo II de [CE], aunque aquí las presentaremos en el lenguaje de la teoría de esquemas desarrollada en [E]. Debemos señalar que en [CE] trabajábamos únicamente con curvas definidas sobre cuerpos perfectos, mientras que aquí no necesitaremos esa hipótesis salvo cuando lo indiquemos explícitamente.

Recordemos que una *ecuación de Weierstrass* (homogénea) con coeficientes en un cuerpo K es una ecuación cúbica de la forma

$$F = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0,$$

con $a_i \in K$.

Sea $\bar{K}$ una clausura algebraica de K. En primer lugar demostraremos que F es irreducible en $\bar{K}[X,Y,Z]$ (luego también en $K[X,Y,Z]$). Para ello es más práctico razonar en términos de la geometría clásica. Consideremos el conjunto algebraico proyectivo $V(F) \subset \mathrm{P}^2(\bar{K})$ en sentido clásico, es decir, el conjunto de los puntos de $\mathrm{P}^2(\bar{K})$ cuyas coordenadas homogéneas cumplen la ecuación. Observamos que corta a la recta $Z = 0$ únicamente en el punto $o = [0,1,0]$. Para estudiar este punto podemos deshomogeneizar la ecuación respecto de Y, con lo que nos queda la ecuación

$$F_*(X,Z) = Z + a_1XZ + a_3Z^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0.$$

El punto o se corresponde ahora con $o = (0,0)$.

Consideremos un factor irreducible F_0 de F en $\bar{K}[X,Y,Z]$, que será un polinomio homogéneo que definirá una curva irreducible $V(F_0)$. Es claro que no puede ser $F_0 = Z$, luego $V(F_0)$ corta a $V(Z)$ al menos en un punto (por [GA 3.24]). Ahora bien, como $V(F_0) \subset V(F)$, dicho punto no puede ser sino o. Esto implica que $F_{0*}(0,0) = 0$. Por consiguiente, si F puede descomponerse en factores irreducibles, esta factorización dará lugar a una descomposición de $F_*(X,Z)$ en otros tantos factores, todos los cuales se anularán en $(0,0)$. Si hay más de uno (no necesariamente distintos), podemos factorizar $F_* = f_1f_2$, con $f_1(0,0) = f_2(0,0) = 0$. Aplicando la regla de derivación del producto, esto implica que

$$\left.\frac{\partial F_*}{\partial Z}\right|_{(0,0)} = 0,$$

mientras que un calculo directo muestra que la derivada vale 1, contradicción.

A partir de aquí consideraremos la curva proyectiva en sentido abstracto

$$C/K = \mathrm{Proy}(K[X,Y,Z]/(F)) = \mathrm{Proy}K[x,y,z].$$

Puesto que, según acabamos de ver, el polinomio F es irreducible, tenemos que C/K es una curva íntegra y, más aún, geométricamente íntegra.

El hecho de que, en términos clásicos, la curva corte a la recta $Z = 0$ sólo en el punto $[0, 1, 0]$, se traduce ahora en que el cerrado $V(z) \subset C$ contiene únicamente al punto $o = (x, z)$. Esto es algo que podemos constatar directamente: Por una parte, o es ciertamente un ideal primo homogéneo de $K[x, y, z]$. Es primo porque

$$K[x, y, z]/o \cong K[X, Y, Z]/(X, Z) \cong K[Y],$$

que es un dominio íntegro. Por otra parte, los generadores x, y, z satisfacen la ecuación de Weierstrass,

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

luego un ideal primo homogéneo $\mathfrak{p} \in C$ que contenga a z debe contener también a x^3, luego a x, de modo que $o \subset \mathfrak{p}$. Además se ha de dar la igualdad, pues si tuviera algún generador homogéneo no contenido en o, sería de la forma y^n, luego tendríamos que $y \in \mathfrak{p}$ y, por consiguiente, $\mathfrak{p} = (x, y, z)$, contradicción.

Para estudiar el punto o consideramos su entorno afín

$$D(y) = \mathrm{Esp}(K[X, Z]/(F_*)),$$

en el cual se corresponde con el punto $o = (x, z)$, visto ahora como ideal de $K[X, X]/(F_*)$. Vemos que es un punto racional, y además es geométricamente regular, pues su única antiimagen en $U_{\bar{K}}$, que es también $o = (x, z)$, es regular, según se desprende del criterio jacobiano 4.1, ya que

$$\left.\frac{\partial F_*}{\partial Z}\right|_{(0,0)} = 1.$$

Como o es geométricamente regular, en particular es regular. Esto es prácticamente todo lo que necesitamos saber del punto o: que es racional y geométricamente regular. Para estudiar los restantes puntos de C consideraremos el abierto afín $U = D(z)$ definido por la deshomogeneización de F respecto de Z:

$$f = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6 = 0.$$

En la práctica escribiremos siempre las ecuaciones de Weierstrass en su forma afín f, es decir, deshomogeneizadas respecto de Z. El polinomio f define una curva afín $U = \mathrm{Esp}(K[X, Y]/(f))$, pero, cuando hablemos de "la curva definida por una ecuación de Weierstrass (afín)", no nos referiremos a U/K, sino a la curva proyectiva C/K definida por la ecuación homogénea correspondiente. A los puntos de U los llamaremos "puntos finitos" de la curva C, mientras que o (el único punto de C que no está en U) será el "punto infinito" de C.

Recogemos en un teorema todo lo que hemos obtenido:

Teorema 4.20 *Sea K un cuerpo y C/K el conjunto algebraico proyectivo definido por una ecuación de Weierstrass*

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

con coeficientes en K. Entonces, C es una curva geométricamente íntegra con un único punto infinito o, que es racional y geométricamente regular.

Las curvas definidas por ecuaciones de Weierstrass no son necesariamente regulares, pero a lo sumo tienen un punto singular:

Teorema 4.21 *Si C/K es una curva definida por una ecuación de Weierstrass, entonces es geométricamente regular salvo a lo sumo en un punto, necesariamente finito. Si tiene un punto singular, entonces es racional, y la normalización de C es isomorfa a P^1_K.*

Demostración: Como C/K es geométricamente íntegra, su normalización C'/k también lo es (por el teorema [E 3.61]). Por consiguiente, $p_a(C) \geq 0$ y $p_a(C') \geq 0$. Si C/K tiene un punto singular, el teorema 4.17 implica que $p_a(C') < p_a(C) = 1$, luego ha de ser $p_a(C) = 1$ y $p_a(C') = 0$.

El teorema 4.17 nos da también que C/K sólo puede tener un punto singular p, necesariamente racional. La restricción de π a $C' \setminus \pi^{-1}[\{p\}] \longrightarrow C \setminus \{p\}$ es la normalización de $C \setminus \{p\}$, pero esta curva es normal, luego, por la unicidad, la restricción es un isomorfismo. En particular, como C contiene un punto racional distinto de p, (el punto infinito), su antiimagen en C' también es racional, luego el teorema [E 10.23] nos da que $C' \cong \mathrm{P}^1_K$.

Si aplicamos la parte ya probada a $C_{\bar{K}}$, donde $\bar{K}$ es la clausura algebraica de K, dado que $C_{\bar{K}}/\bar{K}$ también es una curva definida por una ecuación de Weierstrass, concluimos que $C_{\bar{K}}$ tiene a lo sumo un punto singular, luego C/K tiene a lo sumo un punto geométricamente singular, necesariamente finito, pues ya hemos visto que el punto infinito es geométricamente regular. ∎

Vamos a probar que, salvo en casos muy particulares, si una curva definida por una ecuación de Weierstrass tiene un punto geométricamente singular, de hecho es singular, pero para ello necesitamos estudiar más a fondo las ecuaciones. El primer paso es recordar las definiciones siguientes:

Definición 4.22 A cada ecuación de Weierstrass se le asocian las cantidades siguientes:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, & c_4 &= b_2^2 - 24b_4,\\ b_4 &= 2a_4 + a_1a_3, & c_6 &= -b_2^3 + 36b_2b_4 - 216b_6,\\ b_6 &= a_3^2 + 4a_6, & \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, & j &= c_4^3/\Delta. \end{aligned}$$

En particular, Δ es el *discriminante* de la ecuación y j (definido sólo cuando $\Delta \neq 0$) es su *invariante.*

Una simple comprobación muestra que todo cambio de variables de la forma

$$X = u^2X' + r, \qquad Y = u^3Y' + su^2X' + t, \qquad u, r, s, t \in K, \quad u \neq 0,$$

transforma una ecuación de Weierstrass en otra. En términos más conceptuales, se comprueba que el homomorfismo de anillos $K[X, Y, Z] \longrightarrow K[X', Y', Z']$ dado por

$$X \mapsto u^2X' + r, \qquad Y \mapsto u^3Y' + su^2X' + t, \qquad Z \mapsto Z'$$

define un automorfismo de K-álgebras, que a su vez induce un K-automorfismo

$$K[X,Y,Z]/(F) \longrightarrow K[X',Y',Z']/(F'),$$

donde F' es la ecuación de Weierstrass que resulta del cambio de variables. A su vez, este automorfismo induce un isomorfismo

$$\mathrm{Proy}(K[X',Y',Z']/(F')) \longrightarrow \mathrm{Proy}(K[X,Y,Z]/(F))$$

que transforma el punto infinito en el punto infinito y que, restringido a los abiertos definidos por las ecuaciones afines, se identifica con el automorfismo

$$\mathrm{Esp}(K[X',Y']/(f')) \longrightarrow \mathrm{Esp}(K[X,Y]/(f))$$

inducido por el automorfismo de K-álgebras $K[X,Y] \longrightarrow K[X,Y]$ determinado por el cambio de variables. En definitiva: tenemos que las ecuaciones de Weierstrass relacionadas por un cambio de variables del tipo indicado determinan curvas isomorfas.

Una comprobación rutinaria demuestra el teorema siguiente:

Teorema 4.23 *Al aplicar a una ecuación de Weierstrass un cambio de variables de la forma*

$$X = u^2X' + r, \qquad Y = u^3Y' + su^2X' + t, \qquad u,r,s,t \in K, \quad u \neq 0,$$

sus constantes se transforman según las fórmulas siguientes:

$$\begin{aligned}
ua_1' &= a_1 + 2s,\\
u^2a_2' &= a_2 - sa_1 + 3r - s^2,\\
u^3a_3' &= a_3 + ra_1 + 2t,\\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t+rs)a_1 + 3r^2 - 2st,\\
u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1,\\
\hline
u^2b_2' &= b_2 + 12r,\\
u^4b_4' &= b_4 + rb_2 + 6r^2,\\
u^6b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3,\\
u^8b_8' &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4,\\
\hline
u^4c_4' &= c_4,\\
u^6c_6' &= c_6,\\
u^{12}\Delta' &= \Delta,\\
j' &= j.
\end{aligned}$$

El teorema [EC 2.7] muestra las simplificaciones que pueden llevarse a cabo en una ecuación de Weierstrass mediante la aplicación de cambios de variables oportunos. Dichas simplificaciones permiten a su vez estudiar el posible punto geométricamente singular de una curva definida por una ecuación de Weierstrass, precisando el teorema 4.21:

Teorema 4.24 *Sea C/K la curva definida por una ecuación de Weierstrass de discriminante Δ. Si $\operatorname{car} K = 2, 3$ supondremos que K es perfecto. Entonces C/K es geométricamente regular si y sólo si $\Delta \neq 0$, y en caso contrario tiene un único punto geométricamente singular, necesariamente singular, finito y racional.*

DEMOSTRACIÓN: La prueba es exactamente la misma que la de [CE 2.8] (y no la repetiremos). Sólo hemos de hacer algunas observaciones derivadas del hecho de que en [CE] suponíamos que el cuerpo K es perfecto, cosa que no vamos a hacer aquí. Cuando K es perfecto, la regularidad coincide con la regularidad geométrica y por ello, aunque en el enunciado de [CE 2.8] se dice que C/K es regular salvo a lo sumo en un punto, lo que realmente se demuestra es que es geométricamente regular salvo a lo sumo en un punto, pues lo que se hace en la prueba puede interpretarse como la aplicación del criterio jacobiano 4.1 a la curva $C_{\bar{K}}$ (es decir, se prueba que todos los puntos de $C_{\bar{K}}$ son regulares salvo a lo sumo uno de ellos).

Por lo demás, el carácter perfecto de K sólo se utiliza para probar que el punto geométricamente singular es racional cuando la característica de K es 2 o 3, y por ello hemos incluido esta hipótesis en el enunciado.

Por último, en [CE 2.8] se prueba que si $\Delta = 0$ hay un punto finito, racional que no es geométricamente regular, pero, si K no es perfecto, eso no implica que sea singular. Es lo único que tendremos que demostrar aquí.

Concretamente, lo que se prueba en [CE 2.8] bajo la hipótesis de que $\Delta = 0$, es que existe un par $(r, t) \in K^2$ que cumple la ecuación de Weierstrass y que anula sus dos derivadas parciales. Haciendo el cambio de variables $X = X' + r$, $Y = Y' + t$ podemos cambiar la ecuación de Weierstrass y suponer que el punto geométricamente singular es $P = (0, 0)$.

Que el punto cumpla la ecuación de Weierstrass equivale a que $a_6 = 0$, y que anule a las derivadas equivale a que $a_3 = a_4 = 0$, luego la ecuación de Weierstrass se reduce ahora a

$$f(X, Y) = Y^2 + a_1XY - X^3 - a_2X^2 = 0.$$

En términos de ideales, el punto racional $(0, 0)$ se corresponde con el ideal $\mathfrak{p} = (X, Y)$ de

$$K[x, y] = K[X, Y]/(f).$$

Éste es el único punto de C que es geométricamente singular, y hemos de ver que es singular. Para ello consideramos su anillo local $\mathcal{O}_{C,\mathfrak{p}}$, que es la localización respecto de $\mathfrak{p}$ de $K[x, y]$ y cumple $\dim \mathcal{O}_{C,\mathfrak{p}} = 1$. Su ideal maximal es $\mathfrak{m} = (x, y)$ y lo que hemos de probar es que $\mathfrak{m}$ no es principal.

Ahora bien, según [AC 5.52], el número mínimo de generadores de $\mathfrak{m}$ coincide con la dimensión de $\mathfrak{m}/\mathfrak{m}^2$ como espacio vectorial sobre $K = \mathcal{O}_{C,\mathfrak{p}}/\mathfrak{m}$. Por consiguiente, basta ver que las clases $\bar{x}$, $\bar{y} \in \mathfrak{m}/\mathfrak{m}^2$ son linealmente independientes sobre K. Para ello tomamos α, $\beta \in K$ y suponemos que $\alpha\bar{x} + \beta\bar{y} = 0$. Hemos de probar que $\alpha = \beta = 0$.

Tenemos que $\alpha x + \beta y \in \mathfrak{m}^2$, es decir, que $\alpha x + \beta y = u/v$, donde $u \in \mathfrak{p}^2$ y $v \in K[x,y] \setminus \mathfrak{p}$. Si $u = \bar{U}$, $v = \bar{V}$, con $U, V \in K[X,Y]$, tenemos que

$$V(\alpha X + \beta Y) - U \in (f), \qquad U \in (X,Y)^2 = (X^2, Y^2, XY), \qquad V \notin (X,Y).$$

Como $f \in (X,Y)^2$, vemos que $V(\alpha X + \beta Y) \in (X^2, Y^2, XY)$ y, teniendo en cuenta que el término independiente de V ha de ser no nulo, esto implica inmediatamente que $\alpha = \beta = 0$. ∎

Definición 4.25 Si K es un cuerpo, una *curva elíptica* definida sobre K es una curva proyectiva íntegra y geométricamente regular E/K de género 1 en la que hemos seleccionado un punto racional $o \in E(K)$.

El teorema [CE 2.3] prueba que toda curva elíptica E/K es isomorfa a una curva definida por una ecuación de Weierstrass con coeficientes en K, de modo que el isomorfismo hace corresponder el punto racional o con el punto infinito de la ecuación de Weierstrass. Además, dos ecuaciones de Weierstrass que definan curvas isomorfas a E/K están relacionadas por un cambio de variables del tipo considerado en el teorema 4.23.

Por el teorema 4.2, toda cúbica plana tiene género 1, luego lo único que necesita cumplir una ecuación de Weierstrass para definir una curva elíptica es que su discriminante sea no nulo.[2]

En realidad, un *isomorfismo* entre curvas elípticas se define como un isomorfismo entre curvas que hace corresponder el punto racional prefijado de una con el punto racional prefijado de la otra. Cuando hablemos de la curva elíptica definida por una ecuación de Weierstrass sobrentenderemos que su punto racional prefijado es su punto infinito. Así podemos decir simplemente que toda curva elíptica E/K es isomorfa a una curva elíptica definida por una ecuación de Weierstrass.

Cuando hablemos de una ecuación de Weierstrass *asociada* a una curva elíptica dada E/K nos referiremos a una ecuación de Weierstrass que defina una curva elíptica isomorfa a E/K.

Observemos que las constantes definidas en 4.22 no pueden asociarse directamente a una curva elíptica dada, sino que dependen concretamente de la ecuación de Weierstrass que consideremos, salvo en el caso del invariante j, de modo que podemos hablar del *invariante* de una curva elíptica dada, definido como el de cualquiera de sus ecuaciones de Weierstrass asociadas.

El teorema [EC 2.9] prueba que dos curvas elípticas E_1/K y E_2/K tienen el mismo invariante si y sólo si $E_{1\bar{K}} \cong E_{2\bar{K}}$, aunque esto no implica necesariamente que $E_1 \cong E_2$. Como los cuerpos que vamos a considerar —cuerpos de cocientes de dominios de Dedekind— no serán algebraicamente cerrados, el invariante no nos será apenas de ninguna utilidad.

[2]La condición sobre que el cuerpo sea perfecto en el teorema 4.24 sólo es necesaria para justificar que si hay un punto geométricamente singular, es racional y singular.

Capítulo V

Superficies fibradas

En este capítulo sentaremos las bases del proyecto que hemos esbozado en la introducción. En la primera sección introduciremos y estudiaremos el concepto de superficie fibrada, que nos permitirá reunir en un único objeto geométrico a una curva proyectiva definida por una ecuación con coeficientes en un dominio de Dedekind D y sus reducciones módulo los divisores primos de D. En la segunda sección estudiaremos las explosiones, que son una familia de aplicaciones birracionales con las cuales podremos eliminar o "resolver" las singularidades de las superficies fibradas obtenidas de este modo, es decir, podremos obtener una superficie regular birracionalmente equivalente a una superficie dada. De momento veremos únicamente casos concretos de resolución de singularidades, y dejaremos para el capítulo siguiente la discusión del problema general. Una vez estemos provistos de ejemplos suficientes, dedicaremos la tercera sección a estudiar con más detenimiento las superficies fibradas y terminaremos con una sección dedicada íntegramente a un ejemplo de resolución de singularidades con el que ilustraremos los conceptos introducidos hasta el momento.

5.1 Modelos de curvas

Supongamos que tenemos una curva proyectiva C/K definida por una ecuación homogénea $F(X,Y,Z) = 0$ con coeficientes en un cuerpo K, el cual es, concretamente, el cuerpo de cocientes de un dominio de Dedekind D. Multiplicando la ecuación por una constante adecuada, podemos suponer que tiene sus coeficientes en D. En tal caso, además del esquema $C = \mathrm{Proy}(K[X,Y,Z]/(F))$, podemos considerar también el esquema $X = \mathrm{Proy}(D[X,Y,Z]/(F))$. En esta sección vamos a ver cómo esta idea abre todo un campo de posibilidades para el estudio de C.

Empecemos recordando los hechos básicos sobre los dominios de Dedekind:

Ante todo, recordemos que un *dominio de Dedekind* es un dominio íntegro D en el que cada ideal propio (es decir, distinto de 0 y D) se descompone de

forma única salvo el orden como producto de ideales primos. Esta definición incluye trivialmente a los cuerpos, porque no tienen ideales propios.

El teorema de Dedekind [N 3.9] afirma que un dominio íntegro D es un dominio de Dedekind si y sólo si es noetheriano, íntegramente cerrado y además $\dim D \leq 1$. Notemos que un dominio íntegro cumple $\dim D = 0$ si y sólo si es un cuerpo.

Si D es un dominio de Dedekind y K es su cuerpo de cocientes, cada ideal primo no nulo $\mathfrak{p}$ de D induce una valoración $v_\mathfrak{p}$ en K (la determinada por que, para cada $\alpha \in D$ no nulo, $v_\mathfrak{p}(\alpha)$ es la multiplicidad de $\mathfrak{p}$ en el ideal (α)).

El teorema [N 3.7] implica que el anillo de enteros de $v_\mathfrak{p}$ es la localización de D respecto de $\mathfrak{p}$, es decir, tenemos que $D_\mathfrak{p} = \{\alpha \in K \mid v_\mathfrak{p}(\alpha) \geq 0\}$.

En otras palabras, $D_\mathfrak{p}$ es lo que se llama un *anillo de valoración discreta.* Los teoremas [N 7.12] y [N 7.13] describen la estructura de estos anillos. En particular son dominios de ideales principales con un único primo no nulo. Recíprocamente, todo dominio de ideales principales con un único primo es un anillo de valoración discreta, pues es un dominio de Dedekind (local) y coincide con la localización respecto de su único primo no nulo.

Aunque vamos a trabajar únicamente con esquemas de Dedekind afines, conviene dar la definición general:

Definición 5.1 Un *esquema de Dedekind* es un esquema normal, localmente noetheriano y de dimensión ≤ 1.

De acuerdo con [E 7.1], consideramos que los esquemas normales son irreducibles (y, por consiguiente, íntegros) por definición. Es claro que un esquema afín $S = \operatorname{Esp} D$ es un esquema de Dedekind si y sólo si D es un dominio de Dedekind.

Si S es un esquema de Dedekind y $s \in S$, entonces $\mathcal{O}_{S,s}$ es un dominio de Dedekind local, luego es un dominio de ideales principales. En particular, los esquemas de Dedekind son regulares.

Si $U \subset S$ es un abierto, entonces U es también un esquema de Dedekind. El teorema [E 7.2] nos da que si U es noetheriano entonces $\mathcal{O}_S(U)$ es un dominio de Dedekind. Más aún, si S es un esquema íntegro noetheriano, tenemos que S es un esquema de Dedekind si y sólo si, para todo abierto afín $U \subset S$, el anillo $\mathcal{O}_S(U)$ es un dominio de Dedekind, si y sólo si, para todo punto cerrado $s \in S$, el anillo $\mathcal{O}_{S,s}$ es un dominio de Dedekind, si y sólo si, para todo punto cerrado $s \in S$, el anillo $\mathcal{O}_{S,s}$ es un dominio de ideales principales.

Ahora introducimos el concepto central en torno al cual gira todo este libro:

Definición 5.2 Una *superficie fibrada* sobre un dominio de Dedekind D es un esquema X/D íntegro, proyectivo y plano sobre D y de dimensión 2. Diremos que X/D es una superficie fibrada *normal* o *regular* si X es normal o regular como esquema. Una *superficie aritmética* es una superficie fibrada regular sobre un dominio de Dedekind de dimensión 1.

A la hora de aplicar la teoría de esquemas resulta útil llamar $S = \operatorname{Esp} D$, de modo que S es un esquema de Dedekind afín, y podemos escribir indistintamente X/D o X/S. En realidad, los resultados elementales no requieren que S sea afín. En lo sucesivo, cuando consideremos un esquema de Dedekind S sobrentenderemos que $\eta \in S$ representa su punto genérico.

Observemos que, en virtud de [E 4.54], que X/D sea plano equivale a que el homomorfismo estructural $\pi : X \longrightarrow S$ sea suprayectivo. (El caso $\dim S = 0$ es trivial.)

La fibra X_η se llama *fibra genérica* de X, mientras que las fibras X_s, donde $s \in S$ es un punto cerrado, se llaman *fibras cerradas* de X.

Si $\dim S = 0$, entonces $S = \operatorname{Esp} k$, donde k es un cuerpo, tenemos una única fibra y X es simplemente una superficie proyectiva sobre k. Éste es el *caso geométrico.* Por contraposición, en el caso en que $\dim S = 1$ *(el caso aritmético)* una superficie fibrada puede verse como una familia de curvas, tal y como se desprende del teorema siguiente:

Teorema 5.3 *Sea X/S una superficie fibrada con $\dim S = 1$. Para cada $s \in S$, la fibra X_s es una curva proyectiva sobre $k(s)$. La fibra genérica X_η es íntegra, y es normal o regular si X lo es.*

Demostración: Por "curva proyectiva" entendemos un conjunto algebraico proyectivo cuyas componentes irreducibles tienen todas dimensión 1. No suponemos que sea reducido o irreducible. Así, las fibras X_s son conjuntos algebraicos proyectivos porque X/S es proyectiva y la proyectividad se conserva por cambios de base. Además son curvas por el teorema 3.9.

Como el homomorfismo estructural $X \longrightarrow S$ es suprayectivo, el punto genérico de X pertenece a X_η, y es obviamente denso, luego X_η es irreducible. Por otra parte, para cada punto $Q \in X_\eta = X \times_S \operatorname{Esp} \mathcal{O}_{S,\eta}$, el teorema [E 3.47] nos da un isomorfismo $\mathcal{O}_{X,Q} \cong \mathcal{O}_{X_\eta,Q}$. Esto prueba que la fibra X_η es reducida, luego es íntegra, y es normal o regular si X lo es. ∎

Observemos que, en las condiciones del teorema anterior, si $S = \operatorname{Esp} D$ y K es el cuerpo de cocientes de D, tenemos que $k(\eta) = K$, luego la fibra genérica X_η es una curva proyectiva sobre K. Más aún, en la prueba hemos visto (tomando como Q el punto genérico de X_η, que se corresponde con el de X), que $K(X) = K(X_\eta)$.

Cuando la fibra genérica es geométricamente íntegra, podemos realizar cambios de base:

Teorema 5.4 *Sea X/S una superficie fibrada con $\dim S = 1$ y tal que su fibra genérica X_η sea geométricamente íntegra. Sea $S = \operatorname{Esp} D$ y sea $S' = \operatorname{Esp} D'$, donde D' es un dominio de Dedekind que extiende a D. Entonces $X' = X \times_S S'$ es una superficie fibrada sobre S'. Además, si $s' \in S'$ y s es su imagen en S, se cumple que*

$$X'_{s'} = X_s \times_{k(s)} \operatorname{Esp} k(s').$$

DEMOSTRACIÓN: Sea $p : X_{S'} \longrightarrow X$ la proyección y sea $i : X_\eta \longrightarrow X$ la inmersión natural. Obviamente, $X_{S'}$ es proyectiva y plana sobre S', pues estas propiedades se conservan por cambios de base. Si $U \subset X$ es un abierto, entonces $\mathcal{O}_X(U)$ es plano sobre D, por lo que el homomorfismo

$$\mathcal{O}_{X_{S'}}(p^{-1}[U]) = \mathcal{O}_X(U) \otimes_D D' \longrightarrow \mathcal{O}_X(U) \otimes_D K(S')$$

$$= \mathcal{O}_X(U) \otimes_D K(S) \otimes_{K(S)} K(S') = \mathcal{O}_{X_\eta}(i^{-1}[U]) \otimes_{K(S)} K(S')$$

es inyectivo y el último anillo es uno de los anillos de la extensión de constantes $(X_\eta)_{K(S')}$ que es una curva íntegra, por hipótesis, luego $\mathcal{O}_{X_{S'}}(p^{-1}[U])$ es un dominio íntegro. Esto prueba que $X_{S'}$ es íntegra.

Si $s' \in S'$ y $s \in S$ es su imagen, entonces

$$X_{S',s'} = X \times_S S' \times_{S'} \operatorname{Esp} k(s') = X \times_S \operatorname{Esp} k(s')$$

$$= X \times_S \operatorname{Esp} k(s) \times_{k(s)} \operatorname{Esp} k(s') = X_s \times_{k(s)} \operatorname{Esp} k(s').$$

El teorema 3.9 aplicado a la fibra genérica nos da que $\dim X_{S'} = 2$, luego $X_{S'}$ es una superficie fibrada. ∎

En particular, mediante un cambio de base, podemos seleccionar una fibra cerrada de una superficie fibrada:

Teorema 5.5 *Sea X/S una superficie fibrada con $\dim S = 1$, sea $s \in S$ un punto cerrado y sea $S' = \operatorname{Esp} \mathcal{O}_{S,s}$. Entonces $X' = X \times_S S'$ es una superficie fibrada sobre S' que tiene únicamente dos fibras: $X'_\eta \cong X_\eta$ y $X'_s \cong X_s$. Además, para cada $x \in X'_s$ se cumple que $\mathcal{O}_{X',x} \cong \mathcal{O}_{X,x}$.*

DEMOSTRACIÓN: Sea $S = \operatorname{Esp} D$, de modo que s se corresponde con un ideal primo no nulo $\mathfrak{p}$ de D. Basta aplicar el teorema anterior con $D' = D_\mathfrak{p}$. Observemos que no hace falta suponer que X_η es geométricamente íntegra, porque ahora D y D' tienen el mismo cuerpo de cocientes, es decir, $K(S) = K(S')$. Esto implica en particular que $X'_\eta \cong X_\eta$, y, como también $k(s) = k(s')$, lo mismo vale para la fibra cerrada. La última parte del enunciado se sigue del teorema [E 3.47]. ∎

Nuestro propósito es estudiar una curva C/K construyendo ciertas superficies fibradas X/S cuya fibra genérica sea C. En primer lugar damos nombre a esto:

Definición 5.6 Sea D un dominio de Dedekind con cuerpo de cocientes K y sea $S = \operatorname{Esp} D$. Un *modelo* de una curva proyectiva normal y conexa C/K es una superficie fibrada normal X/S junto con un isomorfismo $X_\eta \longrightarrow C$ (definido sobre K).

Diremos que un modelo de una curva es regular, suave, etc. si lo es como superficie fibrada. Un *homomorfismo* entre dos modelos X_1 y X_2 de C/K

es un homomorfismo de esquemas definido sobre S que induce un diagrama conmutativo

$$\begin{array}{ccc} X_{1\eta} & \longrightarrow & X_{2\eta} \\ & \searrow & \downarrow \\ & & C \end{array}$$

El punto de partida más elemental para conseguir modelos de una curva dada es el siguiente:

Ejemplo Se D un dominio de Dedekind con cuerpo de cocientes K. Consideremos una curva C/K que sea de la forma

$$C = \mathrm{Proy}(K[X,Y,Z]/(F)),$$

donde $F(X,Y,Z) \in D[X,Y,Z]$ es un polinomio homogéneo no constante irreducible en $K[X,Y,Z]$. Supongamos además que el máximo común divisor (en D) de sus coeficientes es igual a 1, lo que implica que también es irreducible en $D[X,Y,Z]$. En estas condiciones,

$$X = \mathrm{Proy}(D[X,Y,Z]/(F))$$

es obviamente un esquema íntegro proyectivo sobre $S = \mathrm{Esp}\, D$. Si $\mathfrak{p} \in S$, su fibra es

$$X_{\mathfrak{p}} = \mathrm{Proy}(k(\mathfrak{p})[X,Y,Z]/(\bar{F})),$$

donde $\bar{F}$ es la imagen de F en $k(\mathfrak{p})[X,Y,Z]$ (que es no nula porque los coeficientes de F son primos entre sí). En particular, todas las fibras son curvas no vacías, luego el homomorfismo estructural $X \longrightarrow S$ es suprayectivo. El teorema 3.9 nos da que $\dim X = 2$ y, en definitiva, concluimos que X/S es una superficie fibrada.

Según acabamos de ver, la fibra genérica es la curva C/K, luego lo único que le falta a X/S para ser un modelo de C/K es ser normal. Esto no tiene por qué ser cierto en general, sino que dependerá de la curva de partida, o incluso de la elección del polinomio F.

Observemos que, en términos clásicos, las fibras cerradas de X son las reducciones de C/K módulo los divisores primos de D. ∎

Como complemento a este ejemplo vamos a dar una sencilla condición suficiente para que una superficie fibrada sea normal. Nos basaremos en el teorema siguiente:

Teorema 5.7 *Sea D un anillo de valoración discreta, sea K su cuerpo de cocientes y k su cuerpo de restos. Si X/D es un esquema plano tal que X_K es normal y X_k es reducido, entonces X es normal.*

Demostración: Podemos suponer que $X = \mathrm{Esp}\, A$ es afín, donde A es una D-álgebra plana. Esto hace que el homomorfismo $A \longrightarrow A \otimes_D K$ sea inyectivo

y $A \otimes_D K = \mathcal{O}_{X_K}(X_K)$ es un dominio íntegro, luego A también lo es. Hemos de probar que A es íntegramente cerrado. Sea $\mathfrak{m} = (\pi)$ el ideal maximal de D.

Si α es un elemento del cuerpo de cocientes de A entero sobre A, podemos verlo como un elemento del cuerpo de cocientes de $A \otimes_D K$ entero sobre este anillo, que es íntegramente cerrado, luego $\alpha \in A \otimes_D K$. Esto significa que $\alpha = a\pi^{-r}$, para ciertos $a \in A$, $r \in \mathbb{Z}$. Podemos suponer que $a \notin \mathfrak{m}$. Basta probar que $r \leq 0$.

En caso contrario, consideremos una relación

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0,$$

con $a_i \in A$. Multiplicando por π^{rn} obtenemos que $a^n \in \mathfrak{m}$ y, como $D/\mathfrak{m}$ es reducido, ha de ser $a \in \mathfrak{m}$, contradicción. ∎

Como consecuencia:

Teorema 5.8 *Si X/S es una superficie fibrada cuya fibra genérica es normal y cuyas fibras cerradas son reducidas, entonces X es normal.*

Demostración: Tomemos $s \in S$ y $x \in X_s$. Hemos de probar que el anillo $\mathcal{O}_{X,x}$ es íntegramente cerrado.

Sea $S' = \operatorname{Esp} \mathcal{O}_{S,s}$ y sea $X' = X \times_S S'$. El teorema [E 3.47] nos da que x se corresponde con un punto $x' \in X'$ tal que $\mathcal{O}_{X,x} \cong \mathcal{O}_{X',x'}$. Así pues, basta probar que X' es normal.

Si s es el punto genérico de S, entonces X' es la fibra genérica, luego es normal por hipótesis. Si s es un punto cerrado, entonces X'/S' es una superficie fibrada cuya fibra genérica es normal y cuya fibra cerrada es reducida. Por el teorema anterior concluimos que X' es normal. ∎

Ejemplo Sea D un dominio de Dedekind, sea K su cuerpo de cocientes y sea E/K una curva elíptica definida sobre K. Consideremos una ecuación de Weierstrass

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

asociada a E/K con coeficientes en D. (Observemos que, mediante un cambio de variables de la forma $X = u^2X'$, $Y = u^3Y'$, siempre podemos transformar una ecuación de Weierstrass arbitraria en otra con coeficientes de D.) Sea $S = \operatorname{Esp} D$ y sea W/S la superficie fibrada asociada a (la homogeneización de) la ecuación según el ejemplo anterior.

La fibra genérica de W es la curva elíptica E/K, que es normal, y las fibras cerradas son las reducciones de dicha curva módulo los divisores primos de D. En particular son curvas proyectivas sobre cuerpos definidas por ecuaciones de Weierstrass, luego son íntegras. Por el teorema anterior, W es normal, luego es un modelo de E/K. ∎

Definición 5.9 Sea D un dominio de Dedekind, sea K su cuerpo de cocientes y sea $S = \operatorname{Esp} D$. Un *modelo de Weierstrass* W/S es una superficie fibrada determinada por una ecuación de Weierstrass con coeficientes en D (con discriminante no nulo) según el ejemplo anterior.

Más precisamente, diremos que W/S es un *modelo de Weierstrass* de una curva elíptica E/K si W/S es un modelo de Weierstrass y su fibra genérica es isomorfa a E/K.

Notemos que una misma curva elíptica admite diversas ecuaciones de Weierstrass con coeficientes en D y, por consiguiente, diversos modelos de Weierstrass sobre S. No obstante, observemos que si un cambio de variables

$$X = u^2X' + r, \qquad Y = u^3Y' + su^2X' + t$$

cumple que r, s, t, $u \in D$ y u es una unidad en D, entonces el cambio inverso tiene también sus coeficientes en D, por lo que induce un automorfismo de $D[X, Y, Z]$, el cual induce un automorfismo de W. Esto significa que si dos ecuaciones de Weierstrass con coeficientes en D se relacionan mediante un cambio de variables en estas condiciones, ambas definen el mismo modelo de Weierstrass.

Vamos a describir con más detalle los modelos de Weierstrass. Para empezar, llamemos $o_\eta = (x, z) \in W$. Observemos que o_η es ciertamente un ideal primo, pues, como $F \in (X, Z)$, se cumple que $o_\eta = (X, Z)/(F)$, luego

$$D[x, y, z]/o_\eta \cong D[X, Y, Z]/(X, Z) \cong D[Y],$$

que es un dominio íntegro. Llamemos $O = \overline{\{o_\eta\}}$, la clausura de $\{o_\eta\}$ en la topología de Zariski de W, que no es sino el conjunto de los puntos de W que contienen a o_η. Tomemos un punto $\mathfrak{P} \in O$ y sea $\mathfrak{p}$ su imagen en $S = \operatorname{Esp} D$ (tal vez $\mathfrak{p} = 0$). Esto significa que $\mathfrak{P} \cap D = \mathfrak{p}$. En particular, $\mathfrak{p} + (x, z) \subset \mathfrak{P}$. Ahora bien, se ha de dar la igualdad, pues $\mathfrak{P}$ está generado por elementos homogéneos de $D[x, y, z]$, y un generador homogéneo que no esté ya en $\mathfrak{p} + (x, z)$ ha de ser de la forma dy^n, donde $d \in D \setminus \mathfrak{p}$. Como $\mathfrak{P} \cap D = \mathfrak{p}$, ha de ser $d \notin \mathfrak{P}$, luego $y \in \mathfrak{P}$, pero entonces $(x, y, z) \in \mathfrak{P}$, lo cual es imposible.

Si llamamos $o_\mathfrak{p} = \mathfrak{p} + (x, z)$, es claro que $o_\mathfrak{p} \in W_\mathfrak{p}$, y acabamos de probar que $O \cap W_\mathfrak{p} = \{o_\mathfrak{p}\}$. Más concretamente, si tenemos en cuenta que la inmersión $W_\mathfrak{p} \longrightarrow W$ es el homomorfismo inducido por el homomorfismo

$$D[x, y, z] \longrightarrow k(\mathfrak{p})[x, y, z],$$

vemos que el punto $\mathfrak{q} \in W_\mathfrak{p}$ cuya imagen es $o_\mathfrak{p}$ contiene a x y a z, luego ha de ser el punto infinito de $W_\mathfrak{p}$.

Por último, observemos que el hecho de que los generadores x, y, z cumplan la ecuación de Weierstrass implica que $x \in (z)$, luego $o_\eta = (z)$. Con esto hemos probado lo siguiente:

Teorema 5.10 *Sea W/S un modelo de Weierstrass, para cada $s \in S$, sea o_s el punto infinito de W_s y consideremos el cerrado $O = \overline{\{o_\eta\}} \subset W$. Entonces, para todo $s \in S$ se cumple que $O \cap W_s = \{o_s\}$. Además, $o_\eta = (z)$, luego $O = V(z)$ y $W \setminus O = D(z)$, por lo que podemos identificar el abierto $W \setminus O$ con el esquema afín*

$$U = \mathrm{Esp}(D[X,Y]/(f))$$

donde $f(X,Y) \in D[X,Y]$ es la ecuación de Weierstrass deshomogeneizada.

Esto nos permite estudiar los modelos de Weierstrass en términos de un esquema afín tan pronto como podamos desentendernos de los puntos infinitos. Observemos ahora que si $\mathfrak{p} \in S$ es un punto cerrado, entonces

$$k(\mathfrak{p})[x,y] = k(\mathfrak{p})[X,Y]/(f) = (D/\mathfrak{p})[X,Y]/(f) = D[X,Y]/(\mathfrak{p}+(f)) = D[x,y]/\mathfrak{p}.$$

Esto implica que si tenemos representado un punto de $U_\mathfrak{p}$ en términos de un ideal $(\bar{f}_1(x,y),\dots,\bar{f}_n(x,y))$, con $f_i \in D[X,Y]$ (de modo que $\bar{f}_i(X,Y)$ es su imagen en $k(\mathfrak{p})[X,Y]$), entonces, como punto de U se corresponde con el ideal

$$\mathfrak{p} + (f_1(x,y),\dots,f_n(x,y)).$$

Ejemplo Consideremos el modelo de Weierstrass $W/\mathbb{Z}$ correspondiente a la ecuación

$$Y^2 = X^3 + 6.$$

Su discriminante es $\Delta = -2^6 \cdot 3^5$, luego W tiene exactamente dos fibras singulares, W_2 y W_3. La fibra W_2 es la curva definida sobre $\mathbb{Z}/2\mathbb{Z}$ por la ecuación $Y^2 = X^3$, cuyo punto singular, visto como punto de U_2, es $\mathfrak{p}_2 = (x,y)$ el cual, como punto de U es $\mathfrak{p}_2 = (2,x,y)$.

Similarmente, la fibra W_3 es la curva definida por la misma ecuación que U_2, pero ahora considerada sobre el cuerpo $\mathbb{Z}/3\mathbb{Z}$, y su punto singular es $\mathfrak{p}_3 = (x,y)$, que, como punto de U, es $\mathfrak{p}_3 = (3,x,y)$. ∎

Consideremos ahora un modelo de Weierstrass correspondiente a una ecuación de discriminante $\Delta \neq 0$ y sea $\mathfrak{p} \in S$ un punto cerrado. La fibra $W_\mathfrak{p}$ es la cúbica definida por la reducción de la ecuación módulo $\mathfrak{p}$, luego será geométricamente regular salvo si $\mathfrak{p} \mid \Delta$, en cuyo caso tendrá un único punto geométricamente singular. Teniendo en cuenta que W/S es plano, los puntos geométricamente regulares en su fibra son, por definición, los puntos suaves de W. Como Δ sólo puede ser divisible entre un número finito de primos, concluimos que todos los puntos de W son suaves salvo a lo sumo un número finito de ellos, uno en cada una de las fibras correspondientes a los primos de D respecto a los que la ecuación tiene mala reducción. Además, ninguno de estos puntos excepcionales está en el cerrado O de los puntos infinitos.

Los puntos de W que no son suaves son, de hecho, singulares en su fibra, pero eso no significa necesariamente que sean singulares en W. Vamos a dar un criterio sencillo que determina cuándo se da el caso.

Sea $\mathfrak{p} \in S$ un punto cerrado tal que la fibra $W_\mathfrak{p}$ sea singular. Su punto singular es finito y racional, lo cual significa que es un ideal maximal de la forma $(x - \bar{r}, x - \bar{t}) \subset k(\mathfrak{p})[x, y]$, para ciertos r, $t \in D$. El cambio de variables $X' = X + r$, $Y = Y' + t$ nos transforma la ecuación de Weierstrass (sin cambiar el modelo W) en otra para la cual el punto singular de $W_\mathfrak{p}$ es (x, y), lo cual equivale a que $\mathfrak{p} \mid a_3,\ a_4,\ a_6$. (Ver la prueba del teorema 4.24.)

Teorema 5.11 *Sea D un dominio de Dedekind, sea $S = \operatorname{Esp} D$, sea W/S un modelo de Weierstrass y sea $\mathfrak{p}$ un divisor primo de D tal que $\mathfrak{p} \mid a_3,\ a_4,\ a_6$, de modo que la fibra $W_\mathfrak{p}$ tiene un (único) punto singular P. Se cumple que P es regular en W si y sólo si $\mathfrak{p}^2 \nmid a_6$.*

DEMOSTRACIÓN: Sea $S' = \operatorname{Esp} \mathcal{O}_{S,\mathfrak{p}} = \operatorname{Esp} D_\mathfrak{p}$ y sea

$$W' = W \times_S S' = \operatorname{Proy}(D_\mathfrak{p}[X, Y, Z]/(F)),$$

donde F es la ecuación de Weierstrass, luego W' es también un modelo de Weierstrass correspondiente a la misma ecuación, pero ahora sobre $D_\mathfrak{p}$. Además, el teorema [E 3.47] nos da que P se corresponde con un punto $P' \in W'$ tal que $\mathcal{O}_{W,P} \cong \mathcal{O}_{W',P'}$. Como la regularidad de P es, por definición, la regularidad del anillo $\mathcal{O}_{W,P}$, vemos con esto que no perdemos generalidad si suponemos que D es un dominio de Dedekind local, de modo que $\mathfrak{p} = (\pi)$ es un ideal principal.

Podemos trabajar en el abierto afín U de W definido por la ecuación de Weierstrass afín. La fibra $U_\mathfrak{p}/k(\mathfrak{p})$ es la curva definida por la ecuación de Weierstrass

$$Y^2 + \bar{a}_1 XY = X^3 + \bar{a}_2 X^2,$$

cuyo punto singular es el ideal (x, y) de $k(\mathfrak{p})[x, y]$, que se corresponde con el ideal (π, x, y) de $D[x, y]$. Es claro que $\dim \mathcal{O}_{W,P} = 2$, luego P es regular en W si y sólo si (π, x, y) admite un generador con dos elementos.

Si $\mathfrak{p}^2 \nmid a_6$, entonces $a_6 = \epsilon\pi$, donde ϵ es una unidad de D. Los generadores x, y cumplen la ecuación de weierstrass

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

y en ella podemos sustituir $a_6 = \epsilon\pi$ y despejar π, lo que prueba que $\pi \in (x, y)$, luego $(x, y, \pi) = (x, y)$, con lo que P es regular.

Supongamos ahora que $\mathfrak{p}^2 \mid a_6$. Ahora hemos de ver que $\bar{\pi}$, $\bar{x}$, $\bar{y} \in \mathfrak{m}_P/\mathfrak{m}_P^2$ son linealmente independientes sobre $k(\mathfrak{p}) = D[x, y]/\mathfrak{p}$. Tomemos $\bar{\alpha}$, $\bar{\beta}$, $\bar{\gamma} \in k(\mathfrak{p})$ y supongamos que $\bar{\alpha}\bar{\pi} + \bar{\beta}\bar{x} + \bar{\gamma}\bar{y} \in \mathfrak{m}_P^2$. Esto significa que

$$\alpha\pi + \beta x + \gamma y = u/v,$$

con $u \in (\pi, x, y)^2$, $v \notin (\pi, x, y)$. Sea f la ecuación de Weierstrass (afín), de modo que

$$D[x, y] = D[X, Y]/(f).$$

Pongamos que $u = \bar{U}$, $v = \bar{V}$, de modo que

$$V(\alpha\pi + \beta X + \gamma Y) - U \in (f).$$

Teniendo en cuenta que $\pi \mid a_3, a_4, a_6$, es claro que $f \in (\pi, X, Y)^2$, luego

$$V(\alpha\pi + \beta X + \gamma Y) \in (\pi^2, X^2, Y^2, XY, \pi X, \pi Y),$$

donde $V \notin (\pi, X, Y)$, lo cual significa que es un polinomio con término independiente no divisible entre π. Es claro entonces que $\pi \mid \alpha, \beta, \gamma$, luego $\bar{\alpha} = \bar{\beta} = \bar{\gamma} = 0$. ∎

Ejemplo Consideremos el modelo de Weierstrass $W/\mathbb{Z}$ correspondiente a la ecuación

$$Y^2 = X^3 + 2X^2 + 6.$$

El discriminante es $\Delta = -2^6 \cdot 3 \cdot 97$, luego las fibras singulares son W_2, W_3 y W_{97}. que son las curvas dadas por las ecuaciones siguientes:

$$W_2: \quad Y^2 = X^3, \quad W_3: \quad Y^2 = X^2(X+2), \quad W_{97}: \quad Y^2 = (X+66)^2(X+64).$$

En el caso de W_2, el punto singular es claramente $(2, x, y)$. Como $2^2 \nmid 6$, el teorema anterior prueba que el punto es regular en W. El punto singular de W_3 es $(3, x, y)$, y nuevamente concluimos que es regular en W.

El punto singular de W_{97} es $(97, x - 31, y)$, y el cambio $X = X' + 31$ transforma a_6 en

$$a_6' = a_6 + r^2 a_2 + r^3 = 6 + 31^2 \cdot 2 + 31^3 = 3 \cdot 97 \cdot 109.$$

Como no es divisible entre 97^2, este punto también es regular en W, y concluimos que el modelo W/S es regular, es decir, es una superficie aritmética. ∎

Ejemplo Consideremos ahora el modelo de Weierstrass $W/\mathbb{Z}$ dado por la ecuación

$$Y^2 = X^3 + 2X^2 + 4.$$

El discriminante es $\Delta = -2^8 \cdot 5 \cdot 7$, por lo que hay tres fibras singulares. El punto singular de W_2 es $(2, x, y)$, pero ahora resulta que es singular en W, ya que $2^2 \mid a_6$. El punto singular de W_5 es $(5, x - 2, y)$, y es regular en W, pues el cambio de variable $X = X' + 2$ transforma a_6 en

$$a_6' = a_6 + r^2 a_2 + r^3 = 20.$$

El punto singular de W_7 es $(7, x - 1, y)$, que también es regular, pues ahora $a_6' = 7$. Así pues, W tiene tres puntos no suaves, pero sólo un punto singular. ∎

Vemos así cómo las curvas elípticas de los dos ejemplos anteriores tienen la misma reducción módulo 2, a saber, la cúbica singular $Y^2 = X^3$ y, sin embargo, acabamos de encontrar una diferencia entre ellas: la primera define un modelo de Weierstrass regular sobre $\mathbb{Z}_2$ mientras que la segunda define un modelo singular. El ejemplo siguiente muestra que, cuando el modelo de Weierstrass es singular, podemos encontrar otro modelo de la misma curva que sea regular:

Ejemplo Sea $W/\mathbb{Z}_5$ el modelo de Weierstrass de la curva elíptica $E/\mathbb{Q}$ dada por la ecuación

$$Y^2 = X^3 + 25.$$

Observemos que el anillo $\mathbb{Z}_5$ es un anillo de valoración discreta, por lo que W tiene únicamente dos fibras: la curva elíptica sobre $\mathbb{Q}$ determinada por la ecuación y su reducción módulo 5. Vemos que ésta tiene un punto singular $\mathfrak{p} = (5, x, y)$. Consideremos, por otra parte, la superficie fibrada

$$\mathcal{X} = \mathrm{Proy}(\mathbb{Z}_5[X, Y, Z]/(Y^2Z - 5X^3 - Z^3)).$$

Su fibra genérica es la curva proyectiva $\mathcal{X}_\eta/\mathbb{Q}$ definida por la ecuación

$$Y^2Z = 5X^3 + Z^3.$$

El cambio de variables $X = 5X'$, $Y = 5Y'$, $Z' = Z$ determina un automorfismo de $\mathbb{Q}[X, Y, Z]$ que transforma la ecuación de Weierstrass $Y^2Z - X^3 - 25Z^3$ en $25(Y^2Z - 5X^3 - Z^3)$, este automorfismo induce a su vez un isomorfismo[1] $\mathcal{X}_\eta \cong E$.

Por otra parte, la fibra cerrada $\mathcal{X}_5$ es la curva proyectiva sobre $K = \mathbb{Z}/5\mathbb{Z}$ determinada por la ecuación

$$Z(Y + Z)(Y - Z) = 0.$$

Se trata de una curva plana reducida, con tres componentes irreducibles, las tres isomorfas a P^1_k, luego todos sus puntos son geométricamente regulares salvo el punto de intersección, que es $\mathfrak{q} = (5, y, z)$, que es necesariamente singular, pues por él pasan las tres rectas. Así pues, todos los puntos de $\mathcal{X}/\mathbb{Z}_5$ son suaves (y, en particular, regulares) excepto $\mathfrak{q}$. Por otra parte, el teorema 5.8 nos da que $\mathcal{X}/\mathbb{Z}_5$ es normal, luego $\mathcal{X}/\mathbb{Z}_5$ es también un modelo de la curva $E/\mathbb{Q}$.

Sin embargo, a diferencia de $W/\mathbb{Z}_5$, resulta que $\mathcal{X}/\mathbb{Z}_5$ es regular. En efecto, sólo hemos de probar que $\mathfrak{q}$ es regular, para lo cual podemos restringirnos al abierto afín U/S que resulta de deshomogeneizar la ecuación respecto de X:

$$Y^2Z - Z^3 = 5.$$

Como punto de U, tenemos igualmente que $\mathfrak{q} = (5, y, z)$, y lo mismo es cierto si consideramos a $\mathfrak{q}$ como punto de $\mathcal{O}_{X,\mathfrak{q}}$. La regularidad equivale a que podamos eliminar un generador, pero la ecuación muestra que $5 \in (y, z)$, luego $\mathfrak{q} = (y, z)$ y concluimos que $\mathfrak{q}$ es regular en $\mathcal{X}$. ∎

5.2 Explosiones

Las explosiones son una familia muy amplia de homomorfismos birracionales entre esquemas, que, según veremos, nos permitirán resolver las singularidades

[1] Notemos que esto implica que la ecuación es irreducible en $\mathbb{Q}[X, Y, Z]$ y, como sus coeficientes son primos entre sí, también lo es en $\mathbb{Z}_5[X, Y, Z]$, lo que justifica que X es realmente una superficie fibrada.

de las superficies fibradas, es decir, transformar una superficie fibrada singular en otra regular. Empezamos definiéndolas en el caso de esquemas afines.

Sea A un anillo noetheriano e I un ideal de A. Consideramos la A-álgebra graduada

$$\widetilde{A} = \bigoplus_{d\geq 0} I^d,$$

donde entendemos que $I^0 = A$. Pongamos que $I = (f_1, \ldots, f_n)$, y vamos a identificar cada f_i con el correspondiente elemento de $\widetilde{A}_0$, es decir, con $(f_i, 0, 0, \ldots)$, mientras que llamaremos $t_i = (0, f_i, 0, 0, \ldots) \in \widetilde{A}_1$. Es claro que $t_1, \ldots, t_m$ son un generador de $\widetilde{A}$ como A-álgebra. Observemos también que si $P(T_1, \ldots, T_n)$ es un polinomio homogéneo con coeficientes en A, entonces $P(t_1, \ldots, t_n) = 0$ si y sólo si $P(f_1, \ldots, f_n) = 0$.

Definición 5.12 Si $X = \operatorname{Esp} A$ es un esquema afín noetheriano y C es un subesquema cerrado, que será de la forma $C = \operatorname{Esp}(A/I)$, para cierto ideal I, llamaremos *explosión* de X con centro (o sobre) C al esquema $\widetilde{X} = \operatorname{Proy}\widetilde{A}$. La estructura de A-álgebra de $\widetilde{A}$ determina un homomorfismo $\pi : \widetilde{X} \longrightarrow X$.

Veamos algunas propiedades:

a) $\widetilde{X} = \varnothing$ si y sólo si I es nilpotente (lo que equivale a que $C_{\mathrm{red}} = X_{\mathrm{red}}$).

   En efecto, $\widetilde{X} = \varnothing$ si y sólo si todos los t_i son nilpotentes, lo que equivale a que lo sean todos los f_i, lo que equivale a que lo sea I.

b) $\widetilde{A}$ es reducido o íntegro si y sólo si lo es A.

   Una implicación es obvia. Pongamos que A es íntegro pero que $a, b \in \widetilde{A}$ cumplen $ab = 0$, pero $a \neq 0 \neq b$. Sean a_m y b_n sus componentes homogéneas de mayor grado. Entonces $a_m b_n = 0$ (en A) y ambos factores son no nulos, contradicción. El argumento para anillos reducidos es análogo.

c) Sea B una A-álgebra plana y sea $\widetilde{B}$ la B-álgebra graduada asociada a al ideal IB. Entonces $\widetilde{B} \cong B \otimes_A \widetilde{A}$.

   En efecto, $I^d \otimes_A B \cong I^d B = (IB)^d$, por lo que

$$\widetilde{B} \cong \bigoplus_{d\geq 0} I^d \otimes_A B \cong \widetilde{A} \otimes_A B.$$

d) Si I está generado por un elemento regular f_1, entonces $\widetilde{A} \cong A[X]$, por lo que $\widetilde{X} \cong X$.

   En efecto, el homomorfismo $\phi : A[X] \longrightarrow \widetilde{A}$ dado por $X \mapsto t_1$ es claramente un isomorfismo.

e) En general, consideremos el epimorfismo $\phi : A[X_1, \ldots, X_n] \longrightarrow \widetilde{A}$ dado por $X_i \mapsto t_i$. Si llamamos $x_i = X_i/X_1$, tenemos que ϕ induce un epimorfismo $\phi_1 : A[x_2, \ldots, x_n] \longrightarrow \widetilde{A}_{(t_1)}$ dado por $x_i \mapsto t_i/t_1$. Vamos a probar que un polinomio $P \in A[x_2, \ldots, x_n]$ está en el núcleo de ϕ_1 si y sólo si existe un $d \geq 0$ tal que $f_1^d P \in (f_1x_2 - f_2, \ldots, f_1x_n - f_n)$.

En efecto, es claro que cada $f_1x_i - f_i$ está en el núcleo de ϕ_1, luego si $f_1^d P$ está en el ideal generado por estos polinomios, entonces $f_1^d\phi_1(P) = 0$. Pongamos que $\phi_1(P) = u/t_1^n$, donde $u \in I^n$. Entonces $t_1^m f_1^d u = 0$, para cierto $m \geq 0$, luego $f_1^{m+d}u = 0$, luego $\phi_1(P) = 0$.

Consideremos ahora un polinomio P arbitrario. Dividiendo en el anillo $A_{f_1}[x_3, \ldots, x_n][x_2]$ podemos descomponer

$$f_1^{d_1} P = Q_1(x_2, \ldots, x_n)(f_1x_2 - f_2) + R_1(x_3, \ldots, x_n),$$

para ciertos polinomios Q_1, R_1 con coeficientes en A y cierto $d_1 \geq 0$. (Notemos que para que exista la división euclídea f_1 ha de ser una unidad.) Ahora dividimos R_1 entre $f_1x_3 - f_3$ y, tras un número finito de pasos, llegamos a que

$$f_1^d P = \sum_{i=2}^{n} Q_i(f_1x_i - f_i) + a,$$

para cierto $a \in A$ y cierto $d \geq 0$.

Si P está en el núcleo de ϕ_1, entonces a es nulo en $\widetilde{A}_{(t_1)}$, luego existe un $r \geq 0$ tal que $t_1^r a = 0$, lo que equivale a $f_1^r a = 0$. Multiplicando por f_1^r la igualdad anterior obtenemos otra igual pero con $a = 0$.

f) Consideremos ahora el homomorfismo $\psi : A[x_2, \ldots, x_n] \longrightarrow A_{f_1}$ dado por $x_i \mapsto f_i/f_1$. El mismo razonamiento anterior nos da que su núcleo es el mismo que el de ϕ, luego $\widetilde{A}_{(t_1)}$ es isomorfo a la subálgebra de A_{f_1} generada por los elementos f_i/f_1.

g) En particular, si X es un esquema íntegro y ningún f_i es nulo, el esquema $\widetilde{X}$ es la unión de los abiertos principales $U_i = D(t_i)$, que son de la forma $U_i = \operatorname{Esp} A_i$, donde A_i es la A-álgebra generada por los f_j/f_i en el cuerpo de cocientes de A.

h) Consideremos el ideal homogéneo $J = (f_iX_j - f_jX_i)_{i,j}$, que claramente está contenido en el núcleo de ϕ, y llamemos $Z = \operatorname{Proy}(A[X_1, \ldots, X_n]/J)$, que es un subesquema cerrado de P_A^{n-1} y ϕ induce una inmersión cerrada $\widetilde{X} \longrightarrow Z$. Vamos a probar que si Z es íntegro y $f_1, \ldots, f_n$ es un generador minimal de I, entonces $\widetilde{X} \cong Z$.

Para ello basta probar que la inmersión cerrada entre los abiertos principales determinados por t_i y X_i, respectivamente, lo que equivale a comprobar que ϕ induce un isomorfismo

$$(A[X_1, \ldots, X_n]/J)_{([X_i])} \cong \widetilde{A}_{(t_i)}.$$

No perdemos generalidad si suponemos $i = 1$. El miembro izquierdo es igual a $A[x_2, \ldots, x_n]/J_1$, donde $J_1 = (f_i x_j - f_j x_i)_{i,j}$, entendiendo que $x_1 = 1$. Este ideal coincide con $J_1' = (f_1 x_j - f_j)_{j\geq 2}$, pues, módulo J_1', se cumple que $f_j = f_1 x_j$, para $j \geq 1$, luego $f_i x_j - f_j x_i = f_1 x_i x_j - f_1 x_j x_i = 0$.

Hemos de probar que J_1' es el núcleo de ϕ_1, el cual, según hemos probado, está formado por los polinomios P tales que $f_1^d P \in J_1'$. Como Z es íntegro, sabemos que J_1' es primo, luego basta probar que $f_1 \notin J_1'$, pues entonces la condición $f_1^d P \in J_1'$ equivaldrá a $P \in J_1'$. Ahora bien, si $f_1 \in J_1'$, entonces es combinación lineal de los polinomios $f_1 x_i - f_j$ (con coeficientes polinómicos). Igualando los términos independientes obtenemos que f_1 es combinación lineal de $f_2, \ldots, f_n$ con coeficientes en A, lo que contradice la hipótesis de que $f_1, \ldots, f_n$ es un generador minimal de I.

En realidad el concepto de explosión que hemos considerado hasta ahora es la versión local del concepto general que construiremos a continuación.

Definición 5.13 Sea X un esquema. Una $\mathcal{O}_X$-álgebra graduada $\mathcal{B}$ es un haz cuasicoherente de $\mathcal{O}_X$-álgebras con una graduación $\mathcal{B} = \bigoplus_{n\geq 0} \mathcal{B}_n$, donde los $\mathcal{B}_n$ son $\mathcal{O}_X$-módulos cuasicoherentes.

Teorema 5.14 *Sea X un esquema y $\mathcal{B}$ una $\mathcal{O}_X$-álgebra graduada. Entonces existe (salvo isomorfismo) un único X-esquema $f : \operatorname{Proy}\mathcal{B} \longrightarrow X$ tal que existe una familia de isomorfismos $h_U : f^{-1}[U] \longrightarrow \operatorname{Proy}\mathcal{B}(U)$ compatible con las restricciones, donde U recorre los abiertos afines de X.*

Demostración: En primer lugar observemos que si $U \subset X$ es un abierto afín, entonces $\mathcal{B}(U)$ es una $\mathcal{O}_X(U)$-álgebra graduada, luego existe un homomorfismo natural $\operatorname{Proy}\mathcal{B}(U) \longrightarrow U$. Vamos a ver que si $V \subset U$ son abiertos afines en X, entonces existe un isomorfismo natural $\operatorname{Proy}\mathcal{B}(V) \cong \operatorname{Proy}\mathcal{B}(U) \times_U V$. Esto nos da a su vez una inmersión abierta

$$\operatorname{Proy}\mathcal{B}(V) \cong \operatorname{Proy}\mathcal{B}(U) \times_U V \longrightarrow \operatorname{Proy}\mathcal{B}(U) \times_U U \cong \operatorname{Proy}\mathcal{B}(U).$$

Más precisamente, $\operatorname{Proy}\mathcal{B}(V)$ se identifica así con la antiimagen de V en $\operatorname{Proy}\mathcal{B}(U)$. Es con estas inmersiones con las que han de ser compatibles los homomorfismos h_U del enunciado. Por otra parte, conviene observar que estas inmersiones no son sino los homomorfismos inducidos por la restricción $\mathcal{B}(U) \longrightarrow \mathcal{B}(V)$, que es un homomorfismo graduado.

Supongamos en primer lugar que $V = D(a)$, para un cierto $a \in \mathcal{O}_X(U)$. Entonces $\mathcal{O}_X(V) = \mathcal{O}_X(U)_a$ y $\mathcal{B}(V) = \mathcal{B}(U)_a = \mathcal{B}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{O}_X(V)$, y basta aplicar el teorema [3.48].

Si $V \subset U$ es un abierto afín arbitrario, podemos cubrirlo por abiertos principales $W \subset U$, que serán también principales en V. Por la parte ya probada, los esquemas $\operatorname{Proy}\mathcal{B}(W)$ se identifican con los esquemas $\operatorname{Proy}\mathcal{B}(V) \times_V W$, que forman un cubrimiento abierto de $\operatorname{Proy}\mathcal{B}(V) \times_V V \cong V$ y, por otra parte, se identifican con los esquemas $\operatorname{Proy}B(U) \times_U W$, que forman un cubrimiento

abierto de $\operatorname{Proy}\mathcal{B}(U)\times_U V$. Estos isomorfismos se extienden a un isomorfismo $V\cong\operatorname{Proy}\mathcal{B}(U)\times_U V$.

Pasemos ya a la prueba del teorema. La unicidad es inmediata, y los resultados que acabamos de obtener prueban la existencia cuando X es afín, pues en tal caso basta tomar $\operatorname{Proy}\mathcal{B}=\operatorname{Proy}\mathcal{B}(X)$.

También es inmediato que si existe $\operatorname{Proy}\mathcal{B}$ y $U\subset X$ es un abierto arbitrario, entonces existe $\operatorname{Proy}(\mathcal{B}|_U)=(\operatorname{Proy}\mathcal{B})\times_X U$. (Si $V\subset U$ es un abierto afín, su antiimagen en $\operatorname{Proy}(\mathcal{B}|_U)$ es $(\operatorname{Proy}\mathcal{B})\times_X V$, que se identifica con su antiimagen en $\operatorname{Proy}\mathcal{B}$ y, por consiguiente, con $\operatorname{Proy}\mathcal{B}(V)=\operatorname{Proy}\mathcal{B}|_U(V)$.)

Todo esto implica que existe $\operatorname{Proy}\mathcal{B}|_U$, donde U recorre todos los abiertos de X contenidos en un abierto afín. Ahora consideramos la familia $\{U_i\}_i$ de todos los abiertos afines de X, que determina a su vez la familia de esquemas $\pi_i: X_i=\operatorname{Proy}\mathcal{B}(U_i)\longrightarrow U_i\subset X$, definidos sobre X.

Consideramos $X_{ij}=\pi_i^{-1}[U_i\cap U_j]$, que es un subesquema abierto de X_i que cumple las condiciones de $\operatorname{Proy}\mathcal{B}|_{U_i\cap U_j}$. La unicidad nos da un isomorfismo $f_{ij}: X_{ij}\longrightarrow X_{ji}$. Más concretamente, existe un único isomorfismo f_{ij} tal que, para cada abierto afín $W\subset U_i\cap U_j$, se restrinja a la identidad en $\operatorname{Proy}\mathcal{B}(W)$ a través de las inmersiones canónicas

$$\operatorname{Proy}\mathcal{B}(W)\cong\operatorname{Proy}\mathcal{B}(U_i)\times_{U_i}W\longrightarrow\operatorname{Proy}\mathcal{B}(U_i)\times_{U_i}U_i\cong\operatorname{Proy}\mathcal{B}(U_i),$$

$$\operatorname{Proy}\mathcal{B}(W)\cong\operatorname{Proy}\mathcal{B}(U_j)\times_{U_j}W\longrightarrow\operatorname{Proy}\mathcal{B}(U_j)\times_{U_j}U_j\cong\operatorname{Proy}\mathcal{B}(U_j).$$

Esta unicidad hace que se cumplan las hipótesis del teorema [3.40], que nos da un esquema $f:\operatorname{Proy}\mathcal{B}\longrightarrow X$ que contiene como subesquemas abiertos a los esquemas $\operatorname{Proy}\mathcal{B}(U)$. Más concretamente, $\operatorname{Proy}\mathcal{B}(U)=f^{-1}[U]$, pues si un punto $P\in\operatorname{Proy}\mathcal{B}$ cumple que $f(P)\in U$, entonces existe un abierto afín V tal que $P\in\operatorname{Proy}\mathcal{B}(V)$, luego existe un abierto afín tal que $P\in W\subset U\cap V$, luego $P\in f|_U^{-1}[W]=\operatorname{Proy}\mathcal{B}(W)\subset\operatorname{Proy}\mathcal{B}(U)$. Esto prueba el teorema. ∎

Definición 5.15 En las condiciones del teorema anterior, si $Y=\operatorname{Proy}\mathcal{B}$ y $U\subset X$ es un abierto afín, en $\operatorname{Proy}\mathcal{B}(U)$ tenemos definido el haz inversible $\mathcal{O}(1)$ y, si $V\subset U$ es otro abierto afín, se comprueba que $\mathcal{O}(1)$ se restringe al correspondiente haz de $\operatorname{Proy}\mathcal{B}(V)$. (Basta probarlo cuando V es un abierto principal de U, en cuyo caso conocemos explícitamente la inmersión abierta.) Esto hace que los haces $\mathcal{O}(1)$ se extienden a un haz inversible en Y, al que llamaremos $\mathcal{O}_Y(1)$. Notemos que $\mathcal{O}_Y(1)$ no depende únicamente del esquema Y, sino de la $\mathcal{O}_X$-álgebra $\mathcal{B}$.

Ejemplo Si X es un esquema arbitrario, llamamos $\mathcal{O}_X[T_0,\dots,T_r]$ a la $\mathcal{O}_X$-álgebra graduada determinada por que, para cada abierto $U\subset X$, se cumple que $(\mathcal{O}_X[T_0,\dots,T_r])(U)=\mathcal{O}_X(U)[T_0,\dots,T_r]$, con las restricciones inducidas por las restricciones de X. Sea $P=\operatorname{Proy}(\mathcal{O}_X[T_0,\dots,T_r])$ y $\pi: P\longrightarrow X$ el homomorfismo estructural. Entonces, P está determinado por que, para cada abierto afín $U\subset X$, se cumple que

$$\mathcal{O}_P(\pi^{-1}[U])\cong\operatorname{Proy}(\mathcal{O}_X(U)[T_0,\dots,T_r])=\mathrm{P}^r_U\,.$$

Obviamente esto lo cumple el espacio P^r_X, luego, por la unicidad, concluimos que $\mathrm{P}^r_X = \mathrm{Proy}(\mathcal{O}_X[T_0,\dots,T_r])$. Teniendo en cuenta la definición anterior y las observaciones tras la definición [5.49], es claro que el haz $\mathcal{O}_{\mathrm{P}^r_X}(1)$ es el mismo en el sentido de ambas definiciones. ∎

Definición 5.16 Sea X un esquema localmente noetheriano y sea Z un subesquema cerrado, determinado por un haz coherente $\mathcal{I}$ de ideales de $\mathcal{O}_X$. Llamamos *explosión* de X con centro Z al esquema $\widetilde{X} = \mathrm{Proy}\bigoplus_{n\geq 0}\mathcal{I}^n \longrightarrow X$, entendiendo que $\mathcal{I}^0 = \mathcal{O}_X$.

Notemos que si X es afín entonces $\mathcal{I} = \widetilde{I}$, para cierto ideal I de $\mathcal{O}_X(X)$, y entonces $\widetilde{X}$ coincide con el definido en 5.12. Más aún, por el teorema anterior, si $U \subset X$ es un abierto afín, entonces la restricción de $\pi : \widetilde{X} \longrightarrow X$ a $\pi^{-1}[U]$ es la explosión de U con centro $Z \cap U$ (con la estructura de subesquema cerrado determinada por $\mathcal{I}|_U$). En otros términos, toda explosión es localmente la explosión de un esquema afín.

Veamos ahora las propiedades básicas de las explosiones, para lo que conviene introducir la notación siguiente:

En general, si $f : Y \longrightarrow X$ es un homomorfismo de esquemas e $\mathcal{I}$ es un haz cuasicoherente de ideales de $\mathcal{O}_X$, entonces tenemos un homomorfismo canónico $f^*\mathcal{I} \longrightarrow f^*\mathcal{O}_X = \mathcal{O}_Y$. Llamaremos $\mathcal{I}\mathcal{O}_Y$ a su imagen.

Teorema 5.17 *Sea X un esquema localmente noetheriano, sea Z un subesquema cerrado determinado por un haz cuasicoherente $\mathcal{I}$ de ideales de $\mathcal{O}_X$ y llamemos $\pi : \widetilde{X} \longrightarrow X$ a la explosión de centro Z. Entonces:*

a) π es un isomorfismo si y sólo si $\mathcal{I}$ es inversible.

b) $\pi : \widetilde{X} \longrightarrow X$ es un homomorfismo propio.

c) Si $f : Y \longrightarrow X$ es un homomorfismo plano de esquemas localmente noetherianos y $\rho : \widetilde{Y} \longrightarrow Y$ es la explosión de Y con centro en el subesquema determinado por $\mathcal{I}\mathcal{O}_Y$, entonces $\widetilde{Y} \cong \widetilde{X} \times_X Y$.

d) π se restringe a un isomorfismo $\pi^{-1}[X \setminus Z] \longrightarrow X \setminus Z$.

e) Si X es íntegro, $\widetilde{X}$ también lo es, y si $\mathcal{I} \neq 0$ entonces π es birracional y, por consiguiente, $\dim \widetilde{X} = \dim X$.

f) $\mathcal{I}\mathcal{O}_{\widetilde{X}} = \mathcal{O}_{\widetilde{X}}(1)$. En particular $\mathcal{I}\mathcal{O}_{\widetilde{X}}$ es un haz inversible.

g) Si X es afín, entonces $\mathcal{O}_{\widetilde{X}}(1)$ es muy amplio respecto a π.

Demostración: a) Si $\mathcal{I}$ es inversible, entonces X puede cubrirse por abiertos afines U tales que $\mathcal{I}(U)$ está generado por un elemento regular, luego la propiedad d) tras la definición 5.12 nos da que π es un isomorfismo.

Si π es un isomorfismo, la propiedad f) de este teorema (cuya prueba no usa este apartado) implica que $\mathcal{I}\mathcal{O}_{\widetilde{X}} = \mathcal{I}$ es inversible.

b) Si X es afín, entonces π es obviamente proyectivo, luego propio sobre X. Ser propio es local en la base, luego todas las explosiones son propias.

c) Sea $U \subset X$ un abierto afín y $V \subset f^{-1}[U]$ un abierto afín. La propiedad c) tras la definición 5.12 implica que $\widetilde{V} \cong \widetilde{U} \times_U V = \widetilde{U} \times_X V$. Los dos miembros son abiertos en $\widetilde{Y}$ y $\widetilde{X} \times_X Y$, respectivamente, y al variar U y V cubren ambos esquemas. Es fácil ver que los isomorfismos son consistentes entre sí, por lo que se extienden a un isomorfismo entre los espacios completos.

d) Sea $U = X \setminus Z$. Entonces $\mathcal{I}|_U = \mathcal{O}_X$, luego a) implica que la explosión $\widetilde{U} = \pi^{-1}[U] \longrightarrow U$ es un isomorfismo.

e) La propiedad b) tras la definición 5.12 implica que $\widetilde{X}$ es localmente íntegro. Basta probar que es conexo. Si $\widetilde{X} = U \cup V$, donde U y V son abiertos no vacíos, entonces ha de ser $\pi^{-1}[X \setminus Z] \subset U$. Tomemos $P \in V$, de modo que $\pi(P) \in Z$, sea W un entorno afín de $\pi(P)$, que necesariamente cortará a $X \setminus Z$. Cualquier punto $Q \in W \setminus Z$ tiene una antiimagen $Q' \in U$, pero entonces es claro que $\pi^{-1}[W]$ no puede ser conexo, pero ha de serlo por la propiedad b) citada.

Si $\mathcal{I} \neq 0$ (puesto que X es íntegro) la propiedad a) tras la definición 5.12 implica que $\pi^{-1}[X \setminus Z] \neq \varnothing$, luego π es birracional. La igualdad de las dimensiones se sigue del teorema 3.10.

f) No perdemos generalidad si suponemos que $X = \operatorname{Esp} A$, en cuyo caso $\mathcal{I} = \widetilde{I}$, donde $I = (f_1, \ldots, f_n)$ es un ideal de A. A partir de aquí usamos la notación previa a la definición 5.12. Sea $U_i = D(t_i)$, la restricción $\pi|_{U_i} : U_i \longrightarrow X$ se corresponde con el homomorfismo natural $A \longrightarrow \widetilde{A}_{(t_i)}$.

Por otra parte, $(\pi^*\mathcal{I})(U_i) = I \otimes_A \widetilde{A}_{(t_i)}$, de donde se sigue que $(\mathcal{I}\mathcal{O}_{\widetilde{X}})(U_i)$ es el ideal de $\widetilde{A}_{(t_i)}$ generado por $f_1, \ldots, f_n$. Ahora bien, como $f_j = f_i(t_j/t_i)$, resulta que $(\mathcal{I}\mathcal{O}_{\widetilde{X}})(U_i)$ está generado por f_i, mientras que el $\mathcal{O}_{\widetilde{X}}(U_i)$-módulo $\mathcal{O}_{\widetilde{X}}(1)(U_i)$ está generado por t_i. Las relaciones

$$f_j = f_i(t_j/t_i), \qquad t_j = t_i(t_j/t_i)$$

implican que los isomorfismos dados por $f_i \mapsto t_i$ se extienden a un isomorfismo $\mathcal{I}\mathcal{O}_{\widetilde{X}} \cong \mathcal{O}_{\widetilde{X}}(1)$.

g) Mantenemos la notación del apartado anterior. El epimorfismo natural $A[X_1, \ldots, X_n] \longrightarrow \widetilde{A}$ induce una inmersión cerrada $i : \widetilde{X} \longrightarrow \mathrm{P}^{n-1}_A$, y es claro que $i^*\mathcal{O}_{\mathrm{P}^{n-1}_A}(1) = \mathcal{O}_{\widetilde{X}}(1)$. ∎

Ahora demostraremos que la explosión de un esquema proyectivo es proyectiva. Para ello necesitamos un resultado previo.

Teorema 5.18 *Sea X un esquema, $\mathcal{B}$ una $\mathcal{O}_X$-álgebra graduada y $\mathcal{N}$ un haz inversible en X. Sea $\mathcal{C}$ la $\mathcal{O}_X$-álgebra graduada dada por $\mathcal{C}_n = \mathcal{N}^n \otimes_{\mathcal{O}_X} \mathcal{B}_n$. Entonces existe un isomorfismo $\rho : \operatorname{Proy} \mathcal{B} \longrightarrow \operatorname{Proy} \mathcal{C}$ tal que $\rho^*\mathcal{O}_{\operatorname{Proy} \mathcal{C}}(1) = \mathcal{O}_{\operatorname{Proy} \mathcal{B}}(1)$.*

DEMOSTRACIÓN: Es fácil ver que $\mathcal{C}$ tiene una estructura natural de $\mathcal{O}_X$-álgebra graduada. Sea $\{U_i\}$ un cubrimiento de X por abiertos afines tales que existen isomorfismos $\phi_i : \mathcal{N}|_{U_i} \longrightarrow \mathcal{O}_{U_i}$. Éstos inducen claramente isomorfismos de $\mathcal{O}_X(U_i)$-álgebras $\psi_i : \mathcal{C}|_{U_i} \longrightarrow \mathcal{B}|_{U_i}$, que a su vez inducen isomorfismos de esquemas $\rho_i : (\operatorname{Proy}\mathcal{B})|_{U_i} \longrightarrow (\operatorname{Proy}\mathcal{C})|_{U_i}$. Si partimos de otros isomorfismos ϕ_i' llegamos a otros isomorfismos ρ_i', de forma que $\rho_i' \circ \rho_i^{-1}$ es el automorfismo inducido por $\phi_i' \circ \phi_i^{-1} : \mathcal{O}_{U_i} \longrightarrow \mathcal{O}_{U_i}$, que necesariamente está inducido por la multiplicación por un $a_i \in \mathcal{O}_X(U_i)^*$. Ahora bien, es claro que esto induce la identidad sobre $\operatorname{Proy}\mathcal{B}(U_i)$ (induce la identidad en cada anillo $\mathcal{B}(U_i)_{(t)}$), luego concluimos que $\rho_i = \rho_i'$. Teniendo esto en cuenta es fácil ver que los ρ_i se extienden a un isomorfismo ρ, como indica el enunciado. La última igualdad se sigue de una comprobación rutinaria a partir de la construcción. ∎

Teorema 5.19 *Sea A un anillo noetheriano y X/A un esquema cuasiproyectivo sobre A. Si $\pi : \widetilde{X} \longrightarrow X$ es una explosión con centro en el subesquema cerrado asociado a un haz de ideales $\mathcal{I}$, entonces π es proyectivo sobre A y $\mathcal{I}\mathcal{O}_{\widetilde{X}}$ es un haz muy amplio para π.*

DEMOSTRACIÓN: Sea $\mathcal{N}$ un haz amplio en X. Sustituyéndolo por una potencia, podemos suponer que $\mathcal{N}\otimes_{\mathcal{O}_X}\mathcal{I}$ tiene un generador global. (Observemos que $\mathcal{I}$ es finitamente generado, pues X es noetheriano.) Consideremos la $\mathcal{O}_X$-álgebra

$$\mathcal{C} = \bigoplus_{n\geq 0} (\mathcal{N}^n \otimes_{\mathcal{O}_X} \mathcal{I}^n).$$

(Notemos que la primera potencia se refiere al producto tensorial, mientras que la segunda al producto de ideales.) El teorema anterior nos da un isomorfismo $\rho : \widetilde{X} \longrightarrow \operatorname{Proy}\mathcal{C}$. Llamemos $f : \operatorname{Proy}\mathcal{C} \longrightarrow X$ al homomorfismo natural. El hecho de que $\mathcal{C}_1$ tenga un generador global implica (por el teorema [5.32]) que existe un epimorfismo $\mathcal{O}_X^{r+1} \longrightarrow \mathcal{C}_1$. Este epimorfismo induce a su vez un epimorfismo $\mathcal{O}_X[T_0,\ldots,T_r] \longrightarrow \mathcal{C}$, el cual induce a su vez una inmersión cerrada

$$i : \operatorname{Proy}\mathcal{C} \longrightarrow \mathrm{P}^r_X,$$

de modo que $i^*\mathcal{O}_{\mathrm{P}^r_X}(1) = \mathcal{O}_{\operatorname{Proy}\mathcal{C}}(1)$. Ahora basta considerar el isomorfismo $\rho : \widetilde{X} \longrightarrow \operatorname{Proy}\mathcal{C}$ dado por el teorema anterior, con el que podemos formar la inmersión cerrada $j = \rho \circ i : \widetilde{X} \longrightarrow \mathrm{P}^r_X$, que está definida sobre X y cumple que $j^*\mathcal{O}_{\mathrm{P}^r_X}(1) = \mathcal{O}_{\widetilde{X}}(1)$. ∎

Ahora es inmediato el teorema siguiente:

Teorema 5.20 *Si X/S es una superficie fibrada y $\pi : \widetilde{X} \longrightarrow X$ es la explosión de X respecto de un subesquema cerrado distinto del propio X, entonces $\widetilde{X}/S$ es una superficie fibrada.*

DEMOSTRACIÓN: El teorema 5.17 nos da que $\widetilde{X}$ es un esquema íntegro de dimensión 2, acabamos de ver que $\widetilde{X}/S$ es proyectivo y, como el homomorfismo estructural es suprayectivo, es plano. ∎

Finalmente estamos en condiciones de manejar ejemplos de explosiones con una relativa "facilidad". Empezamos con el caso de una curva:

Ejemplo Consideremos la curva C/k definida por la ecuación

$$Y^2 + a_1XY = X^3 + a_2X^2.$$

(Se trata de una ecuación de Weierstrass con $a_3 = a_4 = a_6 = 0$, lo cual equivale a que la curva sea singular en el punto $(0,0)$.) Vamos a calcular la explosión $\pi : \widetilde{C} \longrightarrow C$ con centro en el punto singular. En principio sabemos que $\widetilde{C}$ es una curva proyectiva íntegra y que π es un homomorfismo birracional, necesariamente finito (todo homomorfismo entre curvas proyectivas es constante o finito). Vamos a probar que $\widetilde{C}$ es normal, con lo que será la normalización de C. En otras palabras, mediante la explosión habremos "resuelto la singularidad" de C, en un sentido que precisaremos más adelante.

Puesto que la explosión es un isomorfismo fuera de la fibra del punto singular, basta probar que las antiimágenes de dicho punto son regulares en $\widetilde{X}$. Por consiguiente, basta estudiar la explosión del abierto afín U formado por los puntos finitos de C. Como punto de $U = \operatorname{Esp} k[x,y]$, el punto singular es $\mathfrak{m} = (x,y)$. Para ajustarnos a la notación empleada en la definición 5.12, llamamos $A = k[x,y]$, $f_1 = x$, $f_2 = y$ y llamamos $t_1 = x$, $t_2 = y$ a los elementos correspondientes de grado 1 en $\widetilde{A}$. Según la propiedad g tras la definición 5.12, sabemos que $\widetilde{U} = D(t_1) \cup D(t_2)$. Ahora bien, la relación

$$t_2^2 + a_1t_1t_2 = f_1t_1^2 + a_2t_1^2$$

implica que $V(t_1) = \varnothing$, ya que si t_1 pertenece a un ideal $\mathfrak{p} \in \operatorname{Proy}\widetilde{A}$, entonces también $t_2^2 \in \mathfrak{p}$, luego $t_2 \in \mathfrak{p}$, lo cual es imposible. Así pues, $\widetilde{U} = V(t_1)$. La misma propiedad g nos da que $\widetilde{U} = \operatorname{Esp} k[x,y,y/x] = \operatorname{Esp} k[x,t]$, donde $t = y/x$. Obviamente, x, t cumplen la ecuación que resulta de sustituir $Y = XT$ en la ecuación de C:

$$X^2(T^2 + a_1T - a_2 - X) = 0.$$

Como $k[x,t]$ es un dominio íntegro, podemos eliminar el primer factor, y nos queda que x, t cumplen la ecuación

$$X = T^2 + a_1T - a_2.$$

Claramente es irreducible, luego

$$\widetilde{U} = \operatorname{Esp}\left(k[X,T]/(X - T^2 - a_1T + a_2)\right).$$

El hecho de que X pueda despejarse en la ecuación se traduce en que la proyección inducida por la inclusión $k[T] \longrightarrow k[x,t]$ sea un isomorfismo, cuyo inverso está inducido por el homomorfismo $k[x,t] \longrightarrow k[T]$ dado por las sustituciones $x \mapsto T^2 - a_1T + a_2$, $t \mapsto T$.

En particular vemos que $\widetilde{U} \cong A^1_k$ es regular, como queríamos probar. Pero, más aún, ahora tenemos una descripción explícita de la normalización: El homomorfismo $\pi : \widetilde{U} \longrightarrow U$ se corresponde con la inclusión $k[x,y] \longrightarrow k[x,t]$. Si lo componemos con el isomorfismo que hemos encontrado, obtenemos el homomorfismo $\pi : A^1_k \longrightarrow U$ inducido por el homomorfismo de k-álgebras $k[x,y] \longrightarrow k[T]$ dado por

$$x \mapsto T^2 + a_1T - a_2, \qquad y \mapsto T(T^2 + a_1T - a_2).$$

Notemos que $\widetilde{U}$ contiene todos los puntos de $\widetilde{U}$ excepto uno (la antiimagen del punto infinito de C). Por el teorema 4.21 sabemos que $\widetilde{C} \cong \mathrm{P}^1_k$, luego la normalización completa

$$\pi : \mathrm{P}^1_k \longrightarrow C$$

es el homomorfismo que, restringido a A^1_k coincide con el que acabamos de calcular y que hace corresponder el punto infinito de P^1_k con el punto infinito de C.

Como aplicación, podemos estudiar la fibra del punto singular, que es el espectro de

$$k[T] \otimes_{k[x,y]} k[x,y]/(x,y) = k[T]/(T^2 + a_1T - a_2).$$

Vemos que consta de un único punto racional si $b_2 = a_1^2 + 4a_2 = 0$, y de dos puntos (racionales o no) en caso contrario. (Si $\operatorname{car} k = 2$ hemos de suponer que k es perfecto.) ∎

Ahora vamos a calcular la explosión de una superficie fibrada:

Ejemplo Consideremos de nuevo la superficie de Weierstrass $W/\mathbb{Z}_5$ dada por la ecuación

$$Y^2 = X^3 + 25.$$

(Véase la página 135.) Su fibra cerrada tiene un punto singular x_0, y vamos a calcular la explosión $\pi : \widetilde{W} \longrightarrow W$ con centro en dicho punto. Sabemos que $\widetilde{W}$ es una superficie fibrada y que $\pi|_{\widetilde{W}\setminus\pi^{-1}[\{x_0\}]} : \widetilde{W} \setminus \pi^{-1}[\{x_0\}] \longrightarrow W \setminus \{x_0\}$ es un isomorfismo. En particular, $\widetilde{W}$ tiene la misma fibra genérica que W. Sólo hemos de estudiar su fibra cerrada, para lo cual basta calcular la explosión del abierto $U = \operatorname{Esp}\mathbb{Z}_5[x,y]$ formado por los puntos finitos de W. Como punto de U, el punto singular es $x_0 = \mathfrak{p} = (5,x,y)$.

Ahora tenemos que $\widetilde{U}$ es unión de tres abiertos afines, que llamaremos U_1, U_2, U_3. El primero es, por ejemplo,

$$U_1 = \operatorname{Esp}\mathbb{Z}_5[x,y,x/5,y/5] = \operatorname{Esp}\mathbb{Z}_5[x_1,y_1],$$

donde $x_1 = x/5$, $x_2 = y/5$. Teniendo en cuenta que x, y satisfacen la ecuación de Weierstrass, tenemos que x_1, y_1 cumplen la ecuación

$$25y_1^2 = 125x_1^3 + 25,$$

luego $y_1^2 = 5x_1^3 + 1$. Es claro que el polinomio $Y^2 - 5X^3 - 1$ es irreducible en $\mathbb{Z}_5[X,Y]$. (Por ejemplo, porque un cambio de variables lineal en $\mathbb{Q}[X,Y]$ lo transforma en la ecuación de Weierstrass, y esto implica que es irreducible en $\mathbb{Q}[X,Y]$, luego también en $\mathbb{Z}_5[X,Y]$, teniendo en cuenta que sus coeficientes son primos entre sí en $\mathbb{Z}_5$.) Por consiguiente,

$$U_1 = \operatorname{Esp}(\mathbb{Z}_5[X,Y]/(Y^2 - 5X^3 - 1)).$$

Consideremos ahora $U_2 = \operatorname{Esp}\mathbb{Z}_5[x, y, 5/x, y/x] = \mathbb{Z}_5[x, y', z]$, donde hemos llamado $y' = y/x$, $z = 5/x$. Los generadores cumplen las ecuaciones

$$x^2y'^2 = x^3 + x^2z^2, \qquad xz = 5.$$

Como $\mathbb{Z}_5[x, y', z]$ es un dominio íntegro (un subanillo del cuerpo de cocientes de $\mathbb{Z}_5[x, y]$), podemos simplificar la primera ecuación y resulta

$$y'^2 = x + z^2, \qquad xz = 5.$$

El hecho de que se pueda despejar x en la primera ecuación se traduce en que $\mathbb{Z}_5[x, y', z] = \mathbb{Z}_5[y', z]$ y los generadores satisfacen la ecuación

$$y'^2z - z^3 = 5.$$

Esta ecuación es irreducible, por ejemplo porque al homogeneizarla respecto de x y deshomogeneizarla respecto de z obtenemos la ecuación de U_1, que ya sabemos que es irreducible. Así pues,

$$U_2 = \operatorname{Esp}(\mathbb{Z}_5[Y, Z]/(Y^2Z - Z^2 - 5)).$$

La relación que hemos señalado sobre las ecuaciones de U_1 y U_2 tiene su interpretación: En primer lugar, observemos que la relación entre los generadores de $\mathbb{Z}_5[x_1, y_1]$ y los de $\mathbb{Z}_5[y', z]$ es la dada por

$$x_1 = 1/z, \quad y_1 = y'/z, \qquad y' = y_1/x_1, \quad z = 1/x_1,$$

lo que se interpreta como que $U_1 \cap U_2$ es $D(x_1)$ en U_1 y $D(z)$ en U_2, y las ecuaciones anteriores definen el isomorfismo entre $D(x_1)$ y $D(z)$ que se corresponde con la identidad a través de las identificaciones $U_1 \cong \operatorname{Esp}\mathbb{Z}_5[x_1, y_1]$, $U_2 = \operatorname{Esp}\mathbb{Z}_5[y', z]$. En segundo lugar, si llamamos

$$\mathcal{X} = \operatorname{Proy}(\mathbb{Z}_5[X, Y, Z]/(Y^2Z - 5X^3 - Z^3)),$$

que no es sino la superficie fibrada estudiada en el ejemplo de la página 135, tenemos que $U_1 \cong D(z) \subset \mathcal{X}$, $U_2 \cong D(x) \subset \mathcal{X}$ y, al representar

$$D(z) = \operatorname{Esp}\mathbb{Z}_5[\bar{x}, \bar{y}], \qquad D(x) = \operatorname{Esp}\mathbb{Z}_5[y^*, z^*],$$

donde $\bar{x} = x/z$, $\bar{y} = y/z$, $y^* = y/x$, $z^* = z/x$, la correspondencia entre los generadores es la misma que la que hemos encontrado entre x_1, y_1 e y', z. Esto implica que los isomorfismos $U_1 \cong D(z)$, $U_2 \cong D(x)$ se extienden hasta un isomorfismo $U_1 \cup U_2 \longrightarrow D(z) \cup D(x) \subset \mathcal{X}$.

Nos falta considerar el abierto $U_3 = \mathbb{Z}_5[x, y, 5/y, x/y] = \mathbb{Z}_5[x', y, z']$, donde $x' = x/y$, $z' = 5/y$. Los generadores cumplen las ecuaciones

$$x'^3y + z'^2 = 1, \qquad yz' = 5.$$

Las relaciones entre los generadores son:

$$x_1 = x'/z', \quad y_1 = 1/z', \qquad y' = 1/x', \quad z = z'/x',$$

de donde se sigue que $U_1 \cap U_3 = D(z')$, $U_2 \cap U_3 = D(x')$, luego un punto de U_3 que no esté en $U_1 \cup U_2$ tendría que estar en $V(x', z') = \varnothing$ (por la primera ecuación de U_3). Esto significa que $U_3 \subset U_1 \cup U_2$, luego $\widetilde{U} = U_1 \cup U_2$ y tenemos una representación de $\widetilde{U}$ como el abierto $D(z) \cup D(x) \subset \mathcal{X}$.

Podríamos probar que este isomorfismo entre el abierto $\widetilde{U}$ de $\widetilde{W}$ y un abierto de $\mathcal{X}$ se extiende a un isomorfismo $\widetilde{W} \cong \mathcal{X}$, pero más adelante será inmediato.[2] Observemos que $\widetilde{W} \setminus \widetilde{U}$ consta exactamente de dos puntos, las antiimágenes de los puntos infinitos de las dos fibras de W y, por otra parte, $\mathcal{X} \setminus \widetilde{U}$ también consta de dos puntos, pues es $V(\bar{x}, \bar{z}) \subset D(y)$, donde $\bar{x} = x/y$, $\bar{z} = z/y$ y $D(y) = \operatorname{Esp} \mathbb{Z}_5[\bar{x}, \bar{z}]) = \operatorname{Esp} \mathbb{Z}_5[X, Z]/(Z - 5X^3 - Z^3)$, luego

$$X \setminus \widetilde{U} = \operatorname{Esp}(\mathbb{Z}_5[X, Z]/(X, Z)) = \operatorname{Esp} \mathbb{Z}_5,$$

que, ciertamente, consta de dos puntos.

Admitiendo a partir de aquí que $\widetilde{W} = \mathcal{X}$, vemos que la fibra cerrada $\mathcal{X}_5$ viene dada por la ecuación homogénea $Y^2Z - Z^3 = 0$, luego consta de tres rectas, que podemos llamar

$$\Gamma_1 = (5, Z), \quad \Gamma_2 = (5, Z + Y), \quad \Gamma_3 = (5, Z - Y).$$

Si $\mathcal{I}$ es el haz de ideales de $\mathcal{O}_W$ que determina al punto singular x_0 (el centro de la explosión), es claro que $\pi^*\mathcal{I}$ es el haz de ideales de $\mathcal{O}_{\widetilde{W}}$ que determina la fibra de x_0. En la prueba del teorema 5.17 f) hemos visto que

$$(\pi^*\mathcal{I})(U_1) = (5) \subset \mathbb{Z}_5[x_1, y_1], \qquad (\pi^*\mathcal{I})(U_2) = (x) = (y'^2 - z^2) \subset \mathbb{Z}_5[y', z].$$

Esto significa que π envía a x_0 toda la fibra cerrada de U_1, que está determinada por la ecuación $y_1^2 - 1 = 0$, es decir, por las dos rectas afines:

$$\Gamma_2 \cap U_1 = (5, y_1 + 1), \qquad \Gamma_3 \cap U_1 = (5, y_1 - 1).$$

En cambio, la fibra cerrada de U_2 viene dada por la ecuación $y'^2 z - z^3 = 0$, por lo que consta de las rectas afines

$$\Gamma_1 \cap U_2 = (5, z), \quad \Gamma_2 \cap U_2 = (5, y' + z), \quad \Gamma_3 \cap U_2 = (5, y' - z),$$

de las cuales, sólo las dos últimas se contraen a x_0, mientras que, por el contrario, $\pi|_{\Gamma_1 \cap U_2} : \Gamma_1 \cap U_2 \longrightarrow U_5$ es suprayectiva. (Sabemos a priori que ha de ser así, porque π es suprayectiva, y los puntos de la fibra cerrada U_5 no pueden tener antiimágenes sino en $\Gamma_1 \cap U_2$.) Más aún, necesariamente, el punto de Γ_1 que no está en U_2 tiene que ser la antiimagen del punto infinito de U_5, luego concluimos que $\pi|_{\Gamma_1} : \Gamma_1 \longrightarrow W_5$ es suprayectiva.

Con más detalle aún: si componemos con π la inmersión cerrada $\Gamma_1 \longrightarrow \widetilde{W}$ que resulta de considerar a Γ_1 con la estructura de subesquema cerrado reducido, obtenemos un homomorfismo de esquemas $\pi|_{\Gamma_1} : \Gamma_1 \longrightarrow W_5$ suprayectivo,

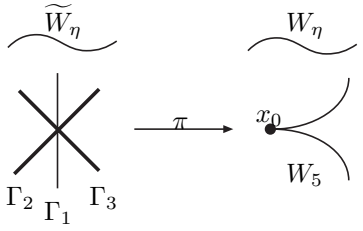
[2] Porque $\widetilde{W}$ y $\mathcal{X}$ son ambas superficies regulares minimales.

que es un isomorfismo salvo en la antiimagen del punto singular de W_5. Por consiguiente, se trata de un homomorfismo birracional entre dos curvas proyectivas, y $\Gamma_1 \cong \mathrm{P}^1_{\mathbb{Z}/5\mathbb{Z}}$ es regular, luego se trata de la normalización de W_5. Considerando el ejemplo anterior, podemos concluir que, de hecho, $\pi|_{\Gamma_1}$ es biyectiva.

Explícitamente: Sabemos que $\pi|_{U_1}$ es el homomorfismo asociado a la inclusión $\mathbb{Z}_5[x,y] \subset \mathbb{Z}_5[y',z]$, luego $\pi|_{\Gamma_1 \cap U_2}$ es el homomorfismo de esquemas asociado al homomorfismo de anillos

$$(\mathbb{Z}/5\mathbb{Z})[x,y] = \mathbb{Z}_5[x,y]/(5) \longrightarrow \mathbb{Z}_5[y',z]/(5,z) = (\mathbb{Z}/5\mathbb{Z})[Y]$$

Tenemos que $x \mapsto y'^2 - z^2$, $y \mapsto xy' = y'^3 - y'z^2$, luego, al formar los cocientes, la correspondencia se reduce a $x \mapsto Y^2$, $y \mapsto Y^3$, que es, ciertamente, la expresión explícita para la normalización que habíamos encontrado en el ejemplo anterior.



La figura resume la estructura de la explosión $\pi : \widetilde{W} \longrightarrow W$. Es un isomorfismo sobre las fibras genéricas y contrae a x_0 dos de las componentes irreducibles de la fibra cerrada de $\widetilde{W}$, mientras que, restringida a Γ_1, es la normalización de la fibra cerrada W_5. ∎

Nota En el cálculo explícito de explosiones, el punto técnico más delicado es encontrar las ecuaciones que determinan la estructura de esquema de los abiertos afines que en el ejemplo anterior hemos llamado U_1, U_2 y U_3. Mejor dicho, lo delicado no es encontrarlas, que es fácil, sino justificar que las ecuaciones que encontramos fácilmente son realmente las que buscamos. En esta nota vamos a dar un argumento general aplicable en la mayoría de los casos que vamos a considerar en lo sucesivo.

Partimos de un anillo de valoración discreta D (en el ejemplo anterior $\mathbb{Z}_5$) cuyo ideal maximal esté generado por un primo π (en el ejemplo anterior $\pi = 5$), y consideramos un esquema afín

$$X = \mathrm{Esp}(D[X,Y]/(f(X,Y))),$$

donde $f(X,Y)$ es un polinomio no constante irreducible en $D[X,Y]$. Vamos a determinar explícitamente las ecuaciones que determinan la explosión de X con centro en el punto $\mathfrak{p} = (\pi, x, y)$. Sabemos que $\widetilde{X}$ es la unión de tres abiertos afines. El primero es $U_1 = \mathrm{Esp}\, D[x, y, x/\pi, y/\pi] = \mathrm{Esp}\, D[x_1, y_1]$, donde hemos llamado $x_1 = x/\pi$, $y_1 = y/\pi$. Los generadores x_1, y_1 cumplen

$$f(\pi x_1, \pi y_1) = 0,$$

es decir, son raíces del polinomio $f(\pi X, \pi Y)$. Podemos descomponer este polinomio en la forma

$$f(\pi X, \pi Y) = \pi^d g(X,Y),$$

donde $g(X,Y) \in D[X,Y]$ no es divisible entre π. Es claro entonces que también se cumple $g(x_1,y_1) = 0$ y la cuestión es justificar que g es irreducible, pues entonces tenemos un epimorfismo

$$D[X,Y]/(g(X,Y)) \longrightarrow D[x_1,y_1],$$

donde el anillo de la izquierda es un dominio íntegro de dimensión 2. Si no fuera un isomorfismo, concluiríamos que $D[x_1,y_1]$ tendría dimensión menor que 2, lo cual es imposible, pues sabemos que las explosiones conservan la dimensión.

El argumento que hemos empleado en el ejemplo anterior vale en general: si llamamos K al cuerpo de cocientes de D, el automorfismo $K[X,Y] \longrightarrow K[X,Y]$ dado por $X \mapsto \pi X$, $Y \mapsto \pi Y$ transforma $f(X,Y)$ en $\pi^d g(X,Y)$, luego éste es irreducible en $K[X,Y]$, y lo mismo vale para $g(X,Y)$. Como sus coeficientes son primos entre sí, esto implica a su vez que $g(X,Y)$ es irreducible en $D[X,Y]$.

Consideremos ahora $U_2 = \operatorname{Esp} D[x,y,y/x,\pi/x] = \operatorname{Esp} D[x,y',z]$, donde hemos llamado $y' = y/x$, $z = \pi/x$. (El caso de U_3 es completamente análogo, así que no necesitamos considerarlo.) Vamos a hacer en este contexto general lo mismo que hemos hecho en el ejemplo anterior. Para ello, observamos que podemos expresar $f(X,Y) = f(X,Y,\pi)$, donde $f(X,Y,Z) \in D[X,Y,Z]$ es un polinomio cuyos coeficientes son todos unidades en D. De este modo,

$$D[x,y] = D[X,Y]/(f(X,Y)) = D[X,Y,Z]/(F(X,Y,Z), Z-\pi).$$

Los generadores x, y', z cumplen $y = xy'$, $\pi = xz$, luego son raíces del polinomio $f(X,XY,XZ)$. Podemos factorizarlo como

$$f(X,XY,XZ) = X^d g(X,Y,Z),$$

donde g no es divisible entre X y sus coeficientes siguen siendo unidades en D. En particular, esto implica que $g \notin (X,\pi) \subset D[X,Y]$. Vamos a probar que

$$D[x,y',z] = D[X,Y,Z]/(g(X,Y,Z), XZ-\pi).$$

En el ejemplo anterior hemos tenido la "suerte" de que podíamos despejar X en $g(X,Y,Z) = 0$ y reducir el problema a una única ecuación, que además hemos podido relacionar fácilmente con la ecuación de U_1. Todo esto no es posible en general.

Es claro que x, y', z son raíces de los polinomios $g(X,Y,Z)$ y $XZ-\pi$. Hemos de probar que si $p(X,Y,Z) \in D[X,Y,Z]$ es un polinomio (que podemos suponer irreducible) tal que $p(x,y',z) = 0$, entonces $p \in (g, XZ-\pi)$. Para ello, trabajando en el cuerpo $K(X,Y,Z)$, consideramos el natural e que hace que

$$q(X,Y,Z) = X^e p(X, Y/X, Z/X)$$

sea un polinomio no divisible entre X. Así, $q(X,XY,XZ) = X^e p(X,Y,Z)$, luego $q(x,y,\pi) = x^e p(x,y',z) = 0$, luego

$$q(X,Y,Z) = a(X,Y,Z)f(X,Y,Z) + b(X,Y,Z)(Z-\pi),$$

para ciertos polinomios a y b. Por consiguiente,

$$X^e p(X,Y,Z) = a(X,XY,XZ)X^d g(X,Y,Z) + b(X,XY,XZ)(XZ-\pi).$$

Redefiniendo a y b, hemos llegado a una expresión de la forma

$$X^e p(X,Y,Z) = a(X,Y,Z)X^d g(X,Y,Z) + b(X,Y,Z)(XZ-\pi).$$

Consideremos el dominio íntegro $A = D[X,Y,Z]/(XZ-\pi)$. El ideal (x) es primo, pues

$$A/(x) = D[X,Y,Z]/(X,XZ-\pi) = (D/(\pi))[Y,Z],$$

que es un dominio íntegro. Como es un anillo noetheriano, tiene que haber un máximo exponente m tal que $x^m \mid a(x,y,z)$. Esto significa que

$$a(X,Y,Z) = X^m u(X,Y,Z) + v(X,Y,Z)(XZ-\pi).$$

Esta igualdad nos permite reemplazar a por u, d por $d+m$ y b por $b+X^d gv$ en la igualdad precedente y suponer que x no divide a $a(x,y,z)$ en el dominio A. Por otra parte, x tampoco puede dividir a $g(x,y,z)$, ya que esto significaría que

$$g(X,Y,Z) = Xu(X,Y,Z) + v(X,Y,Z)(XZ-\pi) \in (X,\pi).$$

Así pues, la igualdad

$$x^e p(x,y,z) = a(x,y,z)x^d g(x,y,z)$$

implica que $e \le d$. Por consiguiente, volviendo a la igualdad en $D[X,Y,Z]$, concluimos que $X^e \mid b(X,Y,Z)$, luego $p(X,Y,Z) \in (g(X,Y,Z), XZ-\pi)$, como había que probar. ∎

Terminamos la sección demostrando algunas propiedades adicionales de las explosiones:

Teorema 5.21 *Sea $f : W \longrightarrow X$ un homomorfismo entre esquemas localmente noetherianos, sea $\mathcal{I}$ un haz cuasicoherente de ideales de X y $\mathcal{J} = \mathcal{I}\mathcal{O}_W$. Sean $\pi : \widetilde{X} \longrightarrow X$ y $\rho : \widetilde{W} \longrightarrow W$ las explosiones con centro en los subesquemas determinados por estos haces. Entonces existe un único homomorfismo de esquemas $\tilde{f}$ que hace conmutativo el diagrama siguiente:*

$$\begin{array}{ccc} \widetilde{W} & \xrightarrow{\tilde{f}} & \widetilde{X} \\ {\scriptstyle\rho}\downarrow & & \downarrow{\scriptstyle\pi} \\ W & \xrightarrow[f]{} & X \end{array}$$

Demostración: Supongamos en primer lugar que $X = \operatorname{Esp} A$, $W = \operatorname{Esp} B$. Entonces f está determinado por un homomorfismo $A \longrightarrow B$, el haz $\mathcal{I}$ está determinado por un ideal I de A, y $\mathcal{J}$ está determinado por el ideal J generado

por la imagen de I. Obviamente, tenemos entonces un homomorfismo graduado $\widetilde{A} \longrightarrow \widetilde{B}$, que induce un homomorfismo $\widetilde{W} \longrightarrow \widetilde{X}$ que cumple lo pedido.

Supongamos ahora que $U = \operatorname{Esp} C$ y $V = \operatorname{Esp} D$ son abiertos afines en X y W respectivamente, de modo que $V \subset f^{-1}[U]$. Entonces tenemos diagramas conmutativos correspondientes

$$\begin{array}{ccc} W & \xrightarrow{f} & X \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle j} \\ V & \xrightarrow[f|_V]{} & U \end{array} \qquad\qquad \begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ C & \longrightarrow & D \end{array}$$

Claramente, $\mathcal{I}(U) = (j^*\mathcal{I})(U) = I \otimes_A C$, por lo que $\mathcal{I}|_U = \mathcal{I}\mathcal{O}_U$ está determinado por el ideal generado por I en C. Igualmente, $\mathcal{J}|_V$ está determinado por el ideal generado por I en D. Tenemos, pues, un diagrama conmutativo

$$\begin{array}{ccc} \widetilde{W} & \xrightarrow{\tilde{f}} & \widetilde{X} \\ \uparrow & & \uparrow \\ \widetilde{V} & \xrightarrow[\widetilde{f|_V}]{} & \widetilde{U} \end{array}$$

donde las flechas verticales son las inclusiones naturales. En otras palabras, el homomorfismo $\tilde{f}$ que sabemos construir explícitamente para f e $\mathcal{I}$, se restringe al que sabemos construir para $f|_V$ e $\mathcal{I}|_U$.

Esto nos da la existencia en el caso en que los esquemas no son necesariamente afines. En efecto, cubrimos W por abiertos afines W_i, cada uno de los cuales está contenido en la antiimagen por f de un abierto afín X_i de X, de modo que f se restringe a homomorfismos $f_i : W_i \longrightarrow X_i$, para los que sabemos construir homomorfismos $\tilde{f}_i : \widetilde{W}_i \longrightarrow \widetilde{X}_i$. Si $P \in \widetilde{W}_i \cap \widetilde{W}_j$, podemos tomar abiertos afines $f(\rho(P)) \in U \subset X_i \cap X_j$ y $\rho(P) \in V \subset f^{-1}[U]$. Sucede entonces que $\tilde{f}_i$ y $\tilde{f}_j$ se restringen al mismo homomorfismo $\widetilde{V} \longrightarrow \widetilde{U}$, luego todos los $\tilde{f}_i$ se extienden a un homomorfismo $\tilde{f}$ que cumple el teorema.

Ahora probamos la unicidad. En primer lugar, si $U \subset X$ es un abierto afín y $V = f^{-1}[U]$. Un homomorfismo $\tilde{f}$ que cumpla el teorema se restringe a un homomorfismo $\widetilde{V} \longrightarrow \widetilde{U}$ que también lo cumple, luego basta demostrar la unicidad cuando $X = \operatorname{Esp} A$ es afín (y noetheriano).

Por otra parte, si llamamos $f' = \rho \circ f$, es claro que $\mathcal{I}\mathcal{O}_{\widetilde{W}} = \mathcal{J}\mathcal{O}_{\widetilde{W}}$, luego se trata de un haz inversible, lo que hace que la explosión de $\widetilde{W}$ respecto de $\mathcal{I}\mathcal{O}_{\widetilde{W}}$ sea el propio $\widetilde{W}$. Por lo tanto, un homomorfismo f que cumpla el teorema para f, lo cumple también para f', por lo que basta probar la unicidad en el caso en que $\mathcal{J}$ es un haz inversible en W y, por consiguiente, $\widetilde{W} = W$.

Sea $\mathcal{I} = \widetilde{I}$, donde I es un ideal de A, y sea $f_1, \ldots, f_n$ un generador. Sea $i : \widetilde{X} \longrightarrow \mathrm{P}^{n-1}_X$ la inmersión cerrada considerada en la prueba de 5.17 g),

de modo que $\mathcal{O}_{\widetilde{X}}(1) = i^*\mathcal{O}_{\mathrm{P}^{n-1}_X}(1)$. Para cualquier $\tilde{f}$ que cumpla el teorema, tenemos el diagrama conmutativo

$$\begin{array}{ccc} \widetilde{X} & \xrightarrow{i} & \mathrm{P}^{n-1}_X \\ {\scriptstyle\tilde{f}}\uparrow & \overset{\pi}{\searrow} & \downarrow \\ W & \xrightarrow[f]{} & X \end{array}$$

luego $\mathcal{J} = \mathcal{I}\mathcal{O}_W = (\mathcal{I}\mathcal{O}_{\widetilde{X}})\mathcal{O}_W = (\mathcal{O}_{\widetilde{X}}(1))\mathcal{O}_W = (\mathcal{O}_{\mathrm{P}^{n-1}_X}(1))\mathcal{O}_W$.

Equivalentemente, si llamamos $g = \tilde{f} \circ i$, tenemos un epimorfismo

$$g^* : g^*\mathcal{O}_{\mathrm{P}^{n-1}_X}(1) \longrightarrow \mathcal{I},$$

que es un isomorfismo porque ambos haces son inversibles.

Por otra parte, la prueba de 5.17 f) muestra que el isomorfismo $\mathcal{I}\mathcal{O}_{\widetilde{X}} \cong \mathcal{O}_{\widetilde{X}}(1)$ identifica $\pi^*(f_i) \in \mathcal{I}\mathcal{O}_{\widetilde{X}}(\widetilde{X})$ con $i^*(X_i) \in i^*\mathcal{O}_{\mathrm{P}^{n-1}_X}(1) = \mathcal{O}_{\widetilde{X}}(1)$. Por consiguiente, si llamamos $u_i = f^*(f_i) \in \mathcal{J}(W)$, el diagrama conmutativo nos da que

$$u_i = \tilde{f}^*(\pi^*(f_i)) = \tilde{f}^*(i^*(X_i)) = g^*(X_i).$$

En resumen, si $\tilde{f}$ cumple el teorema, entonces la composición $g = \tilde{f} \circ i$ cumple que $g^*\mathcal{O}_{\mathrm{P}^{n-1}_X}(1) \cong \mathcal{J}$ y $g^*(X_i) = u_i$. Según el teorema [5.33], esto implica que $\tilde{f} \circ i$ está unívocamente determinado y, como i es una inmersión cerrada, $\tilde{f}$ también. ∎

De aquí se deduce inmediatamente que las explosiones están caracterizadas por la propiedad universal siguiente:

Teorema 5.22 *Sea $\pi : \tilde{X} \longrightarrow X$ una explosión de un esquema localmente noetheriano y sea $\mathcal{I}$ el haz de ideales que determina su centro. Entonces, para todo homomorfismo $f : W \longrightarrow X$ tal que $\mathcal{I}\mathcal{O}_W$ es inversible, existe un único homomorfismo $g : W \longrightarrow \widetilde{X}$ que hace conmutativo el diagrama*

$$\begin{array}{ccc} W & \xrightarrow{g} & \widetilde{X} \\ & \overset{f}{\searrow} & \downarrow \pi \\ & & X \end{array}$$

Teorema 5.23 *En las condiciones del teorema* 5.21*, si el homomorfismo f es una inmersión cerrada, también lo es $\tilde{f}$.*

Demostración: Se deduce de la construcción de $\tilde{f}$ vista en la demostración del teorema 5.21. Puesto que ser una inmersión cerrada es una propiedad local en la base, no perdemos generalidad si suponemos que X es afín, en cuyo caso Y también lo es. Si $X = \operatorname{Esp} A$, $W = \operatorname{Esp} B$, tenemos que el homomorfismo $A \longrightarrow B$ asociado a f es un epimorfismo, luego también lo es el homomorfismo $\widetilde{A} \longrightarrow \widetilde{B}$, de donde se sigue que $\tilde{f}$ es una inmersión cerrada. ∎

Definición 5.24 Sea $\pi : \widetilde{X} \longrightarrow X$ la explosión de un esquema localmente noetheriano X respecto de un subesquema cerrado Z. Si W es un subesquema cerrado de X, el subesquema cerrado $\widetilde{W}$ de $\widetilde{X}$ dado por el teorema anterior se llama *transformada estricta* de W.

El teorema siguiente nos describe más detalladamente las explosiones de esquemas regulares respecto de centros regulares:

Teorema 5.25 *Sea $\pi : \widetilde{X} \longrightarrow X$ una explosión de un esquema localmente noetheriano regular con centro en un subesquema regular Y determinado por un haz de ideales $\mathcal{I}$. Entonces:*

a) $\widetilde{X}$ es regular.

b) Para cada $x \in Y$, la fibra $\widetilde{X}_x$ es isomorfa a $\mathrm{P}^{r-1}_{k(x)}$, donde

$$r = \dim_x X - \dim_x Y.$$

c) Si $Y' = \pi^{-1}[Y]$, con la estructura de subesquema cerrado dada por $\mathcal{I}\mathcal{O}_{\widetilde{X}}$, entonces la inmersión cerrada $Y' \longrightarrow \widetilde{X}$ es una inmersión regular.

Demostración: El teorema 5.17 d) implica que $\widetilde{X}$ es regular en todos los puntos de $\pi^{-1}[X \setminus Y]$, luego sólo hemos de comprobar la regularidad en los puntos $P \in \widetilde{X}$ cuya imagen es un punto $x \in Y$. Si U es un entorno afín de x, entonces $\tilde{U} = \pi^{-1}[U]$ es un entorno afín de P. Además, la fibra $\widetilde{X}_x$ coincide con $\widetilde{U}_x$, luego, tanto para probar a) como para probar b), podemos suponer que X es afín y noetheriano.

Si $X = \operatorname{Esp} A$, llamemos $X' = \operatorname{Esp} A_x$ y consideremos el diagrama conmutativo

$$\begin{array}{ccc} \widetilde{X}' & \longrightarrow & \widetilde{X} \\ {\scriptstyle \pi'}\downarrow & & \downarrow{\scriptstyle \pi} \\ X' & \longrightarrow & X \end{array}$$

Por el teorema 5.17 c), sabemos que $\widetilde{X}' = \widetilde{X} \times_X X'$. Además, los homomorfismos que aparecen en el diagrama son las proyecciones. En particular, es claro que $\widetilde{X}'_x \cong \widetilde{X}_x$, luego para probar b) podemos suponer que X es un esquema noetheriano local y que x es su punto cerrado. También podemos suponer esto para la prueba de a), pues si $P' \in \widetilde{X}'$ es el punto correspondiente a P en $\widetilde{X}'_x$, se cumple que $\mathcal{O}_{\widetilde{X}',P'} \cong \mathcal{O}_{\widetilde{X},P}$, pues esto equivale a que $(\widetilde{A}_x)_{P'} \cong \widetilde{A}_P$ (y tenemos que $P' = P_x$ y que $A \setminus x \subset \widetilde{A} \setminus P$).

Pongamos, pues, que $X = \operatorname{Esp} A$, donde A es un anillo local regular. Entonces $Y = \operatorname{Esp} A/I$, para cierto ideal I de A. Como x es regular tanto en X como en Y, tenemos que A/I también es regular. Por [AC 5.19] tenemos que el ideal maximal de A es de la forma $\mathfrak{m} = (f_1, \ldots, f_d)$, donde $d = \dim \mathcal{O}_{X,x}$, y además $I = (f_1, \ldots, f_r)$, para cierto $r \leq d$ (que es el que aparece en el enunciado de b).

Sea $J = (f_iX_j - f_jX_i)_{1\leq i,j\leq r}$, sea $B = A[X_1,\dots,X_r]/J$ y $Z = \operatorname{Proy} B$. Vamos a probar que Z es íntegro, con lo que la propiedad h) tras la definición 5.12 nos dará que $Z \cong \widetilde{X}$.

En cualquier caso, tenemos una inmersión cerrada $\widetilde{X} \longrightarrow Z$ definida sobre X. Veamos que el homomorfismo natural $\pi' : Z \longrightarrow X$ se restringe a un isomorfismo $\pi'^{-1}[X \setminus Y] \longrightarrow X \setminus Y$. En efecto, $X \setminus Y$ es la unión de los abiertos $D(f_i)$, para $1 \leq i \leq r$, y se cumple que $\pi'^{-1}[D(f_i)] = D(f_i) = D(f_ix_i)$. (La última igualdad se sigue de las relaciones $f_ix_j = f_jx_i$.)

La restricción de π' al abierto $D(f_ix_i)$ se corresponde con el homomorfismo $A_{f_i} \longrightarrow B_{(f_ix_i)}$ dado por $a/f_i^m \mapsto ax_i^m/(f_ix_i)^m$. Es fácil ver que se trata de un isomorfismo. Por ejemplo, $x_j/(f_ix_i) = (f_jx_i^2)/(f_ix_i)^2$ y, usando este tipo de transformación, se ve fácilmente que todo elemento de $B_{(f_ix_i)}$ es de la forma $ax_i^m/(f_ix_i)^m$, cuya antiimagen es a/f_i^m. La inyectividad es inmediata.

Así pues, π' se restringe a un isomorfismo sobre cada $\pi'^{-1}[D(f_i)]$, luego también sobre $\pi'^{-1}[X \setminus Y]$.

Si $y \in Y$, tenemos que $Z_y = Z \times_X \operatorname{Esp} k(y) \cong \operatorname{Proy}(B \otimes_A k(y))$, y es fácil ver que

$$B \otimes_A k(y) \cong k(y)[X_1,\dots,X_r],$$

por lo que $Z_y \cong \mathrm{P}^{r-1}_{k(y)}$.

De este modo, $\pi' : Z \longrightarrow X$ es un homomorfismo propio (es proyectivo), suprayectivo y con fibras conexas. Esto implica que Z es conexo, pues si pudiéramos descomponer $Z = U \cup V$, para ciertos abiertos disjuntos no vacíos U y V, entonces cada fibra de π' está contenida en uno de ellos, luego $\pi'[U]$ y $\pi'[V]$ serían cerrados disjuntos no vacíos en X, lo cual es imposible, pues el punto cerrado de X pertenece a todos los cerrados no vacíos.

Si demostramos que Z es regular, en particular será localmente íntegro y, como es conexo, será íntegro. Esto probará que $\widetilde{X} \cong Z$ y tendremos a). Además, el isomorfismo hace corresponder a π con π', y ya hemos comprobado que las fibras de π' cumplen b), con lo que ambos apartados estarán demostrados.

Basta probar que Z es regular en cada punto cerrado $z \in Z$. Observemos que $z \in Z_x$, porque $Z \longrightarrow X$ es propio. Pongamos que $z \in D(x_1)$. Es fácil ver que $B_{(x_1)} = A[X_2,\dots,X_r]/J_1$, donde $J_1 = (f_i - f_1X_i)_{2\leq i\leq r}$. Un entorno de z en Z_x es $D(x_1)_x$, que es el espectro de $B_{(x_1)} \otimes_A (A/\mathfrak{m}_x) = B_{(x_1)}/\mathfrak{m}_xB_{(x_1)}$, de modo que la inmersión cerrada $D(x_1)_x \longrightarrow D(x_1)$ se corresponde con el homomorfismo natural $B_{(x_1)} \longrightarrow B_{(x_1)}/\mathfrak{m}_xB_{(x_1)}$, lo que a su vez implica que el epimorfismo $\mathcal{O}_{Z,z} \longrightarrow \mathcal{O}_{Z_x,z}$ tiene por núcleo el ideal generado por $f_1,\dots,f_d$. Como $\mathcal{O}_{Z_x,z}$ es regular de dimensión $r-1$, su ideal maximal admite un generador con $r-1$ elementos, luego $\mathfrak{m}_z = (f_1,\dots,f_d,g_2,\dots,g_r)$, para ciertos $g_i \in \mathfrak{m}_z$. Notemos que en $\mathcal{O}_{Z,z}$ se cumplen las relaciones $f_i = f_1x_i$, para $i = 2,\dots,r$, luego en realidad $\mathfrak{m}_z = (f_1,g_2,\dots,g_r,f_{r+1},\dots,f_d)$. Así pues, $\dim \mathcal{O}_{Z,z} \leq \mu(\mathfrak{m}_z) \leq d$.

Consideremos ahora la inmersión cerrada $\operatorname{Esp} B_{(x_1)} \longrightarrow \operatorname{Esp} A[X_2,\dots,X_r]$, que nos permite considerar a z como un ideal maximal de $A[X_2,\dots,X_r]$ tal que $z \cap A = x$. El epimorfismo $A[X_2,\dots,X_r] \longrightarrow k(x)[X_2,\dots,X_r]$ tiene por núcleo

el ideal generado por x en el anillo de polinomios, luego hace corresponder a z con un ideal maximal de $k(x)[X_2,\dots,X_r]$, cuya altura es obviamente $r-1$. Por consiguiente, la altura de z en $A[X_2,\dots,X_r]$ es $\geq d+r-1$. Esto se traduce en que $\dim \mathcal{O}_{A_A^{r-1},z} \geq d+r-1$.

Por otra parte, tenemos un epimorfismo $\mathcal{O}_{A_A^{r-1},z} \longrightarrow \mathcal{O}_{Z,z}$ cuyo núcleo está generado por los generadores de J_1, que son $r-1$. Vamos a probar que cada generador disminuye la dimensión a lo sumo en una unidad, de modo que podremos concluir que $\dim \mathcal{O}_{Z,z} \geq d+r-1-(r-1)=d$. A su vez esto implicará que $\dim \mathcal{O}_{Z,z} = \mu(\mathfrak{m}_z) = d$, lo que significa que z es regular en Z.

Lo que hemos de probar es que si A es un anillo noetheriano local y $f \in A$ no es una unidad, entonces $\dim A/(f) \geq \dim A - 1$. Para ello consideramos una cadena de ideales primos en A: $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d$. Si $f \in \mathfrak{p}_0$ entonces en $A/(f)$ tenemos una cadena de la misma longitud, mientras que si $f \notin \mathfrak{p}_0$, entonces f no es un divisor de cero en $A/\mathfrak{p}_0$, por lo que [AC 4.58] nos da que $\dim A/(\mathfrak{p}_0+(f)) \geq d-1$, luego también $\dim A/(f) \geq d-1$.

Falta probar c). Observemos que, ciertamente, el ideal $\mathcal{IO}_{\widetilde{X}}$ define una estructura de esquema sobre Y', es decir, que $V(\mathcal{IO}_{\widetilde{X}}) = Y'$. Basta comprobar la igualdad sobre cada abierto $U_i = V(t_i)$. En la prueba de 5.17 f) hemos visto que $\mathcal{IO}_{\widetilde{X}}(U_i)$ está generado por $f_1,\dots,f_r$ o, simplemente, por f_i. Así, un ideal $\mathfrak{p} \in U_i$ pertenece a $V(\mathcal{IO}_{\widetilde{X}}) \cap U_i$ si y sólo si $f_i \in \mathfrak{p}$, si y sólo si $f_1,\dots,f_r \in \mathfrak{p}$, si y sólo si $f_1,\dots,f_r \in \pi(\mathfrak{p})$, si y sólo si $\pi(\mathfrak{p}) \in Y$.

Ahora, c) es consecuencia inmediata de que el ideal $\mathcal{IO}_{\widetilde{X}}$ es inversible. ∎

5.3 La geometría de las superficies fibradas

Presentamos aquí las propiedades básicas de las superficies fibradas. Entre las más elementales tenemos ésta, que muestra que, realmente, la fibra genérica es "genérica":

Teorema 5.26 *Sea S un esquema íntegro, X/S un esquema plano reducido y sean $f,g : X \longrightarrow Y$ dos homomorfismos en un esquema separado Y. Si ambos coinciden sobre la fibra genérica de X, entonces $f=g$.*

Demostración: Cubrimos S con abiertos afines W. Como f y g se restringen a homomorfismos $\pi_X^{-1}[W] \longrightarrow \pi_Y^{-1}[W]$ que cumplen las mismas hipótesis, basta probar el teorema en el caso en que $S = \operatorname{Esp} D$. Llamemos $K = K(S)$.

Si $U = \operatorname{Esp} A$ es un abierto afín en Y y $V = \operatorname{Esp} B$ es un abierto afín en $f^{-1}[U] \cap g^{-1}[U]$, tenemos que $f|_V$ y $g|_V$ se corresponden con dos homomorfismos $A \longrightarrow B$ que, compuestos con el monomorfismo $B \longrightarrow B \otimes_D K$, son iguales, luego ambos homomorfismos son iguales, $f|_V = g|_V$ y $f = g$ por el teorema [E 4.16]. ∎

Según el teorema [E A.16], el teorema siguiente es una condición suficiente para que las fibras de una superficie fibrada sean conexas:

Teorema 5.27 *Si $\pi : X \longrightarrow S$ es una superficie fibrada con $\dim S = 1$ y la fibra genérica X_η es geométricamente íntegra, el homomorfismo canónico $\mathcal{O}_S \longrightarrow \pi_*\mathcal{O}_X$ es un isomorfismo.*

DEMOSTRACIÓN: El homomorfismo $\mathcal{O}_X(X) \longrightarrow \mathcal{O}_{X_\eta}(X_\eta)$ inducido por la proyección es inyectivo, ya que, para cada abierto afín $U \subset X$, el homomorfismo $\mathcal{O}_X(U) \longrightarrow \mathcal{O}_X(U)\otimes_D K(S)$ es inyectivo, ya que $\mathcal{O}_X(U)$ es plano sobre D. Ahora bien, $\mathcal{O}_{X_\eta}(X_\eta) = K(S)$ por [E 4.26] y $\mathcal{O}_X(X)$ es entero sobre D por [E 4.24], luego ha de ser $\mathcal{O}_X(X) = D$. Como $\pi_*\mathcal{O}_X$ es cuasicoherente (por [E 5.9]), concluimos que $\pi_*\mathcal{O}_X = \mathcal{O}_S$. ∎

Así, vemos que las fibras de cualquier modelo de una curva elíptica son siempre conexas. En general, cuando una superficie fibrada tiene fibras disconexas, las componentes conexas de cada fibra pueden separarse en fibras distintas mediante un cambio de base:

Teorema 5.28 *Sea X/S una superficie fibrada normal con $\dim S = 1$, sea η el punto genérico de S y $\rho : S' \longrightarrow S$ la normalización de S en $H^0(X_\eta, \mathcal{O}_{X_\eta})$. Entonces:*

a) ρ es finito y plano.

b) El homomorfismo estructural $\pi : X \longrightarrow S$ factoriza como $X \longrightarrow S' \longrightarrow S$, de modo que X/S' es una superficie fibrada normal con la misma fibra genérica X_η.

c) Las fibras de X/S' son conexas.

d) Si $s \in S$ es un punto cerrado y $s_1, \ldots, s_n$ son sus antiimágenes en S', entonces X_s es unión disjunta de curvas X_i, para $i = 1, \ldots, n$, de modo que X_{s_i} es un subesquema cerrado de X_i con el mismo espacio topológico subyacente.

DEMOSTRACIÓN: Tenemos que $S = \operatorname{Esp} D$, donde D es un dominio de Dedekind. Como X/S es propio, sabemos que $A = H^0(X, \mathcal{O}_X)$ es una D-álgebra finitamente generada, y además es un dominio íntegro íntegramente cerrado porque X es normal.

Para cada $x \in X$, el anillo $\mathcal{O}_{X,x}$ es un $\mathcal{O}_{S,\pi(x)}$-módulo plano, luego es libre de torsión por [AC A8]. Como además es un dominio íntegro, esto equivale a que el homomorfismo $\mathcal{O}_{S,\pi(x)} \longrightarrow \mathcal{O}_{X,x}$ es inyectivo, y de aquí se deduce que lo mismo sucede con el homomorfismo $\mathcal{O}_S(S) \longrightarrow \mathcal{O}_X(X)$, es decir, el homomorfismo $D \longrightarrow A$. A su vez, esto implica que si $\mathfrak{P}$ es un ideal primo de A y $\mathfrak{p} = \mathfrak{P} \cap A$, el homomorfismo natural $D_\mathfrak{p} \longrightarrow A_\mathfrak{P}$ sea también inyectivo, por lo que $A_\mathfrak{P}$ es un $D_\mathfrak{p}$-módulo libre de torsión y, por consiguiente, es plano. En definitiva, A es un D-módulo plano.

Si K es el cuerpo de cocientes de D, por el teorema [E 6.15] sabemos que $L = H^0(X_\eta, \mathcal{O}_{X_\eta}) = A \otimes_D K$. Por [E 4.26] sabemos que L es un cuerpo, luego ha de ser el cuerpo de cocientes de A. Así pues, A es la clausura normal de D

en L y, por consiguiente, $S' = \operatorname{Esp} A$. En particular, A es también un dominio de Dedekind.

Ahora a) es evidente y, como todos los anillos de $\mathcal{O}_X$ son A-álgebras, es claro que π factoriza como indica b). Es claro que X/S' es una superficie proyectiva. Para que sea una superficie fibrada sólo nos falta ver que es plana, para lo cual basta con que el homomorfismo $\pi' : X \longrightarrow S'$ sea suprayectivo. Si $s \in S$, tenemos que

$$X_s = X \times_S \operatorname{Esp} k(s) = X \times_{S'} S' \times_S \operatorname{Esp} k(s) = X \times_{S'} \operatorname{Esp}(A \otimes_D k(s)).$$

Cuando $s = \eta$ es el punto genérico de S, tenemos que $k(s) = K$ y queda que $X_\eta = X \times_{S'} \operatorname{Esp} L$, que es la fibra genérica de X/S'. En particular, el punto genérico de S' está en la imagen de X, luego ésta es todo S' y así queda probado b).

c) Es consecuencia del principio de conexión de Zariski (teorema [E A16]), ya que, por construcción, $\pi'_* \mathcal{O}_X = \mathcal{O}_{S'}$.

Para probar d) basta observar que, si $s \in S$ se corresponde con el ideal maximal $\mathfrak{p}$ de A, entonces

$$S'_s = S' \times_S k(s) = \operatorname{Esp}(A \otimes_D (D/\mathfrak{p})) = \operatorname{Esp}(A/\mathfrak{p}A).$$

Si s_i se corresponde con el ideal maximal $\mathfrak{P}_i$ de A, resulta que

$$\mathcal{O}_{S'_s, s_i} = (A/\mathfrak{p}A)_{\mathfrak{P}_i} \cong \mathcal{O}_{S', s_i}/\mathfrak{p}\mathcal{O}_{S,s}.$$

La fibra S'_s es la unión disjunta de los esquemas $P_i = \operatorname{Esp}(\mathcal{O}_{S', s_i}/\mathfrak{p}\mathcal{O}_{S,s})$ y los epimorfismos naturales $\mathcal{O}_{S', s_i}/\mathfrak{p}\mathcal{O}_{S,s} \longrightarrow \mathcal{O}_{S', s_i}/\mathfrak{P}_i = k(s_i)$ dan lugar a inmersiones cerradas $\operatorname{Esp} k(s_i) \longrightarrow P_i$ que son homeomorfismos, pues ambos esquemas constan de un único punto.

Antes hemos visto que $X_s = X \times_{S'} S'_s$, luego X_s es la unión disjunta de los esquemas $X_i = X \times_{S'} P_i$ y existen inmersiones cerradas $X_{s_i} \longrightarrow X_i$ que son homeomorfismos, tal y como afirma d). ∎

Ahora describimos los divisores primos de una superficie fibrada:

Teorema 5.29 *Sea X/S una superficie fibrada y supongamos que* $\dim S = 1$.

a) Si x es un punto cerrado de la fibra genérica X_η, entonces $\Gamma = \overline{\{x\}}$ es un subconjunto cerrado irreducible de X de dimensión 1. *Además, la restricción $\Gamma \longrightarrow S$ del homomorfismo estructural de X es finita y suprayectiva, y es un isomorfismo si x es racional.*

b) Si $\Gamma \subset X$ es un cerrado irreducible de dimensión 1, *o bien es una componente irreducible de una fibra cerrada, o bien es de la forma descrita en el apartado anterior.*

Demostración: a) Obviamente Γ es irreducible, pues es la clausura de un conjunto irreducible. El conjunto $\pi[\Gamma]$ es cerrado en S (porque X/S es proyectivo) y contiene al punto genérico η, luego $\pi[\Gamma] = S$.

Como x es cerrado en X_η, tenemos que $\Gamma \cap X_\eta = \{x\}$, luego $\Gamma \neq X$ y, por consiguiente, $\dim \Gamma \leq 1$.

Si $s \in S$ es cerrado, el teorema 5.3 nos da que $\dim X_s = 1$, luego se cumple que $\dim(\Gamma \cap X_s) \leq 1$. Si se diera la igualdad, la intersección tendría una componente irreducible de dimensión 1, que sería un cerrado irreducible contenido en Γ y de la misma dimensión que Γ, luego habría de ser todo Γ. Tendríamos entonces que $\Gamma \subset X_s$, en contradicción con la suprayectividad de π. Así pues, las fibras de $\pi|_\Gamma$ son finitas, y el teorema [E 4.43] nos da que $\pi|_\Gamma$ es un homomorfismo finito. El teorema [AC 3.68] implica ahora que $\dim \Gamma = 1$.

Si x es racional (como punto de X_η/K), es decir, si $k(x) = K = K(S)$, entonces $\pi : \Gamma \longrightarrow S$ es un homomorfismo finito y birracional. Como S es normal, el teorema [E A.21] implica que es un isomorfismo.

b) Tenemos que $\pi[\Gamma]$ es un cerrado irreducible de S, luego, o bien es un punto, o bien $\pi[\Gamma] = S$. En el primer caso Γ está contenido en la fibra de un punto cerrado, y como Γ y la fibra tienen ambos dimensión 1, concluimos que Γ es una componente irreducible de dicha fibra. En el segundo caso Γ contiene un punto $x \in X_\eta$, luego también contiene a $\overline{\{x\}}$, que por a) es irreducible y de dimensión 1, luego $\Gamma = \overline{\{x\}}$. ∎

Definición 5.30 Sea X/S una superficie fibrada y sea Γ un divisor primo de X. Diremos que Γ es *horizontal* si $\dim S = 1$ y $\pi|_\Gamma : \Gamma \longrightarrow S$ es suprayectiva. Si $\pi[\Gamma]$ se reduce a un punto diremos que Γ es *vertical.*

En estos términos, el teorema anterior afirma que todo divisor primo es horizontal o vertical. Más en general, diremos que un divisor de Weil es *horizontal* o *vertical* si todos sus divisores primos lo son.

Ejemplo Si W/S es un modelo de Weierstrass, sus divisores primos verticales son sus fibras (porque son irreducibles), mientras que el conjunto O descrito en el teorema 5.10 es un ejemplo de divisor primo horizontal. Es el divisor "infinito", que contiene al punto infinito de cada una de las fibras. El hecho de que corte a cada fibra exactamente en un punto es, como hemos visto, consecuencia de que el punto o_η es racional. Para otros puntos no tiene por qué ser cierto.

Consideremos, por poner un ejemplo concreto, el modelo de Weierstrass $W/\mathbb{Z}$ asociado a la ecuación

$$Y^2 = X(X^2 + 1).$$

El punto racional $u = (x, y) \in W_\eta$ da lugar al divisor horizontal $\Gamma = \overline{\{u\}}$ que corta a cada fibra en el punto racional $(p, x, y) \in W_p$. Sin embargo, el punto cerrado $v = (x^2 + 1, y) \in W_\eta$ (que se corresponde con el par de puntos conjugados $(x \pm i, y) \in W_{\eta\,\mathbb{Q}}$) cumple que

$$\overline{\{v\}} \cap W_p = \begin{cases} \{(2, x+1, y)\} & \text{si } p = 2, \\ \{(p, x+a, y), (p, x-a, y)\} & \text{si } a^2 \equiv -1 \text{ (mód } p), \ p \neq 2, \\ \{(p, x^2+1, y)\} & \text{si } p \equiv -1 \text{ (mód } 4). \end{cases}$$

∎

En las superficies aritméticas podemos identificar las fibras cerradas con divisores:

Teorema 5.31 *Sea X/S una superficie fibrada con $\dim S = 1$, sea $s \in S$ un punto cerrado y sean $\Gamma_1, \dots, \Gamma_d$ las componentes irreducibles de la fibra X_s. Entonces, X_s coincide con el subesquema cerrado asociado al divisor de Cartier $\pi^*(s)$, donde $\pi : X \longrightarrow S$ es el homomorfismo estructural. Si X/S es normal en codimensión 1, este divisor se corresponde a su vez con el divisor de Weil $\Gamma_1^{r_1} \cdots \Gamma_d^{r_d}$, en el que las multiplicidades vienen dadas por $r_i = v_{\xi_i}(p)$, donde $\xi_i \in \Gamma_i$ es el punto genérico, $p \in \mathcal{O}_{S,s}$ es un primo y v_{ξ_i} es la valoración del anillo de valoración discreta $\mathcal{O}_{X,\xi_i}$.*

Demostración: Podemos ver a s como divisor (primo) de Weil en S. Como S es regular, s se corresponde a su vez con un divisor de Cartier, lo que nos permite considerar su imagen inversa $D = \pi^*(s) \in \mathrm{Div}_c(X)$. Como s es un divisor entero, también lo es D. Vamos a comprobar que, considerados como esquemas, $X_s = D$.

En primer lugar observamos que podemos sustituir S por cualquier entorno afín de s, y de este modo podemos suponer que, si $S = \mathrm{Esp}\, D$, el divisor de Cartier s está definido por un único $p \in D$. Esto significa que, si $\mathfrak{p}$ es el ideal de D que se corresponde con s, se cumple $v_{\mathfrak{p}}(p) = 1$ y $v_{\mathfrak{q}}(p) = 0$ para todo $\mathfrak{q} \neq \mathfrak{p}$. A su vez, esto implica que $\mathfrak{p} = (p)$. Si U es un abierto afín en X, entonces

$$\mathcal{O}_{X_s}(X_s \cap U) = \mathcal{O}_X(U) \otimes_A (A/(p)) \cong \mathcal{O}_X(U)/p\mathcal{O}_X(U),$$

de donde deducimos que X_s es el subesquema cerrado asociado de X al haz de ideales $p\mathcal{O}_X$, pero, por definición de $\pi^*(s)$, es inmediato que $\mathcal{O}_X(D^{-1}) = p\mathcal{O}_X$, luego $X_s = D$ como esquemas. Cuando la superficie es normal en codimensión 1, el teorema 4.4 nos da que los exponentes de cada Γ_i en el divisor de Weil asociado a D vienen dados por $r_i = v_{\xi_i}(D_{\xi_i}) = v_{\xi_i}(p)$. ∎

De acuerdo con el teorema 4.3, las fibras de las superficies fibradas normales son esquemas de Cohen-Macaulay, de modo que no tienen puntos asociados que no sean cuasigenéricos. Ahora vamos a probar que si la superficie es localmente una intersección completa (en particular, si es regular), lo mismo le sucede a cada fibra. Recordemos ([E 9.27]) que ésta es la condición para que esté definido el haz canónico.

Teorema 5.32 *Sea X/S una superficie fibrada con $\dim S = 1$ y que sea localmente una intersección completa, sea $s \in S$ un punto cerrado y $E \mid X_s$ un divisor de Cartier vertical entero. Entonces $E/k(s)$ es también localmente una intersección completa.*

Demostración: Como la propiedad es local, podemos suponer que tenemos un diagrama conmutativo

$$\begin{array}{ccccc} E & \longrightarrow & X & \longrightarrow & A^n_S \\ & \searrow & \uparrow & & \uparrow \\ & & X_s & \longrightarrow & A^n_{k(s)} \end{array}$$

donde las flechas horizontales son inmersiones cerradas y las de la fila superior son regulares. Por definición de inmersión regular, esto significa que, para cada $x \in E$, tenemos que $\mathcal{O}_{E,x} = \mathcal{O}_{A^n_S,x}/(b_1,\dots,b_m)$, donde $b_1,\dots,b_m$ es una sucesión regular. En particular (ver las observaciones tras [AC 5.22]) tenemos que

$$\dim \mathcal{O}_{E,x} = \dim \mathcal{O}_{A^n_S,x} - m.$$

Por otra parte, como X/S y A^n_S/S son planos, tenemos ([E 4.52]) que

$$\dim \mathcal{O}_{E,x} = \dim \mathcal{O}_{X_s,x} = \dim \mathcal{O}_{X,x} - \dim \mathcal{O}_{S,s},$$

$$\dim \mathcal{O}_{A^n_{k(s)},x} = \dim \mathcal{O}_{A^n_S,x} - \dim \mathcal{O}_{S,s},$$

de donde se sigue que $\dim \mathcal{O}_{E,x} = \dim \mathcal{O}_{A^n_{k(s)},x} - m$. Como

$$\mathcal{O}_{E,x} = \mathcal{O}_{A^n_{k(s)},x}/(b_1,\dots,b_m),$$

es fácil ver que $b_1,\dots,b_m$ son también una sucesión regular en $\mathcal{O}_{A^n_{k(s)},x}$. (Por el teorema [AC 5.18], cada b_i rebaja a lo sumo la dimensión en una unidad, y si es un divisor de 0 es claro que no la rebaja.) Esto prueba que la inmersión $E \longrightarrow A^n_{k(s)}$ es regular, luego $E/k(s)$ es localmente una inmersión completa. ∎

Notemos que una mínima variante del argumento anterior (eliminando el divisor) muestra que todas las fibras de X/S (incluida la genérica) son localmente intersecciones completas.

5.4 Un ejemplo de desingularización

Hemos visto un ejemplo de cómo podemos eliminar un punto singular de una superficie aritmética mediante una explosión. No obstante, a veces es necesario realizar varias explosiones sucesivas. Dedicamos íntegramente esta última sección a discutir un ejemplo de desingularización no trivial. Concretamente, partiremos de la superficie fibrada $X/\mathbb{Z}$ definida por la ecuación de Selmer:

$$3X^3 + 4Y^3 + 5Z^5 = 0.$$

El criterio jacobiano implica que esta ecuación define una curva geométricamente regular sobre todo cuerpo de característica distinta de 2, 3 o 5.

No vamos a necesitar este hecho, pero en el último ejemplo del capítulo VIII de [CE] se demuestra que esta curva no tiene puntos racionales sobre $\mathbb{Q}$, mientras que sí que los tiene sobre cada cuerpo p-ádico $\mathbb{Q}_p$ y, por consiguiente, sobre cada cuerpo finito $\mathbb{Z}/p\mathbb{Z}$. Así pues, $X_\eta/\mathbb{Q}$ no es una curva elíptica, mientras que sí que lo es cada fibra X_p (sobre $\mathbb{Z}/p\mathbb{Z}$) para todo primo $p \neq 2, 3, 5$.

Los únicos posibles puntos singulares de X han de estar en las fibras X_2, X_3 o X_5. Empezando por la última, vemos que se trata de la curva proyectiva sobre $\mathbb{Z}/5\mathbb{Z}$ definida por la ecuación homogénea

$$3X^3 + 4Y^3 = 0.$$

El criterio jacobiano muestra que su único punto no geométricamente regular es el asociado al ideal homogéneo $(5, x, y)$. Ahora bien, un entorno afín de este punto en X es la superficie determinada por la deshomogeneización de la ecuación respecto de Z, que es

$$3X^3 + 4Y^3 + 5 = 0,$$

y, como ideal de $\mathbb{Z}[x, y]$, el punto es $\mathfrak{p} = (5, x, y) = (x, y)$, y esto implica que el ideal maximal de $\mathcal{O}_{X,\mathfrak{p}}$ está generado también por dos elementos, luego $\mathfrak{p}$ es regular en X. Así pues, en X_5 hay un punto no suave, pero ningún punto singular en X.

Para estudiar la fibra X_2 podemos sustituir X por $X \times_{\mathbb{Z}} \operatorname{Esp} \mathbb{Z}_2$ y considerar que X está definido sobre el anillo de valoración discreta $\mathbb{Z}_2$. La fibra X_2 es la curva proyectiva sobre $k = \mathbb{Z}/2\mathbb{Z}$ dada por la ecuación

$$X^3 + Z^3 = (X + Z)(X^2 + XZ + Z^2) = 0.$$

Vemos que consta de dos componentes irreducibles con multiplicidad 1:

$$\Gamma_1 = (2, x + z), \qquad \Gamma_2 = (2, x^2 + xz + z^2).$$

La primera es una recta $\Gamma_1 \cong \mathrm{P}^1_k$, mientras que la segunda es una cónica singular, cuyo punto singular es, concretamente, el punto $p_0 = (2, x, z)$ en el que corta a Γ_1. Vemos así que todos los puntos de la fibra son geométricamente regulares (luego suaves en X, luego regulares) excepto el punto de intersección de las componentes.

Podríamos probar que p_0 es, de hecho, singular en X, pero podremos llegar a esta conclusión indirectamente al calcular la explosión $\widetilde{X} \longrightarrow X$ de centro p_0. En efecto, el teorema 5.25 afirma que si p_0 fuera regular, su fibra en la explosión sería isomorfa a P^1_k, pero vamos a ver que es una recta doble, de modo que será isomorfa a P^1_k con la estructura de subesquema cerrado reducido, pero no con la estructura de esquema asociada a la fibra.

Para determinar la fibra de p_0 en $\widetilde{X}$ y, más en general, la fibra $\widetilde{X}_2$ de la explosión, podemos restringirnos al entorno afín U de p_0 determinado por la deshomogeneización de la ecuación respecto de Y, que es

$$3X^3 + 5Z^3 + 4 = 0.$$

Como ideal de $\mathbb{Z}_2[x, z]$, el punto p_0 se corresponde con el ideal $\mathfrak{p} = (2, x, z)$. La explosión $\widetilde{U}$ es unión de tres abiertos. Dejamos que el lector calcule las ecuaciones de $U_1 = \operatorname{Esp} \mathbb{Z}_2[x, z, x/2, z/2]$ y que compruebe que su fibra cerrada es vacía, por lo que podemos prescindir de U_1.

En cuanto a $U_2 = \operatorname{Esp} \mathbb{Z}_2[x, z, z/x, 2/x] = \operatorname{Esp} \mathbb{Z}_2[x, z', u]$, sustituyendo $z = xz'$, $2 = xu$ en la ecuación y dividiendo entre x^2, llegamos a que está determinado por las ecuaciones

$$3x + 5xz'^3 + u^2 = 0, \qquad xu = 2.$$

Por último, $U_3 = \operatorname{Esp}\mathbb{Z}_2[x, z, x/z, 2/z] = \operatorname{Esp}\mathbb{Z}_2[x', z, u']$ está determinado por las ecuaciones

$$3x'^3z + 5z + u'^2 = 0, \qquad zu' = 2.$$

Los puntos cuasigenéricos de la fibra cerrada $\widetilde{U}_2$ son los primos minimales del ideal $(2) \subset \mathbb{Z}_2[x, z', u]$. Si $\mathfrak{P}$ es uno de ellos, como $2 \in \mathfrak{P}$, la segunda ecuación implica que $x \in \mathfrak{P}$ o bien $u \in \mathfrak{P}$. En el primer caso, la primera ecuación implica que también $u \in \mathfrak{P}$. En el segundo caso, la primera ecuación nos da que $x(z'^3 + 1) = x(z' + 1)(z'^2 + z' + 1) \in \mathfrak{P}$. En total, llegamos a que el ideal (2) tiene tres primos minimales:

$$\mathfrak{P}_1 = (2, u, z' + 1), \quad \mathfrak{P}_2 = (2, u, z'^2 + z' + 1), \quad \mathfrak{P}_3 = (2, u, x).$$

Podemos comprobar que son realmente primos viendo que sus cocientes son dominios íntegros. Por ejemplo,

$$\mathbb{Z}_2[x, z', u]/\mathfrak{P}_2 \cong \mathbb{Z}_2[X, Z, U]/(2, U, Z^2 + Z + 1)$$

$$\cong k[X, Z]/(Z^2 + Z + 1) \cong k'[X],$$

donde $k' = k[Z]/(Z^2 + z + 1)$ es el cuerpo de cuatro elementos.

Similarmente, el ideal $(2) \subset k[x', z, u']$ tiene los tres primos minimales

$$\mathfrak{Q}_1 = (2, u', x' + 1), \quad \mathfrak{Q}_2 = (2, u', x'^2 + x' + 1), \quad \mathfrak{Q}_3 = (2, u', x').$$

Así pues, las fibras cerradas de $\widetilde{U}_2$ y $\widetilde{U}_3$ tienen tres componentes irreducibles cada una, pero éstas resultan ser las intersecciones con los abiertos correspondientes de tres únicas componentes irreducibles de $\widetilde{X}_2$, a las que llamaremos Γ_1, Γ_2 y Γ_3. Para comprobar que es así observamos que la relación entre los sistemas coordenados de U_2 y U_3 es la dada por

$$x' = 1/z', \quad z = xz', \quad u' = u/z', \qquad x = x'z, \quad z' = 1/x', \quad u = u'/x'.$$

Esto significa que $U_2 \cap U_3$ es $D(z')$ en U_2 y $D(x')$ en U_3. Así, por ejemplo, el ideal $\mathfrak{P}_2$ define una componente irreducible en U_2 cuya intersección con $U_2 \cap U_3$ viene dada por el ideal $(2, u, z'^2 + z' + 1) \subset D(z')$ que se corresponde con el ideal

$$(2, u'/x', 1/x'^2 + 1/x' + 1) = (2, u', 1 + x' + x'^2) \subset D(x'),$$

que a su vez se corresponde con el ideal $\mathfrak{Q}_2$ de U_3.

La fibra de $\mathfrak{p}$ respecto de la explosión es

$$U_{2,\mathfrak{p}} = \operatorname{Esp}(\mathbb{Z}_2[x, z', u]/(x)),$$

cuyo único primo minimal es $\mathfrak{P}_3$, pero con multiplicidad mayor que 1. Concretamente, su multiplicidad es $v_{\mathfrak{P}_3}(x)$. Para calcularla observamos que el ideal maximal de $\mathcal{O}_{\widetilde{U},\mathfrak{P}_3}$ es $\mathfrak{P}_3 = (u)$, ya que, en este anillo local,

$$x = \frac{u^2}{z'^3 + 1}.$$

En efecto, notemos que $z'^3+1 \notin \mathfrak{P}_3$, porque $\mathbb{Z}_2[x,z',u]/\mathfrak{P}_3 = k[Z]$. Por consiguiente, $v_{\mathfrak{P}_3}(x) = 2$. Según observábamos más arriba, esto prueba que $\mathfrak{p}$ es singular en X.

Observemos que Γ_3 tiene multiplicidad 2 en la fibra $\widetilde{X}_\mathfrak{p}$ (respecto de la explosión), pero su multiplicidad en la fibra $\widetilde{X}_2$ (respecto del homomorfismo estructural) es $v_{\mathfrak{P}_3}(2) = v_{\mathfrak{P}_3}(xu) = 3$.

Hemos probado que Γ_3 es la única componente irreducible de $\widetilde{X}_2$ que se contrae al punto $\mathfrak{p}$ de X_2. Ahora vamos a ver que la explosión transforma Γ_1 y Γ_2 en las componentes del mismo nombre en X (y ésta es la razón por la que las hemos llamado así). En efecto, la explosión $U_2 \longrightarrow U$ está asociada al homomorfismo $\mathbb{Z}_2[x,z] \longrightarrow \mathbb{Z}_2[x,z',u]$ dado por

$$x \mapsto x, \quad z \mapsto xz'.$$

La antiimagen de $\mathfrak{P}_1$ (es decir, la imagen del punto genérico de Γ_1) contiene a 2 y a $x+z = x(1+z')$, luego contiene a $(2, x+z)$, y se tiene que dar la igualdad o, de lo contrario, $\Gamma_1 \subset \widetilde{U}$ se contraería a un punto de U, pero sólo Γ_3 puede contraerse a un punto. Similarmente se concluye que $\Gamma_2 \subset \widetilde{U}$ tiene por imagen a $\Gamma_2 \subset U$.

Podríamos calcular las multiplicidades de Γ_1 y Γ_2, pero han de ser iguales a 1, porque la explosión se restringe a un isomorfismo sobre un entorno de sus puntos genéricos y Γ_1 y Γ_2 tienen multiplicidad 1 en U.

Notemos que, en $\widetilde{U}$, se cumple que $\Gamma_1 \cap \Gamma_2 = \varnothing$ (pues no se cortan ni en U_2 ni en U_3), mientras que ambas componentes cortan a Γ_3 en puntos distintos, que, por ejemplo, en U_2 vienen dados por los ideales

$$\Gamma_1 \cap \Gamma_3 = (2, u, x, z'+1), \qquad \Gamma_2 \cap \Gamma_3 = (2, u, x, z'^2+z'+1).$$

(También se cortan en U_3, pero los puntos resultan ser los correspondientes a estos dos por el cambio de coordenadas.)

Por último, vamos a determinar la estructura de subesquema cerrado reducido de Γ_1, Γ_2 y Γ_3. La más simple es Γ_3, que está contenida en la unión de los dos abiertos afines $\Gamma_3 \cap U_2$ y $\Gamma_3 \cap U_3$, y los dos son isomorfos a A^1_k, pues

$$\mathbb{Z}_2[x,z',u]/\mathfrak{P}_3 \cong k[Z], \qquad \mathbb{Z}_2[x',z,u']/\mathfrak{Q}_3 \cong k[Z].$$

Por consiguiente, Γ_3 es una curva proyectiva regular birracionalmente equivalente a A^1_k, luego $\Gamma_3 \cong \mathrm{P}^1_k$, porque dos curvas proyectivas regulares birracionalmente equivalentes son isomorfas.

Lo mismo vale para Γ_1 con la única salvedad de que no está cubierto por los abiertos $\Gamma_1 \cap U_2$ y $\Gamma_1 \cap U_3$, porque Γ_1 contiene también la antiimagen del único punto de $\Gamma_1 \subset X$ que no está en U. Ahora bien, como este punto es regular y la explosión es un isomorfismo fuera de la fibra de $\mathfrak{p}$, podemos concluir igualmente que $\Gamma_1 \subset \widetilde{X}$ es una curva proyectiva regular birracionalmente equivalente a P^1_k, luego $\Gamma_1 \cong \mathrm{P}^1_k$.

Para Γ_2 sucede también que no está cubierta por U_2 y U_3, pero además resulta que

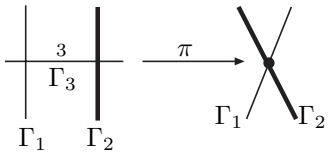
$$\mathbb{Z}_2[x, z', u]/\mathfrak{P}_2 \cong k'[X], \quad \mathbb{Z}_2[x', z, u']/\mathfrak{Q}_2 \cong k'[Z],$$

donde k' es el cuerpo de 4 elementos. Así pues, $\Gamma_2 \cap U_2 \cong A^1_{k'}$, $\Gamma_2 \cap U_3 \cong A^1_{k'}$. Más aún, los puntos de Γ_2 que no están en $\widetilde{U}$ tienen un entorno isomorfo a $\Gamma_2 \cap D(z) \subset X$, que es la curva asociada al ideal $(2, x^2 + x + 1) \subset \mathbb{Z}_2[x, y]$, y también

$$\mathbb{Z}_2[x, y]/(2, x^2 + x + 1) \cong k'[Y].$$

En suma, con la estructura de subesquema cerrado reducido, todo punto de $\Gamma_2 \subset \widetilde{X}$ tiene un entorno isomorfo a $A^1_{k'}$. Esto prueba que Γ_2 (con su estructura de esquema ya fijada) está definido sobre k', y resulta ser una curva proyectiva regular birracionalmente equivalente a $\mathrm{P}^1_{k'}$. Así pues, $\Gamma_2 \cong \mathrm{P}^1_{k'}$.

En particular, vemos que, aunque $\Gamma_2 \subset \widetilde{X}$ y $\Gamma_2 \subset X$ son birracionalmente equivalentes, no son isomorfos, pues el primero es regular y, tras una extensión de constantes, se escinde en dos rectas proyectivas disjuntas, isomorfas a $\mathrm{P}^1_{k'}$, luego es geométricamente regular; por el contrario, el segundo tiene un punto singular y se escinde en dos rectas proyectivas, también isomorfas a $\mathrm{P}^1_{k'}$, pero que se cortan en un punto singular. (Más precisamente, $\Gamma_2 \subset \widetilde{X}$ es la normalización de $\Gamma_2 \subset X$.)



Con esto tenemos ya la estructura de la fibra cerrada $\widetilde{U}_2$. Está formada por dos componentes simples $\Gamma_1 \cong \mathrm{P}^1_k$ y $\Gamma_2 \cong \mathrm{P}^1_{k'}$ que se biyectan con las componentes irreducibles de U_2 y una componente triple $\Gamma_2 \cong \mathrm{P}^1_k$ que se contrae al punto singular de U_2. De aquí se sigue que los puntos de Γ_1 y Γ_2 que no están en Γ_3 son suaves en $\widetilde{X}$, y en particular regulares. Los puntos de Γ_3 no pueden ser suaves, pues no son reducidos en la fibra, luego no son regulares en ella, pero esto no impide que sean regulares en $\widetilde{X}$.

Vamos a ver que todos los puntos de Γ_3 son regulares en $\widetilde{X}$ excepto aquellos en los que corta a Γ_1 y a Γ_2. En efecto, consideremos un punto que esté en U_2 (con U_3 se razona análogamente). Será un ideal $\mathfrak{P}$ que contiene a $\mathfrak{P}_3$ pero no a $z'^3 + 1$. Como $\mathbb{Z}_2[x, z', u]/\mathfrak{P}_3 \cong k[Z]$, será, concretamente, de la forma

$$\mathfrak{P} = (2, u, x, p(z')),$$

y, como ideal de $\mathcal{O}_{\widetilde{X},\mathfrak{P}}$, se cumple que $\mathfrak{P} = (u, p(z'))$, pues $2 = xu$ y

$$x = \frac{u^2}{z'^3 + 1}.$$

Esto prueba que $\mathfrak{P}$ es regular. No necesitamos probar que los dos puntos que faltan son realmente singulares en $\widetilde{X}$, pues ahora vamos a calcular la explosión de $X^1 = \widetilde{X}$ respecto de Γ_3 con la estructura de subesquema cerrado reducido,

y el teorema 5.25 implica que si fueran regulares sus fibras se reducirían a un punto cada una. Sin embargo, veremos que no es así.

Como sabemos que las fibras de los puntos de Γ_3 serán todas triviales excepto a lo sumo las de los puntos de intersección con Γ_1 y Γ_2 y ambos puntos están en U_2, podemos limitarnos a calcular la explosión de U_2. En este abierto, tenemos que $\Gamma_3 = (2, x, u) = (x, u)$, luego la explosión será la unión de dos abiertos, U_{21} y U_{22}.

El primero es $U_{21} = \operatorname{Esp} \mathbb{Z}_2[x, z', u, x/u] = \operatorname{Esp} \mathbb{Z}_2[x', z', u]$, cuyos generadores cumplen las ecuaciones

$$3x' + 5x'z'^3 + u = 0, \qquad x'u^2 = 2.$$

Como podemos despejar u en la primera ecuación, resulta que

$$\mathbb{Z}_2[x', z', u] = \mathbb{Z}_2[x', z']$$

y los generadores cumplen la ecuación

$$x'^3(3 + 5z'^3)^2 = 2.$$

Se comprueba que es irreducible. El segundo abierto es

$$U_{22} = \operatorname{Esp} \mathbb{Z}_2[x, z', u, u/x] = \operatorname{Esp} \mathbb{Z}_2[x, z', u'],$$

cuyos generadores cumplen

$$3 + 5z'^3 + xu'^2 = 0, \qquad x^2u' = 2.$$

Los puntos genéricos de las componentes irreducibles de la fibra cerrada de U_{21} son

$$\mathfrak{P}_3 = (2, x'), \quad \mathfrak{P}_4 = (2, z' + 1), \quad \mathfrak{P}_5 = (2, z'^2 + z' + 1),$$

mientras que los de U_{22} son

$$\mathfrak{Q}_1 = (2, u', z' + 1), \quad \mathfrak{Q}_2 = (2, u', z'^2 + z' + 1).$$

$$\mathfrak{Q}_4 = (2, x, z' + 1), \quad \mathfrak{Q}_5 = (2, x, z'^2 + z' + 1),$$

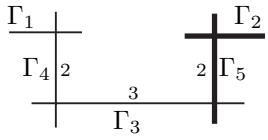
Los subíndices están elegidos de modo que $\mathfrak{P}_i$ y $\mathfrak{Q}_i$ definen abiertos en la misma componente irreducible Γ_i de la fibra cerrada $\tilde{X}_2^1$. Esto se comprueba sin dificultad teniendo en cuenta que $x = ux' = -x'^2(3 + 5z'^3) \in \mathfrak{P}_4 \cap \mathfrak{P}_5$.

También es fácil ver que Γ_4 se contrae al punto $(2, u, x, z' + 1)$ y Γ_5 se contrae a $(2, u, x, z'^2 + z' + 1)$. Basta tener en cuenta que la explosión $U_{21} \longrightarrow U_2$ está inducida por el homomorfismo de anillos $\mathbb{Z}_2[x, z', u] \longrightarrow \mathbb{Z}_2[x', z']$ dado por

$$x \mapsto -x'^2(3 + 5z'^3), \quad u \mapsto -x'(3 + 5z'^3).$$

Por consiguiente, Γ_1, Γ_2 y Γ_3 han de corresponderse con las componentes irreducibles de la fibra cerrada de U_2 con el mismo nombre. (Es fácil ver

que, concretamente, la correspondencia es la que determina la elección de los subíndices.)



La fibra cerrada de U_{21} tiene ecuación

$$x'^3(z'+1)^2(z'^2+z'+1)^2=0,$$

de donde se sigue que Γ_3 tiene multiplicidad 3 (esto ya lo sabíamos) y Γ_4 y Γ_5 tienen multiplicidad 2. Analizando las intersecciones, se comprueba sin dificultad que la estructura de la fibra cerrada es la que indica la figura. También es fácil ver que $\Gamma_1\cong\Gamma_2\cong\Gamma_3\cong \mathrm{P}^1_k$, $\Gamma_4\cong\Gamma_5\cong \mathrm{P}^1_{k'}$.

Teniendo en cuenta que la explosión es un isomorfismo fuera de la antiimagen de Γ_3, los posibles puntos singulares de $\widetilde{X}^1$ han de estar en $\Gamma_4\cup\Gamma_5$. Ahora bien, $\mathfrak{P}_4=(2,z'+1)=(z'+1)$, de donde se sigue que todos los puntos de $\Gamma_4\cap U_{21}$ se corresponden con ideales generados por dos elementos, luego son regulares en $\widetilde{X}^1$. El único punto de Γ_4 que no está en U_{21} es el punto de intersección con Γ_1, es decir, $\mathfrak{q}=(2,x,z'+1,u')$. Pero en $\mathcal{O}_{\widetilde{X}^1,\mathfrak{q}}$ se cumple que $\mathfrak{q}=(x,u')$, pues

$$z'+1=-\frac{(1+2z'^3)2+xu'^2}{z'^2+z'+1}.$$

Similarmente se razona con Γ_5. Resulta, pues, que $\widetilde{X}^1$ es un modelo regular de la curva de Selmer sobre $\mathbb{Z}_2$.

Seguidamente consideramos la superficie fibrada definida por la ecuación de Selmer sobre $\mathbb{Z}_3$. Ahora la fibra cerrada tiene ecuación $(Y-Z)^3=0$, luego está formada por una recta $\Gamma_1\cong \mathrm{P}^1_k$ con multiplicidad 3 (donde ahora llamamos $k=\mathbb{Z}/3\mathbb{Z}$). Estudiemos el abierto afín $D(x)=\operatorname{Esp}\mathbb{Z}_3[y,z]$, cuyos generadores cumplen la ecuación

$$3+4y^3+5z^3=0.$$

La componente irreducible de la fibra cerrada es $(3,y-z)$. Como

$$\mathbb{Z}_3[y,z]/(3,y-z)=k[Y],$$

un punto cerrado de la fibra es de la forma $\mathfrak{p}=(3,y-z,p(y))$, pero observamos que

$$3+3y^3+6y^3+y^3-z^3=0,$$

luego

$$3(1+y^3+2z^3)=-(y^3-z^3)=-(y^2+yz+z^2)(y-z),$$

luego

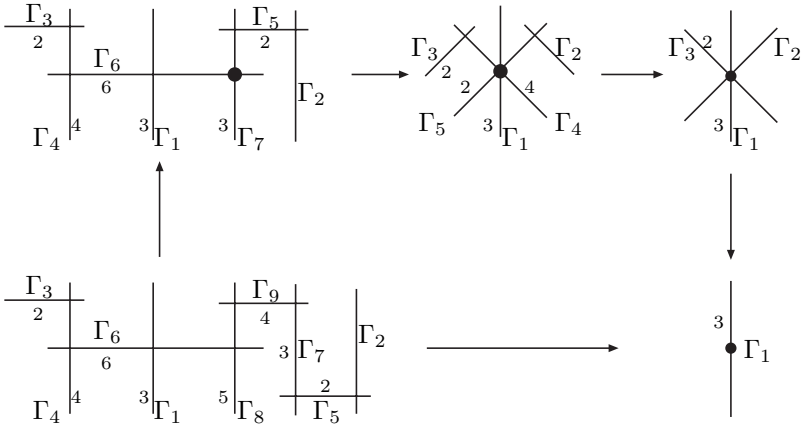
$$3=-\frac{y^2+yz+z^2}{1+y^3+2z^3}(y-z),$$

donde el denominador no está en $\mathfrak{p}$. Por consiguiente, el ideal maximal de $\mathcal{O}_{X,\mathfrak{p}}$ admite un generador con dos elementos, y esto prueba que $\mathfrak{p}$ es regular en X. Esto sólo nos deja un posible punto singular, el único punto de la fibra cerrada

que no está en $D(x)$, a saber, $(3, x, y-z)$. Para estudiarlo podemos restringirnos al abierto afín $U = D(z)$, en el que la ecuación de X es

$$3X^3 + 4Y^3 + 5 = 0,$$

y el punto se corresponde con el ideal $\mathfrak{p} = (3, x, y-1)$. Esta vez son necesarias cuatro explosiones sucesivas para llegar a una superficie regular. La figura resume el proceso:



Todas las componentes irreducibles son isomorfas a P^1_k y tienen la multiplicidad indicada (igual a 1 si no se especifica). Los únicos puntos singulares son los destacados. Nos limitaremos a dar un esbozo del proceso y dejaremos los detalles a cargo del lector.

En primer lugar, para simplificar los cálculos, hacemos el cambio de variable $y = y' - 1$, con lo que el punto singular pasa a ser $(3, x, y)$. La ecuación se transforma en:

$$3x^3 + 4y^3 + 12y^2 + 12y + 9 = 0.$$

La transformación $y = xy_1$, $3 = xz$ nos da la superficie definida por las ecuaciones

$$3x + 4xy_1^3 + 4y_1 z + z^2 = 0, \quad xz = 3.$$

La fibra cerrada tiene tres componentes irreducibles, cuyos puntos genéricos son

$$\Gamma_1 = (3, y_1, z), \quad \Gamma_2 = (3, x, y_1 + z), \quad \Gamma_3 = (3, x, z).$$

Las tres se cortan en un único punto singular: $(3, x, y_1, z) = (x, y_1, z)$. La transformación $y_1 = xy_2$, $z = xz_1$ nos lleva a la superficie determinada por las ecuaciones

$$xz_1 + 4x^2y_2^3 + 12y_2^2 + 4y_2z_1 + z_1^2 = 0, \qquad x^2z_1 = 3.$$

La fibra cerrada consta de tres componentes irreducibles, cuyos puntos genéricos son

$$\Gamma_1 = (3, y_2, z_1), \quad \Gamma_4 = (3, x, z_2), \quad \Gamma_5 = (3, x, y_2 + z_1).$$

Las tres se cortan en un único punto singular: $(3, x, y_2, z_1) = (x, y_2, z_1)$. La transformación $y_2 = xy_3$, $z_2 = xz_1$ nos lleva a las ecuaciones:

$$z_2 + 4x^3y_3^3 + 12y_3^2 + 4y_3z_2 + z_2^2 = 0, \qquad x^3z_2 = 3.$$

La fibra cerrada consta de tres componentes irreducibles, cuyos puntos genéricos son

$$\Gamma_1 = (3, y_3, z_2), \quad \Gamma_6 = (3, x, z_2), \quad \Gamma_7 = (3, x, y_3 + z_2 + 1).$$

El único punto singular es la intersección de las dos últimas: $(3, x, y_3+1, z_2)$. Hacemos el cambio de variables $y_3 = y_3' - 1$, con lo que el punto se convierte en (x, y_3, z_2), y las ecuaciones pasan a ser

$$-3z_2+4x^3y_3^3-12x^3y_3^2+12x^3y_3-4x^3+12y_3^2-24y_3+4y_3z_2+z_2^2+12 = 0,\ x^3z_2 = 3.$$

La transformación $y_4 = xy_3$, $z_3 = xz_2$ nos lleva a las ecuaciones $x^4z_3 = 3$,

$$-x^3z_3^2+4x^4y_4^3-12x^3y_4^2+12x^2y_4-4x+12y_4^2-8x^3y_4z_3+4y_4z_3+z_3^2+4x^2z_3 = 0.$$

La fibra cerrada consta de tres componentes irreducibles, cuyos puntos genéricos son

$$\Gamma_1 = (3, xy_4 - 1, z_3), \quad \Gamma_8 = (3, x, z_3), \quad \Gamma_9 = (3, x, y_4 + z_3).$$

La superficie obtenida de este modo resulta ser regular.

Terminamos la sección con una observación: hemos trabajado con las curvas definidas por la ecuación de Selmer sobre $\mathbb{Z}_2$ y $\mathbb{Z}_3$ por una simple cuestión de comodidad. Podríamos haber trabajado igualmente sobre $\mathbb{Z}$ para obtener dos superficies sobre $\mathbb{Z}$, una con una única singularidad en la fibra del 2 y otra con una única singularidad en la fibra del 3. A su vez, estas dos superficies pueden pegarse para formar una superficie regular $X/\mathbb{Z}$ cuyas fibras coinciden con las de la superficie de partida excepto X_2 y X_3, que tendrán la estructura que hemos obtenido. No obstante, no merece la pena entrar en ello porque más adelante será inmediato.[3]

[3]Véase el ejemplo de la página 220

Capítulo VI

Superficies regulares

En las tres secciones de este capítulo sentaremos las bases del estudio de las superficies aritméticas que realizaremos en el capítulo siguiente. En la primera expondremos los resultados básicos de la teoría de intersecciones de curvas en superficies regulares; en la segunda estudiaremos las aplicaciones birracionales entre superficies fibradas normales, y demostraremos, entre otras cosas, que todo homomorfismo birracional entre superficies fibradas regulares es una composición de explosiones de puntos cerrados; y en la tercera enunciaremos el teorema de Lipman sobre desingularización de superficies excelentes y, a partir de él, demostraremos que toda superficie fibrada (con fibra geométricamente regular) admite una desingularización.

6.1 Intersecciones de curvas

Consideremos un esquema noetheriano regular y conexo X de dimensión 2. En este contexto los divisores de Weil se identifican con los de Cartier, por lo que no distinguiremos entre ambos. Sean D, $E \in \mathrm{Div}(X)$ dos divisores enteros primos entre sí. Esto se traduce en que $D \cap E$ tiene dimensión 0, luego, dado cualquier punto cerrado $P \in X$, existe un entorno afín U de P tal que $D \cap E \cap U \subset \{P\}$.

Pongamos que $P \in D \cap E$ y que $U = \mathrm{Esp}\, A$, de modo que P se corresponde con un ideal maximal $\mathfrak{m}$ de A. Entonces $I = \mathcal{O}_X(D^{-1})(U) + \mathcal{O}_X(E^{-1})(U)$ es un ideal de A tal que $V(I) = \{\mathfrak{m}\}$, lo que a su vez implica que el único ideal primo de $A_\mathfrak{m}$ que contiene a $I_\mathfrak{m}$ es el ideal maximal, luego $A_\mathfrak{m}/I_\mathfrak{m}$ tiene dimensión cero (pero no es nulo). Si $P \notin D \cap E$, entonces $A_\mathfrak{m}/I_\mathfrak{m} = 0$.

Así pues, hemos probado que, para todo punto cerrado $P \in X$, se cumple que

$$\mathcal{O}_{X,P}/(\mathcal{O}_X(D^{-1})_P + \mathcal{O}_X(E^{-1})_P)$$

es un anillo noetheriano de dimensión 0, y es nulo si y sólo si $P \notin D \cap E$.

Por el teorema [AC 4.38] sabemos que los anillos noetherianos de dimensión 0 tienen longitud finita, lo cual justifica la definición siguiente:

Definición 6.1 Sea X un esquema noetheriano regular y conexo de dimensión 2 y sean D, $E \in \mathrm{Div}(X)$ dos divisores enteros primos entre sí. Para cada punto cerrado $P \in X$ definimos el *número de intersección* de D y E en P como

$$i_P(D,E) = l_{\mathcal{O}_{X,P}}\big(\mathcal{O}_{X,P}/(\mathcal{O}_X(D^{-1})_P + \mathcal{O}_X(E^{-1})_P)\big).$$

Es obvio que $i_P(D,E) = i_P(E,D)$, y hemos visto que $i_P(D,E) = 0$ si y sólo si $P \notin D \cap E$.

Por el teorema 4.3 sabemos que los puntos asociados de E coinciden con sus puntos cuasigenéricos, luego el teorema [E 8.32] nos garantiza que está definido el divisor $D|_E = i^*(D) \in \mathrm{Div}_c(E)$. Vamos a probar que, si $P \in E$ es un punto cerrado, entonces

$$i_P(D,E) = v_P(D|_E).$$

En efecto, como todas las definiciones son locales, no perdemos generalidad si suponemos que $X = \mathrm{Esp}\, A$ es afín y que D y E están definidos por elementos a, $b \in A$, respectivamente. Así, $\mathcal{O}_X(D^{-1}) = (a)$ y $\mathcal{O}_X(E^{-1}) = (b)$.

Considerando E como subesquema cerrado de X, es $E = \mathrm{Esp}(A/(b))$. El divisor $i^*(D)$ está definido por $[a] \in A/(b)$, luego, de acuerdo con la definición [E 8.26], tenemos que

$$v_P(D|_E) = l_{(A/(b))_P}((A/(b))_P/([a])) = l_{A_P}(A_P/(a,b)) = i_P(D,E).$$

De esta relación se deduce que el número de intersección es bilineal, es decir, que

$$i_P(DF,E) = i_P(D,E) + i_P(F,E),$$

donde los tres divisores tienen sus soportes sin componentes irreducibles comunes.

Si $D \in \mathrm{Div}(X)$ es un divisor cualquiera, podemos expresarlo en la forma $D = D_0/D_\infty$, donde los divisores D_0 y D_∞ no tienen divisores primos comunes y el soporte de D es la unión de sus soportes. Si $E \in \mathrm{Div}(X)$ es otro divisor primo con D, podemos definir

$$i_P(D,E) = i_P(D_0,E_0) - i_P(D_\infty,E_0) - i_P(D_0,E_\infty) + i_P(D_\infty,E_\infty).$$

Es inmediato que esta extensión de i_P es también bilineal y simétrica. Ya sabemos que $i_P(D,E) = 0$ significa que $P \notin D \cap E$. El teorema siguiente nos da el significado de $i_P(D,E) = 1$ para el caso de divisores primos:

Teorema 6.2 *Sea X un esquema noetheriano regular y conexo de dimensión 2, sean D y E dos divisores primos distintos y $P \in D \cap E$. Las afirmaciones siguientes son equivalentes:*

a) $i_P(D,E) = 1$.

b) $\mathcal{O}_X(D^{-1})_P + \mathcal{O}_X(E^{-1})_P = \mathfrak{m}_P$.

c) D y E, como esquemas, son regulares en P y $T_PX = T_PD \oplus T_PE$.

DEMOSTRACIÓN: La condición $P \in D \cap E$ implica que

$$\mathcal{O}_X(D^{-1})_P + \mathcal{O}_X(E^{-1})_P \subset \mathfrak{m}_P.$$

Por definición, a) equivale a que el cociente $\mathcal{O}_{X,P}/(\mathcal{O}_X(D^{-1})_P + \mathcal{O}_X(E^{-1})_P)$ tenga longitud 1, y esto equivale claramente a que la inclusión anterior sea una igualdad, es decir, a que se cumpla b).

Respecto a c), observemos ante todo que la inmersión cerrada $D \longrightarrow X$ induce un monomorfismo de $k(P)$-espacios vectoriales $T_P D \longrightarrow T_P X$, que nos permite considerar a $T_P D$ (y análogamente a $T_P E$) como subespacio de $T_P X$.

Pongamos que $\mathcal{O}_X(D^{-1})_P = f\mathcal{O}_{X,P}$, $\mathcal{O}_X(E^{-1})_P = g\mathcal{O}_{X,P}$. En estos términos, b) equivale a que $\mathfrak{m}_P = (f, g)$, de donde se sigue que el ideal maximal de $\mathcal{O}_{D,P}$ está generado por g, luego $\dim_{k(P)} T_P D \leq 1$, luego P es regular en D, y lo mismo sucede con E.

Sean $d_P f$, $d_P g$ las clases de f y g en $\mathfrak{m}_P/\mathfrak{m}_P^2 = T_P X^*$. Suponiendo b) y teniendo en cuenta que X es regular, resulta que $d_P f$ y $d_P g$ son una base del espacio cotangente de X en P. Es claro que $T_P D$ se identifica con el subespacio de $T_P X$ anulado por $d_P f$ y $T_P E$ se identifica con el subespacio anulado por $d_P g$. Esto implica que $T_P X = T_P D + T_P E$ y, como los dos sumandos tienen dimensión 1, la suma ha de ser directa. Así pues, tenemos c).

Recíprocamente, si suponemos c), según el teorema [AC 5.19] podemos escoger f de modo que, como antes, $\mathcal{O}_X(D^{-1})_P = f\mathcal{O}_{X,P}$ y además $\mathfrak{m}_P = (f, f')$, para cierto f'. Al igual que antes, vemos que $T_P D$ se identifica con el subespacio de $T_P X$ anulado por $d_P f$ y, análogamente, podemos tomar g de modo que $T_P E$ sea el subespacio anulado por $d_P g$. La hipótesis sobre la suma directa implica entonces que $T_P X^* = \langle d_P f, d_P g\rangle$, es decir, que $\mathfrak{m}_P/\mathfrak{m}_P^2$ está generado por las clases de f y g. El teorema [AC 4.52] implica entonces que $\mathfrak{m}_P = (f, g)$, y esto es la propiedad b). ∎

Definición 6.3 Cuando dos divisores primos D y E cumplan las condiciones del teorema anterior diremos que *se cortan transversalmente* en P. Si D y E son regulares en P y cumplen $i_P(D, E) \geq 2$, entonces se dice que son *tangentes* en P. (Si no exigimos la regularidad, por el propio teorema resultaría que un divisor singular en un punto dado sería tangente a cualquier otro que pasara por dicho punto.)

Ejemplo Consideremos $X = \mathrm{P}^2_k$, de modo que los divisores primos en X son simplemente las curvas proyectivas planas íntegras definidas sobre k. Consideremos la circunferencia C dada por la ecuación $X^2 + Y^2 - Z^2 = 0$ y las rectas R_0 y R_1 dadas por $X = 0$ y $X = Z$ respectivamente. Las intersecciones $C \cap R_i$ están todas en el plano afín $A^2_k = V(Z)$, por lo que, para calcular los números de intersección, podemos deshomogeneizar respecto de Z, con lo que las ecuaciones pasan a ser:

$$C:\ X^2 + Y^2 = 1, \quad R_1:\ X = 0, \quad R_2:\ X = 1.$$

Observamos que $C \cap R_1$ consta de los puntos $(0, \pm 1)$ que, en términos de ideales de $k[X,Y]$, son $P_1 = (X, Y-1)$ y $P_2 = (X, Y+1)$. Como divisor de Cartier, C está definido en A^2_k por la función $X^2 + Y^2 - 1 \in \mathcal{O}_{\mathrm{P}^2_k}(A^2_k)$ y $C|_{R_1}$ es el divisor de Cartier de R_1 que, sobre su parte finita, está definida por la imagen de esta función por el homomorfismo

$$k[X,Y] \longrightarrow k[X,Y]/(X) \cong k[Y],$$

que define la inmersión cerrada $i : R_1 \cap A^2_k \longrightarrow A^2_k$. En suma, $C|_{R_1}$ es el divisor de Cartier en $R_1 = A^1_k$ definido por la función $Y^2 - 1$. Por otra parte, como punto de R_1, el punto P_1 es $(Y-1)$. Así pues,

$$i_{P_1}(C, R_1) = v_{P_1}(Y^2 - 1) = v_{P_1}(Y+1) + v_{P_1}(Y-1) = 1.$$

Aquí hemos usado el teorema 4.4, en virtud del cual v_{P_1} es la valoración asociada al ideal maximal $\mathfrak{m} = (Y-1)$ en el anillo de valoración discreta $\mathcal{O}_{R_1,P_1}$. Claramente, tenemos también que $i_{P_2}(C, R_1) = 1$, luego la recta y la circunferencia se cortan transversalmente en sus dos puntos de intersección.

Alternativamente, usando la caracterización b) del teorema 6.2, bastaba observar que

$$\mathcal{O}_X(C^{-1})_{P_1} + \mathcal{O}_X(R_1^{-1})_{P_1} = (X^2 + Y^2 - 1, X) = (Y^2 - 1, X) = (Y - 1, X)$$

es el ideal maximal de $\mathcal{O}_{X,P_1}$. (Hemos usado que $Y+1$ es una unidad en este anillo, por lo que podemos cambiar $Y^2 + 1$ por $Y - 1$.)

Por otra parte, $C \cap R_2$ consta de un único punto $P = (X-1, Y)$. Ahora, la imagen de la ecuación de C por el homomorfismo

$$k[X,Y] \longrightarrow k[X,Y]/(X-1) \cong k[Y]$$

es Y^2 y, como punto de $R_2 = A^1_k$, el punto P es (Y). Así pues,

$$i_P(C, R_2) = v_P(Y^2) = 2,$$

lo que significa que C y R_2 son tangentes en P. ∎

Ejemplo En la sección 5.4, partiendo de la superficie $X/\mathbb{Z}_2$ definida por la curva de Selmer, hemos encontrado una superficie regular $\mathcal{X}/\mathbb{Z}_2$ cuya fibra cerrada consta de 5 componentes irreducibles. Vamos a ver que todas ellas se cortan transversalmente. Manteniendo la notación empleada allí, tenemos que los puntos de intersección de Γ_3 con Γ_4 y Γ_5 están contenidos en el abierto afín U_{21}, cuya ecuación es

$$x'^3(z'+1)^2(z'^2 + z' + 1)^2 = 2,$$

de modo que $\Gamma_3 = (2, x')$, $\Gamma_4 = (2, z'+1)$, $\Gamma_5 = (2, z'^2 + z' + 1)$. Basta aplicar el teorema 6.2 b), pues, por ejemplo, $P = \Gamma_3 \cap \Gamma_4 = (x', z'+1)$ (donde comprobamos que el ideal es primo porque el cociente es un cuerpo), y el ideal

$$\mathcal{O}_{\mathcal{X}}(\Gamma_3^{-1}) + \mathcal{O}_{\mathcal{X}}(\Gamma_4^{-1}) = (x', z'+1)$$

es trivialmente el ideal maximal de $\mathcal{O}_{X,P}$. Esto prueba que $i_P(\Gamma_3 \cap \Gamma_4) = 1$, e igualmente se razona que $i_{P'}(\Gamma_3 \cap \Gamma_5) = 1$, donde P' es el punto de intersección correspondiente. Razonando en el abierto U_{22} se concluye igualmente que los cortes de $\Gamma_1 \cap \Gamma_2$ y $\Gamma_4 \cap \Gamma_5$ son transversales.

El lector que haya calculado la desingularización de $X/\mathbb{Z}_3$ puede comprobar con igual facilidad que las nueve componentes irreducibles de la superficie regular obtenida se cortan transversalmente. ∎

Ahora vamos a definir el número de intersección global de dos divisores E y F de una superficie fibrada regular X/S que "cuente" el número de puntos en que se cortan uno y otro. Ponemos "contar" entre comillas porque queremos contar cada punto de intersección "algebraicamente", es decir, tantas veces como indica la "multiplicidad" u "orden de contacto" dada por el número de intersección local $i_P(E,F)$ que ya hemos definido. De este modo, los puntos donde los divisores son tangentes (y donde alguno de ellos es singular) se cuentan dos o más veces.

Según esto, el número de intersección $i(E,F)$ debería ser simplemente la suma

$$i(E,F) = \sum_P i_P(E,F),$$

donde P recorre los puntos de $E \cap F$ (o, equivalentemente, los puntos de la superficie X/S), pero en realidad hay otro motivo por el que una intersección en un punto "debería" contarse varias veces y que no está recogido en la definición del número de intersección local:

Ejemplo Tomemos $X = \mathrm{P}^2_{\mathbb{R}}$ y consideremos los divisores primos E y F determinados respectivamente por las ecuaciones

$$X^2 + Y^2 = 0, \qquad X = Z.$$

Vemos que $E \cap F$ consta de un único punto P, que está contenido en el abierto afín $A^2_{\mathbb{R}} = V(Z)$, donde se identifica con el ideal

$$P = (X^2 + Y^2, X - 1) = (X - 1, Y^2 + 1).$$

Por 6.2 b) es inmediato que $i_P(E,F) = 1$, pero E es una cónica singular que, tras la extensión de constantes $\mathbb{C}/\mathbb{R}$, se descompone en dos rectas de ecuaciones

$$X + iY = 0, \qquad X - iY = 0,$$

y F corta a estas rectas en $P_1 = (X - 1, Y + i)$, $P_2 = (X - 1, Y - i)$, que son los puntos de $A^1_{\mathbb{C}}$ que se identifican con P en $A^2_{\mathbb{R}}$. Así pues, resulta razonable considerar que la intersección de E y F en P es doble, no porque E y F sean tangentes en P, sino porque el punto P representa en $A^2_{\mathbb{R}}$ a un par de puntos conjugados de $A^2_{\mathbb{C}}$. El valor concreto 2 es $\operatorname{grad}_{\mathbb{R}} P = |k(P) : \mathbb{R}| = 2$. ∎

En el caso geométrico, es decir, cuando la superficie X/S con la que trabajamos es una superficie sobre un cuerpo $S = \operatorname{Esp} k$, esto nos llevaría a definir el

número de intersección global de dos divisores E y F como

$$i(E,F) = \sum_P i_P(E,F)\,\mathrm{grad}_k\, P.$$

Sin embargo, en el caso aritmético, es decir, cuando $\dim S = 1$, no tenemos un mismo cuerpo base k, sino que, para cada punto $P \in X_s$ hemos de considerar su grado sobre el cuerpo $k(s)$ asociado a su fibra. Para que esta definición "funcione correctamente" nos vemos obligados a restringir la definición del número de intersección global de dos divisores al caso en que al menos uno de ellos es vertical.

Consideremos, pues, una superficie fibrada regular arbitraria X/S. Si $s \in S$ es un punto cerrado, llamaremos $\mathrm{Div}_s(X)$ al conjunto de los divisores de X cuyo soporte está contenido en la fibra X_s. Obviamente se trata de un subgrupo de $\mathrm{Div}(X)$. Si $\dim S = 0$ y s es el único punto de S, entonces $X_s = X$ y $\mathrm{Div}_s(X) = \mathrm{Div}(X)$. Si $\dim S = 1$, entonces $\mathrm{Div}_s(X)$ es el $\mathbb{Z}$-módulo libre generado por las componentes irreducibles de la curva X_s.

En este segundo caso, si D es un divisor entero no trivial que divide al divisor X_s, esto significa que existe otro divisor entero E tal que $X_s = DE$, por lo que $\mathcal{O}_X(X_s^{-1}) = \mathcal{O}_X(D^{-1})\mathcal{O}_X(E^{-1}) \subset \mathcal{O}_X(D^{-1})$, luego existe una inmersión cerrada $i : D \longrightarrow X_s$, luego podemos ver a D como curva proyectiva sobre $k(s)$.

En el caso geométrico entenderemos la condición $D \mid X_s$ como trivial. Puesto que X es una superficie proyectiva sobre $k = k(s)$, también tenemos trivialmente que D es una curva proyectiva sobre k.

Teorema 6.4 *Sea X/S una superficie fibrada regular y sea $s \in S$ un punto cerrado. Entonces existe una única aplicación bilineal de $\mathbb{Z}$-módulos*

$$i_s : \mathrm{Div}(X) \times \mathrm{Div}_s(X) \longrightarrow \mathbb{Z}$$

que cumple las propiedades siguientes:

a) Si $D \in \mathrm{Div}(X)$ y $E \in \mathrm{Div}_s(X)$ no tienen primos en común, entonces

$$i_s(D,E) = \sum_P i_P(D,E)\ \mathrm{grad}_{k(s)}\, P,$$

donde P recorre los puntos cerrados de X_s.

b) La restricción de i_s a $\mathrm{Div}_s(X) \times \mathrm{Div}_s(X)$ es simétrica.

c) Si D y D' son linealmente equivalentes, entonces $i_s(D,E) = i_s(D',E)$.

d) Si $E \mid X_s$ es un divisor entero no trivial, entonces

$$i_s(D,E) = \mathrm{grad}_{k(s)}\, \mathcal{O}_X(D)|_E.$$

DEMOSTRACIÓN: La unicidad se deduce de la bilinealidad y de la propiedad d), ya que si $E \in \mathrm{Div}_s(X)$, podemos expresarlo de forma única como $E = \Gamma_1^{n_1} \cdots \Gamma_r^{n_r}$, donde los Γ_i son los divisores primos de X_s en el caso aritmético o divisores primos arbitrarios de X en el caso geométrico, y $n_i \in \mathbb{Z}$. En cualquier caso son curvas proyectivas (íntegras) sobre $k(s)$. La propiedad d) exige entonces que

$$i_s(D, E) = \sum_i n_i \operatorname{grad}_{k(s)} \mathcal{O}_X(D)|_{\Gamma_i}.$$

Vamos a demostrar que, tomando esta fórmula como definición, se cumplen las propiedades del enunciado. La bilinealidad es obvia.

a) La bilinealidad de i_s e i_P permite reducir la comprobación al caso en que D y E son divisores primos distintos. En tal caso está definida la imagen inversa $D|_E$, de modo que $\mathcal{O}_X(D)|_E = \mathcal{O}_E(D|_E)$, luego

$$i_s(D, E) = \operatorname{grad}_{k(s)} D|_E = \sum_P v_P(D|_E) \operatorname{grad}_{k(s)} P = \sum_P i_P(D, E) \operatorname{grad}_{k(s)} P.$$

b) Si $D = \Gamma_1^{m_1} \cdots \Gamma_r^{m_r}$, entonces

$$i_s(D, E) = \sum_{i,j} m_i n_j i_s(\Gamma_i, \Gamma_j),$$

y se cumple que $i_s(\Gamma_i, \Gamma_j) = i_s(\Gamma_j, \Gamma_i)$, trivialmente si $i = j$ y por a) si $i \neq j$.

c) Por la linealidad, podemos suponer nuevamente que E es primo. Si los divisores D y D' son linealmente equivalentes, entonces $\mathcal{O}_X(D) \cong \mathcal{O}_X(D')$, luego $\mathcal{O}_X(D)|_E \cong \mathcal{O}_X(D')|_E$ y ambos haces tienen el mismo grado.

d) Por el teorema 4.11 tenemos que

$$\operatorname{grad}_{k(s)} \mathcal{O}_X(D)|_E = \sum_i l(\mathcal{O}_{E,\xi_i}) \operatorname{grad}_{k(s)} \mathcal{O}_X(D)|_{\Gamma_i},$$

donde ξ_i es el punto genérico de Γ_i. Ahora bien, por la observación tras dicho teorema, tenemos que $l(\mathcal{O}_{E,\xi_i}) = v_{\Gamma_i}(E) = n_i$ y, por consiguiente, el miembro derecho es $i_s(D, E)$. ∎

Observaciones La definición de $i_s(E, F)$ que proporciona el teorema anterior es mucho más general que la fórmula explícita del apartado a), la cual sólo es válida cuando los divisores no tienen primos comunes. En particular, si $P \in \mathrm{Div}_s(X)$ es un divisor primo vertical, tenemos definido el *número de autointersección* $i_s(P, P)$, que no puede interpretarse en términos de intersecciones de divisores.

En la demostración hemos visto que $i_s(E, F)$ está completamente determinado por las propiedades a) y d). Por otra parte, puede probarse que todo divisor D es linealmente equivalente a otro divisor primo con cualquier divisor E prefijado, por lo que $D \cdot E$ también está completamente determinado por las propiedades a) y c).

Lo que explica por qué conviene "contar" los puntos de intersección con las multiplicidades que les hemos asignado es que así se consigue que el número de intersección global tenga las propiedades algebraicas que afirma el teorema, en particular que sea bilineal y compatible con la equivalencia de divisores. ∎

En el caso geométrico tenemos definida una única forma bilineal simétrica $\mathrm{Div}(X) \times \mathrm{Div}(X) \longrightarrow \mathbb{Z}$, que induce una forma bilineal simétrica

$$\mathrm{Pic}(X) \times \mathrm{Pic}(X) \longrightarrow \mathbb{Z}.$$

En lugar de $i_s(D, E)$ es más habitual la notación $D \cdot E$, y este número se llama *número de intersección* de los dos divisores.

Si los divisores son primos entre sí, el número de intersección puede interpretarse como el número de puntos en $D \cap E$, entendiendo, como ya hemos explicado antes del teorema, que cada punto P representa en realidad a $\operatorname{grad} P$ puntos y que a la intersección hay que asignarle una multiplicidad $i_P(D, E)$. En particular, si D y E son divisores primos regulares como esquemas, que se cortan únicamente en puntos racionales y lo hacen transversalmente, entonces $D \cdot E$ es literalmente el número de puntos de $D \cap E$.

Para $X = \mathrm{P}^2_k$ los números de intersección son muy fáciles de calcular. Basta tener en cuenta que $\operatorname{grad} : \mathrm{Pic}(\mathrm{P}^2_k) \longrightarrow \mathbb{Z}$ es un isomorfismo, por lo que si D y E son divisores de grados m y n respectivamente y H_1, H_2 son dos hiperplanos distintos, se cumple que D y E son linealmente equivalentes a H_1^m y H_2^n respectivamente, luego

$$D \cdot E = H_1^m \cdot H_2^n = mn(H_1 \cdot H_2) = mn,$$

ya que H_1 y H_2 se cortan transversalmente en un único punto racional. La relación

$$D \cdot E = (\operatorname{grad} D)(\operatorname{grad} E)$$

no es sino una forma del teorema de Bezout.

En el caso aritmético, si E es un divisor vertical, es decir, un divisor cuyos divisores primos sean todos verticales, podemos definir $D \cdot E$ como el divisor de Weil en S dado por

$$v_s(D \cdot E) = i_s(D, E_s),$$

donde E_s representa al divisor compuesto por los divisores primos de E con soporte en X_s. En otras palabras, no tenemos definido un único número de intersección, sino un número de intersección para cada fibra.

Vamos a probar algunos resultados fundamentales sobre los números de intersección en el caso aritmético, para lo cual necesitamos primeramente un hecho técnico, a saber, la posibilidad de reducir el cálculo al caso de superficies aritméticas sobre anillos de valoración discreta.

Para ello observamos que si X/S es una superficie aritmética y $s \in S$ es un punto cerrado, entonces $X' = X \times_X \operatorname{Esp} \mathcal{O}_{S,s}$ es también una superficie

aritmética (sobre $\mathcal{O}_{S,s}$). Es una superficie fibrada por el teorema 5.5, y es regular porque si $x \in X'$ pertenece a la fibra cerrada X'_s, entonces $\mathcal{O}_{X',x} \cong \mathcal{O}_{X,x}$ (teorema [E 3.47]), luego x es regular en X', y si x pertenece a la fibra genérica X'_η, entonces x es regular en $X'_\eta \cong C/K$ y X'_η es abierta en X', luego x también es regular en X'. El resultado que necesitamos es el siguiente:

Teorema 6.5 *Sea X/S una superficie aritmética, sea $s \in S$ un punto cerrado, sea $S' = \operatorname{Esp} \mathcal{O}_{S,s}$, sea $X' = X \times_S S'$, sea $p : X' \longrightarrow X$ la proyección natural y sean $D \in \operatorname{Div}(X)$, $E \in \operatorname{Div}_s(X)$. Entonces*

$$D \cdot E = p^* D \cdot p^* E.$$

DEMOSTRACIÓN: Podemos suponer que E es primo. Tenemos el diagrama conmutativo

$$\begin{array}{ccccc} X'_s & \longrightarrow & X' & \longrightarrow & S' \\ \downarrow & & \downarrow p & & \downarrow \\ X_s & \longrightarrow & X & \longrightarrow & S \end{array}$$

donde el homomorfismo entre las fibras es un isomorfismo. El hecho de que E sea una componente irreducible de X_s se traduce en que, si $\mathcal{I}$ es el haz de ideales de $\mathcal{O}_X$ asociado a X_s, entonces $\mathcal{I} \subset \mathcal{O}_X(E^{-1})$. Por otra parte, el haz $\mathcal{I}'$ de ideales de $\mathcal{O}_{X'}$ asociado a X'_s es $p^*\mathcal{I} \subset p^*\mathcal{O}_X(E^{-1}) = \mathcal{O}_{X'}(p^*E^{-1})$. En efecto, sea $V = \operatorname{Esp} A$ un entorno afín de s (de modo que s se corresponda con un ideal maximal $\mathfrak{p}$ de A), sea $U = \operatorname{Esp} B$ un abierto afín de X contenido en la antiimagen de V, de modo que tenemos la sucesión exacta

$$0 \longrightarrow \mathcal{I}(U) \longrightarrow B \longrightarrow B \otimes_A k(\mathfrak{p}) \longrightarrow 0.$$

De ella obtenemos la sucesión exacta

$$0 \longrightarrow \mathcal{I}(U)_\mathfrak{p} \longrightarrow B_\mathfrak{p} \longrightarrow B_\mathfrak{p} \otimes_A k(\mathfrak{p}) \longrightarrow 0.$$

Es fácil ver que el último anillo es igual a $B_\mathfrak{p} \otimes_{A_\mathfrak{p}} k(\mathfrak{p})$, así como que, llamando $U' = p^{-1}[U] = U \times_V \operatorname{Esp} A_\mathfrak{p}$, se cumple que

$$(p^*\mathcal{I})(U') = \mathcal{I}(U) \otimes_B B \otimes_A A_\mathfrak{p} = \mathcal{I}(U)_\mathfrak{p}.$$

Por consiguiente, tenemos la sucesión exacta

$$0 \longrightarrow (p^*\mathcal{I})(U') \longrightarrow \mathcal{O}_{X'}(U') \longrightarrow \mathcal{O}_{X'_s}(U' \cap X'_s) \longrightarrow 0,$$

de la que se deduce que $\mathcal{I}'(U') = (p^*\mathcal{I})(U')$.

Podemos cubrir X' por abiertos afines U' que sean de la forma indicada o bien que sean de la forma $U' = p^{-1}[U]$ con $U \cap X_s = \varnothing$, y en este caso la igualdad anterior es trivial. Esto prueba que $\mathcal{I}' = p^*\mathcal{I}$, como habíamos afirmado. Esto nos da inmersiones cerradas

$$p^*E \longrightarrow X'_s \longrightarrow X'.$$

Ahora es fácil ver que el isomorfismo $X'_s \longrightarrow X_s$ hace corresponder a p^*E con E como esquemas. En efecto, si, en un abierto afín $U \subset X$, el anillo $\mathcal{O}_X(E^{-1})(U)$ está generado por un elemento $b \in \mathcal{O}_X(U)$, entonces $\mathcal{O}_{X_s}(E^{-1})(X_s \cap U)$ está generado por la clase de b módulo $\mathcal{I}(U)$. Por otra parte, si $U' = p^{-1}[U]$, tenemos que $\mathcal{O}_{X'}(p^*E^{-1})(U')$ está generado por la imagen de b en $\mathcal{O}_{X'}(U')$, luego $\mathcal{O}_{X'_s}(p^*E^{-1})(X'_s \cap U)$ está generado por la clase de esta imagen módulo $\mathcal{I}'(U')$. Esto significa que el isomorfismo $\mathcal{O}_{X_s}(X_s \cap U) \cong \mathcal{O}_{X'_s}(X'_s \cap U')$ hace corresponder $\mathcal{O}_{X_s}(E^{-1})(X_s \cap U)$ con $\mathcal{O}_{X'_s}(p^*E^{-1})(X'_s \cap U)$, luego, vistos como subesquemas de X'_s y X_s, respectivamente, se cumple que $p^*E \cong E$. Más aún, tenemos un diagrama conmutativo

$$\begin{array}{ccc} p^*E & \xrightarrow{j} & X' \\ {\scriptstyle r}\downarrow & & \downarrow{\scriptstyle p} \\ E & \xrightarrow[i]{} & X \end{array}$$

donde r es un isomorfismo. Ahora basta observar que

$$D \cdot E = \operatorname{grad}_{k(s)} i^*D = \operatorname{grad}_{k(s)} r^*i^*D = \operatorname{grad}_{k(s)}(p^*D)|_{p^*E} = p^*D \cdot p^*E.$$

■

Observemos que si, en las condiciones del teorema anterior, llamamos también $s \in S'$ al único punto cerrado y $\rho : S' \longrightarrow S$ es el homomorfismo natural, se cumple que $\rho^*s = s$, vistos como divisores de Cartier. En efecto, si $\{(U_i, f_i)\}_i$ define a s como divisor de Weil de S y $U_i = \operatorname{Esp} A$ contiene a s (al que podemos identificar con un primo $\mathfrak{p}$ de A), entonces A es un dominio de Dedekind y $f_i \in A$ cumple que $v_\mathfrak{p}(f_i) = 1$, luego f_i, como elemento de $A_\mathfrak{p}$, cumple lo mismo. Dado que $A_\mathfrak{p}$ no contiene más primos, concluimos que ρ^*s está definido por el par (S', f_i), el cual define al divisor de Cartier correspondiente al divisor de Weil s.

Puesto que $X_s = \pi^*s$, ahora podemos concluir (siempre en las condiciones del teorema anterior) que $X'_s = p^*X_s$.

Con esto podemos probar un resultado fundamental:

Teorema 6.6 *Sea X/S una superficie aritmética y $s \in S$ un punto cerrado. Si $E \in \operatorname{Div}_s(X)$, entonces $E \cdot X_s = 0$.*

Demostración: Por el teorema anterior y la observación que acabamos de hacer, no perdemos generalidad si suponemos que S es local, es decir, es el espectro de un dominio de Dedekind local, que será un dominio de ideales principales, luego su grupo de clases es trivial y el divisor s es principal. Esto implica a su vez que $X_s = \pi^*s$ también es principal. Como i_s induce una forma bilineal en $\operatorname{Pic}_s(X) \times \operatorname{Pic}_s(X)$ y X_s es trivial en el grupo de clases, la conclusión es inmediata. ■

Como primera aplicación observamos que si $\Gamma_1, \ldots, \Gamma_n$ son los divisores primos (las componentes irreducibles) de la fibra X_s, entonces la bilinealidad nos reduce el cálculo de cualquier producto $D \cdot E$, con D, $E \in \operatorname{Div}_s(X)$, al cálculo

de los productos $\Gamma_i \cdot \Gamma_j$ para $i \neq j$, que pueden calcularse por la propiedad a) del teorema 6.4, y a las autointersecciones $\Gamma_i^2 = \Gamma_i \cdot \Gamma_i$. El teorema anterior nos proporciona una fórmula sencilla para calcular éstas a partir de aquéllos:

Teorema 6.7 *Sea X/S una superficie aritmética, sea $s \in S$ un punto cerrado y sea $X_s = \Gamma_1^{d_1} \cdots \Gamma_r^{d_r}$ el divisor de Weil asociado a la fibra. Entonces*

$$\Gamma_i^2 = -\frac{1}{d_i} \sum_{j \neq i} d_j \, \Gamma_j \cdot \Gamma_i.$$

DEMOSTRACIÓN: Basta desarrollar linealmente la relación $\Gamma_i \cdot X_s = 0$. ∎

Ejemplo Consideremos la desingularización $\mathcal{X}/\mathbb{Z}_5$ calculada en el ejemplo de la página 144. Su fibra cerrada es $\mathcal{X}_5 = \Gamma_1 \cdot \Gamma_2 \cdot \Gamma_3$, donde las componentes se cortan transversalmente en un único punto racional. Esto se traduce en que $\Gamma_i \cdot \Gamma_j = 1$ cuando $i \neq j$. Ahora podemos calcular

$$\Gamma_1^2 = -\Gamma_2 \cdot \Gamma_1 - \Gamma_3 \cdot \Gamma_1 = -2,$$

y lo mismo vale para los demás índices, luego la matriz $(\Gamma_i \cdot \Gamma_j)_{i,j}$ que determina las intersecciones de los divisores verticales resulta ser

$$\begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix}.$$

∎

Ejemplo Consideremos ahora la superficie fibrada $\mathcal{X}/\mathbb{Z}_2$ que hemos obtenido en la sección 5.4 al desingularizar la ecuación de Selmer. La fibra cerrada es $\mathcal{X}_2 = \Gamma_1 \cdot \Gamma_2 \cdot \Gamma_3^3 \cdot \Gamma_4^2 \cdot \Gamma_5^2$, y todas las componentes se cortan transversalmente en un punto racional, excepto Γ_2 y Γ_5, que se cortan entre sí y cortan a Γ_3 en puntos de grado 2. Es fácil calcular entonces la matriz de intersecciones:

$$\begin{pmatrix} -2 & 0 & 0 & 1 & 0 \\ 0 & -4 & 0 & 0 & 2 \\ 0 & 0 & -2 & 1 & 2 \\ 1 & 0 & 1 & -2 & 0 \\ 0 & 2 & 2 & 0 & -4 \end{pmatrix}$$

Por ejemplo,

$$\Gamma_5^2 = -\frac{1}{2}(\Gamma_2 \cdot \Gamma_5 + 3\Gamma_3 \cdot \Gamma_5) = -4.$$

El lector puede calcular como ejercicio la matriz correspondiente a la desingularización $\mathcal{X}/\mathbb{Z}_3$. ∎

Observemos ahora que $\mathrm{Div}_s(X)_{\mathbb{R}} = \mathrm{Div}_s(X) \otimes_{\mathbb{Z}} \mathbb{R}$ es un espacio vectorial de dimensión finita, que tiene por base a las componentes irreducibles de X_s. Es obvio que i_s determina una forma bilineal simétrica $\langle\ ,\ \rangle_s$ sobre este espacio.

Teorema 6.8 *Sea X/S una superficie aritmética y $s \in S$ un punto cerrado. La forma bilineal $\langle\ ,\ \rangle_s$ en $\mathrm{Div}_s(X)_{\mathbb{R}}$ es semidefinida negativa, es decir, cumple que $\langle v, v\rangle_s \leq 0$ para todo $v \in \mathrm{Div}_s(X)_{\mathbb{R}}$. Si la fibra X_s es conexa, entonces $\langle v, v\rangle_s = 0$ si y sólo si $v \in \langle X_s\rangle_{\mathbb{R}}$.*

Demostración: Sea $X_s = \Gamma_1^{d_1} \cdots \Gamma_r^{d_r}$. Podemos suponer que $r \geq 0$, ya que, de lo contrario, la forma bilineal es nula y el teorema es trivial. Llamemos $b_{ij} = d_i d_j \Gamma_i \cdot \Gamma_j$. Notemos que, por 6.4 a), se cumple que $b_{ij} \geq 0$ si $i \neq j$. Por otra parte,

$$\sum_j b_{ij} = X_s \cdot \Gamma_i^{d_i} = 0.$$

Tomemos $v = \sum_i \Gamma_i^{x_i} \in \mathrm{Div}_s(X)_{\mathbb{R}}$ y sea $y_i = x_i/d_i$. Entonces

$$\langle v, v\rangle_s = \sum_{i,j} b_{ij}\, y_i y_j = -\sum_{i<j} b_{ij}(y_i - y_j)^2 \leq 0.$$

Además, $\langle v, v\rangle_s = 0$ si y sólo si $y_i = y_j$ cuando $b_{ij} \neq 0$, es decir, cuando $\Gamma_i \cap \Gamma_j \neq \varnothing$. Si X_s es conexa, esto equivale a que todos los y_i sean iguales, es decir, a que v sea múltiplo de X_s. ∎

Los resultados que hemos probado hasta aquí han tratado sobre la intersección de divisores verticales. Ahora vamos a ocuparnos de la intersección de un divisor horizontal con otro vertical. El análogo al teorema 6.6 es el siguiente:

Teorema 6.9 *Sea X/S una superficie aritmética, sea $s \in S$ un punto cerrado, sea D un divisor primo horizontal y sea ξ su punto genérico. Entonces*

$$D \cdot X_s = |k(\xi) : K(S)|.$$

Demostración: Como D es primo, la estructura de esquema en D como subesquema de X es la estructura de subesquema cerrado reducido. La inclusión induce un epimorfismo $\mathcal{O}_{X,\xi} \longrightarrow \mathcal{O}_{D,\xi} = K(D)$, que a su vez induce un epimorfismo $k(\xi) \longrightarrow K(D)$ que, obviamente, ha de ser un isomorfismo de cuerpos.

Por otra parte, podemos considerar la restricción $h : D \longrightarrow S$ del homomorfismo estructural, que es suprayectiva porque D es horizontal. El diagrama conmutativo

$$\begin{array}{ccc} D & \xrightarrow{i} & X \\ & \searrow^{h} & \downarrow{\scriptstyle \pi} \\ & & S \end{array}$$

muestra que el isomorfismo $k(\xi) \cong K(D)$ es un $K(S)$-isomorfismo, luego en el miembro derecho de la fórmula del enunciado podemos sustituir $k(\xi)$ por $K(D)$. Claramente:

$$D \cdot X_s = \sum_P i_P(D, X_s)\ \mathrm{grad}_{k(s)}\, P = \sum_P v_P(X_s|_D)\, |k(P) : k(s)| = v_s(h_*(X_s|_D)),$$

(cf. [E 8.41].) Ahora observamos que $X_s|_D = i^*\pi^* s = h^* s$, luego [E 8.42] nos da que

$$D \cdot X_s = v_s(h_* h^* s) = |K(D) : K(S)|,$$

como queríamos probar. ∎

Estudiamos ahora las autointersecciones de los divisores horizontales. El problema para calcular D^2 mediante el teorema 6.4 d) es calcular el haz $\mathcal{O}_X(D)|_D$, lo cual no puede hacerse en términos de divisores (pues no existe $D|_D$).

Teorema 6.10 *Sea X un esquema localmente noetheriano y $D \in \mathrm{Div}_c(X)$ un divisor entero. Entonces $\mathcal{O}_X(D)|_D = \omega_{D/X}$.*

Demostración: La inmersión cerrada $i : D \longrightarrow X$ es regular, luego, en la definición de haz canónico [E 9.27] podemos tomar $Z = X$, de modo que

$$\omega_{D/X} = \mathcal{C}^*_{D/X}.$$

Notemos que no hemos de calcular el determinante porque el haz normal $\mathcal{C}^*_{D/X}$ tiene rango 1. En efecto, el esquema D está definido por el haz de ideales $\mathcal{I} = \mathcal{O}_X(D^{-1})$, luego, según la definición [E 7.61], tenemos que

$$\mathcal{C}_{D/X} = i^*(\mathcal{I}/\mathcal{I}^2) \cong i^*(\mathcal{I} \otimes_{\mathcal{O}_X} \mathcal{O}_X/\mathcal{I}) \cong i^*(\mathcal{O}_X(D^{-1})) \otimes_{\mathcal{O}_D} \mathcal{O}_D \cong \mathcal{O}_X(D^{-1})|_D.$$

Por consiguiente, $\omega_{D/X} = \mathcal{O}_X(D)|_D$. ∎

Esto nos da una relación importante:

Teorema 6.11 *Sea X/S una superficie fibrada regular, sea $s \in S$ un punto cerrado y $E \in \mathrm{Div}_s(X)$ un divisor entero no trivial tal que $E \mid X_s$. Entonces*

$$\omega_{E/k(s)} \cong (\mathcal{O}_X(E) \otimes_{\mathcal{O}_X} \omega_{X/S})|_E.$$

Demostración: Recordemos que la hipótesis $E \mid X_s$ es vacía cuando $\dim S = 0$. En cualquier caso, nos asegura que tenemos una inmersión cerrada $E \longrightarrow X_s$ que nos permite considerar a E como una curva proyectiva sobre $k(s)$. En particular, el homomorfismo $E \longrightarrow S$ factoriza como $E \longrightarrow \mathrm{Esp}\, k(s) \longrightarrow S$, de donde se sigue fácilmente que $E \times_S \mathrm{Esp}\, k(s) \cong E$.

Así, por una parte, $X \longrightarrow S$ es localmente una intersección completa porque X y S son regulares (teorema [E 7.69 b]), $X_s \longrightarrow \mathrm{Esp}\, k(s)$ lo es por ser un cambio de base, y $E \longrightarrow X_s$ lo es por ser un cambio de base de $E \longrightarrow X$, que es una inmersión regular. Por último, $E \longrightarrow \mathrm{Esp}\, k(s)$ lo es por composición y $\mathrm{Esp}\, k(s) \longrightarrow S$ lo es de nuevo por [E 7.69]. También es claro que todos los homomorfismos son proyectivos, por lo que todos los haces canónicos del enunciado y los que vamos a considerar en la prueba están bien definidos.

Por una parte tenemos que

$$\omega_{E/S} = \omega_{E/X} \otimes_{\mathcal{O}_E} \omega_{X/S}|_E = \mathcal{O}_X(E)|_E \otimes_{\mathcal{O}_E} \omega_{X/S}|_E.$$

Por otra parte, si $f : E \longrightarrow \mathrm{Esp}\, k(s)$ es el homomorfismo estructural,

$$\omega_{E/S} = \omega_{E/k(s)} \otimes_{\mathcal{O}_E} f^* \omega_{k(s)/S} \cong \omega_{E/k(s)}.$$

Aquí hemos usado que el grupo de Picard de $\mathrm{Esp}\, k(s)$ es trivial. ∎

Como consecuencia inmediata obtenemos:

Teorema 6.12 (Fórmula de adjunción) *Sea X/S una superficie fibrada regular, $s \in S$ un punto cerrado, $E \in \mathrm{Div}_s(X)$ un divisor entero no trivial tal que $E \mid X_s$ y $W_{X/S}$ un divisor canónico (es decir, un divisor cuya clase en $\mathrm{Div}(X)$ se corresponde con la clase canónica de $\mathrm{Pic}(X)$). Entonces*

$$p_a(E) = 1 + \frac{1}{2}(E^2 + W_{X/S} \cdot E).$$

Demostración: Basta tomar grados en el isomorfismo del teorema anterior. Teniendo en cuenta las observaciones tras [E 10.20], vemos que

$$2p_a(E) - 2 = \mathrm{grad}((EW_{X/S})|_E) = (EW_{X/S}) \cdot E = E^2 + W_{X/S} \cdot E.$$

∎

Ejemplo En el caso particular en que $X = \mathrm{P}^2_k$ y E es una curva de grado d, el teorema [E 9.25] nos da que $W_{X/k}$ se corresponde con $\mathcal{O}_X(-3)$, luego la fórmula de adjunción se reduce a la fórmula del teorema 4.2:

$$p_a(E) = 1 + \frac{1}{2}(d^2 - 3d) = \frac{(d-1)(d-2)}{2}.$$

∎

Otro caso particular de interés se da cuando tomamos como E toda la fibra. Podemos enunciarlo así:

Teorema 6.13 *Sea X/S una superficie fibrada regular, $s \in S$ un punto cerrado y $W_{X/S}$ un divisor canónico. Entonces, el género de la fibra genérica X_η viene dado por*

$$p_a(X_\eta) = 1 + \frac{1}{2}\, W_{X/S} \cdot X_s.$$

Demostración: Basta tener en cuenta que $X_s^2 = 0$ por 6.6 y que todas las fibras tienen el mismo género, por [E 6.38] (ver la observación posterior). ∎

6.2 Aplicaciones birracionales

Para estudiar los homomorfismos entre superficies fibradas necesitaremos el concepto más general de aplicación racional (o birracional), que es un homomorfismo (birracional) no definido necesariamente en todos los puntos, sino que admite singularidades. En particular, veremos que una forma práctica de definir un homomorfismo entre dos esquemas es definir en principio una aplicación racional entre ellos y después demostrar que está definida en todos los puntos.

En primer lugar conviene recordar el teorema [E A.21]:

Teorema 6.14 *Sea $f : X \longrightarrow Y$ un homomorfismo propio y birracional, donde X es un esquema íntegro e Y es un esquema normal localmente noetheriano. Sea V el conjunto de los puntos de X que son aislados en su fibra. Entonces existe un abierto $U \subset Y$ tal que $V = f^{-1}[U]$ y f se restringe a un isomorfismo $V \longrightarrow U$. Además, todas las fibras de f son conexas.*

En las condiciones del teorema anterior, el cerrado $X \setminus V$ se llama *lugar excepcional* de f.

Definición 6.15 Sean X, Y dos esquemas íntegros sobre un esquema S de modo que Y/S sea separado. Una *aplicación racional* $f : X \longrightarrow Y$ definida sobre S es una clase de equivalencia en el conjunto de homomorfismos $U \longrightarrow Y$ definidos sobre S, donde U es un abierto no vacío en X, respecto a la relación dada por $g \sim h$ si y sólo si g y h coinciden en la intersección de sus dominios. El teorema [E 4.16] garantiza que esta relación es ciertamente una relación de equivalencia.

Es claro que si $f : X \longrightarrow Y$ es una aplicación racional y llamamos U a la unión de todos los dominios de los homomorfismos que componen f, entonces f contiene un único homomorfismo de dominio U, al que llamaremos también f. Al abierto U lo llamaremos *dominio de definición* de f. Diremos que f *está definida* en un punto $x \in X$ si x pertenece a su dominio de definición.

Diremos que una aplicación racional $f : X \longrightarrow Y$ es una *aplicación birracional* si se restringe a un isomorfismo entre un abierto (no vacío) de X y un abierto de Y.

Podemos identificar los homomorfismos $X \longrightarrow Y$ con las aplicaciones racionales $X \longrightarrow Y$ cuyo dominio de definición es X. En particular, los homomorfismos birracionales $X \longrightarrow Y$ (en el sentido de [E 4.6]) se identifican con las aplicaciones birracionales definidas sobre todo X.

En el estudio de las aplicaciones racionales es útil el concepto de gráfica. Lo introducimos primero para homomorfismos:

Definición 6.16 Sean X, Y esquemas íntegros definidos sobre un esquema S y supongamos que Y/S es separado. Sea $f : X \longrightarrow Y$ un homomorfismo definido sobre S. Llamamos *gráfica* de f a la imagen Γ_f del homomorfismo natural $X \longrightarrow X \times_S Y$. Observemos que dicho homomorfismo puede descomponerse como $X \longrightarrow X \times_Y Y \longrightarrow X \times_S Y$, donde la primera parte es un isomorfismo y la segunda una inmersión cerrada ([E 4.12]), luego la gráfica Γ_f es cerrada en $X \times_S Y$ y, con la estructura de subesquema cerrado reducido, es isomorfa a X.

Con más detalle, tenemos el diagrama siguiente:

$$\begin{array}{ccc} \Gamma_f & \longrightarrow & X \times_S Y \\ \uparrow & \swarrow & \\ X & & \end{array}$$

en el que la flecha vertical es un isomorfismo, la siguiente es una inmersión cerrada y la tercera es la proyección. La composición de las tres es la identidad en X, mientras que la composición de las dos primeras es la inmersión natural. Equivalentemente, la restricción a Γ_f de la proyección en X es un isomorfismo.

Definición 6.17 Sean X, Y esquemas íntegros definidos sobre un esquema S y supongamos que Y/S es separado. Sea $f : X \longrightarrow Y$ una aplicación racional definida sobre S y sea U su dominio de definición. Llamaremos *gráfica* de f a la clausura $\Gamma_f \subset X \times_S Y$ de la gráfica del homomorfismo $U \longrightarrow Y$ que determina a f. Consideraremos a Γ_f como subesquema cerrado de $X \times_S Y$ con la estructura de subesquema cerrado reducido.

Si llamamos $\Gamma_f^0 \subset U \times_S Y$ a la gráfica del homomorfismo que define a f, tenemos que Γ_f^0 es irreducible (es isomorfo a U), luego Γ_f también es irreducible, luego es un esquema íntegro. Como Γ_f^0 es cerrado en $U \times_S Y$, resulta que $\Gamma_f \cap (U \times_S Y) = \Gamma_f^0$, luego Γ_f^0 es abierto en Γ_f.

Es claro que la proyección en X se restringe a un homomorfismo $\Gamma_f \longrightarrow X$ que se restringe a su vez a un isomorfismo $\Gamma_f^0 \longrightarrow U$, luego se trata de un homomorfismo birracional.

Observemos que si f está definida en todo X, entonces Γ_f es la misma definida en 6.16, y la aplicación birracional que acabamos de definir es un isomorfismo. Recíprocamente, si la proyección se restringe a un isomorfismo en Γ_f, entonces ha de ser $U = X$. En efecto, tenemos el diagrama conmutativo

$$\begin{array}{ccccccc} X & \longrightarrow & \Gamma_f & \longrightarrow & X \times_S Y & \longrightarrow & Y \\ \uparrow & & \uparrow & & \uparrow & \nearrow & \\ U & \longrightarrow & \Gamma_0 & \longrightarrow & U \times_S Y & & \end{array}$$

donde el homomorfismo $U \longrightarrow Y$ calculado a través de la fila inferior es f, y la fila superior es, por lo tanto, una extensión de f a X. Como U es el mayor dominio posible de f, ha de ser $U = X$.

Observemos también que si f está definida en un punto $x \in X$, entonces existe un único punto $\xi \in \Gamma_f$ tal que $p_X(\xi) = x$. En efecto, existe ξ porque p_X se restringe a un isomorfismo de Γ_f^0 en U, y es único porque, si $p_X(\xi) = x$, entonces $\xi \in (U \times_S Y) \cap \Gamma_f = \Gamma_f^0$. Además, es claro que $p_Y(\xi) = f(x)$.

Así pues, podemos considerar al homomorfismo $\Gamma_f \longrightarrow Y$ como una "modificación" de la aplicación racional $X \longrightarrow Y$ que elimina los puntos donde ésta no está definida, en el sentido de que tenemos un homomorfismo birracional $\Gamma_f \longrightarrow X$ tal que cada punto $x \in X$ donde f está definida tiene una única antiimagen en Γ_f sobre el que la proyección actúa igual que f.

Esto nos lleva a definir la *transformada total* de un punto $x \in X$ como $f(x) = p_Y[p_X|_{\Gamma_f}^{-1}[\{x\}]] \subset Y$. Según acabamos de ver, cuando f está definida en x, la transformada total de x es simplemente $f(x)$ en el sentido usual. (En sentido estricto, es el conjunto $\{f(x)\}$, pero podemos pasar por alto el matiz.)

Teorema 6.18 *Sea S $f : X \longrightarrow Y$ una aplicación birracional entre superficies fibradas normales. Si $x \in X$ es un punto donde f no está definida, se cumple que x es un punto cerrado, su transformada total $f(x)$ es un cerrado conexo cuyas componentes irreducibles tienen dimensión 1 y la aplicación birracional inversa $f^{-1} : Y \longrightarrow X$ está definida sobre todos los puntos cuasigenéricos de $f(x)$, y les asigna como imagen el punto x.*

DEMOSTRACIÓN: El teorema [E 7.6] nos da que x ha de tener codimensión ≥ 2, luego ha de ser un punto cerrado. Por otra parte, los esquemas $(X \times_S Y)/Y$ y Γ_f/Y son propios, por lo que $f(x)$ es cerrado en Y.

Sea $Z = \Gamma_f$ la gráfica de f y consideremos la proyección $p : Z \longrightarrow X$, que es un homomorfismo propio y birracional. Sea $U \subset Y$ el abierto dado por el teorema 6.14, que claramente ha de ser el dominio de definición de f, luego tenemos que $x \notin U$. Por consiguiente, la fibra Z_x es conexa y no tiene puntos aislados, luego no puede reducirse a un punto, luego sus componentes irreducibles han de tener todas dimensión 1.

Ahora consideramos la proyección $q : Z \longrightarrow Y$. Como Z_x es conexa, su imagen, $f(x)$, también lo es. Falta probar que tiene también dimensión 1. Para ello consideramos el diagrama conmutativo

$$\begin{array}{ccccc} Z & \longrightarrow & X \times_S Y & \longrightarrow & Y \\ \uparrow & & \uparrow & & \\ Z_x & \longrightarrow & (X \times_S Y)_x & & \end{array}$$

Observemos que, si llamamos $s \in S$ a la imagen de x,

$$(X \times_S Y)_x = Y \times_S \operatorname{Esp} k(x) = Y_s \times_{k(s)} \operatorname{Esp} k(x),$$

de modo que la proyección $Z_x \longrightarrow Y$ puede descomponerse como

$$Z_x \longrightarrow Y_s \times_{k(s)} \operatorname{Esp} k(x) \longrightarrow Y_s \longrightarrow Y.$$

Los homomorfismos primero y último son inmersiones cerradas, mientras que el central es un homomorfismo finito. En definitiva, la proyección $Z_x \longrightarrow f(x)$ es finita y suprayectiva, al igual que su restricción a cada componente irreducible de Z_x en su imagen. El teorema [E 4.45] implica entonces que todas las componentes irreducibles de $f(x)$ tienen también dimensión 1.

Por último, es fácil ver que f y f^{-1} tienen la misma gráfica (salvo el orden de los factores), de modo que, si y es un punto cuasigenérico de $f(x)$, podemos calcular su transformada total por f^{-1} usando las proyecciones p y q. Notemos que f^{-1} está definida en y porque no es un punto cerrado, luego sólo hay un punto en Z cuya proyección sea y. Dicho punto ha de ser un punto cuasigenérico de Z_x, luego su proyección en X ha de ser x. ∎

Así pues, en las condiciones del teorema anterior, una aplicación birracional f está definida en un punto cerrado si y sólo si su transformada total es un punto cerrado. (Y en los puntos no cerrados f siempre está definida.)

Vamos a dar ahora un criterio en términos de valoraciones para que una aplicación birracional esté definida en un punto

Definición 6.19 Sea X/S un esquema íntegro separado, sea $K = K(X)$, sea $v : K^* \longrightarrow \mathbb{Z}$ una valoración y sea $\mathcal{O}_v \subset K$ su anillo de enteros. Entonces $\operatorname{Esp}\mathcal{O}_v$ tiene únicamente dos puntos: el punto genérico y el punto cerrado. Además tenemos una inmersión abierta $\operatorname{Esp}K \longrightarrow \operatorname{Esp}\mathcal{O}_v$ cuya imagen es el punto genérico.

La composición $\operatorname{Esp}K \longrightarrow X \longrightarrow S$ determina una aplicación racional $\operatorname{Esp}\mathcal{O}_v \longrightarrow S$. Si esta aplicación está definida también sobre el punto cerrado de $\operatorname{Esp}\mathcal{O}_v$, diremos que *$v$ está definida sobre S*. (Y entonces, $\operatorname{Esp}\mathcal{O}_v$ es un esquema definido sobre S y la inmersión $\operatorname{Esp}K \longrightarrow \operatorname{Esp}\mathcal{O}_v$ está definida sobre S.)

Por ejemplo, si $P \in X$ es un punto normal de codimensión 1, entonces $\mathcal{O}_{X,P}$ es un anillo de valoración discreta que determina una valoración $v_P : K^* \longrightarrow \mathbb{Z}$. Está definida sobre S, pues el homomorfismo natural $\operatorname{Esp}\mathcal{O}_{X,P} \longrightarrow X \longrightarrow S$ extiende al homomorfismo $\operatorname{Esp}K \longrightarrow X \longrightarrow S$. A las valoraciones de la forma v_P, donde P es un punto normal de codimensión 1 en X, las llamaremos *valoraciones normales* de X.

Es claro que si X/S es un esquema separado normal, existe una biyección entre los divisores primos de X y las valoraciones normales de X. En efecto, basta observar que dos primos distintos no pueden determinar la misma valoración v o, de lo contrario, tendríamos dos homomorfismos $\operatorname{Esp}\mathcal{O}_v \longrightarrow X$ definidos sobre S que extenderían al homomorfismo natural $\operatorname{Esp}K \longrightarrow X$.

Vamos a dar condiciones para que una valoración dada sea normal.

Definición 6.20 Sea X/S un esquema íntegro separado, sea $K = K(X)$, sea $v : K^* \longrightarrow \mathbb{Z}$ una valoración definida sobre S y sea $\mathcal{O}_v \subset K$ su anillo de enteros. Un *centro* de v es un punto $P \in X$ tal que existe un homomorfismo f, definido sobre S, que hace conmutativo el diagrama siguiente:

$$\begin{array}{ccc} \operatorname{Esp}\mathcal{O}_v & \xrightarrow{f} & \operatorname{Esp}\mathcal{O}_{X,P} \\ \uparrow & \nearrow & \\ \operatorname{Esp}K & & \end{array}$$

Esto equivale a que tenemos un homomorfismo $\mathcal{O}_{X,P} \longrightarrow \mathcal{O}_v$ (de anillos locales) que conmuta con las inclusiones en K o, más simplemente, equivale a las inclusiones $\mathcal{O}_{X,P} \subset \mathcal{O}_v$, $\mathfrak{m}_P \subset \mathfrak{m}_v$ (la segunda condición hace falta para que la inclusión sea un homomorfismo de anillos locales).

En general, si $A \subset B \subset K$ son dos anillos locales contenidos en el mismo cuerpo K, se dice que B *domina* a A si el ideal maximal de A está contenido en el ideal maximal de B.

Componiendo con el homomorfismo natural $\operatorname{Esp}\mathcal{O}_{X,P} \longrightarrow X$ obtenemos un homomorfismo $\operatorname{Esp}\mathcal{O}_v \longrightarrow X$, definido sobre S, cuya imagen es P y que extiende

al homomorfismo natural $\operatorname{Esp} K \longrightarrow X$. Esto prueba que si v tiene un centro, éste es único.

Una valoración v es normal si y sólo si tiene un centro P normal de codimensión 1. En efecto, en tal caso tenemos que $\mathcal{O}_V$ domina a $\mathcal{O}_{X,P}$, de donde se sigue la igualdad $\mathcal{O}_{X,P} = \mathcal{O}_v$.

En efecto, en general, *un anillo de valoración discreta A no puede ser dominado estrictamente por un anillo B contenido en su cuerpo de cocientes,* pues, si $b \in B \setminus A$, tendríamos que $v(b) > 1$, luego $v(1/b) < 1$, luego $1/b \in \mathfrak{m}_A \subset \mathfrak{m}_B$, luego $1 \in \mathfrak{m}_B$, contradicción.

Por consiguiente, $v = v_P$. (Recíprocamente, es inmediato que v_P tiene centro P, tomando como f la identidad.)

Teorema 6.21 *Si X/S es un esquema íntegro propio, toda valoración en X definida sobre S tiene un único centro.*

Demostración: Basta aplicar el teorema [E 4.29], según el cual, el homomorfismo $\operatorname{Esp} K \longrightarrow X$ se extiende a un homomorfismo $\operatorname{Esp} \mathcal{O}_v \longrightarrow X$ definido sobre S. Consideramos la imagen $P \in X$ del punto cerrado de $\operatorname{Esp} \mathcal{O}_v$. Es claro que el homomorfismo se descompone como $\operatorname{Esp} \mathcal{O}_v \xrightarrow{f} \operatorname{Esp} \mathcal{O}_{X,x} \longrightarrow X$ y f está definido sobre S, luego P es un centro de v. ∎

Si X/S, Y/S son esquemas íntegros separados y $f : X \longrightarrow Y$ es una aplicación birracional definida sobre S, entonces f nos permite identificar los cuerpos $K(X) = K(Y) = K$. En particular, cada valoración en X puede verse como una valoración en Y, y viceversa.

Teorema 6.22 *Sea $f : X \longrightarrow Y$ una aplicación birracional entre superficies fibradas normales. Si, para todo divisor primo P de Y, la valoración v_P es normal en X, entonces f está definida sobre todo X.*

Demostración: Supongamos que f no está definida en un punto $x \in X$. Por 6.18 sabemos que x es cerrado y que su transformada total $f(x)$ tiene dimensión 1. Sea $P \in f(x)$ uno cualquiera de sus puntos cuasigenéricos. Llamemos Z a la gráfica de f. La proyección $q : Z \longrightarrow Y$ es un homomorfismo birracional. Sea $z \in Z_P$. Si identificamos ambos anillos con subanillos de $K(Z) = K(Y)$, el homomorfismo $q_z : \mathcal{O}_{Y,P} \longrightarrow \mathcal{O}_{Z,z}$ nos da que $\mathcal{O}_{Z,z}$ domina a $\mathcal{O}_{Y,P}$ y, como éste es un anillo de valoración discreta (según hemos visto antes del teorema 6.21), ha de ser $\mathcal{O}_{Y,P} = \mathcal{O}_{Z,z}$.

Por otra parte, la proyección $p : Z \longrightarrow X$ cumple $p(z) = x$, luego tenemos que $\mathcal{O}_{Y,P} = \mathcal{O}_{Z,z}$ domina a $\mathcal{O}_{X,x}$, y esto implica que v_P, como valoración en X, tiene centro x, luego no es una valoración normal, ya que x no tiene codimensión 1. Esto contradice la hipótesis del teorema. ∎

Terminaremos la sección con un par de aplicaciones. Observemos en primer lugar que si X/S es una superficie fibrada regular y $x \in X$ es un punto cerrado, la explosión $\pi : \widetilde{X} \longrightarrow X$ de centro x (considerado como subesquema cerrado íntegro) convierte a $\widetilde{X}/S$ en una superficie fibrada regular (Teoremas 5.20 y 5.25).

Teorema 6.23 *Sea $f : X \longrightarrow Y$ un homomorfismo birracional entre superficies fibradas regulares y sea $y \in Y$ un punto tal que $\dim X_y = 1$. Entonces f se descompone como un homomorfismo birracional $g : X \longrightarrow \widetilde{Y}$ seguido de la explosión $\pi : \widetilde{Y} \longrightarrow Y$ de centro y.*

DEMOSTRACIÓN: Sea $g = f \circ \pi^{-1} : X \longrightarrow \widetilde{Y}$, que, en principio, es una aplicación racional. Hemos de probar que está definida en todo X. Supongamos que existe un punto $x \in X$ donde no está definida. Por el teorema 6.18 sabemos que es un punto cerrado y que la transformada total $E = g(x)$ tiene todas sus componentes irreducibles de dimensión 1.

El teorema 5.17 nos da que π^{-1} está definida en $Y \setminus \{y\}$, luego g está definida en $X \setminus X_y$. Así pues, $f(x) = y$. Si ξ es un punto cuasigenérico de E, sabemos que $g^{-1}(\xi) = x$, luego $f(g^{-1}(\xi)) = y$, pero $g^{-1} \circ f = \pi$, luego $\pi(\xi) = y$, luego $\xi \in \widetilde{Y}_y$. Así pues, $E \subset \widetilde{Y}_y$. El teorema 5.25 nos da que $\widetilde{Y}_y \cong \mathrm{P}^1_{k(y)}$. En particular la fibra es irreducible, luego $E = \widetilde{Y}_y$.

Si identificamos los cuerpos de funciones $K(X) = K(Y) = K(\widetilde{Y})$, las relaciones $g^{-1}(\xi) = x$ y $f(x) = y$ nos dan las inclusiones

$$\mathcal{O}_{Y,y} \subset \mathcal{O}_{X,x} \subset \mathcal{O}_{\widetilde{Y},\xi},$$

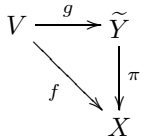
donde hay que entender que cada anillo es dominado por el siguiente.

Por el teorema 6.14, la fibra X_y es conexa, luego todas sus componentes irreducibles tienen dimensión 1. Sea D el producto de dichas componentes, consideradas como divisores primos (con multiplicidad 1). Así, como divisores, tenemos que $D \mid X_y$, luego el haz de ideales $\mathcal{I}$ de $\mathcal{O}_X$ asociado a X_y está contenido en $\mathcal{O}_X(D^{-1})$ y, en particular, $\mathcal{I}_x \subset \mathcal{O}_X(D^{-1})_x$.

Es fácil ver que $\mathcal{I}_x = \mathfrak{m}_y\mathcal{O}_{X,x}$, luego, si llamamos $\alpha \in \mathfrak{m}_x$ a un generador del ideal $\mathcal{O}_X(D^{-1})_x$, tenemos la inclusión $\mathfrak{m}_y\mathcal{O}_{X,x} \subset \alpha\mathcal{O}_{X,x}$. Equivalentemente, $\alpha^{-1}\mathfrak{m}_y\mathcal{O}_{X,x} \subset \mathcal{O}_{X,x}$, luego el miembro izquierdo es un ideal de $\mathcal{O}_{X,x}$.

Vamos a probar que en realidad $\alpha^{-1}\mathfrak{m}_y\mathcal{O}_{X,x} = \mathcal{O}_{X,x}$. En caso contrario tendríamos la inclusión $\alpha^{-1}\mathfrak{m}_y\mathcal{O}_{X,x} \subset \mathfrak{m}_x$, luego $\mathfrak{m}_y\mathcal{O}_{X,x} \subset \alpha\mathfrak{m}_x \subset \mathfrak{m}_x^2 \subset \mathfrak{m}_\xi^2$, luego $\mathfrak{m}_y\mathcal{O}_{\widetilde{Y},\xi} \subset \mathfrak{m}_\xi^2 \subsetneq \mathfrak{m}_\xi$, luego el anillo $\mathcal{O}_{\widetilde{Y}_y,\xi} = \mathcal{O}_{\widetilde{Y},\xi}/\mathfrak{m}_y\mathcal{O}_{\widetilde{Y},\xi}$ no sería reducido. (Porque $\mathcal{O}_{\widetilde{Y},\xi}$ es un anillo de valoración discreta, y no tiene más ideal primo que $\mathfrak{m}_\xi$, luego el ideal $\mathfrak{m}_y\mathcal{O}_{\widetilde{Y},\xi}$ no es radical.) Pero esto es imposible, ya que la fibra $\widetilde{Y}_y$ es reducida (es isomorfa a una recta proyectiva).

Así pues, el ideal $\mathfrak{m}_y\mathcal{O}_{X,x} = \alpha\mathcal{O}_{X,x}$ es principal. Tomemos un entorno afín $U = \operatorname{Esp} A$ de y y un entorno afín $V = \operatorname{Esp} B$ de x tal que $V \subset f^{-1}[U]$. El punto cerrado y de U está asociado al haz coherente $\mathcal{J}$ de $\mathcal{O}_U$ determinado por un ideal maximal $\mathfrak{m}$, y $\mathfrak{m}_y\mathcal{O}_{V,x} = (\mathcal{J}\mathcal{O}_V)_x$. Así pues, reduciendo V, podemos suponer que el haz $\mathcal{J}\mathcal{O}_V$ es libre de rango 1. El teorema 5.22 nos da un diagrama conmutativo



donde el homomorfismo g ha de ser una restricción de la aplicación birracional que estamos considerando, luego concluimos que g está definida en x, cuando habíamos supuesto lo contrario. ∎

Como consecuencia:

Teorema 6.24 *Sea $f : X \longrightarrow Y$ un homomorfismo birracional entre superficies fibradas regulares. Si f no es un isomorfismo, se descompone como una cadena finita de explosiones, cada una de las cuales tiene por centro un punto cerrado.*

DEMOSTRACIÓN: Si f no es un isomorfismo, su lugar excepcional $\mathcal{E}$ no puede ser vacío. Tomemos un punto $y \in Y$ en su imagen. El teorema anterior nos da una descomposición de f como $X \xrightarrow{g} \widetilde{Y} \xrightarrow{\pi} Y$, donde el segundo homomorfismo es la explosión de centro y. Como el esquema de Dedekind base es afín, sabemos que $\widetilde{Y}$ es también una superficie fibrada.

Sea $\mathcal{E}'$ el lugar excepcional de g. Observemos que $\mathcal{E}' \subset \mathcal{E}$, pues si $x \in \mathcal{E}'$, entonces pertenece a una fibra (respecto de g) con más de un punto, que estará contenida en su fibra respecto de f, luego ésta tampoco será trivial, luego $x \in \mathcal{E}$.

Sea $\Gamma = \pi^{-1}[y]$, que es una curva irreducible en $\widetilde{Y}$. Es claro que $g^{-1}[\Gamma] \subset \mathcal{E}$, luego ha de haber una componente irreducible Γ' de $g^{-1}[\Gamma]$ tal que $g[\Gamma'] = \Gamma$. Si $x \in \Gamma'$, su fibra respecto de g ha de ser finita, pero no puede tener puntos aislados, luego $\Gamma' \cap \mathcal{E}' = \varnothing$.

Con esto hemos probado que $\mathcal{E}'$ tiene menos componentes irreducibles que $\mathcal{E}$, luego, repitiendo el argumento un número finito de veces, llegamos a una aplicación g que es un isomorfismo. ∎

En la prueba del teorema anterior vemos que si $\mathcal{E}$ es irreducible, entonces g ha de ser un isomorfismo. Por consiguiente:

Teorema 6.25 *Sea $f : X \longrightarrow Y$ un homomorfismo birracional entre superficies fibradas regulares cuyo lugar excepcional sea irreducible. Entonces f es la explosión respecto de un punto cerrado.*

Veamos ahora una aplicación del criterio 6.22, para lo que necesitamos una definición:

Definición 6.26 Sea X/S una superficie fibrada normal y $\mathcal{E}$ un conjunto de curvas verticales íntegras en X proyectivas sobre S. Una *contracción* de las curvas de $\mathcal{E}$ es una superficie fibrada normal Y/S junto con un homomorfismo proyectivo birracional $f : X \longrightarrow Y$ tal que, para cada curva vertical íntegra proyectiva E en X, se cumple que $f[E]$ se reduce a un punto si y sólo si $E \in \mathcal{E}$.

Teorema 6.27 *En las condiciones de la definición anterior, si existe la contracción, es única salvo isomorfismo.*

DEMOSTRACIÓN: Sea $f' : X \longrightarrow Y'$ otra contracción. Entonces existe una única aplicación racional $g : Y \longrightarrow Y'$, definida sobre S, tal que $f' = f \circ g$. Basta probar que g está definida en todo Y, pues del mismo modo podemos construir su inversa.

Es claro que el lugar excepcional de f está formado por la unión de las curvas de $\mathcal{E}$, de modo que su imagen es el conjunto finito de puntos de Y en que éstas se transforman. Si llamamos V al complementario de esta imagen, vemos que V contiene a todos los puntos de codimensión 1. Si $\xi \in Y$ es uno de estos puntos y $\eta \in X$ es su antiimagen, tenemos que el homomorfismo natural $\mathcal{O}_{Y,\xi} \longrightarrow \mathcal{O}_{X,\eta}$ es un isomorfismo. Si identificamos $K(Y) = K(X)$ a través de f, dicho homomorfismo es una inclusión, con lo que $\mathcal{O}_{Y,\xi} = \mathcal{O}_{X,\xi'}$, y así, vemos que las valoraciones normales de Y se identifican con las valoraciones normales en X cuyo centro no está en el lugar excepcional de f.

Lo mismo es válido para f', con el mismo lugar singular, luego concluimos que, a través de g, todas las valoraciones normales de Y' son también normales en Y, y viceversa, luego g es un isomorfismo. ∎

6.3 Resolución de singularidades

Nos ocupamos ahora del problema de desingularizar superficies fibradas. Por razones técnicas nos vemos obligados a trabajar con superficies reducidas, no necesariamente íntegras. (Concretamente, esto es debido a que hemos de considerar cambios de base que no conservan la integridad de las superficies). Empezamos generalizando la definición [E 4.6] de homomorfismo birracional al caso de homomorfismos entre esquemas reducidos arbitrarios. Notemos que si X es un esquema reducido y ξ es un punto cuasigenérico, entonces $\mathcal{O}_{X,\xi}$ es un cuerpo (es el cuerpo de funciones racionales de $\overline{\{\xi\}}$).

Definición 6.28 Sea $f : X \longrightarrow Y$ un homomorfismo de tipo finito entre esquemas noetherianos reducidos. Diremos que f es *birracional* si biyecta los puntos cuasigenéricos $\xi_1, \ldots, \xi_n$ de X con los puntos cuasigenéricos $\xi'_1, \ldots, \xi'_n$ de Y, y los homomorfismos $f_\xi : \mathcal{O}_{Y,\xi'_i} \longrightarrow \mathcal{O}_{X,\xi_i}$ son isomorfismos.

Notemos que, ciertamente, esta definición extiende a [E 4.6]. Si f es afín, además de birracional, $U = \operatorname{Esp} A$, es un abierto afín de Y y $f^{-1}[U] = \operatorname{Esp} B$, el homomorfismo $A \longrightarrow B$ inducido por f biyecta los primos minimales $\mathfrak{P}_i$ de B con los primos minimales $\mathfrak{p}_i$ de A, de modo que tenemos monomorfismos $A/\mathfrak{p}_i \longrightarrow B/\mathfrak{P}_i$. Como A es reducido, esto implica que $A \longrightarrow B$ es también un monomorfismo. En otros términos, hemos probado que el homomorfismo natural $\mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X$ es inyectivo.

Definición 6.29 Si X es un esquema reducido localmente noetheriano, una *desingularización* de X es un homomorfismo propio birracional $\pi : Z \longrightarrow X$ tal que Z es regular. Diremos que es una *desingularización estricta* de X si el conjunto $U = \operatorname{Reg}(X)$ de los puntos regulares de X es abierto y π se restringe a un isomorfismo $\pi^{-1}[U] \longrightarrow U$.

La existencia de desingularizaciones de esquemas es un problema muy complejo de la geometría algebraica. Observemos que toda curva algebraica reducida admite una desingularización (su normalización), pero la existencia de

desingularizaciones en dimensiones superiores no es trivial en absoluto. A título ilustrativo, citamos el teorema siguiente (que no vamos a necesitar):

Teorema [Hironaka] *Toda variedad algebraica reducida sobre un cuerpo de característica* 0 *admite una desingularización estricta.*

En característica prima, el problema sigue abierto. En esta sección daremos condiciones para que una superficie fibrada admita una desingularización a partir de un resultado general de Lipman sobre desingularización de superficies, que enunciaremos sin demostración. Más concretamente, vamos a ver cómo es posible construir una sucesión de homomorfismos birracionales que, bajo ciertas hipótesis, dan lugar a una desingularización. En esta sección necesitaremos los resultados sobre anillos y esquemas excelentes que hemos expuesto en la primera parte del libro.

Empezamos generalizando el concepto de normalización al caso de esquemas reducidos, no necesariamente íntegros:

Definición 6.30 Sea X un esquema noetheriano reducido y sean $W_1, \dots, W_n$ sus componentes irreducibles, consideradas como subesquemas íntegros. Consideremos las normalizaciones $\pi_i : W_i' \longrightarrow W_i$. Llamaremos *normalización* de X a la unión disjunta $X_1 = W_1' \cup \cdots \cup W_n'$, sobre la que los homomorfismos π_i inducen un homomorfismo $\pi : X_1 \longrightarrow X$, claramente birracional. Notemos que si X es un esquema íntegro, la normalización que acabamos de definir es la que ya teníamos definida.

Sean $\xi_1, \dots, \xi_n$ los puntos cuasigenéricos de X. Si $U = \operatorname{Esp} A$ es un abierto afín en X que contiene, digamos, los puntos $\xi_1, \dots, \xi_r$, éstos se corresponden con los primos minimales $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ de A, de modo que $U \cap X_i = \operatorname{Esp}(A/\mathfrak{p}_i)$ y $\pi_i^{-1}[U \cap U_i] = \operatorname{Esp} B_i$, donde B_i es la clausura entera de $A/\mathfrak{p}_i$ en su cuerpo de cocientes, que es $A_{\mathfrak{p}_i}$ o, equivalentemente, $\mathcal{O}_{X,\xi_i}$. (Notemos que $A_{\mathfrak{p}_i}$ es reducido, luego tenemos un monomorfismo $A/\mathfrak{p}_i \longrightarrow A_{\mathfrak{p}_i}/\mathfrak{p}_i A_{\mathfrak{p}_i} = A_{\mathfrak{p}_i}$.)

Si X es un esquema excelente noetheriano reducido, entonces A es un anillo de Nagata, luego B_i es finito sobre $A/\mathfrak{p}_i$, luego también sobre A y, por consiguiente, $\pi^{-1}[U] = \operatorname{Esp}(B_1 \oplus \cdots \oplus B_r)$ también es finito sobre A, luego $\pi : X_1 \longrightarrow X$ es un homomorfismo finito. Más aún, en tal caso X_1 es también un esquema excelente noetheriano reducido con un número finito de componentes irreducibles (el mismo número que tiene X, luego, en particular, es íntegro si y sólo si X lo es). Además X_1 es unión disjunta de abiertos normales.

Por ser esquemas excelentes reducidos, los conjuntos de puntos regulares de los esquemas X y X_1 son abiertos (no vacíos, ya que contienen a los puntos cuasigenéricos). En suma, si X es un esquema excelente noetheriano reducido, cumple las tres propiedades siguientes:

D1 *El conjunto* $\operatorname{Reg}(X)$ *de los puntos regulares de* X *es abierto no vacío.*

D2 *La normalización* $X_1 \longrightarrow X$ *es un homomorfismo finito.*

D3 *El conjunto* $\operatorname{Reg}(X_1)$ *es también un abierto no vacío.*

Consideremos ahora un esquema reducido arbitrario X que cumpla estas tres propiedades, y supongamos además que $\dim X = 2$. Por ser normal, todo punto $P \in X_1$ de codimensión 1 es regular, ya que $\mathcal{O}_{X_1,P}$ es un dominio íntegro noetheriano local de dimensión 1 íntegramente cerrado, luego es un dominio de Dedekind local, luego es un anillo de valoración discreta, luego es regular. Por consiguiente, el conjunto $\mathrm{Sing}(X_1)$ de los puntos singulares de X_1 tiene dimensión 0, luego está formado por un número finito de puntos.

Sea $X_1' \longrightarrow X_1$ la explosión de centro el conjunto de puntos singulares de X_1 (con la estructura de subesquema cerrado reducido). Obviamente, es la suma directa de las explosiones de las componentes conexas (o irreducibles) de X_1 respecto de los puntos singulares que contienen, que son homomorfismos birracionales propios (y proyectivos sobre un anillo noetheriano D si X lo es). Entenderemos que $X_1' = X_1$ si X_1 es regular.

En definitiva, el homomorfismo $f : X_1' \longrightarrow X$ es propio y birracional, y es proyectivo si X es proyectivo sobre un anillo noetheriano D. Además, si $U = \mathrm{Reg}(X)$, se restringe a un isomorfismo $f^{-1}[U] \longrightarrow U$.

El esquema X_1' es también reducido y de dimensión 2. Si también cumple las propiedades **D1, D2, D3** (cosa que sucede ciertamente si X es excelente y noetheriano, pues entonces X_1' también lo es), podemos considerar a su vez la normalización $X_2 \longrightarrow X_1'$ y la explosión $X_2' \longrightarrow X_2$ del subesquema $\mathrm{Sing}(X_2)$ y, en general, mientras no dejen de cumplirse ambas propiedades, podemos ir construyendo una sucesión de homomorfismos propios birracionales

$$\cdots \longrightarrow X_3 \longrightarrow X_2 \longrightarrow X_1 \longrightarrow X$$

que son proyectivos si X es proyectivo sobre un esquema afín noetheriano S.

A esta sucesión (cuando exista) la llamaremos *sucesión canónica* de X. Es claro que si un X_n es regular, entonces el homomorfismo $X_n \longrightarrow X$ es una desingularización estricta de X, a la que llamaremos *desingularización canónica* de X. Hemos probado que la sucesión canónica está definida cuando X es un esquema excelente noetheriano reducido de dimensión 2, y el teorema de Lipman afirma que, de hecho, proporciona una desingularización:

Teorema 6.31 (Lipman) *Si X es un esquema reducido excelente noetheriano de dimensión 2, entonces existe su desingularización canónica.*

Vamos a aplicar este teorema al caso de las superficies fibradas. Necesitamos algunos resultados previos:

Consideremos un esquema localmente noetheriano X y un haz coherente $\mathcal{F}$ en X. Recordemos que el soporte de $\mathcal{F}$ es

$$\mathrm{sop}\,\mathcal{F} = \{x \in X \mid \mathcal{F}_x \neq 0\}.$$

Se trata de un conjunto cerrado, pues si $\mathcal{F}_x = 0$, podemos tomar un entorno afín noetheriano $U = \mathrm{Esp}\,A$ de x, de modo que $\mathcal{F}|_U = \widetilde{M}$, para cierto A-módulo finitamente generado M. El punto x se corresponde con un ideal $\mathfrak{p} \in \mathrm{Esp}\,A$, de

modo que $M_\mathfrak{p} = 0$. Si $m_1, \dots, m_n$ es un generador de M, existe un $s \in A \setminus \mathfrak{p}$ tal que $sm_i = 0$, luego $M_s = 0$, luego $\mathfrak{p} \in D(s) \subset \operatorname{sop}\mathcal{F}$.

Si $U \subset X$ es abierto y $s \in \mathcal{O}_X(U)$, la multiplicación por s define un homomorfismo $\alpha_{U,s} : \mathcal{F}(U) \longrightarrow \mathcal{F}(U)$, que a su vez define un homomorfismo de haces $\alpha_U(s) : \mathcal{F}|_U \longrightarrow \mathcal{F}|_U$. De este modo, tenemos definido un homomorfismo de módulos $\alpha_U : \mathcal{O}_X(U) \longrightarrow \operatorname{Hom}_{\mathcal{O}_X|_U}(\mathcal{F}|_U, \mathcal{F}|_U)$, que a su vez determina un homomorfismo de haces $\alpha : \mathcal{O}_X \longrightarrow \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{F})$.

Llamaremos *anulador* de $\mathcal{F}$ al núcleo de α, y lo representaremos por $\operatorname{An}\mathcal{F}$, que es un haz cuasicoherente en X. Así, para cada abierto afín $U \subset X$, tenemos que $(\operatorname{An}\mathcal{F})(U)$ es el núcleo de α_U o, más explícitamente,

$$(\operatorname{An}\mathcal{F})(U) = \{s \in \mathcal{O}_X(U) \mid s\mathcal{F}(U) = 0\}.$$

Similarmente, si $x \in X$, se cumple que

$$(\operatorname{An}\mathcal{F})_x = \{s \in \mathcal{O}_{X,x} \mid s\mathcal{F}_x = 0\}.$$

Por consiguiente:

$$x \notin V(\operatorname{An}\mathcal{F}) \Leftrightarrow (\operatorname{An}\mathcal{F})_x = \mathcal{O}_{X,x} \Leftrightarrow \mathcal{F}_x = 0 \Leftrightarrow x \notin \operatorname{sop}\mathcal{F}.$$

Así pues: $\operatorname{sop}\mathcal{F} = V(\operatorname{An}\mathcal{F})$.

Teorema 6.32 *Sea $f : X \longrightarrow Y$ un homomorfismo finito birracional entre esquemas noetherianos reducidos. Si existe un haz inversible de ideales $\mathcal{L} \subset \mathcal{O}_Y$ tal que f se restringe a un isomorfismo sobre $f^{-1}[Y \setminus V(\mathcal{L})]$, entonces f es la explosión respecto de un subesquema cerrado de Y con soporte $V(\mathcal{L})$.*

Demostración: Por [E 5.18] sabemos que $f_*\mathcal{O}_X$ es un haz coherente en Y, y tenemos un homomorfismo $\mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X$. Consideremos el homomorfismo $\pi : \operatorname{Proy}((f_*\mathcal{O}_X)[T]) \longrightarrow Y$. Si $U \subset Y$ es un abierto afín, entonces

$$\pi^{-1}[U] = \operatorname{Proy}(\mathcal{O}_X(f^{-1}[U])[T]) = \operatorname{Esp}(\mathcal{O}_X(f^{-1}[U])) = f^{-1}[U].$$

La unicidad del teorema [E A.5] nos da que

$$X = \operatorname{Proy}((f_*\mathcal{O}_X)[T]).$$

Por hipótesis tenemos que $(f_*\mathcal{O}_X)|_{Y\setminus V(\mathcal{L})} \cong \mathcal{O}_Y|_{Y\setminus V(\mathcal{L})}$, luego el haz coherente $\mathcal{M} = f_*\mathcal{O}_X/\mathcal{O}_Y$ cumple $\operatorname{sop}\mathcal{M} \subset V(\mathcal{L})$. Según las observaciones previas al teorema, $V(\operatorname{An}\mathcal{M}) \subset V(\mathcal{L})$, luego $\mathcal{L}$ está contenido en el radical de $\operatorname{An}\mathcal{M}$, es decir, existe un $r \geq 1$ tal que $\mathcal{L}^r f_*\mathcal{O}_X \subset \mathcal{O}_Y$. Consideremos el ideal $\mathcal{I} = \mathcal{L}^{r+1} f_*\mathcal{O}_X$, que claramente cumple

$$\mathcal{L}^{r+1} \subset \mathcal{I} = \mathcal{L}(\mathcal{L}^r f_*\mathcal{O}_X) \subset \mathcal{L},$$

luego $V(\mathcal{I}) = V(\mathcal{L})$. Ahora aplicamos el teorema 5.18 con $\mathcal{N} = \mathcal{L}^{r+1}$, de donde obtenemos que

$$X = \operatorname{Proy}(\bigoplus_{n\geq 1} (\mathcal{L}^{r+1})^n \otimes_{\mathcal{O}_Y} f_*\mathcal{O}_X) \cong \operatorname{Proy}(\bigoplus_{n\geq 1} \mathcal{I}^n).$$

Para el último isomorfismo, observemos que $f_*\mathcal{O}_X$ es una $\mathcal{O}_Y$-álgebra y que el hecho de que $\mathcal{L}$ sea inversible (es decir, localmente principal) asegura que los productos tensoriales son canónicamente isomorfos a los productos de ideales y módulos. Así pues, X es la explosión respecto del subesquema cerrado de Y asociado a $\mathcal{I}$. ∎

Teorema 6.33 *Sea D un anillo de valoración discreta, sea $\pi \in D$ un primo y $\hat{D}$ la compleción de D. Sea Y/D un esquema plano localmente noetheriano y sea $\hat{Y} = Y \otimes_D \operatorname{Esp}\hat{D}$. Sea $\mathcal{I}$ un haz de ideales de $\mathcal{O}_{\hat{Y}}$ tal que $V(\mathcal{I}) \subset V(\pi)$ y sea $f : W \longrightarrow \hat{Y}$ la explosión de centro $V(\mathcal{I})$. Entonces existe un ideal $\mathcal{I}_0$ de $\mathcal{O}_Y$ tal que $V(\mathcal{I}_0) \subset V(\pi)$ de modo que f se obtiene por cambio de base de la explosión $g : X \longrightarrow Y$ de centro $V(\mathcal{I}_0)$.*

Demostración: Sea $\pi : \hat{Y} \longrightarrow Y$ la proyección natural. Como Y es plano sobre D, el homomorfismo natural $\mathcal{O}_Y \longrightarrow \pi_*\mathcal{O}_{\hat{Y}} = \mathcal{O}_Y \otimes_D \hat{D}$ es inyectivo, lo que nos permite definir $\mathcal{I}_0 = \pi_*\mathcal{I} \cap \mathcal{O}_Y$, que claramente es un haz de ideales de $\mathcal{O}_Y$. La hipótesis $V(\mathcal{I}) \subset V(\pi)$ equivale a que $\pi \in \operatorname{rad}\mathcal{I}$, de donde se sigue inmediatamente que $\pi \in \operatorname{rad}\mathcal{I}_0$, luego $V(\mathcal{I}_0) \subset V(\pi)$. (Para cada abierto afín $U \subset Y$ tenemos un n tal que $\pi^n \in \mathcal{I}(\hat{U}) \cap \mathcal{O}_Y(U) = \mathcal{I}_0(U)$.)

Veamos ahora que $\mathcal{I} = \pi^*\mathcal{I}_0$. Basta ver que, para todo abierto afín $U \subset Y$, se cumple que $(\pi^*\mathcal{I}_0)(\pi^{-1}[U]) = \mathcal{I}_0(U) \otimes_D \hat{D}$ coincide con $\mathcal{I}(\pi^{-1}[U])$. Por simplificar la notación, llamamos $A = \mathcal{O}_Y(U)$, $I = \mathcal{I}(\pi^{-1}[U]) \subset A \otimes_D \hat{D}$, $I_0 = \mathcal{I}_0(U) = I \cap A$. Tomemos n tal que $\pi^n \in I$. Hemos de probar que $I = I_0 \otimes_D \hat{D}$.

Una inclusión es obvia. Por otra parte, todo elemento de $\hat{D}$ es congruente módulo π^n con un elemento de D, de donde se sigue fácilmente que

$$I = I_0 + \pi^n(A \otimes_D \hat{D}) \subset I_0 \otimes_D \hat{D}.$$

Con la notación empleada en el 5.17, lo que tenemos es que $\mathcal{I} = \mathcal{I}_0\mathcal{O}_{\hat{Y}}$. El apartado c) de dicho teorema (aplicado al homomorfismo π, que es plano) nos da la conclusión. ∎

Abordamos ahora la existencia de desingularizaciones de superficies fibradas en el caso local:

Teorema 6.34 *Sea D un anillo de valoración discreta y X/D una superficie fibrada. Sean K y $\hat{K}$ los cuerpos de cocientes de D y $\hat{D}$, respectivamente, sea $\hat{X} = X \times_D \operatorname{Esp}\hat{D}$ y sea $p : \hat{X} \longrightarrow X$ la proyección.*

a) p induce un isomorfismo entre las fibras cerradas de $\hat{X}$ y X.

b) Si $x \in X$ pertenece a la fibra cerrada, entonces $\hat{\mathcal{O}}_{\hat{X},p^{-1}(x)} \cong \hat{\mathcal{O}}_{X,x}$.

c) Si la fibra genérica X_K es regular y X admite una desingularización, entonces $X_{\hat{K}}$ es regular.

d) Si $X_{\hat{K}}$ es regular, entonces X admite una desingularización estricta.

DEMOSTRACIÓN: a) Esto se debe a que si $\mathfrak{m}$ es el ideal maximal de D, entonces $\mathfrak{m}\hat{D}$ es el ideal maximal de $\hat{D}$ y $D/\mathfrak{m} \cong \hat{D}/\mathfrak{m}\hat{D}$. Por lo tanto,

$$\hat{X}_{\mathfrak{m}\hat{D}} = X \times_D \operatorname{Esp}\hat{D} \times_{\hat{D}} \operatorname{Esp}(\hat{D}/\mathfrak{m}\hat{D}) \cong X \times_D \operatorname{Esp}(D/\mathfrak{m}D) = X_{\mathfrak{m}}.$$

b) Tomemos un entorno afín $U = \operatorname{Esp} A$ de x, que se identifica con un ideal primo $\mathfrak{p}$ de A tal que $\pi \in \mathfrak{p}$ (donde π es un primo de D). Sea $\mathfrak{P} \in \operatorname{Esp}(A \otimes_D \hat{D})$ su única antiimagen en $\hat{X}$. Claramente,

$$A/(\pi^n) \cong A \otimes_D D/(\pi^n) \cong (A \otimes_D \hat{D}) \otimes_{\hat{D}} \hat{D}/(\pi^n) \cong (A \otimes_D \hat{D})/(\pi^n).$$

Además, el isomorfismo no es sino el homomorfismo inducido por la inclusión $A \longrightarrow A \otimes_D \hat{D}$. Por lo tanto, $\mathfrak{p}/(\pi^n)$ se corresponde con $\mathfrak{P}/(\pi^n)$. Localizando obtenemos que

$$A_{\mathfrak{p}}/(\pi^n) \cong (A \otimes_D \hat{D})_{\mathfrak{P}}/(\pi^n).$$

Equivalentemente,

$$\mathcal{O}_{X,x}/(\pi^n) \cong \mathcal{O}_{\hat{X},p^{-1}(x)}/(\pi^n).$$

Dividiendo entre $\mathfrak{m}_x^n/(\pi^n)$ y el ideal correspondiente a través del isomorfismo, concluimos que

$$\mathcal{O}_{X,x}/\mathfrak{m}_x^n \cong \mathcal{O}_{\hat{X},p^{-1}(x)}/\mathfrak{m}_{p^{-1}(x)}^n.$$

Tomando límites inversos obtenemos el isomorfismo entre las compleciones.

c) Sea $Z \longrightarrow X$ una desingularización y llamemos $\hat{Z} = Z \times_D \operatorname{Esp}\hat{D}$. Tomemos un punto $z \in Z_{\hat{K}} \subset \hat{Z}$. Como $\hat{Z}/\hat{D}$ es propio, $\overline{\{z\}}$ corta a la fibra cerrada, cuyos puntos son regulares en $\hat{Z}$ por b) (aplicado a Z) y [AC 5.11]. Esto implica a su vez que z es regular en $\hat{Z}$, luego también en el abierto $Z_{\hat{K}}$. Así pues, $Z_{\hat{K}}$ es regular.

Por otra parte, tenemos un homomorfismo birracional $Z_K \longrightarrow X_K$ entre curvas proyectivas regulares, luego es un isomorfismo, luego también $X_{\hat{K}} \cong Z_{\hat{K}}$, luego $X_{\hat{K}}$ es regular.

d) Si $U \subset X$ es un abierto afín, entonces

$$\mathcal{O}_X(U) \otimes_D \hat{D} \subset \mathcal{O}_X(U) \otimes_D \hat{K} = \mathcal{O}_{X_{\hat{K}}}(U_{\hat{K}}).$$

Como $X_{\hat{K}}$ es reducido, concluimos que $\hat{X}$ también lo es. Por otra parte, las fibras de $\hat{X}/\hat{D}$ tienen dimensión 1, la fibra cerrada por a) y la fibra genérica porque es una extensión de constantes de la curva X_K ([AC 3.77]). El teorema [E 4.52] nos da entonces que $\dim \hat{X} = 2$. Ciertamente, $\hat{X}/\hat{D}$ es proyectivo y el anillo $\hat{D}$ es excelente, luego podemos aplicar el teorema 6.31, según el cual la sucesión canónica está definida para $\hat{X}$ y da lugar a una desingularización.

Consideremos la normalización $\hat{X}_1 \longrightarrow \hat{X}$. Por hipótesis, la fibra genérica de $\hat{X}$ es regular, luego la normalización es un isomorfismo sobre su antiimagen en $\hat{X}_1$. Puesto que la fibra cerrada es $V(\pi\mathcal{O}_{\hat{X}})$ (donde π es un primo de D),

el teorema 6.32 nos da que la normalización es una explosión con centro en un subesquema cerrado de soporte $V(\pi\mathcal{O}_{\hat{X}})$.

El teorema 6.33 nos da que $\hat{X}_1 \longrightarrow \hat{X}$ se obtiene por cambio de base a partir de una explosión $X_1 \longrightarrow X$ cuyo lugar excepcional está contenido en la fibra cerrada de X_1. En particular, tenemos un diagrama conmutativo

$$\begin{array}{ccc} \hat{X}_1 & \longrightarrow & \hat{X} \\ \downarrow & & \downarrow \\ X_1 & \longrightarrow & X \end{array}$$

Por a), las flechas verticales se restringen a isomorfismos sobre las fibras cerradas y, como la flecha horizontal superior es un homomorfismo finito, concluimos que las fibras de la flecha inferior también son finitas (para puntos de la fibra genérica de X es trivial, pues sus fibras constan de un único punto). Según 5.19, la explosión $X_1 \longrightarrow X$ es proyectiva, luego por [E A.22] es finita.

Los homomorfismos locales asociados a $\hat{X}_1 \longrightarrow X_1$ son fielmente planos, luego los teoremas 3.43 y 1.18 nos dan que X_1 es normal. (Tal y como se señala en la prueba del primero, la implicación que estamos usando no usa la hipótesis de suavidad.)

En resumen, concluimos que $X_1 \longrightarrow X$ es la normalización de X. Más aún, es claro que X_1/D es una superficie fibrada normal. Vamos a probar que su conjunto de puntos regulares es abierto (y notemos que el mismo argumento vale para X en lugar de X_1). Según 3.26 basta probar que cada subesquema cerrado íntegro $Y \subset X_1$ contiene un abierto regular.

Si Y corta a la fibra genérica de X_1, entonces Y_K es un conjunto algebraico íntegro y es abierto en Y, luego contiene un abierto de puntos regulares que también será abierto en Y. En caso contrario Y está contenido en la fibra cerrada de X_1, luego es un conjunto algebraico sobre $k(\pi)$ y también contiene un abierto regular.

Con esto hemos probado que X cumple las condiciones **D1, D2** y **D3** necesarias para construir su sucesión canónica. En particular, esto implica que el conjunto S de los puntos singulares de X_1 es un cerrado finito. Lo mismo vale para el conjunto $\hat{S}$ de los puntos singulares de $\hat{X}_1$. En particular, ambos están contenidos en las fibras cerradas respectivas, luego el apartado b) nos da que ambos conjuntos se corresponden por la proyección $\hat{X}_1 \longrightarrow X_1$. Más precisamente, si llamamos $\hat{\mathcal{J}}$ y $\mathcal{J}$ a los haces de ideales que determinan las fibras cerradas respectivas y $\mathcal{I}$ es el haz de ideales de $\mathcal{O}_{X_1}$ que determina a S con la estructura de subesquema cerrado reducido, entonces, para cada abierto afín U de X, tenemos que

$$\mathcal{O}_{X_1}(U)/\mathcal{J}(U) \longrightarrow \mathcal{O}_{\hat{X}_1}(\hat{U})/\hat{\mathcal{J}}(\hat{U})$$

es un isomorfismo, y transforma el ideal $\mathcal{I}(U)/\mathcal{J}(U)$ en $\mathcal{I}(U)\mathcal{O}_{\hat{X}_1}(\hat{U})/\hat{\mathcal{J}}(\hat{U})$. Como también $\mathcal{O}_{X_1}(U)/\mathcal{I}(U) \cong \mathcal{O}_{\hat{X}_1(\hat{U})}/\mathcal{I}(U)\mathcal{O}_{\hat{X}_1}(\hat{U})$, el cociente de la derecha es re-

ducido, luego concluimos que la estructura de subesquema cerrado reducido en $\hat{S}$ está definida por el haz de ideales $\mathcal{I}\mathcal{O}_{\hat{X}_1}$.

Ahora podemos aplicar 5.17 c), según el cual la explosión $\hat{X}_1'$ de $\hat{X}_1$ con centro $\hat{S}$ se obtiene por cambio de base de la explosión X_1' de X_1 con centro S. En particular, $(X_1')_{\hat{K}} = (\hat{X}_1')_{\hat{K}} \cong (\hat{X}_1)_{\hat{K}} \cong \hat{X}_{\hat{K}} = X_{\hat{K}}$ es regular.

Así pues, X_1' se encuentra en las mismas condiciones que X, luego razonando inductivamente concluimos que está definida la sucesión canónica

$$\cdots \longrightarrow X_3 \longrightarrow X_2 \longrightarrow X_1 \longrightarrow X$$

y que, a través del cambio de base $\operatorname{Esp}\hat{D} \longrightarrow \operatorname{Esp} D$ da lugar a la sucesión canónica de $\hat{X}$. Más aún, hemos visto que $\hat{X}_i$ es regular si y sólo si lo es X_i, luego algún X_i es regular, y el homomorfismo $X_i \longrightarrow X$ es una desingularización estricta de X. ∎

De aquí podemos pasar al caso global:

Teorema 6.35 *Sea X/S una superficie fibrada sobre un esquema de Dedekind S de dimensión 1 y cuya fibra genérica sea regular. Las afirmaciones siguientes son equivalentes:*

a) X admite una desingularización.

b) El conjunto $\operatorname{Reg}(X)$ es abierto y, para cada punto cerrado $s \in S$, la curva $X \times_S \operatorname{Esp}\mathrm{F}(\hat{\mathcal{O}}_{S,s})$ es regular. (Aquí F representa el cuerpo de cocientes.)

c) El conjunto $\operatorname{Sing}(X)$ de los puntos singulares de X está contenido en una unión finita de fibras cerradas $X_{s_1} \cup \cdots \cup X_{s_r}$, y, para cada $i = 1, \ldots, r$, la curva $X \times_S \operatorname{Esp}\mathrm{F}(\hat{\mathcal{O}}_{S,s_i})$ es regular.

Si se cumplen estas condiciones, entonces X admite una desingularización estricta, que además es un homomorfismo proyectivo.

Demostración: Para cada punto cerrado $s \in S$, definimos

$$X_{(s)} = X \times_S \operatorname{Esp}\mathcal{O}_{S,s},$$

que es una superficie fibrada sobre el anillo de valoración discreta $D_s = \mathcal{O}_{S,s}$, y su fibra genérica es $X_{(s)} \times_{D_s} \operatorname{Esp} K = X \times_S \operatorname{Esp} K$, donde $K = K(S)$, luego se trata de la fibra genérica de X, que es regular por hipótesis. Por [E 4.47] sabemos que la fibra cerrada de $X_{(s)}$ es isomorfa a X_s y, más aún, para cada $x \in X_s$ se cumple que $\mathcal{O}_{X_{(s)},x} \cong \mathcal{O}_{X,x}$.

a) $\Rightarrow$ c) Sea $Z \longrightarrow X$ una desingularización. Entonces, la fibra genérica $Z_\eta = Z \times_S \operatorname{Esp}\mathcal{O}_{S,\eta}$ es un esquema regular y $Z_\eta \longrightarrow X_\eta$ es un homomorfismo birracional y suprayectivo entre curvas, luego es la normalización de X_η, luego es un isomorfismo.

Más aún, si $x \in X_\eta$ se corresponde con $z \in Z_\eta$, la desingularización induce un isomorfismo $\mathcal{O}_{Z,z} \cong \mathcal{O}_{Z_\eta,z} \cong \mathcal{O}_{X_\eta,x} \cong \mathcal{O}_{X,x}$. Por [E A.19] concluimos que x

tiene un entorno isomorfo a un entorno de z, en particular regular, luego existe un abierto regular $U \subset X$ que contiene a X_η o, equivalentemente, el conjunto $\mathrm{Sing}(X)$ de los puntos singulares de X está contenido en un cerrado C cuya proyección en S no contiene a η, luego es finita. En otros términos, $\mathrm{Sing}(X)$ está contenido en una unión finita de fibras cerradas.

Notemos ahora que $Z_{(s_i)} \longrightarrow X_{(s_i)}$ es una desingularización de X_{s_i}, pues obviamente es un homomorfismo propio y birracional, y los anillos locales del esquema $Z_{(s_i)}$ (correspondientes a puntos cerrados) también son anillos locales de Z, luego son regulares. Ahora basta aplicar el teorema anterior (apartado c) a $X_{(s_i)}$.

c) $\Rightarrow$ b) Vamos a probar que todo punto regular $x \in X$ tiene un entorno de puntos regulares. Esto es trivial salvo si $x \in X_{s_i}$, para cierto i. En tal caso basta probar que x tiene un entorno en X_{s_i} de puntos regulares en X. Consideremos nuevamente las superficies $X_{(s_i)}$. Dado que un punto de X_{s_i} es regular en X si y sólo si lo es en $X_{(s_i)}$, basta probar que $\mathrm{Reg}(X_{(s_i)})$ es abierto.

Tomando un entorno de un punto arbitrario, podemos suponer que $X_{(s_i)}$ es afín, y entonces podemos aplicar el teorema 3.26, con lo que basta probar que todo subesquema cerrado íntegro $Y \subset X_{(s_i)}$ contiene un abierto regular. Esto es cierto para $Y = X_i$ sin más que considerar la fibra genérica, que es abierta. Si $Y \subsetneq X_{(s_i)}$, o bien Y corta a la fibra genérica, en cuyo caso Y_η es un conjunto algebraico íntegro abierto en Y, luego contiene un abierto de puntos regulares, o bien Y está contenido en la fibra cerrada de $X_{(s_i)}$, con lo que es un conjunto algebraico sobre $k(s_i)$, y también contiene un abierto regular.

Sea ahora $s \in S$ tal que $X_s \subset \mathrm{Reg}(X)$. Entonces $X_{(s)}$ es regular, luego admite trivialmente una desingularización, luego el teorema 6.34 nos da que el esquema $X \times_S \mathrm{Esp}\,\mathrm{F}(\hat{\mathcal{O}}_{S,s})$ es regular.

b) $\Rightarrow$ a) Sea $f : X_1 \longrightarrow X$ la normalización de X. La fibra genérica de X_1 es normal (porque sus anillos locales son también anillos locales de X_1), luego $X_{1\eta} \cong X_\eta$. Similarmente, para cada $s \in S$, el homomorfismo $f_s : X_{1(s)} \longrightarrow X_{(s)}$ es la normalización del cambio de base. (Se sigue fácilmente de 3.12.) Como la fibra genérica de $X_{(s)}$ es la misma que la de X, podemos aplicar el teorema anterior. En la prueba del apartado d) hemos visto que f_s es finito, y de aquí se sigue a su vez que f también lo es, pues, para cada $x' \in X_{1,s}$, el homomorfismo $\mathcal{O}_{X,f(x')} \longrightarrow \mathcal{O}_{X_1,x'}$ inducido por f se corresponde con el inducido por f_s a través de los isomorfismos dados por el teorema [E 3.47].

En particular, los teoremas [E 5.48] y [E 5.52] nos dan que X_1/S es un esquema proyectivo, luego es una superficie fibrada, y también es proyectiva la normalización $X_1 \longrightarrow X$.

Notemos que $\mathrm{Sing}(X)$ está contenido en una unión finita de fibras cerradas, pues su proyección en S es un cerrado que no contiene al punto genérico. Si la fibra X_s es regular, entonces $X_{(s)}$ es regular, luego f_s es un isomorfismo, luego la fibra $X_{1,s}$ también es regular. En suma, $\mathrm{Sing}(X_1)$ está contenido también en una unión finita de fibras cerradas.

Más aún, $X_{(s)}$ tiene un abierto de puntos regulares, luego lo mismo le sucede a $X_{1(s)}$, luego cada fibra de X_1 tiene a lo sumo un número finito de puntos singulares, luego $\mathrm{Sing}(X_1)$ es un cerrado finito.

Con esto hemos probado que X cumple las condiciones **D1, D2** y **D3** para construir la sucesión canónica. Así pues, ahora consideramos la explosión $X_1' \longrightarrow X_1$ de centro $\mathrm{Sing}(X_1)$ (que es proyectiva por el teorema 5.19, luego X_1' es una superficie fibrada). Como es un isomorfismo sobre la antiimagen de $\mathrm{Reg}(X_1)$, en particular induce un isomorfismo sobre las fibras genéricas, luego la fibra genérica de X_1' es regular. También es obvio que $\mathrm{Sing}(X_1')$ está contenido en una unión finita de fibras cerradas, luego, por la implicación anterior, $\mathrm{Reg}(X_1')$ es abierto.

Por otra parte, el homomorfismo $X_1' \times_S \mathrm{Esp}\,\mathrm{F}(\hat{\mathcal{O}}_{S,s}) \longrightarrow X \times_S \mathrm{Esp}\,\mathrm{F}(\hat{\mathcal{O}}_{S,s})$ es un isomorfismo, ya que se obtiene por cambio de base del isomorfismo entre las fibras genéricas. En suma, hemos probado que X_1' cumple las mismas hipótesis que X_1. Tenemos además el diagrama conmutativo siguiente:

$$\begin{array}{ccccc} X'_{1(s)} & \longrightarrow & X_{1(s)} & \longrightarrow & X_{(s)} \\ \downarrow & & \downarrow & & \downarrow \\ X_1' & \longrightarrow & X_1 & \longrightarrow & X \end{array}$$

donde la fila superior es la explosión del conjunto de puntos singulares seguida de la normalización. Esto es consecuencia del teorema 5.17 c), ya que si $\mathcal{I}$ es el haz de ideales que define la estructura de subesquema cerrado reducido en $\mathrm{Sing}(X_1)$, entonces $\mathcal{I}\mathcal{O}_{X_{1(s)}}$ define la estructura de subesquema cerrado reducido en $\mathrm{Sing}(X_{1(s)})$. Esto a su vez se debe a que, si $S = \mathrm{Esp}\,D$, s se corresponde con un ideal maximal $\mathfrak{p}$ de D y U es un abierto afín de X_1, entonces $\mathcal{I}(U)_{\mathfrak{p}}$ es claramente un ideal radical de $\mathcal{O}_{X_1}(U)_{\mathfrak{p}}$ cuyos primos minimales se corresponden con los primos minimales de $\mathcal{I}(U)$ en la fibra de $\mathfrak{p}$.

Razonando inductivamente, vemos que está definida la sucesión canónica

$$\cdots \longrightarrow X_2 \longrightarrow X_1 \longrightarrow X,$$

cuyos homomorfismos son proyectivos y que la sucesión canónica de $X_{(s)}$ se obtiene de ésta por cambio de base.

Además, para un n suficientemente grande resulta que $X_{n(s)}$ es regular, para todo punto cerrado $s \in S$ (ya que esto es trivial salvo para un número finito de puntos $s \in S$, aquellos cuya fibra no es regular). Esto implica a su vez que X_n es regular, con lo que el homomorfismo (proyectivo) $X_n \longrightarrow X$ es una desingularización estricta de X. ∎

En particular tenemos el teorema siguiente:

Teorema 6.36 *Si X/S es una superficie fibrada (donde $\dim S = 1$) cuya fibra genérica sea geométricamente regular, entonces X admite una desingularización.*

Demostración: Los puntos de la fibra genérica (vistos como puntos de X) son suaves y, por el teorema [E A.34], el conjunto de los puntos suaves de X es abierto, luego la proyección en S de su complementario es un cerrado que no contiene al punto genérico, luego es finito.

Esto prueba que el conjunto de los puntos de X que no son suaves (en particular $\mathrm{Sing}(X)$) está contenido en una unión finita de fibras. Si X_{s_i} es una de ellas, la curva $X \times_S \mathrm{Esp}\,\mathrm{F}(\hat{\mathcal{O}}_{S,s_i})$ se obtiene por cambio de base de la fibra genérica de X, luego es regular, y se cumple la condición c) del teorema anterior. ∎

Observemos que si una superficie fibrada X/S (sobre un esquema de Dedekind de dimensión 1) admite una desingularización, el teorema 6.35 nos da que tiene una desingularización estricta $X' \longrightarrow X$ que es un homomorfismo proyectivo, de modo que X'/S es una superficie aritmética. Ahora podemos demostrar un teorema general sobre existencia de modelos de curvas:

Teorema 6.37 *Sea D un dominio de Dedekind con cuerpo de cocientes K y sea $S = \mathrm{Esp}\,D$. Entonces, toda curva proyectiva íntegra geométricamente regular C/K tiene al menos un modelo regular sobre S.*

Demostración: Podemos representar a C en la forma

$$C = \mathrm{Proy}(K[X_0, \ldots, X_n]/(F_1, \ldots, F_m)),$$

donde los F_i son polinomios homogéneos con coeficientes en K. Multiplicándolos por elementos adecuados de D podemos exigir que todos los F_i tengan sus coeficientes en D. Consideremos ahora el esquema

$$\mathcal{C}_0 = \mathrm{Proy}(D[X_0, \ldots, X_n]/(F_1, \ldots, F_m)).$$

Claramente es un esquema proyectivo sobre S. Por el teorema [E 3.49], su fibra genérica es

$$\mathcal{C}_{0,\eta} = C_0 \times_D \mathrm{Esp}\,K = C.$$

Sea $\mathcal{C}$ la clausura de $\mathcal{C}_{0,\eta}$ en $\mathcal{C}$, dotada de la estructura de subesquema cerrado reducido. Como $\mathcal{C}_{0,\eta}$ es irreducible, también lo es su clausura, luego $\mathcal{C}/S$ es un esquema íntegro proyectivo, y sigue siendo cierto que $\mathcal{C}_\eta = C$ (porque tenemos una inmersión cerrada suprayectiva $\mathcal{C}_\eta \longrightarrow \mathcal{C}_{0,\eta} = C$).

En particular tenemos que $\mathcal{C}_\eta \neq \varnothing$, luego la imagen del homomorfismo estructural $\mathcal{C} \longrightarrow S$ es densa, luego el teorema [E 4.54] implica que $\mathcal{C}$ es plano sobre S y, aplicando 3.9 a la fibra genérica, concluimos que $\dim \mathcal{C}_0 = 2$. Por consiguiente, $\mathcal{C}/S$ es una superficie fibrada. Por el teorema 6.36, admite una desingularización $\mathcal{C}_r$, que es un modelo regular de C/K. ∎

Capítulo VII

Superficies minimales

Es bien conocido que toda curva proyectiva íntegra C/k es birracionalmente equivalente a una curva proyectiva regular (su normalización), y que dos curvas proyectivas regulares birracionalmente equivalentes son isomorfas (por [E 7.6]), de modo que, en definitiva, cada curva proyectiva íntegra C/k es birracionalmente equivalente a una única curva proyectiva regular C'/k. Así, en cierta medida, la geometría de C/k puede estudiarse a través de la geometría de C/k. Si en lugar de curvas consideramos superficies fibradas, la situación es más compleja.

En el capítulo anterior hemos visto que también es cierto que, en el caso aritmético $\dim S = 1$, toda superficie fibrada X/S (cuya fibra genérica sea geométricamente regular) es birracionalmente equivalente a una superficie aritmética, aunque, para obtener esta generalización, hemos tenido que sustituir el concepto de normalización por el de desingularización, pues la normalización de una superficie fibrada no tiene por qué ser regular.

En este capítulo generalizaremos al contexto de las superficies aritméticas el hecho de que dos curvas proyectivas regulares birracionalmente equivalentes son isomorfas, pero la generalización no puede ser la obvia: dos superficies aritméticas birracionalmente equivalentes no son necesariamente isomorfas. Para comprobarlo basta considerar el teorema 5.25: si X/S es una superficie aritmética y $\widetilde{X}/S$ es la explosión de X con centro en un punto cerrado $x \in X_s$, entonces $\widetilde{X}/S$ es otra superficie aritmética birracionalmente equivalente a X cuya fibra $\widetilde{X}_s$ tiene una componente irreducible más, luego no es isomorfa a X.

Lo que haremos aquí será definir el concepto de superficie aritmética minimal, de modo que seguirá siendo cierto que toda superficie fibrada puede desingularizarse hasta una superficie aritmética minimal y —ahora sí— dos superficies aritméticas minimales birracionalmente equivalentes son isomorfas.

En particular, cada superficie fibrada será birracionalmente equivalente a una única superficie aritmética minimal, y así, la conclusión será que el concepto análogo en dimensión 2 al de una curva proyectiva regular no es el de una mera superficie aritmética, sino el concepto de superficie aritmética minimal.

7.1 Equivalencia birracional de superficies

La definición de equivalencia birracional entre superficies, o incluso entre esquemas íntegros arbitrarios, es la generalización obvia de la definición para curvas:

Definición 7.1 Se dice que dos esquemas íntegros X/S e Y/S son *birracionalmente equivalentes* si existe una aplicación birracional $f : X \longrightarrow Y$ (definida sobre S) o, equivalentemente, si contienen abiertos isomorfos (sobre S) no vacíos.

Según acabamos de observar, si S es un esquema de Dedekind afín de dimensión 1, toda superficie fibrada X/S cuya fibra sea geométricamente regular es birracionalmente equivalente a una superficie aritmética, y el problema que nos queda pendiente es estudiar la relación que podemos encontrar entre distintas superficies aritméticas birracionalmente equivalentes. Para ello conviene introducir el preorden siguiente:

Si X/S e Y/S son superficies birracionalmente equivalentes, diremos que X *domina* a Y (y lo representaremos por $Y \preceq X$) si existe un homomorfismo birracional[1] $X \longrightarrow Y$ definido sobre S.

Esta notación es útil para asimilar los conceptos que vamos a introducir, pero debe ser tomada con cierta cautela: obviamente, la relación $Y \preceq X$ es reflexiva y transitiva, pero no es antisimétrica, ni siquiera en el sentido amplio de que si $Y \preceq X$ y $X \preceq Y$, entonces $X \cong Y$.

En estos términos, nuestro objetivo es demostrar que (bajo ciertas hipótesis) en cada clase de equivalencia birracional de superficies aritméticas existe una superficie "minimal" Y/S, única salvo isomorfismo, que cumple que $Y \preceq X$ para toda superficie Y en su misma clase.[2]

Veamos que las clases de equivalencia birracional de superficies aritméticas coinciden con las clases de modelos regulares de curvas. Para ello necesitamos demostrar una variante del teorema [E A29]:

Teorema 7.2 *Sean X/S, Y/S dos esquemas íntegros, separados, de tipo finito sobre un esquema localmente noetheriano S y fijemos un punto $s \in S$. Para cada homomorfismo $\phi : X \times_S \operatorname{Esp} \mathcal{O}_{S,s} \longrightarrow Y \times_S \operatorname{Esp} \mathcal{O}_{S,s}$ definido sobre S existe un entorno abierto U de s y un único homomorfismo $f : X \times_S U \longrightarrow Y \times_S U$ definido sobre S tal que ϕ se obtiene de f por cambio de base. Si ϕ es un isomorfismo, también lo es f.*

Demostración: Podemos sustituir S por un entorno afín de s y suponer que $S = \operatorname{Esp} D$ es afín. Observemos que los abiertos de la forma $W \times_S \operatorname{Esp} \mathcal{O}_{S,s}$, donde W es un abierto afín de X, forman una base de $X \times_S \operatorname{Esp} \mathcal{O}_{S,s}$. En

[1] Notemos que hablamos de un homomorfismo birracional y no una mera aplicación birracional, es decir, exigimos que X e Y sean birracionalmente equivalentes a través de una aplicación birracional definida sobre todo el esquema X.

[2] En realidad la definición de superficie minimal será ligeramente más fuerte que ésta. Más adelante daremos los detalles.

efecto, dado un abierto $W' \subset X \times_S \operatorname{Esp} \mathcal{O}_{S,s}$ y un punto $x \in W'$, tomamos un entorno afín de x de la forma $W'' = W_0 \times_S \operatorname{Esp} \mathcal{O}_{S,s}$, donde $W_0 = \operatorname{Esp} A$ es un abierto afín en X. Entonces existe un abierto principal $W''' \subset W''$ tal que $x \in W''' \subset W' \cap W''$. Ahora bien, si s se corresponde con un ideal $\mathfrak{p}$ de D, entonces $W'' = \operatorname{Esp} A_{\mathfrak{p}}$, y es claro que W''' ha de ser de la forma $\operatorname{Esp}(A_u)_{\mathfrak{p}}$, para cierto $u \in A$, es decir, de la forma $W''' = W \times \operatorname{Esp} \mathcal{O}_{S,s}$, donde $W = \operatorname{Esp} A_f$ es un abierto principal en W.

Cubrimos Y con un número finito de abiertos afines V. Para cada uno de estos abiertos, cubrimos $\phi^{-1}[V \times_S \operatorname{Esp} \mathcal{O}_{S,s}]$ con un número finito de abiertos $W \times_S \operatorname{Esp} \mathcal{O}_{S,s}$, y consideramos las restricciones

$$W \times_S \operatorname{Esp} \mathcal{O}_{S,s} \longrightarrow V \times_S \operatorname{Esp} \mathcal{O}_{S,s}.$$

Por [E A29] existe un abierto afín $s \in U \subset S$ tal que estos homomorfismos están inducidos por homomorfismos (unívocamente determinados)

$$f_{(V,W)} : W \times_S U \longrightarrow V \times_S U.$$

Reduciendo U, podemos suponer que es el mismo entorno de s para todos los pares (W, V). Si V y V' son dos de los abiertos, tomamos un abierto afín (no vacío) $V'' \subset V \cap V'$ y formamos el correspondiente homomorfismo $f_{(W'',V'')} : W'' \times_S U' \longrightarrow V'' \times_S U'$, donde podemos suponer que $W'' \subset W \cap W'$ y $U' \subset U$. Por la unicidad, éste ha de coincidir con las restricciones de $f_{(V,W)}$ y $f_{(V',W')}$, con lo que estos dos homomorfismos coinciden en un abierto y, por consiguiente, coinciden en la intersección de sus dominios. Esto prueba que todos ellos determinan un homomorfismo $f : X \times_S U \longrightarrow Y \times_S U$.

Si ϕ es un isomorfismo, el inverso de ϕ nos permite construir el homomorfismo inverso de f. ∎

Como consecuencia inmediata:

Teorema 7.3 *Dos superficies aritméticas son birracionalmente equivalentes si y sólo si sus fibras genéricas son isomorfas.*

Demostración: Sean X/S e Y/S dos superficies aritméticas. Es claro que una aplicación birracional $X \longrightarrow Y$ induce una aplicación birracional $X_\eta \longrightarrow Y_\eta$, luego las fibras genéricas son dos curvas proyectivas regulares birracionalmente equivalentes, luego son isomorfas.

Recíprocamente, un isomorfismo entre las fibras genéricas es un isomorfismo

$$X \times_S \operatorname{Esp} \mathcal{O}_{S,\eta} \longrightarrow Y \times_S \operatorname{Esp} \mathcal{O}_{S,\eta},$$

y el teorema anterior nos da un isomorfismo

$$X \times_S U \longrightarrow Y \times_S U,$$

que, a través de los isomorfismos $X \times_S S \cong X$, $Y \times_S S \cong Y$, se convierte en un isomorfismo entre abiertos respectivos en X e Y. Por consiguiente, ambas superficies son birracionalmente equivalentes. ∎

En otros términos, acabamos de probar que dos modelos regulares de una misma curva son birracionalmente equivalentes, y que, si a partir de un modelo regular construimos otra superficie aritmética birracionalmente equivalente, su fibra genérica será la misma, luego será un modelo regular de la misma curva.

7.2 Superficies relativamente minimales

Consideremos una superficie aritmética X/S y vamos a abordar el problema de si existe otra superficie aritmética Y/S no isomorfa a X tal que $Y \preceq X$, es decir, tal que exista un homomorfismo birracional $X \longrightarrow Y$, que no podrá ser un isomorfismo. En tal caso, el teorema 6.24 nos permite descomponerlo en una cadena

$$X = X_0 \longrightarrow X_1 \longrightarrow \cdots \longrightarrow X_{n-1} \longrightarrow X_n = Y$$

de explosiones de puntos cerrados. Aplicando el teorema 5.25 de derecha a izquierda obtenemos inductivamente que todos los esquemas intermedios son superficies aritméticas.

Así pues, si existe un homomorfismo birracional $X \longrightarrow Y$ que no sea un isomorfismo, donde Y es una superficie aritmética, entonces existe otro (el que resulta de cambiar Y por el X_1 de la sucesión anterior) que es la explosión con centro en un punto cerrado $y \in Y$

El teorema 5.25 nos dice que $X \longrightarrow Y$ tiene una única fibra no trivial, que es una curva $P \cong \mathrm{P}^1_{k(y)}$. En términos de la definición 6.26, tenemos que Y es la contracción de P a un punto (regular). Esto nos lleva a la definición siguiente:

Definición 7.4 Sea X/S una superficie fibrada regular. Un divisor primo regular E en X es un *divisor excepcional* si existe una superficie fibrada regular Y/S y un homomorfismo $f : X \longrightarrow Y$ definido sobre S tal que $f[E]$ se reduzca a un punto y $f : X \setminus E \longrightarrow Y \setminus f[E]$ sea un isomorfismo.

En otras palabras, E es excepcional si puede contraerse a un punto regular $p = f[E]$. Notemos que en tal caso E es el lugar excepcional de f, luego el teorema 6.25 nos da que f es la explosión de centro p.

Hemos probado que si X/S es una superficie aritmética y existe una superficie aritmética $Y \preceq X$ no isomorfa a X, entonces X contiene un divisor excepcional. Recíprocamente, si X contiene un divisor excepcional $E \subset X_s$, su contracción $X \longrightarrow Y$ nos da una superficie aritmética no isomorfa a X, pues la fibra Y_s contiene una componente irreducible menos que X_s. Esto nos lleva a otra definición:

Definición 7.5 Una superficie aritmética X/S es *relativamente minimal* si no contiene ningún divisor excepcional.

En estos términos, hemos visto que una superficie aritmética X/S es relativamente minimal si y sólo si, para toda superficie aritmética Y, se cumple que todo homomorfismo birracional $X \longrightarrow Y$ es un isomorfismo, lo cual es casi lo

mismo (pero no exactamente lo mismo) que la afirmación siguiente: Si $Y \preceq X$ entonces $Y \cong X$.

El teorema siguiente nos permitirá reconocer fácilmente las superficies relativamente minimales:

Teorema 7.6 *Sean X/S e Y/S superficies fibradas regulares, sea $f : X \longrightarrow Y$ la explosión de Y con centro un punto cerrado $y \in Y$, sea $E = X_y$ y sea $s \in S$ la imagen de y. Entonces $E \cong \mathrm{P}^1_{k(y)}$, $k(y) = \mathcal{O}_E(E)$, $\mathcal{O}_X(E)|_E \cong \mathcal{O}_E(-1)$ y $E^2 = -|k(y) : k(s)|$.*

Demostración: El isomorfismo $E \cong \mathrm{P}^1_{k(y)}$ nos lo da el teorema 5.25, y esto implica que $\mathcal{O}_E(E) = k(y)$. Por 6.10 sabemos que $\mathcal{O}_X(E)|_E \cong \omega_{E/X}$, luego hemos de probar que $\omega_{E/X} \cong \mathcal{O}_E(-1)$.

Sea $V = f^{-1}[U]$, donde U es un entorno afín de y. Entonces $\omega_{V/X}$ es trivial, por lo que $\omega_{E/X} = \omega_{E/V}$. Por consiguiente, no perdemos generalidad si suponemos que Y es afín (aunque entonces ya no es una superficie fibrada, lo que tenemos es que f es la explosión de una superficie íntegra regular con centro en un punto cerrado).

Pongamos que $Y = \operatorname{Esp} A$ y que y se corresponde con un ideal maximal I (o, equivalentemente, con el haz de ideales $\mathcal{I} = \tilde{I}$). Entonces

$$X = \operatorname{Proy} \bigoplus_{d\geq 0} I^d,$$

mientras que $\mathcal{J} = \mathcal{I}\mathcal{O}_X = \mathcal{O}_X(1)$ es el haz cuasicoherente asociado al ideal homogéneo

$$J = I \oplus I^2 \oplus I^3 \oplus \cdots \subset A \oplus I \oplus I^2 \oplus \cdots = B$$

El subesquema cerrado de X asociado a este haz (o a este ideal) tiene por soporte E y, concretamente, es

$$E = \operatorname{Proy} \bigoplus_{d\geq 0} (I^d/I^{d+1}).$$

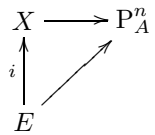
Observemos que los cocientes no se alteran si localizamos todos los ideales respecto de I, con lo que el teorema [AC 5.9] nos da que

$$B/J = \operatorname{gr}_I(A_I) \cong k(y)[X, Y],$$

luego $E \cong \mathrm{P}^1_{k(y)}$, como ya sabíamos. (Lo que hemos obtenido de nuevo es que la representación anterior de E como esquema proyectivo se corresponde con la representación usual de $\mathrm{P}^1_{k(y)}$.) La identidad $(B/J) \otimes_B (J/J^2) \cong (B/J) \otimes_B J$ implica que

$$\mathcal{C}_{E/X} = i^*(\mathcal{J}/\mathcal{J}^2) \cong i^*\mathcal{J} \cong i^*\mathcal{O}_X(1) \cong \mathcal{O}_E(1).$$

El último isomorfismo se debe a que tenemos un diagrama conmutativo



por el que $\mathcal{O}_{\mathrm{P}^n_A}(1)$ se transforma en $\mathcal{O}_X(1)$ y en $\mathcal{O}_E(1)$. Así pues,

$$\omega_{E/X} = \mathcal{C}^*_{E/X} \cong \mathcal{O}_E(-1).$$

Finalmente podemos calcular, según el teorema 6.4

$$E^2 = \operatorname{grad}_{k(s)} \mathcal{O}_E(-1) = |k(y) : k(s)| \operatorname{grad}_{k(y)} \mathcal{O}_E(-1) = -|k(y) : k(s)|.$$

■

Si en el teorema anterior eliminamos toda referencia explícita a la contracción nos queda el enunciado siguiente:

Teorema 7.7 *Si X/S es una superficie fibrada regular, $s \in S$ y $E \subset X_s$ es un divisor excepcional de X y $k' = \mathcal{O}_E(E)$, entonces $E \cong \mathrm{P}^1_{k'}$ y $E^2 = -|k' : k(s)|$.*

Ejemplo La desingularización $\mathcal{X}/\mathbb{Z}_5$ calculada en el ejemplo de la página 144 es relativamente minimal, pues su fibra tiene tres componentes irreducibles, Γ_1, Γ_2 y Γ_3, todas ellas isomorfas a P^1_k (donde $k = \mathbb{Z}/5\mathbb{Z}$). Para que alguna de ellas fuera un divisor excepcional debería cumplir $\Gamma_i^2 = -1$, pero en la página 179 hemos visto que $\Gamma_1^2 = -2$. ■

Ejemplo La desingularización $\mathcal{X}/\mathbb{Z}_2$ que hemos obtenido en la sección 5.4 al desingularizar la ecuación de Selmer es relativamente minimal, pues su fibra cerrada tiene cinco componentes: $\Gamma_1 \cong \Gamma_3 \cong \Gamma_4 \cong \mathrm{P}^1_k$ y $\Gamma_2 \cong \Gamma_5 \cong \mathrm{P}^1_{k'}$, donde $k = \mathbb{Z}/2\mathbb{Z}$ y k' es el cuerpo de cuatro elementos. Para que las tres primeras pudieran ser divisores excepcionales deberían cumplir $\Gamma_1^2 = -1$, mientras que las otras dos deberían cumplir $\Gamma_i^2 = -2$, pero en la página 179 hemos visto que no es así. El lector puede comprobar que la desingularización de la ecuación de Selmer sobre $\mathbb{Z}_3$ también es relativamente minimal. ■

Ejemplo El modelo de Weierstrass $W/\mathbb{Z}$ asociado a la ecuación

$$Y^2 = X^3 + 2X^2 + 6$$

es relativamente minimal. En efecto, en la página 134 hemos visto que es una superficie aritmética, y sus divisores primos son sus fibras cerradas, y todas ellas son curvas elípticas o cúbicas singulares, en cualquier caso, no son isomorfas a rectas proyectivas, luego no pueden ser divisores excepcionales. ■

Veamos un sencillo resultado general:

Teorema 7.8 *Toda superficie aritmética suave es relativamente minimal.*

Demostración: Si X/S es una superficie aritmética suave y E es un divisor vertical, digamos contenido en la fibra X_s, con $s \in S$ (cerrado), entonces $X_s/k(s)$ es geométricamente regular, luego sus componentes irreducibles son disjuntas dos a dos. En particular, el número de intersección de E y cualquier otra componente irreducible de X_s es nulo, luego el teorema 6.7 se reduce a que $E^2 = 0$, luego E no es excepcional. ■

El criterio de Castelnuovo afirma que las condiciones del teorema 7.7 no sólo son necesarias, sino también suficientes para que un divisor sea excepcional. Para probarlo necesitamos algunos resultados previos.

Teorema 7.9 *Sea X un esquema de tipo finito sobre un anillo noetheriano A, sea $f : X \longrightarrow \mathrm{P}^n_A$ un homomorfismo definido sobre A, sea $\mathcal{L} = f^*\mathcal{O}_{\mathrm{P}^n_A}(1)$, sea $s \in \operatorname{Esp} A$ y sea Z un subesquema cerrado conexo de X_s que sea proyectivo sobre $k(s)$. Entonces $f[Z]$ se reduce a un punto si y sólo si $\mathcal{L}|_Z \cong \mathcal{O}_Z$.*

Demostración: Es claro que $\mathcal{L}|_Z = (f|_Z)^*(\mathcal{O}_{\mathrm{P}^n_A}(1))$, luego no perdemos generalidad si suponemos que $X = Z$, con lo que X es una variedad proyectiva reducida y conexa sobre un cuerpo k. Sea $s_0, \ldots, s_n$ el generador global de $\mathcal{L}$ asociado a f según el teorema [E 5.33]. Recordemos que si $\mathrm{P}^n_k = \operatorname{Proy}(k[X_0, \ldots, X_n])$, entonces $s_i = f^*X_i$, y que

$$f^{-1}[D(X_i)] = X_{s_i} = \{x \in X \mid \mathcal{L}_x = s_{i,x}\mathcal{O}_{X,x}\}.$$

Supongamos que $f[X] = \{y\}$. Digamos que, por ejemplo, $y \in D(X_0)$. Entonces $X = X_{s_0}$, luego $\mathcal{L} = s_0\mathcal{O}_X \cong \mathcal{O}_X$. Recíprocamente, supongamos que $\mathcal{L} = e\mathcal{O}_X$, para cierto $e \in \mathcal{L}(X)$. Sea $K = \mathcal{O}_X(X)$. Por el teorema [E 4.26], sabemos que K es un cuerpo de grado finito sobre k.

Pongamos que $s_i = eb_i$, para ciertos $b_i \in K$. Los b_i no pueden ser todos nulos, luego, si llamamos $Y = \operatorname{Esp} K$, son obviamente un generador global de $\mathcal{O}_K$. Sea $g : Y \longrightarrow \mathrm{P}^n_k$ el homomorfismo asociado a los b_i. Por otra parte, la identidad $\mathcal{O}_Y(Y) \longrightarrow \mathcal{O}_X(X)$ induce un homomorfismo $h : X \longrightarrow Y$. La composición $h \circ g : X \longrightarrow \mathrm{P}^n_k$ transforma el haz $\mathcal{O}_{\mathrm{P}^n_k}(1)$ en $\mathcal{O}_X$, y las indeterminadas X_i se corresponden con los elementos b_i. A su vez tenemos un isomorfismo $\mathcal{O}_X \cong \mathcal{L}$ que transforma los b_i en los s_i, luego, por la unicidad del teorema [E 5.33], resulta que $f = h \circ g$. Ahora bien, Y consta únicamente de un punto, luego lo mismo le sucede a la imagen de f. ∎

Con esto podemos dar una condición suficiente (y puede probarse que también es necesaria) para la existencia de la contracción de una familia de curvas:

Teorema 7.10 *Sea X/S una superficie aritmética sobre un esquema de Dedekind afín S de dimensión 1 y sea $D \in \operatorname{Div}_c(X)$ tal que*

a) $\operatorname{grad} \mathcal{O}_X(D)|_{X_\eta} > 0$ *(donde η es el punto genérico de S).*

b) $\mathcal{O}_X(D)$ *tiene un generador global.*

c) Si E es una curva íntegra vertical (proyectiva), entonces $\mathcal{O}_X(D)|_E$ es trivial o bien tiene orden infinito en $\operatorname{Pic}(E)$.

Entonces, si llamamos $\mathcal{E}$ al conjunto de las curvas íntegras proyectivas verticales E tales que $\mathcal{O}_X(D)|_E$ es trivial, existe la contracción de las curvas de $\mathcal{E}$.

Demostración: El teorema 4.8 nos da que el haz $\mathcal{O}_X(D)|_{X_\eta}$ es amplio. Si cambiamos D por una potencia suya, el conjunto $\mathcal{E}$ no cambia, luego podemos suponer que $\mathcal{O}_X(D)|_{X_\eta}$ es muy amplio.

Sea $S = \operatorname{Esp} A$ y sea $f : X \longrightarrow \mathrm{P}^n_A$ el homomorfismo asociado a un generador global de $\mathcal{O}_X(D)$. Como X es proyectiva, la imagen $Z = f[X]$ es cerrada y, si la consideramos como subesquema íntegro de P^n_A, tenemos que f induce un homomorfismo $f : X \longrightarrow Z$ suprayectivo. Tenemos un diagrama conmutativo

$$\begin{array}{ccccc} X & \xrightarrow{f} & Z & \longrightarrow & \mathrm{P}^n_A \\ \uparrow & & \uparrow & & \uparrow \\ X_\eta & \xrightarrow[f_\eta]{} & Z_\eta & \longrightarrow & \mathrm{P}^n_{k(\eta)} \end{array}$$

Es claro que f_η es suprayectivo y es fácil ver que la fila inferior completa es el homomorfismo correspondiente a un generador global de $\mathcal{O}_X(D)|_{X_\eta}$, por lo que es una inmersión cerrada. En definitiva, f_η es un isomorfismo. Por [E 3.47] tenemos que $K(X) \cong K(X_\eta) \cong K(Z_\eta) \cong K(Z)$, luego $f : X \longrightarrow Z$ es un homomorfismo birracional. Como es proyectivo, $f_*\mathcal{O}_X$ es un haz coherente en Z, por [E 6.24].

Consideremos ahora el homomorfismo afín $\pi : Y \longrightarrow Z$ dado por el teorema [E A.5], es decir, el que cumple que $\pi_*\mathcal{O}_Y = f_*\mathcal{O}_X$. Como f es birracional, los anillos de $f_*\mathcal{O}_X$ son subanillos de $K(Z)$ con cuerpo de fracciones $K(Z)$, luego π también es birracional. Más aún, por [E A.8], π es un homomorfismo finito. Además, como X es normal, los anillos de $f_*\mathcal{O}_X$ son íntegramente cerrados, luego Y también es normal. Esto implica que π es la normalización de Z, y por definición de normalización tenemos un diagrama conmutativo

$$\begin{array}{ccc} Y & \xrightarrow{\pi} & Z \\ {\scriptstyle g}\uparrow & \nearrow_{f} & \downarrow \\ X & \longrightarrow & S \end{array}$$

Observemos que Y/S es proyectivo por [E 5.52], luego es una superficie fibrada normal. Sea $E \subset X$ una curva vertical íntegra (proyectiva). Por el teorema anterior sabemos que la imagen $f[E]$ se reduce a un punto si y sólo si $\mathcal{O}_X(D)|_E \cong \mathcal{O}_E$, es decir, si y sólo si $E \in \mathcal{E}$. Ahora bien, como π es finito, $f[E]$ se reduce a un punto si y sólo si $g[E]$ se reduce a un punto. Por consiguiente, g es la contracción de las curvas de $\mathcal{E}$. ∎

Observemos ahora un hecho elemental:

Teorema 7.11 *Sea X un esquema localmente noetheriano y D, $E \in \operatorname{Div}_c(X)$ dos divisores, el segundo entero. Entonces existe una sucesión exacta*

$$0 \longrightarrow \mathcal{O}_X(D) \longrightarrow \mathcal{O}_X(DE) \longrightarrow i_*(\mathcal{O}_X(DE)|_E) \longrightarrow 0,$$

donde $i : E \longrightarrow X$ es la inmersión natural.

Demostración: Partimos de la sucesión exacta

$$0 \longrightarrow \mathcal{O}_X(E^{-1}) \longrightarrow \mathcal{O}_X \longrightarrow i_*\mathcal{O}_E \longrightarrow 0.$$

Como el haz $\mathcal{O}_X(DE)$ es localmente libre, al multiplicar por $\otimes_{\mathcal{O}_X}\mathcal{O}_X(DE)$ obtenemos la sucesión exacta del enunciado. ∎

Teorema 7.12 *Sea X/S una superficie fibrada regular, sea $s \in S$ un punto cerrado y E un divisor primo contenido en la fibra X_s. Supongamos además que $E \cong \mathrm{P}^1_{k'}$, para cierto cuerpo k', finito sobre $k(s)$, así como que $E^2 < 0$. Sea $H \in \mathrm{Div}_c(X)$ un divisor entero tal que $H^1(X, \mathcal{O}_X(H)) = 0$. Entonces:*

a) Si $r = H \cdot E/(-E^2)$, entonces $H^1(X, \mathcal{O}_X(HE^i)) = 0$, para $0 \le i \le r$.

b) Si $\mathcal{O}_X(H)$ tiene un generador global y r es entero, entonces $\mathcal{O}_X(HE^r)$ tiene también un generador global y $\mathcal{O}_X(HE^r)|_E \cong \mathcal{O}_E$.

Demostración: Probamos a) por inducción sobre i. El caso $i = 0$ es la hipótesis del teorema. Si es cierto para $i \le r-1$, tenemos que

$$m = \mathrm{grad}_{k(s)}\, \mathcal{O}_X(HE^{i+1})|_E = (HE^{i+1}) \cdot E = (r-(i+1))(-E^2) \ge 0,$$

y, como $\mathcal{O}_X(HE^{i+1})|_E \cong \mathcal{O}_E(m')$ (donde $m = |k' : k(s)|m'$), el teorema [E 6.19] nos permite concluir que $H^1(E, \mathcal{O}_X(HE^{i+1})|_E) = 0$. Por otra parte, el teorema anterior nos da una sucesión exacta

$$0 \longrightarrow \mathcal{O}_X(HE^i) \longrightarrow \mathcal{O}_X(HE^{i+1}) \longrightarrow i_*(\mathcal{O}_X(HE^{i+1})|_E) \longrightarrow 0,$$

de la que, teniendo en cuenta [E 6.20], obtenemos la sucesión exacta de cohomología

$$0 = H^1(X, \mathcal{O}_X(HE^i)) \longrightarrow H^1(X, \mathcal{O}_X(HE^{i+1})) \longrightarrow 0.$$

Así pues, $H^1(X, \mathcal{O}_X(HE^{i+1})) = 0$.

Para probar b) observamos que $(HE^r) \cdot E = 0$, luego $\mathrm{grad}\, \mathcal{O}_X(HE^r)|_E = 0$, y esto implica que $\mathcal{O}_X(HE^r)|_E \cong \mathcal{O}_E$ (por [E 8.18]). En particular, $\mathcal{O}_X(HE^r)|_E$ tiene un generador global. Además, la sucesión exacta anterior para $i = r-1$ nos da la sucesión exacta de cohomología

$$H^0(X, \mathcal{O}_X(HE^r)) \longrightarrow H^0(E, \mathcal{O}_X(HE^r)|_E) \longrightarrow H^1(X, \mathcal{O}_X(HE^{r-1})) = 0.$$

Podemos tomar, pues, un $t \in \mathcal{O}_X(HE^r)(X)$ cuya imagen en $\mathcal{O}_X(HE^r)|_E(E)$ sea un generador global. Así, si $P \in E$, tenemos que el homomorfismo

$$\mathcal{O}_X(HE^r)_P \longrightarrow \mathcal{O}_X(HE^r)_P \otimes_{\mathcal{O}_{X,P}} (\mathcal{O}_{X,P}/\mathcal{O}_X(E^{-1})_P)$$

transforma t_P en un generador, y lo mismo vale para el homomorfismo

$$\mathcal{O}_X(HE^r)_P \longrightarrow \mathcal{O}_X(HE^r)_P \otimes_{\mathcal{O}_{X,P}} (\mathcal{O}_{X,P}/\mathfrak{m}_P).$$

Por consiguiente, llamando $M_P = \mathcal{O}_X(HE^r)_P$, en la sucesión exacta

$$\langle t_P\rangle \otimes_{\mathcal{O}_{X,P}} k(P) \longrightarrow M_P \otimes_{\mathcal{O}_{X,P}} k(P) \longrightarrow (M_P/\langle t_P\rangle) \otimes k(P) \longrightarrow 0$$

el primer homomorfismo es suprayectivo, luego $(M_P/\langle t_P\rangle)\otimes k(P) = 0$ y el lema de Nakayama implica entonces que $M_P = \langle t_P\rangle$. Así pues, t es un generador global para los puntos $P \in E$.

Por otra parte, el homomorfismo natural $\mathcal{O}_X(H) \longrightarrow \mathcal{O}_X(HE^r)$ dado por el teorema anterior es un isomorfismo en los puntos $P \in X \setminus E$, luego un generador global de $\mathcal{O}_X(H)$ determina un generador global de $\mathcal{O}_X(HE^r)$ sobre los puntos de $X \setminus E$, y concluimos que $\mathcal{O}_X(HE^r)$ tiene un generador global. ∎

Teorema 7.13 *Sea X/S una superficie fibrada regular, sea $s \in S$ un punto cerrado y E un divisor primo contenido en la fibra X_s. Supongamos además que $E \cong \mathrm{P}^1_{k'}$, para cierto cuerpo k', finito sobre $k(s)$, así como que $E^2 < 0$. Entonces existe la contracción $f : X \longrightarrow Y$ de E, (pero Y no es necesariamente regular).*

Demostración: Sea $S = \operatorname{Esp} A$ y sea $\mathcal{L}$ un haz muy amplio en X (sobre A). En la prueba del teorema [E 8.34] se ve que $\mathcal{L} \cong \mathcal{O}_X(H_0)$, donde $H_0 \in \operatorname{Div}_c(X)$ es un divisor entero. Por el teorema [E 6.21], cambiando H_0 por una potencia suya, podemos suponer que $H^1(X, \mathcal{O}_X(H_0^n)) = 0$ para todo $n \geq 1$. Si Γ es un divisor primo vertical de X, entonces $\mathcal{O}_X(H_0)|_\Gamma$ es un haz muy amplio, luego $H_0 \cdot \Gamma > 0$ por 4.8.

Sean $m = -E^2 > 0$ y $r = H_0 \cdot E > 0$ y llamemos $D = H_0^m E^r$. Así, si consideramos un primo vertical $\Gamma \neq E$, tenemos que $D^n \cdot \Gamma \geq mH_0 \cdot \Gamma > 0$, luego $\mathcal{O}_X(D^n)|_\Gamma \ncong \mathcal{O}_\Gamma$. Por otra parte, el teorema anterior aplicado a $H = H_0^m$ nos da que $\mathcal{O}_X(D)$ tiene un generador global y que $\mathcal{O}_X(D)|_E \cong \mathcal{O}_E$.

En el caso $\dim S = 1$, tenemos que $D|_{X_\eta}$ es un divisor entero no trivial, luego

$$\operatorname{grad} \mathcal{O}_X(D)|_{X_\eta} = \operatorname{grad}(\mathcal{O}_{X_\eta}(D|_{X_\eta})) > 0.$$

Por consiguiente, D cumple las hipótesis del teorema 7.10 con $\mathcal{E} = \{E\}$, lo que nos da la existencia de la contracción cuando $\dim S = 1$.

En el caso geométrico, la prueba de 7.10 se puede adaptar. Vamos a hacerlo por completitud, aunque, a la larga, sólo nos va a interesar el caso aritmético. El argumento siguiente es válido en ambos casos:

Observemos en primer lugar que en la prueba del teorema anterior hemos visto que podemos considerar un generador global de $\mathcal{O}_X(D)$ formado por (la imagen de) un generador global de $\mathcal{O}_X(H)$ más un elemento t determinado módulo $\mathcal{O}_X(HE^{r-1})(X)$, por lo que, teniendo en cuenta que

$$\mathcal{O}_X(D)|_{X\setminus E} \cong \mathcal{O}_X(H)|_{X\setminus E},$$

podemos exigir que $t|_{X\setminus E} = 0$.

El generador global de $\mathcal{O}_X(H)$ lo podemos tomar de modo que determine una inmersión cerrada $X \longrightarrow \mathrm{P}^{n-1}_A$. Si llamamos $f : X \longrightarrow \mathrm{P}^n_A$ al homomorfismo inducido por el generador global de $\mathcal{O}_X(D)$, es fácil ver que su restricción a $X \setminus E$ es la composición de la inmersión $X \setminus E \longrightarrow \mathrm{P}^{n-1}_A$ con la inmersión $\mathrm{P}^{n-1}_A \longrightarrow \mathrm{P}^n_A$ dada por $X_n = 0$.

Sea $Z = f[X]$, dotado de la estructura de subesquema cerrado reducido (luego integro) de P^n_A. (Aquí usamos que X es proyectivo sobre A.) Llamaremos también $f : X \longrightarrow Z$ al homomorfismo suprayectivo inducido por f. Por 7.9 sabemos que $f[E]$ se reduce a un punto, luego $f[X \setminus E]$ es abierto en Z y $f : X \longrightarrow Z$ es un homomorfismo birracional. Como es proyectivo, $f_*\mathcal{O}_X$ es un haz coherente en Z, por [E 6.24]. A partir de aquí, el argumento de 7.10 es válido palabra por palabra. ∎

Así pues, bajo las hipótesis del teorema anterior, lo único que nos falta para asegurar que E es un divisor excepcional de X es que Y sea regular y, más concretamente, que sea regular en el punto cerrado $y = f[E]$, ya que $Y \setminus \{y\}$ es isomorfo a un abierto de X, luego es regular. El teorema siguiente nos permitirá determinar cuándo se da el caso.

Teorema 7.14 *En las condiciones del teorema anterior, tomemos un entorno afín V de y, sea $\mathfrak{m}$ el ideal maximal de $A = \mathcal{O}_Y(V)$ correspondiente a y, sea $U = f^{-1}[V]$, sea $\mathcal{I} = \mathcal{O}_X(E^{-1})|_U$ y $n \geq 0$. Entonces se cumple lo siguiente:*

a) Para cada $m \geq n+1$, tenemos que $H^1(U, \mathcal{I}^n/\mathcal{I}^m) = 0$.

b) $H^1(U, \mathcal{I}^n) = 0$.

c) El haz $\mathcal{I}^n$ tiene un generador global.

d) $H^0(U, \mathcal{I}^n) = \mathfrak{m}^n$.

e) Si $d = -E^2/|k' : k(s)|$, entonces $k' = k(y)$ y $\dim_{k(y)} T_yY = d+1$.

Demostración: Observemos que, como $f : V \longrightarrow U$ es birracional, induce un isomorfismo que nos permite identificar $K(U) = K(V) = K$, y considerar como inclusiones tanto a los homomorfismos asociados a f como a las restricciones. En particular, tenemos que $A = \mathcal{O}_V(V) \subset \mathcal{O}_U(U) \subset K$. Por el teorema [E 4.24] tenemos que $\mathcal{O}_U(U)$ es entero sobre A y, como V es normal, A es íntegramente cerrado, de modo que $\mathcal{O}_U(U) = A$. En otros términos, el homomorfismo $A \longrightarrow \mathcal{O}_V(V)$ es un isomorfismo. En particular, esto hace que d) tenga sentido.

a) Notemos que $d = -\operatorname{grad}_{k'} \mathcal{O}_X(E)|_E$, de modo que $\mathcal{O}_X(E^{-1})|_E \cong \mathcal{O}_E(d)$, pues $E \cong \mathrm{P}^1_{k'}$ y el $\mathrm{P}^1_{k'}$ el grado determina un isomorfismo entre el grupo de Picard y $\mathbb{Z}$. Sea $i : E \longrightarrow U$ la inmersión cerrada. Para todo $k \geq 0$,

$$\mathcal{I}^k/\mathcal{I}^{k+1} = \mathcal{I}^k \otimes_{\mathcal{O}_U} \mathcal{O}_U/\mathcal{I} = \mathcal{O}_X(E^{-k})|_U \otimes_{\mathcal{O}_U} i_*\mathcal{O}_E = i_*\mathcal{O}_X(E^{-k})|_E = i_*\mathcal{O}_D(kd).$$

Por lo tanto, $H^1(U, \mathcal{I}^k/\mathcal{I}^{k+1}) = H^1(E, \mathcal{O}_E(kd)) = 0$ (por [E 6.19]). Ahora consideramos la sucesión exacta

$$0 \longrightarrow \mathcal{I}^m/\mathcal{I}^{m+1} \longrightarrow \mathcal{I}^n/\mathcal{I}^{m+1} \longrightarrow \mathcal{I}^n/\mathcal{I}^m \longrightarrow 0,$$

de la que obtenemos la sucesión exacta

$$0 = H^1(U, \mathcal{I}^m/\mathcal{I}^{m+1}) \longrightarrow H^1(U, \mathcal{I}^n/\mathcal{I}^{m+1}) \longrightarrow H^1(U, \mathcal{I}^n/\mathcal{I}^m).$$

De aquí se sigue que $H^1(U, \mathcal{I}^n/\mathcal{I}^m) = 0$ por inducción sobre $m \geq n+1$.

b) Tomemos un ideal $\mathfrak{p} \in V$ distinto de $\mathfrak{m}$ y consideremos la proyección $\pi : U' = U \times_A \operatorname{Esp} A_{\mathfrak{p}} \longrightarrow U$. Si $V_0 \subset V$ es un entorno afín de $\mathfrak{p}$ que no contenga a $\mathfrak{m}$, resulta que $U_0 = f^{-1}[V_0] \subset U$ es también afín, porque f es un isomorfismo fuera de y. Es claro que $U' = U_0 \times_A \operatorname{Esp} A_{\mathfrak{p}}$, pues la composición de π con f ha de coincidir con la composición de la segunda proyección con $\operatorname{Esp} A_{\mathfrak{p}} \longrightarrow \operatorname{Esp} A$, luego toma imágenes en V_0. Así pues, U' es un esquema afín. Los teoremas [E 6.15] y [E 6.17] nos dan que

$$H^1(U, \mathcal{I}^n)_{\mathfrak{p}} \cong H^1(U', \pi^*\mathcal{I}^n) = 0.$$

Si probamos que también $H^1(U, \mathcal{I}^n)_{\mathfrak{m}} = 0$, entonces podremos concluir que $H^1(U, \mathcal{I}^n) = 0$. Para ello usamos el teorema de las funciones formales [E A12], según el cual

$$H^1(U, \mathcal{I}^n) \otimes_A \hat{A} \cong \varprojlim_k H^1(U, \mathcal{I}^n/\mathfrak{m}^k\mathcal{I}^n),$$

donde $\hat{A}$ es la compleción de A respecto de la topología $\mathfrak{m}$-ádica.

Observemos ahora que el haz de ideales $\mathfrak{m}\mathcal{O}_U$ es el que determina la fibra de y, es decir, determina un subesquema cerrado de U cuyo espacio subyacente es E, y lo mismo le sucede al haz $\mathcal{I}$. Más concretamente, $\mathcal{I}$ determina en E la estructura de esquema asociada a E como divisor primo, luego, según 4.6, se trata de la estructura de subesquema cerrado irreducible. Esto implica que (en cada abierto afín de U) $\mathcal{I}$ es el radical de $\mathfrak{m}\mathcal{O}_U$. Teniendo en cuenta que U es noetheriano, podemos concluir que $\mathcal{I}^r \subset \mathfrak{m}\mathcal{O}_U \subset \mathcal{I}$, para cierto $r \geq 1$. Por consiguiente, cada haz $\mathfrak{m}^k\mathcal{I}^n$ contiene a un haz $\mathcal{I}^m$ para m suficientemente grande, y cada $\mathcal{I}^m$ contiene un $\mathfrak{m}^k\mathcal{I}^n$ para k grande. De aquí se sigue que

$$H^1(U, \mathcal{I}^n)_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} \hat{A} \cong H^1(U, \mathcal{I}^n) \otimes_A \hat{A} \cong \varprojlim_{m \geq n} H^1(U, \mathcal{I}^n/\mathcal{I}^m) = 0.$$

En otras palabras, la compleción $\widehat{H^1(U, \mathcal{I}^n)_{\mathfrak{m}}}$ es nula, pero, como la topología $\mathfrak{m}$-ádica es de Hausdorff, la inmersión de $H^1(U, \mathcal{I}^n)_{\mathfrak{m}}$ en su compleción es inyectiva,[3] luego también $H^1(U, \mathcal{I}^n)_{\mathfrak{m}} = 0$, y esto termina la prueba de b).

c) Basta probar que $\mathcal{I}$ admite un generador global. Si $x \in U \setminus E$, entonces $\mathcal{I}_x = \mathcal{O}_{U,x}$. Sea $\mathfrak{p} \neq \mathfrak{m}$ la imagen de x en $V = \operatorname{Esp} A$. Tomemos $h \in \mathfrak{m} \setminus \mathfrak{p}$. Según las observaciones al principio de la prueba, podemos considerar también que $h \in \mathcal{O}_U(U)$. Entonces, su imagen en $\mathcal{O}_E(E)$ pertenece a todos los ideales $\mathfrak{m}_P$ con $P \in E$. Puesto que E es reducido, esto implica que dicha imagen es nula o, lo que es lo mismo, que $h \in \mathcal{I}$. Como el homomorfismo $\mathcal{O}_{U,x} \longrightarrow \mathcal{O}_{V,\mathfrak{p}}$ es un isomorfismo, resulta que $h_x \notin \mathfrak{m}_x$, luego h genera $\mathcal{I}$ en x.

Falta llegar a la misma conclusión para puntos $x \in E$. Para ello consideramos la sucesión exacta

$$0 \longrightarrow \mathcal{I}^2 \longrightarrow \mathcal{I} \longrightarrow i_*\mathcal{I}|_E \longrightarrow 0,$$

de la que se deduce que el homomorfismo $H^0(U, \mathcal{I}) \longrightarrow H^0(E, \mathcal{I}|_E)$ es suprayectivo, ya que $H^1(U, \mathcal{I}^2) = 0$. Como $\mathcal{I}|_E \cong \mathcal{O}_E(d)$ tiene un generador global,

[3] Ver la prueba de [E A15].

podemos tomar $t \in H^0(U,\mathcal{I})$ cuya imagen genere $\mathcal{I}|_{E,x}$. Así, el homomorfismo

$$\mathcal{I}_x \longrightarrow \mathcal{I}_x \otimes_{\mathcal{O}_{U,x}} (\mathcal{O}_{U,x}/\mathcal{I}_x)$$

transforma t_x en un generador, y lo mismo vale para el homomorfismo

$$\mathcal{I}_x \longrightarrow \mathcal{I}_x \otimes_{\mathcal{O}_{U,x}} (\mathcal{O}_{U,x}/\mathfrak{m}_x).$$

Por consiguiente, en la sucesión exacta

$$\langle t_x\rangle \otimes_{\mathcal{O}_{U,x}} k(x) \longrightarrow \mathcal{I}_x \otimes_{\mathcal{O}_{U,x}} k(x) \longrightarrow (\mathcal{I}_x/\langle t_x\rangle) \otimes_{\mathcal{O}_{U,x}} k(P) \longrightarrow 0,$$

el primer homomorfismo es suprayectivo, luego $(\mathcal{I}_x/\langle t_x\rangle) \otimes_{\mathcal{O}_{U,x}} k(P) = 0$, y el lema de Nakayama implica entonces que $\mathcal{I}_x = \langle t_x\rangle$. Así pues, t es un generador global en x.

d) En la prueba del apartado anterior hemos visto que si $h \in \mathfrak{m}$, entonces, como elemento de $\mathcal{O}_U(U)$, está en $\mathcal{I}(U)$, es decir, que tenemos la inclusión

$$\mathfrak{m} \subset H^0(U,\mathcal{I}).$$

Recíprocamente, si $h \in \mathcal{I}(U)$, ha de ser $h \in \mathfrak{m}$, pues en caso contrario, si $P \in E$, el homomorfismo $\mathcal{O}_{V,\mathfrak{m}} \longrightarrow \mathcal{O}_{U,P}$ transformaría la unidad $h_{\mathfrak{m}}$ en $h_P \in \mathcal{I}_P \subsetneq \mathcal{O}_{U,P}$, lo cual es absurdo. Así pues, $H^0(U,\mathcal{I}) = \mathfrak{m}$.

En general es claro que $\mathfrak{m}^n \subset H^0(U,\mathcal{I}^n)$. Notemos que los haces $\mathcal{I}^n$ son localmente libres de rango 1, por lo que se comprueba inmediatamente que el homomorfismo $\mathcal{I}^n \otimes_{\mathcal{O}_U} \mathcal{I} \longrightarrow \mathcal{I}^{n+1}$ es un isomorfismo. Por ello, para terminar la prueba basta aplicar el teorema 4.15. Para ello, notemos que $H^1(U,\mathcal{O}_U) = 0$ por b) para $n = 0$.

e) Se cumple que

$$\mathfrak{m}^n/\mathfrak{m}^{n+1} = H^0(U,\mathcal{I}^n)/H^0(U,\mathcal{I}^{n+1}) \cong H^0(U,\mathcal{I}^n/\mathcal{I}^{n+1})$$

porque $H^1(U,\mathcal{I}^n) = 0$. Teniendo en cuenta lo que hemos obtenido en a),

$$\mathfrak{m}^n/\mathfrak{m}^{n+1} = H^0(E,\mathcal{O}_E(nd)).$$

Si tomamos $n = 0$ queda $k(y) = A/\mathfrak{m} = H^0(E,\mathcal{O}_E) = k'$, mientras que si hacemos $n = 1$ obtenemos que

$$\dim_{k(y)} T_yY = \dim_{k(y)} H^0(E,\mathcal{O}_E(d)) = d+1.$$

(Notemos que $H^0(E,\mathcal{O}_E(d))$ es el espacio vectorial de las formas de grado d en dos variables.) ∎

Reuniendo todo lo que hemos probado obtenemos el resultado que perseguíamos:

Teorema 7.15 (Criterio de Castelnuovo) *Sea X/S una superficie fibrada regular, sea $s \in S$ y $E \subset X_s$ un divisor primo vertical. Sea $k' = H^0(E,\mathcal{O}_E)$. Entonces E es un divisor excepcional si y sólo si $E \cong \mathrm{P}^1_{k'}$ y $E^2 = -|k' : k(s)|$.*

DEMOSTRACIÓN: Una implicación es el teorema 7.7. Si E cumple las condiciones indicadas, el teorema 7.13 nos da que existe la contracción de E, aunque la superficie Y resultante no sea necesariamente regular en $y = f[E]$. No obstante, el teorema anterior nos da que sí que lo es, ya que $d = 1$ y $\dim_{k(y)} T_yY = 2$. ∎

Vamos a necesitar la siguiente caracterización de los divisores excepcionales de una superficie fibrada en términos de la clase canónica:

Teorema 7.16 *Sea X/S una superficie fibrada regular, sea $W_{X/S}$ un divisor canónico y $E \subset X_s$ un divisor primo vertical.*

a) El divisor E es excepcional si y sólo si $W_{X/S} \cdot E < 0$ y $E^2 < 0$. Además, en tal caso $W_{X/S} \cdot E = E^2$.

b) Si $\dim S = 1$ y $p_a(X_\eta) \geq 1$ (donde η es el punto genérico de S), entonces E es un divisor excepcional si y sólo si $W_{X/S} \cdot E < 0$.

DEMOSTRACIÓN: a) Llamemos $k' = H^0(E, \mathcal{O}_E)$ y $m = |k' : k(s)|$. Supongamos en primer lugar que E es excepcional. Entonces el teorema 7.15 nos da que $E^2 = -m$ y

$$\chi_{k(s)}(\mathcal{O}_E) = m\chi_{k'}(\mathcal{O}_E) = m\chi_{k'}(\mathrm{P}^1_{k'}) = m.$$

La fórmula de adjunción 6.12 implica entonces que

$$1 - \chi_{k(s)}(\mathcal{O}_E) = p_a(E) = 1 + \frac{1}{2}(E^2 + W_{X/S} \cdot E),$$

luego

$$W_{X/S} \cdot E = -E^2 - 2\chi_{k(s)}(\mathcal{O}_E) = -m < 0.$$

Supongamos ahora que E es un divisor primo que cumple las desigualdades. Notemos que, considerado como subesquema cerrado de X es íntegro por el teorema 4.6, y es localmente una intersección completa por 5.32. La fórmula de adjunción nos da igualmente la relación

$$W_{X/S} \cdot E + E^2 = -2\chi_{k(s)}(\mathcal{O}_E),$$

que, más explícitamente, es

$$\mathrm{grad}_{k(s)}\, \omega_{X/S}|_E + \mathrm{grad}_{k(s)}\, \mathcal{O}_X(E)|_E = -2\chi_{k(s)}(\mathcal{O}_E),$$

o también

$$\mathrm{grad}_{k'}\, \omega_{X/S}|_E + \mathrm{grad}_{k'}\, \mathcal{O}_X(E)|_E = -2\chi_{k'}(\mathcal{O}_E) = -2 + 2\dim_{k'} H^1(E, \mathcal{O}_E).$$

Por hipótesis, el miembro izquierdo es menor que 0, luego necesariamente $H^1(E, \mathcal{O}_E) = 0$, y así $p_a(E) \leq 0$. Por el teorema 4.16 sabemos que E/k' es una cónica. Más aún, como los dos sumandos de la izquierda son negativos, ha de ser

$$\mathrm{grad}_{k'}\, \omega_{X/S}|_E = \mathrm{grad}_{k'}\, \mathcal{O}_X(E)|_E = -1,$$

luego $W_{X/S} \cdot E = E^2 = -m$ y $\mathcal{O}_X(E^{-1})|_E$ se corresponde con un divisor de Cartier entero en E de grado 1. El teorema 4.18 implica que $E \cong \mathrm{P}^1_{k'}$, luego el criterio de Castelnuovo nos da que E es excepcional.

b) Si $S = \operatorname{Esp} D$ y K es el cuerpo de cocientes de D, entonces K es plano sobre D, luego podemos aplicar los teoremas [E 6.15], [E 9.29] y [E 9.32], de modo que

$$H^0(X, \omega_{X/S}) \otimes_D K = H^0(X_\eta, \omega_{X_\eta/K}) \cong H^1(X_\eta, \mathcal{O}_{X_\eta}).$$

La hipótesis sobre el género de X_η equivale a que

$$\dim_K H^1(X_\eta, \mathcal{O}_{X_\eta}) \geq \dim_K H^0(X_\eta, \mathcal{O}_{X_\eta}) \geq 1,$$

luego $H^0(X, \omega_{X/S}) \neq 0$, lo que a su vez implica que existe un divisor canónico $W_{X/S}$ que además es entero. Entonces, la relación $W_{X/S} \cdot E < 0$ sólo puede darse si $E \mid W_{X/S}$. Pongamos que $W_{X/S} = E^a D$, donde $a \geq 0$ y D es un divisor entero primo con E. Así, $aE^2 = W_{X/S} \cdot E - D \cdot E < 0$, luego $E^2 < 0$ y a) implica que E es un divisor excepcional. ∎

Si una superficie aritmética X tiene un divisor excepcional, podemos contraerlo hasta un punto, con lo que obtenemos una nueva superficie aritmética $X_1 \preceq X$. Si ésta tiene a su vez otro divisor excepcional, podemos contraerlo también, con lo que obtenemos una nueva superficie aritmética $X_2 \preceq X_1$, y así sucesivamente. Vamos a probar que, tras un número finito de pasos, llegamos a una superficie sin divisores excepcionales, es decir, a una superficie relativamente minimal. Ello se sigue fácilmente del teorema siguiente:

Teorema 7.17 *Si X/S es una superficie aritmética,*[4] *existe a lo sumo un número finito de fibras que contienen divisores excepcionales.*

Demostración: Consideremos en primer lugar el caso en que la fibra genérica X_η es geométricamente regular. Sea $U \subset X$ el conjunto de puntos suaves, que es abierto por [E A34] y por hipótesis contiene a X_η. Entonces $\pi[X \setminus U]$ es cerrado en S, y no es todo S, ya que no contiene al punto genérico η, luego consta de un número finito de puntos. Así pues, $V = S \setminus \pi[X \setminus U]$ es un abierto no vacío y X_s es geométricamente regular para todo $s \in V$. El mismo razonamiento del teorema 7.8 implica que X_s no contiene divisores excepcionales.

Ahora consideremos el caso en que $H^0(X, \omega_{X/S}) \neq 0$. Si $h \in H^0(X, \omega_{X/S})$ es no nulo, ha de existir un punto $x \in X$ tal que h sea un generador global de $\omega_{X/S}$ en x. En caso contrario, para cada abierto afín $U = \operatorname{Esp} A$ donde $\omega_{X/S}$ sea libre, tendríamos que $h|_U = aw$, donde w es una base de $\omega_{X/S}|_U$ y $a \in A$ estaría en la intersección de todos los ideales primos de A, luego sería nulo, luego $h|_U = 0$ y tendríamos que $h = 0$. Así pues, el conjunto $C \subset X$ formado por los puntos donde $\omega_{X/S}$ no tiene un generador global es un cerrado estrictamente contenido en X.

[4] Por simplicidad excluiremos de la prueba un caso que no nos va a hacer falta, a saber, cuando $\operatorname{car} k(S) = 2$ y $p_a(X_\eta) \leq 0$, aunque el teorema también es cierto en este caso.

A continuación observamos que si E es un divisor excepcional, el teorema 7.16 implica que $\operatorname{grad}\omega_{X/S}|_E < 0$, luego $H^0(E,\omega_{X/S}|_E) = 0$. Esto implica que $E \subset C$, ya que si $\omega_{X/S}$ tuviera un generador global en un punto $x \in E$, dicho generador induciría un generador global de $\omega_{X/S}|_E$ en x. Así pues, sólo puede haber un número finito de divisores excepcionales.

Finalmente veamos el caso en que $H^0(X,\omega_{X/S}) = 0$. Consideremos la descomposición $X \longrightarrow S' \longrightarrow S$ dada por el teorema anterior (y notemos que, obviamente, X/S' es también una superficie aritmética). Como allí, digamos que $S = \operatorname{Esp} D$ y sea K el cuerpo de cocientes de D. Al igual que en la prueba de 7.16, vemos que

$$0 = H^0(X,\omega_{X/S}) \otimes_D K = H^0(X_\eta,\omega_{X_\eta/K}) \cong H^1(X_\eta,\omega_{X_\eta/K}),$$

lo que implica que $p_a(X_\eta) \leq 0$. Sea $L = K(S') = H^0(X_\eta,\mathcal{O}_{X_\eta})$, de modo que X_η/L es una cónica regular, por el teorema 4.16. Si no es geométricamente regular, el teorema 4.13 nos da que ha de ser $\operatorname{car} K = 2$ y, como hemos indicado, no trataremos este caso.

Así pues, suponemos que X_η/L es geométricamente regular y, según hemos visto al principio de la prueba, el teorema se cumple para X/S', es decir, que tiene sólo un número finito de divisores excepcionales, pero el criterio de Castelnuovo muestra que los divisores excepcionales de X/S son los mismos que los de X/S'. ∎

Ahora ya es fácil probar que el proceso de contracción de divisores excepcionales es necesariamente finito:

Teorema 7.18 *Si X/S es una superficie aritmética, existe una superficie aritmética relativamente minimal Y/S y un homomorfismo birracional $f : X \longrightarrow Y$*

Demostración: Sea $g : X \longrightarrow X'$ la contracción de un divisor excepcional $E \subset X_s$. Observemos que si otra fibra cerrada $X_{s'}$, con $s' \neq s$, no contiene divisores excepcionales, entonces $X'_{s'}$ tampoco puede contenerlos.

En efecto, si $E' \subset X'_{s'}$ fuera un divisor excepcional, puesto que g es un isomorfismo en $X \setminus E$, podemos considerar también $E' \subset X_{s'}$, y vamos a probar que E' es también un divisor excepcional de X. Para ello consideramos el homomorfismo birracional $h : X \longrightarrow X''$ que resulta de componer g con la contracción de E'. Claramente, el lugar excepcional $\mathcal{E}$ de h es la unión disjunta de E y E'.

El teorema 6.23 nos da una descomposición de h como $X \longrightarrow \widetilde{X''} \longrightarrow X''$, donde $\widetilde{X''}$ es la explosión de X'' con centro en la imagen de E. Estamos en la situación estudiada en la prueba del teorema 6.24, donde se ve que el lugar excepcional de $X \longrightarrow \widetilde{X''}$ ha de ser exactamente el divisor E', lo que prueba que E' es excepcional en X.

Con esto hemos probado que, al contraer un divisor excepcional, el número de fibras que contienen divisores excepcionales (que es finito por el teorema anterior) no aumenta, y el número de componentes irreducibles de tales fibras disminuye en una unidad, luego tras un número finito de contracciones tenemos que llegar a una superficie aritmética Y/S sin divisores excepcionales. ∎

7.3 Superficies minimales

Finalmente estamos en condiciones de estudiar el concepto central de este capítulo:

Definición 7.19 Una superficie aritmética X/S es *minimal* si toda aplicación birracional $Y \longrightarrow X$ entre superficies aritméticas definidas sobre S es un homomorfismo birracional (es decir, está definida sobre toda la superficie Y).

En esencia, esto significa que $X \preceq Y$ para toda superficie aritmética Y/S birracionalmente equivalente a X/S, pero es importante observar que en realidad la definición afirma un poco más, ya que no sólo afirma que *existe* un homomorfismo birracional $Y \longrightarrow X$, sino que *todas* las aplicaciones birracionales $Y \longrightarrow X$ son homomorfismos birracionales. Por ejemplo, esto es crucial para concluir que dos superficies aritméticas minimales birracionalmente equivalentes son necesariamente isomorfas.

Observemos que toda superficie aritmética minimal X/S es relativamente minimal, pues si $f : X \longrightarrow Y$ es un homomorfismo birracional, entonces su inversa $f^{-1} : Y \longrightarrow X$ es, en principio, una aplicación birracional, pero ha de ser también un homomorfismo birracional, y las composiciones $f \circ f^{-1}$ y $f^{-1} \circ f$ se restringen a la identidad en sendos abiertos, luego son la identidad, por lo que f es un isomorfismo.

En esta sección demostraremos que, si la fibra genérica cumple $p_a(X_\eta) \geq 1$, también se cumple el recíproco: si X/S es relativamente minimal, entonces es minimal.

Empezamos observando lo siguiente: Si X/S' es una superficie fibrada, $S' \longrightarrow S$ es un homomorfismo finito (que nos permite considerar a X/S como superficie fibrada) y E, $F \in \mathrm{Div}_{s'}(X)$, entonces

$$(E \cdot F)_S = |k(s') : k(s)|(E \cdot F)_{S'},$$

donde $s \in S$ es la imagen de s'. En efecto, por linealidad podemos suponer que E y F son divisores primos, y entonces basta aplicar el teorema 6.4 d).

Consecuentemente, el criterio de Castelnuovo implica que un divisor E es excepcional respecto a X/S si y sólo si lo es respecto a X/S'.

Con esto podemos probar:

Teorema 7.20 *Sea X/S una superficie fibrada regular cuya fibra genérica tenga género $p_a(X_\eta) \geq 1$. Entonces, dos divisores excepcionales distintos en X son necesariamente disjuntos.*

Demostración: Sean E_1 y E_2 dos divisores excepcionales en X distintos entre sí y supongamos que no son disjuntos. El teorema 5.28 nos da una factorización $X \longrightarrow S' \longrightarrow S$ tal que las fibras de X/S' son las componentes conexas de las fibras de X/S. Puesto que $E_1 \cap E_2 \neq \varnothing$, necesariamente están en la misma

fibra X_s, para cierto $s \in S'$. Por la observación precedente, también son divisores excepcionales respecto a S', luego no perdemos generalidad si suponemos que las fibras de X son conexas.

Sea $k'_i = H^0(E_i, \mathcal{O}_{E_i})$. Podemos suponer que $k'_1 \geq k'_2$. Entonces

$$(E_1E_2)^2 = E_1^2 + E_2^2 + 2E_1 \cdot E_2 = -|k'_1 : k(s)| - |k'_2 : k(s)| + 2\,\mathrm{grad}_{k'_1}\, \mathcal{O}_X(E_2)|_{E_1},$$

luego $(E_1E_2)^2 \geq 0$. Por el teorema 6.8 concluimos que $E_1E_2 = rX_s$, para cierto número real r (necesariamente racional). Como los divisores se cortan, $r > 0$, y el teorema 6.13, junto con el teorema 7.16, nos da que

$$p_a(X_\eta) = 1 + \frac{1}{2r}\,(W_{X/S} \cdot E_1 + W_{X/S} \cdot E_2) < 1,$$

en contradicción con lo supuesto. ∎

Finalmente podemos probar el teorema principal:

Teorema 7.21 *Toda superficie aritmética relativamente minimal X cuya fibra genérica cumpla $p_a(X_\eta) \geq 1$ es minimal.*

Demostración: Sea $f : Y \longrightarrow X$ una aplicación birracional definida sobre S, donde Y/S es otra superficie aritmética. Hemos de probar que f está definida en todo Y. Sea Γ su gráfica, de modo que tenemos un homomorfismo birracional $\Gamma \longrightarrow Y$. Éste induce un isomorfismo entre las fibras genéricas, que, a su vez, para cada punto cerrado $s \in S$, induce un isomorfismo $\Gamma \times_S \mathrm{Esp}\,\hat{\mathcal{O}}_{S,s} \longrightarrow Y \times_S \mathrm{Esp}\,\hat{\mathcal{O}}_{S,s}$. Como Y admite trivialmente una desingularización, cumple la propiedad b) del teorema 6.35, luego lo mismo le sucede a Γ, luego también Γ admite una desingularización $Z \longrightarrow \Gamma$. Se trata de un homomorfismo proyectivo, luego Z/S es una superficie aritmética.

Componiendo el homomorfismo $Z \longrightarrow \Gamma$ con los homomorfismos naturales $\Gamma \longrightarrow X$ y $\Gamma \longrightarrow Y$ obtenemos homomorfismos birracionales $f_1 : Z \longrightarrow Y$ y $f_2 : Z \longrightarrow X$ tales que $f = f_1^{-1} \circ f_2$.

Supongamos que existe un divisor excepcional E de Z tal que $f_1[E]$ y $f_2[E]$ son puntos. En tal caso, consideramos la contracción $Z \longrightarrow Z'$ de E, que es otra superficie aritmética, y observamos que las aplicaciones birracionales $f'_1 : Z' \longrightarrow Y$, $f'_2 : Z' \longrightarrow X$ son, de hecho, homomorfismos birracionales. En efecto, f'_1 se restringe a un isomorfismo $Z' \setminus \{p'\} \longrightarrow Y \setminus \{p\}$, pero, según 6.18, si f'_i no estuviera definida en p', su inversa transformaría una curva en p', lo cual es imposible. Lo mismo vale para f'_2.

Claramente, se sigue cumpliendo que $f = f_1'^{-1} \circ f'_2$. En la prueba de 7.18 hemos visto que una sucesión de contracciones

$$Z \longrightarrow Z' \longrightarrow Z'' \longrightarrow \cdots$$

es necesariamente finita, luego, tras un número finito de pasos, podemos suponer que no existe ningún divisor excepcional de Z que tanto f_1 como f_2 lo transformen en un punto.

Vamos a probar que f_1 es un isomorfismo, con lo que f estará definida sobre todo Y, tal y como queremos probar. En caso contrario, el teorema 6.24 nos da que su lugar excepcional contiene un divisor excepcional E tal que $f_1[E]$ se reduce a un punto. Según lo que acabamos de establecer, $f_2[E]$ no puede ser un punto.

De nuevo por 6.24, podemos descomponer $f_2 = g_1 \circ \cdots \circ g_n$ como composición de explosiones de puntos cerrados (o, equivalentemente, contracciones de divisores excepcionales).

Sea E_1 el lugar excepcional de g_1. Como $f_2[E]$ no es un punto, necesariamente $E_1 \neq E$ y el teorema anterior nos da que $E \cap E_1 = \varnothing$. El criterio de Castelnuovo implica entonces que $g_1[E]$ es un divisor excepcional. En efecto, si $g_1 : Z \longrightarrow Z'$ y $E' = g_1[E]$, es claro que $\mathcal{O}_Z(E) = g_1^*\mathcal{O}_{Z'}(E')$ y, como g_1 se restringe a un isomorfismo en un entorno de E, concluimos que $\mathcal{O}_Z(E)|_E \cong \mathcal{O}_{Z'}(E')|_{E'}$, luego $E^2 = E'^2$.

Razonando igualmente con cada g_i llegamos a que $f_2[E]$ es un divisor excepcional en X, en contradicción con que X es relativamente minimal. ∎

En particular, todos los ejemplos que hemos dado de superficies relativamente minimales, son en realidad ejemplos de superficies minimales, pues las fibras genéricas tenían género 1 en todos los casos.

Combinando el teorema anterior con 7.18 y con la definición de superficie minimal, tenemos la siguiente consecuencia inmediata:

Teorema 7.22 *Si X/S es una superficie aritmética cuya fibra genérica cumpla $p_a(X_\eta) \geq 1$, existe una superficie aritmética minimal Y/S y un homomorfismo birracional $f : X \longrightarrow Y$. Además, el par (Y, f) es único salvo isomorfismo.*

En términos de modelos de curvas, teniendo en cuenta el teorema 6.37 concluimos inmediatamente:

Teorema 7.23 *Sea D un dominio de Dedekind con cuerpo de cocientes K y sea $S = \operatorname{Esp} D$. Entonces, toda curva proyectiva íntegra geométricamente regular C/K de género $p_a(C) \geq 1$ tiene un modelo regular minimal, único salvo isomorfismo.*

Teorema 7.24 *Sea D un dominio de Dedekind con cuerpo de cocientes K, sea $S = \operatorname{Esp} D$, sea C/K una curva proyectiva íntegra geométricamente regular tal que $p_a(C) \geq 1$ y sea X/S su modelo regular minimal. Para cada punto cerrado $s \in S$, se cumple que $X \times_S \operatorname{Esp} \mathcal{O}_{S,s}$ es el modelo regular minimal de C/K sobre $\operatorname{Esp} \mathcal{O}_{S,s}$.*

Demostración: Llamemos $X' = X \times_S \operatorname{Esp} \mathcal{O}_{S,s}$. En las observaciones previas al teorema 6.5 hemos visto que es una superficie aritmética sobre $\mathcal{O}_{S,s}$. La proyección $p : X' \longrightarrow X$ es plana, luego el teorema [E 9.29] nos da que $p^*\omega_{X/D} = \omega_{X'/\mathcal{O}_{S,s}}$. Por consiguiente, si la fibra cerrada de X' contuviera un divisor excepcional E (al que podemos ver también como divisor de X), tendríamos que $\omega_{X/D}|_E = \omega_{X'/\mathcal{O}_{S,s}}|_E$, de donde se sigue que

$$K_{X/D} \cdot E = K_{X'/\mathcal{O}_{S,s}} \cdot E,$$

y el teorema 7.16 implica que E también es excepcional en X, lo cual es absurdo. Así pues, X' es relativamente minimal y, por el teorema 7.21 es minimal. ∎

Ejemplo Sea $X/\mathbb{Z}$ la superficie fibrada definida por la ecuación de Selmer que consideramos en la sección 5.4 y sea $\mathcal{X}/\mathbb{Z}$ su modelo regular minimal. Para cada primo $p \in \mathbb{Z}$, la fibra $\mathcal{X}_p$ es isomorfa a la del esquema $\mathcal{X} \times_{\mathbb{Z}} \operatorname{Esp} \mathbb{Z}_p$ que, por el teorema anterior, es el modelo regular minimal de la curva de Selmer sobre $\mathbb{Z}_p$.

Ahora bien, conocemos los modelos regulares minimales de la curva de Selmer sobre todos los anillos $\mathbb{Z}_p$: para $p = 2$, 3 son las desingularizaciones que hemos calculado en la sección 5.4. (En el ejemplo de la página 206 hemos visto que son relativamente minimales, luego son minimales.) Para los demás primos, son las superficies $X \times_{\mathbb{Z}} \operatorname{Esp} \mathbb{Z}_p$. En efecto, todas ellas son superficies aritméticas y, para $p \neq 5$, son suaves, luego relativamente minimales (teorema 7.8). Para $p = 2$, tenemos que X_2 es una curva irreducible singular, luego no puede ser isomorfa a $\mathrm{P}^1_{k'}$, para ningún cuerpo k', luego no es un divisor excepcional, luego $X \times_{\mathbb{Z}} \operatorname{Esp} \mathbb{Z}_5$ es relativamente minimal, luego es minimal.

Así pues, podemos concluir que, para $p \neq 2, 3$, se cumple que $\mathcal{X}_p \cong X_p$, mientras que $\mathcal{X}_2$ y $\mathcal{X}_3$ son las fibras de las desingularizaciones calculadas en la sección 5.4 (y, por supuesto, $\mathcal{X}_\eta$ es la curva de Selmer).

En general, de este modo se reduce el estudio de los modelos regulares minimales de una curva cualquiera X/S al estudio de sus modelos regulares minimales sobre los anillos de valoración discreta $\mathcal{O}_{S,s}$. ∎

Terminamos con dos observaciones sencillas sobre superficies minimales. La primera es que podemos caracterizarlas en términos de los divisores canónicos:

Teorema 7.25 *Sea X/S una superficie aritmética cuya fibra genérica cumpla que $p_a(X_\eta) \geq 1$ y sea $W_{X/S}$ un divisor canónico. Entonces X/S es minimal si y sólo si $W_{X/S} \cdot E \geq 0$ para todo divisor primo vertical E.*

Demostración: El teorema 7.16 nos da que X/S cumple la condición del enunciado si y sólo si no tiene divisores excepcionales, es decir, si es relativamente minimal, y esto equivale a que X/S sea minimal por 7.21. ∎

En segundo lugar, en la prueba del teorema 7.3 hemos visto que todo isomorfismo entre las fibras genéricas de dos superficies aritméticas se extiende a una aplicación birracional entre ellas (y la extensión es única por el teorema 5.26). Si ambas superficies son minimales, la extensión será un isomorfismo. En particular, es inmediato el teorema siguiente:

Teorema 7.26 *Si X/S es una superficie aritmética minimal y $K = K(S)$, la aplicación natural $\mathrm{Aut}_S(X) \longrightarrow \mathrm{Aut}_K(X_\eta)$ es biyectiva.*

7.4 Desingularizaciones minimales

En esta sección vamos a demostrar una generalización del teorema 7.25. De hecho, desde un punto de vista lógico hubiera sido más sencillo demostrar primero el teorema 7.29 y obtener 7.25 como consecuencia inmediata, pero hemos

preferido seguir este orden por no introducir nuevos conceptos innecesarios en el argumento que nos ha llevado a la existencia de superficies minimales.

El asunto que nos ocupa es que, en general, una superficie fibrada admite muchas desingularizaciones no isomorfas entre sí, pero vamos a ver que es posible construir una desingularización minimal, única salvo isomorfismo:

Definición 7.27 Sea Y/S una superficie fibrada normal. Una *desingularización minimal* de Y es una desingularización $f : X \longrightarrow Y$ tal que cualquier otra desingularización $Z' \longrightarrow Y$ se descompone de forma única como

$$Z' \xrightarrow{g} Z \xrightarrow{f} Y,$$

donde g es una aplicación birracional.

Es evidente que si una superficie admite una desingularización minimal, ésta es única salvo isomorfismo. El teorema siguiente demuestra la existencia de lo que podríamos llamar una *"desingularización relativamente minimal":*

Teorema 7.28 *Sea W/S una superficie fibrada normal con* $\dim S = 1$. *Si W/S admite una desingularización, entonces admite una desingularización cuyo lugar excepcional no contiene divisores excepcionales.*

Demostración: Sea $f : X \longrightarrow W$ una desingularización de W. Si su lugar excepcional contiene un divisor excepcional E, podemos considerar su contracción $g : X \longrightarrow X'$. La aplicación birracional $f' = g^{-1} \circ f : X' \longrightarrow W$ se restringe a un homomorfismo $X' \setminus \{g[E]\} \longrightarrow W \setminus \{f[E]\}$, y el teorema 6.18 implica entonces que f' está definida en todo X', ya que en caso contrario la transformada total $f'(g[E])$ sería una curva en W cuya imagen por f'^{-1} debería ser el punto $g[E]$, pero eso es imposible, ya que los únicos puntos de W que pueden tener imagen $g[E]$ son los puntos cerrados de la imagen del lugar excepcional de f.

Así pues, hemos factorizado f en la forma $X \longrightarrow X' \longrightarrow W$, y f' es otra desingularización de f. En la prueba del teorema 7.18 hemos visto que es imposible construir una sucesión infinita de contracciones de divisores excepcionales a partir de una superficie aritmética dada, luego, tras un número finito de pasos, hemos de llegar a una desingularización $f' : X' \longrightarrow W$ cuyo lugar excepcional no contenga divisores excepcionales de X'. ∎

Observemos que si en el teorema anterior partimos de una desingularización estricta, terminamos también con una desingularización estricta.

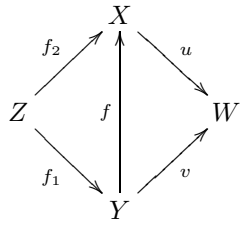
Teorema 7.29 *Sea W/S una superficie fibrada normal cuya fibra genérica cumpla $p_a(W_\eta) \geq 1$. Supongamos además que* $\dim S = 1$. *Una desingularización de W/S es minimal si y sólo si su lugar excepcional no contiene divisores excepcionales.*

DEMOSTRACIÓN: Sea $X \longrightarrow W$ una desingularización de W/S cuyo lugar excepcional no contenga divisores excepcionales de X. Para probar que es minimal tomamos otra desingularización $X' \longrightarrow W$ que, según el teorema anterior, se descompone como $X' \longrightarrow Y \longrightarrow W$, donde la segunda desingularización cumple también que su lugar excepcional no contiene divisores excepcionales de Y.

Basta probar que dos desingularizaciones $u : X \longrightarrow W$ y $v : Y \longrightarrow W$ de W que cumplan esta propiedad sobre los divisores excepcionales son isomorfas. El isomorfismo es necesariamente único, pues ha de ser la aplicación birracional $f = v \circ u^{-1} : Y \longrightarrow X$.

Estamos exactamente en las condiciones del teorema 7.21 (salvo que ahora no es cierto que X no tenga divisores excepcionales, sino que no tiene divisores excepcionales en el soporte de u). Notemos que $X_\eta \cong W_\eta$, por lo que también contamos la hipótesis $p_a(X_\eta) \geq 1$.

Toda la prueba del teorema 7.21 es válida ahora palabra por palabra. Concretamente, obtenemos un diagrama conmutativo



donde Z es una superficie aritmética y f_1, f_2 son homomorfismos birracionales. Queremos probar que f_1 es un isomorfismo. En caso contrario su soporte contiene un divisor excepcional E tal que $f_2[E]$ es un divisor excepcional en X. En la prueba de 7.21 esto nos daba una contradicción porque X era minimal, ahora, en cambio, lo que sucede es que $f_1[E]$ ha de estar contenido en el lugar excepcional de u por la conmutatividad del diagrama, con lo que seguimos teniendo una contradicción.

Esto prueba que f es un homomorfismo birracional y, cambiando los papeles de X e Y, también lo es f^{-1}, luego f es un isomorfismo.

El recíproco es trivial: si $Y \longrightarrow W$ es una desingularización minimal pero su lugar excepcional contuviera divisores excepcionales, podríamos factorizarla según el teorema anterior: $Y \xrightarrow{f} X \longrightarrow W$, donde $X \longrightarrow W$ es también una desingularización minimal de W/S. El razonamiento anterior prueba que f es un isomorfismo, pero no puede serlo, pues resulta de contraer al menos un divisor excepcional de Y. ∎

Ahora podemos precisar el teorema 6.36:

Teorema 7.30 *Sea W/S una superficie fibrada normal, donde $\dim S = 1$, cuya fibra genérica sea geométricamente regular y cumpla $p_a(W_\eta) \geq 1$. Entonces W/S admite una desingularización minimal, que además será estricta.*

7.5 La estructura de grupo de una curva elíptica

Como aplicación de la teoría de superficies minimales vamos a dar una demostración abstracta (sin ecuaciones) de que las curvas elípticas son variedades abelianas. Se trata del teorema [E 10.28], aunque ahora estamos en condiciones de eliminar la hipótesis de que el cuerpo base sea perfecto.

Empezamos definiendo la operación de grupo sobre los conjuntos de puntos racionales:

Teorema 7.31 *Sea E/K una curva elíptica y $o \in E(K)$ un punto racional arbitrario. Sea K'/K una extensión arbitraria de cuerpos. Para cada par de puntos $(x, y) \in E(K') \times E(K')$, existe un único punto $m_{K'}(x, y) \in E(K')$ tal que $m_{K'}(x, y)o \sim xy$ (donde $\sim$ representa la equivalencia lineal).*

Demostración: Podemos ver a x, y, o como divisores de Cartier de grado 1 en $E(K')$, de modo que $\operatorname{grad}_{K'}(xy/o) = 1$ y, por la fórmula tras la definición [E 10.21], vemos que $\dim_{K'}(xy/o) = 2$. En particular, podemos tomar una $f \in L(xy/o)$ no nula, lo que significa que el divisor $D = (f)xy/o$ es entero, y tiene grado 1 (Teorema [E 10.13]). Por consiguiente, D ha de ser un punto racional $z \in E(K')$, un punto que cumple $zo \sim xy$. La unicidad es consecuencia inmediata del teorema [E 10.14]. ∎

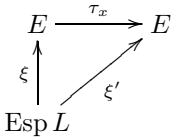
Observemos ahora que la aplicación $E(K') \longrightarrow \mathrm{Cl}^0(E_{K'})$ determinada por $x \mapsto x/o$ es inyectiva, por el teorema [E 10.14], y permite transportar a $E(K')$ la estructura de grupo de $\mathrm{Cl}^0(E_{K'})$, y el resultado es precisamente la operación que hemos llamado $m_{K'}$. Así pues, concluimos que $m_{K'}$ convierte al conjunto $E(K')$ en un grupo abeliano. Es claro que si K''/K' es una extensión arbitraria, entonces $E(K')$ es un subgrupo de $E(K'')$.

Recordemos que, según las observaciones tras la definición [E 3.66], podemos identificar los puntos de $E(K')$ con homomorfismos $f : \operatorname{Esp} K' \longrightarrow E_{K'}$ definidos sobre K' o también con homomorfismos $f : \operatorname{Esp} K' \longrightarrow E$ definidos sobre K.

Teorema 7.32 *Sea E/K una curva elíptica y fijemos un punto $o \in E(K)$. Para cada $x \in E(K)$, existe un único automorfismo $\tau_x : E \longrightarrow E$ tal que, para cada extensión K'/K, la aplicación $\tau_x : E(K') \longrightarrow E(K')$ es la traslación determinada por x.*

Demostración: Sea $L = K(E) = \mathcal{O}_{E,\xi}$, donde $\xi \in E(L)$ es el punto genérico de E. Según lo dicho, podemos considerar $\xi : \operatorname{Esp} L \longrightarrow E$ (definido sobre K), o $\xi : \operatorname{Esp} L \longrightarrow E_L$ (definido sobre L).

Fijamos un punto $x \in E(K)$ y sea $\xi' = m_L(x, \xi) \in E(L)$. Esto significa que $x\xi \sim o\xi'$ en E_L. Existe un homomorfismo τ_x (definido sobre K) que hace conmutativo el diagrama



En efecto, por el teorema [E 4.5] tenemos que ξ' se extiende a un entorno U de ξ y, por [E 7.6] dicha extensión se extiende a su vez hasta E. Si identificamos τ_x con su extensión a E_L, tenemos un diagrama análogo definido sobre L, y entonces es claro que $\tau_x(\xi) = \xi'$ (en E_L).

Si $j = 1 \times \xi : E \times_K \operatorname{Esp} L \longrightarrow E \times_K E$, tenemos el diagrama conmutativo

$$\begin{array}{ccc} E_L & \xrightarrow{j} & E \times_K E \\ {\scriptstyle\xi}\uparrow & \nearrow_{(\xi,\xi)} & \uparrow{\scriptstyle\Delta=(1,1)} \\ \operatorname{Esp} L & \xrightarrow[\xi]{} & E \end{array}$$

En particular, $j(\xi) \in \Delta_E$. Por otra parte, tenemos el diagrama conmutativo:

$$\begin{array}{ccccc} \operatorname{Esp} L & \xrightarrow{(\xi',1)} & E_L & \xrightarrow{j} & E \times_K E \\ {\scriptstyle\xi'}\downarrow & \searrow^{(\xi',\xi')} & \downarrow{\scriptstyle 1\times\xi'} & \swarrow_{1\times\tau_x} & \\ E & \xrightarrow[\Delta]{} & E \times_K E & & \end{array}$$

Observemos que $(\xi', 1)$ se identifica con ξ', de donde concluimos que

$$j(\xi') \in \Gamma'_{\tau_x} = (1 \times \tau_x)^{-1}[\Delta_E].$$

Es claro que τ_x no es constante, luego es suprayectivo, y el diagrama conmutativo siguiente:

$$\begin{array}{ccc} E & \xrightarrow{(\tau_x,1)} & E \times_K E \\ {\scriptstyle\tau_x}\downarrow & & \downarrow{\scriptstyle 1\times\tau_x} \\ E & \xrightarrow[\Delta]{} & E \times_K E \end{array}$$

muestra que Γ'_{τ_x} es la imagen de $(\tau_x, 1)$, luego es la gráfica de τ_x salvo que las coordenadas están intercambiadas. En particular, podemos ver a Γ'_{τ_x} como un divisor de Weil de $X = E \times_K E$, que es una superficie regular, luego también podemos verlo como un divisor de Cartier.

Vamos a considerar a X/E como una superficie fibrada con la segunda proyección como homomorfismo estructural. (Notemos que E no es un esquema afín, pero sólo vamos a usar propiedades elementales de las superficies fibradas, que son válidas aunque el esquema base sea proyectivo.) Observemos que $E \times_K E$ es un esquema íntegro, ya que si U y V son abiertos en E, tenemos un monomorfismo

$$\mathcal{O}_E(U) \otimes_K \mathcal{O}_E(V) \longrightarrow \mathcal{O}_E(U) \otimes_K L,$$

y el segundo anillo es uno de los anillos de la extensión de constantes E_L, que es íntegra porque las curvas elípticas son geométricamente íntegras. Notemos también que la fibra genérica es $X_\xi = E \times_K E \times_E \operatorname{Esp} L = E_L$, y la inmersión natural es $j : E_L \longrightarrow X$.

Los puntos cerrados de E_L son los puntos genéricos de los divisores horizontales de X. Por consiguiente, de $j(\xi) \in \Delta_E$ se sigue que $j(\xi)$ es el punto genérico de Δ_E. Igualmente, $j(\xi')$ es el punto genérico de Γ'_{τ_x}, $j(x)$ es el punto genérico de $\{x\} \times E$ y $j(o)$ es el punto genérico de $\{o\} \times E$.

Vamos a razonar con los cuatro casos al mismo tiempo. Para ello, llamamos $p \in X_\xi$ a cualquiera de los cuatro puntos (ξ, ξ', x, o) y $q = j(p) \in X$. Notemos que, en cualquiera de los cuatro casos, $\overline{\{q\}}$ es isomorfo a una extensión de constantes de E, luego es un conjunto algebraico sobre K geométricamente íntegro.

Los teoremas [E 8.32] y [E 8.38] nos dan que $j^*(q) = p^{e_{p/q}}$. Vamos a comprobar que el exponente es 1. Tomando un entorno afín $U = \operatorname{Esp} A$ de q en X, el homomorfismo j se corresponde con el homomorfismo natural $A \longrightarrow A \otimes_K L$. Considerando a q como ideal de A, tenemos que

$$(A \otimes_K L)/(q \otimes_K L) \cong (A/q) \otimes_K L,$$

que es un dominio íntegro, porque $\operatorname{Esp}(A/q)$ es isomorfo a un abierto de $\overline{\{q\}}$, luego es geométricamente íntegro. Además tiene dimensión 1, porque es una extensión de constantes de una K-álgebra de dimensión 1. Como obviamente $q \otimes_K L \subset p$, concluimos que $p = q \otimes_K L$ o, lo que es lo mismo, $p = q(A \otimes_K L)$, de donde también $\mathfrak{m}_p = \mathfrak{m}_q \mathcal{O}_{X_\xi, p}$, luego $e_{p/q} = 1$, como queríamos probar.

En definitiva, hemos probado que

$$j^*(\Delta_E) = \xi, \quad j^*(\Gamma'_{\tau_x}) = \xi', \quad j^*(\{x\} \times E) = x, \quad j^*(\{o\} \times E) = o.$$

De este modo, si llamamos

$$F = \frac{(\{x\} \times E)\Delta_E}{(\{o\} \times E)\Gamma'_{\tau_x}},$$

tenemos que $j^*(F) \sim 1$ en X_ξ.

Observemos ahora que $j_\xi^\sharp : K(X) \longrightarrow K(X_\xi)$ es un isomorfismo, por lo que todo divisor principal de $K(X_\xi)$ es de la forma $j^*((f))$, para cierta $f \in K(X)$ no nula. En particular,

$$j^*(F) = j^*((f))$$

para cierta $f \in K(X)$ no nula, o también: $j^*(F/(f)) = 1$. Por consiguiente, el divisor $F/(f)$ no puede contener divisores horizontales, luego es vertical. Como X/E es suave, sus fibras cerradas son reducidas, luego son isomorfas a E, es decir, son divisores primos. Así pues, $F/(f)$ es un producto de fibras cerradas. Equivalentemente, $F/(f) = p^*D$, donde D es un divisor de E y $p : X \longrightarrow E$ es la segunda proyección. Equivalentemente:

$$\frac{(\{x\} \times E)\Delta_E}{(\{o\} \times E)\Gamma'_{\tau_x}} \sim p^*D.$$

Consideremos ahora un punto cerrado $y \in E$. La fibra de y en X es

$$X_y = E \times_K E \times_E \operatorname{Esp} k(y) = E_{k(y)}.$$

En particular es irreducible y, como E/K es suave, también lo es X/E, por lo que la fibra X_y es reducida y, por consiguiente, es un divisor primo vertical. Llamemos $i_y : X_y \longrightarrow X$ a la inmersión cerrada.

Sea ahora $F = \overline{\{P\}}$ un divisor primo horizontal en X tal que $k(P) = k(E) = L$. Esto lo cumplen los cuatro divisores primos $\{x\} \times E$, $\{o\} \times E$, Δ_E y Γ'_{τ_x}, ya que sus puntos genéricos son (las imágenes en X de) x, o, ξ y $\xi' \in E_L(L)$.

El teorema 6.9 nos da[5] que $F \cdot X_y = 1$, luego F corta a X_y en un único punto p tal que $i_p(F, X_y) = 1$, lo que a su vez significa que si, como divisores de Cartier, F y X_y están definidos en p por f y $g \in \mathcal{O}_{X,p}$, entonces $l_{\mathcal{O}_{X,p}}(\mathcal{O}_{X,p}/(f,g)) = 1$, con lo que $(f,g) = \mathfrak{m}_p$, luego la imagen de f por $\mathcal{O}_{X,p} \longrightarrow \mathcal{O}_{X,p}/(g) = \mathcal{O}_{X_y,p}$ es el ideal maximal, luego $i_y^* F = p$.

Es fácil ver que x, o, y, $\tau_x(y) \in X_y$ pertenecen, respectivamente, a cada uno de los cuatro divisores que estamos manejando: $\{x\} \times E$, $\{o\} \times E$, Δ_E y Γ'_{τ_x}. Por ejemplo, en el cuarto caso tenemos el diagrama conmutativo

$$\begin{array}{ccccc} X_y & \xrightarrow{1\times y} & X & \xrightarrow{1\times\tau_x} & X \\ {\scriptstyle (y\circ\tau_x,1)}\uparrow & & {\scriptstyle (y\circ\tau_x,y\circ\tau_x)}\nearrow & & \uparrow{\scriptstyle \Delta} \\ \operatorname{Esp} k(y) & & \xrightarrow[y\circ\tau_x]{} & & E \end{array}$$

que muestra que $(1 \times \tau_x)(\tau_x(y)) \in \Delta_E$, luego $\tau_x(y) \in \Gamma'_{\tau_x}$.

Así pues, hemos probado que

$$i_y^*(\{x\} \times E) = x, \quad i_y^*(\{o\} \times E) = o, \quad i_y^*(\Delta_E) = y, \quad i_y^*(\Gamma'_{\tau_x}) = \tau_x(y).$$

Por otra parte, el diagrama conmutativo

$$\begin{array}{ccc} X_y & \xrightarrow{i_y} & X \\ \downarrow & & \downarrow{\scriptstyle p} \\ \operatorname{Esp} k(y) & \xrightarrow[y]{} & E \end{array}$$

muestra que $i_y^*(p^*\mathcal{O}_X(D)))$ es un haz libre, ya que todos los haces en $\operatorname{Esp} k(y)$ lo son. Aplicando todo esto a la relación que teníamos entre divisores de X, obtenemos la relación $xy/o\tau_x(y) \sim 1$ en $E_{k(y)}$.

Si, en particular, aplicamos esto a un punto $y \in E(K')$, tenemos un homomorfismo $y : \operatorname{Esp} K' \longrightarrow E$ definido sobre K que factoriza como

$$\operatorname{Esp} K' \longrightarrow \operatorname{Esp} k(y) \longrightarrow E,$$

y la relación que tenemos en $E_{k(y)}$ se extiende a $E_{K'}$, y así concluimos que $\tau_x(y) = m_{K'}(x,y)$, es decir, que $\tau_x(y)$ es la traslación de y por x.

[5]Podemos cambiar X por $X' = E \times_K S$, donde $S \subset E$ es un entorno afín de y, de modo que X' es una superficie fibrada sobre un dominio de Dedekind.

Observemos que esta propiedad aplicada cuando K' es la clausura algebraica de K nos da que $\tau_x : E \longrightarrow E$ es único, en virtud del teorema [E 3.67]. Falta probar que $\tau_x : E \longrightarrow E$ es un automorfismo, pero esto es consecuencia de la unicidad, en virtud de la cual $\tau_0 = 1$ y $\tau_x \circ \tau_y = \tau_{m_K(x,y)}$ luego, en particular, $\tau_x \circ \tau_{-x} = \tau_{-x} \circ \tau_x = 1$, lo que prueba que, en efecto, τ_x es un automorfismo. ∎

Finalmente estamos en condiciones de probar que las estructuras de grupo dadas por el teorema 7.31 están inducidas por una estructura de variedad abeliana sobre la curva elíptica:

Teorema 7.33 *Si E/K es una curva elíptica y $o \in E(K)$ es un punto racional prefijado, entonces E/K admite una estructura de variedad abeliana tal que, para toda extensión K'/K la estructura de grupo inducida en $E(K')$ es la dada por la aplicación $m_{K'}$.*

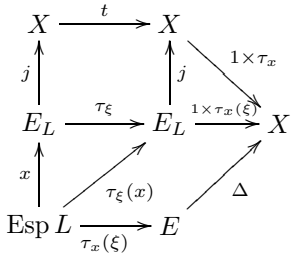
Demostración: Sea $L = K(E)$. Para cada abierto afín $S \subset E$, la superficie $X_S = E \times_K S$ es una superficie aritmética sobre S cuya fibra genérica es

$$E \times_K S \times_S \operatorname{Esp} L = E \times_K \operatorname{Esp} L = E_L,$$

que es una curva elíptica (que cumple $p_a(E_L) = 1$), y no tiene divisores excepcionales porque sus fibras cerradas son todas isomorfas a extensiones de constantes de E. El teorema 7.21 nos da que X_S es minimal.

Si $\xi \in E$ es el punto genérico, podemos verlo como punto racional $\xi \in E_L$, por lo que tenemos definida la traslación genérica $\tau_\xi : E_L \longrightarrow E_L$, definida sobre L. Por 7.26, se extiende a un único S-homomorfismo $t_S : E \times_K S \longrightarrow E \times_K S$. La unicidad permite extender estos homomorfismos a un único homomorfismo $t : E \times_K E \longrightarrow E \times_K E$ definido sobre E. Sea $m : E \times_K E \longrightarrow E$ la composición de t con la primera proyección. Claramente m está definido sobre K.

Tomemos un punto $x \in E(K)$ y formemos el diagrama conmutativo:

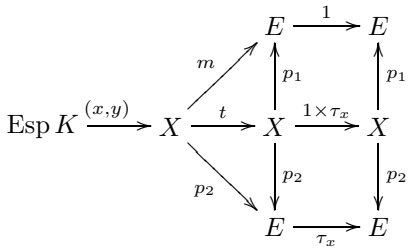


Notemos que el rombo inferior conmuta porque

$$\tau_x(\xi) = m_L(x, \xi) = m_L(\xi, x) = \tau_\xi(x).$$

Del diagrama se desprende que $(1 \times \tau_x)(t(j(x))) \in \Delta_E$, pero $j(x)$ es el punto genérico de $\{x\} \times E$, luego $(1 \times \tau_x)[t[\{x\} \times E]] \subset \Delta_E$. Fijado otro punto

$y \in E(K)$, consideramos el diagrama conmutativo



Puesto que $(1 \times \tau_x)(t(x,y)) \in \Delta_E$, sus dos proyecciones coinciden y, por la conmutatividad del diagrama, éstas son: $m(x,y) = \tau_x(y) = m_K(x,y)$.

Para tener una estructura de variedad abeliana necesitamos también un automorfismo $i : E \longrightarrow E$ (definido sobre K) que a cada elemento de $E(K)$ le asigne su inverso. La podemos definir como la composición

$$i : E \xrightarrow{(o,1)} E \times_K E \xrightarrow{t^{-1}} E \times_K E \xrightarrow{p_1} E.$$

En efecto, observemos ante todo que cada punto racional $p \in E \times_K E$ está completamente determinado por sus proyecciones, ya que si éstas son x e y, entonces p está en la intersección de la fibra X_y y el divisor primo horizontal $\{x\} \times E$, y dicha intersección se reduce a un punto por el teorema 6.9 (podemos sustituir E por un abierto afín para considerar superficies fibradas sobre un dominio de Dedekind).

Así pues, dado $x \in E(K)$, tenemos que $((o,1) \circ t^{-1})(x) \in X(K)$ tiene proyecciones $i(x)$ y x, luego al aplicarle t y p_1 obtenemos

$$m_K(i(x), x) = ((o,1) \circ p_1)(x) = o(x) = o.$$

Esto prueba que $i(x)$ es el inverso de x.

Falta probar que m e i inducen la estructura de grupo no sólo en $E(K)$, sino en $E(K')$ para cualquier extensión K'/K. Equivalentemente, hemos de ver que las extensiones de constantes $m_{K'}$ e $i_{K'}$ son los homomorfismos m e i correspondientes a la curva elíptica $E_{K'}$.

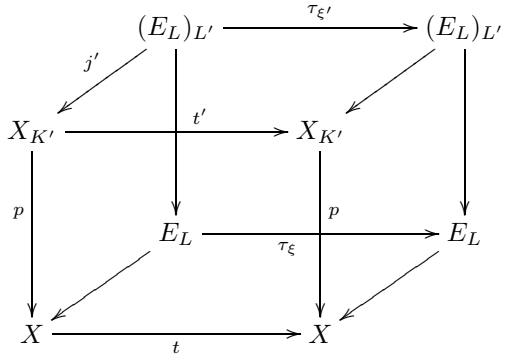
Notemos que $X' = E_{K'} \times_{K'} E_{K'} = (E \times_K E) \times_K \operatorname{Esp} K' = X_{K'}$, lo que nos permite hablar de la extensión de constantes $m_{K'} : X_{K'} \longrightarrow E_{K'}$.

Observemos en primer lugar que, si llamamos $L' = K(E_{K'})$, entonces

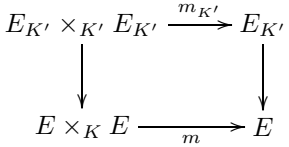
$$(E_{K'})_{L'} = E \times_K \operatorname{Esp} K' \times_{K'} \operatorname{Esp} L' = E \times_K \operatorname{Esp} L' = E_{L'}$$

$$= E \times_K \operatorname{Esp} L \times_L \operatorname{Esp} L' = (E_L)_{L'}.$$

Es claro que la proyección $E_{K'} \longrightarrow E$ transforma el punto genérico $\xi' \in E_{K'}$ en el punto genérico $\xi \in E$, luego la proyección $E_{L'} \longrightarrow E_L$ también transforma ξ' en ξ, lo que significa que el punto racional ξ de E_L se identifica con ξ' a través de la inclusión $E(L) \subset E(L')$. Esto nos da la conmutatividad de la cara posterior del cubo



La cara superior y la inferior conmutan por definición de t y t', mientras que las caras laterales conmutan obviamente. De aquí se sigue fácilmente que $j' \circ t' \circ p = j' \circ p \circ t$ o, lo que es lo mismo, que los homomorfismos $t' \circ p$ y $p \circ t$ coinciden sobre la fibra genérica de $X_{K'}$, luego son iguales por 5.26. Esto prueba la conmutatividad de la cara anterior del cubo. Componiendo con las proyecciones, se sigue inmediatamente la conmutatividad del diagrama



La conmutatividad del diagrama correspondiente para i se sigue igualmente de la conmutatividad de la cara anterior del cubo. ∎

Capítulo VIII

Modelos de curvas elípticas

En el capítulo anterior hemos visto que toda curva proyectiva íntegra geométricamente regular de género ≥ 1 (en particular toda curva elíptica) definida sobre el cuerpo de cocientes de un dominio de Dedekind admite un modelo regular minimal, único salvo isomorfismo. En este capítulo estudiaremos con más detalle el caso de las curvas elípticas.

La conexión entre los modelos regulares minimales y la teoría clásica sobre curvas elípticas se establece a través de los modelos de Weierstrass. Para establecer dicha conexión dedicaremos la primera sección a caracterizar intrínsecamente los modelos de Weierstrass, es decir, en términos de su geometría de superficie fibrada. Así, en la segunda sección podremos demostrar que, bajo ciertas hipótesis, contrayendo a puntos todas las componentes irreducibles menos una de cada fibra cerrada del modelo regular minimal, se obtiene un modelo de Weierstrass. Esto siempre es posible cuando el dominio de Dedekind es un dominio de ideales principales, en particular en el caso local, es decir, cuando se trata de un anillo de valoración discreta.

En la tercera sección entenderemos mejor lo que sucede: es posible pasar por contracción del modelo regular minimal a un modelo de Weierstrass cuando la curva elíptica admite una ecuación de Weierstrass minimal, en el sentido de la teoría clásica, lo cual siempre es posible en el caso local, pero no siempre en el caso global. Esta relación entre el modelo regular minimal y los modelos de Weierstrass nos permitirá reformular en términos del primero la teoría clásica sobre los tipos de reducción de curvas elípticas, de lo cual nos encargaremos en la sección cuarta. En la última refinaremos esta teoría clasificando las posibles fibras cerradas de los modelos regulares minimales.

8.1 Modelos de Weierstrass

Recordemos (definición 5.9) que el modelo de Weierstrass sobre un dominio de Dedekind D asociado a una ecuación de Weierstrass

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

con coeficientes en D y discriminante no nulo, es el esquema proyectivo W/S (donde $S = \operatorname{Esp} D$) definido por (la homogeneización de) la ecuación. Sabemos que es una superficie fibrada normal cuyas fibras cerradas son las curvas definidas por las reducciones de la ecuación módulo los divisores primos de D, de modo que todas ellas son geométricamente íntegras, y todas salvo un número finito de ellas son curvas elípticas y, en particular, geométricamente regulares. Las que no lo son, tienen un único punto que no es geométricamente regular y que, de hecho, es singular.

Así pues, W/S es suave salvo a lo sumo en un número finito de puntos, que son los únicos posibles puntos singulares de W (aunque no lo son necesariamente).

Si llamamos o_η al punto infinito de la fibra genérica W_η, el teorema 5.10 prueba que el divisor horizontal $O = \overline{\{o_\eta\}}$ corta a cada fibra cerrada en su correspondiente punto infinito. Además, sabemos que, si una cúbica definida por una ecuación de Weierstrass tiene un punto singular, éste no puede ser su punto infinito, así que O está contenido en el abierto de puntos suaves de W.

Observemos ahora que la inmersión cerrada $i : W \longrightarrow \mathrm{P}^2_D$ es una inmersión regular. En efecto, el haz $\mathcal{I} = \mathrm{N}(i^\#)$ de ideales de $\mathcal{O}_{\mathrm{P}^2_D}$ que define a W es localmente principal, pues, en cada abierto afín $D(X)$, $D(Y)$, $D(Z)$, está generado por la deshomogeneización correspondiente de la ecuación de Weierstrass. En particular, el núcleo de cada homomorfismo $\mathcal{O}_{\mathrm{P}^2_D,x} \longrightarrow \mathcal{O}_{W,x}$ está generado por un elemento no nulo, que es regular, ya que los anillos son dominios íntegros.

Esto implica que W/S es localmente una intersección completa y, en particular, que está definido el haz canónico $\omega_{W/S}$. Si W/S fuera suave, tendríamos que $\omega_{W/S} = \Omega^1_{W/S}$, pero esto no es cierto en general. Vamos a relacionar ambos haces. En principio tenemos que

$$\omega_{W/S} = \mathcal{N}_{W/\,\mathrm{P}^2_D} \otimes_{\mathcal{O}_W} i^*\Omega^2_{\mathrm{P}^1_D\,/D}.$$

El teorema [E 7.41] nos da la sucesión exacta

$$i^*(\mathcal{I}/\mathcal{I}^2) \longrightarrow i^*(\Omega^1_{\mathrm{P}^2_D\,/D}) \longrightarrow \Omega^1_{W/D} \longrightarrow 0,$$

donde $\mathcal{I}$ es el haz de ideales de P^2_D que define a W. Observemos que $\mathcal{I}$ es localmente principal: si U es un abierto afín contenido en uno de los tres subespacios afines $D(X)$, $D(Y)$ o $D(Z)$, entonces $\mathcal{I}(U)$ está generado por la deshomogeneización correspondiente de la ecuación de Weierstrass.

Definimos un homomorfismo

$$\psi : i^*(\mathcal{I}/\mathcal{I}^2) \otimes_{\mathcal{O}_W} \Omega^1_{W/S} \longrightarrow i^*\Omega^2_{\mathrm{P}^2_D\,/D}$$

del modo siguiente: fijamos un abierto afín $U \subset \mathrm{P}^2_D$ (tal que $\mathcal{I}(U)$ sea principal) y tomamos $V = i^{-1}[U]$, de forma que V recorre una base de abiertos afines de W. Tenemos entonces que $\mathcal{O}_W(V) = \mathcal{O}(U)/\mathcal{I}(U)$, así como una sucesión exacta de $\mathcal{O}(V)$-módulos

$$\mathcal{I}(U)/\mathcal{I}^2(U) \xrightarrow{\delta} \Omega^1_{\mathcal{O}(U)/D} \otimes_{\mathcal{O}(U)} \mathcal{O}_W(V) \xrightarrow{\alpha} \Omega^1_{\mathcal{O}(V)/D} \longrightarrow 0,$$

donde $\delta([f]) = df \otimes 1$. Llamamos

$$\psi_V : (\mathcal{I}(U)/\mathcal{I}(U)^2) \otimes_{\mathcal{O}(V)} \Omega^1_{\mathcal{O}(V)/D} \longrightarrow \Omega^2_{\mathcal{O}(U)/D} \otimes_{\mathcal{O}(U)} \mathcal{O}_W(V)$$

al homomorfismo dado por

$$\psi_V([f] \otimes \alpha(\omega)) = (df \wedge \omega) \otimes 1.$$

Está bien definido porque $\mathcal{I}(U)$ está generado por un elemento f_0, luego el núcleo de α está generado por df_0, y se cumple que $df_0 \wedge df_0 = 0$.

Es claro que los homomorfismos ψ_V determinan un único homomorfismo de haces ψ. Teniendo en cuenta que $i^*(\mathcal{I}/\mathcal{I}^2)$ es el haz dual de $\mathcal{N}_{W/\,\mathrm{P}^2_D}$, multiplicando por este último haz, vemos que ψ induce un homomorfismo

$$\phi : \Omega^1_{W/S} \longrightarrow \mathcal{N}_{W/\,\mathrm{P}^2_D} \otimes_{\mathcal{O}_X} i^*\Omega^2_{\mathrm{P}^2_D/D} = \omega_{W/S}.$$

Vamos a describirlo explícitamente. Para ello consideramos los abiertos afines $U = D(Z)$, $U' = D(Y)$ en P^2_D, y sean V y V' sus antiimágenes en W. Notemos que $W = V \cup V'$, pues un ideal primo de $D[X,Y,Z]$ que contenga a Y, Z y a la ecuación de Weierstrass F, contiene también a W.

Podemos identificar $V = \mathrm{Esp}(D[X,Y]/(f))$, donde $f = F(X,Y,1)$ es la deshomogeneización de la ecuación de Weierstrass. Las clases de X e Y módulo f se identifican con $x = X/Z$, $y = Y/Z \in \mathcal{O}_X(V)$.

Similarmente, $V' = \mathrm{Esp}(D[X,Z]/(g))$, donde $g = F(X,1,Z)$. Ahora las clases de X y Z se identifican con $s = X/Y$, $t = Z/Y \in \mathcal{O}_X(V')$. Así, en $\mathcal{O}_X(V \cap V')$ tenemos las relaciones $s = x/y$, $t = 1/y$.

Nos centramos primeramente en el abierto V. Es claro que $[f]$ es una $\mathcal{O}_X(V)$-base de $\mathcal{I}(U)/\mathcal{I}(U)^2$, así como que $dX \wedge dY$ es una D-base de $\Omega^2_{D[X,Y]/D}$, luego $w = [f]^* \otimes ((dX \wedge dY) \otimes 1)$ es una base de

$$\omega_{X/S}(V) = (\mathcal{I}(U)/\mathcal{I}(U)^2)^* \otimes_{\mathcal{O}_X(V)} (\Omega^2_{D[X,Y]/D} \otimes_{D[X,Y]} \mathcal{O}_X(V)).$$

Ahora vemos que

$$\phi_V(dx) = (1 \otimes \psi_U)([f]^* \otimes ([f] \otimes dx)) = [f]^* \otimes (df \wedge dx)$$

$$= [f]^* \left(\frac{\partial f}{\partial x}\, dx + \frac{\partial f}{\partial y}\, dy \right) \wedge dx = -\frac{\partial f}{\partial y}\, [f]^* \otimes ((dX \wedge dY) \otimes 1)$$

$$= (2y + a_1 x + a_3)\, w$$

Observemos que $h = 2y + a_1x + a_3$ no puede ser 0 en $\mathcal{O}_W(V)$, ya que esto exigiría que $2 = a_1 = a_3 = 0$, y esto implica que el discriminante de la ecuación de Weierstrass es 0. Por consiguiente, podemos tomar un abierto $V' \subset V$ suave sobre S y tal que $2y + a_1x + a_3$ sea una unidad de $\mathcal{O}_W(V')$. Entonces $\Omega^1_{V'/S}$ es un $\mathcal{O}_W(V')$-módulo libre de rango 1 (teorema [E 7.53]) y

$$\phi_{V'} \left(\frac{dx}{2y + a_1x + a_3} \right)$$

es una base de $\omega_{W/S}(V')$. Por consiguiente, $\phi_{V'}$ es suprayectivo, y todo epimorfismo entre módulos libres de rango 1 es un isomorfismo. Así pues, obtenemos que $\Omega^1_{W/S}|_{V'} \cong \omega_{W/S}|_{V'}$ y, en particular, si llamamos ξ al punto genérico de W, resulta que ϕ induce un isomorfismo $\Omega^1_{W/S,\xi} \cong \omega_{W/S,\xi}$.

Observemos que $\omega_{W/S,\xi} = \Omega^1_{K(W)/K}$ es un espacio vectorial sobre $K(W)$ de dimensión 1. Está generado por dx y dy, pero, como x e y cumplen la relación $f(x,y) = 0$, vemos que

$$\frac{\partial f}{\partial x}\,dx + \frac{\partial f}{\partial y}\,dy = 0,$$

de modo que

$$dy = \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}\,dx,$$

luego dx es una base de $\Omega^1_{K(W)/K}$.

Como W es un esquema íntegro, el teorema [E 5.21] nos da que las restricciones de los haces $\omega_{W/S}$ y $\Omega^1_{W/S}$ son inyectivas, luego podemos identificarlos con subhaces del haz constante $\Omega^1_{K(W)/K} = dx\,\mathcal{O}_W$. En estos términos, acabamos de ver que

$$\omega_{W/S}|_V = w\mathcal{O}_W|_V$$

se identifica con $\omega\,\mathcal{O}_{W|_V}$, donde

$$\omega = \frac{dx}{2y + a_1x + a_3} \in \Omega^1_{K(W)/K}.$$

Razonando análogamente con el abierto V', concluimos que

$$\omega_{W/S}|_{V'} = w'\mathcal{O}_W|_{V'}$$

se identifica con $\omega'\mathcal{O}_{W|_{V'}}$, donde

$$\omega' = -\left(\frac{\partial g}{\partial s}\right)^{-1} dt.$$

Concretamente:

$$g(s,t) = s^3 + a_2s^2t + a_4st^2 + a_6t^3 - t - a_1st - a_3t^2,$$

luego

$$\omega' = \frac{dt}{a_1t - 3s^2 - 2a_2st - a_4t^2}.$$

Usando las relaciones $s = x/y$, $t = 1/y$ en $K(W)$ obtenemos que

$$dt = -(1/y^2)dy = -\frac{1}{y^2}\,\frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}\,dx,$$

El denominador de ω' es $a_1/y - 3x^2/y^2 - 2a_2x/y^2 - a_4/y^2$, luego

$$\omega' = -\frac{1}{a_1y - 3x^2 - 2a_2x - a_4}\,\frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}\,dx = \omega.$$

Así pues, $\omega \in \Omega^1_{K(W)/K}$ se identifica tanto con un elemento $w \in \omega_{W/S}(V)$ como con un elemento $w' \in \omega_{W/S}(V')$. Esto significa que w y w' coinciden en un abierto y, por consiguiente, coinciden en $V \cap V'$. Así pues, se extienden a un elemento $\omega \in \omega_{W/S}(W)$.

El hecho de que $\omega_{W/S}|_V = \omega|_V \mathcal{O}_W|_V$ y $\omega_{W/S}|_{V'} = \omega|_{V'}\mathcal{O}_W|_{V'}$ implica que, en definitiva, $\omega_{W/S} = \omega\mathcal{O}_W$, de modo que el haz canónico es libre.

El teorema siguiente resume los resultados que hemos obtenido:

Teorema 8.1 *Sea D un dominio de Dedekind, sea K su cuerpo de cocientes, sea $S = \operatorname{Esp} D$, sea W/S el modelo asociado a una ecuación de Weierstrass con coeficientes en D y sea o_η el punto infinito de su fibra genérica. Entonces:*

a) El divisor $O = \overline{\{o_\eta\}}$ está formado por los puntos infinitos de todas las fibras, y todos ellos son suaves en W.

b) Las fibras de W son geométricamente íntegras.

c) W/S es localmente una intersección completa y $\omega_{W/S} = \omega\mathcal{O}_X$, donde

$$\omega = \frac{dx}{2y + a_1x + a_3} \in \Omega^1_{K(W)/K}.$$

d) Si $\pi : W \longrightarrow S$ es el homomorfismo estructural, $\pi_*\omega_{W/S} = \omega\mathcal{O}_S$.

Demostración: Sólo falta probar la última propiedad, pero ésta es consecuencia del teorema 5.27, que nos da la igualdad $\pi_*\mathcal{O}_W = \mathcal{O}_S$. ∎

El resto de esta sección está dedicado a probar que estas propiedades caracterizan a los modelos de Weierstrass (teorema 8.6). Para ello necesitamos algunos resultados previos.

Teorema 8.2 *Sea D un anillo de valoración discreta, sea K su cuerpo de cocientes, sea (π) su ideal maximal y $k = D/\pi D$ su cuerpo de restos. Sea M un D-módulo finitamente generado y $M[\pi] = \{m \in M \mid \pi m = 0\}$. Entonces*

$$\dim_k(M \otimes_D k) = \dim_K(M \otimes_D K) + \dim_k M[\pi].$$

Demostración: Consideremos una sucesión exacta

$$0 \longrightarrow M' \longrightarrow L \xrightarrow{\phi} M \longrightarrow 0,$$

donde L es un D-módulo libre de rango finito. Notemos que, al ser D un dominio de ideales principales, el submódulo M' también es libre.[1] Multiplicando por $\otimes_D k$ obtenemos una sucesión exacta

$$M'/\pi M' \longrightarrow L/\pi L \longrightarrow M/\pi M \longrightarrow 0.$$

[1] Teorema 7.29 de mi libro de Álgebra.

Es fácil determinar el núcleo del primer homomorfismo, con lo que obtenemos una sucesión exacta

$$0 \longrightarrow (\pi L \cap M')/\pi M' \longrightarrow M'/\pi M' \longrightarrow L/\pi L \longrightarrow M/\pi M \longrightarrow 0.$$

El homomorfismo $\pi L \longrightarrow M$ dado por $\pi x \mapsto \phi(x)$ induce un isomorfismo

$$(\pi L \cap M')/\pi M' \cong M[\pi].$$

Por consiguiente:

$$\dim_k(M/\pi M) - \dim_k M[\pi] = \dim_k(L/\pi L) - \dim_k(M'/\pi M')$$

$$= \dim_k L \otimes_D k - \dim_k M' \otimes_D k = \dim_K L \otimes_D K - \dim_K M' \otimes_D K$$

$$= \dim_K M \otimes_D K.$$

En la última igualdad hemos usado que K es plano sobre D, por lo que $\otimes_D K$ conserva la exactitud de la sucesión exacta de partida. ∎

Teorema 8.3 *Sea D un anillo de valoración discreta, sea $S = \operatorname{Esp} D$, sea η el punto genérico de S y s el punto cerrado. Sea $f : X \longrightarrow S$ un homomorfismo proyectivo y $\mathcal{F}$ un haz coherente en X plano sobre S. Fijado $p \geq 1$, se cumple que*

$$\dim_{k(s)} H^p(X_s, \mathcal{F}_s) \geq \dim_{k(\eta)} H^p(X_\eta, \mathcal{F}_\eta).$$

Además, se da la igualdad si y sólo si $H^p(X, \mathcal{F})$ es un D-módulo libre y el homomorfismo canónico

$$H^p(X, \mathcal{F}) \otimes_D k(s) \longrightarrow H^p(X_s, \mathcal{F}_s)$$

es un isomorfismo.

Demostración: Sea π un primo en D. Como $\mathcal{F}$ es plano sobre D, es libre de torsión [AC A.8], luego tenemos una sucesión exacta

$$0 \longrightarrow \mathcal{F} \xrightarrow{\pi} \mathcal{F} \longrightarrow \mathcal{F}/\pi\mathcal{F} \longrightarrow 0.$$

De ella deducimos la sucesión exacta

$$H^p(X, \mathcal{F}) \xrightarrow{\pi} H^p(X, \mathcal{F}) \longrightarrow H^p(X, \mathcal{F}/\pi\mathcal{F}) \longrightarrow H^{p+1}(X, \mathcal{F}) \xrightarrow{\pi} H^{p+1}(X, \mathcal{F})$$

que podemos reducir a

$$0 \longrightarrow H^p(X, \mathcal{F})/\pi H^p(X, \mathcal{F}) \longrightarrow H^p(X, \mathcal{F}/\pi\mathcal{F}) \longrightarrow H^{p+1}(X, \mathcal{F})[\pi] \longrightarrow 0.$$

Observemos que, si llamamos $p : X_s \longrightarrow X$ a la inmersión cerrada natural, entonces $p_*\mathcal{F}_s = \mathcal{F}/\pi\mathcal{F}$, luego, según [E 6.20], $H^p(X_s, \mathcal{F}_s) = H^p(X, \mathcal{F}/\pi\mathcal{F})$, y la sucesión exacta anterior puede escribirse así:

$$0 \longrightarrow H^p(X, \mathcal{F}) \otimes_D k(s) \longrightarrow H^p(X_s, \mathcal{F}_s) \longrightarrow H^{p+1}(X, \mathcal{F})[\pi] \longrightarrow 0.$$

Por otra parte, como $k(\eta)$ es plano sobre D, el teorema [E 6.15] nos da que

$$H^p(X_\eta, \mathcal{F}_\eta) \cong H^p(X, \mathcal{F}) \otimes_D k(\eta),$$

luego, teniendo en cuenta el teorema anterior,

$$\dim_{k(s)} H^p(X_s, \mathcal{F}_s) = \dim_{k(s)} H^p(X, \mathcal{F}) \otimes_D k(s) + \dim_{k(s)} H^{p+1}(X, \mathcal{F})[\pi]$$

$$= \dim_{k(\eta)} H^p(X_\eta, \mathcal{F}_\eta) + \dim_{k(s)} H^p(X, \mathcal{F})[\pi] + \dim_{k(s)} H^{p+1}(X, \mathcal{F})[\pi].$$

Esto nos da la desigualdad del enunciado, y la igualdad equivale a que

$$H^p(X, \mathcal{F})[\pi] = H^{p+1}(X, \mathcal{F})[\pi] = 0.$$

A su vez, esto equivale a que los D-módulos $H^p(X, \mathcal{F})$ y $H^{p+1}(X, \mathcal{F})$ sean libres de torsión. Como D es un dominio de ideales principales, esto equivale a su vez a que sean libres. Por otra parte, en vista de la sucesión exacta, la condición $H^{p+1}(X, \mathcal{F})[\pi] = 0$ equivale también al isomorfismo del enunciado. ∎

Teorema 8.4 *Sea C/k una curva proyectiva íntegra de género $p_a(C) = 1$. Supongamos que C contiene un punto p geométricamente regular y racional sobre k. Entonces:*

a) $\dim_k H^0(C, \mathcal{O}_C) = \dim_k H^1(C, \mathcal{O}_C) = 1$.

b) Para $n \geq 1$, se cumple que $\dim_k H^0(C, \mathcal{O}_C(p^n)) = n$, $H^1(C, \mathcal{O}_C(p^n)) = 0$.

Demostración: Observemos en primer lugar que el punto p tiene un entorno de puntos regulares. Por [E 8.21], como divisor de Weil, p se corresponde con un divisor de Cartier en dicho entorno, luego existe un entorno afín U de p y un $f \in \mathcal{O}_C(U)$ tal que, para cada punto cerrado $P \in U$, se cumple que

$$v_P(f) = \begin{cases} 1 & \text{si } P = p, \\ 0 & \text{si } P \neq p. \end{cases}$$

Tomando $1 \in \mathcal{O}_C(C \setminus \{p\})$, formamos un divisor de Cartier de C que podemos identificar con p. Esto da sentido al apartado b) del enunciado. Observemos que $f \in \mathcal{O}^*_{C,P}$ para todo $P \in U$, $P \neq p$, y, trivialmente, $1 \in \mathcal{O}^*_{C,P}$ para todo $P \in C \setminus \{p\}$. Esto implica que $\mathcal{O}_C(p)|_{C\setminus\{p\}} = \mathcal{O}_C|_{C\setminus\{p\}}$.

a) Por [E 4.26] sabemos que $H^0(C, \mathcal{O}_C)$ es una extensión finita de k. En particular es un subcuerpo de $K(C)$ entero sobre $\mathcal{O}_{C,p}$. Ahora bien, como p es normal, tenemos que $H^0(C, \mathcal{O}_C) \subset \mathcal{O}_{C,p}$. De aquí obtenemos una inclusión $H^0(C, \mathcal{O}_C) \longrightarrow k(p) = k$, luego $H^0(C, \mathcal{O}_C) = k$. La hipótesis $p_a(C) = 1$ implica entonces que $H^1(C, \mathcal{O}_C) = 0$.

b) Tomemos $u \in H^0(C, \mathcal{O}_C(p))$ y veamos que $u \in k$.

Notemos que $u|_{C\setminus\{p\}} \in \mathcal{O}_C(C \setminus \{p\})$, luego, si $u \notin k$ ha de ser $u \notin \mathcal{O}_{C,p}$. Como $(u)p \geq 1$, tenemos que $v_P(u) \geq 0$ para todo punto cerrado $P \neq p$ y

$v_p(u) = -1$. Por [E 10.13] sabemos que $\mathrm{grad}(u) = 0$, luego, visto como divisor de Weil, ha de ser $(u) = q/p$, para un cierto punto racional $q \in C$, $q \neq p$.

De este modo, si $r \in C$ es un punto cerrado distinto de p y q, tenemos que $v_r(u) = 0$, es decir, que $l(\mathcal{O}_{C,r}/(u)) = 0$, luego $u \in \mathcal{O}_{C,r}^*$.

Como p es regular, $v_p(1/u) = 1$ implica que $1/u \in \mathcal{O}_{C,p}$ y, más en general, que $1/u \in \mathcal{O}_C(C \setminus \{q\})$.

Consideremos ahora el espacio proyectivo $\mathrm{P}^1_k = \mathrm{Proy}(k[X,Y])$, y en él los abiertos afines $U = D(X) = \mathrm{Esp}(k[Y/X])$, $V = D(Y) = \mathrm{Esp}(k[X/Y])$. El homomorfismo $k[Y/X] \longrightarrow \mathcal{O}_C(C \setminus \{p\})$ dado por $Y/X \mapsto u$ induce un homomorfismo $C \setminus \{p\} \longrightarrow U$ y, análogamente, el homomorfismo $k[X/Y] \longrightarrow \mathcal{O}_C(C \setminus \{q\})$ dado por $X/Y \mapsto 1/u$ induce un homomorfismo $C \setminus \{q\} \longrightarrow V$.

Si $G = \mathrm{Esp}\, A$ es un abierto afín en $C \setminus \{p,q\}$ y $W = U \cap V$, podemos identificar $W = \mathrm{Esp}\, k[t,1/t]$, de modo que las inclusiones $W \longrightarrow U$ y $W \longrightarrow V$ se corresponden respectivamente con los monomorfismos $k[X/Y] \longrightarrow k[t,1/t]$ y $k[Y/X] \longrightarrow k[t,1/t]$ dados por $X/Y \mapsto t$, $Y/X \mapsto 1/t$.

El homomorfismo $G \longrightarrow U$ es el asociado al homomorfismo $k[Y/X] \longrightarrow A$ dado por $Y/X \mapsto u$, que factoriza como

$$\begin{array}{ccc} k[Y/X] & \longrightarrow & k[t,1/t] \\ & \searrow & \downarrow \\ & & A \end{array}$$

donde la flecha vertical está determinada por $t \mapsto u$. Esto significa que $G \longrightarrow U$ factoriza como $G \longrightarrow W \longrightarrow U$ y, análogamente, $G \longrightarrow V$ factoriza como $G \longrightarrow W \longrightarrow V$, con el mismo homomorfismo $G \longrightarrow W$. Equivalentemente, lo que tenemos es que ambos homomorfismos son el mismo o, también que los homomorfismos $C \setminus \{p\} \longrightarrow U$ y $C \setminus \{q\} \longrightarrow V$ coinciden en su dominio común y, por lo tanto, determinan un homomorfismo $\phi : C \longrightarrow \mathrm{P}^1_k$ (definido sobre k).

Si $\mathrm{Esp}\, A$ es un entorno afín de p, como u no es una unidad de A (ya que no lo es de $\mathcal{O}_{C,p}$), podemos tomar un ideal $\mathfrak{p} \in \mathrm{Esp}\, A$ tal que $u \in \mathfrak{p}$, con lo que $(Y/X) \subset \phi(\mathfrak{p})$ y, como (Y/X) es maximal, $\phi(\mathfrak{p}) = (Y/X)$. Visto como elemento de $\mathrm{P}^1_k = \mathrm{Proy}(k[X,Y])$, el ideal (Y/X) es (Y). Esto prueba que (Y) está en la imagen de ϕ, y análogamente se prueba que lo está (X), luego ϕ no es constante, luego es un homomorfismo finito (por [E 10.1]).

Llamemos $\infty = (Y)$, que es un punto racional de P^1_k que, visto como divisor de Cartier, cumple $\phi^*\infty = p$. En efecto, el divisor ∞ está representado por los pares $(U, Y/X)$, $(V,1)$, luego $\phi^*\infty$ está representado por los pares $(\phi^{-1}[U], u)$, $(\phi^{-1}[V],1)$, que claramente representan al divisor p. Como ambos divisores tienen grado 1, el teorema [E 10.9] implica que $k(C) = k(\mathrm{P}^1_k)$, es decir, que ϕ es un homomorfismo finito birracional. Como P^1_k es normal, esto implica que ϕ es un isomorfismo, luego $p_a(C) = p_a(\mathrm{P}^1_k) = 0$, contradicción.

Con esto hemos probado que $H^0(C, \mathcal{O}_C(p)) = k$ o, equivalentemente, que $\dim_k H^0(C, \mathcal{O}_C(p)) = 1$.

Por hipótesis, $p_a(C) = 1 - \chi_k(\mathcal{O}_C) = 1$, luego $\chi_k(\mathcal{O}_C) = 0$. El teorema [E 10.11] nos da entonces que $\chi_k(\mathcal{O}_C(p)) = 1$, luego $\dim_k H^1(C, \mathcal{O}_C(p)) = 0$.

El teorema [E 10.10] nos da una sucesión exacta

$$0 \longrightarrow \mathcal{O}_C(p^{n-1}) \longrightarrow \mathcal{O}_C(p^n) \longrightarrow \mathcal{O}_C(p)|_p \longrightarrow 0,$$

de la que deducimos la sucesión exacta

$$0 \longrightarrow H^0(C, \mathcal{O}_C(p^{n-1})) \longrightarrow H^0(C, \mathcal{O}_C(p^n)) \longrightarrow V$$

$$\longrightarrow H^1(C, \mathcal{O}_C(p^{n-1})) \longrightarrow H^1(C, \mathcal{O}_C(p^n)) \longrightarrow 0,$$

donde $V = H^0(p, \mathcal{O}_C(p)|_p) \cong k$. En efecto, si U es un entorno afín de p tal que $\mathcal{O}_C(p)|_U \cong \mathcal{O}_C(U)$, entonces $\mathcal{O}_C(p)|_p \cong \mathcal{O}_C|_p \cong \mathcal{O}_p$, luego

$$H^0(p, \mathcal{O}_C(p)|_p) \cong \mathcal{O}_p(\{p\}) = k(p) = k.$$

Ahora basta razonar inductivamente: Si el teorema es cierto para $n-1$, la sucesión exacta se reduce a

$$0 \longrightarrow H^0(C, \mathcal{O}_C(p^{n-1})) \longrightarrow H^0(C, \mathcal{O}_C(p^n)) \longrightarrow V \longrightarrow 0$$

$$0 \longrightarrow H^1(C, \mathcal{O}_C(p^n)) \longrightarrow 0,$$

de donde se sigue inmediatamente que es cierto para n. ∎

Observemos que, en las condiciones del teorema anterior, el teorema [E 10.17] implica que $\mathcal{O}_C(p^n)$ tiene un generador global para todo $n \geq 2$.

Teorema 8.5 *Sea D un dominio de Dedekind, $S = \operatorname{Esp} D$ y $\pi : X \longrightarrow S$ una superficie fibrada cuya fibra genérica X_η sea isomorfa a una curva elíptica (dada por una ecuación de Weierstrass sobre D). Sea $o \in X_\eta$ su punto infinito y sea $O = \overline{\{o\}} \subset X$. Supongamos que O está contenido en el abierto de puntos suaves de X. Esto nos permite considerar a O (o, equivalentemente, a o) como divisor de Cartier de X. Supongamos además que las fibras X_s son íntegras, para todo $s \in S$. Entonces:*

a) Para todo $n \geq 2$, el haz $\mathcal{O}_X(O^n)$ admite un generador global.

b) El haz $\mathcal{L} = D^1\pi_*\mathcal{O}_X$ es inversible y, para todo $n \geq 1$, el haz $\pi_*\mathcal{O}_X(O^n)$ es localmente libre de rango n.

c) El haz $\pi_*\mathcal{O}_X(O)$ es libre y, para $n \geq 2$, tenemos una sucesión exacta

$$0 \longrightarrow \pi_*\mathcal{O}_X(O^{n-1}) \longrightarrow \pi_*\mathcal{O}_X(O^n) \longrightarrow \mathcal{L}^n \longrightarrow 0.$$

d) Si $\mathcal{L}$ es libre, entonces también lo son todos los haces $\pi_*\mathcal{O}_X(O^n)$ y, para $n \geq 2$, el homomorfismo canónico

$$\bigoplus_{2a+3b\leq n} \pi_*\mathcal{O}_X(O^2)^a \otimes_{\mathcal{O}_S} \pi_*\mathcal{O}_X(O^3)^b \longrightarrow \pi_*\mathcal{O}_X(O^n)$$

es suprayectivo.

DEMOSTRACIÓN: En primer lugar vamos a demostrar que todas las fibras de X cumplen las hipótesis del teorema anterior. Ante todo, como la fibra genérica es una curva elíptica, se cumple que $p_a(X_\eta) = 1$, luego $p_a(X_s) = 1$ para todo $s \in S$, por [E 6.38]. Por hipótesis o es geométricamente regular en X_η y racional sobre K (el cuerpo de cocientes de D). Esto ya sitúa a X_η en las hipótesis del teorema anterior. Consideremos ahora una fibra cerrada X_s, con $s \in S$.

Podemos tomar un punto $x \in X_s \cap O$. Basta probar que es geométricamente regular y racional sobre $k(s)$. De hecho, si vemos que es racional, bastará probar que es regular, por [E 7.24].

Cambiando X por $X \times_S \operatorname{Esp} \mathcal{O}_{S,s}$ se conservan las fibras X_s y X_η, luego podemos suponer que D es un anillo de valoración discreta. Como o es un punto racional de X_η, tenemos un homomorfismo

$$\operatorname{Esp} K \longrightarrow X_\eta = X_K$$

definido sobre K cuya imagen es o. Por [E 4.28] se extiende a un (único) homomorfismo $\operatorname{Esp} D \longrightarrow X$ definido sobre D. Como es propio, su imagen es un cerrado de dos puntos que contiene a o, luego la imagen del punto cerrado de $\operatorname{Esp} D$ ha de ser el punto x.

Sea $U \subset X$ un entorno afín de x, que contendrá necesariamente a o. Si $U = \operatorname{Esp} A$, entonces o se corresponde con un ideal $\mathfrak{p} \in \operatorname{Esp} A$ y x se corresponde con $\mathfrak{m} \in \operatorname{Esp} A$ tal que $\mathfrak{p} \subset \mathfrak{m}$.

Tenemos homomorfismos $D \longrightarrow A \longrightarrow D$ cuya composición es la identidad y de modo que la antiimagen de 0 por el segundo es $\mathfrak{p}$. Esto nos da que el homomorfismo natural $D \longrightarrow A/\mathfrak{p}$ es un isomorfismo. En particular, si llamamos $\pi \in D$ a un primo, tenemos un isomorfismo $k(s) = D/(\pi) \longrightarrow A/\mathfrak{m} = k(x)$, luego $x \in X_s$ es un punto racional.

Falta probar que $\mathfrak{m}$ es regular en la fibra $A \otimes_D (D/(\pi)) = A/\pi A$, lo cual equivale a que el anillo $A_\mathfrak{m}/\pi A_\mathfrak{m}$ sea regular. Observemos que $A/\mathfrak{p}$ es un anillo local (porque es isomorfo a D), luego coincide con $A_\mathfrak{m}/\mathfrak{p}A_\mathfrak{m}$. En lo sucesivo podemos cambiar A por $A_\mathfrak{m}$, con lo que tenemos que A es un anillo local regular (porque x es regular en X) con un ideal primo $\mathfrak{p}$ tal que $A/\mathfrak{p} \cong D$ es regular. Hemos de probar que $A/\pi A$ es regular.

Según [AC 5.19], tenemos que $\mathfrak{p} = (u)$ y $\mathfrak{m} = (u, v)$. Como $\mathfrak{m}/\mathfrak{p} = (\pi)$, resulta que $\mathfrak{m} = (u, \pi)$, luego $\mathfrak{m}/(\pi) = (u)$. Esto prueba que $A/(\pi)$ es regular.

Hemos probado algo más: si volvemos a llamar $A = \mathcal{O}_X(U)$, donde U es un entorno afín de x, lo que hemos visto es que $\mathfrak{p}A_\mathfrak{m} = (u)$ y, localizando A respecto a un $f \in A \setminus \mathfrak{m}$ (es decir, reduciendo el entorno de x), podemos suponer que $u \in A$ y $\mathfrak{p} = (u)$. Esto significa que $v_\mathfrak{p}(u) = 1$ y, necesariamente, $v_\mathfrak{q}(u) = 0$ para cualquier otro $\mathfrak{q} \in U$ de codimensión 1 (ya que en tal caso $\mathfrak{p} \subset \mathfrak{q}$ y entonces $\mathfrak{p} = \mathfrak{q}$). En otros términos, (U, u) define el divisor O, y hemos visto que $\mathfrak{m}A_\mathfrak{m}/\pi A_\mathfrak{m} = (u)$, es decir, que la imagen de u en $\mathcal{O}_{X_s}(U \cap X_s)$ genera el ideal maximal de $\mathcal{O}_{X_s,x}$, luego $v_x(O|_{X_s}) = 1$. Así pues, $O|_{X_s} = x$.

También es cierto que $O|_{X_\eta} = o$, pues la fibra genérica se corresponde con el anillo $A \otimes_D K$ y, por definición, $\mathfrak{p}$ es la antiimagen en A del ideal correspondiente

con o. Si $\mathfrak{p} = (u)$ en A, lo mismo es válido en la localización $A \otimes_D K$, luego $v_o(O|_{X_\eta}) = 1$ y concluimos como antes.

Consideremos ahora el haz $\mathcal{O}_X(O^n)$. Su imagen inversa en $X \times_S \operatorname{Esp} \mathcal{O}_{S,s}$, donde $s \in S$ es un punto cerrado, es un haz inversible (en particular plano sobre $\mathcal{O}_{S,s}$) cuya restricción a la fibra X_s es $\mathcal{O}_{X_s}(p^n)$, donde $\{p\} = O \cap X_s$, y cuya restricción a X_η es $\mathcal{O}_{X_\eta}(o^n)$. Por 8.4 tenemos que $\dim_{k(s)} H^i(X_s, \mathcal{O}_X(O^n)_s)$ (para cualquier $s \in S$, cerrado o no) depende únicamente de n e i, luego el teorema 8.3 (juntamente con [E 6.15]) implica que $H^i(X, \mathcal{O}_X(O^n)) \otimes_D \mathcal{O}_{S,s}$ es un $\mathcal{O}_{S,s}$-módulo libre, y que

$$H^i(X, \mathcal{O}_X(O^n)) \otimes_D k(s) \cong H^i(X_s, \mathcal{O}_X(O^n)_s). \tag{8.1}$$

Por la observación tras el teorema 8.4, para $n \geq 2$ se cumple que $\mathcal{O}_X(O^n)_s$ tiene un generador global. A través del isomorfismo anterior (para $i = 0$), podemos formar un subconjunto $G \subset H^0(X, \mathcal{O}_X(O^n))$ cuya imagen en cada $H^0(X_s, \mathcal{O}_X(O^n)_s)$ sea un generador global. Llamamos $\mathcal{G}$ al subhaz de $\mathcal{O}_X(O^n)$ definido como sigue: si $U \subset X$ es un abierto, entonces $\mathcal{G}(U)$ está formado por los $u \in \mathcal{O}_X(O^n)(U)$ tales que $u_x \in \langle g_x \mid g \in G\rangle_{\mathcal{O}_{X,x}}$. Claramente, G es un generador global de $\mathcal{G}$. Para probar a) basta ver que $\mathcal{O}_X(O^n) = \mathcal{G}$.

Si $x \in X$ pertenece a la fibra X_s, tenemos el diagrama siguiente:

$$\begin{array}{ccccccc}
\mathcal{G}_x \otimes_{\mathcal{O}_{X,x}} \mathcal{O}_{X_s,x} & \longrightarrow & \mathcal{O}_X(O^n)_x \otimes_{\mathcal{O}_{X,x}} \mathcal{O}_{X_s,x} & \longrightarrow & (\mathcal{O}_X(O^n)/\mathcal{G})_x \otimes_{\mathcal{O}_{X,x}} \mathcal{O}_{X_s,x} & \longrightarrow & 0 \\
 & \searrow & \downarrow & & & & \\
 & & \mathcal{O}_X(O^n)_{s,x} & & & &
\end{array}$$

donde la flecha vertical es el isomorfismo natural y la fila superior es exacta. Por construcción de $\mathcal{G}$, la flecha oblicua es suprayectiva, luego la primera flecha horizontal también lo es. Esto implica que

$$(\mathcal{O}_X(O^n)/\mathcal{G})_x \otimes_{\mathcal{O}_{X,x}} \mathcal{O}_{X_s,x} = 0,$$

luego también

$$(\mathcal{O}_X(O^n)/\mathcal{G})_x \otimes_{\mathcal{O}_{X,x}} k(x) = 0.$$

Por el lema de Nakayama concluimos que $(\mathcal{O}_X(O^n)/\mathcal{G})_x = 0$ para todo punto $x \in X$, luego, tal y como queríamos probar, $\mathcal{O}_X(O^n) = \mathcal{G}$.

Veamos ahora b). Observemos que, según, [E 6.42], el haz $\mathcal{L}$ no es sino el haz coherente en S determinado por el D-módulo $H^1(X, \mathcal{O}_X)$. Antes hemos probado (en el caso $n = 0$) que $H^1(X, \mathcal{O}_X)$ es localmente libre y que

$$H^1(X, \mathcal{O}_X)_s \otimes_{\mathcal{O}_{S,s}} k(s) \cong H^1(X_s, \mathcal{O}_{X_s}).$$

Según 8.4, la dimensión sobre $k(s)$ de este espacio es igual a 1, lo que implica a su vez que $H^1(X, \mathcal{O}_X)_s$ tiene rango 1 sobre $\mathcal{O}_{S,s}$. Esto significa que $\mathcal{L}$ es localmente libre de rango 1. También tenemos los isomorfismos

$$H^0(X, \mathcal{O}_X(O^n))_s \otimes_{\mathcal{O}_{S,s}} k(s) \cong H^0(X_s, \mathcal{O}_X(O^n)_s),$$

y ahora la dimensión sobre $k(s)$ es n, luego $H^0(X, \mathcal{O}_X(O^n))_s$ es un $\mathcal{O}_{S,s}$-módulo libre de rango n y el haz $\pi_*\mathcal{O}_X(O^n)$ es localmente libre de rango n,

Para probar c) consideramos la inmersión cerrada $i : O \longrightarrow X$. Por el teorema 5.29, tenemos que es un isomorfismo. Sea $\sigma' : S \longrightarrow O$ el isomorfismo inverso y sea $\sigma : S \longrightarrow X$ la composición $\sigma = \sigma' \circ i$.

Partimos de la sucesión exacta

$$0 \longrightarrow \mathcal{O}_X(O^{n-1}) \longrightarrow \mathcal{O}_X(O^n) \longrightarrow i_*i^*\mathcal{O}_X(O^n) \longrightarrow 0 \tag{8.2}$$

dada por el teorema 7.11 (para $n \geq 1$). Para cada $s \in S$, y todo $n \geq 2$, el isomorfismo (8.1) es

$$H^1(X, \mathcal{O}_X(O^{n-1}))_s \otimes_{\mathcal{O}_{S,s}} k(s) \cong H^1(X_s, \mathcal{O}_X(O^{n-1})_s) = 0,$$

donde la última igualdad nos la da el teorema 8.4. El lema de Nakayama implica entonces que $H^1(X, \mathcal{O}_X(O^{n-1}))_s = 0$ para todo $s \in S$ o, lo que es lo mismo, que $D^1\pi_*\mathcal{O}_X(O^{n-1}) = 0$.

Esto significa que al aplicar el funtor π_* a la sucesión exacta anterior obtenemos otra sucesión exacta:

$$0 \longrightarrow \pi_*\mathcal{O}_X(O^{n-1}) \longrightarrow \pi_*\mathcal{O}_X(O^n) \longrightarrow \mathcal{L}_n \longrightarrow 0, \tag{8.3}$$

donde $\mathcal{L}_n = \pi_*i_*i^*\mathcal{O}_X(O^n)$. Notemos que $i\circ\pi = \pi'$ y, como π' es un isomorfismo, π'_* es lo mismo que σ'^*, luego

$$\mathcal{L}_n = \pi'_*i^*\mathcal{O}_X(O^n) = \sigma'^*i^*\mathcal{O}_X(O^n) = \sigma^*\mathcal{O}_X(O^n) = \sigma^*\mathcal{O}_X(O)^n = \mathcal{L}_1^n.$$

Si aplicamos π_* a la sucesión (8.2) con $n = 1$, teniendo en cuenta que, según hemos visto, $D^1\pi_*\mathcal{O}_X(O) = 0$, obtenemos la sucesión exacta

$$0 \longrightarrow \mathcal{O}_S \longrightarrow \pi_*\mathcal{O}_X(O) \longrightarrow \mathcal{L}_1 \longrightarrow \mathcal{L} \longrightarrow 0 \tag{8.4}$$

(donde hemos usado el teorema 5.27). Para cada $s \in S$, tenemos una sucesión exacta

$$0 \longrightarrow \pi_*\mathcal{O}_X(O)_s/\mathcal{O}_{S,s} \longrightarrow \mathcal{L}_{1s} \longrightarrow \mathcal{L}_s \longrightarrow 0.$$

Dado que $\mathcal{L}_s$ es un $\mathcal{O}_{S,s}$-módulo libre, tenemos que $\mathrm{Tor}^{\mathcal{O}_{S,s}}(\mathcal{L}_s, k(s)) = 0$, luego también es exacta la sucesión

$$0 \longrightarrow (\pi_*\mathcal{O}_X(O)_s/\mathcal{O}_{S,s}) \otimes_{\mathcal{O}_{S,s}} k(s) \longrightarrow \mathcal{L}_{1s} \otimes_{\mathcal{O}_{S,s}} k(s) \longrightarrow \mathcal{L}_s \otimes_{\mathcal{O}_{S,s}} k(s) \longrightarrow 0.$$

Ahora bien, los dos últimos $k(s)$-espacios vectoriales tienen dimensión 1, luego el epimorfismo es un isomorfismo y $(\pi_*\mathcal{O}_X(O)_s/\mathcal{O}_{S,s}) \otimes_{\mathcal{O}_{S,s}} k(s) = 0$. Por el lema de Nakayama concluimos que $\pi_*\mathcal{O}_X(O)_s/\mathcal{O}_{S,s} = 0$ o, lo que es lo mismo, que $\pi_*\mathcal{O}_X(O) = \mathcal{O}_S$. Volviendo a la sucesión (8.4) concluimos que $\mathcal{L}_1 \cong \mathcal{L}$. Por consiguiente, la sucesión exacta (8.3) se corresponde con la del enunciado.

La primera parte de d) es inmediata por inducción sobre $n \geq 2$ a partir de la sucesión exacta de c) y usando [AC 1.32]. (Notemos que el caso $n = 0$ es trivial, por 5.27.)

Para la segunda parte, recordemos que $\pi_*\mathcal{O}_X(O^n)$ es el haz coherente en $S = \operatorname{Esp} D$ inducido por el D-módulo

$$L(O^n) = \mathcal{O}_X(O^n)(X) = \{f \in K(X)^* \mid v_o(f) \geq -n\} \cup \{0\}.$$

El homomorfismo del enunciado es el inducido por los homomorfismos

$$L(O^n) \otimes_D L(O^m) \longrightarrow L(O^{n+m})$$

dados por $f \otimes g \mapsto fg$. Puesto que $\operatorname{rang} L(O) = 1$ y $\operatorname{rang} L(O^2) = 2$, ha de haber una $f \in L(O^2) \setminus L(O)$, es decir, tal que $v_o(f) = -2$. El homomorfismo del enunciado es trivialmente suprayectivo para $n = 2$ o $n = 3$. Si $n \geq 4$ y $g \in L(O^n)$, entonces $g/f \in L(O^{n-2})$. Razonando inductivamente, podemos suponer que existe

$$h \in \bigoplus_{2a+3b \leq n-2} L(O^2)^a \otimes_D L(O^3)^b$$

cuya imagen en $L(O^{n-2})$ es g/f, y entonces la imagen de fh es g. ∎

Ahora ya podemos probar el teorema 8.6 que caracteriza los modelos de Weierstrass de las curvas elípticas. En realidad, para probar 8.6 en toda su generalidad necesitamos un resultado sobre dualidad que vamos a enunciar sin demostración, pero en lo sucesivo sólo necesitaremos el caso particular de 8.6 en el que $\operatorname{Pic}(S) = 1$, y veremos que en este caso la prueba no requiere el resultado en cuestión.

Recordemos que, según [E 9.8] y [E 9.32], si X/k es un esquema proyectivo de dimensión n que sea localmente una intersección completa y $\mathcal{M}$ es un haz coherente en X, tenemos un isomorfismo

$$\operatorname{Hom}_{\mathcal{O}_X}(\mathcal{M}, \omega_{X/k}) \longrightarrow H^n(X, \mathcal{M})^*.$$

Más en general:

Teorema *Sea D un anillo noetheriano y X/D un esquema proyectivo y plano que sea localmente una intersección completa y cuyas fibras tengan dimensión n. Entonces, para cada haz coherente $\mathcal{M}$ en X tenemos un isomorfismo*

$$\operatorname{Hom}_{\mathcal{O}_X}(\mathcal{M}, \omega_{X/D}) \longrightarrow H^n(X, \mathcal{M})^*,$$

donde el asterisco indica el D-módulo dual formado por los homomorfismos con imagen en D.

De hecho sólo necesitamos el caso particular en el que X/S es una superficie fibrada (con lo que $n = 1$) y $\mathcal{M} = \mathcal{O}_X$, lo que nos da el isomorfismo

$$H^0(X, \omega_{X/S}) \cong H^1(X, \mathcal{O}_X). \tag{8.5}$$

Teorema 8.6 *Sea D un dominio de Dedekind, sea $S = \operatorname{Esp} D$ y $\pi : X \longrightarrow S$ una superficie fibrada cuya fibra genérica X_η sea isomorfa a una curva elíptica E (dada por una ecuación de Weierstrass sobre D). Sea $o \in X_\eta$ su punto infinito y sea $O = \overline{\{o\}} \subset X$. Supongamos que O está contenido en el abierto de puntos suaves de X y que, para todo $s \in S$, las fibras X_s son íntegras. Entonces:*

a) X/S es localmente una intersección completa y $\pi_*\omega_{X/S}$ es un haz inversible.

b) Si $\pi_*\omega_{X/S}$ es libre, entonces X/S es el modelo de Weierstrass de E asociado a una ecuación de Weierstrass con coeficientes en D.

Demostración: Supongamos en primer lugar que el haz $D^1\pi_*\mathcal{O}_X$ es libre, lo que nos sitúa en las hipótesis de 8.5. Equivalentemente, tenemos que $H^1(X, \mathcal{O}_X)$ es un A-módulo libre de rango 1. Como en la prueba de 8.5, llamemos $L(O^n) = \mathcal{O}_X(O^n)(X)$. Tenemos que $L(O^n) \subset K(X)$ es un D-módulo libre de rango n, $L(O) = D$ y cada $L(O^{n+1})$ tiene a $L(O^n)$ como sumando directo.

Por consiguiente, podemos tomar $x \in L(O^2)$, $y \in L(O^3)$ tales que $\{1, x\}$ es una D-base de $L(O^2)$ y $\{1, x, y\}$ es una D-base de $L(O^3)$. Según 8.5, tenemos que

$$\{1, x, x^2, x^3, y, y^2, xy\}$$

es una base de $L(O^6)$, luego $\{x^3, y^2\}$ es un generador de $L(O^6)/L(O^5)$ (que es un D-módulo libre de rango 1).

Notemos ahora que $y^2/x \in L(O^4)$, y una base de $L(O^4)$ es $1, x, x^2, y$, luego y^2 es combinación lineal (con coeficientes en D) de x, x^2, x^3, xy, luego existe un $\alpha \in D$ no nulo tal que $y^2 - \alpha x^3 \in L(O^5)$.

Esto implica que x^3 es por sí solo un sistema generador de $L(O^6)/L(O^5)$ y, al ser un módulo libre de torsión, x^3 es una base.

Razonando con x^3/y concluimos igualmente que y^2 también es una base del cociente, luego, en la relación $y^2 - \alpha x^3 \in L(O^5)$, el escalar α ha de ser una unidad de D. Multiplicando por α^2 tenemos que $(\alpha y)^2 - (\alpha x)^3 \in L(O^5)$, luego, cambiando x e y por αx y αy, podemos suponer que $\alpha = 1$. Por consiguiente, existen $a_i \in D$ tales que

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Como $\{1, x, y\}$ es un generador global de $\mathcal{O}_X(O^3)$, según [E 5.33] define un S-homomorfismo $\phi : X \longrightarrow \mathrm{P}^2_D$. Observemos que, por construcción de $\mathcal{O}_X(O^3)$, se cumple que $X_1 = X \setminus O$ y, sobre este abierto, ϕ se corresponde con el homomorfismo $D[X, Y] \longrightarrow \mathcal{O}_X(X_1)$ dado por $X \mapsto x$, $Y \mapsto y$, luego $\phi[X \setminus O]$ y, por consiguiente, $\phi[X]$ está contenido en la superficie W/S determinada por la ecuación de Weierstrass con coeficientes a_i. Así pues, podemos considerar que $\phi : X \longrightarrow W$.

Es fácil comprobar que el homomorfismo $\phi_\eta : X_\eta \longrightarrow W_\eta$ es el asociado a un generador global de la imagen inversa de $\mathcal{O}_X(\mathcal{O}^3)$ en X_η, que, según hemos visto en la prueba de 8.5, es $\mathcal{O}_{X_\eta}(o^3)$. Según [E 10.24], este haz es muy amplio, ya que o^3 tiene grado 3, luego ϕ_η es una inmersión cerrada. Como, en cualquier

caso, W_η es una curva irreducible, ϕ_η ha de ser un isomorfismo, luego $W_\eta \cong E$ es una curva elíptica.

Como X y X_η tienen el mismo cuerpo de funciones racionales, vemos que ϕ es birracional. Además W es normal por ser un modelo de Weierstrass y, como las fibras de ambas superficies son íntegras, cada punto de W tiene a lo sumo un número finito de antiimágenes en X. El teorema [E A21] nos permite concluir que ϕ es un isomorfismo. En particular, según 8.1, concluimos que X/S es localmente una intersección completa y que el haz $\pi_*\omega_{X/S}$ es libre.

Notemos que si $\mathrm{Pic}(S) = 1$, entonces el haz $D^1\pi_*\mathcal{O}_X$, que es inversible por el teorema 8.5, es, de hecho, libre, con lo que no hay nada más que probar.

En el caso general, podemos cubrir S con abiertos afines U donde $D^1\pi_*\mathcal{O}_X$ sea libre. Si $X' = \pi^{-1}[U]$, tenemos que $D^1\pi_*\mathcal{O}_{X'} = (D^1\pi_*\mathcal{O}_X)|_U$, luego, por la parte ya probada, tenemos que X' es localmente una intersección completa, y lo mismo vale para X. En particular está definido el haz canónico $\omega_{X/S}$, y el isomorfismo (8.5) equivale al isomorfismo de haces $\pi_*\omega_{X/S} \cong (D^1\pi_*\mathcal{O}_X)^*$, luego la hipótesis de b) equivale a que $D^1\pi_*\mathcal{O}_X$ sea libre, y de nuevo estamos en el caso ya probado. ∎

Nota Insistimos en que, tal y como ya habíamos indicado y como se ve en la prueba, la hipótesis adicional $\mathrm{Pic}(S) = 1$ en 8.6 evita el uso del teorema de dualidad que hemos enunciado previamente sin demostración. Esta hipótesis equivale a que D sea un dominio de ideales principales. En particular se cumple si D es (un dominio de Dedekind) local.

8.2 El modelo regular minimal

Como en la sección precedente, sea D un dominio de Dedekind con cuerpo de cocientes K, sea $S = \mathrm{Esp}\, D$ y sea E/K una curva elíptica. Según el teorema 7.23, la curva E/K admite un modelo regular minimal único salvo isomorfismo. Tal y como hemos explicado en la introducción, aquí vamos a estudiar bajo qué condiciones es posible obtener un modelo de Weierstrass de E/K contrayendo algunas componentes irreducibles de las fibras cerradas del modelo regular minimal.

Ante todo notemos que si X/S es cualquier modelo normal de E/K, el teorema [E 4.26] nos da que $H^0(X_\eta, \mathcal{O}_{X_\eta}) = K$ y, como D es íntegramente cerrado, el teorema 5.28 implica que las fibras de X son conexas.

Ahora observamos que el teorema 6.13 nos permite refinar el teorema 7.25:

Teorema 8.7 *Si X/S es el modelo regular minimal de una curva elíptica y $W_{X/S}$ es un divisor canónico, entonces $W_{X/S} \cdot D = 0$ para todo divisor primo vertical D.*

DEMOSTRACIÓN: Si $D \subset X_s$, entonces $X_s = \Gamma_1^{d_1} \cdots \Gamma_n^{d_n}$, para ciertos divisores primos verticales Γ_i, uno de los cuales es D, y ciertos naturales $d_i > 0$. El teorema 6.13 nos da que

$$0 = W_{X/S} \cdot X_s = \sum_i d_i \, W_{X/S} \cdot \Gamma_i,$$

y el teorema 7.25 implica que $W_{X/S} \cdot \Gamma_i = 0$ para todo i. ∎

En realidad podemos describir con más detalle el divisor canónico del teorema anterior:

Según el teorema [E 9.29], tenemos que $\omega_{X/S}|_{X_\eta} = \omega_{X_\eta/K}$ y, según lo visto al principio de la sección [E 10.4], $\omega_{X/S}|_{X_\eta} = \mathcal{O}_{X_\eta}$. Sea $i : X_\eta \longrightarrow X$ la inmersión natural. Observemos que si E es un divisor horizontal en X, entonces i^*E tiene soporte $E \cap X_\eta$, que es un punto distinto para cada divisor E, luego $W_{X/S}$ ha de ser un divisor vertical.

Por el teorema anterior tenemos que $W_{X/S} \cdot W_{X/S} = 0$. Como las fibras de X/S son conexas, el teorema 6.8 nos da que

$$W_{X/S} = \prod_s X_s^{d_s},$$

para ciertos $d_s \in \mathbb{Q}$, donde s recorre un número finito de puntos cerrados de S. Ahora bien, el exponente de cada divisor primo de $W_{X/S}$ ha de ser un número entero. Vamos a probar que cada fibra X_s contiene al menos un divisor primo con multiplicidad 1, y así podremos concluir que los d_s son enteros. Para ello consideramos el punto $o \in X_\eta$, que es un punto racional, y formamos el divisor horizontal $O = \overline{\{o\}}$. El teorema 6.9 nos da que $O \cdot X_s = 1$, luego O corta únicamente a una componente irreducible de X_s, que además tiene multiplicidad 1.

En suma, los divisores canónicos de los modelos regulares minimales son productos finitos de fibras con exponentes enteros. El teorema 8.7 puede verse ahora como una consecuencia de 6.6.

Veamos una aplicación:

Teorema 8.8 *Si $\pi : X \longrightarrow S$ es el modelo regular minimal de una curva elíptica, entonces $\pi_*\omega_{X/S}$ es un haz inversible en S y el homomorfismo natural $\pi^*\pi_*\omega_{X/S} \longrightarrow \omega_{X/S}$ es un isomorfismo.*

DEMOSTRACIÓN: Sea $W_{X/S}$ un divisor canónico que, según acabamos de probar, es de la forma $\prod X_s^{d_s}$, donde el producto es finito y $d_s \in \mathbb{Z}$. Sea $E = \prod s^{d_s} \in \mathrm{Div}_c(S)$ y sea $\mathcal{L} = \mathcal{O}_S(E)$. Tenemos entonces que $\omega_{X/S} = \pi^*\mathcal{L}$ y, por [E 5.22]:

$$\pi_*\omega_{X/S} = \pi_*(\mathcal{O}_X \otimes_{\mathcal{O}_X} \pi^*\mathcal{L}) \cong \pi_*\mathcal{O}_X \otimes_{\mathcal{O}_S} \mathcal{L} = \mathcal{O}_S \otimes_{\mathcal{O}_S} \mathcal{L} = \mathcal{L}.$$

De aquí se deduce el isomorfismo del enunciado. ∎

El teorema siguiente nos permitirá extraer más consecuencias de 8.7:

Teorema 8.9 *Sea X/S una superficie aritmética, $s \in S$ un punto cerrado, Γ una componente irreducible de X_s y $k' = H^0(\Gamma, \mathcal{O}_\Gamma)$. Entonces, $K_{X/S} \cdot \Gamma = 0$ si y sólo si se cumple una de las condiciones siguientes (las dos primeras son equivalentes):*

a) $H^1(\Gamma, \mathcal{O}_\Gamma) = 0$ *y* $\Gamma^2 = -2|k' : k(s)|$.

b) Γ *es una cónica sobre* k' *y* $\operatorname{grad}_{k'} \mathcal{O}_X(\Gamma)|_\Gamma = -2$.

c) $p_a(X_\eta) = 1$ *y* Γ *es una componente conexa de* X_s.

DEMOSTRACIÓN: Observemos en primer lugar que

$$\Gamma^2 = \operatorname{grad}_{k(s)} \mathcal{O}_X(\Gamma)|_\Gamma = |k' : k(s)| \operatorname{grad}_{k'} \mathcal{O}_X(\Gamma)|_\Gamma.$$

Esto nos da la equivalencia entre las segundas partes de a) y b). Si se cumple a), entonces $p_a(\Gamma) \leq 0$, y 4.16 nos da que Γ/k' es una cónica, es decir, b).

Recíprocamente, si se cumple b), entonces $p_a(\Gamma) = 0$. Tal y como se ve en la prueba de 4.16, esto implica que $H^1(\Gamma, \mathcal{O}_\Gamma) = 0$, luego tenemos a).

Observemos que a) implica trivialmente que $\Gamma^2 < 0$, mientras que c) implica que $\Gamma^2 = 0$ (por 6.7). Por lo tanto, basta probar que la condición $K_{X/S} \cdot \Gamma = 0$ equivale a a) en el caso $\Gamma^2 < 0$ y equivale a c) en el caso $\Gamma^2 = 0$. Lo primero es consecuencia inmediata de la fórmula de adjunción:

$$\Gamma^2 + K_{X/S} \cdot \Gamma = 2p_a(\Gamma) - 2 = 2|k' : k(s)|(-1 + \dim_{k'} H^1(\Gamma, \mathcal{O}_\Gamma)).$$

Supongamos, pues, que $\Gamma^2 = 0$. La prueba del teorema 6.8 muestra que entonces Γ es una componente conexa de X_s. En efecto, con la notación de dicha prueba, pongamos que $\Gamma = \Gamma_1$. Entonces $y_1 > 0$, $y_i = 0$ para $i \neq 1$. La condición $\Gamma^2 = 0$ implica que todos los y_i en la componente conexa de Γ han de ser iguales, luego dicha componente conexa ha de reducirse a Γ.

Si la fibra X_s es conexa (de modo que $X_s = \Gamma^d$), entonces la fórmula del teorema 6.13 nos da la equivalencia con c). En el caso general consideramos la descomposición $X \xrightarrow{\pi'} S' \longrightarrow S$ dada por el teorema 5.28 y sea $X_{s'}$ la fibra de Γ sobre S'. Notemos que Γ sigue siendo una componente conexa de una fibra de X/S', por lo que seguimos teniendo que $\Gamma^2 = 0$ en X/S'.

Según [E 9.28] tenemos que $\omega_{X/S} = \omega_{X/S'} \otimes_{\mathcal{O}_X} \pi'^* \omega_{S'/S}$, y el último haz es trivial porque $\operatorname{Pic}(S') = 1$, luego

$$K_{X/S} \cdot \Gamma = \operatorname{grad}_{k(s)} \omega_{X/S}|_\Gamma = \operatorname{grad}_{k(s)} \omega_{X/S'}|_\Gamma$$

$$= |k(s') : k(s)| \operatorname{grad}_{k(s')} \omega_{X/S'}|_\Gamma = |k(s') : k(s)|\, K_{X'/S} \cdot \Gamma.$$

Así pues, $K_{X/S} \cdot \Gamma = 0$ equivale a que $K_{X/S'} \cdot \Gamma = 0$ que, por el caso de la fibra conexa, que ya hemos considerado, equivale a que $p_a(X_{\eta'}) = 1$, donde η' es el punto genérico de S'. Ahora bien, $X_\eta = X_{\eta'}$ y la condición sobre el género equivale a

$$\dim_{k(\eta)} H^0(X_\eta, \mathcal{O}_{X_\eta}) = \dim_{k(\eta)} H^1(X_\eta, \mathcal{O}_{X_\eta}),$$

y el cambio de base sólo multiplica ambos miembros por $|k(\eta') : k(\eta)|$, luego llegamos a que $K_{X/S} \cdot \Gamma = 0$ equivale a c). ∎

Combinando esto con 8.7 y con el hecho de que las fibras de los modelos regulares de las curvas elípticas son conexas obtenemos información sobre los divisores primos verticales de los modelos regulares minimales de las curvas elípticas:

Teorema 8.10 *Si X/S es el modelo regular minimal de una curva elíptica y $s \in S$ es un punto cerrado tal que la fibra X_s no es irreducible, entonces, cada componente irreducible $\Gamma \subset X_s$ es una cónica sobre el cuerpo $k = H^0(\Gamma, \mathcal{O}_\Gamma)$, y además $\Gamma^2 = -2|k : k(s)|$.*

A partir de aquí nos centramos en el problema de relacionar el modelo regular minimal de una curva elíptica con sus modelos de Weierstrass. Vamos a necesitar un caso particular del criterio 7.10 para la existencia de la contracción de una familia de curvas. Lo deduciremos del teorema siguiente:

Teorema 8.11 *Sea X/S una superficie fibrada con $\dim S = 1$, sea C un divisor de Cartier horizontal y entero en X y sea $\mathcal{L} = \mathcal{O}_X(C)$. Entonces existe un natural $m_0 \geq 1$ tal que $\mathcal{L}^m$ admite un generador global para todo $m \geq m_0$.*

Demostración: Sea $S = \operatorname{Esp} D$ y sea K el cuerpo de cocientes de D. Identificaremos $\mathcal{L}^m = \mathcal{O}_X(C^m)$. El divisor $C|_{X_\eta}$ es entero y no trivial, luego $\operatorname{grad} C|_{X_\eta} > 0$, luego es amplio por el teorema 4.8. Los teoremas [E 6.15] y [E 6.25] nos dan que

$$H^1(X, \mathcal{L}^m) \otimes_D K = H^1(X_\eta, \mathcal{L}^m|_{X_\eta}) = 0$$

para todo m suficientemente grande. Esto significa que $H^1(X, \mathcal{L}^m)$ es un D-módulo de torsión y, como es finitamente generado, tiene longitud finita. (Es un cociente de sumas directas de módulos de la forma D/dD, con $d \neq 0$, y éstos tienen longitud finita porque, como anillos, tienen dimensión 0.)

Por otra parte, el teorema 7.11 nos da una sucesión exacta

$$0 \longrightarrow \mathcal{L}^{m-1} \longrightarrow \mathcal{L}^m \longrightarrow i_*(\mathcal{L}^m|_C) \longrightarrow 0,$$

donde $i : C \longrightarrow X$ es la inmersión cerrada natural. De aquí obtenemos la sucesión exacta de cohomología

$$H^0(X, \mathcal{L}^m) \longrightarrow H^0(C, \mathcal{L}^m|_C) \longrightarrow H^1(X, \mathcal{L}^{m-1}) \longrightarrow H^1(X, \mathcal{L}^m) \longrightarrow 0.$$

Aquí hemos usado que $H^1(C, \mathcal{L}^m|_C) = 0$, porque C es un esquema afín, ya que C/S es finito (teorema 5.29). Como consecuencia, la longitud de $H^1(X, \mathcal{L}^m)$ es menor o igual que la de $H^1(X, \mathcal{L}^{m-1})$ y así, para todo $m \geq m_0 - 1$, ha de ser constante.

Si $m \geq m_0$, el epimorfismo $H^1(X, \mathcal{L}^{m-1}) \longrightarrow H^1(X, \mathcal{L}^m)$ es, de hecho, un isomorfismo (ya que el núcleo tiene longitud 0). La sucesión exacta anterior nos da entonces que el homomorfismo $H^0(X, \mathcal{L}^m) \longrightarrow H^0(C, \mathcal{L}^m|_C)$ es suprayectivo.

Si $x \in C$, vamos a ver que el homomorfismo natural

$$f : H^0(X, \mathcal{L}^m) \otimes_{\mathcal{O}_X(X)} \mathcal{O}_{X,x} \longrightarrow \mathcal{L}^m_x$$

es suprayectivo. Para ello consideramos el diagrama siguiente, cuya fila superior es exacta:

$$\begin{array}{ccccccc} \operatorname{Im} f \otimes_{\mathcal{O}_{X,x}} k(x) & \longrightarrow & \mathcal{L}^m_x \otimes_{\mathcal{O}_{X,x}} k(x) & \longrightarrow & (\mathcal{L}^m_x / \operatorname{Im} f) \otimes_{\mathcal{O}_{X,x}} k(x) & \longrightarrow & 0 \\ \uparrow & \nearrow & & & & & \\ H^0(X, \mathcal{L}^m) & & & & & & \end{array}$$

La flecha oblicua representa el homomorfismo

$$H^0(X, \mathcal{L}^m) \longrightarrow H^0(C, \mathcal{L}^m|_C) \longrightarrow (\mathcal{L}^m|_C)_x \cong \mathcal{L}^m_x \otimes_{\mathcal{O}_{X,x}} \mathcal{O}_{C,x} \longrightarrow \mathcal{L}^m_x \otimes_{\mathcal{O}_{X,x}} k(x).$$

Hemos probado que la primera flecha es un epimorfismo, la segunda lo es porque, al ser C afín, el haz $\mathcal{L}^m|_C$ tiene un generador global, y la última es obviamente suprayectiva. Esto hace que la primera flecha horizontal del esquema precedente sea suprayectiva, con lo que

$$(\mathcal{L}^m_x / \operatorname{Im} f) \otimes_{\mathcal{O}_{X,x}} k(x) = 0.$$

El lema de Nakayama implica entonces que f es suprayectiva, como queríamos probar. Equivalentemente, el haz $\mathcal{L}^m$ tiene un generador global en x. Para puntos $x \notin C$ esto es cierto trivialmente, ya que en tal caso $\mathcal{L}^m_x = \mathcal{O}_{X,x}$ y $1 \in \mathcal{O}_X(X) \subset \mathcal{L}^m(X)$. Así pues, $\mathcal{L}^m$ tiene un generador global. ∎

Como consecuencia:

Teorema 8.12 *Sea X/S una superficie fibrada con $\dim S = 1$, sea C un divisor de Cartier horizontal y entero en X y sea $\mathcal{E}$ el conjunto de todos los divisores primos verticales en X disjuntos con (el soporte de) C. Entonces existe la contracción de las curvas de $\mathcal{E}$.*

Demostración: Según el teorema anterior, cambiando C por una potencia adecuada, podemos suponer que $\mathcal{L} = \mathcal{O}_X(C)$ tiene un generador global, y además esto no altera el conjunto $\mathcal{E}$. Así C cumple la hipótesis b) del teorema 7.10. Respecto a la condición c), si E es una curva vertical, tenemos que $C|_E$ es un divisor entero, que será trivial si $E \in \mathcal{E}$ y tendrá grado positivo (luego $\mathcal{O}_X(C)$ tendrá orden infinito) en caso contrario. Esto significa que C cumple la condición c) y que la familia $\mathcal{E}$ de 7.10 es la misma que estamos considerando aquí. Igualmente, $C|_{X_\eta}$ es un divisor entero y no trivial, luego se cumple la condición a) y esto garantiza la existencia de la contracción. ∎

Con esto llegamos al resultado principal de esta sección:

Teorema 8.13 *Sea D un dominio de Dedekind con cuerpo de cocientes K, sea $S = \operatorname{Esp} D$, sea E/K una curva elíptica, sea $o \in E$ un punto racional, sea $\rho : X \longrightarrow S$ el modelo regular minimal de E/K y sea $O = \overline{\{o\}} \subset X$.*

a) El conjunto $\mathcal{E}$ de divisores primos verticales en X que no cortan a O es finito, y existe su contracción $f : X \longrightarrow W$. Además, $\pi : W \longrightarrow S$ es localmente una intersección completa, $f_*\omega_{X/S} = \omega_{W/S}$ y $f^*\omega_{W/S} = \omega_{X/S}$.

b) Si el haz $\rho_*\omega_{X/S}$ es libre (por ejemplo, si $\mathrm{Pic}(S) = 1$), entonces W/S es un modelo de Weierstrass de E y $\omega_{X/S} = \omega\mathcal{O}_X$, $\omega_{W/S} = \omega\mathcal{O}_W$, donde ω es la forma diferencial definida en el teorema 8.1.

Demostración: a) En la prueba del teorema 6.36 hemos visto que todas las fibras de X son geométricamente regulares salvo a lo sumo un número finito de ellas. Por otra parte, todas las fibras son conexas y una fibra conexa y geométricamente regular ha de ser irreducible, luego concluimos que X tiene a lo sumo un número finito de fibras reducibles.

Ahora bien, los divisores horizontales cortan a todas las fibras, luego, si una fibra X_s contiene un elemento de $\mathcal{E}$, es que no es irreducible. Esto prueba que $\mathcal{E}$ es finito.

Como X es regular, podemos considerar a O como un divisor de Cartier entero y el teorema anterior nos da la existencia de la contracción $g : X \longrightarrow W$. Por el teorema 6.9 tenemos que $O \cdot X_s = 1$, luego O corta únicamente a una componente irreducible de X_s, que además tiene multiplicidad 1. Todas las demás componentes se contraen a puntos, luego la fibra W_s es irreducible.

Identificando $W_s = \pi^*(s)$, tenemos que $X_s = \rho^*(s) = f^*(\pi^*(s))$, lo que exige que la multiplicidad de W_s en sí misma sea también 1. Esto implica que la fibra W_s es íntegra.

En efecto, si tomamos un abierto afín arbitrario en W_s, digamos $\operatorname{Esp} A$, tenemos que A tiene un único primo minimal $\mathfrak{p}$, que es además el único primo asociado porque W es normal (teorema 4.3), luego $\mathfrak{p}$ contiene todos los divisores de A. Por otra parte, $l(A_\mathfrak{p}) = 1$, lo que implica que $\mathfrak{p}A_\mathfrak{p} = 0$, luego $\mathfrak{p} = 0$ (aquí usamos que no hay divisores de cero fuera de $\mathfrak{p}$) y A es un dominio íntegro.

La igualdad $O \cdot X_s = 1$ implica, según 6.4 a), que $O \cap X_s = \{p\}$, donde $p \in X$ es un punto racional. Además, 6.2 nos da que p es regular en X_s y, al ser racional, es geométricamente regular ([E 7.24]). Equivalentemente, p es un punto suave de X. Como g es un isomorfismo en un entorno de O, concluimos que los puntos de (la imagen de) O son suaves en W. Esto nos permite aplicar el teorema 8.6, que nos da que W/S es localmente una intersección completa.

Para probar la igualdad $f_*\omega_{X/S} = \omega_{W/S}$ observamos en primer lugar que f induce un isomorfismo $K(W) \longrightarrow K(X)$, de modo que podemos considerar los haces $f_*\mathcal{O}_X$ y $\mathcal{O}_W$ como subhaces del haz constante $K(W)$ en W. A través de estas identificaciones, los homomorfismos inducidos por f se convierten en inclusiones, luego $\mathcal{O}_W$ se convierte en un subhaz de $f_*\mathcal{O}_X$. Más aún, en la prueba de [E A17] se ve que $f_*\mathcal{O}_X = \mathcal{O}_W$.

Similarmente, por el mismo argumento visto en la prueba del teorema 8.1, podemos identificar a $\omega_{X/S}$ con un subhaz del haz constante $\Omega^1_{K(X)/K}$ en X y a $\omega_{W/S}$ con un subhaz del haz constante $\Omega^1_{K(W)/K}$ en W. Por consiguiente, $f_*\omega_{X/S}$ se identifica también con un subhaz del haz constante $\Omega^1_{K(W)/K}$. Hemos

de probar que dos subhaces son iguales, para lo cual basta ver que lo son sus restricciones a un cubrimiento abierto de W.

En la prueba del teorema 8.6 se ve que W/S es localmente un modelo de Weierstrass, es decir, que podemos cubrir S por abiertos afines U tales que $\pi^{-1}[U]/U$ sea un modelo de Weierstrass de E/K y, en particular, la restricción $\omega_{W/S}|_{\pi^{-1}[U]} = \omega_{\pi^{-1}[U]/U}$ es libre. Por el teorema 8.8, podemos tomar los abiertos U tales que las restricciones $(\rho_*\omega_{X/S})|_U$ sean libres. Notemos que esto implica que $\omega_{X/S}|_{\rho^{-1}[U]} = \omega_{\rho^{-1}[U]/U}$ también es libre.

El cubrimiento de S que hemos tomado determina un cubrimiento de W, y basta probar que los subhaces $f_*\omega_{X/S}$ y $\omega_{W/S}$ coinciden sobre los abiertos de este cubrimiento. Equivalentemente, podemos suponer que $\omega_{W/S} = \omega\mathcal{O}_W$ y que $\omega_{X/S} = \omega'\mathcal{O}_X$, para ciertos ω, $\omega' \in \Omega^1_{K(X)/K}$. En particular, $f_*\omega_{X/S} = \omega'\mathcal{O}_W$.

Como $\Omega^1_{K(X)}/K$ es un $K(X)$-espacio vectorial de dimensión 1, podemos tomar un $h \in K(X)$ tal que $\omega' = h\omega$. Si $U \subset X$ es un abierto que no corte al lugar excepcional de f (es decir, a los divisores de $\mathcal{E}$), entonces $V = f[U]$ es abierto en W y $f|_U$ es un isomorfismo, luego $(f_*\omega_{X/S})(V) = \omega_{W/S}(V)$, luego $h|_U = h|_V$ ha de ser una unidad en $\mathcal{O}_X(U) = \mathcal{O}_W(V)$. Esto significa que el divisor (h) tiene su soporte contenido en el lugar excepcional de f y, en particular, es un divisor vertical. Por consiguiente, está definido el número de intersección $(h)\cdot(h)$, y ha de ser $(h)\cdot(h) = 0$ porque el número de intersección es compatible con la equivalencia de divisores. El teorema 6.8 implica entonces que cada $(h)_s$ es un múltiplo de X_s, pero hay al menos una componente irreducible de cada fibra que no puede formar parte del soporte de h, luego ha de ser $(h) = 1$.

Así pues, $h \in \mathcal{O}_X(X)^* = D^*$, luego $\omega'\mathcal{O}_W = \omega\mathcal{O}_W$, como teníamos que probar. Por último, según el teorema 8.8 tenemos que

$$f^*\omega_{W/S} = f^*f_*\omega_{X/S} = \omega_{X/S}.$$

b) Por a) tenemos que $\pi_*\omega_{W/S} = \pi_*f_*\omega_{X/S} = \rho_*\omega_{X/S}$, luego 8.6 implica[2] que W/S es un modelo de Weierstrass de E/K. El teorema 8.1 nos da entonces que $\omega_{W/S} = \omega\mathcal{O}_W$ y, consecuentemente, $\omega_{X/S} = f^*(\omega\mathcal{O}_W) = \omega\mathcal{O}_X$. ∎

Así pues, tal y como habíamos anunciado, vemos que podemos conseguir un modelo de Weierstrass a partir del modelo regular minimal cuando D es un dominio de ideales principales y, en particular, cuando es un anillo de valoración discreta. En la sección siguiente veremos que el modelo de Weierstrass obtenido de este modo no es uno cualquiera.

8.3 El modelo de Weierstrass minimal

Como en las secciones precedentes, sea D un dominio de Dedekind con cuerpo de cocientes K y sea E/K una curva elíptica. Fijemos una ecuación de Weierstrass asociada a E/K con coeficientes en D. Para cada divisor primo $\mathfrak{p} \in S = \operatorname{Esp} D$, podemos considerar la reducción módulo $\mathfrak{p}$ de la ecuación, que

[2]Notemos que, bajo la hipótesis $\operatorname{Pic}(S) = 1$, no se requiere el teorema de dualidad que hemos usado sin prueba en la demostración de 8.6.

determina una curva sobre $k(\mathfrak{p}) = D/\mathfrak{p}$ que no es sino la fibra $W_\mathfrak{p}$ del modelo de Weierstrass W/S correspondiente a la ecuación.

En términos clásicos, se dice que la ecuación tiene *buena reducción* módulo $\mathfrak{p}$ si la reducción $W_\mathfrak{p}$ es una curva elíptica, lo cual equivale a su vez a que $\mathfrak{p}$ no divida al discriminante Δ de la ecuación. En caso contrario se dice que la ecuación tiene *mala reducción* módulo $\mathfrak{p}$, y entonces $W_\mathfrak{p}$ tiene un punto singular.

Nótese que decimos que *la ecuación,* y no *la curva elíptica,* tiene buena o mala reducción, pues una misma curva elíptica puede admitir ecuaciones de Weierstrass distintas con reducciones distintas módulo un mismo primo. Para evitar la dependencia de la ecuación podemos decir que una curva E/K tiene *buena reducción* módulo un primo $\mathfrak{p}$ si *existe* una ecuación de Weierstrass asociada a E con coeficientes en D que tenga buena reducción módulo $\mathfrak{p}$, y en caso contrario decimos que E/K tiene *mala reducción* módulo $\mathfrak{p}$.

Si $v_\mathfrak{p}$ es la valoración en K asociada a $\mathfrak{p}$, diremos que una ecuación de Weierstrass con coeficientes en D es *minimal* para $\mathfrak{p}$ si su discriminante Δ cumple que $v_\mathfrak{p}(\Delta)$ es el mínimo posible. Si llamamos $\delta_\mathfrak{p}$ a este valor mínimo, tenemos que E/K admite buena reducción módulo $\mathfrak{p}$ si y sólo si $\delta_\mathfrak{p} = 0$. Una ecuación de Weierstrass de E/K es una ecuación *minimal (global)* si lo es para todo primo (no nulo) $\mathfrak{p}$ de D. Observemos que toda curva elíptica E/K admite obviamente una ecuación de Weierstrass minimal para un primo dado, pero no tiene por qué admitir una ecuación de Weierstrass minimal global.

Observemos ahora que el tipo de reducción de una ecuación de Weierstrass módulo un divisor primo depende obviamente, más que de la ecuación en sí, del modelo de Weierstrass definido por la ecuación, en el sentido de que si dos ecuaciones de Weierstrass de una misma curva elíptica determinan modelos de Weierstrass isomorfos, entonces las dos tendrán el mismo tipo de reducción módulo cualquier primo de D, luego los discriminantes de ambas ecuaciones deben ser divisibles exactamente por los mismos primos de D. Más aún, vamos a ver que ambos se diferencian en una unidad de D.

Consideremos para ello dos modelos de Weierstrass W/S y W'/S de una misma curva elíptica E/K. Aquí es importante entender que una curva elíptica es un par (E, o), donde $o \in E(K)$, de modo que "la misma curva elíptica" significa que los isomorfismos $W_\eta \cong E \cong W'_\eta$ transforman los puntos infinitos de las fibras genéricas en el mismo punto o.

Dichos isomorfismos determinan K-isomorfismos $K(W) \cong K(E) \cong K(W')$, que a su vez nos permiten identificar $\Omega^1_{K(W)/K} \cong \Omega^1_{K(E)/K} \cong \Omega^1_{W'/K}$. En particular, podemos considerar las formas diferenciales ω y ω' dadas por el teorema 8.1 como elementos de $\Omega^1_{K(E)/K}$.

Los modelos W/S y W/S' se construyen a partir de sendas ecuaciones de Weierstrass de E/K, luego ambas están relacionadas por un cambio de variable del tipo descrito en el teorema 4.23, y una comprobación rutinaria a partir de las relaciones dadas por dicho teorema muestra que ω y ω' están relacionadas de la forma $\omega' = u\omega$, mientras que, por ese mismo teorema, los discriminantes respectivos cumplen $\Delta = u^{12}\Delta'$, con $u \in K^*$.

Supongamos ahora que los dos modelos de Weierstrass son isomorfos, o, equivalentemente, que tenemos dos ecuaciones de Weierstrass que definen un mismo modelo W/S (y determinan el mismo punto infinito en la fibra genérica). Entonces, tanto ω como ω' son bases de $\omega_{W/S}$. En particular, ambas son bases del $\mathcal{O}_W(W)$-módulo $\omega_{W/S}(W)$, donde $\mathcal{O}_W(W) = D$. Por consiguiente, u tiene que ser una unidad de D, y u^{12} también. Esto justifica la definición siguiente:

Definición 8.14 Sea D un dominio de Dedekind con cuerpo de cocientes K, sea $S = \operatorname{Esp} D$ y sea W/S un modelo de Weierstrass de una curva elíptica E/K. Llamaremos *discriminante* de W al ideal Δ_W de D generado por el discriminante de cualquier ecuación de Weierstrass de E/K con coeficientes en D que defina a W.

Acabamos de probar que Δ_W es independiente de la elección de la ecuación de Weierstrass con la que construimos W (siempre entendiendo que el punto racional $o \in W_\eta$ es fijo).

Diremos que un modelo de Weierstrass W/S es *minimal* en un punto cerrado $s \in S$ si $v_s(\Delta_W)$ toma el menor valor posible δ_s, donde v_s es la valoración en K cuyo anillo de enteros es $\mathcal{O}_{S,s}$. Diremos que W es un *modelo de Weierstrass minimal (global)* si lo es en todo punto cerrado $s \in S$.

Así pues, un modelo de Weierstrass es minimal (en un punto $s = \mathfrak{p}$, resp. global) si y sólo si está definido por una ecuación de Weierstrass minimal (en $\mathfrak{p}$, resp. global), si y sólo si cualquier ecuación de Weierstrass que lo define es minimal (en $\mathfrak{p}$, resp. global).

En este punto conviene precisar un pequeño matiz:

Teorema 8.15 *Sea D un dominio de Dedekind con cuerpo de cocientes K, sea E/K una curva elíptica, sea $s \in S$ un punto cerrado y sea W/S un modelo de Weierstrass de E/K minimal en un punto cerrado $s \in S$. Entonces se cumple que $W \times_S \operatorname{Esp} \mathcal{O}_{S,s}$ es un modelo de Weierstrass minimal (global) de E sobre el dominio $\mathcal{O}_{S,s}$.*

Demostración: El punto s se corresponde con un divisor primo $\mathfrak{p}$ de D, de modo que $\mathcal{O}_{S,s} = D_\mathfrak{p}$. El modelo W/S está definido por una ecuación de Weierstrass con coeficientes en D tal que $v_\mathfrak{p}(\Delta)$ es el mínimo posible, y entonces $W \times_S \operatorname{Esp} \mathcal{O}_{S,s}$ es el modelo de Weierstrass definido por esa misma ecuación, pero, en principio, no tenemos la garantía de que sea minimal, porque podría existir otra ecuación de Weierstrass asociada a E con coeficientes en $D_\mathfrak{p}$ con un discriminante Δ' tal que $v_\mathfrak{p}(\Delta') < v_\mathfrak{p}(\Delta)$. Sólo hemos de probar que esto no puede suceder.

Los coeficientes de esta hipotética ecuación serían fracciones de elementos de D con denominadores no divisibles entre $\mathfrak{p}$. Sea $u \in D$ el producto de todos ellos, que también es una unidad de $D_\mathfrak{p}$. De acuerdo con 4.23, el cambio de variables $X = u^{-1}X'$, $Y = u^{-3}Y'$ transforma la ecuación en otra cuyos coeficientes están en D y cuyo discriminante es $\Delta'' = u^{12}\Delta'$, luego $v(\Delta') = v_\mathfrak{p}(\Delta'') \geq v_\mathfrak{p}(\Delta)$, por la minimalidad de Δ.

Por último, observemos que el modelo es minimal global porque $\mathcal{O}_{S,s}$ sólo tiene un punto cerrado. ∎

Vamos a abordar el problema de la existencia de modelos de Weierstrass minimales (globales). Empezamos con algunos resultados previos.

Teorema 8.16 *Sea $f : X' \longrightarrow X$ la explosión de un punto cerrado x de una superficie fibrada regular X/S y sea $E \subset X'$ el lugar excepcional de f. Entonces*

$$\omega_{X'/S} = f^*\omega_{X/S} \otimes_{\mathcal{O}_{X'}} \mathcal{O}_{X'}(E).$$

Demostración: Como $f|_{X'\setminus E} : X' \setminus E \longrightarrow X \setminus \{x\}$ es un isomorfismo, se cumple que $\omega_{X'/S}|_{X'\setminus E} = (f^*\omega_{X/S})|_{X'\setminus E}$. Por consiguiente, el haz

$$\omega_{X'/S} \otimes_{\mathcal{O}_{X'}} (f^*\omega_{X/S})^{-1}$$

tiene su soporte contenido en E, luego es el haz asociado a un divisor de Cartier E^r, para cierto $r \in \mathbb{Z}$. Equivalentemente:

$$\omega_{X'/S} = f^*\omega_{X/S} \otimes_{\mathcal{O}_{X'}} \mathcal{O}_{X'}(E^r).$$

Ahora multiplicamos por $\mathcal{O}_{X'}(E)$ y restringimos a E, con lo que el teorema 6.11 nos da la igualdad

$$\omega_{E/k(s)} = (f^*\omega_{X/S})|_E \otimes_{\mathcal{O}_{X'}} \mathcal{O}_{X'}(E)|_E^{r+1},$$

donde $s \in S$ es el punto cerrado que cumple $x \in X_s$. Observemos ahora que $\omega_{X/S}$ es libre en un entorno de x, luego $f^*\omega_{X/S}$ es libre en un entorno de E, luego $(f^*\omega_{X/S})|_E \cong \mathcal{O}_E$. Si tomamos grados sobre $k(s)$ nos queda

$$\operatorname{grad}_{k(s)} \omega_{E/k(s)} = (r+1)E^2.$$

Por último, E es un divisor excepcional de X, luego, por el criterio de Castelnuovo (teorema 7.15) y teniendo en cuenta el teorema [E 9.25]:

$$-2|k' : k(s)| = -(r+1)|k' : k(s)|,$$

luego ha de ser $r = 1$. ∎

Teorema 8.17 *Sea $f : X' \longrightarrow X$ un homomorfismo birracional entre superficies fibradas regulares sobre S. Entonces $H^0(X', \omega_{X'/S}) = H^0(X, \omega_{X/S})$ como subgrupos de $\Omega^1_{K(X)/K}$, donde $K = K(S)$.*

Demostración: Tal y como ya hemos visto en la prueba del teorema 8.13, f induce un isomorfismo $K(X') \cong K(X)$ que nos permite identificar los anillos de $\mathcal{O}_{X'}$ y $\mathcal{O}_X$ con subanillos de $K(X)$. A su vez, los módulos de los respectivos haces canónicos se identifican con submódulos de $\Omega^1_{K(X)/K}$.

Por el teorema 6.24, podemos suponer que f es la explosión de un punto cerrado $x \in X$, y el teorema anterior nos da entonces un monomorfismo de

haces $f^*\omega_{X/S} \longrightarrow \omega_{X'/S}$ (notemos que $\mathcal{O}_{X'} \subset \mathcal{O}_{X'}(E)$) que se corresponde con la inclusión cuando identificamos a ambos con subhaces del haz constante $\Omega^1_{K(X)/K}$. En particular

$$H^0(X, \omega_{X/S}) \subset H^0(X', \omega_{X'/S}).$$

Por otra parte,

$$H^0(X', \omega_{X'/S}) \subset H^0(X' \setminus E, \omega_{X'/S}) = H^0(X \setminus \{x\}, \omega_{X/S}) = H^0(X, \omega_{X/S}).$$

La última igualdad se debe a que podemos cubrir X con abiertos afines U donde $\omega_{X/S}$ es libre. Las restricciones $H^0(U, \omega_{X/S}) \longrightarrow H^0(U \setminus \{x\}, \omega_{X/S})$ son isomorfismos por el teorema [E 7.5], luego la restricción

$$H^0(X \setminus \{x\}, \omega_{X/S}) \longrightarrow H^0(X, \omega_{X/S})$$

también es un isomorfismo, que se corresponde con la identidad cuando consideramos a $\omega_{X/S}$ como subhaz del haz constante $\Omega^1_{K(X)/S}$. ∎

Con esto estamos en condiciones de dar una condición necesaria y suficiente para que una curva elíptica admita un modelo de Weierstrass minimal:[3]

Teorema 8.18 *Sea D un dominio de Dedekind y K su cuerpo de cocientes. Sea E/K una curva elíptica y $\rho : X \longrightarrow S$ su modelo regular minimal. Se cumple que E/K admite un modelo de Weierstrass minimal W/S si y sólo si el haz $\rho_*\omega_{X/S}$ es libre, y en tal caso W/S es necesariamente isomorfo al modelo construido en el teorema* 8.13.

Demostración: Supongamos en primer lugar que $\rho_*\omega_{X/S}$ es libre y vamos a probar que el modelo de Weierstrass W/S dado por el teorema 8.13 es minimal. Para ello tomamos otro modelo de Weierstrass W'/S y consideramos una desingularización $f' : X' \longrightarrow W'$. Como X es el modelo regular minimal de E, existe un homomorfismo birracional $g : X' \longrightarrow X$.

Podemos considerar los módulos de todos los haces canónicos como submódulos del haz constante $\Omega^1_{K(E)/K}$. Vistos así, llamando $F \subset X'$ al lugar excepcional de f', tenemos las inclusiones

$$H^0(X', \omega_{X'/S}) \subset H^0(X' \setminus F, \omega_{X'/S}) = H^0(W' \setminus f'[F], \omega_{W'/S}) = H^0(W', \omega_{W'/S}),$$

donde la última igualdad la tenemos por el mismo razonamiento que hemos empleado en la prueba del teorema anterior. Por consiguiente:

$$H^0(W, \omega_{W/S}) = H^0(X, \omega_{X/S}) = H^0(X', \omega_{X'/S}) \subset H^0(W', \omega_{W'/S}),$$

donde la primera igualdad se debe al teorema 8.13 y la segunda al teorema anterior. Finalmente observamos que, tal y como hemos visto antes de la definición 8.14, los haces canónicos $\omega_{W/S}$ y $\omega'_{W/S}$ están generados por formas

[3]Como de costumbre, si añadimos la hipótesis $\mathrm{Pic}(S) = 1$ obtenemos la existencia y unicidad del modelo de Weierstrass minimal sin necesidad del teorema de dualidad usado sin demostración en la prueba del teorema 8.6.

diferenciales relacionadas en la forma $\omega' = u\omega$, para cierto $u \in K^*$, y entonces los discriminantes de los modelos cumplen la relación $\Delta = u^{12}\Delta'$. La inclusión anterior implica que $u^{-1} \in D$, luego $\Delta \mid \Delta'$. Esto prueba que el modelo de Weierstrass W/S es minimal.

Mantengamos ahora la hipótesis de que $\rho_*\omega_{X/S}$ es libre y vamos a probar que el modelo de Weierstrass minimal es único salvo isomorfismo. Para ello suponemos ahora que W'/S es otro modelo de Weierstrass minimal. Todo lo dicho previamente sigue siendo válido ahora, pero, además, u ha de ser una unidad de D, luego ω' es a la vez una base de $\omega_{W'/S}$, de $\omega_{X/S}$ y de $\omega_{W/S}$. En particular:

$$\omega_{W'/S} = \omega'\mathcal{O}_{W'}, \qquad \omega_{X/S} = \omega'\mathcal{O}_X.$$

Aplicando repetidas veces el teorema 8.16 a una descomposición de g en explosiones de puntos cerrados, concluimos que

$$\omega_{X'/S} = g^*\omega_{X/S} \otimes_{\mathcal{O}_{X'}} \mathcal{O}_{X'}(H) = \omega'\mathcal{O}_{X'}(H),$$

donde H es un divisor entero en X' cuyo soporte es el lugar excepcional de g. Como los haces $\omega_{X'/S}$ y $\omega_{W'/S}$ coinciden fuera del soporte de f', el soporte de H ha de estar contenido en dicho soporte. En definitiva, tenemos que el lugar excepcional de g está contenido en el lugar excepcional de f'.

Hasta aquí hemos trabajado con una desingularización arbitraria f' de W', pero podemos elegir concretamente una desingularización minimal (teorema 7.30). En particular se trata de una desingularización estricta, y sabemos que su lugar excepcional no contiene divisores excepcionales de X'.

Esto implica que X' no tiene divisores excepcionales, ya que, de tener alguno, podríamos iniciar con él una cadena de contracciones de divisores excepcionales que terminaría en una superficie (relativamente) minimal, es decir, en X, luego todo divisor excepcional de X' está necesariamente en el lugar excepcional de g y, según hemos visto, también en el de f'. Esto prueba que X' es una superficie minimal, luego g es un isomorfismo o, equivalentemente, podemos considerar que $X' = X$.

Tenemos así una desingularización estricta $f' : X \longrightarrow W'$. Sea $o \in E(K)$ el punto infinito de E/K. Sean O y O' las clausuras respectivas de o en X y W'. Es claro que $O' = f'[O]$. Si $s \in S$, en la prueba de 8.13 hemos visto que O corta a una única componente irreducible Γ de X_s. Si $f'[\Gamma]$ fuera un punto, dicho punto estaría en $O' \cap W'_s$, luego sería un punto suave de W', y en particular regular, con lo que f' no sería una desingularización estricta de W'.

Como las fibras de W' son irreducibles, ha de ser $f'[\Gamma] = W'_s$. Por otra parte, cualquier otra componente irreducible de X_s se ha de contraer a un punto, ya que de lo contrario f' tampoco sería una desingularización estricta.

Con esto hemos probado que f' es la contracción de los divisores primos de X que no cortan a O. La unicidad de la contracción (teorema 6.27) implica que $W' = W$.

Supongamos ahora que $\pi' : W' \longrightarrow S$ es un modelo de Weierstrass minimal de E/K, pero no que el haz $\rho_*\omega_{X/S}$ sea libre. En cualquier caso, es un haz inversible por el teorema 8.8. Consideremos un abierto afín $U \subset S$ donde $\rho_*\omega_{X/S}$ sea libre. Entonces $\pi'^{-1}[U]/U$ es un modelo de Weierstrass de E/K (correspondiente a la misma ecuación de Weierstrass, pero considerada ahora con coeficientes en $\mathcal{O}_S(U)$). Es claro que sigue siendo un modelo de Weierstrass minimal. Por otra parte, $\rho^{-1}[U]/U$ sigue siendo el modelo regular minimal de E/K. La parte ya probada nos da un homomorfismo $\rho^{-1}[U] \longrightarrow \pi'^{-1}[U]$ que no es sino la contracción de los primos verticales de $\rho^{-1}[U]$ que no cortan a $O \cap \rho^{-1}[U]$. Todas estas contracciones pueden pegarse para formar un homomorfismo $X \longrightarrow W'$ que no es sino la contracción de todos los primos verticales de X que no cortan a O. En definitiva, de nuevo tenemos que $W' = W$.

Finalmente, el teorema 8.13 nos da que $\pi_*\omega_{W/S} = \pi_* f_* \omega_{X/S} = \rho_*\omega_{X/S}$, luego concluimos que $\rho_*\omega_{X/S}$ es libre por el teorema 8.1. ∎

Observemos que la hipótesis de que $\rho_*\omega_{X/S}$ sea libre es equivalente a que $\omega_{X/S}$ sea libre, por el teorema 8.8.

Así pues, cuando una curva elíptica E/K admite un modelo de Weierstrass minimal W/S, éste es único salvo isomorfismo, por lo que podemos hablar de *"el modelo de Weierstrass minimal"* de E/K sobre S. En particular, tenemos demostrada su existencia (y unicidad) cuando D es un dominio de ideales principales. En cuanto a su relación con el modelo regular minimal, aún podemos decir un poco más:

Teorema 8.19 *Sea D un dominio de Dedekind y K su cuerpo de cocientes. Sea E/K una curva elíptica y $\rho : X \longrightarrow S$ su modelo regular minimal. Si W'/S es un modelo de Weierstrass de E/K tal que existe un homomorfismo birracional $X \longrightarrow W'$, entonces W' es el modelo de Weierstrass minimal de E/K.*

Demostración: Como X no contiene divisores excepcionales, la desingularización $f' : X \longrightarrow W'$ es necesariamente la desingularización minimal de W'/S, luego, en particular, es una desingularización estricta. El mismo razonamiento empleado en la prueba del teorema anterior muestra que f' es necesariamente la dada por el teorema 8.13, luego W' coincide con la superficie W/S considerada en dicho teorema. En particular sabemos que W/S es un modelo de Weierstrass. Esto hace que el haz $\rho_*\omega_{X/S} = \rho_*\omega_{W/S}$ sea libre, luego W/S es minimal por el teorema anterior. ∎

En resumen, la situación es la siguiente: si $s \in S$ es un punto cerrado, el modelo regular minimal de E/K sobre $\mathcal{O}_{S,s}$ está determinado por el modelo regular minimal de E/K sobre $\mathcal{O}_{S,s}$ (en el sentido de que aquél se obtiene de éste por contracción de todas las componentes irreducibles de la fibra cerrada menos una). Los modelos regulares minimales de E/K sobre todos los anillos locales $\mathcal{O}_{S,s}$ se pueden "reunir" en una única superficie aritmética, el modelo regular minimal sobre S, mientras que no siempre es posible "reunir" en un único modelo de Weierstrass minimal (global) todos los modelos de Weierstrass minimales locales. Cuando es posible, el modelo de Weierstrass minimal se obtiene igualmente por contracción a partir del modelo regular minimal.

8.4 Reducción de curvas elípticas

Ahora estamos en condiciones de dar una definición de reducción de una curva algebraica que, como consecuencia de los resultados de la sección anterior, generaliza a la noción usual de reducción de una curva elíptica:

Definición 8.20 Sea D un dominio de Dedekind con cuerpo de cocientes K, sea $S = \operatorname{Esp} D$ y sea C/K una curva proyectiva íntegra geométricamente regular. Para cada punto cerrado $s \in S$, diremos que C/K tiene *buena reducción* en s (o módulo $\mathfrak{p}$, si interpretamos s como un ideal maximal $\mathfrak{p}$ de D) si admite un modelo suave sobre $\operatorname{Esp} \mathcal{O}_{S,s}$. En caso contrario diremos que tiene *mala reducción* en s. Diremos que C/K tiene *buena reducción* sobre S si tiene buena reducción en todos los puntos cerrados de S.

Observemos que si C/K admite un modelo X/S tal que la fibra $X_s/k(s)$ es geométricamente regular, entonces C/K tiene buena reducción en s, pues $X \times_S \operatorname{Esp} \mathcal{O}_{S,s}$ es un modelo suave de C/K sobre $\operatorname{Esp} \mathcal{O}_{S,s}$. En general, las fibras cerradas de los modelos de C/K se llaman *reducciones* de C/K.

Por otra parte, si tenemos un modelo X/S tal que la fibra X_s no sea geométricamente regular (o un modelo no suave sobre $\mathcal{O}_{S,s}$) eso no significa que C/K tenga mala reducción en s, puesto que nada impide que exista otro modelo que cumpla la definición. Esto hace que, aparentemente, la definición anterior no sea muy operativa, pero no es así porque, en la práctica, todo se reduce a estudiar el modelo regular minimal:

Teorema 8.21 *Sea D un dominio de Dedekind con cuerpo de cocientes K, sea $S = \operatorname{Esp} D$ y sea C/K una curva proyectiva íntegra geométricamente regular de género $p_a(C) \geq 1$. Entonces C/K tiene buena reducción sobre S si y sólo si el modelo regular minimal X/S es suave, y en tal caso es (salvo isomorfismo) el único modelo suave de C/K sobre S.*

Demostración: Notemos que el modelo regular minimal X/S existe por el teorema 7.23. Si C/K tiene buena reducción en un punto $s \in S$, entonces existe un modelo suave $Y/\mathcal{O}_{S,s}$. El teorema 7.8 nos da que es relativamente minimal, y 7.21 implica entonces que es el modelo regular minimal de C/K sobre $\mathcal{O}_{S,s}$.

Por otra parte, según el teorema 7.24, el modelo $X \times_S \operatorname{Esp} \mathcal{O}_{S,s}$ también es minimal. La unicidad de los modelos minimales implica que $X \times_S \operatorname{Esp} \mathcal{O}_{S,s} \cong Y$, luego la fibra X_s es geométricamente regular, para todo $s \in S$, lo que significa que X/S es suave. El recíproco es trivial. La unicidad se debe una vez más a los teoremas 7.8 y 7.21. ∎

Observemos que, a pesar del carácter global del enunciado, el teorema anterior puede usarse localmente: la curva C/K tiene buena reducción en un punto $s \in S$ si y sólo si tiene buena reducción sobre $\operatorname{Esp} \mathcal{O}_{S,s}$, si y sólo si el modelo regular minimal de C/K sobre $\operatorname{Esp} \mathcal{O}_{S,s}$ es suave (lo que a su vez equivale a que su única fibra cerrada sea geométricamente regular).

Antes de centrarnos en el caso de las curvas elípticas demostramos un sencillo hecho general:

Teorema 8.22 *Sea D un dominio de Dedekind con cuerpo de cocientes K y C/K una curva íntegra geométricamente regular. Entonces C/K tiene buena reducción en todos los puntos de $S = \operatorname{Esp} D$ salvo a lo sumo en un número finito de ellos.*

DEMOSTRACIÓN: El teorema 6.37 nos da que C/K tiene al menos un modelo regular X/S, y en la prueba del teorema 6.36 hemos visto que todas las fibras de X son geométricamente regulares salvo a lo sumo un número finito de ellas. ∎

En el caso de las curvas elípticas, la noción general de buena reducción que acabamos de introducir coincide con la usual:

Teorema 8.23 *Sea D un dominio de Dedekind con cuerpo de cocientes K y sea E/K una curva elíptica. Sea $s \in S$ un punto cerrado y sea $W/\mathcal{O}_{S,s}$ el modelo de Weierstrass minimal de E sobre $\mathcal{O}_{S,s}$. Entonces E/K tiene buena reducción en s si y sólo si la fibra W_s es geométricamente regular.*

DEMOSTRACIÓN: Notemos que si W_s es geométricamente regular, entonces $W/\mathcal{O}_{S,s}$ es suave y E/K tiene buena reducción en s. Recíprocamente, si la reducción es buena, el teorema anterior nos da que el modelo regular minimal $X/\mathcal{O}_{S,s}$ es suave. Como la fibra cerrada X_s es conexa y geométricamente regular, ha de ser irreducible, luego el conjunto $\mathcal{E}$ del teorema 8.13 a) es vacío, luego $X = W$ por 8.18. Consecuentemente, W_s es geométricamente regular. ∎

Así pues, vemos que el modelo regular minimal y el modelo de Weierstrass minimal coinciden en el caso de buena reducción. Sin embargo, cuando no sabemos si la reducción es buena o mala, resulta que podemos estudiarlo con el modelo regular minimal en lugar de con el modelo de Weierstrass minimal.

Terminaremos la sección recordando los resultados (clásicos) sobre los tipos de reducción de una curva elíptica en términos de los modelos de Weierstrass minimales y en la sección siguiente veremos la extensión que obtenemos al considerar el modelo regular minimal.

El teorema siguiente recoge lo que ya sabemos y un poco más:

Teorema 8.24 *Sea C/k una cúbica plana definida por una ecuación de Weierstrass. Si $\operatorname{car} k = 2, 3$ supondremos además que k es perfecto. Sea C^0 el abierto de sus puntos (geométricamente) regulares. Entonces se da una de las dos posibilidades siguientes:*

a) C/k es una curva elíptica (y esto sucede si y sólo si $\Delta \neq 0$).

b) C/k tiene un único punto singular p, racional sobre k. Sea $\pi : C' \longrightarrow C$ la normalización de C. Entonces $C' \cong \mathrm{P}^1_k$ y se cumple una de las tres posibilidades siguientes:

b.1) *C'_p consta de un punto doble racional y $C^0 \cong A^1_k$. (Esto sucede si y sólo si $\Delta = 0$ y $c_4 = 0$, y en tal caso decimos que p es una* cúspide.*)*

b.2) C'_p *consta de dos puntos racionales y* $C^0 \cong A^1_k \setminus \{0\}$ *(y en tal caso decimos que* p *es un* nodo racional).

b.3) C'_p *consta de un punto* q *tal que* $k(q)/k$ *es una extensión separable de grado* 2 *(y en tal caso decimos que* p *es un* nodo irracional).

Demostración: El apartado a) es el teorema 4.24, y el apartado b) se sigue de 4.24 y 4.21. Dentro de este apartado, no perdemos generalidad si hacemos un cambio de variables en la ecuación de Weierstrass para que el punto singular sea $(0,0)$, de modo que la ecuación cumple $a_3 = a_4 = a_6 = 0$. El ejemplo de la página 143 describe la normalización, y allí hemos visto que la fibra del punto singular es

$$C'_p = \mathrm{Esp}(k[T]/(T^2 + a_1T - a_2)).$$

El caso b.1) se da si y sólo si el discriminante del polinomio $T^2 + a_1T - a_2$ es nulo. Este discriminante es $b_2 = a_1^2 + 4a_2$, ahora bien, la condición $b_2 = 0$ no se conserva por cambios de variables. Observamos, no obstante, que, siendo $a_3 = a_4 = 0$, $c_4 = b_2^2$, y la condición $c_4 = 0$ sí que se conserva por cambios de variables, luego se puede comprobar en cualquier ecuación de Weierstrass asociada a E. El resto del teorema es evidente. ∎

(Véase la sección 2.3 de [CE] para más detalles sobre esta clasificación.)

De aquí obtenemos la clasificación básica de los tipos de mala reducción de una curva elíptica:

Definición 8.25 Sea D un dominio de Dedekind con cuerpo de fracciones K, sea $S = \mathrm{Esp}\, D$, sea E/K una curva elíptica, sea $s \in S$ un punto cerrado donde E/K tenga mala reducción y sea $W/\mathcal{O}_{S,s}$ el modelo de Weierstrass minimal de E/K sobre $\mathcal{O}_{S,s}$. Diremos que E/K tiene *reducción aditiva, reducción multiplicativa racional* o *reducción multiplicativa irracional* en s (o módulo $\mathfrak{p}$, si s se corresponde con un divisor primo $\mathfrak{p}$ de D) según si la curva W_s tiene una cúspide, un nodo racional o un nodo irracional.

8.5 Reducción del modelo regular minimal

Aquí vamos a obtener la clasificación de Kodaira-Néron de las fibras cerradas del modelo regular minimal de una curva elíptica. En el capítulo siguiente veremos otra demostración alternativa basada en el cálculo explícito de las desingularizaciones de los modelos de Weierstrass, que resultará mucho más larga y farragosa, pero que, a cambio, proporcionará un algoritmo explícito para determinar el tipo de fibra que corresponde a una curva elíptica dada.

En virtud del teorema 7.24, es suficiente estudiar modelos sobre un anillo de valoración discreta. Así pues, en toda esta sección D será un anillo de valoración discreta con cuerpo de cocientes K y cuerpo de restos k. Como de costumbre, llamaremos $S = \mathrm{Esp}\, D$. Consideramos una curva elíptica E/K, su modelo regular minimal $\mathcal{E}/S$ y su modelo de Weierstrass minimal W/S.

NOTA: *Si* $\operatorname{car} k = 2, 3$ *supondremos además que* k *es perfecto.*

Podemos identificar la fibra cerrada de $\mathcal{E}$ con un divisor $\mathcal{E}_s = \Gamma_1^{d_1} \cdots \Gamma_n^{d_n}$, donde $\Gamma_1, \ldots, \Gamma_n$ son sus componentes irreducibles. Según el teorema 8.18, el esquema W se obtiene a partir de $\mathcal{E}$ por contracción de todos los divisores Γ_i menos uno, concretamente, menos el único que corta al divisor horizontal $O = \overline{\{o\}} \subset \mathcal{E}$. Podemos numerar las componentes irreducibles de forma que Γ_1 sea este divisor. En la prueba de 8.7 se ve además que $\Gamma_1 \cap O$ se reduce a un único punto racional, así como que $d_1 = 1$.

Si $\mathcal{E}_s$ es irreducible (es decir, si $n = 1$), entonces no hay ningún divisor vertical que contraer, por lo que $\mathcal{E} = W$ y $\mathcal{E}_s = W_s$ es una cúbica geométricamente íntegra definida por una ecuación de Weierstrass sobre k.

Diremos que E/K tiene reducción de tipo I_0, I_1, $\mathrm{I}_{1,2}$ o II cuando la fibra $\mathcal{E}_s$ es irreducible y E/K tiene el tipo de reducción que indicamos a continuación:

I_0	buena reducción
I_1	reducción multiplicativa racional
$\mathrm{I}_{1,2}$	reducción multiplicativa irracional
II	reducción aditiva

En estos casos, $\mathcal{E}_s = W_s$ es la propia cúbica singular.

Pasamos ahora al caso en que $\mathcal{E}_s$ es reducible ($n \geq 2$), en el cual contamos con el teorema 8.10, que nos garantiza que cada curva Γ_i es una cónica sobre el cuerpo $k_i = H^0(\Gamma_i, \mathcal{O}_{\Gamma_i})$ y, llamando $r_i = |k_i : k|$, se cumple que $\Gamma_i^2 = -2r_i$.

El teorema 6.7 nos da que

$$2r_i d_i = \sum_{j \neq i} d_j \, \Gamma_j \cdot \Gamma_i.$$

Además, r_i divide al grado de cualquier punto de Γ_i, luego $r_i \mid \Gamma_j \cdot \Gamma_i$.

Observemos también que si Γ_i contiene un punto regular p, racional sobre k, como $k_i \subset k(p)$, ha de ser $k_i = k$ (o sea, $r_i = 1$) y el teorema 4.19 implica que $\Gamma_i \cong \mathrm{P}^1_k$.

Esto se aplica a Γ_1, luego $r_1 = d_1 = 1$ y, por consiguiente,

$$2 = \sum_{j \geq 2} d_j \, \Gamma_j \cdot \Gamma_1.$$

Esta igualdad implica que Γ_1 corta a las demás componentes irreducibles a lo sumo en dos puntos. Supongamos primeramente que, en efecto, las corta en dos puntos distintos. A su vez hay dos posibilidades: que en los dos puntos de intersección corte a la misma componente (digamos Γ_2) o que corte a una distinta en cada punto (digamos a Γ_2 y Γ_n).

Analicemos la primera posibilidad. En tal caso $d_2 = 1$ y $\Gamma_1 \cdot \Gamma_2 = 2$. Esto significa que los dos puntos de intersección son racionales sobre k y que son regulares en Γ_1 y Γ_2. Así pues, $\Gamma_2 \cong \mathrm{P}^1_k$. Además:

$$2 = \sum_{j \neq 2} d_j \, \Gamma_j \cdot \Gamma_2,$$

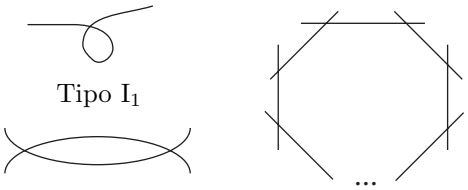
luego Γ_2 no puede cortar a ninguna otra componente irreducible distinta de Γ_1, luego $\Gamma_1 \cup \Gamma_2$ forman una componente conexa de $\mathcal{E}_s$, que es conexa, luego concluimos que $\mathcal{E}_s = \Gamma_1 \cup \Gamma_2$.

La segunda posibilidad es similar: ha de ser $d_2 = 1$ y $\Gamma_1 \cdot \Gamma_2 = 1$, lo cual significa que el punto de intersección es racional sobre k y regular en ambas componentes. Por consiguiente, $\Gamma_2 \cong \mathrm{P}^1_k$. La relación

$$2 = \sum_{j\neq 2} d_j\, \Gamma_j \cdot \Gamma_2$$

se traduce ahora en que Γ_2 sólo puede cortar a una tercera componente, digamos Γ_3, de forma que $\Gamma_2 \cdot \Gamma_3 = 1$. Nuevamente concluimos que $d_3 = 1$ y que $\Gamma_3 \cong \mathrm{P}^1_k$. A su vez, Γ_3 cortará a otra componente, y el proceso continúa hasta que una de ellas, Γ_m corte a Γ_1, con lo que $\Gamma_1, \ldots, \Gamma_m$ formarán una componente conexa de $\mathcal{E}_s$, luego $m = n$.

A estas posibilidades las llamaremos $\mathrm{I_n}$, es decir, $\Gamma_i \cong \mathrm{P}^1_k$, cada curva corta transversalmente a la siguiente en un único punto y la última corta transversalmente a la primera (salvo si $n = 2$, en que Γ_1 y Γ_2 se cortan transversalmente en dos puntos).



Notemos también que Γ_1 es la normalización de W_s, luego E/K tiene en este caso reducción multiplicativa racional.

A partir de aquí suponemos que Γ_1 sólo corta a las demás componentes irreducibles en un punto p, que necesariamente cumplirá $|k(p) : k| \leq 2$.

Supongamos ahora que $|k(p) : k| = 2$, con lo que, si Γ_1 corta, por ejemplo, a Γ_2, se cumple que $\Gamma_1 \cdot \Gamma_2 = 2$, $i_p(\Gamma_1, \Gamma_2) = d_2 = 1$ y Γ_1 ya no puede cortar a más componentes irreducibles. Por otra parte, $k_2 \subset k(p)$, luego tenemos dos posibilidades:
Si $k_2 = k(p)$, entonces $\Gamma_2 \cong \mathrm{P}^1_{k_2}$ por 4.19, y la relación es

$$2 = \sum_{j\geq 3} d_j\, \Gamma_j \cdot \Gamma_2.$$

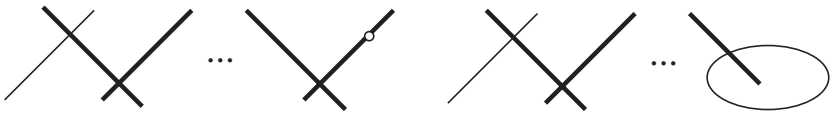
Si Γ_2 corta a Γ_3 en un punto q, ha de ser $k(p) \subset k(q)$, luego sólo es posible que $\Gamma_2 \cdot \Gamma_3 = 2$, $d_3 = 1$, $k(q) = k(p)$. El proceso puede continuarse n veces hasta que, necesariamente, $k_n = k$. Entonces $d_n = r_n = 1$ y la relación

$$2 = \sum_{j\neq n} d_j\, \Gamma_j \cdot \Gamma_n$$

(con $\Gamma_{n-1}\cdot\Gamma_n = 2$) implica que Γ_n ya no corta a más componentes irreducibles.

En resumen: cada componente irreducible corta transversalmente a la siguiente en un único punto (sin cerrar el círculo), todos los puntos de intersección tienen el mismo cuerpo de restos k', tal que $|k' : k| = 2$, se cumple que $\Gamma_1 \cong \mathrm{P}^1_k$, $\Gamma_2 \cong \cdots \cong \Gamma_{n-1} \cong \mathrm{P}^1_{k'}$ y Γ_n es una cónica sobre k.

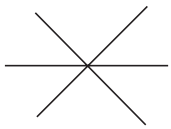
A esta configuración la llamaremos $\mathrm{I}_{2n-1,2}$ si Γ_n es singular y $\mathrm{I}_{2n-2,2}$ si es regular. (En cuyo caso es geométricamente regular por los teoremas 4.13 y 4.14.)



Tipo $\mathrm{I}_{2n-1,2}$ Tipo $\mathrm{I}_{2n-2,2}$

Notemos también que en este caso E/K tiene reducción multiplicativa irracional.

Nos queda considerar el caso en que Γ_1 corta a las demás componentes irreducibles en un único punto racional p (con lo que E/K tiene reducción aditiva).



Tipo IV

Como máximo, Γ_1 puede cortar a otras dos componentes. Si es así, digamos que corta a Γ_2 y Γ_3, se ha de cumplir que $d_2 = d_3 = \Gamma_1\cdot\Gamma_2 = \Gamma_1\cdot\Gamma_3 = 1$, de donde se sigue que $\Gamma_1 \cong \Gamma_2 \cong \Gamma_3 \cong \mathrm{P}^1_k$, las tres componentes se cortan transversalmente dos a dos y no pueden cortar a ninguna otra. A esta posibilidad la llamaremos tipo IV.

A partir de aquí suponemos que Γ_1 corta únicamente a otra componente Γ_2 en un punto racional p. Así pues, $2 = d_2\Gamma_1\cdot\Gamma_2$.

Si $d_2 = 1$ y $\Gamma_1\cdot\Gamma_2 = 2$, entonces Γ_2 ya no puede cortar a más componentes, luego $\mathcal{E}_s = \Gamma_1 \cup \Gamma_2$. Caben dos posibilidades:

Si p es regular en Γ_2, entonces $\Gamma_2 \cong \mathrm{P}^1_k$ y el hecho de que $i_p(\Gamma_1, \Gamma_2) = 2$ es una condición de tangencia. A esta posibilidad la llamaremos Tipo III.

La segunda posibilidad es que Γ_2 sea una cónica sobre k con p como punto singular. Es el tipo IV_2.

Tipo III Tipo IV_2

Nos queda la posibilidad $d_2 = 2$ y $\Gamma_1\cdot\Gamma_2 = 1$. En este caso $\Gamma_2 \cong \mathrm{P}^1_k$ y

$$3 = \sum_{j\geq 3} d_j\,\Gamma_j\cdot\Gamma_2.$$

Supongamos en primer lugar que $d_j = 1$ para todo $j \geq 3$. Entonces tenemos tres posibilidades:

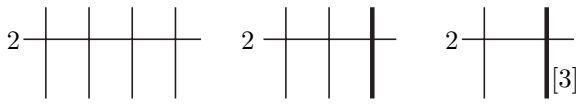
Tipo I_0^* La componente Γ_2 corta a otras tres componentes, Γ_3, Γ_4, Γ_5 con $\Gamma_j \cdot \Gamma_2 = 1$. Necesariamente, los puntos de intersección son racionales y los cortes son transversales, luego $\Gamma_i \cong \mathrm{P}^1_k$. Además ninguna de las tres componentes puede cortar a ninguna otra. (En particular, los puntos de corte de Γ_2 con las demás componentes han de ser distintos dos a dos.)

Tipo $\mathrm{I}_{0,2}^*$ La componente Γ_2 corta a otra componente Γ_3 con $\Gamma_3 \cdot \Gamma_2 = 1$ y a otra componente Γ_4 con $\Gamma_4 \cdot \Gamma_2 = 2$. Entonces $\Gamma_2 \cap \Gamma_3$ es racional, el corte es transversal y $\Gamma_3 \cong \mathrm{P}^1_k$. Además Γ_3 no puede cortar a ninguna otra componente. Respecto a Γ_4, si tomamos $q \in \Gamma_2 \cap \Gamma_4$, la ecuación

$$2r_4 = \sum_{j \neq 4} d_j \, \Gamma_j \cdot \Gamma_4$$

implica que $2 \leq r_4 \leq |k(q) : k| \leq \Gamma_4 \cdot \Gamma_2 = 2$, luego se ha de cumplir que $r_4 = |k(q) : k| = 2$. En particular, q es el único punto de intersección entre Γ_2 y Γ_4 y el corte es transversal. Concluimos además que $\Gamma_4 \cong \mathrm{P}^1_{k(q)}$.

Tipo $\mathrm{I}_{0,3}^*$ La componente Γ_2 corta a otra componente Γ_3 con $\Gamma_3 \cdot \Gamma_2 = 3$. Al igual que en el caso anterior, se deduce que la intersección se produce en un único punto q tal que $|k(q) : k| = 3$, el corte es transversal y $\Gamma_3 \cong \mathrm{P}^1_{k(q)}$.



Tipo I_0^* Tipo $\mathrm{I}_{0,2}^*$ Tipo $\mathrm{I}_{0,3}^*$

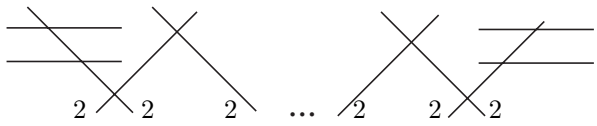
Pasamos ahora al caso en que Γ_2 corta a otra componente irreducible, digamos Γ_4, con $d_4 = 2$. Entonces ha de cortar a otra más, digamos Γ_3, con $d_3 = 1$. Necesariamente $\Gamma_2 \cdot \Gamma_3 = \Gamma_2 \cdot \Gamma_4 = 1$. Esto implica que $\Gamma_i \cong \mathrm{P}^1_k$ para $i = 1, \ldots, 4$ y que todas ellas se cortan transversalmente en puntos racionales distintos. Ahora Γ_3 ya no puede cortar a más componentes, pero Γ_4 sí. Concretamente, tenemos que

$$2 = \sum_{j \geq 5} d_j \, \Gamma_j \cdot \Gamma_4.$$

Si Γ_4 corta a otra componente Γ_5 con $d_5 = 2$, entonces $\Gamma_5 \cdot \Gamma_4 = 1$, el corte es transversal en un punto racional y $\Gamma_5 \cong \mathrm{P}^1_k$. En suma, Γ_5 está en las mismas condiciones que Γ_4. Podemos repetir el argumento hasta llegar a un Γ_{m-1} con $d_{m-1} = 2$ que corte a una componente Γ_m con $d_m = 1$.

A su vez, tenemos dos posibilidades: o bien $\Gamma_{m-1} \cdot \Gamma_m = 1$ y Γ_{m-1} corta a otra componente Γ_{m+1} tal que $d_{m+1} = \Gamma_{m-1} \cdot \Gamma_{m+1} = 1$, o bien $\Gamma_{m-1} \cdot \Gamma_m = 2$.

En el primer caso, deducimos como siempre que los cortes son transversales en puntos racionales distintos, con lo que $\Gamma_m \cong \Gamma_{m+1} \cong \mathrm{P}^1_k$. Además Γ_m y Γ_{m+1} no pueden cortar a ninguna componente aparte de a Γ_{m-1}, y tenemos el tipo que llamaremos I_{n-5}^* (notemos que ha de ser $n \geq 6$):

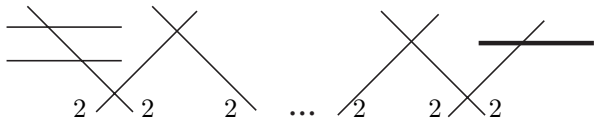


Tipo $\mathrm{I}^*_{\mathrm{n}-5}$

En el caso $\Gamma_{m-1}\cdot\Gamma_m = 2$, la ecuación

$$2r_m = \sum_{j\neq m} d_j\,\Gamma_j\cdot\Gamma_m,$$

teniendo en cuenta que $d_{m-1}\Gamma_{m-1}\cdot\Gamma_m = 4$, implica que $r_m \geq 2$ y, como en el caso $\mathrm{I}^*_{0,2}$, concluimos que Γ_{m-1} y Γ_m se cortan en un único punto q de grado 2 sobre k, así como que el corte es transversal, y $\Gamma_m \cong \mathrm{P}^1_{k(q)}$. Además Γ_m no puede cortar a más componentes y tenemos el tipo que llamaremos $\mathrm{I}^*_{\mathrm{n}-4,2}$:



Tipo $\mathrm{I}^*_{\mathrm{n}-4,2}$

La última posibilidad para Γ_2 es que corte a otra componente Γ_3 con $d_3 = 3$. Entonces $\Gamma_2\cdot\Gamma_3 = 1$, con lo que el corte es transversal en un punto racional y $\Gamma_3 \cong \mathrm{P}^1_k$. Las posibilidades para las intersecciones de Γ_3 vienen dadas por la relación

$$4 = \sum_{j\geq 4} d_j\,\Gamma_j\cdot\Gamma_3.$$

Observemos además que, en esta fórmula, no puede ser $d_j = 1$, ya que entonces, la fórmula correspondiente a Γ_j nos daría que $3\,\Gamma_3\cdot\Gamma_j \leq 2r_j$, luego $\Gamma_3\cdot\Gamma_j \leq r_j$, lo cual es absurdo, ya que $r_j \mid \Gamma_3\cdot\Gamma_j$.

Supongamos en primer lugar que todas las componentes a las que corta Γ_3 tienen multiplicidad $d_j = 2$. Esto da lugar a su vez a dos posibilidades:

Si Γ_3 corta a otras dos componentes Γ_4 y Γ_5, ha de ser $\Gamma_3\cdot\Gamma_4 = \Gamma_3\cdot\Gamma_5 = 1$, con lo que los cortes son transversales en puntos racionales y $\Gamma_4 \cong \Gamma_5 \cong \mathrm{P}^1_k$. Se cumple que

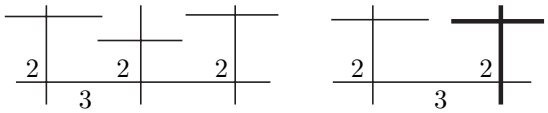
$$1 = \sum_{j\geq 6} d_j\,\Gamma_j\cdot\Gamma_5,$$

luego Γ_5 corta transversalmente a otra componente $\Gamma_6 \cong \mathrm{P}^1_k$ con $d_6 = 1$, y lo mismo vale para Γ_4. Tenemos el tipo IV^*.

La otra opción es que Γ_3 corte a una única componente Γ_4 con $\Gamma_3\cdot\Gamma_4 = 2$. Los argumentos usuales nos dan que ha de ser $r_4 = 2$ y que ambas componentes se cortan transversalmente en un punto q de grado 2 sobre k, de modo que $\Gamma_4 \cong \mathrm{P}^1_{k(q)}$. Para Γ_4 tenemos que

$$2 = \sum_{j\geq 5} d_j\,\Gamma_j\cdot\Gamma_4,$$

Como r_4 tiene que dividir a todos los números de intersección, sólo cabe un sumando con $\Gamma_5 \cdot \Gamma_4 = 2$, $d_5 = 1$. Así Γ_4 y Γ_5 se cortan transversalmente en un punto q' tal que $k(q) = k(q')$, con lo que $\Gamma_5 \cong \mathrm{P}^1_{k(q')}$. Además Γ_5 ya no puede cortar a más componentes irreducibles. A la configuración resultante la llamaremos IV^*_2.



Tipo IV^* Tipo IV^*_2

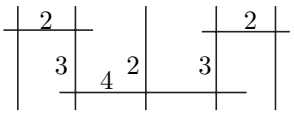
No puede ocurrir que Γ_3 corte a otra componente Γ_4 con $d_4 = 3$, ya que entonces tendría que cortar a otra componente con $d_5 = 1$ y ya hemos descartado esta posibilidad. Supongamos ahora que Γ_3 corta a Γ_4 con $d_4 = 4$ (la máxima multiplicidad posible). Entonces $\Gamma_3 \cdot \Gamma_4 = 1$ y Γ_3 no corta a más componentes. Como siempre, el corte es transversal en un punto racional y $\Gamma_4 \cong \mathrm{P}^1_k$. Ahora tenemos:

$$5 = \sum_{j\geq 5} d_j\, \Gamma_j \cdot \Gamma_4.$$

Una vez más, es imposible que algún $d_j = 1$, pues ello nos llevaría a que $4\,\Gamma_j \cdot \Gamma_4 \leq 2r_j$, lo cual es imposible. Supongamos que Γ_4 corta a Γ_5 con $d_5 = 2$. Si fuera $\Gamma_5 \cdot \Gamma_4 = 2$, entonces Γ_4 tendría que cortar a otra componente con $d_6 = 1$, lo cual es imposible. Por consiguiente, ha de ser $\Gamma_5 \cdot \Gamma_4 = 1$, luego $\Gamma_5 \cong \mathrm{P}^1_k$ y el corte es transversal. Además Γ_5 no puede cortar otras componentes.

Así, Γ_4 ha de cortar a una última componente Γ_6 con $d_6 = 3$ y $\Gamma_6 \cdot \Gamma_4 = 1$. Por lo tanto, $\Gamma_6 \cong \mathrm{P}^1_k$ y tenemos:

$$2 = \sum_{j\geq 7} d_j\, \Gamma_j \cdot \Gamma_6.$$



Tipo III^*

Volvemos a descartar la posibilidad $d_j = 1$, con lo que Γ_6 ha de cortar a una componente Γ_7 con $d_7 = 2$ y $\Gamma_7 \cdot \Gamma_6 = 1$. Nuevamente $\Gamma_7 \cong \mathrm{P}^1_k$ y se ha de cumplir que

$$1 = \sum_{j\geq 8} d_j\, \Gamma_j \cdot \Gamma_7,$$

luego Γ_7 corta a una única componente Γ_8 con $d_8 = 1$ y $\Gamma_7 \cdot \Gamma_8 = 1$. Ésta a su vez ya no puede cortar a ninguna otra más. Hemos obtenido la reducción de tipo III^*.

Por último, supongamos que Γ_4 no corta a ninguna componente posterior con $d_j = 2$. Si cortara a otra Γ_5 con $d_5 = 3$, tendría que cortar a otra Γ_6 con $d_6 = 2$, y este caso ya lo hemos tratado. Si fuera $d_5 = 4$ tendría que ser $d_6 = 1$, luego no hay más posibilidad que $d_5 = 5$, con lo que $\Gamma_4 \cdot \Gamma_5 = 1$. Entonces

$$6 = \sum_{j\geq 6} d_j\, \Gamma_j \cdot \Gamma_5.$$

Si fuera $d_j \leq 2$, tendríamos que

$$\Gamma_j \cdot \Gamma_5 \leq \frac{2}{5} r_j d_j < r_j,$$

luego ha de ser $d_j \geq 3$. Vamos a descartar $d_j = 3$, con lo que la única posibilidad será $d_j = 6$.

Si Γ_5 cortara a Γ_6 con $d_6 = 3$, entonces $r_6 \leq \Gamma_5 \cdot \Gamma_6 \leq 2$, luego

$$6r_6 = 5\,\Gamma_5 \cdot \Gamma_6 + \sum_{j\geq 7} d_j\,\Gamma_j \cdot \Gamma_6.$$

De aquí deducimos en primer lugar que $\Gamma_5 \cdot \Gamma_6 = r_6$, lo que a su vez implica que el sumatorio sólo puede tener un sumando con $d_7 = 1$ y $\Gamma_7 \cdot \Gamma_6 = r_6$. En particular $r_7 \leq r_6$, pero la fórmula para Γ_7 nos da que $2r_7 \geq 3r_6$, lo cual es absurdo.

En definitiva, concluimos que Γ_5 corta a una componente Γ_6 con $d_6 = 6$ y $\Gamma_5 \cdot \Gamma_6 = 1$. Como siempre, el corte es transversal, $r_6 = 1$ y $\Gamma_6 \cong \mathrm{P}^1_k$.

Llamemos t al máximo natural tal que existe una sucesión de componentes irreducibles $\Gamma_1, \ldots, \Gamma_t$ tales que $d_i = i$ y cada una corta transversalmente a la siguiente en un punto racional. Hemos probado que $t \geq 6$. Es fácil ver que cada componente Γ_i con $i < t$ corta únicamente a la siguiente y a la anterior de la forma indicada.

Tenemos entonces que

$$t + 1 = \sum_{j\geq t+1} d_j\,\Gamma_j \cdot \Gamma_t.$$

Supongamos que Γ_t corta únicamente a una componente más, digamos Γ_{t+1}, de modo que $d_{t+1}\,\Gamma_{t+1} \cdot \Gamma_t = t + 1$. Entonces ha de ser $\Gamma_{t+1} \cdot \Gamma_t \geq 2$ o, de lo contrario, Γ_{t+1} prolongaría la sucesión en contra de la maximalidad de t. Observemos que

$$t\,\Gamma_{t+1} \cdot \Gamma_t \leq 2d_{t+1}r_{t+1} \leq (t + 1)r_{t+1}.$$

Como $\Gamma_{t+1} \cdot \Gamma_t = hr_{t+1}$, ha de ser $ht \leq t + 1$, luego $h = 1$. Concluimos que $r_{t+1} = \Gamma_{t+1} \cdot \Gamma_t \geq 2$. Por consiguiente:

$$2\,\frac{t+1}{r_{t+1}}\,r_{t+1} = tr_{t+1} + \sum_{j\geq t+2} d_j\,\Gamma_j \cdot \Gamma_{t+1}.$$

En primer lugar, esto implica que $2t+2 \geq tr_{t+1}$ y, si fuera $r_{t+1} \geq 3$, entonces $t \leq 2$, contradicción. Así pues, $r_{t+1} = 2$. La igualdad anterior se reduce a

$$2 = \sum_{j\geq t+2} d_j\,\Gamma_j \cdot \Gamma_{t+1}.$$

Como $2 = r_{t+1} \mid \Gamma_{t+1} \cdot \Gamma_{t+1}$, el sumatorio tiene únicamente un sumando, con $d_{t+1} = 1$, pero entonces

$$2r_{t+2} \geq \frac{t+1}{2}\,\Gamma_{t+2} \cdot \Gamma_{t+1}$$

y, como r_{t+2} divide al número de intersección, queda que $(t+1)/2 \leq 2$, luego $t \leq 5$, contradicción.

Con esto hemos probado que Γ_t ha de cortar al menos a dos componentes, Γ_{t+1} y Γ_{t+2}. El argumento usual nos da que $d_{t+1} \geq t/2$, $d_{t+1} \geq t/2 \geq 3$, por lo que Γ_t sólo puede cortar a Γ_{t+1} y Γ_{t+2}.

Si t es impar, ha de ser $d_{t+1} = d_{t+2} = (t+1)/2$, con $\Gamma_t \cdot \Gamma_{t+1} = \Gamma_t \cdot \Gamma_{t+2} = 1$. En particular, $r_{t+1} = r_{t+2} = 1$. Tenemos que

$$1 = \sum_{j \geq t+2} d_j \, \Gamma_j \cdot \Gamma_{t+1},$$

por lo que el sumatorio tiene sólo un sumando con $d_j = 1 = \Gamma_j \cdot \Gamma_{t+1} = 1$, $r_j = 1$, de donde se sigue a su vez que

$$2 = 2d_j r_j \geq d_{t+1} \, \Gamma_j \cdot \Gamma_{t+1} = \frac{t+1}{2},$$

de donde $t \leq 5$, contradicción.

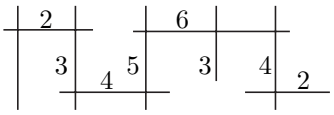
Concluimos que t es par, con lo que ha de ser $d_{t+1} = t/2$, $d_{t+2} = (t+2)/2$, $\Gamma_t \cdot \Gamma_{t+1} = \Gamma_t \cdot \Gamma_{t+2} = 1$, $r_{t+1} = r_{t+2} = 1$.

El cálculo usual muestra que Γ_{t+1} no corta a más componentes irreducibles. En cuanto a Γ_{t+2} tenemos que

$$2 = \sum_{j \geq t+3} d_j \, \Gamma_j \cdot \Gamma_{t+2}.$$

La cota usual para los d_j es $d_j \geq (t+2)/4 \geq 2$, luego el sumatorio sólo puede tener un sumando, con $d_{t+3} = 2$ y $\Gamma_{t+3} \cdot \Gamma_{t+2} = 1$. Esto nos lleva a que

$$4 - \frac{t+2}{2} = \sum_{j \geq t+4} d_j \, \Gamma_j \cdot \Gamma_{t+3}.$$



Tipo II*

El miembro izquierdo ha de ser ≥ 0, lo que implica que $t \leq 6$ (luego, de hecho, $t = 6$) y la igualdad anterior prueba que $\Gamma_{t+3} = \Gamma_9$ ya no corta a más componentes. En suma, hemos obtenido la última configuración posible, a la que llamaremos II*.

Con esto hemos probado el teorema siguiente:

Teorema 8.26 (Kodaira, Néron) *Sea $S = \operatorname{Esp} D$, donde D es un anillo de valoración discreta con cuerpo de cocientes K y cuerpo de restos k. Sea $\mathcal{E}/S$ el modelo regular minimal de una curva elíptica E/K. Si $\operatorname{car} k = 2, 3$ suponemos además que k es perfecto. Entonces la fibra cerrada $\mathcal{E}_s/k$ tiene una de las formas descritas en la tabla* 8.1.

También hemos visto que la curva E/K tiene buena reducción cuando tiene tipo I_0, tiene reducción multiplicativa racional cuando tiene tipo I_n, con $n \geq 1$, tiene reducción multiplicativa irracional cuando tiene tipo $\mathrm{I}_{n,2}$, con $n \geq 1$ y tiene reducción aditiva en todos los demás casos.

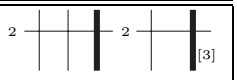
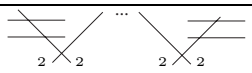
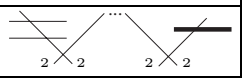
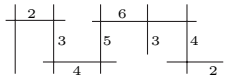
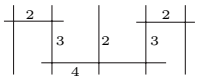
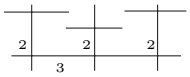
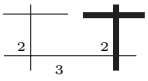
Tipo	Nº comp.	Configuración	Tipo	Nº comp.	Configuración
I_0	1				
I_1	1		$\mathrm{I}_{1,2}$	1	
I_n	$n \geq 2$		$\mathrm{I}_{\mathrm{n},2}$ n par	$\frac{n+2}{2}$	
II	1		$\mathrm{I}_{\mathrm{n},2}$ $\mathrm{n}\geq 2$ n impar	$\frac{n+1}{2}$	
III	2				
IV	3		IV_2	2	
I_0^*	5		$\mathrm{I}_{0,2}^*$, $\mathrm{I}_{0,3}^*$	4, 3	
I_n^*	$n+5$		$\mathrm{I}_{\mathrm{n},2}^*$	$n+4$	
II^*	9				
III^*	8				
IV^*	7		IV_2^*	5	

Tabla 8.1: Posibles configuraciones de la fibra cerrada $\mathcal{E}_s$.

En esta tabla hay que entender lo siguiente:

- El valor de n es siempre ≥ 1 salvo cuando se indica lo contrario.
- Los tipos I_0, I_1, $\mathrm{I}_{1,2}$ y II corresponden a curvas cúbicas: una curva elíptica en el primer caso y malas reducciones de curvas elípticas en los restantes (multiplicativa racional, multiplicativa irracional y aditiva, respectivamente).
- En todos los demás casos, una curva abierta representa a P_k^1 si no está en negrita y a $\mathrm{P}_{k'}^1$ en caso contrario, donde k' es una extensión cuadrática de k (la misma para todas las componentes de una misma fibra), excepto en el tipo $\mathrm{I}_{0,3}^*$, donde la extensión es cúbica (lo cual se señala con un [3]).
- En el tipo $\mathrm{I}_{\mathrm{n},2}$ la elipse representa una cónica geométricamente regular sobre k, mientras que la recta en negrita con un punto blanco representa (como en el tipo IV_2) una cónica sobre k' con un punto singular.
- Los números (salvo el [3] del tipo $\mathrm{I}_{0,3}^*$) representan la multiplicidad de cada componente en la fibra. Las que no tienen número tienen multiplicidad 1.
- Los cortes entre componentes distintas son todos transversales excepto el del tipo III, que tiene número de intersección 2 en el punto. En el tipo IV son transversales dos a dos.
- Los puntos de corte p entre dos componentes distintas son racionales salvo si una de las componentes está en negrita, en cuyo caso $k(p) = k'$.

Ejemplo Si $X/\mathbb{Z}$ es el modelo regular minimal de la curva elíptica dada por la ecuación de Weierstrass $Y^2 = X^3 + 25$, en el ejemplo de la página 144 hemos visto que su fibra X_5 es de tipo IV. ∎

Ejemplo Si $X/\mathbb{Z}$ es el modelo regular minimal de la ecuación de Selmer considerada en la sección 5.4, en principio no podíamos asegurar a priori que sus fibras cerradas se tuvieran que corresponder con los tipos que hemos obtenido, porque $X_\eta/\mathbb{Q}$ no es una curva elíptica (porque, aunque tiene género 1, no tiene puntos racionales, ni, por lo tanto, modelos de Weierstrass), pero lo cierto es que hemos probado que la fibra X_2 es de tipo IV_2^* y la fibra X_3 es de tipo II^*.

Por otra parte, la fibra X_5 es la curva proyectiva sobre $\mathbb{Z}/5\mathbb{Z}$ dada por la ecuación homogénea

$$3X^3 + 4Y^3 = 3(X + 2Y)(X^2 + 3XY + 4Y^2) = 0,$$

por lo que es de tipo IV_2. Las fibras restantes (teniendo en cuenta que tienen puntos racionales) son de tipo I_0. ∎

Capítulo IX

El algoritmo de Tate

Vamos a dar un algoritmo debido a Tate para determinar explícitamente la estructura de la fibra cerrada del modelo regular minimal de una curva elíptica definida por una ecuación de Weierstrass. Esto nos proporcionará una demostración alternativa (bastante más larga) del teorema 8.26.

9.1 Descripción del algoritmo

A lo largo de este capítulo, D será un anillo de valoración discreta con cuerpo de cocientes K y cuerpo de restos k. Como en el capítulo anterior, si $\operatorname{car} k = 2, 3$, supondremos además que k es perfecto. Llamaremos $\pi \in D$ a un elemento primo cualquiera. Consideramos una curva elíptica E/K determinada por una ecuación de Weierstrass

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \qquad a_i \in K,$$

la cual determina un modelo de Weierstrass W/S, donde $S = \operatorname{Esp} D$.

Usaremos la notación $a_{ij} = \pi^{-j}a_i$. Para cada $d \in D$, llamaremos $\bar{d} \in k$ a su clase de restos.

El modelo regular minimal que pretendemos calcular no depende de la ecuación de Weierstrass de E/K que consideremos, por lo que muchos pasos del algoritmo que vamos a describir requerirán realizar cambios de variables del tipo descrito en el teorema 4.23, es decir, de la forma

$$X = u^2X' + r, \qquad Y = u^3Y' + su^2X' + t, \qquad u, r, s, t \in K, \quad u \neq 0.$$

Concretamente, si alguno de los coeficientes de la ecuación dada no está en D, lo primero que hemos de hacer es un cambio de variables de la forma $X = \pi^{-2n}X'$, $Y = \pi^{-3n}Y'$ con $n \geq 1$ suficientemente grande como para que los nuevos coeficientes cumplan $a_i \in D$.

A partir de aquí, el algoritmo de Tate se divide en 11 pasos. Cada uno de los 10 primeros tiene una hipótesis local, que si se cumple nos da que la fibra

cerrada $\mathcal{E}_s$ es de un tipo concreto (con lo que el algoritmo termina) y, en caso contrario, su negación se convierte en una hipótesis acumulativa para todos los pasos siguientes. El undécimo paso consiste en realizar un cambio de variables y volver a empezar desde el paso 1.

Los pasos intermedios requerirán en varias ocasiones realizar cambios de variables, pero todos ellos tendrán $u = 1$, por lo que el discriminante de la ecuación de Weierstrass permanecerá invariante. Por el contrario, si se cumplen las condiciones necesarias para llegar al paso 11, demostraremos que el cambio de variables $X = \pi^2 X'$, $Y = \pi^3 Y'$ nos llevará a una nueva ecuación cuyos coeficientes seguirán estando en D, por lo que podremos empezar con ella desde el paso 1, pero el nuevo discriminante será $\Delta' = \Delta/\pi^{12}$, y así

$$v(\Delta') = v(\Delta) - 12 < v(\Delta).$$

El hecho de que $v(\Delta)$ disminuya cada vez que llegamos al paso 11 (y no se modifique en los otros pasos) garantiza que, tras un número finito de iteraciones, el algoritmo debe terminar.

Así pues, si el algoritmo llega al paso 11, esto significa que la ecuación de Weierstrass de partida no era minimal. Dicho de otro modo, si en el paso 1 partimos de una ecuación minimal, el algoritmo terminará necesariamente antes de llegar al paso 11, pero si no es así, llegaremos a una ecuación minimal tras un número finito de iteraciones.

Enunciamos ahora el algoritmo. En cada paso, subrayamos la hipótesis local, es decir, la que no se cumplirá en los pasos siguientes:

Paso 1 Si $\underline{\pi \nmid \Delta}$, entonces la fibra cerrada es de tipo I_0.

Paso 2 Supongamos que $\pi \mid \Delta$. Entonces con un cambio de variables[1] se consigue que

$$\pi \mid a_3, a_4, a_6, \qquad \pi \mid b_4, b_6, b_8$$

Si $\underline{\pi \nmid b_2}$, la reducción es multiplicativa y la fibra cerrada es de tipo $\mathrm{I_n}$ o $\mathrm{I_n^*}$, donde $n = v(\Delta)$. Se da el primer caso si y sólo si el polinomio $T^2 + \bar{a}_1 T - \bar{a}_2$ tiene sus raíces en k.

Paso 3 Supongamos que $\pi \mid b_2$. Entonces la reducción es aditiva y con un cambio de variables se consigue que

$$\pi \mid a_1, a_2, a_3, a_4, a_6.$$

Si $\pi^2 \nmid a_6$, la fibra cerrada es de tipo II.

Paso 4 Supongamos que $\pi^2 \mid a_6$. Si $\underline{\pi^2 \nmid a_4}$, la fibra cerrada es de tipo III.

Paso 5 Supongamos que $\pi^2 \mid a_4$. Si además $\underline{\pi^3 \nmid b_6}$, entonces la fibra cerrada es de tipo IV o IV_2. Se da el primer caso si y sólo si las raíces del polinomio $Y^2 + \bar{a}_{3,1} Y - \bar{a}_{6,2}$ están en k.

[1] Por concisión no indicamos aquí los cambios de variable que hay que hacer en cada paso, pero en la prueba los determinaremos explícitamente.

Paso 6 Supongamos que $\pi^3 \mid b_6$. Entonces, con un cambio de variables se consigue que

$$\pi \mid a_1, a_2, \quad \pi^2 \mid a_3, a_4, \quad \pi^3 \mid a_6.$$

Consideramos el polinomio

$$P(T) = T^3 + a_{2,1}T^2 + a_{4,2}T + a_{6,3}.$$

Si $P(T)$ tiene raíces simples en $\bar{k}$, la fibra cerrada es de tipo I_0^*, $\mathrm{I}_{0,2}^*$ o $\mathrm{I}_{0,3}^*$, según si las raíces están todas en k, hay una en k y dos fuera de k o las tres están fuera de k.

Paso 7 Supongamos que $P(T)$ tiene al menos una raíz de multiplicidad mayor que 1. Entonces, con un cambio de variables se consigue que

$$\pi \mid a_1, a_2, \quad \pi^2 \mid a_3, \quad \pi^3 \mid a_4, \ \pi^4 \mid a_6.$$

Si $P(T)$ tiene una raíz doble, la fibra cerrada es de tipo $\mathrm{I}_{\mathrm{n}}^*$ o $\mathrm{I}_{\mathrm{n},2}^*$. Cuando $\operatorname{car} k \neq 2$, el valor de n es $n = v(\Delta) - 6$. En general, n puede calcularse mediante el procedimiento siguiente:

- Consideramos el polinomio $P_1(T) = T^2 + \bar{a}_{3,2}T - \bar{a}_{6,4}$. Si tiene raíces simples en $\bar{k}$, entonces el tipo es I_1^* o $\mathrm{I}_{1,2}^*$ según si tales raíces están o no en k.
- Supongamos que $P_1(T)$ tiene una raíz doble. Entonces, con un cambio de variables se consigue que

  $$\pi^3 \mid a_3, \quad \pi^5 \mid a_6.$$

  Consideramos el polinomio $Q_1(T) = \bar{a}_{2,1}T^2 + \bar{a}_{4,2}T + \bar{a}_{6,5}$. Si tiene raíces simples en $\bar{k}$, entonces el tipo es I_2^* o $\mathrm{I}_{2,2}^*$ según si tales raíces están o no en k.
- Supongamos que $Q_1(T)$ tiene una raíz doble. Entonces, con un cambio de variables se consigue que

  $$\pi^3 \mid a_4, \quad \pi^6 \mid a_6.$$

  Consideramos el polinomio $P_2(T) = T^2 + \bar{a}_{3,3}T - \bar{a}_{6,6}$. Si tiene raíces simples en $\bar{k}$, entonces el tipo es I_3^* o $\mathrm{I}_{3,2}^*$ según si tales raíces están o no en k.
- Supongamos que $P_2(T)$ tiene una raíz doble. Entonces, con un cambio de variables se consigue que

  $$\pi^4 \mid a_3, \quad \pi^7 \mid a_6.$$

  Consideramos el polinomio $Q_2(T) = \bar{a}_{2,1}T^2 + \bar{a}_{4,3}T + \bar{a}_{6,7}$. Si tiene raíces simples en $\bar{k}$, entonces el tipo es I_4^* o $\mathrm{I}_{4,2}^*$ según si tales raíces están o no en k.

Este proceso termina necesariamente tras un número finito de pasos.

Paso 8 Supongamos que $P(T)$ tiene una raíz triple. Entonces, con un cambio de variables se consigue que

$$\pi \mid a_1, \quad \pi^2 \mid a_2, a_3, \quad \pi^3 \mid a_4, \quad \pi^4 \mid a_6.$$

Consideramos el polinomio $P_1(T) = T^2 + \bar{a}_{3,2}T - \bar{a}_{6,4}$. Si tiene raíces simples en $\bar{k}$, la fibra cerrada es de tipo IV^* o IV_2^*, según si las raíces están o no en k.

Paso 9 Supongamos que $P_1(T)$ tiene una raíz doble. Entonces, con un cambio de variables se consigue que

$$\pi^3 \mid a_3, \quad \pi^5 \mid a_6.$$

Si $\pi^4 \nmid a_4$, entonces la fibra cerrada es de tipo III^*.

Paso 10 Supongamos que $\pi^4 \mid a_4$. Si $\pi^6 \nmid a_6$, entonces la fibra cerrada es de tipo II^*.

Paso 11 Supongamos que $\pi^6 \mid a_6$. Entonces tenemos que

$$\pi \mid a_1, \quad \pi^2 \mid a_2, \quad \pi^3 \mid a_3, \quad \pi^4 \mid a_4, \quad \pi^6 \mid a_6,$$

luego el cambio de variables $X = \pi^2 X'$, $Y = \pi^3 Y'$ nos da una nueva ecuación de Weierstrass con coeficientes en D, con la que volvemos a empezar desde el paso 1.

9.2 Inicio de la prueba

Partimos del modelo de Weierstrass W/S determinado por la ecuación dada y, tras varias explosiones (tal vez ninguna), llegaremos a un superficie aritmética X/S y un homomorfismo birracional $\pi : X \longrightarrow W$, de modo que la fibra cerrada X_s será de uno de los tipos de la tabla 8.1.

Observemos en primer lugar que esto ya implica que X/S es el modelo regular minimal de E/K. En efecto, sólo hay que probar que la superficie X/S es minimal, para lo cual basta con que sea relativamente minimal, es decir, con que no tenga divisores excepcionales. Ahora bien, usando el teorema 6.7, es fácil calcular las autointersecciones de todas las componentes irreducibles de una fibra de cualquiera de los tipos de la tabla 8.1, lo que nos permite concluir que X/S no tiene divisores excepcionales.

Por ejemplo, en el tipo $\mathrm{I_n}$ ($n \geq 2$) todas las autointersecciones valen $\Gamma_i^2 = -2$, y deberían ser -1 para que Γ_i fuera excepcional. En el tipo $\mathrm{I_{n,2}}$, tenemos que $\Gamma_1^2 = -2$ (cuando debería ser -1 para ser excepcional) y $\Gamma_i^2 = -4$ para $i > 1$ (cuando debería ser[2] -2). (Sólo tenemos en cuenta las componentes isomorfas a $\mathrm{P}^1_{k'}$, para cierto k', ya que esto es necesario para que puedan ser

[2]No es casual que el valor real sea siempre el doble del que sería necesario para que fueran excepcionales, sino que es consecuencia del teorema 8.10.

divisores excepcionales.) Similarmente se comprueban sin dificultad todos los demás casos.

Más aún, el teorema 8.19 nos permite concluir que el modelo W/S (asociado a la ecuación que estemos considerando en ese momento, tras los cambios de variables que hayamos realizado) es el modelo de Weierstrass minimal de E/K, de modo que el algoritmo de Tate termina siempre con una ecuación minimal.

Los primeros pasos del algoritmo son los más simples, porque son los casos en los que el modelo de Weierstrass W/S es suave, con lo que coincide con el modelo regular minimal y no hay que calcular ninguna explosión.

Paso 1 El primer paso es inmediato: si $\pi \nmid \Delta$, entonces la curva E/K tiene buena reducción y, por definición, la fibra cerrada de $\mathcal{E}/S = W/S$ es de tipo I_0. ∎

Paso 2 A partir de aquí suponemos que $\pi \mid \Delta$, pero no la hipótesis local del paso 2. Resulta entonces que la fibra W_s tiene un punto singular, necesariamente racional. Para calcularlo hay que resolver (en k) el sistema de ecuaciones que resulta de igualar a 0 las derivadas parciales de la ecuación de Weierstrass:

$$\frac{\partial F}{\partial X} = \bar{a}_1 Y - 3X^2 - 2\bar{a}_2 X - \bar{a}_4 = 0, \quad \frac{\partial F}{\partial Y} = 2Y + \bar{a}_1 X + \bar{a}_3 = 0.$$

El lector puede encontrar fácilmente fórmulas generales para la solución, si bien tendrá que distinguir tres casos, según que la característica de k sea 2, 3 u otra cualquiera. Pongamos que la solución es $(X, Y) = (\bar{r}, \bar{t})$, para ciertos r, $t \in D$. Entonces, el cambio de variables

$$X = X' + r, \qquad Y = Y' + t$$

transforma la ecuación en otra para la cual el punto singular es $(0, 0)$, lo cual se traduce en que $\bar{a}_3 = \bar{a}_4 = \bar{a}_6 = 0$, tal y como se afirma en el enunciado del paso 2. Las definiciones de b_4, b_6, b_8 implican inmediatamente que éstos también son nulos en k, es decir, que son divisibles entre π. De acuerdo con el teorema 8.24 (véase la prueba) la singularidad de W_s será un nodo si el polinomio

$$T^2 + \bar{a}_1 T - \bar{a}_2$$

tiene dos raíces simples en $\bar{k}$, y será una cúspide si tiene una raíz doble. A su vez, esto se reduce a que su discriminante $\bar{b}_2 = \bar{a}_1^2 + 4\bar{b}_2$ cumpla $\bar{b}_2 \neq 0$ o $\bar{b}_2 = 0$, respectivamente. En el primer caso, la reducción es multiplicativa racional si el polinomio anterior tiene sus raíces en k y multiplicativa irracional en caso contrario.

Ahora es inmediato que, bajo la hipótesis local del paso 2, es decir, si $\pi \nmid b_2$, la fibra cerrada es de tipo $\mathrm{I_n}$ o $\mathrm{I_{n,2}}$, y además sólo en este caso, ya que estos tipos son los únicos que corresponden a la reducción multiplicativa. Más concretamente, sabemos que la fibra será de tipo $\mathrm{I_n}$ si la reducción es multiplicativa racional y será de tipo $I_{n,2}$ en caso contrario. No obstante, para probar que el valor de n es precisamente $n = v(\Delta)$ vamos a tener que calcular explícitamente el

modelo regular minimal, con lo que no vamos a necesitar esta observación y, tal y como hemos afirmado, obtendremos una prueba alternativa del teorema 8.26 independiente de la dada en el capítulo anterior.

Recordemos el teorema 5.11, según el cual el modelo W/S es regular si y sólo si $\pi^2 \nmid a_6$. Con esto podemos probar el caso $n = 1$ del paso 2. En efecto, si $\pi \nmid b_2$ y $v(\Delta) = 1$, entonces $v(b_8) = 1$, porque todos los otros sumandos de la definición de Δ son divisibles entre π^2. Como

$$b_8 = b_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \equiv b_2a_6 \pmod{\pi^2},$$

resulta que $\pi^2 \nmid a_6$, por lo que $W/S = \mathcal{E}/S$ y concluimos que la fibra cerrada es de tipo I_1 o $\mathrm{I}_{1,2}$.

Recíprocamente, si $\pi \nmid b_2$ y $v(\Delta) \geq 2$, entonces $\pi^2 \mid b_8$, luego $\pi^2 \mid a_6$ y el modelo de Weierstrass es singular, por lo que tendremos que resolver la singularidad.

Nos ocuparemos de ello en la sección siguiente. Ahora nos ocupamos del Paso 3, que, con lo visto hasta aquí, es ya inmediato:

Paso 3 Ya hemos visto que si $\pi \mid b_2$ la reducción es aditiva, puesto que el polinomio

$$T^2 + \bar{a}_1T - \bar{a}_2$$

tiene una raíz doble en $\bar{k}$. De hecho, estará en k, porque, como anula también a la derivada, ha de ser

$$\bar{\alpha} = \begin{cases} -\bar{a}_1/2 & \text{si } \operatorname{car} k \neq 2 \\ \sqrt{\bar{a}_2} & \text{si } \operatorname{car} k = 2. \end{cases}$$

Este $\alpha \in D$ cumple que

$$T^2 + \bar{a}_1T - \bar{a}_2 = (T - \bar{\alpha})^2,$$

de modo que

$$a_1 \equiv -2\alpha \pmod{\pi}, \qquad -a_2 \equiv \alpha^2 \pmod{\pi}.$$

El cambio $Y = Y' + \alpha X'$ en la ecuación de Weierstrass nos da que

$$a_1' = a_1 + 2\alpha \equiv 0 \pmod{\pi},$$

$$a_2' = a_2 - \alpha a_1 - \alpha^2 = (a_2 + \alpha^2) - \alpha(a_1 + 2\alpha) \equiv 0 \pmod{\pi},$$

así como que $a_3' = a_3$, $a_4' = a_4 - \alpha a_3$, $a_6' = a_6$, luego ahora $\pi \mid a_1, a_2, a_3, a_4, a_6$, tal y como afirma el enunciado del paso 3.

Si suponemos que $\pi^2 \nmid a_6$, el teorema 5.11 nos da que $\mathcal{E}/S = W/S$ y, por definición, la fibra cerrada es de tipo II. ∎

Llegados a este punto tenemos pendiente demostrar el paso 2 bajo la hipótesis adicional $v(\Delta) \geq 2$ (que implica $\pi^2 \mid a_6$) y los pasos siguientes al paso 3,

que también suponen $\pi^2 \mid a_6$. Así pues, a partir de aquí trabajaremos bajo las hipótesis

$$\pi \mid a_3, a_4, \quad \pi^2 \mid a_6,$$

comunes a ambos contextos, sin suponer ni $\pi \nmid b_2$ (la hipótesis local del paso 2) ni $\pi \mid b_2$ (la hipótesis acumulada desde el paso 3).

El teorema 5.11 nos da que el modelo de Weierstrass W/S tiene un punto singular, que, visto como punto del abierto $W_0 \subset W$ determinado por la ecuación de Weierstrass afín, se identifica con el ideal $\mathfrak{m} = (\pi, x, y)$. Vamos a calcular la explosión $\widetilde{W}$ de W con centro en $\mathfrak{m}$, aunque en la práctica nos bastará calcular la explosión de W_0. Para ello nos basamos en la nota de la página 147.

La explosión $\widetilde{W_0}$ está formada por la unión de tres abiertos principales, que llamaremos W_1, W_2 y W_3. El primero es el espectro de $D[x, y, x/\pi, y/\pi] = D[x_1, y_1]$, donde $x = \pi x_1$, $y = \pi y_1$. De la ecuación de Weierstrass obtenemos la relación:

$$y_1^2 + a_1 x_1 y_1 + a_{3,1} y_1 = \pi x_1^3 + a_2 x_1^2 + a_{4,1} x_1 + a_{6,2}.$$

El segundo abierto, W_2, es el espectro de $D[x, y, y/x, \pi/x] = D[x, y', \pi']$ y los generadores cumplen las ecuaciones[3]

$$x\pi' = \pi, \qquad y'^2 + a_1 y' + a_{3,1} y'\pi' = x + a_2 + a_{4,1}\pi' + a_{6,2}\pi'^2.$$

(Hemos sustituido $y = xy'$, y también $\pi = x\pi'$ cuando ha sido necesario, para dividir entre x^2.) Finalmente, W_3 es el espectro del anillo $D[x, y, x/y, \pi/y] = D[y, x'', \pi'']$, cuyos generadores cumplen las ecuaciones

$$\pi'' y = \pi, \quad 1 + a_1 x'' + a_{3,1}\pi'' = x''^3 y + a_2 x''^2 + a_{4,1} x''\pi'' + a_{6,2}\pi''^2.$$

Los sistemas de coordenadas de estos tres abiertos están relacionados de forma natural. Por ejemplo, teniendo en cuenta que $x_1 = x/\pi$, $y_1 = y/\pi$, $x'' = x/y$, $\pi'' = \pi/y$, deducimos que

$$x_1 = x''/\pi'', \qquad y_1 = 1/\pi''.$$

Esto significa que $W_1 \cap W_3$ es $D(\pi'')$ en W_3. Similarmente concluimos que $W_2 \cap W_3$ es $D(x')$ en W_3. Ahora bien, por la segunda ecuación de W_3, sucede que $V(x'', \pi'') = \varnothing$ o, lo que es lo mismo, que $W_3 = D(x'') \cup D(y'')$. En otros términos, como abiertos de la explosión $\widetilde{W_0}$, se cumple que $W_3 \subset W_1 \cup W_2$, por lo que $\widetilde{W_0} = W_1 \cup W_2$ y podemos prescindir de W_3.

Observemos a continuación que, como en la segunda ecuación de W_2 se puede despejar la variable x, resulta que $D[x, y', \pi'] = D[y', \pi']$ y los generadores satisfacen la ecuación

$$(y'^2 + a_1 y' + a_{3,1} y'\pi' - a_2 - a_{4,1}\pi' - a_{6,2}\pi'^2)\pi' = \pi.$$

[3]Notemos que $\pi' = \pi/x$ es, por definición, un elemento del cuerpo de cocientes de $D[x, y]$, no de D o de K.

Así pues, la explosión $\widetilde{W}_0$ está determinada por los datos siguientes:

$$\begin{array}{ll}
W_1 & y_1^2 + a_1x_1y_1 + a_{3,1}y_1 = \pi x_1^3 + a_2x_1^2 + a_{4,1}x_1 + a_{6,2} \\
W_{1s} & y_1^2 + \bar{a}_1x_1y_1 - \bar{a}_2x_1^2 + \bar{a}_{3,1}y_1 - \bar{a}_{4,1}x_1 - \bar{a}_{6,2} = 0 \\
W_2 & y'^2\pi' + a_1y'\pi' + a_{3,1}y'\pi'^2 = \pi + a_2\pi' + a_{4,1}\pi'^2 + a_{6,2}\pi'^3 \\
W_{2s} & (y'^2 + \bar{a}_1y' - \bar{a}_2 + \bar{a}_{3,1}y'\pi' - \bar{a}_{4,1}\pi' - \bar{a}_{6,2}\pi'^2)\pi' = 0
\end{array}$$

Ambos abiertos están relacionados por el cambio de coordenadas

$$x_1 = 1/\pi', \qquad y_1 = y'/\pi', \quad \text{o} \quad y' = y_1/x_1, \quad \pi' = 1/x_1.$$

Esto ha de entenderse como que $W_1 \cap W_2$ es $D(x_1) \subset W_1$ y $D(\pi') \subset W_2$.

La fibra W_{1s} es una cónica (afín), que puede ser irreducible o descomponerse en dos componentes irreducibles. En cualquier caso, como $W_1 = D(\pi)$ en $\widetilde{W}_0$, en la prueba del teorema 5.17 f) hemos visto que la fibra de $\mathfrak{m}$ en W_1 es el cerrado asociado al ideal (π), es decir, toda la fibra cerrada W_{1s}. Así pues, concluimos que la explosión contrae W_{1s} al punto $\mathfrak{m}$.

La fibra cerrada de W_2 está formada por la recta de ecuación $\pi' = 0$ y una cónica (afín), que no es exactamente "otra". En efecto, consideremos la cónica proyectiva C/k definida por la ecuación

$$Y^2 + \bar{a}_1XY - \bar{a}_2X^2 + \bar{a}_{3,1}YZ - \bar{a}_{4,1}XZ - \bar{a}_{6,2}Z^2 = 0.$$

Claramente, $C = D(Z) \cup D(X)$ y, deshomogeneizando respecto de Z y respecto de X, respectivamente, vemos que la cónica afín $D(Z)$ es isomorfa a W_{1s} y que $D(X)$ es isomorfa a la cónica de W_{2s}. Más aún, comparando las ecuaciones del cambio de coordenadas entre W_1 y W_2 con las correspondientes ecuaciones para $D(Z)$ y $D(X)$, concluimos que ambos isomorfismos coinciden en $D(X) \cap D(Z)$, luego determinan un isomorfismo de C en un subconjunto cerrado de $\widetilde{W}_{0s}$, una cónica proyectiva a la que llamaremos también C.

En estos términos, tenemos que $W_{1s} \subset C$, mientras que $C \cap W_{2s}$ es la cónica afín que hemos encontrado en W_{2s}. Más concretamente, la diferencia entre C y W_{1s} es la intersección

$$C \cap V(\pi') = V(\pi, \pi', y'^2 + a_1y' - a_2),$$

la cual consistirá en dos puntos racionales, un punto de grado 2 sobre k o de un punto doble racional según si el polinomio $T^2 + \bar{a}_1T - \bar{a}_2$ tiene dos raíces simples en k, dos raíces simples en $\bar{k} \setminus k$ o una raíz doble en k, es decir, en función de que E/K tenga reducción multiplicativa (racional o irracional) o aditiva. Por otra parte, la diferencia entre C y $C \cap W_{2s}$ es la intersección

$$W_{1s} \cap V(x_1) = V(\pi, x_1, y_1^2 + a_{3,1}y_1 - a_{6,2}),$$

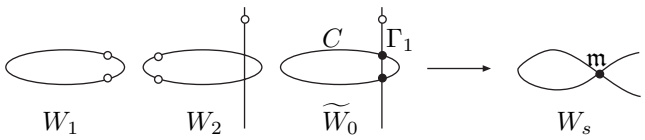
también formada por uno o dos puntos cerrados.

En particular, C es la clausura en $\widetilde{W}$ de W_{1s} y de $C \cap W_{2s}$. Como sabemos que la explosión contrae W_{1s} al punto $\mathfrak{m}$, lo mismo vale para toda la cónica C. Por otra parte, como la explosión ha de ser suprayectiva, la fibra $W_s \cap W_0$ ha de tener una antiimagen en $\widetilde{W}_0$, y ésta no puede ser sino la recta $\pi' = 0$. Como W_s tiene un punto no contenido en W_0 (el punto infinito), la clausura de esta recta en $\widetilde{W}$, a la que llamaremos Γ_1, ha de tener un punto no contenido en $\widetilde{W}_0$, que se corresponda con el punto infinito de W_s. Si consideramos a Γ_1 con la estructura de subesquema cerrado reducido, tenemos que $\Gamma_1 \cap W_2 \cong A^1_k$, luego es una curva proyectiva regular (también es regular en el punto infinito, porque la explosión es un isomorfismo fuera de la fibra de $\mathfrak{m}$) birracionalmente equivalente a P^1_k, luego $\Gamma_1 \cong \mathrm{P}^1_k$.

Observemos que $\Gamma_1 \cap W_2 = V(\pi, \pi')$, por lo que ya hemos calculado la intersección

$$\Gamma_1 \cap C = V(\pi, \pi', y'^2 + a_1 y' - a_2).$$

La figura ilustra la situación (donde, concretamente, hemos representado el caso en que Γ_1 corta a C en dos puntos distintos).



9.3 Conclusión del paso 2

En esta sección suponemos la hipótesis local del paso 2, a saber, que $\pi \nmid b_2$. También podemos suponer que $v(\Delta) \geq 2$, pues el caso $v(\Delta) = 1$ ya lo hemos discutido. Esto implica a su vez que $\pi^2 \mid a_6$, por lo que podemos continuar en el punto en que lo hemos dejado en la sección anterior.

Si igualamos a cero las derivadas de la ecuación de W_{1s} obtenemos el sistema de ecuaciones lineales

$$-2\bar{a}_2 x_1 + \bar{a}_1 y_1 - \bar{a}_{4,1} = 0,$$

$$\bar{a}_1 x_1 + 2y_1 + \bar{a}_{3,1} = 0,$$

cuyo determinante es $\bar{b}_2 \neq 0$. Por lo tanto, tiene una solución $(\bar{\alpha}, \bar{\beta})$. El cambio de variables $X = X' + \pi\alpha$, $Y = Y' + \pi\beta$ en la ecuación original nos lleva a una nueva ecuación en la que el sistema anterior tiene solución $(0,0)$, por lo que $\bar{a}_{3,1} = \bar{a}_{4,1} = 0$. A su vez, esto hace que $W_{1s} = C \cap W_1$ tiene a lo sumo un punto geométricamente singular, que será el punto racional $(0,0)$ supuesto que pertenezca a C, lo que equivale a que $\bar{a}_{6,2} = 0$.

Observemos ahora que si C tiene un punto geométricamente singular, éste ha de estar en W_1. En efecto, tras el cambio de variables que acabamos de realizar, la ecuación de $C \cap W_2$ se reduce a

$$y'^2 + \bar{a}_1 y' - \bar{a}_2 - \bar{a}_{6,2}\pi'^2 = 0.$$

Por otra parte, $W_1 \cap W_2 = D(\pi')$, y si un punto de $V(\pi')$ fuera geométricamente singular, sería un punto racional $(\alpha, 0)$, donde α sería raíz del polinomio $T^2 + \bar{a}_1 T - \bar{a}_2$ y también de su derivada, lo cual es imposible.

En resumen: todos los puntos de la cónica C son geométricamente regulares salvo quizá uno. Esto sucede si y sólo si $\bar{a}_{62} = 0$, y en tal caso el punto singular es el punto que en W_{1s} tiene coordenadas $(0,0)$, es decir, el ideal $\mathfrak{p}_1 = (\pi, x_1, y_1)$. Por otra parte, es fácil comprobar la congruencia

$$\Delta \equiv -b_2^2 b_8 \equiv -b_2^3 a_6 \text{ (mód } \pi^4),$$

de la que deducimos que C es geométricamente regular si y sólo si $v(\Delta) = 2$.

Esto hace que todos los puntos de $\widetilde{W}$ sean suaves salvo quizá el punto $\mathfrak{p}_1$ (si es que pertenece a C) y los puntos de $C \cap \Gamma_1$. Éstos, ciertamente, no son suaves, pero sucede que son regulares, pues la ecuación de W_2 nos da que

$$\pi = (y'^2 + a_1 y' - a_2)\pi' + (a_{3,1} y' - a_{4,1} - a_{6,2}\pi')\pi'^2,$$

por lo que

$$(\pi, \pi', y'^2 + a_1 y' - a_2) = (\pi', y'^2 + a_1 y' - a_2).$$

Esto significa que cualquier ideal maximal que contenga a este ideal está generado por dos elementos (π' y un factor irreducible de $y'^2 + a_1 y' + a_2$), luego es un punto regular.

En definitiva, si $v(\Delta) = 2$, concluimos que $\widetilde{W}$ es regular, y su fibra cerrada es de tipo I_2 o $\mathrm{I}_{2,2}$, según si $C \cap \Gamma_1$ consta de dos puntos racionales o de un punto doble. (En el primer caso, al tener un punto racional, la cónica C ha de ser isomorfa a P^1_k.) Esto prueba el caso $n = 2$ del paso 2.

Supongamos ahora que $v(\Delta) \geq 3$ o, equivalentemente, que $\bar{a}_{6,2} = 0$ y que C tiene a $\mathfrak{p}_1$ como único punto singular, que es, a su vez, el único posible punto singular de $\widetilde{W}$. Ahora bien, la congruencia anterior muestra que $v(\Delta) = 3$ si y sólo si $\pi^4 \nmid a_6$, en cuyo caso $a_{6,2} = \epsilon\pi$, donde ϵ es una unidad en D, por lo que la ecuación de W_1 permite despejar π y muestra que $\pi \in (x_1, y_1)$, lo que a su vez implica que $\mathfrak{p}_1$ es regular en $\widetilde{W}$, luego $\widetilde{W}$ es regular. La fibra es de tipo I_3 o $\mathrm{I}_{3,2}$, según que las raíces del polinomio $T^2 + \bar{a}_1 T - \bar{a}_2$ estén o no en k. Esto prueba el caso $n = 3$ del paso 2.

Supongamos ahora que $\pi^4 \mid a_6$ (o, equivalentemente, que $v(\Delta) \geq 4$) y vamos a calcular la explosión de $\widetilde{W}$ con centro en $\mathfrak{p}_1$. Es suficiente calcular la explosión de W_1. Podemos expresarla como unión de tres abiertos afines, W_{11}, W_{12} y W_{13}. El primero es el espectro de $D[x_1, y_1, x_1/\pi, y_1/\pi] = D[x_2, y_2]$, donde los generadores satisfacen la ecuación

$$y_2^2 + a_1 x_2 y_2 + a_{3,2} y_2 = \pi^2 x_2^3 + a_2 x_2^2 + a_{4,2} x_2 + a_{6,4}.$$

El segundo es el espectro de $D[x_1, y_1, y_1/x_1, \pi/x_1] = D[x_1, y_1', \pi']$, cuyos generadores satisfacen las ecuaciones

$$y_1'^2 + a_1 y_1' + a_{3,2} y_1' \pi' = \pi x_1 + a_2 + a_{4,2}\pi' + a_{6,4}\pi'^2, \qquad \pi = x_1 \pi'.$$

Por último, el tercero es el espectro de $D[x_1, y_1, x_1/y_1, \pi/y_1] = D[y_1, x_1', \pi'']$, cuyas ecuaciones son

$$1 + a_1x_1' + a_{3,2}\pi'' = \pi x_1'^3 y_1 + a_2 x_1'^2 + a_{4,2}\pi'' + a_{6,4}\pi'', \qquad \pi = y_1\pi''.$$

Ahora bien, $W_{11} \cap W_{13} = D(\pi'')$ y $W_{12} \cap W_{13} = D(x_1')$ en W_{13} y la ecuación muestra que $V(x_1', \pi'') = \varnothing$, luego $W_{13} \subset W_{11} \cup W_{12}$ y esto nos permite prescindir de W_{13}.

Observemos además que la fibra cerrada W_{11s} es la cónica de ecuación

$$y_2^2 + \bar{a}_1x_2y_2 + \bar{a}_{3,2}y_2 = \bar{a}_2x_2^2 + \bar{a}_{4,2}x_2 + \bar{a}_{6,4}.$$

Si igualamos sus derivadas a 0, obtenemos el sistema de ecuaciones

$$-2\bar{a}_2x_2 + \bar{a}_1y_2 - \bar{a}_{4,2} = 0,$$

$$\bar{a}_1x_2 + 2y_2 + \bar{a}_{3,2} = 0,$$

cuyo determinante es $\bar{b}_2 \neq 0$. Si la solución es $(\bar{\alpha}, \bar{\beta})$, el cambio de variables $X = X' + \pi^2\alpha$, $Y = Y' + \pi^2\beta$ en la ecuación original nos permite suponer desde aquí que $\bar{a}_{3,2} = \bar{a}_{4,2} = 0$. En definitiva, tenemos:

W_{11}	$y_2^2 + a_1x_2y_2 + a_{3,2}y_2 = \pi^2x_2^3 + a_2x_2^2 + a_{4,2}x_2 + a_{6,4}$
W_{11s}	$y_2^2 + \bar{a}_1x_2y_2 - \bar{a}_2x_2^2 = \bar{a}_{6,4}$
W_{12}	$y_1'^2 + a_1y_1' + a_{3,2}y_1'\pi' = \pi x_1 + a_2 + a_{4,2}\pi' + a_{6,4}\pi'^2, \quad x_1\pi' = \pi$
W_{12s}	$y_1'^2 + \bar{a}_1y_1' - \bar{a}_{6,4}\pi'^2 = \bar{a}_2, \quad x_1\pi' = 0$

La fibra W_{11s} es una cónica afín (tal vez reducible) que sabemos que se ha de contraer a $\mathfrak{p}_1$. Para analizar W_{12s} observamos que un ideal primo de $D[x_1, y_1', \pi']$ que contenga a π ha de contener a x_1 o a π', lo que a su vez implica que contendrá a uno de los ideales siguientes:

$$I_1 = (\pi, \pi', y_1'^2 + a_1y_1' - a_2),$$

$$I_2 = (\pi, x_1, y_1'^2 + a_1y_1' - a_2 - a_{6,4}\pi'^2).$$

Teniendo en cuenta la relación entre las coordenadas de los dos abiertos:

$$x_1 = x_2\pi, \quad y_1' = y_2/x_2, \quad \pi' = 1/x_2,$$

es fácil ver que la cónica afín $V(I_2)$ se corresponde con W_{11s}, de modo que la unión de ambas es una cónica proyectiva C_2, que se contrae a $\mathfrak{p}_1$ por la explosión. De hecho, se cumple que C_2 es la fibra de $\mathfrak{p}_1$, porque la cónica afín $C_1 = V(I_1)$ se corresponde con la cónica $C \cap W_1$. En efecto: si el polinomio $T^2 + a_1T - a_2$ es irreducible en $k[T]$, entonces I_1 es un ideal primo que, teniendo en cuenta la inclusión $D[x_1, y_1] \subset D[x_1, y_1', \pi']$, contiene a los generadores de C, luego su

imagen por la explosión tiene que ser C o bien el punto $\mathfrak{p}_1$, pero este segundo caso no puede darse, ya que I_1 no contiene a x_1, pues

$$D[x_1, y_1', \pi']/I_1 \cong k'[X],$$

donde $k' = k[T]/(T^2 + a_1T - a_2)$ y el isomorfismo hace corresponder $\bar{x}_1 \mapsto X$. Si el polinomio es reducible, el argumento se adapta cambiando k' por k e I_1 por cada uno de sus dos primos minimales.

Observemos ahora que $C_1 \cap C_2 = V(\pi, x_1, \pi', y_1'^2 + a_1y_1' - a_2)$ está formado por dos puntos racionales distintos o un único punto de grado 2 sobre k. Más concretamente, se da el primer caso si C_1 (o, equivalentemente, C) es reducible y el segundo si es irreducible. Las ecuaciones de W_{12} muestran que

$$(\pi, x_1, \pi', y_1'^2 + a_1y_1' - a_2) = (x_1, \pi'),$$

y esto implica que los puntos de la intersección son regulares. En particular, todos los puntos de C_1 son regulares en la explosión. Consideremos ahora C_2. Si tiene un punto geométricamente singular, ha de estar en $C_2 \cap W_{11}$, ya que $W_{11} \cap W_{12} = D(\pi')$ y

$$C \cap W_{12} \cong \mathrm{Esp}(\bar{k}[Y, Z]/(Y^2 + \bar{a}_1Y - \bar{a}_2 - \bar{a}_{6,4}Z^2)).$$

Si esta cónica tuviera un punto geométricamente singular en $V(z)$, sería un punto racional de la forma $(\alpha, 0)$, donde α sería una raíz del polinomio $T^2 + \bar{a}_1T - \bar{a}_2$ y de su derivada, lo cual es imposible.

Así pues, C_2 tiene a lo sumo un punto geométricamente singular, lo cual sucederá si y sólo si $\bar{a}_{6,4} = 0$, y en tal caso será el punto racional $(0, 0)$ de W_{11s}, es decir, el ideal $\mathfrak{p}_2 = (\pi, x_2, y_2)$. Tras el último cambio de variable, tenemos la congruencia

$$\Delta \equiv -b_2^2b_8 \equiv -b_2^3a_6 \ (\text{mód } \pi^6),$$

por lo que $v(\Delta) = 4$ si y sólo si $\bar{a}_{6,4} \neq 0$, si y sólo si C_2 es geométricamente regular, lo cual implica a su vez que la explosión es regular. Si C_1 es reducible, entonces $C_2 \cong \mathrm{P}^1_k$, luego la fibra cerrada consta de cuatro componentes irreducibles de tipo I_4. Por el contrario, si C_1 es irreducible, la fibra es claramente de tipo $\mathrm{I}_{4,2}$. Esto prueba el caso $n = 4$ del paso 2.

Supongamos ahora que $v(\Delta) \geq 5$, con lo que $\bar{a}_{6,4} = 0$ y C_2 tiene a $\mathfrak{p}_2$ como único punto singular. La congruencia anterior prueba que $v(\Delta) = 5$ si y sólo si $\pi^6 \nmid a_6$, con lo que $a_{6,4} = \epsilon\pi$, donde ϵ es una unidad de D, y la ecuación de W_{11} nos permite despejar π para probar que $\mathfrak{p}_2 = (x_2, y_2)$ es regular en la explosión, luego ésta es una superficie aritmética. Observemos que C_2 es reducible (en k) si y sólo si lo es C_1, por lo que la fibra cerrada tiene la estructura de I_5 si las cónicas son reducibles y de $\mathrm{I}_{5,2}$ en caso contrario. Esto prueba el caso $n = 5$ del paso 2.

Supongamos ahora que $v(\Delta) \geq 6$, con lo que $\pi^6 \mid a_6$. Ahora tendríamos que calcular la explosión de W_{11} con centro $\mathfrak{p}_2$. Ahora bien, la ecuación de W_1 es idéntica a la de W_{11} salvo que la primera tiene πx_1^3, $a_{3,1}$, $a_{4,1}$, $a_{6,2}$ donde

la segunda tiene $\pi^2 x_2^3$, $a_{3,2}$, $a_{4,2}$, $a_{6,4}$. Todo lo que hemos razonado desde el cálculo de la explosión de W_1 sigue siendo válido en general si partimos de una ecuación

$$y_i^2 + a_1 x_i y_i + a_{3,i} y_i = \pi^i x_i^3 + a_2 x_i^2 + a_{4,i} x_i + a_{6,2i}.$$

Así, por inducción probamos que, cuando $v(\Delta) = n$, la fibra cerrada del modelo regular minimal de E/K es de tipo $\mathrm{I_n}$ o $\mathrm{I_{n,2}}$, según si el polinomio $T^2 + \bar{a}_1 T - \bar{a}_2$ tiene o no sus raíces en k. Esto termina la prueba del paso 2.

9.4 Los pasos intermedios

Paso 4 A partir de aquí suponemos las hipótesis acumuladas hasta el paso 4, pero no su hipótesis local, concretamente, tenemos que

$$\pi \mid a_1, a_2, a_3, a_4, \qquad \pi^2 \mid a_6, b_6, b_8.$$

Podemos enlazar con lo dicho al final de la sección 9.2. En particular, tenemos la explosión $\widetilde{W}$, cuya fibra cerrada consta de la recta Γ_1 y de la cónica C, que en el abierto W_2 tienen ecuaciones

$$\pi' = 0, \qquad y'^2 + \bar{a}_{3,1} y' \pi' - \bar{a}_{4,1} \pi' - \bar{a}_{6,2} \pi'^2 = 0.$$

Su intersección es el punto racional $\mathfrak{p} = (\pi, y', \pi')$. Notemos que es regular en $\widetilde{W}$, pues la ecuación de W_2 implica que $\pi \in (y', \pi')$, por lo que $\mathfrak{p} = (y', \pi')$.

Ahora consideramos la hipótesis local del paso 4, a saber, que $\pi^2 \nmid a_4$, de modo que $\bar{a}_{4,1} \neq 0$. Esto implica que C es geométricamente regular (las derivadas de la ecuación de C tanto en W_1 como en W_2 no pueden anularse simultáneamente), luego todos los puntos de la fibra cerrada de $\widetilde{W}_s$ son suaves en $\widetilde{W}$ excepto $\mathfrak{p}$, luego $\widetilde{W}$ es regular.

Por otra parte, la cónica C es irreducible (por ejemplo, porque de la ecuación de $C \cap W_1$ podemos despejar x_1, lo que se traduce en que $C \cap W_1 \cong A_k^1$). Como tiene un punto racional, esto implica que $C \cong \mathrm{P}_k^1$. Por último, en el anillo $\mathcal{O}_{C,\mathfrak{p}}$ se cumple que

$$\pi' = \frac{y'^2}{-\bar{a}_{3,1} y' + \bar{a}_{6,2} \pi' + \bar{a}_{4,1}} \in (y'),$$

luego $\mathfrak{p} = (y')$ y $\Gamma_1 \cdot C = i_{\mathfrak{p}}(\Gamma_1, C) = v_{\mathfrak{p}}(\pi') = 2$. Con esto podemos afirmar que $\mathcal{E}/S$ es $\widetilde{W}/S$, y que la fibra cerrada es de tipo III. ∎

Paso 5 Suponemos ahora que $\pi^2 \mid a_4$, de modo que $\bar{a}_{4,1} = 0$. Ahora la cónica C es (en W_2):

$$y'^2 + \bar{a}_{3,1} y' \pi' - \bar{a}_{6,2} \pi'^2 = 0.$$

La condición local $\pi^3 \nmid b_6 = \pi^2(a_{3,1}^2 + 4a_{6,2})$ equivale a que el discriminante del polinomio $Y^2 + \bar{a}_{3,1} Y - \bar{a}_{6,2}$ sea no nulo, luego la cónica se descompone en $\bar{k}$ en producto de dos rectas distintas entre sí y distintas de $\pi' = 0$, y todas ellas se cortan en el punto $\mathfrak{p}$, que ya hemos visto que es regular en $\widetilde{W}_0$. Nuevamente, la explosión es suave y la fibra cerrada es de tipo IV o IV_2. ∎

Paso 6 Por las hipótesis acumuladas tenemos que $\pi \mid a_1, a_2, a_3$, $\pi^2 \mid a_4, a_6$. Ahora estamos suponiendo que

$$Y^2 + \bar{a}_{3,1}Y - \bar{a}_{6,2} = (Y - \bar{\alpha})^2,$$

para cierto $\alpha \in D$, de modo que

$$a_{3,1} + 2\alpha \equiv 0 \text{ (mód } \pi), \qquad a_{6,2} + \alpha^2 \equiv 0 \text{ (mód } \pi).$$

Hacemos el cambio de variables $Y' = Y + \alpha\pi$, con lo que $a'_1 = a_1$, $a'_2 = a_2$,

$$a'_3 = \pi a_{3,1} + 2\pi\alpha \equiv 0 \text{ (mód } \pi^2),$$

$$a'_4 = \pi^2 a_{4,2} - \pi^2 \alpha a_{1,2} \equiv 0 \text{ (mód } \pi^2),$$

$$a'_6 = a_6 - \pi\alpha a_3 - \pi^2\alpha^2 = \pi^2(a_{6,2} + \alpha^2) - \alpha\pi^2(a_{3,1} + 2\alpha) \equiv 0 \text{ (mód } \pi^3).$$

Ahora la fibra cerrada de $\widetilde{W}_0$ consta de una recta simple Γ_1, que en W_2 tiene ecuación $\pi' = 0$, y una recta doble Γ_2, que en W_2 tiene ecuación $y'^2 = 0$ y en W_1 es $y_1^2 = 0$.

Los puntos de Γ_1 son suaves excepto el punto $\mathfrak{p} = (\pi, y', \pi')$, donde corta a Γ_2, el cual, no obstante, es regular, según hemos visto al principio de la sección. Así pues, $\widetilde{W}_0$ sólo puede tener puntos singulares sobre la recta doble Γ_2. Más concretamente, la ecuación de W_1 implica que

$$\pi = \frac{y_1 + a_1x_1 + a_{3,1}}{x_1^3 + a_{2,1}x_1^2 + a_{4,2}x_1 + a_{6,3}}\, y_1,$$

de donde se desprende que W_1 es regular[4] en todos los puntos de $\Gamma_2 = (\pi, y_1)$ que no estén en $V(\pi, y_1, x_1^3 + a_{2,1}x_1^2 + a_{4,2}x_1 + a_{6,3})$, es decir, salvo a lo sumo en tres puntos. Notemos además que el único punto de Γ_2 que no está en W_1 es el punto de $\Gamma_2 \cap V(\pi') \subset \Gamma_1$, que es $\mathfrak{p}$, y ya hemos destacado que es regular.

Vamos a calcular la explosión de la recta completa Γ_2. Notemos que está completamente contenida en $\widetilde{W}_0$, por lo que podemos calcular simplemente la explosión $\widetilde{W}'_0$ de $\widetilde{W}_0$. Ahora bien, hemos visto que Γ_2 es regular salvo a lo sumo en tres puntos de W_1, y la propiedad d) tras la definición 5.12 implica que la explosión es un isomorfismo sobre la antiimagen del complementario de dichos puntos. Por consiguiente, no es necesario calcular la explosión de W_2, pues su fibra cerrada constará al menos de dos componentes, a las que seguiremos llamando Γ_1 y Γ_2, que se corresponderán con las componentes del mismo nombre en W_2, la primera será una recta simple y la segunda una recta doble, y ambas serán regulares salvo quizá Γ_2 en a lo sumo tres puntos, donde puede cortar a nuevas componentes irreducibles,[5] pero éstas nos las encontraremos al estudiar

[4] El argumento completo es el siguiente: como $D[x_1, y_1]/(\pi, y_1) \cong k[T]$, que es un dominio de ideales principales, un ideal maximal $\mathfrak{P}$ que contenga a Γ_2 ha de ser de la forma $(\pi, y_1, P(x_1))$ y, como $\pi \in (y_1)$, de hecho es igual a $(y_1, P(x_1))$, luego tiene dos generadores y esto implica que $\mathcal{O}_{W_1,\mathfrak{P}}$ es regular.)

[5] En virtud de la misma propiedad d), el hecho de que, en efecto, vamos a encontrar tales componentes, demostrará que, ciertamente, Γ_2 es singular en tales puntos.

la explosión de W_1. Además, la explosión de W_2 será regular en todos los puntos salvo quizá en los de las componentes "nuevas", cosa que, de nuevo, podemos estudiar desde W_1.

Por el mismo motivo, podemos predecir que al calcular la fibra cerrada de la explosión de W_1 nos encontraremos una componente irreducible doble $\Gamma_2 \subset \widetilde{W}_1$ y tal vez otras más que se contraigan a puntos de $\Gamma_2 \subset W_1$.

En efecto, la explosión de centro (π, y_1) está determinada por dos abiertos afines, W_{11} y W_{12}. El primero es el espectro del álgebra $D[x_1, y_1, y_1/\pi] = D[x_1, y_2]$, cuyos generadores satisfacen la ecuación

$$\pi y_2^2 + a_1 x_1 y_2 + a_{3,1} y_2 = x_1^3 + a_{2,1} x_1^2 + a_{4,2} x_1 + a_{6,3}.$$

Por otra parte, W_{12} es el espectro de $D[x_1, y_1, \pi/y_1] = D[x_1, y_1, \pi']$, cuyos generadores cumplen las ecuaciones

$$y_1 \pi' = \pi, \quad y_1 + a_1 x_1 + a_{3,1} = x_1^3 \pi' + a_{2,1} x_1^2 \pi' + a_{4,2} x_1 \pi' + a_{6,3} \pi'.$$

Como podemos despejar y_1, podemos eliminar este generador, y los otros dos cumplen la ecuación

$$(x_1^3 + a_{2,1} x_1^2 + a_{4,2} x_1 + a_{6,3}) \pi'^2 = a_1 x_1 \pi' + a_{3,1} \pi' + \pi.$$

Para referencias posteriores destacamos las ecuaciones de ambos abiertos y las de sus fibras cerradas:

W_{11}	$\pi y_2^2 + a_1 x_1 y_2 + a_{3,1} y_2 = x_1^3 + a_{2,1} x_1^2 + a_{4,2} x_1 + a_{6,3}$
W_{11s}	$P(x_1) = 0$
W_{12}	$(x_1^3 + a_{2,1} x_1^2 + a_{4,2} x_1 + a_{6,3}) \pi'^2 = a_1 x_1 \pi' + a_{3,1} \pi' + \pi$
W_{12s}	$P(x_1) \pi'^2 = 0$

Aquí $P(T)$ es el polinomio definido en el enunciado del paso 6, aunque de momento no suponemos nada sobre sus raíces.

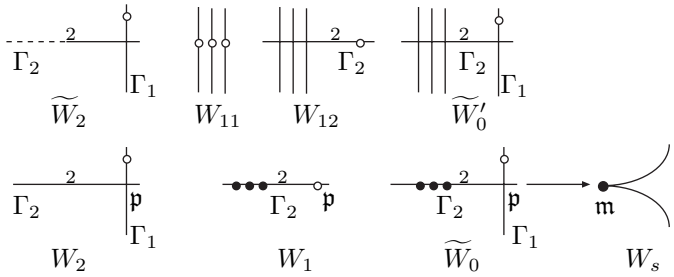
La relación entre ambos sistemas de coordenadas es que $\pi' = 1/y_2$. Más concretamente, esto significa que $W_{11} \cap W_{12}$ es $D(y_2)$ en W_{11} y $D(\pi')$ en W_{12}, y la relación indicada determina el isomorfismo entre ambos abiertos que se corresponde con la identidad cuando se considera a ambos como subesquemas abiertos de $\widetilde{W}'$.

Observemos ahora las fibras cerradas. Es claro que W_{11s} tiene tantas componentes irreducibles como divisores primos distintos tiene el polinomio $P(T)$, las cuales se corresponden a través del isomorfismo natural con otras tantas componentes irreducibles de W_{12}, pero éste tiene una más, a saber, la recta doble (π, π').

Tal y como habíamos predicho, vamos a comprobar que las componentes irreducibles de W_{11s} se contraen a puntos de Γ_2. En efecto, cada una de ellas

es de la forma $\mathfrak{P} = (\pi, Q(x_1))$, donde $Q(T)$ es un factor irreducible de $P(T)$ en $k[T]$. El homomorfismo $k[x_1, y_1] \longrightarrow k[x_1, y_2]$ que induce la restricción de la explosión a las fibras cerradas cumple $y_1 \mapsto \pi y_2 = 0$, luego la antiimagen de $\mathfrak{P}$ contiene a $(Q(x_1), y_1)$, que es un ideal maximal de $k[x_1, y_1]$. Así pues, la imagen de $\mathfrak{P}$ es ciertamente un punto cerrado en Γ_2.

Como la propia recta doble Γ_2 ha de tener una antiimagen y no tiene ninguna en W_{11}, su antiimagen ha de ser la recta doble (π, π'), lo cual implica a su vez que ésta tiene que identificarse con (un abierto de) la recta correspondiente en la explosión de W_2 y que habíamos llamado también Γ_2. Con esto tenemos ya una descripción completa de la fibra cerrada de $\widetilde{W}'$:



Al igual que en $\widetilde{W}$, la fibra cerrada contiene una recta Γ_1 cuya imagen en W recorre toda la fibra cerrada W_s, y esta recta corta a una recta doble Γ_2 que se contrae al punto singular de W_s. Pero en $\widetilde{W}'$ tenemos nuevas componentes irreducibles que se contraen a puntos de Γ_2 en $\widetilde{W}$. Estas componentes son las asociadas al ideal $(\pi, P(x_1))$, y su número depende de las raíces del polinomio $P(T)$. El análisis de estas componentes lo llevaremos a cabo en los pasos siguientes del algoritmo.

Para terminar la descripción general de $\widetilde{W}'$ observamos que todos los puntos de Γ_2 son regulares, pues la ecuación de W_{12} muestra que $\pi \in (\pi')$.

Bajo la hipótesis local del paso 6, es decir, que $P(T)$ tiene tres raíces simples[6] en $\bar{k}$, es inmediato que la fibra cerrada de W_{11} consta de tres rectas simples isomorfas a A^1_k, o de dos rectas simples isomorfas a A^1_k y $A^1_{k'}$, respectivamente (donde k' es una extensión cuadrática de k), o bien de una recta simple $A^1_{k'}$ (donde k'/k es una extensión cúbica), según que $P(T)$ tenga sus tres raíces en k, tenga una en k y dos fuera de k, o tenga las tres fuera de k. En cualquiera de los tres casos, sus puntos son suaves excepto los puntos en los que las rectas cortan a Γ_2, pero ya hemos visto que éstos son regulares, luego $\widetilde{W}'$ es regular y tenemos las configuraciones I^*_0, $\mathrm{I}^*_{0,2}$, $\mathrm{I}^*_{0,3}$. (Notemos que las clausuras en $\widetilde{W}'$ de las rectas afines que hemos encontrado han de ser rectas proyectivas, isomorfas a P^1_k o $\mathrm{P}^1_{k'}$.)

[6]En la práctica, esto equivale s que π no divida al discriminante

$$\Delta(P) = \pi^{-6}(-4a_2^3a_6 + a_2^2a_4^2 - 4a_4^3 - 27a_6^2 + 18a_2a_4a_6),$$

que es una condición fácil de comprobar.

Paso 7 Supongamos ahora que $P(T)$ tiene una raíz en $\bar{k}$ de multiplicidad mayor que 1. Dicha raíz ha de estar necesariamente en k, porque es raíz de $P(T)$ y de su derivada, luego su polinomio mínimo tiene grado 1. Por ejemplo, si $\operatorname{car} k \neq 2, 3$, al dividir un polinomio $T^3 + bT^2 + xT + d$ entre su derivada obtenemos:

$$T^3 + bT^2 + cT + d = (3T^2 + 2bT + c)\left(\frac{1}{3}T + \frac{1}{9}b\right) + \left(\frac{2}{3}c - \frac{2}{9}b^2\right)T + d - \frac{1}{9}bc.$$

Si el resto es nulo, entonces la derivada ha de tener una raíz doble, ya que si tuviera dos raíces simples distintas, el polinomio de partida tendría dos raíces dobles, lo cual es imposible. En tal caso, el polinomio tiene una raíz triple, y será la raíz del cociente, luego es $r = -b/3$. Si el resto es no nulo, entonces no puede ser constante, y concluimos que

$$r = \frac{bc - 9d}{6c - 2b^2}.$$

Si $\operatorname{car} k = 2$, el resto ha de ser 0, aunque esto no significa que la raíz sea triple. La derivada es $T^2 + c = (T + \sqrt{c})^2$, donde $\sqrt{c} \in k$ porque suponemos que k es perfecto, y ésta es la raíz buscada.

Si $\operatorname{car} k = 3$, la derivada es $2bT + c$, luego $r = c/b$, salvo que b sea nulo, en cuyo caso también ha de serlo c, y concluimos que el polinomio tiene una raíz triple $r = -\sqrt[3]{d} \in k$.

El cambio de variable (en la ecuación de Weierstrass original) $X = X' + \pi r$ hace que $\pi \mid a'_{4,2}$, $\pi \mid a'_{6,3}$ o, lo que es lo mismo, que $P(T) = T^3 + \bar{a}_{2,1}T^2$, de modo que la raíz múltiple es ahora $r = 0$. En resumen, a partir de aquí tenemos que

$$\pi \mid a_1, a_2, \quad \pi^2 \mid a_3, \quad \pi^3 \mid a_4, \quad \pi^4 \mid a_6.$$

Además, la condición local del paso 7 (que la raíz sea doble y no triple) equivale a que $\pi^2 \nmid a_2$. Terminaremos este paso en la sección siguiente, de modo que el paso 8 enlazará con este punto.

9.5 Conclusión del paso 7

Suponemos a partir de aquí que $\pi^2 \nmid a_2$, con lo que la fibra cerrada de $\widetilde{W}'$ tiene una componente doble Γ_2 que corta a dos componentes simples Γ_1 y Γ_3, así como a otra componente doble Γ_4, que es la única que puede contener puntos singulares. Concretamente, la ecuación de W_{11} muestra que

$$\pi = \frac{x_1^2 + a_{2,1}x_1 + a_{4,2} - a_1 y_2}{y_2^2 + a_{3,2}y_2 - a_{6,4}}\, x_1,$$

por lo que todos los puntos de $\Gamma_4 = (\pi, x_1)$ son regulares en W_1 salvo a lo sumo los de $V(\pi, x_1, y_2^2 + a_{3,2}y_2 - a_{6,4})$. Por otra parte, el único punto de Γ_4 que no

está en W_1 es $\Gamma_4 \cap V(\pi') \subset (\pi, \pi') = \Gamma_2$, es decir, se trata del punto $\Gamma_4 \cap \Gamma_2$, que es regular porque todos los puntos de Γ_2 lo son.

Vamos a calcular la explosión de centro Γ_4. Observemos que Γ_4 se contrae a un punto de Γ_2 que está en W_1, luego Γ_4 está completamente contenida en la antiimagen de W_1, que es $W_{11} \cup W_{12}$, de modo que no necesitamos considerar la explosión de W_2. Ahora bien, por el mismo argumento empleado anteriormente, basta calcular la explosión de W_{11}, pues podemos asegurar que $\widetilde{W}_{12s}$ constará de tres componentes irreducibles Γ_2, Γ_3 y Γ_4, que se corresponderán con las del mismo nombre en W_{11}, y tal vez algunas más, que sólo pueden cortar a Γ_2 en a lo sumo dos puntos y que nos las encontraremos al estudiar la explosión de W_{11}. Además, todos los puntos de la explosión que no estén en $\widetilde{W}_{11}$ serán regulares.

Por otra parte, también podemos afirmar que $\widetilde{W}_{11}$ debe contener dos componentes que se correspondan con Γ_3 y Γ_4, y tal vez otras que corten a Γ_4 en sus puntos singulares. En efecto, $\widetilde{W}_{11}$ es unión de dos abiertos, W_{111} y W_{112}. El primero es el espectro de $D[x_1, y_2, x_1/\pi] = D[x_2, y_2]$, mientras que el segundo es el espectro de $D[x_1, y_2, \pi/x_1] = D[x_1, y_2, \pi']$. Las ecuaciones son las siguientes:

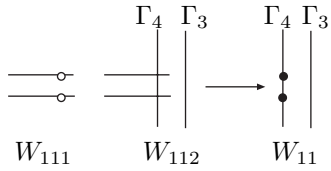
$$\begin{array}{ll}
W_{111} & y_2^2 + a_1x_2y_2 + a_{3,2}y_2 = \pi^2x_2^3 + a_2x_2^2 + a_{4,2}x_2 + a_{6,4} \\
W_{111s} & y_2^2 + \bar{a}_{3,2}y_2 - \bar{a}_{6,4} = 0 \\
W_{112} & x_1\pi' = \pi, \quad y_2^2\pi' + a_1y_2 + a_{3,2}y_2\pi' = x_1^2 + a_{2,1}x_1 + a_{4,2} + a_{6,4}\pi' \\
W_{112s} & x_1\pi' = 0, \quad (y_2^2 + \bar{a}_{3,2}y_2 - \bar{a}_{6,4})\pi' = x_1(x_1 + \bar{a}_{2,1})
\end{array}$$

La fibra cerrada W_{112s} se descompone como $V(I_1) \cup V(I_2) \cup V(I_3)$, donde

$$I_1 = (\pi, x_1, \pi'), \quad I_2 = (\pi, \pi', x_1 + a_{2,1}) \quad I_3 = (\pi, x_1, y_2^2 + a_{3,2}y_2 - a_{6,4}).$$

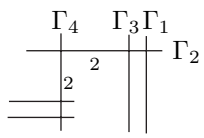
Las componentes irreducibles de $V(I_3)$ se contraen a puntos de Γ_4, pues si $\mathfrak{P}$ es un ideal primo de $D[x_1, y_2, \pi']$ que contiene a I_3, su antiimagen en $D[x_1, y_2]$ es un ideal primo que contiene a $J = (\pi, x_1, y_2^2 + a_{3,2}y_2 - a_{6,4})$, pero el espectro de $D[x_1, y_2]/J$ es finito (tiene a lo sumo dos puntos).

Puesto que $W_{111} \cap W_{112}$ es el abierto principal $D(\pi')$ en W_{112}, es claro que dicha intersección es precisamente $V(I_3) \cap D(\pi')$, es decir, $V(I_3)$ menos los puntos de corte con $V(I_1)$. Por otra parte, $V(I_1)$ y $V(I_2)$ son dos rectas isomorfas a A^1_k, luego, teniendo en cuenta lo que ya sabemos, podemos asegurar que son las antiimágenes de Γ_4 y Γ_3 respectivamente. (Es fácil ver que ésa es la correspondencia correcta y no la contraria.)



En resumen, la situación es la que indica la figura, en la que hemos pasado a llamar Γ_3 y Γ_4 a las rectas $V(I_2)$ y $V(I_1)$ de W_{112}, respectivamente. En particular, podemos afirmar que Γ_3 tiene multiplicidad 1 en W_{112} y Γ_4 tiene multiplicidad 2. Sin embargo, ahora los puntos de Γ_4 son regulares en W_{112}, ya que, si $\mathfrak{P}$ contiene a Γ_4, en $\mathcal{O}_{\mathfrak{P}}$ se cumple que

$$x_1 = \frac{y_2^2 + a_{1,2}x_1y_2 + a_{3,2}y_2 - a_{4,3}x_1 - a_{6,4}}{x_1 + a_{2,1}}\,\pi', \qquad \pi = x_1\pi'.$$



Teniendo en cuenta el análisis previo de la explosión de W_{12}, en total tenemos que la fibra cerrada es como indica la figura, y todos sus puntos son regulares salvo quizá los de W_{121}. Si el polinomio $T^2 + \bar{a}_{3,2}T - \bar{a}_{6,4}$ tiene dos raíces distintas en $\bar{k}$, entonces W_{111} está formado por dos rectas isomorfas a A^1_k o bien a una única recta simple isomorfa a $A^1_{k'}$, donde k' es una extensión cuadrática de k. (Al añadir los puntos de W_{111} tenemos P^1_k o $\mathrm{P}^1_{k'}$.) En particular, todos los puntos son suaves excepto los de la intersección con Γ_4, que ya hemos visto que son regulares. Por consiguiente, la explosión es regular y tenemos una fibra cerrada de tipo I^*_1 o $\mathrm{I}^*_{1,2}$.

Si, por el contrario, $T^2 + \bar{a}_{3,2}T - \bar{a}_{6,4} = (T - \bar{\alpha})^2$, entonces W_{112} consta de una única recta doble $\Gamma_5 \subset W_{111} \cup W_{112}$. La traslación $Y' = Y + \pi^2\alpha$ en la ecuación de Weierstrass original nos da ahora que $\pi^3 \mid a_3$, $\pi^5 \mid a_6$.

El razonamiento habitual nos muestra que Γ_5 puede tener a lo sumo un par de puntos singulares contenidos en W_{111}, por lo que, a la hora de calcular la explosión de Γ_5, basta considerar la de este abierto. En W_{111} la recta Γ_5 es (π, y_2), y las ecuaciones de la explosión son:

$$\begin{array}{ll}
W_{1111} & \pi y_3^2 + a_1x_2y_3 + a_{3,2}y_3 = \pi x_2^3 + a_{2,1}x_2^2 + a_{4,3}x_2 + a_{6,5} \\
W_{1111s} & \bar{a}_{2,1}x_2^2 + \bar{a}_{4,3}x_2 + \bar{a}_{6,5} = 0 \\
W_{1112} & (\pi x_2^3\pi' + a_{2,1}x_2^2\pi' + a_{4,3}x_2\pi' + a_{6,5}\pi' - a_1x_2 - a_{3,2})\pi' = \pi \\
W_{1112s} & (\bar{a}_{2,1}x_2^2 + \bar{a}_{4,3}x_2 + \bar{a}_{6,5})\pi'^2 = 0
\end{array}$$

Es inmediato comprobar que la recta doble (π, π') de W_{1112} se corresponde con Γ_5, pero que ahora todos sus puntos son regulares. La otra parte de la fibra cerrada consiste en una o dos rectas que se contraen a uno o dos puntos de Γ_5.

Si el polinomio $\bar{a}_{2,1}T^2 + \bar{a}_{4,3}T + \bar{a}_{6,5}$ tiene dos raíces distintas en $\bar{k}$, entonces tenemos una o dos nuevas componentes geométricamente regulares, luego todos sus puntos serán suaves en la explosión salvo los puntos de intersección con Γ_5, que, no obstante, ya sabemos que son regulares. En definitiva, hemos llegado a un modelo regular y la fibra cerrada es de tipo I^*_2 o $\mathrm{I}^*_{2,2}$.

La alternativa es que el polinomio tenga una raíz doble $\bar{a}_{2,1}(T - \bar{\alpha})^2$, en cuyo caso, la traslación $X = X + \alpha\pi^2$ en la ecuación de Weierstrass original nos da que $\pi^4 \mid a_4$, $\pi^6 \mid a_6$. Ahora sólo tenemos una componente nueva, Γ_6, con multiplicidad 2. El único punto de Γ_6 que no está en W_{1111} es su intersección con Γ_5, que ya sabemos que es regular, y en W_{1111} tenemos que $\Gamma_6 = (\pi, x_2)$ y

$$\pi = \frac{\pi x_2 + a_{2,1}x_2 + a_{4,3} - a_1y_3}{y_3^2 + a_{3,3}y_3 - a_{6,6}}\, x_2,$$

de donde se sigue que Γ_6 tiene a lo sumo dos puntos singulares y, por el razonamiento habitual, para calcular su explosión basta estudiar la de W_{1111}. Las

ecuaciones son:

W_{11111}	$y_3^2 + a_1x_3y_3 + a_{3,3}y_3 = \pi^2x_3^3 + a_2x_3^2 + a_{4,3}x_3 + a_{6,6}$	
W_{11111s}	$y_3^2 + \bar{a}_{3,3}y_3 - \bar{a}_{6,6} = 0$	
W_{11112}	$x_2\pi' = \pi$	$y_3^2\pi' + a_1y_3 + a_{3,3}y_3\pi' = \pi x_2^2 + a_{2,1}x_2 + a_{4,3} + a_{6,6}\pi'$
W_{11112s}	$x_2\pi' = 0$	$(y_3^2 + \bar{a}_{3,3}y_3 - a_{6,6})\pi' = \bar{a}_{2,1}x_2$

De la relación $\pi = x_2\pi'$ en W_{12112} deducimos que todos los puntos de la recta doble $\Gamma_6 = (\pi, x_2, \pi') = (\pi, \pi')$ son regulares en la superficie, por lo que podemos restringirnos a W_{12111}. Si el polinomio $T^2+\bar{a}_{3,3}T-\bar{a}_{6,6}$ tiene dos raíces distintas en $\bar{k}$, concluimos que la superficie es regular y que su fibra cerrada es de tipo I_3^* o $\mathrm{I}_{3,2}^*$.

Si, por el contrario, $T^2 + \bar{a}_{3,3}T - \bar{a}_{6,6} = (T - \bar{\alpha})^2$, el cambio de variables $Y = Y' + \pi^3\alpha$ nos da que $\pi^4 \mid a_3$, $\pi^7 \mid a_6$, con lo que tenemos una recta doble Γ_7 de ecuación $y_3 = 0$.

Ahora observamos que la ecuación de W_{11111} es idéntica a la de W_{111} salvo por los subíndices, por lo que al calcular la explosión de Γ_7 obtendremos ecuaciones análogas a las de W_{1111} y W_{1112}, y entramos así en un proceso cíclico que sólo se detiene si en algún momento llegamos a una superficie regular con fibra de tipo I_n^* o $\mathrm{I}_{\mathrm{n},2}^*$.

El proceso ha de detenerse tras un número finito de pasos, pues cada dos pasos $v(a_3)$ y $v(a_4)$ aumenta en una unidad y $v(a_6)$ aumenta en dos unidades, lo que implica que $v(b_4)$ aumenta en una unidad, $v(b_6)$ y $v(b_8)$ aumentan en dos unidades y $v(\Delta)$ aumenta en dos unidades, pero todos los cambios de variables dejan invariante a Δ, luego el proceso ha de terminar en un máximo de $v(\Delta)-6$ pasos (porque al inicio del paso 7 podemos asegurar que $v(\Delta) \geq 6$).

Si $\operatorname{car} k \neq 2$, podemos refinar los cálculos y asegurar que $n = v(\Delta) - 6$. En efecto, vamos a calcular $v(\Delta)$ a partir de los datos que tenemos cuando alcanzamos una fibra de tipo I_n^* y vamos a ver que es precisamente $v(\Delta) = n+6$.

A lo largo de todo el proceso tenemos que $v(a_1) \geq 1$ y $v(a_2) = 1$, lo que nos da $v(b_2) = 1$. En cuanto a las demás constantes, varían como indica la tabla siguiente (que contiene cotas inferiores de la valoración en cada una de ellas):

n	a_3	a_4	a_6	b_4	b_6	b_8	Δ
1	2	3	4	3	4	5	7
2	3	3	5	3	5	6	8
3	3	4	6	4	6	7	9
4	4	4	7	4	7	8	10

Del algoritmo se desprende que empezamos con $v(a_3) \geq 2$ y que la cota aumenta una unidad al pasar de n impar a n par, mientras que $v(a_4) \geq 3$ y la cota aumenta una unidad al pasar de n par a n impar. Por su parte $v(a_6) \geq 4$ la cota aumenta una unidad en cada paso, luego $v(a_6) \geq n + 3$.

A partir de aquí podemos razonar inductivamente lo que le sucede a las demás constantes en cada paso. Por ejemplo, como $b_4 = 2a_4 + a_1a_3$, se sigue inmediatamente que empieza con $v(b_4) \geq 3$ y que la cota aumenta una unidad cada dos pasos. También es fácil ver que $v(b_6) \geq 4$ y que la cota aumenta una unidad en cada paso, por lo que $v(b_6) \geq n + 3$.

El punto más delicado es el análisis de b_8. Antes de entrar en él observemos que, según el algoritmo, alcanzamos la fibra de tipo I_1^* cuando el polinomio $T^2 + \bar{a}_{3,2}T - \bar{a}_{6,4}$ tiene raíces distintas en $\bar{k}$, es decir, cuando $\pi \nmid a_{3,2}^2 + 4a_{6,4}$ o, equivalentemente, cuando $v(a_3^2 + 4a_6) = 4$. La condición es análoga para todo n impar aumentando una unidad cada vez el segundo subíndice de $a_{3,2}$ y dos unidades el de $a_{6,4}$. En definitiva, se alcanza la fibra I_n^* con n impar si y sólo si

$$v(a_3^2 + 4a_6) = n + 3.$$

La condición para $n = 2$ es que el polinomio $\bar{a}_{2,1}T^2 + \bar{a}_{4,3}T + \bar{a}_{6,5}$ tenga discriminante no nulo, es decir, $v(a_4^2 - 4a_2a_6) = 6$, y este valor se incrementa dos unidades cada dos pasos, luego la condición general para n par es que

$$v(a_4^2 - 4a_2a_6) = n + 4.$$

Ahora observamos que

$$b_8 = a_1^2a_6 - a_1a_3a_4 - a_4^2 + a_2(a_3^2 + 4a_6) = a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 - (a_4^2 - 4a_2a_6).$$

Se comprueba fácilmente que, para n impar, todos los sumandos de la primera expresión tienen valor $\geq n + 5$, mientras que el último tiene valor exactamente $n + 4$, por lo que $v(b_8) = n + 4$. Si n es par llegamos a la misma conclusión con la segunda expresión. Así pues, cuando alcanzamos la fibra de tipo I_n^* (o $\mathrm{I}_{\mathrm{n},2}^*$) se cumple que $v(b_8) = n + 4$.

A su vez, se comprueba fácilmente que todos los sumandos de

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

tienen valor $\geq n + 7$ excepto el primero, que cumple $v(b_2^2b_8) = n + 6$, por lo que $v(\Delta) = n + 6$.

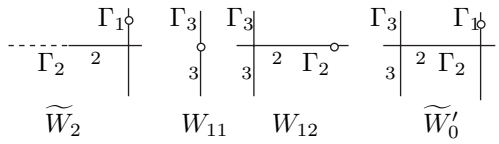
9.6 Los pasos finales

Paso 8 Las hipótesis acumuladas hasta aquí son:

$$\pi \mid a_1, \quad \pi^2 \mid a_2, a_3, \quad \pi^3 \mid a_4, \quad \pi^4 \mid a_6,$$

de modo que ahora $P(T) = T^3$. Volvemos a la situación del final de la sección 9.4, de modo que tenemos la superficie $\widetilde{W}'$, determinada por los abiertos W_{11} y W_{12}. Ahora la fibra cerrada consta ahora de una recta simple Γ_1, una recta doble Γ_2 y una recta triple Γ_3, dada por $x_1 = 0$. Los razonamientos iniciales del paso 7 siguen siendo válidos en este caso (teniendo en cuenta que ahora no existe la componente simple que allí llamábamos Γ_3, sino que la Γ_3

del paso actual se corresponde con la Γ_4 del paso 7). Así, resulta que la fibra cerrada puede contener a lo sumo un par de puntos singulares, a saber, los del cerrado $V(\pi, x_1, y_2^2 + a_{3,2}y_2 - a_{6,4}) \subset W_{11}$.



Vamos a calcular la explosión de centro el ideal $I = (\pi, x_1, y_2^2 + a_{3,2}y_2 - a_{6,4})$. Podemos trabajar únicamente con el abierto W_{11}. Por simplificar la notación, llamaremos $t = y_2^2 + a_{3,2}y_2 - a_{6,4}$. La explosión $\widetilde{W}_{11}$ es unión de tres abiertos afines, W_{111}, W_{112} y W_{113}. El primero es el espectro de $D[x_1, y_2, \pi/t, x_1/t] = D[y_2, \pi', x_1']$. Para calcular las ecuaciones de sus generadores partimos de la ecuación de W_{11}:

$$\pi t = x_1^3 + a_{21}x_1^2 + \pi a_{4,3}x_1 - \pi a_{1,1}x_1y_2,$$

sustituimos $\pi = \pi' t$, $x_1 = x_1' t$:

$$\pi' t^2 = x_1'^3 t^3 + a_{21}x_1'^2 t^2 + a_{4,3}x_1'\pi' t^2 - a_{1,1}x_1' y_2 \pi' t^2,$$

y dividimos entre t^2:

$$\pi' t = \pi, \quad \pi' = x_1'^3 t + a_{21}x_1'^2 + a_{4,3}x_1'\pi' - a_{1,1}x_1' y_2 \pi'.$$

Similarmente, W_{112} es el espectro de $D[x_1, y_2, \pi/x_1, t/x_1] = D[x_1, y_2, \pi'', z]$. Sustituimos $\pi = x_1\pi''$, $t = x_1 z$ en la ecuación de W_{11} y dividimos entre x_1^2:

$$x_1\pi'' = \pi, \quad x_1 z = t, \quad \pi'' z = x_1 + a_{21} + a_{4,3}\pi'' - a_{1,1}y_2\pi''.$$

De la última ecuación podemos despejar x_1, con lo que nos queda

$$(\pi'' z - a_{21} - a_{4,3}\pi'' + a_{1,1}y_2\pi'')\pi'' = \pi,$$
$$(\pi'' z - a_{21} - a_{4,3}\pi'' + a_{1,1}y_2\pi'')z = t.$$

Finalmente, W_{113} es el espectro de $D[y_2, x_1/\pi, t/\pi] = D[x_2, y_2, z']$, con las relaciones

$$z'\pi = t, \quad z' = \pi x_2^3 + a_{21}x_2^2 + a_{4,3}x_2 - a_{1,1}x_2y_2,$$

que se reducen a

$$\pi(\pi x_2^3 + a_{21}x_2^2 + a_{4,3}x_2 - a_{1,1}x_2y_2) = t.$$

En resumen:

W_{111}	$\pi' t = \pi, \quad \pi' = x_1'^3 t + a_{21}x_1'^2 + a_{4,3}x_1'\pi' - a_{1,1}x_1' y_2\pi'$
W_{111s}	$\pi' t = 0, \quad \pi'(1 - \bar{a}_{4,3}x_1' + \bar{a}_{1,1}x_1' y_2) = x_1'^3 t$
W_{112}	$(\pi'' z - a_{21} - a_{4,3}\pi'' + a_{1,1}y_2\pi'')\pi'' = \pi,$ $(\pi'' z - a_{21} - a_{4,3}\pi'' + a_{1,1}y_2\pi'')z = t$
W_{112s}	$t = 0, \quad (z - a_{4,3} + a_{1,1}y_2)\pi''^2 = 0$
W_{113}	$\pi(\pi x_2^3 + a_{21}x_2^2 + a_{4,3}x_2 - a_{1,1}x_2y_2) = t$
W_{113s}	$t = 0$

Analicemos ahora la fibra cerrada. Todo ideal de $\mathcal{O}(W_{111})$ que contenga a π contiene a uno de los ideales

$$I_{11} = (\pi, x_1', \pi'), \quad I_{12} = (\pi, \pi', t), \quad I_{13} = (\pi, t, 1 - a_{4,3}x_1' + a_{1,1}x_1'y_2).$$

Similarmente, en W_{112} tenemos

$$I_{21} = (\pi, \pi'', t), \quad I_{22} = (\pi, t, z - a_{4,3} + a_{1,1}y_2),$$

y en W_{113} únicamente, $I_{31} = (\pi, t)$.

Notemos que los ideales que contienen a t son primos si y sólo si el polinomio $T^2 + \bar{a}_{3,2}T - \bar{a}_{6,4}$ no tiene raíces en k, mientras que, en caso contrario, si

$$T^2 + \bar{a}_{3,2}T - \bar{a}_{6,4} = (T - \bar{\alpha}_1)(T - \bar{\alpha}_2),$$

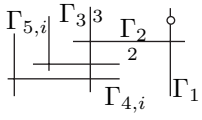
cada uno de ellos determina dos componentes irreducibles disjuntas, las resultantes de sustituir t por $t_1 = y_2 - \alpha_1$ o $t_2 = y_2 - \alpha_2$.

También es claro que las componentes irreducibles correspondientes a estos ideales se contraen a puntos de $\Gamma_3 \subset W_{11}$, por lo que la antiimagen de Γ_3 en la explosión ha de ser el único ideal que no contiene a t, a saber, $I_{1,1}$. Así pues, llamaremos también Γ_3 a la componente irreducible asociada al ideal $I_{1,1}$. Sabemos, pues, que tiene multiplicidad 3 en la explosión.

El ideal I_{12} determina una o dos rectas disjuntas que cortan a Γ_3 en un punto cada una. Las llamaremos $\Gamma_{4,1}$ y (si existe) $\Gamma_{4,2}$. Con el ideal I_{13} hemos de tener una precaución: si $\bar{a}_{4,3} = \bar{a}_{1,1} = 0$, entonces no existe tal ideal, ya que cumpliría $1 \in I_{13}$. Esto no es significativo, porque las componentes irreducibles asociadas a I_{13} son las mismas que las asociadas a I_{22} (como se ve al aplicar el cambio de coordenadas $z = 1/x_1'$). Sucede que $W_{111} \cap W_{112} = D(z)$ en W_{112}, y si $\bar{a}_{4,3} = \bar{a}_{1,1} = 0$ entonces las componentes irreducibles asociadas a I_{22} están contenidas en $V(z)$, por lo que no aparecen en W_{111}.

Llamemos $\Gamma_{5,1}$ y (si existe) $\Gamma_{5,2}$ a las componentes irreducibles asociadas a I_{22} y (tal vez) a I_{13}. Notemos que $W_{111} \cap W_{112} = D(x_1)$ en W_{111}, de donde se sigue que $\Gamma_{5,i} \cap W_{111} \subset W_{112}$, por lo que podemos prescindir en todo momento del ideal I_{13}. En particular, $\Gamma_{5,i} \cap \Gamma_3 = \varnothing$.

Por último, es fácil ver que las componentes irreducibles asociadas a I_{31} son de nuevo las componentes $\Gamma_{5,i}$. Su expresión en W_{113} muestra claramente que tienen multiplicidad 1.



En total, vemos que la estructura de la fibra cerrada de la explosión es la que indica la figura, donde hemos representado el caso en que existen los dos pares de componentes. Vemos que corresponden a los tipos IV* o IV$_2^*$, aunque nos falta comprobar que la superficie es regular y que las componentes $\Gamma_{4,i}$ tienen multiplicidad 2.

Lo segundo es inmediato a partir de la expresión de W_{112}. Si, por ejemplo, existe una única componente irreducible, entonces la fibra cerrada es isomorfa al espectro de

$$k'[Y, Z]/((Z - \bar{a}_{4,3} + \bar{a}_{1,1}\bar{y}_2)Y^2),$$

donde $k' = k[T]/(T^2 + \bar{a}_{3,2}T - \bar{a}_{6,4})$ e $\bar{y}_2 = \bar{T}$. La componente $\Gamma_{4,1}$ se corresponde con $V(Y)$, que obviamente tiene multiplicidad 2. Si hay dos componentes irreducibles, lo mismo es válido cambiando k' por k y tomando $\bar{y}_2 = \bar{\alpha}_i$.

Los puntos de Γ_3 son todos regulares porque $I_{11} = (x_1')$. Si $\mathfrak{P}$ es un ideal primo de $\mathcal{O}(W_{111})$ que contiene a I_2, o bien contiene a x_1', en cuyo caso está en Γ_3 y ya sabemos que es regular, o en $\mathcal{O}_{W_{111},\mathfrak{P}}$ se cumple que

$$t = \frac{1 - a_{22}x_1'^2 t - a_{4,3}x_1' + a_{1,1}x_1'y_2}{x_1'^3}\,\pi', \quad \pi = t\pi',$$

lo que implica la regularidad de $\mathfrak{P}$. En particular, tenemos la regularidad de todos los puntos de $\Gamma_{4,i}$ salvo quizá los que estén en W_{112} y no en W_{111}. Ahora bien, es fácil ver que $I_{21} = (\pi'')$, lo que implica la regularidad de estos puntos.

En cuanto a $\Gamma_{5,i}$, los puntos de estas componentes que están en W_{113} son claramente regulares, pues $I_{31} = (\pi)$ y, como $W_{112} \cap W_{113} = D(\pi'')$ en W_{112}, los únicos puntos de $\Gamma_{5,i}$ que nos falta analizar están en $\Gamma_{5,i} \cap \Gamma_{4,i}$, y ya sabemos que son regulares.

Paso 9 Si $T^2 + \bar{a}_{3,2}T - \bar{a}_{6,4} = (T - \bar{\alpha})^2$, el cambio de variables $Y = Y' + \pi^2\alpha$ hace que $\pi^3 \mid a_3$ y $\pi^5 \mid a_6$. Estamos en la misma situación que al principio del paso anterior, salvo que ahora la componente Γ_3 sólo puede tener un punto singular, a saber, $\mathfrak{m} = (\pi, x_1, y_2)$. Vamos a calcular la explosión de W_{11} con centro $\mathfrak{m}$. La podemos expresar como unión de tres abiertos afines que se obtienen, respectivamente, con los cambios de variables

$$\pi = y_2\pi',\ x_1 = x_1'y_2, \qquad \pi = x_1\pi'',\ y_2 = x_1y_2', \qquad x_1 = \pi x_2,\ y_2 = \pi y_3.$$

Las ecuaciones son:

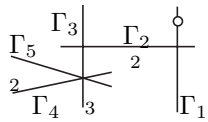
W_{111}	$\pi + a_1x_1' + a_{3,2}\pi' = y_2x_1'^3 + a_{2,1}x_1'^2 + a_{4,3}x_1'\pi' + a_{6,5}\pi'^2,$
	$y_2\pi' = \pi$
W_{111s}	$y_2\pi' = 0, \quad y_2x_1'^3 + (\bar{a}_{4,3}x_1' + \bar{a}_{6,5}\pi')\pi' = 0$
W_{112}	$(\pi y_2'^2 + a_1y_2' + a_{3,2}y_2'\pi'' - a_{2,1} - a_{4,3}\pi'' - a_{6,5}\pi''^2)\pi'' = \pi$
W_{112s}	$(\bar{a}_{4,3} + \bar{a}_{6,5}\pi'')\pi''^2 = 0$
W_{113}	$\pi y_3^2 + a_1x_2y_3 + a_{3,2}y_3 = \pi x_2^3 + a_{2,1}x_2^2 + a_{4,3}x_2 + a_{6,5}$
W_{113s}	$\bar{a}_{4,3}x_2 + \bar{a}_{6,5} = 0$

En W_{111s} encontramos tres componentes irreducibles, asociadas a los ideales primos

$$I_{11} = (\pi, x_1', \pi'), \quad I_{12} = (\pi, y_2, \pi'), \quad I_{13} = (\pi, y_2, a_{4,3}x_1' + a_{6,5}\pi').$$

En W_{112s} encontramos dos componentes irreducibles, asociadas a los ideales $I_{21} = (\pi, \pi'')$, $I_{22} = (\pi, a_{4,3} + a_{6,5}\pi'')$, y es fácil ver que se corresponden respectivamente con las asociadas a I_{12} e I_{13}. Por último, W_{113s} es una recta que se corresponde con las componentes asociadas a I_{13} e I_{22}.

En definitiva, la fibra cerrada de la explosión tiene tres componentes irreducibles, y todas ellas tienen una parte en W_{111s}. Los ideales que contienen a y_2 se contraen claramente a puntos de W_{11}, luego la componente Γ_3 de W_{11} ha de corresponderse en la explosión con la componente determinada por I_{11}. Como de costumbre, la llamaremos también Γ_3, y pasamos a llamar Γ_4 y Γ_5 a las componentes asociadas a I_{12} e I_{13}, respectivamente.



Notemos que la hipótesis local $\pi^4 \nmid a_4$ nos asegura que Γ_3 no coincide con Γ_4. Es claro que las tres componentes se cortan en el punto $\mathfrak{p} = (\pi, x_1', y_2, \pi')$. Las ecuaciones de W_{112s} muestran que Γ_4 tiene multiplicidad 2 y Γ_5 tiene multiplicidad 1 (y sabemos que Γ_3 ha de tener multiplicidad 3). La situación es, pues, la que muestra la figura.

Veamos ahora que todos los puntos son regulares excepto a lo sumo $\mathfrak{p}$. Como todos los puntos de W_{11} son regulares excepto $\mathfrak{m}$ y la explosión es un isomorfismo fuera de la fibra de $\mathfrak{m}$, tenemos que los únicos puntos que pueden ser singulares son los de Γ_4 o Γ_5. Los de Γ_5 son suaves excepto $\mathfrak{p}$, y las ecuaciones de W_{112} muestran que $I_{12} = (\pi'')$, luego todos los puntos de $\Gamma_4 \cap W_{112}$ son regulares, y el único punto que excluimos así es precisamente $\mathfrak{p}$.

Por consiguiente, ahora hemos de calcular la explosión de W_{111} con centro en el punto $\mathfrak{p} = (x_1', y_2, \pi')$.

En primer lugar hacemos los cambios $y_2 = x_1' y_2'$, $\pi' = x_1' \pi''$, sustituyendo previamente $\pi = y_2 \pi'$ en la segunda ecuación de W_{111} (y dividimos entre $x_1'^2$):

$$x_1'^2 y_2' \pi'' = \pi, \quad y_2' \pi'' + a_{1,1} x_1' y_2' \pi'' + a_{3,3} x_1' y_2' \pi''^2 = x_1'^2 y_2' + a_{2,1} + a_{4,3} \pi'' + a_{6,5} \pi''^2.$$

Los otros cambios de variables son

$$x_1' = x_1'' y_2, \ \pi' = y_2 \pi'' \quad \text{y} \quad x_1' = x_1''' \pi', \ y_2 = y_2'' \pi'.$$

En total, llegamos a las ecuaciones:

$$\begin{array}{ll}
W_{1111} & y_2' \pi'' + a_{1,1} x_1' y_2' \pi'' + a_{3,3} x_1' y_2' \pi''^2 = x_1'^2 y_2' + a_{2,1} + a_{4,3} \pi'' + a_{6,5} \pi''^2, \\
& x_1'^2 y_2' \pi'' = \pi \\
W_{1111s} & y_2' \pi'' + \bar{a}_{1,1} x_1' y_2' \pi'' + \bar{a}_{3,3} x_1' y_2' \pi''^2 = x_1'^2 y_2' + \bar{a}_{4,3} \pi'' + \bar{a}_{6,5} \pi''^2, \\
& x_1'^2 y_2' \pi'' = 0 \\
W_{1112} & \pi'' + a_{1,1} x_1'' y_2 \pi'' + a_{3,3} y_2 \pi''^2 = y_2^2 x_1''^3 + a_{2,1} x_1''^2 + a_{4,3} x_1'' \pi'' + a_{6,5} \pi''^2, \\
& y_2^2 \pi'' = \pi \\
W_{1112s} & \pi'' + \bar{a}_{1,1} x_1'' y_2 \pi'' + \bar{a}_{3,3} y_2 \pi''^2 = y_2^2 x_1''^3 + \bar{a}_{4,3} x_1'' \pi'' + \bar{a}_{6,5} \pi''^2, \\
& y_2^2 \pi'' = 0 \\
W_{1113} & y_2'' + a_{1,1} x_1''' y_2'' \pi' + a_{3,3} y_2'' \pi' = y_2'' x_1'''^3 \pi'^2 + a_{2,1} x_1'''^2 + a_{4,3} x_1''' + a_{6,5}, \\
& y_2'' \pi'^2 = \pi \\
W_{1113s} & y_2'' + \bar{a}_{1,1} x_1''' y_2'' \pi' + \bar{a}_{3,3} y_2'' \pi' = y_2'' x_1'''^3 \pi'^2 + \bar{a}_{4,3} x_1''' + \bar{a}_{6,5}, \\
& y_2'' \pi'^2 = 0
\end{array}$$

Las componentes irreducibles de las fibras cerradas son las asociadas a los ideales primos:

$$I_{11} = (\pi, x_1', \pi''), \quad I_{12} = (\pi, y_2', \pi''),$$

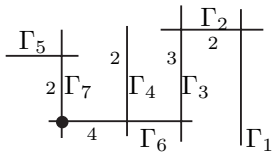
$$I_{13} = (\pi, y_2', a_{4,3} + a_{6,5}\pi''), \quad I_{14} = (\pi, x_1', y_2' - a_{4,3} - a_{6,5}\pi''),$$

$$I_{21} = (\pi, x_1'', \pi''), \quad I_{22} = (\pi, y_2, \pi''), \quad I_{23} = (\pi, y_2, 1 - a_{4,3}x_1'' - a_{6,5}\pi''),$$

$$I_{31} = (\pi, y_2'', a_{4,3}x_1''' + a_{6,5}), \quad I_{32} = (\pi, \pi', y_2'' - a_{4,3}x_1''' - a_{6,5}).$$

Considerando los cambios de coordenadas entre los distintos abiertos se comprueba sin dificultad que las parejas de ideales (I_{31}, I_{13}), (I_{32}, I_{14}), (I_{22}, I_{11}), (I_{23}, I_{14}) determinan la misma componente irreducible, lo que nos reduce el número de componentes hasta 5 (a las que hay que sumar Γ_1 y Γ_2, que no están en W_{111}, por lo que no aparecerán aquí). También es fácil ver que las componentes asociadas a I_{11} e I_{14} se contraen a $\mathfrak{p}$ (porque contienen a x_1', luego también a x_1', y_2, π'). Esto nos deja únicamente a I_{12}, I_{13} e I_{21} como posibles antiimágenes de Γ_3, Γ_4 y Γ_5. Es fácil ver que, concretamente, la correspondencia es

$$I_{21} \mapsto \Gamma_3, \quad I_{12} \mapsto \Gamma_4, \quad I_{13} \mapsto \Gamma_5.$$



Llamaremos Γ_6 a la componente asociada a I_{11} o I_{22} y Γ_7 a la asociada a I_{14} o I_{23}. Analizando las uniones de los ideales se ve fácilmente que la disposición de las componentes es la que indica la figura. Falta comprobar que las multiplicidades de Γ_6 y Γ_7 son las que se indican (4 y 2, respectivamente). De las ecuaciones de W_{1112} se sigue que

$$\pi''(1 + a_{1,1}x_1''y_2 + a_{3,3}y_2\pi'' - a_{2,2}x_1''^2y_2^2 - a_{4,3}x_1'' - a_{6,5}\pi'') = y_2^2x_1''^3,$$

y la expresión entre paréntesis no está en I_{22} (porque módulo I_{22} es $1 - \bar{a}_{43}x_1''$ y $D[x_1'', y_2, \pi'']/I_{22} \cong k[x_1'']$, con x_1'' trascendente sobre k). Por consiguiente, en $\mathcal{O}_{\Gamma_6}$, se cumple que $I_{22} = (y_2)$, luego $v_{\Gamma_6}(y_2) = 1$ y $v_{\Gamma_6}(\pi'') = 2$, lo que a su vez implica que $v_{\Gamma_6}(\pi) = v_{\Gamma_6}(y_2^2\pi'') = 4$, y esto es la multiplicidad de Γ_6.

Para Γ_7 tenemos que

$$\pi''(1 - a_{4,3}x_1'' - a_{6,5}\pi'') = y_2^2x_1''^3 + a_{2,1}x_1''^2 - a_{1,1}x_1''y_2\pi'' - a_{3,3}y_2\pi''^2,$$

donde el miembro derecho está en I_{23} y $\pi'' \notin I_{23}$ (pues en caso contrario el ideal sería maximal). Esto implica que $v_{\Gamma_7}(y_2) = 1$, con lo que la multiplicidad es $v_{\Gamma_7}(\pi) = v_{\Gamma_7}(y_2^2\pi'') = 2$.

Por último, vamos a comprobar que todos los puntos son regulares salvo quizá el punto de intersección de Γ_6 y Γ_7. (Como la explosión es un isomorfismo fuera de la fibra de $\mathfrak{p}$, sabemos que un punto singular ha de estar necesariamente en $\Gamma_6 \cup \Gamma_7$.) La ecuación precedente lo prueba para los puntos de W_{1112}. (Un ideal maximal que contenga a I_{22} o I_{23} tendrá, en principio, cuatro generadores, de entre los que podemos eliminar a π y también a π'' o $1 - a_{4,3}x_1'' - a_{6,5}\pi''$

siempre y cuando no estén los dos en el ideal.) En W_{1111} podemos razonar igual con

$$\pi''(y_2' - a_{4,3} - a_{6,5}\pi'') = x_1'^2 y_2' + a_{2,1} - a_{1,1}x_1'y_2'\pi'' - a_{3,3}x_1'y_2'^2\pi''^2.$$

Con esto tenemos cubiertas ambas componentes (sin necesidad de considerar W_{1113}).

Esto nos lleva a calcular la explosión del punto singular. Podemos considerar únicamente el abierto W_{1112}, en el cual el punto es $\mathfrak{q} = (y_2, \pi'', 1 - a_{4,3}x_1'')$. La sustitución

$$\pi'' = y_2\pi''', \quad 1 - a_{4,3}x_1'' = y_2 z$$

nos da las ecuaciones

$$z\pi''' + a_{1,1}x_1''\pi''' + a_{3,3}y_2\pi'''^2 = x_1''^3 + a_{2,2}x_1''^2 y_2\pi''' + a_{6,5}\pi'''^2,$$

$$y_2^3\pi''' = \pi, \quad 1 - a_{4,3}x_1'' = y_2 z.$$

Es fácil ver que la fibra cerrada tiene dos componentes irreducibles, asociadas a los ideales

$$I_{11} = (\pi, \pi''', x_1'', y_2 z - 1), \quad I_{12} = (\pi, y_2, 1 - a_{4,3}x_1'').$$

La primera es Γ_3, mientras que la segunda se contrae a $\mathfrak{q}$, luego es nueva, y la llamaremos Γ_8. Observemos que $I_{12} = (y_2)$, mientras que $\pi''' \notin I_{12}$, de donde se sigue que la multiplicidad de Γ_8 es $v_{\Gamma_8}(\pi) = 3$.

La sustitución

$$y_2 = y_2'\pi'', \ 1 - a_{4,3}x_1'' = z'\pi''$$

nos da las ecuaciones

$$\pi''(y_2'^2 x_1''^3 + a_{2,2}x_1''^2 y_2'^2\pi'' + a_{6,5} - a_{1,1}x_1''y_2' - a_{3,3}y_2'\pi'') = 1 - a_{4,3}x_1'',$$

$$y_2'^2\pi''^3 = \pi.$$

También tenemos dos ideales:

$$I_{21} = (\pi, y_2', 1 - a_{4,3}x_1'' - a_{6,5}\pi''), \quad I_{22} = (\pi, \pi'', 1 - a_{4,3}x_1'').$$

Es claro que el primero se corresponde con Γ_7, mientras que el segundo es otra vez Γ_8. Por último, la sustitución

$$y_2 = (1 - a_{4,3}x_1'')y_2'', \quad \pi'' = (1 - a_{4,3}x_1'')\tilde{\pi}$$

nos da las ecuaciones

$$\tilde{\pi} + a_{1,1}x_1''y_2''\tilde{\pi} + a_{3,3}y_2''\tilde{\pi}^2(1 - a_{4,3}x_1'')$$

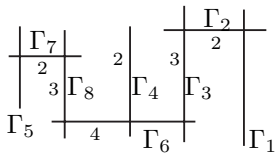
$$= x_1''^3 y_2''^2 + a_{2,2}x_1''^2 y_2''^2\tilde{\pi}(1 - a_{4,3}x_1'') + a_{6,5}\tilde{\pi}^2,$$

$$y_2''^2\tilde{\pi}(1 - a_{4,3}x_1'')^3 = \pi.$$

Tenemos cuatro ideales:

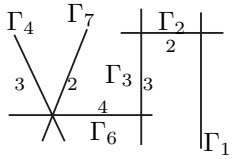
$$I_{31} = (\pi, y_2'', \tilde{\pi}), \quad I_{32} = (\pi, \tilde{\pi}, x_1''),$$
$$I_{33} = (\pi, 1 - a_{4,3}x_1''), \quad I_{34} = (\pi, y_2'', 1 - a_{6,5}\tilde{\pi}),$$

que corresponden a Γ_6, Γ_3, Γ_8 y Γ_7, respectivamente. (Notemos que si $\pi \mid a_{6,5}$ entonces Γ_7 no corta a este último abierto de la explosión.) Es fácil ver que su disposición es la que indica la figura.



Vemos que corresponde al tipo III*. Sólo hemos de probar que la superficie a la que hemos llegado es regular. Sólo podría tener singularidades sobre la componente Γ_8, y es inmediato que no los hay, ya que $I_{12} = (y_2)$, $I_{22} = (\pi'')$, $I_{33} = (1 - a_{4,3}x_1'')$.

Paso 10 Estamos como al principio del paso 9: ya tenemos calculada la explosión de W_{11} con centro en el punto $\mathfrak{m}$. La única diferencia es que ahora la fibra cerrada es algo más simple. En primer lugar, observamos que la fibra cerrada de W_{113} es vacía, por lo que podemos olvidarnos de este abierto. Por otra parte, tenemos que $I_{12} = I_{13}$, $I_{21} = I_{22}$, por lo que sólo tenemos dos componentes irreducibles: Γ_3 y Γ_4, ésta con multiplicidad 3 (como se deduce inmediatamente de la fibra cerrada de W_{112}). Sigue siendo cierto que $\mathfrak{p}$ es el único posible punto singular y, al calcular la explosión de W_{111} con centro $\mathfrak{p}$, obtenemos las mismas ecuaciones que en el paso anterior, salvo que las fibras cerradas son también ligeramente más simples, porque desaparece $\bar{a}_{4,3}$.



Al revisar los ideales de las componentes irreducibles observamos que I_{31} es trivial, así como que $I_{12} = I_{13}$. Los cálculos de las multiplicidades de Γ_6 y Γ_7 siguen siendo válidos, y ahora la configuración es la que indica la figura. El punto $\mathfrak{q}$ sigue siendo el único punto singular, sólo que ahora aparece únicamente en el abierto W_{1111}, donde es $\mathfrak{q} = (x_1', y_2', \pi'')$. Las sustituciones

$$x_1' = x_1''y_2', \ \pi'' = y_2'\pi''', \qquad y_2' = x_1'y_2'', \ \pi'' = x_1'\tilde{\pi}, \qquad x_1' = x_1'''\pi'', \ y_2' = y_2'''\pi'',$$

dan lugar a las ecuaciones siguientes:

$$\begin{array}{ll}
W_{11111} & \pi''' + a_{1,1}x_1''y_2'\pi''' + a_{3,3}x_1''y_2'^2\pi'''^2 \\
& = x_1''^2y_2' + a_{2,2}x_1''^2y_2'^2\pi''' + a_{4,4}x_1''^2y_2'^3\pi'''^2 + a_{6,5}\pi'''^2, \\
& x_1''^2y_2'^4\pi''' = \pi \\
W_{11112} & y_2''\tilde{\pi} + a_{1,1}x_1'y_2''\tilde{\pi} + a_{3,3}x_1'^2y_2''\tilde{\pi}^2 \\
& = x_1'y_2'' + a_{2,2}x_1'^2y_2''\tilde{\pi} + a_{4,4}x_1'^3y_2''\tilde{\pi}^2 + a_{6,5}\tilde{\pi}^2, \\
& x_1'^4y_2''\tilde{\pi} = \pi \\
W_{11113} & y_2''' + a_{1,1}x_1'''y_2'''\pi'' + a_{3,3}x_1'''y_2'''\pi''^2 \\
& = x_1'''^2y_2'''\pi'' + a_{2,2}x_1'''^2y_2'''\pi''^2 + a_{4,4}x_1'''^2y_2'''\pi''^3 + a_{6,5}, \\
& x_1'''^2y_2'''\pi''^4 = \pi
\end{array}$$

Dejamos que el lector compruebe que la estructura de la fibra cerrada de cada abierto es la siguiente: En W_{11111s} tenemos

$$\Gamma_6 = (\pi, x_1'', \pi'''), \quad \Gamma_7 = (\pi, x_1'', 1 - a_{6,5}\pi'''),$$

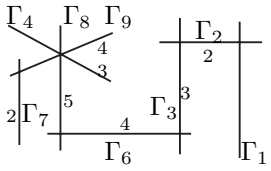
$$\Gamma_8 = (\pi, y_2', \pi'''), \quad \Gamma_9 = (\pi, y_2', 1 - a_{6,5}\pi'''),$$

en W_{11112s} tenemos

$$\Gamma_4 = (\pi, y_2'', \tilde{\pi}), \quad \Gamma_8 = (\pi, x_1', \tilde{\pi}), \quad \Gamma_9 = (\pi, x_1', y_2'' - a_{6,5}\tilde{\pi}),$$

y en W_{11113s}

$$\Gamma_7 = (\pi, x_1''', y_2''' - a_{6,5}), \quad \Gamma_9 = (\pi, \pi'', y_2''' - a_{6,5}).$$



La disposición de las componentes irreducibles es la que indica la figura. Falta comprobar que las multiplicidades de Γ_8 y Γ_9 son las indicadas. Para ello consideramos la ecuación de W_{11111} en la forma siguiente, y observamos que la expresión entre paréntesis no está en $\Gamma_8 = (\pi, y_2', \pi''')$, al igual que x_1''.

$$\pi'''(1 + a_{1,1}x_1''y_2' + a_{3,3}x_1''y_2'^2\pi''' - a_{2,2}x_1''^2y_2'^2 - a_{4,4}x_1''^2y_2'^3\pi''' - a_{6,5}\pi''') = x_1''^2y_2'$$

Concluimos que $\Gamma_8 = (y_2') = (\pi''')$, luego la multiplicidad de Γ_8 es

$$v_{\Gamma_8}(\pi) = v_{\Gamma_8}(x_1''^2y_2'^4\pi''') = 5.$$

De paso hemos probado que todos los puntos de $\Gamma_8 \cap W_{11111}$ son regulares, lo cual excluye únicamente al punto donde Γ_8 corta a Γ_4 y Γ_9, que en W_{11112} es $\mathfrak{r} = (x_1', y_2'', \tilde{\pi})$. En cuanto a Γ_9 observamos que

$$1 - a_{6,5}\pi''' = \frac{(x_1'' + a_{2,2}x_1''y_2'\pi''' + a_{4,4}x_1''y_2'^2\pi'''^2 - a_{1,1}\pi''' - a_{3,3}y_2'\pi'''^2)x_1''y_2'}{\pi'''},$$

lo cual prueba que $\Gamma_9 = (y_2')$, con lo que su multiplicidad es

$$v_{\Gamma_9}(\pi) = v_{\Gamma_9}(x_1''^2y_2'^4\pi''') = 4,$$

y además vemos que todos los puntos de $\Gamma_9 \cap W_{11111}$ son regulares, luego la única singularidad de la superficie es a lo sumo $\mathfrak{r}$. Dejamos a cargo del lector la comprobación de que en la explosión de W_{11112} con centro $\mathfrak{r}$ aparece una última componente Γ_{10} de multiplicidad 6 que nos da finalmente un modelo regular con fibra cerrada de tipo II*. ∎

Con esto termina la prueba del algoritmo, pues del paso 11 no hay nada que probar.

9.7 El caso car $k > 3$

Cuando la característica del cuerpo de restos k (y, por consiguiente, la de K) es distinta de 2 o 3, el algoritmo de Tate puede simplificarse bastante. Bajo estas hipótesis, haciendo $a_1' = a_2' = a_3' = 0$ en las ecuaciones del teorema 4.23 vemos que existen unos únicos r, s, $t \in D$ tales que el cambio de variables correspondiente (con $u = 1$) dan lugar a una ecuación (que seguirá siendo minimal) y que cumple $a_1 = a_2 = a_3 = 0$. Concretamente,

$$s = -\frac{a_1}{2}, \quad r = -\frac{a_2}{3} - \frac{a_1^2}{12}, \quad t = -\frac{a_3}{2} + \frac{a_1 a_3}{6} + \frac{a_1^3}{24}.$$

Es fácil determinar el tipo de reducción de una curva elíptica a partir de una ecuación minimal en estas condiciones:

Teorema 9.1 *Sea D un anillo de valoración discreta, sea K su cuerpo de cocientes y k su cuerpo de restos. Supongamos que* $\operatorname{car} k \neq 2, 3$. *Entonces, toda curva elíptica E/K admite una ecuación de Weierstrass minimal de la forma*

$$Y^2 = X^3 + a_4 X + a_6.$$

Para cualquiera de ellas, la tabla siguiente indica los valores $v(a_4)$, $v(a_6)$ y $v(\Delta)$ en función del tipo de reducción de E/K (donde hay que entender que la columna $\mathrm{I_n}$ *corresponde tanto a* $\mathrm{I_n}$ *como a* $\mathrm{I_{n,2}}$*, e igualmente con los demás tipos que admiten variantes).*

	$\mathrm{I_0}$	$\mathrm{I_n}$	II	III	IV	$\mathrm{I_0^*}$	$\mathrm{I_n^*}$	$\mathrm{IV^*}$	$\mathrm{III^*}$	$\mathrm{II^*}$
$v(a_4)$	≥ 0	$= 0$	≥ 1	$= 1$	≥ 2	≥ 2	$= 2$	≥ 3	$= 3$	≥ 4
$v(a_6)$	≥ 0	$= 0$	$= 1$	≥ 2	$= 2$	≥ 3	$= 3$	$= 4$	≥ 5	$= 5$
$v(\Delta)$	$= 0$	$= n$	$= 2$	$= 3$	$= 4$	$= 6$	$= n + 6$	$= 8$	$= 9$	$= 10$

Recíprocamente, cualquier ecuación de Weierstrass en las condiciones de la tabla es minimal.

Demostración: Observemos que, por las observaciones previas al teorema, una ecuación minimal de la forma indicada es única salvo cambios de variable de la forma $X = u^2 X'$, $Y = u^3 Y'$, donde u es una unidad de D, luego los valores de $v(a_4)$, $v(a_6)$ y $v(\Delta)$ no dependen de la ecuación minimal considerada. Por otra parte, una ecuación en las condiciones de la tabla es minimal por [CE 6.4].

El caso $\mathrm{I_0}$ es obvio. Los tipos $\mathrm{I_n}$ o $\mathrm{I_{n,2}}$ corresponden a la reducción multiplicativa. Observemos que el discriminante minimal es $\Delta = -64a_4^3 - 432a_6^2$ y sabemos que $v(\Delta) = n$, luego si fuera $v(a_4) \geq 1$, también tendríamos que $v(a_6) \geq 1$ y viceversa, con lo que la ecuación reducida sería $Y^2 = X^3$ y la reducción sería aditiva. Por consiguiente, ha de ser $v(a_4) = v(a_6) = 0$.

Para los casos siguientes consideremos la ecuación minimal de E/K a la que se llega mediante el algoritmo de Tate (que no es necesariamente de la forma del enunciado, pero de aquélla se pasa a ésta mediante el cambio de

variables determinado por los r, s, t indicados antes del enunciado). Para evitar confusiones, llamaremos a'_4 y a'_6 a los coeficientes de la ecuación del enunciado y a_i a los de la ecuación dada por el algoritmo de Tate.

A partir del paso 3 del algoritmo de Tate tenemos que $\pi \mid a_1, a_2, a_3, a_4, a_6$, de donde se sigue que $\pi \mid r, s, t$, y el teorema 4.23 nos da que $v(a'_4) \geq 1$, $v(a'_6) \geq 1$.

La reducción es de tipo II cuando $\pi^2 \nmid a_6$, y entonces, en la relación

$$a'_6 = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1,$$

todos los términos del miembro derecho son divisibles entre π^2 excepto el primero, luego $v(a'_6) = 1$. La relación

$$\Delta = -64a_4'^3 - 432a_6'^2$$

implica entonces que $v(\Delta) = 2$.

A partir del paso 4 del algoritmo de Tate tenemos que $\pi^2 \mid a_6$, lo que se traduce en que $v(a'_6) \geq 2$. La reducción es de tipo III si $\pi^3 \nmid b_8$ y, en la definición

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

vemos que todos los términos de la derecha son divisibles entre π^3 salvo quizá el último, luego ha de ser $v(a_4) = 1$. Consideramos ahora la relación

$$a'_4 = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st,$$

en la que todos los términos de la derecha son divisibles entre π^2 menos el primero, luego $v(a'_4) = 1$. Esto implica que $v(\Delta) = 3$.

A partir del paso 5 del algoritmo de Tate tenemos que $\pi^3 \mid b_8$, lo que implica que $v(a_4) \geq 2$ y esto, a su vez, que $v(a'_4) \geq 2$. Ahora tenemos que

$$a'_6 = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \equiv a_6 - ta_3 - t^2 \equiv a_6 + \frac{a_3^2}{4}$$

$$\equiv \frac{b_6}{4} \text{ (mód } \pi^3\text{)}.$$

La reducción es de tipo IV o IV_2 cuando $\pi^3 \nmid b_6$, lo cual se traduce en que $v(a'_6) = 2$ y, por consiguiente, en que $v(\Delta) = 4$.

A partir del paso 6 del algoritmo de Tate tenemos que $\pi^2 \mid a_3, a_4$, $\pi^3 \mid a_6$, lo que implica inmediatamente que $v(a'_6) \geq 3$. Los casos I_0^*, $\mathrm{I}_{0,2}^*$ y $\mathrm{I}_{0,3}^*$ se dan cuando el polinomio

$$P(T) = T^3 + a_{2,1}T^2 + a_{4,2}T + a_{6,3}$$

tiene raíces simples en $\bar{k}$, y en tal caso hemos de probar que $v(\Delta) = 6$. Vamos a ver que podemos suponer que tiene al menos una raíz en k. Si no la tiene, tampoco puede tener raíces en K (ya que, como $P(T)$ tiene coeficientes en D, tal raíz sería entera, luego estaría en D y daría lugar a una raíz de $P(T)$ en k. En particular $P(T)$ es irreducible tanto en $K[T]$ como en $k[T]$.

Sea α una raíz de $P(T)$ en una clausura algebraica de K, y sea $K' = K(\alpha)$. Tenemos que K' es también un cuerpo métrico discreto y completo[7], α es entero en K' y ahora $P(T)$ tiene una raíz en el cuerpo de restos k'. Más aún, se cumple la relación[8] $n = ef$, donde $n = |K' : K| = 2$, $f = |k' : k| = 3$ y e es el índice de ramificación, que, al ser $e = 1$, nos da que la valoración de K' extiende a la de K. Por consiguiente, todas las relaciones de divisibilidad que teníamos en K siguen siendo válidas en K', y $v(\Delta)$ es el mismo en K que en K'.

Equivalentemente, podemos suponer, como indicábamos, que $P(T)$ tiene una raíz en k. Entonces, un cambio de variable (el mismo que se hace en el paso 7 del algoritmo de Tate) nos permite suponer que dicha raíz es 0, lo que a su vez se traduce en que $\pi^4 \mid a_6$, y la reducción de $P(T)$ es

$$P(T) = T(T^2 + \bar{a}_{2,1}T + \bar{a}_{4,2}).$$

Que 0 sea una raíz simple equivale a que $v(a_4) = 2$, y que el polinomio cuadrático tenga raíces simples equivale a que $v(a_2^2 - 4a_4) = 2$. Usando esto calcularemos $v(\Delta)$. Se comprueba inmediatamente que

$$v(b_2) \geq 1, \quad v(b_4) = 2, \quad v(b_6) \geq 4, \quad v(b_8) = 4.$$

A su vez, de aquí deducimos que

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \equiv -b_2^2b_8 - 8b_4^3$$

$$\equiv -(4a_2)^2(-a_4^2) - 8(2a_4)^3 = 16a_4^2(a_2^2 - 4a_4) \text{ (mód } \pi^7),$$

luego, en efecto, $v(\Delta) = 6$.

A partir del paso 7 del algoritmo de Tate tenemos que

$$\pi \mid a_1, a_2, \quad \pi^2 \mid a_3, \quad \pi^3 \mid a_4, \ \pi^4 \mid a_6,$$

y la fibra es de tipo $\mathrm{I}_{\mathrm{n}}^*$ o $\mathrm{I}_{\mathrm{n},2}^*$ si $v(a_2) = 1$. Además, en tal caso ya sabemos que $v(\Delta) = n + 6$. Ahora es inmediato que

$$a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \equiv 2ra_2 + 3r^2 = -\frac{a_2^2}{3} \text{ (mód } \pi^3),$$

luego $v(a_4') = 2$. Similarmente,

$$a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \equiv r^2a_2 + r^3 = \frac{2a_2^3}{27} \text{ (mód } \pi^4),$$

luego $v(a_6') = 3$.

A partir del paso 8 del algoritmo de Tate tenemos que

$$\pi \mid a_1, \quad \pi^2 \mid a_2, a_3, \quad \pi^3 \mid a_4, \quad \pi^4 \mid a_6,$$

[7]Véanse los teoremas 5.27 y 5.28 de mi Geometría algebraica.
[8]Teorema 5.32 de mi Geometría algebraica.

de donde se sigue sin dificultad que $v(a'_4) \geq 3$, $v(a'_6) \geq 4$. Los tipos IV y IV_2 se dan cuando $v(a_3^2 - 4a_6) = 4$. Entonces:

$$a'_6 \equiv a_6 - ta_3 - t^2 \equiv \frac{4a_6 - a_3^2}{4} \text{ (mód } \pi^5),$$

luego $v(a'_6) = 4$. La relación $\Delta = -64a_4'^3 - 432a_6'^2$ implica que $v(\Delta) = 8$.

Dejamos a cargo del lector los dos últimos casos, que no presentan ninguna dificultad. ∎

9.8 Reducción y cambios de base

Sea K un cuerpo métrico discreto y completo, y sea K'/K una extensión de grado n. Según [GA 5.27, 5.28], la extensión K' es también un cuerpo métrico discreto y completo, y su valoración cumple la relación $v_{K'}|_K = ev_K$, para cierto número natural $e \geq 1$ llamado *índice de ramificación* de K'/K. Llamemos D y D' a los respectivos anillos de enteros y k, k' a los cuerpos de restos. Según [GA 5.30], la extensión k'/k es finita, y su grado f se llama *grado de inercia* de K'/K. La relación fundamental entre n, e y f es que $n = ef$ (por [GA 5.32]). Por simplicidad supondremos que el cuerpo de restos k es perfecto.

En esta sección usaremos el algoritmo de Tate para estudiar la relación entre el tipo de reducción de una curva elíptica E/K y el de la curva $E_{K'}/K'$. Partimos de una ecuación de Weierstrass minimal de E/K

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

con $a_i \in D$, que cumpla uno de los casos del algoritmo de Tate.

Observamos en primer lugar que las condiciones que determinan cada tipo de reducción dependen únicamente de los valores $v_K(a_i)$ o $v_K(b_i)$ de la ecuación dada o del tipo de descomposición de determinados polinomios en $\bar{k}$. Por lo tanto, si la extensión es no ramificada (es decir, cumple $e = 1$), tenemos que $v_{K'}|_K = v_K$ y, en cualquier caso, $\bar{k}' = \bar{k}$, por lo que la ecuación de Weierstrass sigue cumpliendo las condiciones del mismo caso del algoritmo de Tate.

Concluimos que las extensiones no ramificadas no alteran el tipo de reducción de E/K. A lo sumo, pueden alterar el *subtipo,* de modo que una reducción de tipo $\mathrm{I}_{n,2}$, IV_2, $\mathrm{I}^*_{n,2}$ o IV^*_2 puede pasar a ser de tipo I_n, IV, I^*_n o IV^*, respectivamente, y una reducción de tipo $\mathrm{I}^*_{0,3}$ puede pasar a tipo $\mathrm{I}^*_{0,2}$ o I^*_0, pues los subtipos 2 o 3 se dan cuando ciertos polinomios de $\bar{k}[X]$ tienen una o varias raíces fuera de k y, si es así, puede que las tengan en k'.

Una condición necesaria para que un subtipo 2 (resp. 3) pueda variar es que 2 (resp. 3) divida al grado de inercia f, pues el polinomio que determina el subtipo tiene el grado que indica el subíndice. La condición no es suficiente. Para determinar si el subtipo varía o no hay que determinar si las raíces del polinomio correspondiente (especificado por el algoritmo de Tate) están o no en k'. En resumen:

Teorema 9.2 *El tipo de reducción de una curva elíptica no se altera por extensiones no ramificadas, y el subtipo tampoco si* $6 \nmid f$.

Consideremos ahora el caso en que $e \geq 1$. Si la característica del cuerpo de restos k es $p = 2$ o $p = 3$, supondremos además que $p \nmid e$.

Tipo I_0 La condición para que la reducción sea de tipo I_0 (es decir, que E tenga buena reducción) es que $v(\Delta) = 0$, y esto sigue siendo cierto en K', luego la reducción de $E_{K'}$ sigue siendo de tipo I_0. Por ello, la buena reducción de una curva elíptica se llama también *reducción estable.*

Tipo $\mathrm{I_n}$ Si E/K tiene reducción de tipo $\mathrm{I_n}$ o $\mathrm{I_{n,2}}$, entonces se cumple que $v(a_3), v(a_4), v(a_6) \geq 1$, $v(b_2) = 0$, $v(\Delta) = n$, y estas condiciones siguen siendo ciertas en K', salvo que ahora $v(\Delta) = en$, luego la reducción de $E_{K'}$ es de tipo $\mathrm{I_{en}}$ o $\mathrm{I_{en,2}}$. (Observemos que la condición para el subtipo se conserva.) Vemos así que se conserva el tipo de reducción aunque se altera el índice n. Por ello, la reducción multiplicativa de una curva elíptica se llama también *reducción semiestable.* (Aunque, por conveniencia, se incluye a la reducción estable como caso particular de la reducción semiestable, de modo que la reducción semiestable es, por definición, la de tipo $\mathrm{I_n}$ o $\mathrm{I_{n,2}}$ para $n \geq 0$.)

Tipo II Si la reducción de E/K es de tipo II, tenemos que $v(a_i) \geq 1$ para todo i, $v(a_6) = 1$. Por consiguiente, en K' tenemos que $v(a_i) \geq e$, $v(a_6) = e$. Dividamos $e = 6c + e'$, con $0 \leq e' < 6$ (y $c \geq 1$ si $e' = 0$). El cambio de variables $X = \pi'^{2c}X'$, $Y = \pi'^{3c}Y'$ (donde π' es un primo de D') nos transforma la ecuación en otra que cumple

$$v(a_i) \geq (6-i)c + e', \qquad v(a_6) = e'.$$

Si $e' = 0$, entonces, $6 \mid e$, y en tal caso estamos suponiendo que la característica de k es distinta de 2, 3. Es inmediato entonces que $v(\Delta) = 0$, por lo que la reducción pasa a ser de tipo I_0.

Si $e' = 1$, la ecuación cumple nuevamente las condiciones del tipo II.

Si $e' = 2$, se comprueba inmediatamente que la ecuación cumple las condiciones del tipo IV o IV_2.

Si $e' = 3$ Se cumplen las condiciones del paso 6 del algoritmo de Tate, pues la reducción del polinomio $P(T)$ es $T^3 + \bar{a}_{6,3}$. En este caso $3 \mid e$, luego estamos suponiendo que la característica de k es distinta de 3, luego $P(T)$ tiene raíces distintas en $\bar{k}$ y concluimos que la reducción es de tipo I_0^*, $\mathrm{I}_{0,2}^*$ o $\mathrm{I}_{0,3}^*$.

Si $e' = 4$ ahora la reducción de $P(T)$ es T^3, luego se cumplen las hipótesis del paso 8 del algoritmo, ya que el discriminante del polinomio $P_1(T)$ cumple $v(a_{3,2}^2 - 4a_{6,4}) = 0$ (teniendo en cuenta que, por hipótesis, la característica de k es distinta de 2). Así pues, la reducción es de tipo IV^* o IV_2^*.

Si $e' = 5$, es claro que la reducción es de tipo II^*.

Tipo III Supongamos ahora que E/K tiene reducción de tipo III, con lo que $v(a_i) \geq 1$, $v(a_4) = 1$, $v(a_6) \geq 2$. Tras la extensión tenemos que $v(a_i) \geq e$, $v(a_4) = e$. Ahora dividimos $e = 4c + e'$ y hacemos el cambio de variables $X = \pi'^{2c}X'$, $Y = \pi'^{3c}Y'$, con lo que

$$v(a_1) \geq 2c + e',\ v(a_2) \geq 2c + e',\ v(a_3) \geq c + e',\ v(a_4) = e',\ v(a_6) = 2c + 2e'.$$

Si $e' = 0$, entonces estamos suponiendo que $\operatorname{car} k \neq 2$, con lo que es fácil ver que $v(\Delta) = 0$ y la reducción es de tipo I_0.

Si $e' = 1$, se vuelven a cumplir las condiciones del tipo III.

Si $e' = 2$ se cumplen las condiciones del paso 6 del algoritmo, pues la reducción del polinomio $P(T)$ es $T(T^2 + \bar{a}_{4,2})$ y, como en este caso suponemos que $\operatorname{car} k \neq 2$, el segundo factor tiene raíces simples no nulas. La reducción será de tipo I_0^* o $\mathrm{I}_{0,2}^*$ (pero el subtipo 3 no puede darse).

Si $e' = 3$ la reducción es claramente de tipo III^*.

Tipo IV Si la reducción de E/K es de tipo IV o IV_2, tenemos que $v(a_i) \geq 1$, $v(a_4) \geq 2$, $v(a_6) \geq 2$, así como que $v(b_6) = 2$. Ahora dividimos $e = 3c + e'$ y el cambio de variables usual nos da que

$$v(a_1) \geq 2c + e',\ v(a_2) \geq c + e',\ v(a_3) \geq e',\ v(a_4) \geq 2c + 2e',\ v(a_6) \geq 2e',$$

y además $v(b_6) = e'$.

Si $e' = 0$ entonces $\operatorname{car} k \neq 3$ y vemos que $v(\Delta) = 0$, luego la reducción es de tipo I_0.

Si $e' = 1$ se vuelven a cumplir las condiciones del tipo IV o IV_2.

Si $e' = 2$ se cumplen las condiciones del paso 8 del algoritmo, pues el discriminante del polinomio $P_1(T)$ cumple $v(a_{3,2}^2 + 4a_{6,4}) = v(b_6) - 2 = 0$. Por lo tanto, la reducción es de tipo IV^* o IV_2^*.

Tipo I_0^* Si la reducción de E/K es de tipo I_0^* (o de cualquiera de sus subtipos) tenemos que

$$v(a_1) \geq 1, \quad v(a_2) \geq 1, \quad v(a_3) \geq 2, \quad v(a_4) \geq 2, \quad v(a_6) \geq 3$$

y, si

$$\Delta_0 = \pi^{-6}(-4a_2^3a_6 + a_2^2a_4^2 - 4a_4^3 - 27a_6^2 + 18a_2a_4a_6)$$

es el discriminante del polinomio $P(T)$, se cumple además que $v(\Delta_0) = 0$. Más aún, si $\operatorname{car} k \neq 2$, el teorema 9.1 nos da que $v(\Delta) = 6$. (En dicho teorema suponíamos que la característica de k era distinta de 2 y 3, pero, revisando el argumento que prueba este hecho en concreto, se ve que también es válido si $\operatorname{car} k = 3$.)

Ahora dividimos $e = 2c + e'$, y el cambio de variables usual nos da que

$$v(a_1) \geq c + e',\ v(a_2) \geq e',\ v(a_3) \geq c + 2e',\ v(a_4) \geq 2e',\ v(a_6) \geq 3e',$$

y el nuevo discriminante es

$$\Delta_0' = \pi'^{-6}(-4a_2'^3a_6' + a_2'^2a_4'^2 - 4a_3'^3 - 27a_6'^2 + 18a_2'a_4'a_6')$$
$$= \pi'^{-12c-6}(-4a_2^3a_6 + a_2^2a_4^2 - 4a_4^3 - 27a_6^2 + 18a_2a_4a_6)$$
$$= \pi'^{6(e'-1)}\Delta_0,$$

luego, en K', se cumple que $v(\Delta_0) = 6(e'-1)$.

Si $e' = 0$ estamos suponiendo que $\operatorname{car} k \neq 2$, luego el discriminante original de la ecuación de Weierstrass cumplía $v(\Delta) = 6$, luego el de la nueva ecuación cumple $v(\Delta) = 0$. Por consiguiente, la reducción es de tipo I_0.

Si $e' = 1$, se siguen cumpliendo las condiciones del tipo I_0^* (o sus subtipos), pues tenemos que $v(\Delta_0) = 0$.

Tipo I_n^* Si E/K es de tipo I_n^* o $\mathrm{I}_{\mathrm{n},2}^*$, tenemos que

$$v(a_1) \geq 1,\ v(a_2) = 1,\ v(a_3) \geq 2,\ v(a_4) \geq 3,\ v(a_6) \geq 4.$$

(Recordemos que, en estas condiciones, $P(T)$ tiene a $T = 0$ como raíz doble, y la condición para que no sea triple es que $v(a_2) = 1$.) Dividimos $e = 2c + e'$ y el cambio de variables nos da

$$v(a_1) \geq c + e',\ v(a_2) = e',\ v(a_3) \geq c + 2e',\ v(a_4) \geq 2c + 3e',\ v(a_6) \geq 2c + 4e'.$$

Si $e' = 0$ estamos suponiendo que $\operatorname{car} k \neq 2$, luego el algoritmo nos da que el discriminante original de la ecuación de Weierstrass cumplía $v(\Delta) = n + 6$, luego ahora cumple

$$v(\Delta) = (n+6)2c - 12c = 2cn = en.$$

Como $v(b_2) = v(a_1^2 + 4a_2) = 0$, la reducción es de tipo I_en o $\mathrm{I}_{\mathrm{en},2}$.

Si $e' = 1$ se vuelven a cumplir las condiciones del paso 7 del algoritmo de Tate. Si $\operatorname{car} k \neq 2$, el discriminante de la ecuación cumple ahora que

$$v(\Delta) = (n+6)(2c+1) - 12c = en + 6,$$

luego la reducción es de tipo I_en^* o $\mathrm{I}_{\mathrm{en},2}^*$. Si $\operatorname{car} k = 2$ se llega a la misma conclusión analizando el algoritmo que calcula el índice. Por ejemplo, si la reducción original era de tipo $\mathrm{I}_{2\mathrm{i}+1}^*$, hemos de probar que la nueva es de tipo $\mathrm{I}_{(2\mathrm{i}+1)\mathrm{e}}^* = \mathrm{I}_{2\mathrm{i}'+1}^*$, donde $i' = 2ci + c + i$.

Tenemos que los coeficientes de la ecuación original cumplían

$$v(a_3) \geq i + 2, \quad v(a_4) \geq i + 3, \quad v(a_6) \geq 2i + 4,$$

luego los coeficientes de la nueva cumplen

$$v(a_3) \geq (i+2)(2c+1) - 3c = 2ci + c + i + 2 = i' + 2,$$
$$v(a_4) \geq (i+3)(2c+1) - 4c = 2ci + 2c + i + 3 \geq i' + 3,$$
$$v(a_6) \geq (2i+4)(2c+1) - 6c = 4ci + 2c + 2i + 4 = 2i' + 4.$$

Además, la primera ecuación cumple que $v(a_{3,i+2}^2 + 4a_{6,2i+4}) = 0$, luego la nueva cumple que

$$v_{K'}(a_{3,i'+2}'^2 + 4a'_{6,2i'+4}) = v_{K'}(a_3'^2 + 4a'_6) - 2i' - 4$$

$$= v_{K'}(a_3^2 + 4a_6) - 6c - 2i' - 4 = (2i+4)e - 6c - 2i' - 4 = 0.$$

Esto prueba que la nueva ecuación cumple las condiciones de la reducción de tipo $\mathrm{I}^*_{(2i+1)e}$ o $\mathrm{I}^*_{(2i+1)e,2}$. Similarmente se razona si la reducción original era de tipo I^*_{2i}.

Tipo IV^* Si E/K es de tipo IV^* o IV^*_2, tenemos que

$$v(a_1) \geq 1,\ v(a_2) \geq 2,\ v(a_3) \geq 2,\ v(a_4) \geq 3,\ v(a_6) \geq 4$$

y $v(b_6) = 4$. Dividimos $e = 3c + e'$, pero no hacemos el cambio de variables usual, sino $X = \pi'^{4c}X$, $Y = \pi'^{6c}Y$, con lo que obtenemos

$$v(a_1) \geq c + e',\ v(a_2) \geq 2c + 2e',\ v(a_3) \geq 2e',\ v(a_4) \geq c + 3e',\ v(a_6) \geq 4e',$$

$$v(b_6) = 4e'.$$

Si $e' = 0$ estamos suponiendo que $\operatorname{car} k \neq 3$, con lo que se ve inmediatamente que $v(\Delta) = 0$, luego la reducción es de tipo I_0.

Si $e' = 1$, se vuelven a cumplir las condiciones para la reducción de tipo IV^* o IV^*_2.

Si $e' = 2$ podemos hacer un nuevo cambio: $X = \pi'^2X$, $Y = \pi'^3Y$, con lo que obtenemos

$$v(a_1) \geq c + 1,\ v(a_2) \geq 2c + 2,\ v(a_3) \geq 1,\ v(a_4) \geq c + 2,\ v(a_6) \geq 2,\ v(b_6) = 2.$$

Así se cumplen las condiciones para la reducción de tipo IV o IV_2.

Tipo III^* Si la reducción de E/K es de tipo III^*, tenemos que

$$v(a_1) \geq 1,\ v(a_2) \geq 2,\ v(a_3) \geq 3,\ v(a_4) = 3,\ v(a_6) \geq 5.$$

Dividimos $e = 4c + e'$ y hacemos el cambio $X = \pi'^{6c}X'$, $Y = \pi'^{9c}Y'$. El resultado es

$$v(a_1) \geq c + e',\ v(a_2) \geq 2c + 2e',\ v(a_3) \geq 3c + 3e',\ v(a_4) = 3e',\ v(a_6) \geq 2c + 5e'.$$

Si $e' = 0$, entonces suponemos que $\operatorname{car} k \neq 2$ y es claro entonces que $v(\Delta) = 0$, luego la reducción es de tipo I_0.

Si $e' = 1$ tenemos de nuevo las condiciones de la reducción de tipo III^*.

Si $e' = 2$ podemos hacer el cambio $X = \pi'^2X'$, $Y = \pi'^3Y'$, con lo que obtenemos

$$v(a_1) \geq c + 1,\ v(a_2) \geq 2c + 2,\ v(a_3) \geq 3c + 3,\ v(a_4) = 2,\ v(a_6) \geq 2c + 4.$$

Se cumplen las condiciones del paso 6 del algoritmo de Tate, pues la reducción del polinomio $P(T)$ es $T(T^2 + a_{4,2})$, que tiene sus raíces simples, pues en este caso suponemos que $\operatorname{car} k \neq 2$.

Si $e' = 3$ podemos hacer el cambio $X = \pi'^4 X'$, $Y = \pi'^6 Y'$, con lo que obtenemos

$$v(a_1) \geq c+1,\ v(a_2) \geq 2c+2,\ v(a_3) \geq 3c+3,\ v(a_4) = 1,\ v(a_6) \geq 2c+3.$$

Se comprueba inmediatamente que la reducción es de tipo III.

Tipo II^* Si la reducción de E/K es de tipo II^*, tenemos

$$v(a_1) \geq 1,\ v(a_2) \geq 2,\ v(a_3) \geq 3,\ v(a_4) \geq 4,\ v(a_6) = 5.$$

Dividimos $e = 6c + e'$ y hacemos el cambio $X = \pi'^{10c} X'$, $Y = \pi'^{15c} Y'$, con lo que obtenemos:

$$v(a_1) \geq c+e',\ v(a_2) \geq 2c+2e',\ v(a_3) \geq 3c+3e',\ v(a_4) \geq 4c+4e',\ v(a_6) = 5e'.$$

Si $e' = 0$ suponemos que $\operatorname{car} k \neq 2, 3$ y es claro que $v(\Delta) = 0$, luego la reducción es de tipo I_0.

Si $e' = 1$ la reducción es de tipo II^*.

Si $e' = 2$, el cambio $X = \pi'^2 X'$, $Y = \pi'^3 Y'$ nos da

$$v(a_1) \geq c+1,\ v(a_2) \geq 2c+2,\ v(a_3) \geq 3c+3,\ v(a_4) \geq 4c+4,\ v(a_6) = 4.$$

La reducción es de tipo IV^* o IV_2^*, porque la reducción del polinomio $P_1(T)$ es $T^2 - a_{6,2}$ y $\operatorname{car} k \neq 2$.

Si $e' = 3$, el cambio $X = \pi'^4 X'$, $Y = \pi'^6 Y'$ nos da

$$v(a_1) \geq c+1,\ v(a_2) \geq 2c+2,\ v(a_3) \geq 3c+3,\ v(a_4) \geq 4c+4,\ v(a_6) = 3.$$

La reducción es de tipo I_0^*, pues la reducción del polinomio $P(T)$ es $T^3 + a_{6,3}$, y estamos suponiendo que $\operatorname{car} k \neq 3$.

Si $e' = 4$, el cambio $X = \pi'^6 X'$, $Y = \pi'^9 Y'$ nos da

$$v(a_1) \geq c+1,\ v(a_2) \geq 2c+2,\ v(a_3) \geq 3c+3,\ v(a_4) \geq 4c+4,\ v(a_6) = 2.$$

Teniendo en cuenta que $\operatorname{car} k \neq 2$, es claro que la reducción es de tipo IV o IV_2.

Si $e' = 5$, el cambio $X = \pi'^8 X'$, $Y = \pi'^{12} Y'$ nos da

$$v(a_1) \geq c+1,\ v(a_2) \geq 2c+2,\ v(a_3) \geq 3c+3,\ v(a_4) \geq 4c+4,\ v(a_6) = 1$$

y la reducción es claramente de tipo II.

Con esto hemos probado el teorema siguiente:

Teorema 9.3 *Sea K un cuerpo métrico discreto y completo, sea K'/K una extensión finita con índice de ramificación e y supongamos que, si la característica del cuerpo de restos es $p = 2, 3$, entonces $p \nmid e$. Entonces, si E/K es una curva*

elíptica, el tipo de reducción de $E_{K'}/K'$ se calcula a partir del de E/K en función del resto de e módulo el valor de m que indica la tabla siguiente, y es el dado por la tabla (en la que no se indican los subtipos).

Tipo	*Reducción*						
e (mód m)	0	1	2	3	4	5	m
$\mathrm{I_n}$	$\mathrm{I_{en}}$						1
II	$\mathrm{I_0}$	II	IV	$\mathrm{I_0^*}$	$\mathrm{IV^*}$	$\mathrm{II^*}$	6
III	$\mathrm{I_0}$	III	$\mathrm{I_0^*}$	$\mathrm{III^*}$			4
IV	$\mathrm{I_0}$	IV	$\mathrm{IV^*}$				3
$\mathrm{I_n^*}$	$\mathrm{I_{en}}$	$\mathrm{I_{en}^*}$					2
$\mathrm{IV^*}$	$\mathrm{I_0}$	$\mathrm{IV^*}$	IV				3
$\mathrm{III^*}$	$\mathrm{I_0}$	$\mathrm{III^*}$	$\mathrm{I_0^*}$	III			4
$\mathrm{II^*}$	$\mathrm{I_0}$	$\mathrm{II^*}$	$\mathrm{IV^*}$	$\mathrm{I_0^*}$	IV	II	6

Vemos, en particular, que (al menos si $\operatorname{car} k \neq 2, 3$) las curvas con reducción aditiva tienen *potencialmente buena reducción* (es decir, que pasan a tener buena reducción tras una extensión adecuada del cuerpo) excepto las de tipo $\mathrm{I_n^*}$, con $n \geq 1$, que tienen *potencialmente reducción multiplicativa.*

Conviene observar que si $p = \operatorname{car} k = 2$, las pruebas de los casos $\mathrm{I_n}$, IV y $\mathrm{IV^*}$ no han necesitado la hipótesis $p \nmid e$ y, cuando $p = 3$, tampoco hemos necesitado esta hipótesis en los casos $\mathrm{I_n}$, $\mathrm{I_n^*}$, III y $\mathrm{III^*}$. En general, sólo nos ha hecho falta esta hipótesis en los casos en que $p \mid m$.

Capítulo X

El modelo de Néron

La geometría de las curvas elípticas está condicionada en gran medida por el hecho de que son variedades abelianas, es decir, por que admiten una estructura de grupo compatible con su estructura geométrica. En este capítulo estudiamos si dicha estructura de grupo puede extenderse a los modelos regulares minimales. La respuesta es negativa, pero veremos que sí podemos definir una estructura de grupo sobre el abierto formado por los puntos suaves del modelo regular minimal. Esto no es trivial en absoluto, y vamos a necesitar bastantes preparativos.

10.1 El esquema de componentes conexas

Desarrollamos aquí un aparato algebraico para tratar con las componentes conexas de un conjunto algebraico y su comportamiento ante productos y cambios de base. El concepto fundamental es del de álgebra separable, que presentamos a continuación:

Teorema 10.1 *Sea k un cuerpo, k_s su clausura separable, $\bar{k}$ su clausura algebraica y A una k-álgebra de dimensión finita sobre k. Las afirmaciones siguientes son equivalentes:*

a) El homomorfismo $\operatorname{Esp} A \longrightarrow \operatorname{Esp} k$ *es llano.*

b) A es producto de un número finito de cuerpos separables sobre k.

c) $A \otimes_k \bar{k}$ es reducida.

d) $A \otimes_k \bar{k} = \bar{k} \oplus \cdots \oplus \bar{k}$.

e) $A \otimes_k k_s = k_s \oplus \cdots \oplus k_s$.

Si k es perfecto, estas condiciones equivalen a que A sea reducida.

Demostración: Observemos que, en general, el teorema [AC 3.82] implica que si A es una k-álgebra de dimensión finita sobre k, entonces $\operatorname{Esp} A =$

$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_d\}$ es un conjunto algebraico finito de dimensión 0, luego A es suma directa de los anillos locales $A_{\mathfrak{p}_i}$, que son k-álgebras locales de dimensión 0.

a) $\Rightarrow$ b) Cada $A_{\mathfrak{p}_i}$ es no ramificado sobre k, lo que significa que el ideal maximal de $A_{\mathfrak{p}_i}$ es el ideal nulo, es decir, que $A_{\mathfrak{p}_i}$ es un cuerpo, y que éste es una extensión separable de k.

b) $\Rightarrow$ a) Si $A = K_1 \oplus \cdots \oplus K_r$, donde K_i/k es una extensión finita separable, entonces $\operatorname{Esp} A$ consta de r puntos, cada uno de los cuales tiene a K_i por anillo local. Claramente, entonces, $\operatorname{Esp} A$ es no ramificado sobre k, y ciertamente es plano, luego es llano.

b) $\Leftrightarrow$ c) La condición b) equivale a que los puntos de $\operatorname{Esp} A$ (como subesquemas abiertos) sean esquemas íntegros X_i tales que $K(X_i)/k$ es separable. Por el teorema [E 3.64], esto equivale a su vez a que cada X_i sea geométricamente reducido, lo que a su vez equivale a que $\operatorname{Esp} A$ sea geométricamente reducido, y esto es c).

c) $\Rightarrow$ d) La $\bar{k}$-álgebra $A \otimes_k \bar{k}$ es suma directa de anillos locales de dimensión 0. Si es reducida, éstos han de ser cuerpos, y extensiones finitas de $\bar{k}$, luego han de ser todos isomorfos a $\bar{k}$.

d) $\Rightarrow$ c) es trivial.

c) $\Leftrightarrow$ e) resulta de aplicar c) $\Leftrightarrow$ b) a la k_s-álgebra $A \otimes_k k_s$.

Obviamente, las condiciones del teorema implican que A es reducida y, si A es reducida, entonces es suma directa de cuerpos. Si k es perfecto serán separables sobre k, con lo que tenemos b). ∎

Definición 10.2 Si k es un cuerpo y A es una k-álgebra de dimensión finita sobre k, diremos que A es *separable* si cumple cualquiera de las condiciones del teorema anterior.

Veamos algunas propiedades adicionales:

Teorema 10.3 *Toda subálgebra, todo cociente, toda suma directa y todo producto tensorial de álgebras separables es separable.*

Demostración: Si A es una subálgebra de B, entonces $A \otimes_k \bar{k}$ es una subálgebra de $B \otimes_k \bar{k}$, y si la segunda es reducida, también lo es la primera.

Si I es un ideal de A, entonces $(A/I) \otimes_k \bar{k} \cong (A \otimes_k \bar{k})/(I \otimes_k \bar{k})$, pero los únicos ideales de $\bar{k} \oplus \cdots \oplus \bar{k}$ son sumas directas de algunos de los sumandos, luego el cociente tiene la misma forma (con menos sumandos).

Si A y B son separables, entonces $(A \oplus B) \otimes_k \bar{k} = (A \otimes_k \bar{k}) \oplus (B \otimes_k \bar{k})$, lo que implica claramente que $A \oplus B$ es separable.

Por último, $(A \otimes_k B) \otimes_k \bar{k} \cong (A \otimes_k \bar{k}) \otimes_{\bar{k}} (B \otimes_k \bar{k})$, que es suma directa de copias de $\bar{k} \otimes_{\bar{k}} \bar{k} = \bar{k}$, luego el producto es separable. ∎

Teorema 10.4 *Si A es una k-álgebra de dimensión finita y L/k es una extensión de cuerpos, entonces A es separable sobre k si y sólo si $A \otimes_k L$ es separable sobre L.*

DEMOSTRACIÓN: Observemos que

$$(A \otimes_k L) \otimes_L \bar{L} = A \otimes_k \bar{L} = (A \otimes_k \bar{k}) \otimes_{\bar{k}} \bar{L}.$$

Por lo tanto, si A es separable sobre k, tenemos que $A \otimes_k \bar{k}$ es suma de copias de $\bar{k}$, luego $(A \otimes_k L) \otimes_L \bar{L}$ es suma de copias de $\bar{L}$.

Recíprocamente, si $A \otimes_k L$ es separable, entonces $A \otimes_k \bar{L}$ es reducida, luego también lo es la subálgebra $A \otimes_k \bar{k}$, luego A es separable. ∎

Definición 10.5 Recordemos que una *acción* de un grupo G sobre un conjunto X es un homomorfismo de G en el grupo de permutaciones de X, de modo que cada $\sigma \in G$ tiene asociada una permutación $x \mapsto x^\sigma$ de X de forma que $x^{\sigma\tau} = (x^\sigma)^\tau$.

Sea k un cuerpo y consideremos el grupo de Galois $G = G(k_s/k)$. Una acción de G sobre un conjunto X es *continua* si existe una extensión finita de Galois L/k tal que $G(k_s/L)$ está contenido en el núcleo de la acción, es decir, que los elementos de $G(k_s/L)$ dejan fijos a todos los elementos de X.

Si G actúa sobre dos conjuntos X e Y, un *isomorfismo* entre ambas acciones es una biyección $f : X \longrightarrow Y$ tal que, para todo $\sigma \in G$ y todo $x \in X$, se cumple que $f(x^\sigma) = f(x)^\sigma$.

Fijemos ahora un cuerpo k y sea $G = G(k_s/k)$. Para cada k-álgebra separable A, llamemos $X_A = \mathrm{Hom}_k(A, k_s)$.

Si $A = K_1 \oplus \cdots \oplus K_r$, donde cada K_i es una extensión separable de k, entonces $\operatorname{Esp} A$ tiene r ideales primos (todos ellos maximales), que son, concretamente, las sumas de los r cuerpos menos uno de ellos. El núcleo de un k-homomorfismo $f : A \longrightarrow k_s$ ha de ser uno de estos ideales, lo cual significa que existe un i tal que $f|_{K_i} : K_i \longrightarrow k_s$ es un k-monomorfismo y $f|_{K_j} = 0$ para todo $j \neq i$. El número de k-monomorfismos $K_i \longrightarrow k_s$ es $|K_i : k| = \dim_k K_i$, luego X_A es un conjunto finito con $\dim_k A$ elementos.

El grupo G actúa sobre X_A mediante $f^\sigma(a) = \sigma(f(a))$, y la acción es continua, pues si L es una extensión finita de Galois de k que contiene a todos los cuerpos K_i, entonces $X_A = \mathrm{Hom}_k(A, L)$, y $G(k_s/L)$ deja invariantes todos los elementos de X_A.

Vamos a probar que si dos k-álgebras A y B determinan acciones isomorfas en X_A y X_B, entonces $A \cong B$.

Sea $k_s^{X_A}$ el conjunto de todas las aplicaciones $X_A \longrightarrow k_s$, que tiene estructura de k_s-álgebra con las operaciones definidas puntualmente. Definimos

$$\phi : A \otimes_k k_s \longrightarrow k_s^{X_A}$$

mediante $\phi(a \otimes \alpha)(f) = f(a)\alpha$. Claramente es un homomorfismo de k_s-álgebras. Veamos que es suprayectivo.

Podemos formar una k-base $\{a_i\}$ de A uniendo k-bases de los cuerpos K_i. Un elemento arbitrario de $A \otimes_k k_s$ es de la forma

$$x = \sum_i a_i \otimes \alpha_i,$$

Dado $g \in k_s^{X_A}$, para que se cumpla $\phi(x) = g$ ha de suceder que, para todo $f \in X_A$, tengamos

$$\sum_i f(a_i)\alpha_i = g(f).$$

Tenemos así un sistema de ecuaciones lineales en las incógnitas α_i, y su matriz de coeficientes es $M = (f(a_i))_{i,f}$. Si ordenamos los homomorfismos f según el cuerpo K_i al que corresponden, la matriz M es una suma diagonal de r cajas, cada una de las cuales es de la forma $(f(a_i))_{i,f}$, donde ahora a_i recorre una k-base de K_i y f recorre los k-monomorfismos $K_i \longrightarrow k_s$. Es conocido que la separabilidad de K_i implica que esta matriz es regular.[1] Así pues, el sistema de ecuaciones tiene solución, y ϕ es suprayectiva.

Como $A \otimes_k k_s$ y $k_s^{X_A}$ son k_s-espacios vectoriales de la misma dimensión, concluimos que ϕ es un k_s-isomorfismo de álgebras.

Definimos ahora acciones de G sobre ambas álgebras, mediante

$$(a \otimes \alpha)^\sigma = a \otimes \sigma(\alpha), \qquad (g^\sigma)(f) = (g(f^{\sigma^{-1}}))^\sigma.$$

Conviene ver la segunda definición desde otro punto de vista más natural: si $X_A = \{f_1, \ldots, f_n\}$, podemos representar los elementos de $k_s^{X_A}$ en la forma $\alpha_1 f_1 + \cdots + \alpha_n f_n$ y, con esta notación, la acción que hemos definido es

$$(\alpha_1 f_1 + \cdots + \alpha_n f_n)^\sigma = \sigma(\alpha_1) f_1^\sigma + \cdots + \sigma(\alpha_n) f_n^\sigma.$$

Vamos a probar que las dos acciones son isomorfas a través de ϕ. Para ello basta observar que

$$\phi(a \otimes \alpha)^\sigma(f) = \phi(a \otimes \sigma(\alpha))(f) = f(a)\sigma(\alpha),$$

$$\phi((a\otimes\alpha)^\sigma)(f) = (\phi(a\otimes\alpha)(f^{\sigma^{-1}}))^\sigma = (f^{\sigma^{-1}}(a)\alpha)^\sigma = (\sigma^{-1}(f(a))\alpha)^\sigma = f(a)\sigma(\alpha).$$

Ahora observamos que el conjunto de los elementos de $A \otimes_k k_s$ fijados por G es A. En efecto, sea $x \in A \otimes_k k_s$ un elemento fijado. Si $\{a_i\}$ es una k-base de A, tenemos que x se expresa de forma única como

$$x = \sum_i a_i \otimes \alpha_i,$$

para ciertos $\alpha_i \in k_s$. Al aplicar $\sigma \in G$ obtenemos que

$$\sigma(x) = \sum_i a_i \otimes \sigma(\alpha_i).$$

Por la unicidad, ha de ser $\sigma(\alpha_i) = \alpha_i$, para todo i y todo σ, luego $\alpha_i \in k$, luego $x \in A \otimes_k k = A$.

[1] Ver, por ejemplo, mi libro de álgebra, definición 10.30.

Como $k_s^{X_A}$ es isomorfo a $A\otimes_k k_s$, ahora podemos concluir que el conjunto de elementos de $k_s^{X_A}$ fijados por G es una k-álgebra $F\cong A$, y que $k_s^{X_A}\cong F\otimes_k k_s$.

Ahora basta tener presente que la acción de G sobre $k_s^{X_A}$ está definida exclusivamente a partir de las acciones de G en X_A y en k_s. Por lo tanto, si dos álgebras A y B definen acciones isomorfas de G sobre X_A y X_B, entonces también serán isomorfas las acciones de G sobre $k_s^{X_A}$ y $k_s^{X_B}$, y también serán isomorfas las k-álgebras de elementos fijados por ambas, pero éstas son isomorfas a A y B respectivamente.

En otras palabras, hemos probado que cada k-álgebra separable A está completamente determinada por el conjunto X_A y la acción de G sobre éste. Ahora vamos a probar que todo conjunto finito X sobre el que G actúa continuamente es isomorfo a un X_A, para cierta k-álgebra separable A.

En primer lugar, es claro que $X_{A\oplus B}=X_A\cup X_B$ (unión disjunta) y que la acción de G sobre $X_{A\oplus B}$ se restringe a las acciones de G sobre X_A y X_B. Por lo tanto, si tenemos un conjunto finito arbitrario X sobre el que G actúa continuamente, podemos descomponerlo en órbitas disjuntas $X_1,\ldots,X_r$ sobre las que G actúa transitivamente. Si probamos que $X_i\cong X_{A_i}$, para cierta k-álgebra separable A_i, entonces $X\cong X_{A_1\oplus\cdots\oplus A_r}$. Por consiguiente, podemos restringirnos al caso en que G actúa transitivamente sobre X.

Sea L/k una extensión finita de Galois tal que los elementos de $G(k_s/L)$ fijen a todos los elementos de X. Sea $x_0\in X$ y sea $H=\{\sigma\in G\mid x_0^\sigma=x_0\}$. Así $G(k_s/L)\subset H\subset G$ y podemos identificar a H con un subgrupo de $G(L/k)$. Sea $A\subset L$ el cuerpo fijado por H. Como A/k es una extensión finita separable, tenemos que A es, en particular, una k-álgebra separable. Vamos a probar que $X\cong X_A$.

Sea $f_0:A\longrightarrow k_s$ la inclusión. Cada $x\in X$ es de la forma $x=\sigma(x_0)$, para cierto $\sigma\in G$, y si $x=\sigma(x_0)=\tau(x_0)$, entonces $\sigma\tau^{-1}\in H$, luego $f_0\circ\sigma\circ\tau^{-1}=f_0$, luego $f_0\circ\sigma=f_0\circ\tau$.

Por consiguiente, podemos definir la aplicación $X\longrightarrow X_A$ determinada por $\sigma(x_0)\mapsto f_0\circ\sigma$. Claramente es inyectiva y, como X y X_A tienen el mismo número de elementos, es biyectiva. También es obvio que determina un isomorfismo entre las acciones de G en X y X_A.

Así pues, hemos probado que las k-álgebras separables se corresponden biunívocamente (salvo isomorfismo) con los conjuntos finitos sobre los que G actúa continuamente. Sin embargo, no era esto realmente lo que nos interesaba, sino un hecho que hemos obtenido colateralmente en la prueba:

Teorema 10.6 *Sea k un cuerpo, V un k_s-espacio vectorial, $X=\{e_1,\ldots,e_n\}$ una base de V y supongamos que $G=G(k_s/k)$ actúa continuamente sobre X, de modo que también actúa sobre V con la acción dada por*

$$(\alpha_1e_1+\cdots+\alpha_ne_n)^\sigma=\sigma(\alpha_1)e_1^\sigma+\cdots+\sigma(\alpha_n)e_n^\sigma.$$

Entonces, el conjunto F de los elementos de V fijados por G es un k-espacio vectorial tal que $V\cong F\otimes_k k_s$.

DEMOSTRACIÓN: Hemos probado que existe una k-álgebra separable A tal que $X \cong X_A$, y es claro entonces que $V \cong k_s^{X_A}$, y también hemos probado que $k_s^{X_A}$ cumple el teorema. ∎

Teorema 10.7 *Sea B una k-álgebra finitamente generada y sea A una subálgebra de B. Entonces A tiene una (única) subálgebra separable A^s que contiene a todas las subálgebras separables de A.*

DEMOSTRACIÓN: Llamemos A^s al producto de todas las subálgebras separables de A. Observemos que k es una subálgebra separable de A, luego siempre existen tales subálgebras. Vamos a demostrar que A^s es un k-espacio vectorial de dimensión finita. Esto implicará que A^s puede expresarse como producto de un número finito de subálgebras separables de A, y esto implica que es separable, ya que si A_1 y A_2 son subálgebras separables de A, entonces A_1A_2 es un cociente de $A_1 \otimes_k A_2$, luego es también separable.

Como $A^s \subset B^s$, basta probar que B^s tiene dimensión finita sobre k o, equivalentemente, podemos suponer que A es finitamente generada sobre k.

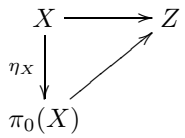
Sea A_1 una subálgebra separable de A, sea $d = \dim_k A_1$. Entonces, $A_1 \otimes_k \bar{k}$ es una subálgebra de $A \otimes_k \bar{k}$ generada por d elementos idempotentes. Ahora bien, $\mathrm{Esp}(A \otimes_k \bar{k})$ es un conjunto algebraico, luego tiene un número finito de componentes conexas, luego también un número finito de abiertos cerrados (las uniones de componentes conexas). El teorema [E 3.7] implica que $A \otimes_k \bar{k}$ tiene un número finito r de elementos idempotentes, y $d \leq r$.

Así pues, partimos de una subálgebra separable A_1 de A, si no contiene a todas las subálgebras separables de A, tomamos otra A_2 y formamos el producto A_1A_2, que es una nueva subálgebra separable de A de dimensión mayor. Como la dimensión no puede exceder r, tras un número finito de pasos llegaremos a una subálgebra separable de A que contiene a todas las demás. Esto prueba que A^s tiene dimensión finita sobre k. ∎

Teorema 10.8 *Si A_1 y A_2 son k-álgebras en las condiciones del teorema anterior, entonces $(A_1 \oplus A_2)^s = A_1^s \oplus A_2^s$.*

DEMOSTRACIÓN: Por una parte, $A_1^s \oplus A_2^s \subset A_1 \oplus A_2$ es una k-álgebra separable, luego $A_1^2 \oplus A_2^s \subset (A_1 \oplus A_2)^s$. Por otra parte, la imagen de $(A_1 \oplus A_2)^s$ por la proyección $A_1 \oplus A_2 \longrightarrow A_i$ ha de ser una subálgebra separable de A_i, luego ha de estar contenida en A_i^s, luego $(A_1 \oplus A_2)^s \subset A_1^s \oplus A_2^s$. ∎

Teorema 10.9 *Sea X/k un conjunto algebraico. Existe un esquema $\pi_0(X)$, finito y llano sobre k, y un k-homomorfismo $\eta_X : X \longrightarrow \pi_0(X)$ tal que, para todo k-homomorfismo $X \longrightarrow Z$ en un esquema finito y llano sobre k, se descompone de forma única como*



DEMOSTRACIÓN: Sea $U_1, \dots, U_n$ un cubrimiento afín de X, de modo que $\mathcal{O}_X(X) \subset \mathcal{O}_X(U_1) \oplus \cdots \oplus \mathcal{O}_X(U_n)$, y ésta es una k-álgebra finitamente generada. Por lo tanto, el teorema anterior nos da que existe $\mathcal{O}_X(X)^s$. Tomamos

$$\pi_0(X) = \operatorname{Esp} \mathcal{O}_X(X)^s,$$

y definimos $X \longrightarrow \pi_0(X)$ como el homomorfismo natural (determinado por el teorema [E 2.11]). Así, si dado un homomorfismo $X \longrightarrow Z$, donde Z/k es finito y llano, tenemos que $Z = \operatorname{Esp} A$, donde A es una k-álgebra separable, y tenemos un k-homomorfismo $A \longrightarrow \mathcal{O}_X(X)$. Su imagen es un cociente de A, luego es una k-álgebra separable, luego podemos factorizarlo de forma única como

$$\begin{array}{ccc} A & \longrightarrow & \mathcal{O}_X(X) \\ & \searrow & \uparrow \\ & & \mathcal{O}_X(X)^s \end{array}$$

De aquí se deduce la factorización del enunciado. ∎

Definición 10.10 Si X/k es un conjunto algebraico, el esquema $\pi_0(X)$ dado por el teorema anterior (que claramente es único salvo isomorfismo) se llama *esquema de componentes conexas* de X.

El teorema siguiente explica este nombre:

Teorema 10.11 *Sea X/k un conjunto algebraico y sea $X = X_1 \cup \cdots \cup X_n$ su descomposición en componentes conexas. Entonces*

$$\pi_0(X) = \pi_0(X_1) \cup \cdots \cup \pi_0(X_n),$$

la unión es disjunta, cada $\pi_0(X_i)$ consta de un único punto (abierto y cerrado en $\pi_0(X)$) y el homomorfismo $\eta_X : X \longrightarrow \pi_0(X)$ se restringe a los homomorfismos $\eta_{X_i} : X_i \longrightarrow \pi_0(X_i)$. En particular η_X es suprayectivo y, conjuntistamente, sus fibras son las componentes conexas de X.

DEMOSTRACIÓN: Claramente, $\mathcal{O}_X(X) = \mathcal{O}_X(X_1) \oplus \cdots \oplus \mathcal{O}_X(X_n)$, luego $\mathcal{O}_X(X)^s = \mathcal{O}_X(X_1)^s \oplus \cdots \oplus \mathcal{O}_X(X_n)^s$, luego $\pi_0(X) = \pi_0(X_1) \cup \cdots \cup \pi_0(X_n)$, unión disjunta.

Por el teorema [E 3.7], la k-álgebra $\mathcal{O}_X(X_i)$ no tiene más idempotentes que 0 y 1, luego $K_i = \mathcal{O}_X(X_i)^s$ ha de ser un cuerpo, una extensión finita separable de k, luego $\pi_0(X_i) = \operatorname{Esp} K_i$ consta de un único punto. El diagrama conmutativo

$$\begin{array}{ccc} \mathcal{O}_X(X)^s & \longrightarrow & \mathcal{O}_X(X) \\ \downarrow & & \downarrow \\ \mathcal{O}_X(X_i)^s & \longrightarrow & \mathcal{O}_X(X_i) \end{array}$$

da lugar a un diagrama conmutativo

$$\begin{array}{ccc} X & \longrightarrow & \pi_0(X) \\ \uparrow & & \uparrow \\ X_i & \longrightarrow & \pi_0(X_i) \end{array}$$

donde las flechas verticales son las inmersiones abiertas, luego f se restringe a los homomorfismos correspondientes para las componentes conexas. ∎

Nota En realidad, π_0 es un funtor de la categoría de los conjuntos algebraicos sobre k en la categoría de los conjuntos algebraicos finitos y llanos sobre k. Esto significa que, además de asignar el conjunto algebraico $\pi_0(X)$ a cada conjunto algebraico X, podemos asignar a cada k-homomorfismo $f : X \longrightarrow Y$ un k-homomorfismo $\pi_0(f) : \pi_0(X) \longrightarrow \pi_0(Y)$.

En efecto, f determina un homomorfismo de anillos $f_Y^\# : \mathcal{O}_Y(Y) \longrightarrow \mathcal{O}_X(X)$, que se restringe a un homomorfismo $\mathcal{O}_Y(Y)^s \longrightarrow \mathcal{O}_X(X)^s$, que a su vez determina el homomorfismo $\pi_0(f)$. Es inmediato comprobar que estas asignaciones son funtoriales, es decir, que son compatibles con la composición de homomorfismos. Más aún, es fácil ver que tenemos el diagrama conmutativo

$$\begin{array}{ccc} X & \xrightarrow{\eta_X} & \pi_0(X) \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \pi_0(f)} \\ Y & \xrightarrow[\eta_Y]{} & \pi_0(Y) \end{array}$$

lo que se interpreta como que $\eta : I \longrightarrow \pi_0$ es una transformación natural. ∎

Necesitamos un par de propiedades de π_0:

Teorema 10.12 *Si X/k es un conjunto algebraico y L/k es una extensión de cuerpos, entonces $\pi_0(X_L) \cong \pi_0(X) \times_k \operatorname{Esp} L$.*

Demostración: Por [E 6.15] tenemos que $\mathcal{O}_{X_L}(X_L) = \mathcal{O}_X(X) \otimes_k L$, luego, llamando $A = \mathcal{O}_X(X)$, lo que hemos de probar es que $(A \otimes_k L)^s \cong A^s \otimes_k L$.

Tenemos un monomorfismo $A^s \otimes_k L \longrightarrow A \otimes_k L$, y $A^s \otimes_k L$ es separable por 10.4. Por lo tanto, $A^s \otimes_k L \subset (A \otimes_k L)^s$.

En otras palabras, sabemos que $A^s \otimes_k L$ es una subálgebra separable de $A \otimes_k L$ y queremos probar que es la mayor subálgebra separable de $A \otimes_k L$. Si hubiera otra mayor, es decir, si tuviéramos $A^s \otimes_k L \subsetneq B \subset A \otimes_k L$, entonces tendríamos también $A^s \otimes_k \bar{L} \subsetneq B \otimes_L \bar{L} \subset A \otimes_k \bar{L}$ y, de nuevo por 10.4, $B \otimes_L \bar{L}$ sería una subálgebra separable de $A \otimes_k \bar{L}$, luego $A^s \otimes_k \bar{L}$ no sería la mayor álgebra separable de $A \otimes_k \bar{L}$. Así pues, no perdemos generalidad si suponemos que L es algebraicamente cerrado.

Veamos en primer lugar que $A^s \otimes_k k_s = (A \otimes_k k_s)^s$.

Observemos que $V = (A\otimes_k k_s)^s$ contiene a todos los elementos idempotentes de $A \otimes_k k_s$. Ello se debe a que si $e \in A \otimes_k k_s$ es idempotente, entonces la k-álgebra $k[e]$ es separable, pues es isomorfa a k o a $k \oplus k$.

Por otra parte, $V \cong k_s^n$. Si $e_1, \ldots, e_n$ es la base canónica de esta descomposición (que, en principio, no es canónica para V, pues no tenemos garantizado que el isomorfismo sea canónico), tenemos que $e_ie_i = e_i$, $e_ie_j = 0$, para $i \neq j$, y los únicos idempotentes de V son las sumas de distintos e_i. Por lo tanto, si $e \in V$ es cualquier idempotente, entonces $e_ie = e_i$ o bien $e_ie = 0$, y esta propiedad caracteriza a los idempotentes e_i.

Si $G = G(k_s/k)$, en los razonamientos previos al teorema 10.6 hemos visto que G actúa sobre $A \otimes_k k_s$, de modo que cada $\sigma \in G$ tiene asociado un automorfismo de $A \otimes_k k_s$ (como k-álgebra). En particular, σ conserva la propiedad que caracteriza a los idempotentes e_i, luego los permuta.

Además, los e_i han de estar contenidos en un subanillo $A \otimes_k L$, donde L/k es una extensión finita de Galois, luego la acción de G sobre la base de V es continua. Estamos, pues, en las condiciones del teorema 10.6, que nos asegura entonces que V está generada como k_s-álgebra por elementos fijados por G. También hemos visto que los elementos de $A \otimes_k k_s$ fijados por G son los de A, luego V está generada por elementos de $V \cap A \subset A^s$. Esta inclusión se debe a que si $x \in V \cap A$, entonces, la k-álgebra $k[x] \subset V$ es separable y, como $k[x] \subset A$, de hecho, $k[x] \subset A^s$, luego $x \in A^s$. Por consiguiente, $V \subset A^s \otimes_k k_s$.

Como $A^s \otimes_k L = (A^s \otimes_k k_s) \otimes_{k_s} L = (A \otimes_k k_s)^s \otimes_{k_s} L$, podemos cambiar k por k_s y suponer que k es separablemente cerrado.

Ahora vamos a probar que $A^s \otimes_k \bar{k} = (A \otimes_k \bar{k})^s$. Esto es trivial si $k = \bar{k}$, luego suponemos lo contrario, y esto existe que k tenga característica prima p.

Nuevamente, $(A \otimes_k \bar{k})^s$ está generada sobre $\bar{k}$ por elementos idempotentes. Sea e uno de ellos. Entonces

$$e = \sum_i a_i \otimes \alpha_i.$$

Como $\bar{k}/k$ es puramente inseparable, existe un natural n tal que $\alpha_i^{p^n} \in k$. Como e es idempotente, tenemos que

$$e = e^{p^n} = \sum_i a_i^{p^n} \otimes \alpha_i^{p^n} \in A \otimes_k k = A.$$

Como antes, esto significa que $e \in A \cap (A \otimes_k \bar{k})^s \subset A^s$, luego concluimos que $(A \otimes_k \bar{k})^s \subset A^s \otimes_k \bar{k}$.

Esto nos permite suponer ahora que $k = \bar{k}$. Observemos que esta reducción consiste simplemente en cambiar $A = \mathcal{O}_X(X)$ por $A \otimes_k \bar{k} = \mathcal{O}_{X_{\bar{k}}}(X_{\bar{k}})$. Equivalentemente, basta probar el teorema cuando k y L son cuerpos algebraicamente cerrados.

Ahora bien, si $X = X_1 \cup \cdots \cup X_n$ es la descomposición de X en componentes conexas, sabemos que $\pi_0(X)$ está formado por n puntos racionales, e igualmente, $\pi_0(X) \otimes_k L$ está formado por n puntos racionales (ahora sobre L). Basta probar

que $X_L = X_{1L} \cup \cdots \cup X_{nL}$ sigue teniendo n componentes conexas o, lo que es lo mismo, que cada X_{iL} sigue siendo conexo. Equivalentemente: basta probar que si X es conexo, también lo es X_L, pero esto es sencillo:

Si $X = X_1 \cup \cdots \cup X_n$ es la descomposición de X en componentes irreducibles, todas ellas son geométricamente irreducibles, luego $X_L = X_{1L} \cup \cdots \cup X_{nL}$ es la descomposición de X_L en componentes irreducibles. Las proyecciones $X_{iL} \longrightarrow X_i$ son suprayectivas, y si $X_i \cap X_j \neq \varnothing$, la intersección contiene un punto cerrado (racional) p, cuya fibra

$$X_{iL} \times_X \operatorname{Esp} k = \operatorname{Esp} L \times_k \operatorname{Esp} K = \operatorname{Esp} L$$

consta de un único punto $p \in X_{iL} \cap X_{jL}$. Esto implica claramente que X_L es conexo. ∎

Teorema 10.13 *Si X/k e Y/k son conjuntos algebraicos, entonces*

$$\pi_0(X \times_k Y) \cong \pi_0(X) \times_k \pi_0(Y).$$

Demostración: Sean $\{U_i\}_i$ y $\{V_j\}_j$ cubrimientos finitos de X e Y por abiertos afines. Las restricciones inducen k-monomorfismos de anillos

$$\mathcal{O}_X(X) \longrightarrow \bigoplus_i \mathcal{O}_X(U_i), \qquad \mathcal{O}_Y(Y) \longrightarrow \bigoplus_j \mathcal{O}_Y(V_j),$$

que a su vez inducen un k-monomorfismo

$$\mathcal{O}_X(X) \otimes_k \mathcal{O}_Y(Y) \longrightarrow \bigoplus_{i,j} \mathcal{O}_{X\times_k Y}(U_i \times_k V_j).$$

Ahora bien, cada elemento de la imagen de este k-monomorfismo determina un elemento de $\mathcal{O}_{X\times Y}(X \times_k Y)$, por lo que, de hecho, tenemos un k-monomorfismo

$$\mathcal{O}_X(X) \otimes_k \mathcal{O}_Y(Y) \longrightarrow \mathcal{O}_{X\times_k Y}(X \times_k Y).$$

A través de él podemos ver a $\mathcal{O}_X(X)^s \otimes_k \mathcal{O}_Y(Y)^s$ como una subálgebra separable de $\mathcal{O}_{X\times Y}(X \times Y)$, luego tenemos una inclusión

$$\mathcal{O}_X(X)^s \otimes_k \mathcal{O}_Y(Y)^s \subset (\mathcal{O}_{X\times_k Y}(X \times_k Y))^s.$$

El isomorfismo del enunciado equivale a la igualdad, y para probar la igualdad basta ver que ambos términos tienen la misma dimensión sobre k. Por el teorema anterior, estas dimensiones no se ven alteradas si cambiamos X e Y por $X_{\bar{k}}$ e $Y_{\bar{k}}$, respectivamente, luego no perdemos generalidad si suponemos que k es algebraicamente cerrado. En tal caso, lo que hemos de probar es que el número de componentes conexas de $X \times_k Y$ es el producto del número de componentes conexas de X por el número de componentes conexas de Y, lo cual se reduce inmediatamente a comprobar que si X e Y son conexos, también lo es $X \times_k Y$.

En efecto, si el producto tuviera dos componentes conexas, podríamos tomar puntos cerrados p y q, uno en cada una de ellas. Si $p_1 \in X$ es la proyección de

p, se trata de un punto cerrado, cuya fibra es $(X \times_k Y)_{p_1} = Y \times_k \operatorname{Esp} k = Y$, luego es conexa. Igualmente es conexa $(X \times_k Y)_{q_2} = X \times_k \operatorname{Esp} k = X$.

Por otra parte, la intersección de las fibras es la fibra de q_2 en $(X \times_k Y)_{p_1}$, es decir:

$$\operatorname{Esp} k \times_X (X \times_k Y) \times_Y \operatorname{Esp} k = \operatorname{Esp} k \times_k \operatorname{Esp} k = \operatorname{Esp} k,$$

luego la intersección no es vacía. Esto prueba que la unión de las fibras es un subespacio conexo de $X \times_k Y$ que contiene a p y a q, en contradicción con que pertenezcan a componentes conexas distintas. ∎

Nota En las pruebas de los dos teoremas precedentes hemos visto que

$$\mathcal{O}_{X_L}(X_L)^s \cong \mathcal{O}_X(X)^s \otimes_k L, \qquad (\mathcal{O}_{X\times_k Y}(X \times_k Y))^s = \mathcal{O}_X(X)^s \otimes_k \mathcal{O}_Y(Y)^s,$$

de donde se sigue inmediatamente que $\eta_{X_L} = \eta_X \times 1$, $\eta_{X\times_k Y} = \eta_X \times \eta_Y$. ∎

Teorema 10.14 *Si X/k es un conjunto algebraico, las componentes conexas de X que son geométricamente conexas se corresponden con los puntos racionales de $\pi_0(X)$. Si una componente conexa tiene un punto racional, entonces es geométricamente conexa.*

Demostración: Podemos suponer que X es conexo. Lo que hemos de probar es que X es geométricamente conexo si y sólo si el punto de $\pi_0(X)$ es racional. En principio, $\pi_0(X) = \operatorname{Esp} K$, donde K/k es una extensión finita separable. Por otra parte, el esquema X será geométricamente conexo si y sólo si $\pi_0(X_{\bar{k}}) = \pi_0(X)_{\bar{k}} = \operatorname{Esp}(K \otimes_k \bar{k})$ consta de un único punto.

Podemos representar $K = k[X]/(f(X))$, donde $f(X) \in k[X]$ es un polinomio separable. Entonces $K \otimes_k \bar{k} = \bar{k}[X]/(f(X))$, luego el número de puntos de $\operatorname{Esp}(K \otimes_k \bar{k})$ es el grado $|K : k|$.

Así pues, X es geométricamente conexo si y sólo si $K = k$, si y sólo si el punto de $\pi_0(X)$ es racional.

Por último, si X tiene un punto racional, su imagen en $\pi_0(X)$ también será racional, luego X será geométricamente conexo. ∎

10.2 Cambios de base planos

Recogemos en esta sección algunos resultados técnicos sobre cambios de base:

Teorema 10.15 *Sea X/S un esquema noetheriano y $T \longrightarrow S$ un cambio de base plano. Si $\mathcal{F}$ es un haz cuasicoherente en X, el diagrama conmutativo*

$$\begin{array}{ccc} X_T & \xrightarrow{f_T} & T \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle \pi} \\ X & \xrightarrow[f]{} & S \end{array}$$

induce un isomorfismo canónico $\pi^* f_* \mathcal{F} \longrightarrow (f_T)_* p^* \mathcal{F}$.

DEMOSTRACIÓN: Podemos definir un homomorfismo natural

$$\psi : f^* f_* \mathcal{F} \longrightarrow \mathcal{F}.$$

Explícitamente (teniendo en cuenta [E 5.8]), si $V \subset S$ y $U \subset f^{-1}[V]$ son abiertos afines, el homomorfismo

$$\psi_U : (f^* f_* \mathcal{F})(U) = \mathcal{M}(f^{-1}[V]) \otimes_{\mathcal{O}_S(V)} \mathcal{O}_{X(U)} \longrightarrow \mathcal{F}(U)$$

es el inducido por la restricción $\mathcal{F}(f^{-1}[V]) \longrightarrow \mathcal{F}(U)$. Aplicando p^* y el diagrama conmutativo obtenemos un homomorfismo

$$(f_T)^* \pi^* f_* \mathcal{F} = p^* f^* f_* \mathcal{F} \longrightarrow p^* \mathcal{F},$$

y aplicando $(f_T)_*$ obtenemos

$$(f_T)_* (f_T)^* \pi^* f_* \mathcal{F} \longrightarrow (f_T)_* p^* \mathcal{F}.$$

Por otra parte, llamando $\mathcal{M} = \pi^* f_* \mathcal{F}$, podemos definir un homomorfismo canónico

$$\phi : \mathcal{M} \longrightarrow g_* g^* \mathcal{M},$$

donde $g = f_T$, determinado por que, si $V' \subset T$ y $U' \subset g^{-1}[V']$ son abiertos afines, la composición

$$\mathcal{M}(V') \xrightarrow{\phi_{V'}} g^*(\mathcal{M})(g^{-1}[V']) \longrightarrow g^*(\mathcal{M})(U') = \mathcal{M}(V') \otimes_{\mathcal{O}_T(V')} \mathcal{O}_{X_T}(U')$$

es el homomorfismo natural.

Componiendo ambos homomorfismos obtenemos el homomorfismo buscado

$$\pi^* f_* \mathcal{F} \longrightarrow (f_T)_* p^* \mathcal{F}.$$

Falta probar que si T/S es plano, se trata de un isomorfismo. Para ello basta probar que lo es su restricción a un entorno afín de cada punto de T, que podemos tomarlo contenido en la antiimagen de un abierto afín en S. Así pues, no perdemos generalidad si suponemos que $S = \operatorname{Esp} A$ y $T = \operatorname{Esp} B$, donde B es una A-álgebra plana. Como los haces son cuasicoherentes, basta probar que el homomorfismo

$$(\pi^* f_* \mathcal{F})(T) \longrightarrow ((f_T)_* p^* \mathcal{F})(T)$$

es un isomorfismo.

Fijamos un abierto afín $U \subset X$ y llamamos $U' = p^{-1}[U] = U_T \subset X_T$, que también es afín. Partimos del homomorfismo

$$\phi_U : (f^* f_* \mathcal{F})(U) = \mathcal{F}(X) \otimes_A \mathcal{O}_X(U) \longrightarrow \mathcal{F}(U)$$

inducido por la restricción. El homomorfismo

$$(f_T)^* \pi^* f_* \mathcal{F} = p^* f^* f_* \mathcal{F} \longrightarrow p^* \mathcal{F},$$

sobre el abierto $p^{-1}[U]$ se corresponde con el homomorfismo

$$\mathcal{F}(X) \otimes_A \mathcal{O}_{X_T}(p^{-1}[U]) \longrightarrow \mathcal{F}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{O}_{X_T}(p^{-1}[U])$$

inducido por la restricción o, también, con

$$\mathcal{F}(X) \otimes_A \mathcal{O}_X(U) \otimes_A B \longrightarrow \mathcal{F}(U) \otimes_A B.$$

A su vez, el homomorfismo

$$g_*g^*\mathcal{M} = (f_T)_*(f_T)^*\pi^*f_*\mathcal{F} \longrightarrow (f_T)_*p^*\mathcal{F}$$

sobre T es el homomorfismo

$$((f_T)^*\pi^*f_*\mathcal{F})(X_T) \longrightarrow (p^*\mathcal{F})(X_T),$$

que está determinado por sus restricciones a los abiertos $p^{-1}[U]$, que acabamos de calcular. Hemos de componer este homomorfismo con

$$\phi_T : \mathcal{M}(T) \longrightarrow (g_*g^*\mathcal{M})(T) = (g^*\mathcal{M})(X_T).$$

Tenemos el diagrama conmutativo

$$\begin{array}{ccccc} \mathcal{M}(T) & \xrightarrow{\phi_T} & (g^*\mathcal{M})(X_T) & \longrightarrow & (p^*\mathcal{F})(X_T) \\ & \searrow & \downarrow & & \downarrow \\ & & (g^*\mathcal{M})(U_T) & \longrightarrow & (p^*\mathcal{F})(U_T) \end{array}$$

Hemos de probar que la fila superior es un isomorfismo y sabemos calcular la fila inferior, que es el homomorfismo inducido por la restricción:

$$\mathcal{M}(T) = \mathcal{F}(X) \otimes_A B \longrightarrow \mathcal{F}(X) \otimes_A \mathcal{O}_X(U) \otimes_A B \longrightarrow \mathcal{F}(U) \otimes_A B.$$

Por último, como X_T/X es plano, el teorema [E 6.15] nos da que el homomorfismo canónico $\mathcal{M}(T) = \mathcal{F}(X) \otimes_A B \longrightarrow (p^*\mathcal{F})(X_T)$ es un isomorfismo, pero este isomorfismo extiende a los homomorfismos anteriores, luego es necesariamente la fila superior del diagrama. ∎

Teorema 10.16 *Sea $f : X \longrightarrow Y$ un homomorfismo entre esquemas noetherianos definidos sobre un esquema S y $T \longrightarrow S$ un cambio de base plano. Sea $Z \subset Y$ la imagen de f (es decir, el subesquema cerrado dado por* [E 2.33]*). Entonces, la imagen de $f_T : X_T \longrightarrow Y_T$ es el subesquema cerrado Z_T.*

Demostración: A través del isomorfismo $X_T = X \times_Y Y_T$, el homomorfismo f_T se corresponde con la proyección y Z_T se corresponde con $Z \times_Y Y_T$. Teniendo en cuenta que Y_T es plano sobre Y, basta probar el teorema en el caso en que $Y = S$.

En la prueba de [E 2.33] se ve que Z es el subesquema cerrado determinado por el núcleo $\mathcal{I}$ del homomorfismo $f^\# : \mathcal{O}_S \longrightarrow f_*\mathcal{O}_X$. Tenemos entonces una sucesión exacta de haces cuasicoherentes:

$$0 \longrightarrow \mathcal{I} \longrightarrow \mathcal{O}_S \longrightarrow f_*\mathcal{O}_X.$$

También es exacta la sucesión:

$$0 \longrightarrow \pi^*\mathcal{I} \longrightarrow \mathcal{O}_T \longrightarrow \pi^* f_*\mathcal{O}_X,$$

pues, para cada $t \in T$, la sucesión local correspondiente es

$$0 \longrightarrow \mathcal{I}_s \otimes_{\mathcal{O}_{S,s}} \mathcal{O}_{T,t} \longrightarrow \mathcal{O}_{S,s} \otimes_{\mathcal{O}_{S,s}} \mathcal{O}_{T,t} \longrightarrow (f_*\mathcal{O}_X)_t \otimes_{\mathcal{O}_{S,s}} \mathcal{O}_{T,t},$$

donde $s = \pi(t)$, y es exacta porque $\mathcal{O}_{T,t}$ es plano sobre $\mathcal{O}_{S,s}$.

Se comprueba inmediatamente la conmutatividad del diagrama

$$\begin{array}{ccc} \mathcal{O}_T & \xrightarrow{f_T^\#} & (f_T)_*\mathcal{O}_{X_T} \\ & \searrow & \uparrow \\ & & \pi^* f_*\mathcal{O}_X \end{array}$$

donde la flecha vertical es el isomorfismo definido en el teorema anterior. Así concluimos que $\pi^*\mathcal{I}$ es el núcleo de $f_T^\#$, luego define la estructura de esquema de la imagen de f_T y, por otra parte, llamando $i : Z \longrightarrow S$ a la inmersión cerrada, podemos repetir el razonamiento con la sucesión exacta

$$0 \longrightarrow \mathcal{I} \longrightarrow \mathcal{O}_S \longrightarrow i_*\mathcal{O}_Z,$$

de la que deducimos la sucesión exacta

$$0 \longrightarrow \pi^*\mathcal{I} \longrightarrow \mathcal{O}_T \longrightarrow \pi^* i_*\mathcal{O}_Z,$$

y de ella concluimos que $\pi^*\mathcal{I}$ es el núcleo de $i_T^\#$, luego define la estructura de esquema de Z_T. En definitiva, llegamos a que Z_T es la imagen de f_T. ∎

Teorema 10.17 *Sea S un anillo localmente noetheriano y $T \longrightarrow S$ un cambio de base plano y suprayectivo. Si $g : X \longrightarrow Y$ es un homomorfismo de S-esquemas noetherianos separados tal que $g_T : X_T \longrightarrow Y_T$ es un isomorfismo, entonces g también es un isomorfismo.*

Demostración: No perdemos generalidad si suponemos que $S = \operatorname{Esp} D$ y $g = \operatorname{Esp} E$, $Y = \operatorname{Esp} A$, donde E es una D-álgebra fielmente plana. Basta probar que X también es afín, pues en tal caso g se corresponde con un homomorfismo de D-álgebras $A \longrightarrow B$ tal que $A \otimes_D E \longrightarrow B \otimes_D E$ es un isomorfismo. Como E es fielmente plano sobre D, esto implica que $A \longrightarrow B$ también es un isomorfismo, luego también lo es g.

Como Y_E es afín y g_E es un isomorfismo, resulta que X_E también es afín. En definitiva, hemos de probar que si $X \times_D \operatorname{Esp} E$ es afín, entonces X también es afín.

Por el teorema de Serre [E 6.17], basta probar que si $\mathcal{M}$ es un haz coherente en X entonces $H^1(X, \mathcal{M}) = 0$. Ahora bien, según el teorema [E 6.15] tenemos que

$$H^1(X, \mathcal{M}) \otimes_D E \cong H^1(X_E, \mathcal{M}_E) = 0,$$

precisamente por [E 6.17]. Nuevamente, el hecho de que E sea fielmente plano sobre D implica que $H^1(X, \mathcal{M}) = 0$. ∎

Combinando los dos resultados anteriores podemos probar:

Teorema 10.18 *Sea S un esquema localmente noetheriano y $T \longrightarrow S$ un cambio de base plano y suprayectivo. Sean X/S e Y/S esquemas íntegros, separados de tipo finito sobre S tales que X_T e Y_T sean íntegros. Consideremos una aplicación racional $f : X \longrightarrow Y$ definida sobre S. Si $f_T : X_T \longrightarrow Y_T$ está definida sobre todo X_T, entonces f está definida sobre todo X.*

Demostración: Sea U el dominio de definición de f. Observemos que $X_T \times_T Y_T \cong (X \times_S Y)_T$ y que, a través de este isomorfismo, el homomorfismo $U_T \longrightarrow X_T \times_T Y_T$ dado por (i_T, f_T) se corresponde con $(i, f)_T$, luego tenemos el diagrama conmutativo

$$\begin{array}{ccc} U_T & \longrightarrow & (X \times_S Y)_T \\ \downarrow & & \downarrow \\ U & \longrightarrow & X \times_S Y \end{array}$$

El teorema 10.16 nos da que $\Gamma_{f_T} = (\Gamma_f)_T$ y, por lo tanto, tenemos el diagrama conmutativo

$$\begin{array}{ccc} \Gamma_{f_T} & \longrightarrow & X_T \\ \downarrow & & \downarrow \\ \Gamma_f & \longrightarrow & X \end{array}$$

Si f_T está definida en todo X_T, la flecha superior es un isomorfismo, luego la flecha inferior también lo es, por el teorema anterior, luego f está definida en todo X. ∎

Veamos otra variante:

Teorema 10.19 *Sea S un esquema localmente noetheriano, sean X'/S, X/S e Y/S esquemas íntegros, separados de tipo finito sobre S. Consideremos una aplicación racional $f : X \longrightarrow Y$ definida sobre S y supongamos que $g : X' \longrightarrow X$ es un homomorfismo plano y suprayectivo tal que la composición $f' : X' \longrightarrow Y$ esté definida sobre todo X'. Entonces f está definida sobre todo X.*

DEMOSTRACIÓN: Sea U el dominio de definición de f. Entonces tenemos el diagrama conmutativo

$$\begin{array}{ccc} g^{-1}[U] & \xrightarrow{(1,f')} & X' \times_S Y \\ \downarrow & & \downarrow \\ X' \times_X U & \longrightarrow & X' \times_X (X \times_S Y) \\ \downarrow & & \downarrow \\ U & \xrightarrow[(1,f)]{} & X \times_S Y \end{array}$$

donde las flechas verticales superiores son isomorfismos. El teorema 10.16 nos permite identificar $\Gamma_{f'} = X' \times_X \Gamma_f$, y tenemos el diagrama conmutativo

$$\begin{array}{ccc} \Gamma_{f'} & \longrightarrow & X' \\ \downarrow & & \downarrow \\ \Gamma_f & \longrightarrow & X \end{array}$$

Si f' está definida en todo X', la flecha superior es un isomorfismo, luego por 10.17 también lo es la flecha inferior, luego f está definida en todo X. ∎

10.3 Esquemas de grupos

Recordemos que el objetivo de este capítulo es dotar de estructura de grupo al abierto de los puntos suaves del modelo regular minimal de una curva elíptica. Para ello necesitamos una noción de "grupo algebraico" más general que la dada, por ejemplo, en [E 11.12], que era válida únicamente para conjuntos algebraicos:

Definición 10.20 Un *esquema de grupos* sobre un esquema S es un esquema G/S junto con tres homomorfismos $m : G \times_S G \longrightarrow G$, $i : G \longrightarrow G$, $e : S \longrightarrow G$, definidos sobre S, que hacen conmutativos los diagramas siguientes:

$$\begin{array}{ccc} G \times_S G \times_S G & \xrightarrow{m\times 1} & G \times_S G \\ {\scriptstyle 1\times m}\downarrow & & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow[m]{} & G \end{array} \qquad \begin{array}{ccc} S \times_S G & \xrightarrow{e\times 1} & G \times_S G \\ & \searrow & \downarrow{\scriptstyle m} \\ & & G \end{array}$$

$$\begin{array}{ccc} G \times_S S & \xrightarrow{1\times e} & G \times_S G \\ & \searrow & \downarrow{\scriptstyle m} \\ & & G \end{array} \qquad \begin{array}{ccccc} G & \xrightarrow{\Delta} & G \times_S G & \xrightarrow[i\times 1]{1\times i} & G \times_S G \\ \downarrow & & & & \downarrow{\scriptstyle m} \\ S & & \xrightarrow[e]{} & & G \end{array}$$

Diremos que G/T es un *esquema de grupos abelianos* si además conmuta el diagrama

$$\begin{array}{ccc} G \times_S G & \xrightarrow{(p_2,p_1)} & G \times_S G \\ & \searrow^{m} & \downarrow{\scriptstyle m} \\ & & G \end{array}$$

Estos diagramas garantizan que, si T/S es un esquema arbitrario, la operación $\bar{m}_T : G(T) \times G(T) \longrightarrow G(T)$ inducida por m de forma natural convierte al conjunto de secciones $G(T)$ en un grupo (abeliano en el caso de un esquema de grupos abelianos).

Por otra parte, los cambios de base $m_T : G_T \times_T G_T \longrightarrow G_T$, $i_T : G_T \longrightarrow G_T$, $e_T : T \longrightarrow G_T$, convierten claramente a G_T/T en un esquema de grupos.

En particular, si $S = \operatorname{Esp} k$ y G/k es una variedad algebraica sobre k, entonces G es un grupo algebraico en el sentido de [E 11.12] y, recíprocamente, todo grupo algebraico G/k en este sentido es un esquema de grupos, pues el teorema [E 3.67] garantiza la conmutatividad de los diagramas de la definición.

En general, llamaremos *grupos algebraicos* a los esquemas de grupos de tipo finito sobre un cuerpo, es decir, que son conjuntos algebraicos (no necesariamente irreducibles o reducidos).

De las dos últimas observaciones se sigue que las fibras de un esquema de grupos G/S son grupos algebraicos.

Ejemplo En $A^1_k = \operatorname{Esp} k[X]$ podemos considerar la estructura de grupo algebraico determinada por el homomorfismo $m : A^1_k \times_k A^1_k \longrightarrow A^1_k$ inducido por el homomorfismo de anillos $k[X] \longrightarrow k[Y, Z]$ dado por $X \mapsto Y + Z$, donde el homomorfismo inverso es el inducido por el homomorfismo $k[X] \longrightarrow k[X]$ dado por $X \mapsto -X$ y en el que $e : \operatorname{Esp} k \longrightarrow A^1_k$ es el homomorfismo inducido por el homomorfismo $k[X] \longrightarrow k$ dado por $X \mapsto 0$.

Es evidente que estos homomorfismos inducen en $A^1_k(\bar{k}) = \bar{k}$ la estructura del grupo aditivo de $\bar{k}$, por lo que A^1_k es ciertamente un grupo algebraico con esta estructura. Lo llamaremos el *grupo aditivo* de k. ∎

Ejemplo En $U_k = A^1_k \setminus \{0\} = \operatorname{Esp} k[X, 1/X]$ podemos considerar la estructura de grupo algebraico determinada por el homomorfismo $m : U_k \times_k U_k \longrightarrow U_k$ inducido por el homomorfismo de anillos $k[X, 1/X] \longrightarrow k[Y, Z, 1/Y, 1/Z]$ dado por $X \mapsto YZ$, donde el homomorfismo inverso es el inducido por el homomorfismo $k[X, 1/X] \longrightarrow k[X, 1/X]$ dado por $X \mapsto 1/X$ y en el que $e : \operatorname{Esp} k \longrightarrow U_k$ es el homomorfismo inducido por el homomorfismo $k[X, 1/X] \longrightarrow k$ dado por $X \mapsto 1$.

Es evidente que estos homomorfismos inducen en $U_k(\bar{k}) = \bar{k}^*$ la estructura del grupo multiplicativo de $\bar{k}$, por lo que U_k es ciertamente un grupo algebraico con esta estructura. Lo llamaremos el *grupo multiplicativo* de k. ∎

Definición 10.21 Un homomorfismo $f : G \longrightarrow H$ entre dos esquemas de grupos sobre S es un *homomorfismo de esquemas de grupos* si hace conmutativos los diagramas obvios:

$$\begin{array}{ccc} G \times_k G & \xrightarrow{m} & G \\ {\scriptstyle f\times f}\downarrow & & \downarrow{\scriptstyle f} \\ H \times_k H & \xrightarrow[m]{} & H \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{i} & G \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ H & \xrightarrow[i]{} & H \end{array} \qquad \begin{array}{ccc} S & \xrightarrow{e} & G \\ & {\scriptstyle e}\searrow & \downarrow{\scriptstyle f} \\ & & H \end{array}$$

Teorema 10.22 *Todo grupo algebraico sobre A^1_k es isomorfo al grupo aditivo de k.*

Demostración: Sea $k[X] \longrightarrow k$ el homomorfismo que determina el elemento neutro y sea $a \in k$ la imagen de X. Es claro que el homomorfismo $k[X] \longrightarrow k[X]$ dado por $X \mapsto X - a$ determina un isomorfismo $\phi : A^1_k \longrightarrow A^1_k$ a través del cual la estructura de grupo algebraico dada se transforma en otra estructura isomorfa para la cual ϕ es un isomorfismo, y para la nueva estructura, el elemento neutro está determinado por el homomorfismo $k[X] \longrightarrow k$ que cumple $X \mapsto 0$. El teorema quedará probado si vemos que, bajo esta hipótesis adicional, la estructura de grupo algebraico dada es exactamente la del grupo aditivo de k.

Consideremos el homomorfismo $k[X] \longrightarrow k[Y, Z]$ que induce la operación de la estructura dada y sea $P(Y, Z) \in k[Y, Z]$ la imagen de X. Entonces, la estructura de grupo algebraico inducida en $A^1_{\bar{k}}$ está asociada al homomorfismo $\bar{k}[X] \longrightarrow \bar{k}[Y, Z]$ determinada igualmente por que $X \mapsto P(Y, Z)$. Un punto racional de $A^1_{\bar{k}} \times_{\bar{k}} A^1_{\bar{k}}$ es de la forma $\mathfrak{p} = (Y - a, Z - b)$, y su imagen por m es el ideal $(X - P(a, b))$, pues, ciertamente, este ideal contiene a la antiimagen de $\mathfrak{p}$ y es maximal. Así pues, si identificamos $A^1_{\bar{k}} = \bar{k}$, lo que tenemos es que la aplicación $\bar{k} \times \bar{k} \longrightarrow \bar{k}$ dada por $(a, b) \mapsto P(a, b)$ determina una estructura de grupo en $\bar{k}$. Sabemos además que el elemento neutro es el punto 0.

Pongamos que $P(Y, Z) = \sum_{i=0}^{n} P_i(Z)Y^i$, para ciertos $P_i(Z) \in k[Z]$. Para cada $z \in \bar{k}$, la aplicación $y \mapsto P(y, z)$ ha de ser biyectiva y, más aún, ha de venir inducida por un isomorfismo de esquemas, que necesariamente ha de venir inducido a su vez por el homomorfismo $\bar{k}[Y] \longrightarrow \bar{k}[Y]$ dado por $Y \mapsto P(Y, z)$. Este homomorfismo ha de ser un automorfismo de $\bar{k}[Y]$, luego $P(Y, z)$ ha de ser irreducible en $\bar{k}[Y]$, luego ha de ser un polinomio de grado 1. Así pues, todos los polinomios $P_i(Z)$ son idénticamente nulos para $i \geq 2$. Por lo tanto, $P(Y, Z) = P_1(Z)Y + P_0(Z)$.

Como $P(0, Z) = Z$, ha de ser, más concretamente, $P(Y, Z) = P_1(Z)Y + Z$. Intercambiando el papel de Y con el de Z concluimos que $P(Y, Z) = Y + Z$, con lo que la estructura de grupo algebraico dada es la del grupo aditivo de k. ∎

Observemos que de la prueba del teorema anterior se sigue que si dos estructuras de grupo sobre A^1_k tienen el mismo elemento neutro, entonces son idénticas.

Teorema 10.23 *Todo grupo algebraico sobre $U_k = \operatorname{Esp} k[X, 1/X]$ es isomorfo al grupo multiplicativo de k.*

DEMOSTRACIÓN: Si el elemento neutro de la estructura dada viene inducido por el homomorfismo $k[X, 1/X] \longrightarrow k$ que cumple $X \mapsto a$, ha de ser $a \neq 0$ pues su tiene por inverso a la imagen de $1/X$, por lo que podemos definir un isomorfismo $k[X, 1/X] \longrightarrow k[X, 1/X]$ mediante $X \mapsto X/a$. Este isomorfismo induce un isomorfismo $U_k \longrightarrow U_k$ que permite definir una estructura de grupo algebraico isomorfa a la dada pero que cumple además que su elemento neutro está inducido por el homomorfismo que cumple $X \mapsto 1$. Basta probar que, con esta hipótesis adicional, la estructura dada es idéntica a la del grupo multiplicativo de k.

Consideremos el homomorfismo $k[X, 1/X] \longrightarrow k[Y, Z, 1/Y, 1/Z]$ que induce la operación del grupo, y sea $P(Y, Z)$ la imagen de X. Como X es una unidad en $k[X, 1/X]$, también $P(Y, Z)$ ha de ser una unidad en $k[Y, Z, 1/Y, 1/Z]$, lo que implica que es de la forma $P(Y, Z) = aX^rY^s$, para ciertos r, $s \in \mathbb{Z}$, $a \in k^*$.

Razonando igual que en el teorema anterior, concluimos que la aplicación $\bar{k}^* \times \bar{k}^* \longrightarrow \bar{k}^*$ dada por $(y, z) \mapsto ay^rz^r$ determina una estructura de grupo en k^* cuyo elemento neutro es 1. Esto implica inmediatamente que ha de ser $P(Y, Z) = YZ$, por lo que la estructura de grupo algebraico es la del grupo multiplicativo de k. ∎

Observemos que, como en el caso del teorema precedente, la prueba del teorema anterior muestra que si dos estructuras de grupo algebraico sobre U_k tienen el mismo elemento neutro, entonces son idénticas.

Teorema 10.24 *Si G/k es un grupo algebraico, la componente conexa G^0 que contiene al elemento neutro es un subgrupo abierto (y cerrado).*

DEMOSTRACIÓN: Claramente G^0 es abierto en G (lo que lo dota automáticamente de estructura de esquema). Que sea un subgrupo significa, por definición, que m e i se restringen a homomorfismos $m : G^0 \times_k G^0 \longrightarrow G^0$, $i : G^0 \longrightarrow G^0$ (así como que $e : \operatorname{Esp} k \longrightarrow G$ tiene su imagen en G^0, lo cual es cierto por definición de G^0).

Como G^0 es conexo, es claro que $i[G^0]$ ha de ser un subconjunto conexo de G, luego está contenido en una componente conexa. Como contiene la imagen de $e \circ i = e$, ha de ser $i[G^0] \subset G^0$, lo cual, teniendo en cuenta que G^0 es abierto, implica fácilmente que i se restringe a un homomorfismo $G^0 \longrightarrow G^0$.

Con m razonamos igualmente, pero para ello hemos de probar que $G^0 \times_k G^0$ es conexo. Esto se debe a que

$$\pi_0(G^0 \times_k G^0) = \pi_0(G^0) \times_k \pi_0(G^0) = \operatorname{Esp} k \times_k \operatorname{Esp} k = \operatorname{Esp} k,$$

ya que G^0 contiene un punto racional (el neutro), luego su imagen en $\pi_0(G^0)$ ha de ser racional, luego $\pi_0(G^0) = \operatorname{Esp} k$. ∎

No es fácil definir el concepto de grupo cociente para esquemas de grupos. (En realidad sí que es fácil, pero lo difícil es demostrar que existen cocientes.)

No obstante, el cociente G/G^0 "debería ser" el conjunto de las componentes conexas de G, y la estructura de esquema más adecuada para este conjunto es la que ya tenemos definida: $\pi_0(G)$. No vamos a probar esto completamente, pero el teorema siguiente contiene una parte de lo que ello supondría:

Teorema 10.25 *Si G/k es un grupo algebraico, existe una única estructura de grupo algebraico en $\pi_0(G)$ tal que el homomorfismo natural $\eta_G : G \longrightarrow \pi_0(G)$ es un homomorfismo de grupos.*

DEMOSTRACIÓN: Tenemos diagramas conmutativos:

$$\begin{array}{ccc} G \times_k G & \xrightarrow{m} & G \\ \downarrow & & \downarrow \\ \pi_0(G) \times_k \pi_0(G) & \xrightarrow[m_0]{} & \pi_0(G) \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{i} & G \\ \downarrow & & \downarrow \\ \pi_0(G) & \xrightarrow[i_0]{} & \pi_0(G) \end{array}$$

donde $m_0 = \pi_0(m)$, $i_0 = \pi_0(i)$. Es fácil ver que m_0 e i_0, juntamente con $e_0 : \operatorname{Esp} k \longrightarrow G \longrightarrow \pi_0(G)$, determinan una estructura de grupo algebraico en $\pi_0(G)$. Por ejemplo, para probar la asociatividad se forma un diagrama cúbico del que deducimos que los dos homomorfismos

$$G \times_k G \times_k G \longrightarrow \pi_0(G) \times_k \pi_0(G) \times_k \pi_0(G) \xrightarrow{u,v} \pi_0(G)$$

coinciden. Estos corresponden con homomorfismos de anillos

$$\mathcal{O}_G(G)^s \xrightarrow{f,g} \mathcal{O}_G(G)^s \otimes_k \mathcal{O}_G(G)^s \otimes_k \mathcal{O}_G(G)^s \longrightarrow \mathcal{O}_G(G) \otimes_k \mathcal{O}_G(G) \otimes_k (\mathcal{O}_G(G).$$

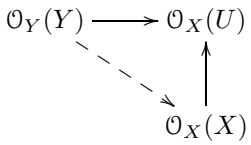
Como el último homomorfismo es un monomorfismo, concluimos que $f = g$, luego $u = v$. Similarmente sucede con los demás diagramas necesarios. Los diagrama indicados al principio de la prueba demuestran ahora que η_G es un homomorfismo de grupos. ∎

Terminamos la sección demostrando una generalización de un teorema de Weil que necesitaremos más adelante para caracterizar los modelos de Néron. Antes necesitamos probar el siguiente hecho elemental:

Teorema 10.26 *Sea $u : X \longrightarrow Y$ una aplicación racional de un esquema normal localmente noetheriano X en un esquema afín Y. Entonces, todas las componentes irreducibles del conjunto de los puntos donde u no está definida tienen codimensión 1 en X.*

DEMOSTRACIÓN: Sea U el dominio de definición de X y sea $Z = X \setminus U$. Sea Z' la unión de las componentes irreducibles de Z que tengan codimensión mayor que 1 en X y sea $X' = X \setminus Z'$. Entonces, podemos ver también a u como aplicación racional $u : X' \longrightarrow Y$, y hemos de probar que u está definida sobre todo X'. Equivalentemente, podemos suponer que u está definida sobre todos los puntos de codimensión 1 de X y demostrar que u está definida sobre todo X.

Según [E 2.11], el homomorfismo $u : U \longrightarrow Y$ está determinado por el homomorfismo de anillos asociado $\mathcal{O}_Y(Y) \longrightarrow \mathcal{O}_X(U)$, y lo que queremos es encontrar un homomorfismo que haga conmutativo el diagrama siguiente:



Ahora bien, esto es trivial, porque [E 7.5] implica que la restricción (la flecha vertical) es un isomorfismo. ∎

Teorema 10.27 *Sea S un esquema noetheriano normal y $u : Z \longrightarrow G$ una aplicación racional definida sobre S de un esquema íntegro suave Z/S en un esquema de grupos íntegro y separado G/S. Si u está definida sobre los puntos de codimensión 1 y sobre los puntos cuasigenéricos de todas las fibras, entonces está definida sobre todo Z.*

Demostración: Sea $s \in S$ y consideremos la aplicación racional

$$u_s : Z \times_S \operatorname{Esp} \mathcal{O}_{S,s} \longrightarrow G \times_S \operatorname{Esp} \mathcal{O}_{S,s}.$$

Si probamos que está definida sobre todo $Z \times_S \operatorname{Esp} \mathcal{O}_{S,s}$, el teorema 7.2 nos da un entorno U de s y un homomorfismo

$$Z \times_S U \longrightarrow G \times_S U$$

que induce a u_s. (No es necesario que Z sea separado, esta hipótesis sólo se usa en 7.2 para probar que a partir de un isomorfismo se obtiene un isomorfismo.)

Este homomorfismo puede verse como una aplicación racional $Z \longrightarrow G$ definida sobre toda la fibra Z_s y sobre la fibra genérica. Además, sobre (un abierto de) la fibra genérica coincide con u, luego por 5.26 coincide con u en todo su dominio.

Claramente, u_s satisface las mismas hipótesis que u, luego no perdemos generalidad si suponemos que el esquema S es local. Sea s su punto cerrado y sea $H \subset G$ un entorno afín de $e(s)$. Entonces, para todo $s' \in S$, tenemos que s está en la clausura de s', luego $e(s') \in H$, luego podemos considerar la sección e como un homomorfismo $e : S \longrightarrow H$.

Como $Z \times_S Z$ es suave sobre Z, el teorema 1.20 (ver el principio de la prueba) nos da que $Z \times_S Z$ es unión de componentes conexas normales (abiertas y cerradas). Sea $W \subset Z \times_S Z$ la componente conexa que contiene a la diagonal Δ.

Consideremos la aplicación racional $v : W \longrightarrow G$ definida por composición:

$$W \xrightarrow{u \times u} G \times_S G \xrightarrow{(1,i)} G \times_S G \xrightarrow{m} G.$$

Sea $U \subset Z$ el dominio de u y $V \subset W \subset Z \times_S Z$ el dominio de v. Claramente $W \cap (U \times_S U) \subset V$. Vamos a probar que V contiene a Δ. Notemos que podemos identificar de forma natural $\Delta = Z$, y así, podemos afirmar que

$$V \cap \Delta \supset (U \times_S U) \cap \Delta = U.$$

Consideremos el diagrama conmutativo:

$$\begin{array}{ccccccc} U \times_S U & \xrightarrow{u\times u} & G \times_S G & \xrightarrow{1\times i} & G \times_S G & \xrightarrow{m} & G \\ \Delta\uparrow & & \Delta\uparrow & & & \nearrow_{e} & \\ U & \xrightarrow[u]{} & G & \longrightarrow & S & & \end{array}$$

Vemos así que $v|_U = \pi|_U \circ e$, donde llamamos π al homomorfismo estructural de Z/S. Esto implica que, como aplicaciones racionales, $v|_{V\cap\Delta} = \pi \circ e$.

Consideremos ahora la aplicación racional $v' : W \longrightarrow H$ definida por la restricción de v a $v^{-1}[H]$. Llamemos $V' \subset V$ a su dominio de definición. Como $v[V \cap \Delta] \subset e[S] \subset H$, tenemos que $V \cap \Delta \subset V'$, luego, más precisamente, $V \cap \Delta = V' \cap \Delta$.

De este modo, si llamamos $F = W \setminus V'$, la inclusión $\Delta \subset V$ que queremos probar equivale a que $\Delta \cap F = \varnothing$. Hemos hecho esta reducción para aplicar el teorema 10.26, que nos da que las componentes irreducibles de F tienen todas codimensión 1 en W.

Supongamos que existe $x \in \Delta \cap F$. Entonces

$$\dim \mathcal{O}_{F,x} = \dim \mathcal{O}_{W,x} - 1.$$

Por otra parte, por hipótesis, todas las componentes irreducibles de $\Delta \setminus U$ tienen codimensión ≥ 2 en Δ y, como $\Delta \cap F \subset \Delta \setminus U$, tenemos que

$$\dim \mathcal{O}_{\Delta,x} - \dim \mathcal{O}_{\Delta\cap F,x} \geq 2.$$

Como Z/S es suave, es localmente una intersección completa, luego el teorema [E 7.71] nos da que la diagonal $\Delta : Z \longrightarrow Z \times_S Z$ es una inmersión regular. Así pues,

$$\mathcal{O}_{\Delta,x} = \mathcal{O}_{W,x}/(f_1, \ldots, f_d),$$

donde $d = \dim \mathcal{O}_{W,x} - \dim \mathcal{O}_{\Delta,x}$. Por consiguiente,

$$\mathcal{O}_{\Delta\cap F,x} = \mathcal{O}_{F,x}/(\bar{f}_1, \ldots \bar{f}_d),$$

donde $\bar{f}_i$ es la imagen de f_i en $\mathcal{O}_{F,x}$ y, por el teorema de los ideales principales:

$$\dim \mathcal{O}_{F,x} - \dim \mathcal{O}_{\Delta\cap F,x} \leq d.$$

Uniendo las desigualdades que hemos obtenido llegamos a una contradicción:

$$2 \leq \dim \mathcal{O}_{\Delta,x} - \dim \mathcal{O}_{\Delta\cap F,x} = \dim \mathcal{O}_{W,x} - d - \dim \mathcal{O}_{\Delta\cap F,x}$$

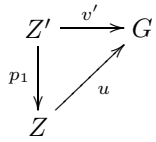
$$\leq \dim \mathcal{O}_{W,x} - \dim \mathcal{O}_{F,x} = 1.$$

Así pues, concluimos que $\Delta \subset V$.

Consideremos ahora $Z' = V \cap (Z \times_S U)$ y sean $p_1, p_2 : Z' \longrightarrow Z$ las proyecciones. Sobre Z' está definido el homomorfismo

$$v' : Z' \xrightarrow{(1,p_2)} V \times_S U \xrightarrow{v\times u} G \times_S G \xrightarrow{m} G.$$

Tenemos el diagrama conmutativo



pues ambas aplicaciones racionales coinciden sobre el abierto $Z' \cap (U \times_S U)$. Como U es suave sobre S, tenemos que Z' es suave sobre Z y, en particular, es plano. Por el teorema 10.19, si probamos que p_1 es suprayectiva, podremos concluir que u está definido sobre todo Z y el teorema estará probado.

Para ello tomamos un punto $x \in Z$ y vamos a ver que la fibra Z'_x no es vacía. Esta fibra es la intersección en

$$(Z \times_S Z)_x = Z \times_S \operatorname{Esp} k(x) = (Z_s)_{k(x)}$$

del abierto $(U_s)_{k(x)}$ con el abierto correspondiente a $V \times_Z \operatorname{Esp} k(x)$, es decir, a la fibra de $p_1 : V \longrightarrow Z$. Esta fibra es no vacía porque V contiene a Δ, luego basta probar que $(U_s)_{k(x)}$ es denso en $(Z_s)_{k(x)}$. Como la proyección $(Z_s)_{k(s)} \longrightarrow Z_s$ es abierta, basta ver que U_s es denso en Z_s, pero esto es cierto por hipótesis, ya que U contiene a los puntos cuasigenéricos de todas las fibras de Z/S. ∎

10.4 El modelo de Néron

El modelo de Néron de una curva elíptica E/K puede definirse como el abierto $\mathcal{N}/S$ de puntos suaves de su modelo regular minimal $\mathcal{E}/S$. Notemos que, en general, no es un modelo de E/K en el sentido que le hemos dado a esta palabra, porque no es un esquema proyectivo. Su interés radica en gran medida a que, como hemos indicado en la introducción, la estructura de variedad abeliana de E/K se extiende a una estructura de esquema de grupos en $\mathcal{N}/S$. Esto es lo que vamos a probar en esta sección.

El argumento requiere diversas reducciones previas que se basarán en los teoremas que demostramos a continuación. El teorema 7.24 afirma que si $\mathcal{E}/S$ es el modelo regular minimal de una curva elíptica E/K y $s \in S$ es un punto cerrado, entonces $\mathcal{E} \times_S \operatorname{Esp} \mathcal{O}_{S,s}$ es el modelo regular minimal de E/K sobre $\operatorname{Esp} \mathcal{O}_{S,s}$. El mismo argumento permite probar otros resultados similares de conservación de la minimalidad:

Teorema 10.28 *Sea X/S una superficie aritmética cuya fibra genérica X_η sea geométricamente regular de género $p_a(X_\eta) \geq 1$. Sea $S' \longrightarrow S$ un homomorfismo entre esquemas de Dedekind (afines) y llamemos $X' = X \times_S S'$ al cambio de base. Supongamos además que se cumple una de las condiciones siguientes:*

a) $S' \longrightarrow S$ *es llano.*

b) $S = \operatorname{Esp} D$ *, donde* D *es un anillo de valoración discreta,* $S' = \operatorname{Esp} \hat{D}$ *y* $S' \longrightarrow S$ *es el homomorfismo natural.*

Entonces, si X/S *es minimal, también lo es* X'/S'*. Si* $S' \longrightarrow S$ *es suprayectivo (lo cual se cumple siempre en el caso b) se cumple el recíproco.*

Demostración: Notemos que, en el caso a), la proyección $p : X' \longrightarrow X$ es llana por [E A27], luego es suave por [E A26], luego X' es regular por [E 7.50]. En el caso b) llegamos a la misma conclusión usando 6.34 (y teniendo en cuenta [AC 5.11]). El teorema [E 9.29] nos da que $\omega_{X'/S'} = p^*\omega_{X/S}$ (teniendo en cuenta el teorema [AC A9] en el caso b).

Supongamos que X'/S' no es minimal, de modo que X' contiene un divisor excepcional $E' \subset X'_{s'}$. Llamemos $E = p[E'] \subset X_s$.

Notemos que $X'_{s'} = X_s \times_{k(s)} \operatorname{Esp} k(s')$ y, como el cambio de base es finito y suprayectivo, la restricción de p a $X'_s \longrightarrow X_s$ también es finita y suprayectiva, y también lo es la restricción $q : E' \longrightarrow E$. Puesto que $\omega_{X/S}|_E = q^*\omega_{X'/S'}|_E$, el teorema [E 10.9] implica que

$$|K(E') : K(E)| \operatorname{grad}_{k(s)} \omega_{X/S}|_E = \operatorname{grad}_{k(s)} \omega_{X'/S'}|_{E'} = K_{X'/S'} \cdot E' < 0$$

por 7.16, luego también $K_{X/S} \cdot E < 0$ y el mismo 7.16 implica que E es un divisor excepcional en X.

Supongamos ahora que X no es minimal, con lo que tiene un divisor excepcional E. Como $S' \longrightarrow S$ es suprayectiva, también lo es $E' = E \times_S S' \longrightarrow E$, por lo que E' es un divisor en X'. Si $X \longrightarrow Z$ es la contracción de E, entonces $X \times_S S' \longrightarrow Z \times_S S'$ es un homomorfismo birracional cuyo lugar singular es no vacío, y $Z' = Z \times_S S'$ es regular por el mismo motivo que X'. Así pues, X' contiene un divisor excepcional y no es relativamente minimal. ∎

Nota Los homomorfismos llanos son de tipo finito por definición. No obstante, vamos a ver que el teorema anterior sigue siendo válido si en el caso a) $S' \longrightarrow S$ es un homomorfismo entre esquemas de Dedekind locales que cumple la definición de homomorfismo llano (es decir, que es plano y no ramificado) salvo que no exigimos que sea de tipo finito.

Veamos en primer lugar que X' es regular. Sea $s' \in S'$ el punto cerrado de S' y sea $s \in S$ su imagen en S. Observemos que la fibra S'_s es el espectro de

$$\mathcal{O}_{S',s'} \otimes_{\mathcal{O}_{S,s}} (\mathcal{O}_{S,s}/\mathfrak{m}_s) \cong \mathcal{O}_{S',s'}/\mathfrak{m}_s\mathcal{O}_{S',s'} = \mathcal{O}_{S',s'}/\mathfrak{m}_{s'} = k(s').$$

Si $x' \in X'_{s'}$, tenemos que

$$X'_x = S' \times_S X \times_X \operatorname{Esp} k(x) = S' \times_S \operatorname{Esp} k(s) \times_{k(s)} \operatorname{Esp} k(x)$$

$$= \operatorname{Esp} k(s') \times_{k(s)} \operatorname{Esp} k(x).$$

Como $k(s')/k(s)$ es separable, el teorema [E 3.57] nos da que X'_x tiene dimensión 0 y es reducido, por lo que $\mathcal{O}_{X'_x,x'}$ es un anillo reducido con un único ideal primo, es decir, es un cuerpo.

El teorema [E 3.46] nos da que $\mathcal{O}_{X',x'}/\mathfrak{m}_x\mathcal{O}_{X',x'} \cong \mathcal{O}_{X'_x,x'}$, luego vemos que $\mathfrak{m}_x\mathcal{O}_{X',x'} = \mathfrak{m}_{x'}$. Ahora observamos que

$$(\mathfrak{m}_x/\mathfrak{m}_x^2) \otimes_{k(x)} k(x') = (\mathfrak{m}_x \otimes_{\mathcal{O}_{X,x}} k(x)) \otimes_{k(x)} k(x') = \mathfrak{m}_x \otimes_{\mathcal{O}_{X,x}} (\mathcal{O}_{X',x'}/\mathfrak{m}_{x'}).$$

Por [AC A7] tenemos que $\mathfrak{m}_x \otimes_{\mathcal{O}_{X,x}} \mathcal{O}_{X',x'} = \mathfrak{m}_x\mathcal{O}_{X',x'} = \mathfrak{m}_x$ y, a través de esta identificación, el último anillo de la cadena de igualdades anteriores se convierte en

$$(\mathfrak{m}_x \otimes_{\mathcal{O}_{X,x}} \mathcal{O}_{X',x'})/\mathfrak{m}_{x'}^2 = \mathfrak{m}_{x'}/\mathfrak{m}_{x'}^2.$$

En total, vemos que $\dim_{k(x)}(\mathfrak{m}_x/\mathfrak{m}_x^2) = \dim_{k(x')}(\mathfrak{m}_{x'}/\mathfrak{m}_{x'}^2)$. Por otra parte, [E 4.52] nos da que $\dim \mathcal{O}_{X',x'} = \dim \mathcal{O}_{X,x}$. Así, como x es regular, también lo es x'.

Así pues, todos los puntos cerrados de X' son regulares y, por [E 7.18] concluimos que X' es regular.

Supongamos ahora que X' contiene un divisor excepcional

$$E' \subset X'_{s'} = X_s \times_{k(s)} \operatorname{Esp} k(s').$$

El teorema [E 3.56] nos da un cuerpo intermedio $k(s) \subset k \subset k(s')$ tal que la extensión $k/k(s)$ es finita y $E' = E''_{k(s')}$, para cierto cerrado $E'' \subset X_s \times_{k(s)} \operatorname{Esp} k$. Sea $E \subset X_s$ la proyección de E''.

La relación $\omega_{X'/S'} = p^*\omega_{X/S}$ sigue siendo válida, pues sólo depende del carácter plano de p. Descomponemos $q : E' \xrightarrow{q_1} E'' \xrightarrow{q_2} E$, donde q_2 es finita y suprayectiva y podemos aplicarle [E 10.9]. Para q_1 usamos [E 10.8]:

$$|K(E'') : K(E)| \operatorname{grad}_{k(s)} \omega_{X/S}|_E = \operatorname{grad}_{k(s)} q_2^*\omega_{X/S}|_E$$

$$= |k : k(s)| \operatorname{grad}_k q_2^*\omega_{X'/S'}|_{E'} = |k : k(s)| \operatorname{grad}_{k(s')} \omega_{X'/S'}|_{E'},$$

luego

$$|K(E'') : K(E)|\, K_{X/S} \cdot E = |k : k(s)|\, K_{X'/S'} \cdot E'$$

y el teorema 7.16 nos da igualmente una contradicción. ∎

Todavía necesitaremos otra variante más:

Teorema 10.29 *Sea X/S una superficie aritmética minimal cuya fibra genérica X_η sea geométricamente regular de género $p_a(X_\eta) \geq 1$. Sea $Y \longrightarrow S$ un homomorfismo suave, sea $\xi \in Y$ un punto de codimensión 1 y sea $S' = \operatorname{Esp} \mathcal{O}_{Y,\xi}$. Entonces $X' = X \times_S S'$ es una superficie minimal sobre S'.*

Demostración: Observemos que Y/S es regular, luego $\mathcal{O}_{Y,\xi}$ es un anillo local regular de dimensión 1, es decir, es un dominio de Dedekind local. Así pues, el teorema 5.4 nos da que X'/S' es una superficie fibrada. Como $X \times_S Y \longrightarrow X$ es suave, el teorema [E 7.50] nos da que $X \times_S Y$ es regular, luego también lo es

$X \times_S S'$, pues los puntos de su fibra cerrada son regulares (en X') por [E 3.47] y los de su fibra abierta lo son porque ésta es una extensión de constantes de X_η.

Si la imagen de ξ en S es el punto genérico η, entonces la fibra cerrada de X' es

$$X_\xi = X \times_S \operatorname{Esp} k(\xi) = X \times_S \operatorname{Esp} k(\eta) \times_{k(\eta)} \operatorname{Esp} k(\xi) = (X_\eta)_{k(\xi)},$$

luego es regular y X'/S' es suave, luego es minimal por 7.8. Supongamos, pues, que la imagen de ξ en S es un punto cerrado s. El esquema X' no se altera si cambiamos Y por un entorno de ξ. Por el teorema [E A33] podemos suponer que existe un homomorfismo llano $g : Y \longrightarrow A^n_S$ tal que f es la composición con el homomorfismo natural $A^n_S \longrightarrow S$. Sea $\xi' \in A^n_S$ la imagen de ξ. Como las fibras de g tienen dimensión 0, el teorema [E 4.52] implica que

$$\dim \mathcal{O}_{A^n_S,\xi'} = \dim \mathcal{O}_{Y,\xi} = 1.$$

Observemos que $A^n_S \longrightarrow S$ es suave, ya que sus fibras son los esquemas $A^n_{k(s)}$, que son regulares (y es plano porque lo es $A^n_{\mathbb{Z}} \longrightarrow \operatorname{Esp}\mathbb{Z}$). Así pues, todo lo que hemos dicho para S' y X' vale para $S'' = \operatorname{Esp}\mathcal{O}_{A^n_S,\xi'}$ y $X'' = X \times_S S''$, de modo que X''/S'' es una superficie aritmética. Si probamos que es minimal, el teorema 10.28 aplicado al homomorfismo llano $S' \longrightarrow S''$ nos dará la minimalidad de X'.

Equivalentemente, podemos suponer que S es un dominio de Dedekind local, que $Y = A^n_S$ y que ξ pertenece a la fibra cerrada $Y_s = A^n_{k(s)}$. Además, ya hemos probado que X'/S' es una superficie aritmética. Observemos que, de hecho, ξ es el punto genérico de $A^n_{k(s)}$, pues ha de ser $\dim \mathcal{O}_{Y_s,\xi} = 0$. Por consiguiente, $k(\xi)$ es el cuerpo de fracciones algebraicas

$$k(\xi) = k(s)(X_1, \ldots, X_n).$$

La fibra cerrada de X'/S' es

$$X'_\xi = X \times_S \operatorname{Esp} k(\xi) = X_s \times_{k(s)} \operatorname{Esp} k(\xi) = (X_s)_{k(\xi)}.$$

Ahora observamos que las componentes irreducibles de X_s siguen siendo irreducibles tras el cambio de base $k(\xi)/k(s)$. Esto se debe a que si A es una $k(s)$-álgebra íntegra, entonces

$$A \times_{k(s)} k(\xi) = A(X_1, \ldots, X_n)$$

es también una $k(\xi)$-álgebra íntegra.

Por consiguiente, si X'/S' tiene un divisor excepcional $E' \subset X'_\xi$, éste será de la forma $E' = E_{k(\xi)}$, para cierta componente irreducible $E \subset X_s$. Ahora podemos razonar como en la nota posterior a 10.28: la proyección $p : X' \longrightarrow X$ es plana, luego $p^*\omega_{X/S} = \omega_{X'/S'}$ y, si $q : E' \longrightarrow E$ es la restricción de p, tenemos también que $\omega_{X'/S'}|_{E'} = q^*\omega_{X/S}|_E$. Por [E 10.8] resulta que:

$$\operatorname{grad}_{k(s)} \omega_{X/S}|_E = \operatorname{grad}_{k(\xi)} q^*\omega_{X/S}|_E = \operatorname{grad}_{k(\xi)} \omega_{X'/S'}|_{E'} < 0,$$

por el teorema 7.16, lo que supone una contradicción. ∎

Los resultados anteriores permitirán las reducciones necesarias para aplicar el teorema siguiente:

Teorema 10.30 *Sea $S = \operatorname{Esp} A$ el espectro de un anillo local, noetheriano y completo. Llamemos $s \in S$ a su punto cerrado. Si $f : X \longrightarrow S$ es un homomorfismo suave, la aplicación canónica $X(S) \longrightarrow X_s(k(s))$ es suprayectiva.*

Demostración: Sea $x \in X_s(k(s))$. Por el teorema [E A.33], existe un entorno U de x en X tal que $f|_U$ se descompone como un homomorfismo llano $g : U \longrightarrow A^n_S$ seguido del homomorfismo natural $A^n_S \longrightarrow S$. Es claro que $g(x)$ se extiende a un homomorfismo $S \longrightarrow A^n_S$. En términos de anillos, se trata de que siempre existe un homomorfismo que cierra el diagrama siguiente:

$$\begin{array}{ccc} A[X_1,\dots,X_n] & \dashrightarrow & A \\ \downarrow & & \downarrow \\ k(s)[X_1,\dots,X_n] & \longrightarrow & k(s) \end{array}$$

Consideramos ahora el homomorfismo llano $Z = U \times_{A^n_S} S \longrightarrow S$. La composición

$$U \xrightarrow{(1,f|_U)} Z \xrightarrow{p} U$$

es la identidad, luego si llamamos $z \in Z_s(k(s))$ a la imagen de x, tenemos que $p(z) = x$. Basta probar que z se extiende a una sección $S \longrightarrow Z$, ya que entonces la composición $S \longrightarrow Z \longrightarrow U \longrightarrow X$ es una sección que extiende a x. Equivalentemente, basta probar el teorema para un homomorfismo llano.

Esto significa que el homomorfismo $A \longrightarrow \mathcal{O}_{X,x}$ es (fielmente) plano (luego es inyectivo, como consecuencia inmediata de 1.23 b) y que $\mathfrak{m}_x = \mathfrak{m}_s\mathcal{O}_{X,x}$. Además, que x sea racional significa que $A/\mathfrak{m}_s \cong \mathcal{O}_{X,x}/\mathfrak{m}_x$.

En particular, $\mathcal{O}_{X,x} = A + \mathfrak{m}_x$, luego $\mathfrak{m}_x = \mathfrak{m}_s(A + \mathfrak{m}_x) = \mathfrak{m}_s + \mathfrak{m}_x^2$ y $\mathcal{O}_{X,x} = A + \mathfrak{m}_x^2$. Por consiguiente,

$$\mathfrak{m}_x = \mathfrak{m}_s(A + \mathfrak{m}_x^2) = \mathfrak{m}_s + \mathfrak{m}_x^3$$

y, en general, es claro que $\mathfrak{m}_x = \mathfrak{m}_s + \mathfrak{m}_x^n$ y $\mathcal{O}_{X,x} = A + \mathfrak{m}_x^n$. Por lo tanto, el homomorfismo $A/\mathfrak{m}_s^n \longrightarrow \mathcal{O}_{X,x}/\mathfrak{m}_x^n$ es suprayectivo. Su núcleo es

$$(\mathfrak{m}_x^n \cap A)/\mathfrak{m}_s^n = (\mathfrak{m}_s^n\mathcal{O}_{X,x} \cap A)/\mathfrak{m}_s^n = 0,$$

de nuevo por 1.23 b. Así pues, los homomorfismos naturales $A/\mathfrak{m}_s^n \longrightarrow \mathcal{O}_{X,x}/\mathfrak{m}_x^n$ son isomorfismos, lo que nos da a su vez un isomorfismo

$$A = \hat{A} \longrightarrow \hat{\mathcal{O}}_{X,x} = \hat{A} \otimes_A \mathcal{O}_{X,x} = A \otimes_A \mathcal{O}_{X,x} = \mathcal{O}_{X,x}.$$

Tenemos, pues un isomorfismo de A-álgebras $\mathcal{O}_{X,x} \longrightarrow A$ que induce una sección

$$S \longrightarrow \operatorname{Esp} \mathcal{O}_{X,x} \longrightarrow X$$

que claramente cumple $s \mapsto x$. ∎

El teorema siguiente contiene todos los hechos previos necesarios para dotar a $\mathcal{N}/S$ de estructura de esquema de grupos:

Teorema 10.31 *Sea D un dominio de Dedekind con cuerpo de cocientes K, sea E/K una curva elíptica, sea $S = \operatorname{Esp} D$, sea $\mathcal{E}/S$ su modelo regular minimal y sea $\mathcal{N} \subset \mathcal{E}$ el abierto formado por sus puntos suaves.*

a) Las aplicaciones canónicas $\mathcal{N}(S) \longrightarrow \mathcal{E}(S) \longrightarrow E(K)$ son biyectivas.

b) Para cada $x \in E(K)$, la traslación $\tau_x : E \longrightarrow E$ se extiende a un automorfismo $\tau_x : \mathcal{E} \longrightarrow \mathcal{E}$.

c) Sea $m : E \times_K E \longrightarrow E$ la ley de grupo en E y consideremos el automorfismo $t = (m, p_2) : E \times_K E \longrightarrow E \times_K E$. Entonces t se extiende a un automorfismo $t : \mathcal{E} \times_S \mathcal{N} \longrightarrow \mathcal{E} \times_S \mathcal{N}$.

d) El homomorfismo m se extiende a un homomorfismo $m : \mathcal{N} \times_S \mathcal{N} \longrightarrow \mathcal{N}$.

Demostración: a) La aplicación canónica $\mathcal{E}(S) \longrightarrow E(K)$ es la que a cada $\sigma \in \mathcal{E}(S)$ le asigna el homomorfismo $(i\circ\sigma, 1)$, que hace conmutativo el diagrama:

$$\begin{array}{ccc} \operatorname{Esp} K & \xrightarrow{(i\circ\sigma,1)} & \mathcal{E}_K \\ {\scriptstyle i}\downarrow & & \downarrow \\ S & \xrightarrow[\sigma]{} & \mathcal{E} \end{array}$$

Claramente es inyectiva, pues si $i \circ \sigma = i \circ \tau$, tomamos un entorno afín $V = \operatorname{Esp} A$ de $\sigma(\eta) = \tau(\eta)$ en $\mathcal{E}$ y un abierto afín $U = \operatorname{Esp} D$ contenido en $\sigma^{-1}[V] \cap \tau^{-1}[V]$, de modo que $\sigma|_U$ y $\tau|_U$ se corresponden con homomorfismos $A \longrightarrow D$ que, compuestos con la inclusión $D \longrightarrow K$ son iguales, luego también lo son sin componer y, por lo tanto, $\sigma|_U = \tau|_U$. El teorema [E 4.16] nos da que $\sigma = \tau$.

Para probar la suprayectividad observamos que un $\tau \in E(K)$ se corresponde con un punto $p \in \mathcal{E}$ tal que $k(p) = K$. Según el teorema 5.29, el divisor horizontal $\Gamma = \overline{\{p\}}$ determina un isomorfismo $p : \Gamma \longrightarrow S$, luego podemos considerar el isomorfismo inverso, que es un elemento $\sigma \in \mathcal{E}(S)$. El diagrama siguiente muestra que σ se corresponde con τ:

$$\begin{array}{ccccc} \operatorname{Esp} K & \xrightarrow{\tau} & \mathcal{E}_K & & \\ \downarrow & \searrow & & \searrow & \\ S & \underset{\sigma}{\overset{p}{\rightleftarrows}} & \Gamma & \longrightarrow & \mathcal{E} \end{array}$$

Según acabamos de ver, la imagen de cualquier $\sigma \in \mathcal{E}(S)$ es un divisor horizontal Γ tal que $K(\Gamma) = K$. El teorema 6.9 implica entonces que, para todo punto cerrado $s \in S$, se cumple $\Gamma \cdot \mathcal{E}_s = 1$, lo cual se traduce en que $\Gamma \cap \mathcal{E}_s$ se reduce a un punto p, racional en $\mathcal{E}_s$, y tal que $i_p(\Gamma, \mathcal{E}_s) = 1$, lo cual implica en particular que p es regular en $\mathcal{E}_s$ y, al ser racional, es geométricamente regular (por [E 7.24]). Así pues, todos los puntos de la imagen de σ son suaves en $\mathcal{E}$. (Lo hemos probado para imágenes de puntos cerrados, pero para el punto genérico

es trivial.) Esto significa que $\sigma : S \longrightarrow \mathcal{E}$ es, de hecho, un homomorfismo $\sigma : S \longrightarrow \mathcal{N}$. Por consiguiente, la inclusión $\mathcal{N}(S) \subset \mathcal{E}(S)$ es, de hecho, una igualdad.

b) es consecuencia inmediata del teorema 7.26.

c) Llamemos $X = E \times_K E$ y $\mathcal{X} = \mathcal{E} \times_S \mathcal{N}$. Entonces X es la fibra genérica de $\mathcal{X}/S$, pues

$$E \times_K E = (\mathcal{E} \times_S \operatorname{Esp} K) \times_K (\mathcal{N} \times_S \operatorname{Esp} K) \cong (\mathcal{E} \times_S \mathcal{N}) \times_S \operatorname{Esp} K.$$

Observemos que t es el automorfismo construido en la prueba de 7.33. El teorema 7.2 nos da que t se extiende a una aplicación birracional $t : \mathcal{X} \longrightarrow \mathcal{X}$ definida en un entorno de X. Hemos de probar que está definida en todo $\mathcal{X}$. Fijado un punto cerrado $s \in S$, consideramos el diagrama conmutativo

$$\begin{array}{ccc} \mathcal{X} \times_S \operatorname{Esp} \mathcal{O}_{S,s} & \xrightarrow{t_s} & \mathcal{X} \times_S \operatorname{Esp} \mathcal{O}_{S,s} \\ \downarrow & & \downarrow \\ \mathcal{X} & \xrightarrow[t]{} & \mathcal{X} \end{array}$$

Basta probar que t_s está definido en todo $\mathcal{X} \times_S \operatorname{Esp} \mathcal{O}_{S,s}$, pues entonces el teorema 7.2 nos da una extensión a un entorno de la fibra $\mathcal{X}_s$ y de la fibra genérica, y sobre ésta coincide con t, luego lo que tenemos es que t está definido sobre toda la fibra $\mathcal{X}_s$. Observemos que

$$\mathcal{X} \times_S \operatorname{Esp} \mathcal{O}_{S,s} = (\mathcal{E} \times_S \operatorname{Esp} \mathcal{O}_{S,s}) \times_{\mathcal{O}_{S,s}} (\mathcal{N} \times_S \operatorname{Esp} \mathcal{O}_{S,s}),$$

Según el teorema 7.24, el primer factor es el modelo regular minimal de E/K sobre $\mathcal{O}_{S,s}$, y es fácil ver que el segundo factor es su abierto de puntos suaves. Además, t_s induce sobre la fibra genérica de $\mathcal{X} \times_S \operatorname{Esp} \mathcal{O}_{S,s}$ el mismo automorfismo $t : E \times_K E \longrightarrow E \times_K E$.

De todo esto se desprende que, para probar que t está definido sobre todo $\mathcal{X}$, podemos suponer que D es un anillo de valoración discreta. El teorema 2.15 nos da un anillo de valoración discreta D' que contiene a D tal que $\mathfrak{m}_{D'} = \mathfrak{m}_D D'$ y $D'/\mathfrak{m}_{D'}$ es la clausura separable de $D/\mathfrak{m}_D$. Notemos que D' es plano sobre D porque D es un dominio de ideales principales y D' es un D-módulo libre de torsión. Así, $\operatorname{Esp} D' \longrightarrow \operatorname{Esp} D$ cumple la definición de homomorfismo llano excepto que no es necesariamente de tipo finito. Podemos aplicar el teorema 10.28 (teniendo en cuenta la nota posterior), y concluir que $\mathcal{X}_{S'}$ es una superficie minimal (donde $S' = \operatorname{Esp} D'$).

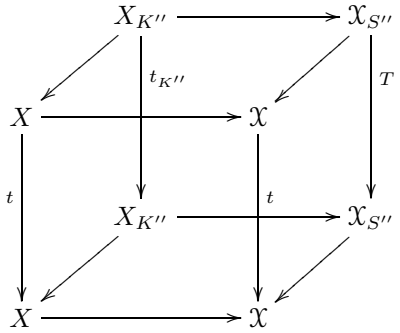
Ahora llamamos $S'' = \operatorname{Esp} \hat{D}'$, donde $\hat{D}'$ es la compleción de D', y el teorema 10.28 nos da también que $\mathcal{X}_{S''}$ es minimal. Observemos que

$$\mathcal{X}_{S''} = \mathcal{E}_{S''} \times_{S''} \mathcal{N}_{S''},$$

y que $\mathcal{N}_{S''}$ es el abierto de los puntos suaves de $\mathcal{E}_{S''}$. (Porque la proyección

$\mathcal{E}_{S''} \longrightarrow \mathcal{E}$ hace corresponder claramente[2] los puntos suaves de $\mathcal{E}_{S''}$ con los puntos suaves de $\mathcal{E}$.) Además, si llamamos $K'' = K(S'')$, la fibra genérica de $\mathcal{X}_{S''}$ es claramente $X_{K''} = E_{K''} \times_{K''} E_{K''}$.

Teniendo en cuenta que $m_{K''}$ es la ley de grupo en $E_{K''}$, es claro que el automorfismo $t_{K''} : X_{K''} \times_{K''} X_{K''} \longrightarrow X_{K''}$ es el considerado en el enunciado para la curva elíptica $E_{K''}$, luego en particular sabemos que se extiende a una aplicación birracional $T : \mathcal{X}_{S''} \longrightarrow \mathcal{X}_{S''}$ (definida sobre S''). En el diagrama siguiente, todas las caras del cubo son conmutativas salvo quizá la de la derecha:



pero esto implica que la cara derecha conmuta sobre la fibra genérica $X_{K''}$, luego por el teorema 5.26, conmuta sobre todo el dominio de T. A su vez, esto implica que $T = t_{S''}$. Por el teorema 10.18, si probamos que $t_{S''}$ está definido sobre todo $\mathcal{X}_{S''}$, tendremos que t está definido sobre todo $\mathcal{X}$, como queremos probar. Equivalentemente, podemos suponer que D es un anillo completo local cuyo cuerpo de restos es separablemente cerrado.

Sea $\lambda \in \mathcal{N}_s$ uno de los puntos cuasigenéricos de la fibra cerrada y consideremos el esquema $T = \operatorname{Esp} \mathcal{O}_{\mathcal{N},\lambda}$. El teorema 10.29 nos da que $\mathcal{E} \times_S T$ es una superficie regular minimal sobre T. Tenemos un diagrama conmutativo

$$\begin{array}{ccc} \mathcal{E} \times_S T & \longrightarrow & \mathcal{E} \times_S \mathcal{N} \\ \uparrow & & \uparrow \\ E \times_K \operatorname{Esp} K(E) & \longrightarrow & E \times_K E \end{array}$$

lo que significa que el cambio de base $\mathcal{E} \times_S T \longrightarrow \mathcal{E} \times_S \mathcal{N}$ envía la fibra genérica a la fibra genérica. Puesto que t es una aplicación birracional en $\mathcal{E} \times_S \mathcal{N}$ definida sobre un entorno de la fibra genérica, el cambio de base

$$t_T : \mathcal{E} \times_S T \longrightarrow \mathcal{E} \times_S T$$

es una aplicación birracional definida en un entorno de la fibra genérica. El teorema 7.26 implica entonces que t_T es un automorfismo definido sobre toda la

[2]La clave está en que, por el teorema [AC 5.73], un punto de un conjunto algebraico C/k es geométricamente regular si y sólo si cualquiera de sus antiimágenes en cualquier extensión de constantes C_K con K algebraicamente cerrado (no necesariamente la clausura algebraica de k) es regular.

superficie $\mathcal{E} \times_S T = \mathcal{E} \times_S \mathcal{N} \times_{\mathcal{N}} \operatorname{Esp} \mathcal{O}_{\mathcal{N},\lambda}$. Por el teorema 7.2, existe un abierto $U \subset \mathcal{N}$, que contiene a λ, tal que t_T se extiende a un único $\mathcal{N}$-automorfismo

$$\mathcal{E} \times_S U \longrightarrow \mathcal{E} \times_S U.$$

Este automorfismo coincide con t sobre la fibra genérica, luego es una restricción de t. (Esto se debe a que las restricciones de ambos a la fibra genérica son E-automorfismos de $E \times_K E$ que coinciden sobre $E \times_K \operatorname{Esp} K(E)$, pero este último esquema es la fibra genérica de $E \times_k E$ vista como superficie sobre E, luego ambos automorfismos coinciden.)

Si t está definido sobre $\mathcal{E} \times_S U_1$ y $\mathcal{E} \times_S U_2$, también lo está sobre $\mathcal{E} \times_S (U_1 \cup U_2)$, luego $\mathcal{E}$ está definido sobre $\mathcal{E} \times_S U$, donde $U \subset \mathcal{N}$ es un abierto que contiene a todos los puntos cuasigenéricos de $\mathcal{N}_s$, es decir, un abierto tal que U_s es denso en $\mathcal{N}_s$.

Tomemos ahora $x \in E(K)$ y consideremos el automorfismo:

$$\mathcal{E} \times_S \tau_x[U] \xrightarrow{1\times\tau_x^{-1}} \mathcal{E} \times_S U \xrightarrow{t} \mathcal{E} \times_S U \xrightarrow{\tau_x\times\tau_x} \mathcal{E} \times_S \tau_x[U]$$

El cambio de base $\times_S \operatorname{Esp} K$ lo convierte en[3]

$$E \times_K E \xrightarrow{1\times\tau_x^{-1}} E \times_K E \xrightarrow{(m,p_2)} E \times_K E \xrightarrow{\tau_x\times\tau_x} E \times_K E$$

y es fácil ver que éste coincide con (m, p_2) (porque ambos automorfismos inducen la misma aplicación sobre $E(\overline{K}) \times E(\overline{K})$). El teorema 5.26 nos da entonces que el primer automorfismo coincide con t en su dominio común, luego t está definido en $\mathcal{E} \times_S \tau_x[U]$.

Así pues, para probar que t está definido en todo $\mathcal{E} \times_S \mathcal{N}$ basta ver que

$$\mathcal{N} = \bigcup_{x \in E(K)} \tau_x[U].$$

Llamemos V al miembro derecho. Así, V es un abierto en $\mathcal{N}$ cerrado para traslaciones, es decir, tal que $\tau_x[V] \subset V$, para todo $x \in E(K)$. Además V_s contiene a todos los puntos cuasigenéricos de $\mathcal{N}_s$ y, obviamente, V_η contiene al punto genérico de E. Por lo tanto, si no se da la igualdad, $C = \mathcal{N} \setminus V$ es un cerrado tal que C_η y C_s tienen ambos dimensión 0 (si no son vacíos), luego ambos son finitos. En suma, C consta a lo sumo de un número finito de puntos de $\mathcal{N}_\eta = E$ y un número finito de puntos de $\mathcal{N}_s$.

Por otra parte, $\mathcal{N}_s(k(s))$ es infinito. En efecto, $\mathcal{N}_s$ es geométricamente regular, luego geométricamente reducido, y el teorema [E 3.68] implica que todo abierto no vacío (en particular, el complementario de todo conjunto finito de puntos racionales) contiene un punto racional.

Por el teorema 10.30, cada $x_s \in \mathcal{N}_s(k(s))$ se extiende a una sección $x \in \mathcal{N}(S)$, que a su vez define un automorfismo $\tau_x = \tau_{x_K} : \mathcal{N} \longrightarrow \mathcal{N}$. Basta probar que,

[3]Con más precisión, lo convierte en la restricción del automorfismo indicado a un cierto abierto de $E \times_K E$.

para cada $u \in C$, existe un $x \in \mathcal{N}(S)$ tal que $u' = \tau_x(u) \notin C$, ya que entonces $u' \in V$ y también $\tau_{-x_K}(v) = u \in V$, con lo que tenemos una contradicción (salvo que C sea vacío).

Para ello demostraremos que si x, $x' \in \mathcal{N}(S)$ cumplen $x_s \neq x'_s$, entonces $\Gamma_{\tau_x} \cap \Gamma_{\tau_{x'}} = \varnothing$. Admitiendo esto, supongamos que $u \in C_\eta$, sea $L = k(u)$ y fijemos un homomorfismo $\operatorname{Esp} L \longrightarrow E$ cuya imagen sea u. Entonces, los homomorfismos $\operatorname{Esp} L \longrightarrow E \xrightarrow{\tau_x} E$ y $\operatorname{Esp} L \longrightarrow E \xrightarrow{\tau_{x'}} E$ son distintos o, de lo contrario, también coincidirían los homomorfismos

$$\operatorname{Esp} L \longrightarrow E \xrightarrow{(1,\tau_x)} E \times_K E, \qquad \operatorname{Esp} L \longrightarrow E \xrightarrow{(1,\tau_{x'})} E \times_K E,$$

y su imagen común estaría en $\Gamma_{\tau_x} \cap \Gamma_{\tau_{x'}} \subset E \times_K E$, que es la fibra genérica de $\Gamma_{\tau_x} \cap \Gamma_{\tau_{x'}} \subset \mathcal{N} \times_S \mathcal{N}$, contradicción.

Si $|L : K| = n$, existen a lo sumo n homomorfismos $\operatorname{Esp} L \longrightarrow E$ cuya imagen sea un punto dado de E, luego hay un número finito de tales homomorfismos cuya imagen está en C_η. Así pues, hay un número finito de puntos $x_s \in \mathcal{N}_s(k(s))$ tales que el homomorfismo

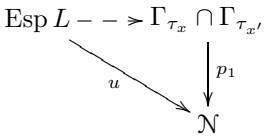
$$\operatorname{Esp} L \longrightarrow E \xrightarrow{(1,\tau_x)} E \times_K E$$

tenga imagen en C_η y, como hay infinitos elementos en $\mathcal{N}_s(k(s))$, concluimos que existe un $x \in \mathcal{N}(S)$ tal que $\tau_x(u) \notin C$.

Si $u \in C_s$ razonamos análogamente, con la única variante de que, como la extensión $k(u)/k(s)$ es puramente inseparable, hay un único homomorfismo $\operatorname{Esp} L \longrightarrow \mathcal{N}_s$ para cada punto de $\mathcal{N}_s$.

Tomamos, pues x, $x' \in \mathcal{N}(S)$ tales que $x_s \neq x'_s$. Observamos en primer lugar que no puede suceder que $\Gamma_{\tau_x} \cap \Gamma_{\tau_{x'}} = \Gamma_{\tau_x}$, ya que entonces $\Gamma_{\tau_x} \subset \Gamma_{\tau_{x'}}$ y, como ambos son cerrados en $\mathcal{N} \times_S \mathcal{N}$ irreducibles de dimensión 2, serían iguales, lo que implicaría que $\tau_x = \tau_{x'}$, de donde $x_K = x'_K$, de donde $x = x'$ (pues ambas secciones coincidirían en $\operatorname{Esp} K$, que es denso en S).

Por consiguiente, $\Gamma_{\tau_x} \cap \Gamma_{\tau_{x'}} \subsetneq \Gamma_{\tau_x} \subset \mathcal{N} \times_S \mathcal{N}$. Pasando a las fibras genéricas, tenemos igualmente que $\Gamma_{\tau_x} \cap \Gamma_{\tau_{x'}} \subsetneq \Gamma_{\tau_x} \subset E \times_K E$. Si $v \in \Gamma_{\tau_x} \cap \Gamma_{\tau_{x'}}$, entonces v no es el punto genérico de Γ_{τ_x}, luego $u = p_1(v)$ no es el punto genérico de E, sino un punto cerrado. Sea $L = k(u)$ y fijemos un homomorfismo $\operatorname{Esp} L \longrightarrow E$. Es claro que los homomorfismos $\operatorname{Esp} L \longrightarrow E \xrightarrow{\tau_x} E$ y $\operatorname{Esp} L \longrightarrow E \xrightarrow{\tau_{x'}} E$ son iguales, pues ambos coinciden con $\operatorname{Esp} L \longrightarrow \Gamma_{\tau_x} \cap \Gamma_{\tau_{x'}}$ seguido de la segunda proyección:



(Notemos que p_1 es una inmersión cerrada.)

Ahora bien, $\operatorname{Esp} L \longrightarrow E$ induce un homomorfismo $\operatorname{Esp} L \longrightarrow E_L$, cuya imagen u' cumple $\tau_x(u') = \tau_{x'}(u')$, luego $\tau_{u'}(x_K) = \tau_{u'}(x'_K)$, luego $x_K = x'_K$, luego $x = x'$, contradicción.

Esto prueba que la fibra genérica de $\Gamma_{\tau_x} \cap \Gamma_{\tau_{x'}}$ es vacía o, lo que es lo mismo, que $\Gamma_{\tau_x} \cap \Gamma_{\tau_{x'}} \subset (\Gamma_{\tau_x})_s$.

Por otra parte, $\Gamma_{\tau_{x'}}$ es un cerrado irreducible de dimensión 2 en $\mathcal{N} \times_S \mathcal{N}$, que tiene dimensión 3, luego $\Gamma_{\tau_{x'}}$ es un divisor primo de Weil en $\mathcal{N} \times_S \mathcal{N}$. El producto es regular, pues es suave sobre $\mathcal{N}$, luego podemos identificar a $\Gamma_{\tau_{x'}}$ con un divisor de Cartier entero. Podemos considerar su imagen inversa a través de la inmersión cerrada $\Gamma_{\tau_x} \longrightarrow \mathcal{N} \times_S \mathcal{N}$, que es un divisor de Cartier en Γ_{τ_x} cuyo soporte es $\Gamma_{\tau_x} \cap \Gamma_{\tau_{x'}}$. Esto prueba que la intersección tiene dimensión 1, luego es una unión de componentes irreducibles de $(\Gamma_{\tau_x})_s$.

A través del isomorfismo $p_1 : \Gamma_{\tau_x} \longrightarrow \mathcal{N}$, la intersección se transforma en una unión de componentes irreducibles de $\mathcal{N}_s$. Como $\mathcal{N}_s$ es geométricamente regular, sus componentes irreducibles también lo son, luego en particular son geométricamente reducidas, y el teorema [E 3.68] nos da que contienen un punto racional $u_s \in \mathcal{N}_s(k(s))$, que se extiende a una sección $u \in \mathcal{N}(S)$. El hecho de que $p_1^{-1}(u_s) \in \Gamma_{\tau_x} \cap \Gamma_{\tau_{x'}}$ se traduce en que $\tau_x(u_s) = \tau_{x'}(u_s)$.

Una propiedad evidente de las traslaciones de una curva elíptica es que $\tau_{x_K}(u_K) = \tau_{u_K}(x_K)$. Por lo tanto, los homomorfismos

$$S \xrightarrow{u} \mathcal{N} \xrightarrow{\tau_x} \mathcal{N} \quad \text{y} \quad S \xrightarrow{x} \mathcal{N} \xrightarrow{\tau_u} \mathcal{N}$$

coinciden sobre $\operatorname{Esp} K$, luego son iguales, luego $\tau_x(u_s) = \tau_u(x_s)$. Igualmente concluimos que $\tau_{x'}(u_s) = \tau_u(x'_s)$, luego $\tau_u(x_s) = \tau_u(x'_s)$, luego $x_s = x'_s$, contradicción.

Con esto tenemos probado que las gráficas son disjuntas y ello concluye la demostración de que la aplicación racional $t : \mathcal{E} \times_S \mathcal{N} \longrightarrow \mathcal{E} \times_S \mathcal{N}$ está definida en todo $\mathcal{E} \times_S \mathcal{N}$. Vamos a probar que es un isomorfismo, para lo cual volvemos al contexto general que indica el enunciado (ya no suponemos que S es local y $k(s)$ separablemente cerrado, etc.).

El automorfismo $i : E \longrightarrow E$ que a cada punto de $E(\bar{K})$ le asigna su opuesto para la estructura de grupo se extiende a un automorfismo $i : \mathcal{E} \longrightarrow \mathcal{E}$ (por el teorema 7.26), que a su vez se restringe a un automorfismo $i : \mathcal{N} \longrightarrow \mathcal{N}$. Es fácil ver que el automorfismo

$$\mathcal{E} \times_S \mathcal{N} \xrightarrow{1\times i} \mathcal{E} \times_S \mathcal{N} \xrightarrow{t} \mathcal{E} \times_S \mathcal{N} \xrightarrow{1\times i} \mathcal{E} \times_S \mathcal{N}$$

es el inverso de t, porque lo es sobre la fibra genérica $E \times_K E$ (donde se comprueba haciendo actuar a su composición con t por la izquierda y la derecha sobre los puntos de $E(\bar{K}) \times E(\bar{K})$). Así pues, t es un automorfismo de $\mathcal{E} \times_S \mathcal{N}$.

d) Basta observar que $\mathcal{N} \times_S \mathcal{N}$ es el abierto de puntos suaves (sobre S) de $\mathcal{E} \times_S \mathcal{E}$ (y, en particular, el de $\mathcal{E} \times_S \mathcal{N}$). En efecto, es claro que los puntos de $\mathcal{N} \times_S \mathcal{N}$ son suaves, ya que el producto es suave sobre $\mathcal{N}$ y éste es suave sobre S. Recíprocamente, si $p : \mathcal{E} \times_S \mathcal{E} \longrightarrow \mathcal{E}$ es una de las proyecciones, hemos de

probar que si $x \in \mathcal{E} \times_S \mathcal{E}$ es suave, entonces $p(x) \in \mathcal{N}$. En caso contrario, si $s \in S$ es la imagen de x, tendríamos que x sería geométricamente regular en $\mathcal{E}_s \times_{k(s)} \mathcal{E}_s$, mientras que $p(x)$ no sería geométricamente regular en $\mathcal{E}_s$. Si $\bar{k}$ es la clausura algebraica de $k(s)$, esto implica a su vez que en $(\mathcal{E}_s)_{\bar{k}} \times_{\bar{k}} (\mathcal{E}_s)_{\bar{k}}$ habría un punto regular cuya proyección en $(\mathcal{E}_s)_{\bar{k}}$ no sería regular. Ahora bien, como $\mathcal{E} \times_S \mathcal{E}$ es plano sobre $\mathcal{E}$, las proyecciones de $(\mathcal{E}_s)_{\bar{k}} \times_{\bar{k}} (\mathcal{E}_s)_{\bar{k}}$ también son planas, y el teorema 3.25 nos da una contradicción.

Como consecuencia, el automorfismo $t : \mathcal{E} \times_S \mathcal{N} \longrightarrow \mathcal{E} \times_S \mathcal{N}$ construido en el apartado c) se restringe a un automorfismo $t : \mathcal{N} \times_S \mathcal{N} \longrightarrow \mathcal{N} \times_S \mathcal{N}$ que, compuesto con la primera proyección, nos da el homomorfismo m del enunciado. ∎

Finalmente obtenemos el resultado que perseguíamos:

Teorema 10.32 *Sea D un dominio de Dedekind con cuerpo de cocientes K, sea E/K una curva elíptica, sea $S = \operatorname{Esp} D$, sea $\mathcal{E}/S$ su modelo regular minimal y sea $\mathcal{N} \subset \mathcal{E}$ el abierto formado por sus puntos suaves. Entonces, el homomorfismo $m : \mathcal{N} \times_S \mathcal{N} \longrightarrow \mathcal{N}$ construido en el teorema anterior, junto con la extensión $i : \mathcal{N} \longrightarrow \mathcal{N}$ del automorfismo $i : E \longrightarrow E$ que a cada punto de $E(\bar{K})$ le asigna su opuesto, y la sección $o : S \longrightarrow \mathcal{N}$ determinada por el punto racional $o \in E(K)$ (que determina su estructura de variedad abeliana), determinan una estructura de esquema de grupos abelianos en $\mathcal{N}$ que sobre la fibra genérica induce la estructura de variedad abeliana de E/K.*

Demostración: Ante todo, observemos que en la prueba del teorema 8.13 hemos visto que $O = \overline{\{o\}} \subset \mathcal{E}$ está, de hecho, contenido en $\mathcal{N}$. Por el teorema 5.29, sabemos que el homomorfismo estructural $\pi : O \longrightarrow S$ es un isomorfismo. En el enunciado estamos llamando $o : S \longrightarrow O \subset \mathcal{N}$ al isomorfismo inverso. Es claro que se trata de la única sección tal que $o(\eta) = o$, ya que esto implica que la imagen de o en $\mathcal{E}$ es O y, al estar definida sobre S, ha de ser necesariamente la inversa del homomorfismo estructural.

Los diagramas de la definición de esquema de grupos son conmutativos porque lo son sobre las fibras genéricas (teorema 5.26), y son conmutativos sobre las fibras genéricas porque sobre ellas se reducen a los diagramas correspondientes a la estructura de variedad abeliana de E/K. ∎

Es claro que la estructura de esquema de grupos en $\mathcal{N}/S$ está completamente determinada por el hecho de que extiende a la estructura de variedad abeliana de E/K, es decir, que no depende de la construcción particular con la que hemos demostrado su existencia.

10.5 Propiedades del modelo de Néron

En las secciones precedentes hemos evitado dar una definición formal de "modelo de Néron" porque es posible dar una definición general válida para conjuntos algebraicos muy generales, aunque su interés se reduce en la práctica al caso de las variedades abelianas. En el caso de una curva elíptica, el modelo de

Néron resultará ser el abierto $\mathcal{N}/S$ de puntos suaves del modelo regular minimal, que hemos estudiado en la sección anterior.

Definición 10.33 Sea D un dominio de Dedekind con cuerpo de cocientes K, sea $S = \operatorname{Esp} D$ y sea X/K un conjunto algebraico geométricamente regular. El *modelo de Néron* de X/K es un esquema suave de tipo finito $\mathcal{N}/S$, cuya fibra genérica sea isomorfa a X/K, y tal que, para todo esquema suave N/S, la aplicación canónica

$$\operatorname{Hom}_S(N, \mathcal{N}) \longrightarrow \operatorname{Hom}_K(N_K, X)$$

es biyectiva.

Es claro que si X/K admite un modelo de Néron $\mathcal{N}/S$, éste es único salvo isomorfismo, ya que si N/S es otro modelo de Néron, el isomorfismo $\mathcal{N}_K \cong N_K$ determina homomorfismos $N \longrightarrow \mathcal{N}$ y $\mathcal{N} \longrightarrow N$ cuyas composiciones $N \longrightarrow N$ y $\mathcal{N} \longrightarrow \mathcal{N}$ inducen la identidad sobre la fibra genérica, luego son la identidad en N y $\mathcal{N}$ respectivamente.

Néron demostró la existencia del modelo de Néron de una variedad abeliana arbitraria. Nosotros demostraremos únicamente la existencia para curvas elípticas.

Observemos que, en general, si X/K es una variedad abeliana, entonces su estructura de grupo algebraico se extiende de forma única a una estructura de esquema de grupos abelianos en su modelo de Néron (admitiendo que éste exista). En efecto, para extender el homomorfismo $m : X \times_K X \longrightarrow X$ aplicamos la definición a $N = \mathcal{N} \times_S \mathcal{N}$, que es un esquema suave (sobre $\mathcal{N}$, luego sobre S) cuya fibra genérica es $X \times_K X$. La conmutatividad de los diagramas de la definición de esquema de grupos se deduce de la conmutatividad de los diagramas correspondientes sobre las fibras genéricas.

Teorema 10.34 *Sea D un dominio de Dedekind, sea K su cuerpo de cocientes, sea $S = \operatorname{Esp} D$, sea E/K una curva elíptica, sea $\mathcal{E}/S$ su modelo regular minimal y sea $\mathcal{N}$ el abierto de los puntos suaves de $\mathcal{E}$. Entonces $\mathcal{N}/S$ es el modelo de Néron de E/K.*

Demostración: Como $\mathcal{E}$ es una superficie aritmética, es claro que $\mathcal{N}$ es separado (y, por definición, suave) sobre S. También sabemos que su fibra genérica es isomorfa a E/K. Sólo falta probar que cumple la propiedad universal de la definición de modelo de Néron.

Consideramos un esquema suave N/S y un homomorfismo $f : N_K \longrightarrow E$. Sea $N = N_1 \cup \cdots \cup N_r$ la descomposición de N en componentes conexas. Cada una de ellas es suave, luego es íntegra. Claramente, $N_K = N_{1,K} \cup \cdots \cup N_{r,K}$. Si encontramos homomorfismos $g_i : N_i \longrightarrow \mathcal{N}$ tales que $g_{i,K} = f|_{N_{i,K}}$, es claro que éstos definen un homomorfismo $g : N \longrightarrow \mathcal{N}$ tal que $g_K = f$. Equivalentemente, podemos suponer que N es íntegro.

El teorema 7.2 nos da un homomorfismo de un abierto de N (que contiene a N_K) en un abierto de $\mathcal{N}$, es decir, una aplicación racional $g : N \longrightarrow \mathcal{N}$, tal

que $g_K = f$. Hemos de probar que g está definida sobre todo N. Según 10.27, basta probar que g está definida sobre los puntos de codimensión 1 y sobre los puntos cuasigenéricos de las fibras de N. Ahora bien, g está definido sobre la fibra genérica y, si ξ es un punto de una fibra cerrada N_s, la relación

$$\dim \mathcal{O}_{N,\xi} = \dim \mathcal{O}_{N_s,\xi} + \dim \mathcal{O}_{S,s},$$

teniendo en cuenta que el último sumando es 1, muestra que ξ es cuasigenérico en N_s si y sólo si tiene codimensión 1. Sea pues, $\xi \in N_s$ un punto de codimensión 1. Basta probar que g está definida en ξ.

Sea $T = \operatorname{Esp} \mathcal{O}_{N,\xi}$ y sea $L = K(T) = K(N)$. Por el teorema 10.29 sabemos que $\mathcal{E}' = \mathcal{E} \times_S T$ es el modelo regular minimal de E_L sobre T, y su abierto de puntos suaves es $\mathcal{N}' = \mathcal{N} \times_S T$. El teorema 10.31 a) nos da que la aplicación natural $\mathcal{N}'(T) \longrightarrow E_L(L)$ es biyectiva.

Aplicamos esto al homomorfismo $\operatorname{Esp} L \longrightarrow N_L \xrightarrow{f_L} \mathcal{N}_L = E_L$, con lo que obtenemos un diagrama conmutativo

$$\begin{array}{ccccc} \operatorname{Esp} L & \longrightarrow & N_L & \xrightarrow{f_L} & \mathcal{N}_L \\ \downarrow & & & & \downarrow \\ T & & \longrightarrow & & \mathcal{N} \end{array}$$

El teorema [E 4.5] nos da un entorno U de ξ y un homomorfismo $h : U \longrightarrow \mathcal{N}$ tal que la fila inferior del diagrama anterior se descompone como

$$\begin{array}{ccccc} \operatorname{Esp} L & \longrightarrow & N_L & \xrightarrow{f_L} & \mathcal{N}_L \\ \downarrow & & & & \downarrow \\ T & \longrightarrow & U & \xrightarrow[h]{} & \mathcal{N} \end{array}$$

Sea ahora $V \subset N$ un abierto no vacío contenido en U y en el dominio de g. Claramente, tenemos los diagramas conmutativos

$$\begin{array}{ccccc} \operatorname{Esp} L & \longrightarrow & N_L & \xrightarrow{f_L} & \mathcal{N}_L \\ & \searrow & & & \downarrow \\ & & V & \xrightarrow[g,h]{} & \mathcal{N} \end{array}$$

luego g y h coinciden sobre el punto genérico de V, luego coinciden en un abierto,[4] luego la aplicación racional g está definida en U y, en particular, en ξ. ∎

Observemos ahora que el teorema 7.24 implica inmediatamente su análogo para modelos de Néron:

[4]Tomamos un abierto afín $G \subset \mathcal{N}$ y un abierto en $G' \subset V$ contenido en $g^{-1}[G] \cap h^{-1}[G]$, de modo que $g|_{G'}$ y $h|_{G'}$ se corresponden con homomorfismos de anillos $A \longrightarrow B$ tales que, compuestos con la inclusión $B \subset L$, son iguales, luego $g|_{G'} = h|_{G'}$.

Teorema 10.35 *Sea D un dominio de Dedekind con cuerpo de cocientes K, sea $S = \operatorname{Esp} D$, sea E/K una elíptica y sea $\mathcal{N}/S$ su modelo de Néron. Para cada punto cerrado $s \in S$, se cumple que $\mathcal{N} \times_S \operatorname{Esp} \mathcal{O}_{S,s}$ es el modelo de Néron de E/K sobre $\operatorname{Esp} \mathcal{O}_{S,s}$.*

Demostración: Si $\mathcal{E}/S$ es el modelo regular minimal de E/K, el teorema 7.24 nos da que $\mathcal{E} \otimes_S \operatorname{Esp} \mathcal{O}_{S,s}$ es el modelo regular minimal de E/K sobre $\mathcal{O}_{S,s}$, y es fácil ver que $\mathcal{N} \otimes_S \operatorname{Esp} \mathcal{O}_{S,s}$ es su abierto de puntos suaves, luego es el modelo de Néron de E/K sobre $\mathcal{O}_{S,s}$. ∎

En particular, la fibra $\mathcal{N}_s$ es la misma para el modelo de Néron de E/K sobre S y sobre $\operatorname{Esp} \mathcal{O}_{S,s}$, luego, para estudiar las fibras cerradas de los modelos de Néron, podemos trabajar únicamente con dominios de Dedekind que sean anillos de valoración discreta. En tal caso, las posibilidades para la fibra $\mathcal{E}_s$ del modelo regular minimal vienen dadas por la tabla 8.1. Observemos que la tabla contiene la estructura de $\mathcal{N}_s$ en cada caso: es el esquema que resulta de eliminar los puntos siguientes:

a) El punto singular de las fibras de tipo I_1 o $\mathrm{I}_{1,2}$ y el de la última componente irreducible del tipo $\mathrm{I}_{n,2}$ con n impar,

b) Todos los puntos en que se cortan dos o más componentes irreducibles (pues son puntos singulares en $\mathcal{E}_s$, luego no suaves en $\mathcal{E}$),

c) Todas las componentes irreducibles de multiplicidad mayor que 1 (sus puntos no son reducidos, luego no son geométricamente regulares).

Puesto que las componentes irreducibles de $\mathcal{N}_s$ no se cortan entre sí, concluimos que las componentes irreducibles de $\mathcal{N}_s$ son también sus componentes conexas.

Definición 10.36 Sea D un dominio de Dedekind con cuerpo de cocientes K, sea E/K una curva elíptica y sea $\mathcal{N}$ su modelo de Néron. Si $s \in S$ es un punto cerrado, la fibra cerrada $\mathcal{N}_s/k(s)$ es un grupo algebraico. Llamaremos $\mathcal{N}_s^0$ a la componente conexa del elemento neutro, que es un subgrupo abierto y cerrado de $\mathcal{N}_s$. Por otra parte, llamaremos $\Phi_{E,s} = \pi_0(\mathcal{N}_s)$ al esquema de componentes conexas de $\mathcal{N}_s$, que también es un grupo algebraico sobre $k(s)$ en virtud del teorema 10.25.

Con más detalle, la sección $o : S \longrightarrow \mathcal{N}$ es la que asigna a η el punto infinito $o_\eta \in \mathcal{N}_\eta = E$, luego el elemento neutro $o_s \in \mathcal{N}_s$ es el punto que cumple $\overline{\{o_\eta\}} \cap \mathcal{N}_s = \{o_s\}$. Por lo tanto, $\mathcal{N}_s^0$ es la intersección con $\mathcal{N}$ de la componente irreducible de $\mathcal{E}_s$ que en la demostración del teorema 8.26 hemos llamado Γ_1 (y que, siguiendo la prueba, podemos identificar en las figuras de la tabla 8.1).

Para todos los tipos de reducción aditiva (teniendo en cuenta 8.24 para el tipo II) vemos que $\mathcal{N}_s^0 \cong A^1_k$, luego el teorema 10.22 nos da que la estructura de grupo de $\mathcal{N}_s^0$ es la del grupo aditivo de k. Cuando la reducción es multiplicativa racional (es decir, de tipo I_n, con $n \geq 1$) vemos que $\mathcal{N}_s^0 \cong A^1_k \setminus \{p\}$ donde p es un

punto racional. Por consiguiente, el teorema 10.23 nos da que la estructura de grupo de $\mathcal{N}_s^0$ es la del grupo multiplicativo de k. La estructura de $\mathcal{N}_s^0$ cuando la reducción es multiplicativa irracional (tipo $\mathrm{I}_{\mathrm{n},2}$) es más delicada, pero, tras una extensión de constantes cuadrática k'/k, se convierte en el grupo multiplicativo de k'. Por último, en el caso de buena reducción (tipo I_0) la estructura de $\mathcal{N}_s^0$ es la estructura de grupo de una curva elíptica.

Según los teoremas 10.11 y 10.14, los puntos de $\Phi_{E,s}$ se corresponden con las componentes conexas (o irreducibles) de $\mathcal{N}_s$ de modo que los puntos de $\Phi_{E,s}(k(s))$ se corresponden con las componentes geométricamente conexas.

De acuerdo con la tabla 8.1, cada componente conexa Γ de $\mathcal{N}_s$ es de uno de los tipos siguientes (llamamos $k = k(s)$ y $\bar{k}$ a una clausura algebraica):

a) Una curva elíptica, que es geométricamente irreducible, luego geométricamente conexa.

b) El abierto de puntos regulares de una cúbica singular Γ' definida por una ecuación de Weierstrass. Entonces $\Gamma'_{\bar{k}}$ es la cúbica singular definida por la misma ecuación de Weierstrass y $\Gamma_{\bar{k}}$ es un abierto en $\Gamma'_{\bar{k}}$, luego Γ es también geométricamente irreducible y geométricamente conexa.

c) Un abierto en P^1_k, con lo que $\Gamma_{\bar{k}}$ es un abierto en $\mathrm{P}^1_{\bar{k}}$ y nuevamente es geométricamente irreducible y geométricamente conexa.

d) Un abierto en una cónica geométricamente íntegra Γ', con lo que Γ es también geométricamente íntegra.

e) Un abierto en $\mathrm{P}^1_{k'}$, donde k'/k es una extensión cuadrática o cúbica. Entonces $\Gamma_{\bar{k}}$ es un abierto denso en $\mathrm{P}^1_{k'} \times_k \operatorname{Esp} \bar{k}$, que es unión de dos o tres componentes conexas isomorfas a $\mathrm{P}^1_{\bar{k}}$, luego Γ es geométricamente disconexa.

f) Un abierto en una cónica reducida singular Γ' (de modo que Γ no contiene al punto singular de Γ'). Entonces $\Gamma'_{\bar{k}}$ es unión de dos componentes irreducibles isomorfas a $\mathrm{P}^1_{\bar{k}}$ que se cortan en un punto, cuya imagen en Γ' es el punto singular. Entonces, $\Gamma_{\bar{k}}$ es un abierto denso en $\Gamma'_{\bar{k}}$ que no contiene al punto de intersección de las dos componentes irreducibles, luego es disconexo y así Γ no es geométricamente conexa.

Teniendo en cuenta todas estas consideraciones, es inmediato que el número de elementos de $\Phi_{E,s}$, $\Phi_{E,s}(k)$ y $\Phi_{E,s}(\bar{k})$ es el dado por la tabla 10.1.

Ahora vamos a relacionar el modelo de Néron con el modelo de Weierstrass minimal. Para ello conviene dar la definición siguiente:

Definición 10.37 Sea D un anillo de valoración discreta con cuerpo de cocientes K, sea E/K una curva elíptica y sea $\mathcal{N}/S$ su modelo de Néron, donde $S = \operatorname{Esp} D$. Definimos $\mathcal{N}^0 = \mathcal{N} \setminus (\mathcal{N}_s \setminus \mathcal{N}_s^0) = \mathcal{N}_\eta \cup \mathcal{N}_s^0$, que es un abierto en $\mathcal{N}$ cuya fibra cerrada es $\mathcal{N}_s^0$.

	$\mathrm{I}_0, \mathrm{II}, \mathrm{II}^*$	$\mathrm{III}, \mathrm{III}^*$	$\mathrm{IV}, \mathrm{IV}^*$	$\mathrm{IV}_2, \mathrm{IV}_2^*$	I_n	$\mathrm{I}_{\mathrm{n},2}$	I_n^*	$\mathrm{I}_{\mathrm{n},2}^*$	$\mathrm{I}_{0,3}^*$
$\Phi_{E,s}$	1	2	3	2	n	$\frac{n+2}{2}$ / $\frac{n+1}{2}$	4	3	2
$\Phi_{E,s}(k)$	1	2	3	1	n	2/1	4	2	1
$\Phi_{E,s}(\bar{k})$	1	2	3	3	n	n	4	4	4

Tabla 10.1: Número de componentes conexas de la fibra cerrada $\mathcal{N}_s$.
(En el tipo $\mathrm{I}_{\mathrm{n},2}$, las dos posibilidades corresponden, respectivamente, al caso en que n es par o impar. En el tipo I_n hay que excluir el caso $n = 0$, que está incluido en la primera columna.)

Del hecho de que $\mathcal{N}_s^0$ sea un subgrupo algebraico de $\mathcal{N}_s$ se sigue que la multiplicación $\mathcal{N} \times_S \mathcal{N} \longrightarrow \mathcal{N}$ se restringe (como aplicación) a una aplicación $\mathcal{N}_s^0 \times_S \mathcal{N}_s^0 \longrightarrow \mathcal{N}_s^0$ (es fácil ver que $\mathcal{N}_s^0 \times_S \mathcal{N}_s^0 = \mathcal{N}_s^0 \times_{k(s)} \mathcal{N}_s^0$), y también lo hace a $\mathcal{N}_\eta \times_S \mathcal{N}_\eta \longrightarrow \mathcal{N}_\eta$, luego se restringe a una aplicación $\mathcal{N}^0 \times_S \mathcal{N}^0 \longrightarrow \mathcal{N}^0$. Lo mismo vale para el homomorfismo $i : \mathcal{N} \longrightarrow \mathcal{N}$, que se restringe a $\mathcal{N}^0 \longrightarrow \mathcal{N}^0$. Como $\mathcal{N}^0$ es abierto en $\mathcal{N}$, esto implica que $\mathcal{N}^0$ hereda de $\mathcal{N}$ una estructura de esquema de grupos. (Observemos que la sección $o : S \longrightarrow \mathcal{N}$ puede verse también como $o : S \longrightarrow \mathcal{N}^0$.)

Teorema 10.38 *Sea $S = \operatorname{Esp} D$, donde D es un anillo de valoración discreta con cuerpo de cocientes K y cuerpo de restos*[5] *k. Sea $\mathcal{E}/S$ el modelo regular minimal de una curva elíptica E/K. Sea W/S el modelo de Weierstrass minimal de E/K, sean $\mathcal{N}$ y W^0 los abiertos de puntos suaves de $\mathcal{E}$ y W, respectivamente y sea $\mathcal{N}^0$ el subgrupo abierto de $\mathcal{N}$ que resulta de eliminar las componentes conexas de $\mathcal{N}_s$ distintas de $\mathcal{N}_s^0$. Entonces, la contracción $\rho : \mathcal{E} \longrightarrow W$ se restringe a un isomorfismo $\rho : \mathcal{N}^0 \longrightarrow W^0$.*

Demostración: Por el teorema 8.18, sabemos que se obtiene de $\mathcal{E}$ mediante la contracción $\rho : \mathcal{E} \longrightarrow W$ de las componentes irreducibles de $\mathcal{E}_s$ que no cortan a $O = \overline{\{o\}} = \{o_\eta, o_s\}$. Si $\mathcal{E}_s$ tiene una única componente irreducible, el teorema es trivial, pues entonces ρ es un isomorfismo, $\mathcal{E} = W$ y $\mathcal{N}^0 = \mathcal{N} = W^0$.

Supongamos, pues, que $\mathcal{E}_s$ tiene más de una componente irreducible. Entonces, la componente Γ_1 que contiene a o_s es isomorfa a P_k^1, por lo que todos sus puntos son suaves excepto los que corten a otras componentes irreducibles. Si llamamos C a la unión de las demás componentes, es claro que $\mathcal{N}_s^0 = \mathcal{E}_s \setminus C$ y $\mathcal{N}^0 = \mathcal{E} \setminus C$. La imagen de C por ρ es un conjunto finito de puntos, pero la tabla 8.1 muestra que, en todos los casos, C es conexo, por lo que $\rho[C]$ es un punto $p \in W_s$.

De este modo, $W \setminus \{p\} \cong \mathcal{E} \setminus C$ es regular y, por la minimalidad de $\mathcal{E}$, no puede ocurrir que W sea también regular en p. Por lo tanto, la fibra W_s ha de tener un punto singular, que ha de ser necesariamente p. Además, p será el único punto no suave de W. En otras palabras, tenemos que $W^0 = W \setminus \{p\}$ y, ciertamente, ρ se restringe a un isomorfismo $\rho : \mathcal{N}^0 \longrightarrow W^0$. ∎

[5] Si $\operatorname{car} k = 2, 3$ suponemos además que k es perfecto. Lo mismo vale para todos los teoremas de esta sección.

En particular, podemos dotar a W^0 de una (única) estructura de esquema de grupos de forma que la estructura de grupo algebraico inducido sobre la fibra genérica E/K es la asociada a su estructura de curva elíptica.

Definición 10.39 Sea $S = \operatorname{Esp} D$, donde D es un anillo de valoración discreta con cuerpo de cocientes K y cuerpo de restos k. Sea $\mathcal{N}/S$ el modelo de Néron de una curva elíptica E/K. Llamaremos *reducción.* $r : E(K) \longrightarrow \mathcal{N}_s(k)$ a la composición de la inversa de la biyección canónica $\mathcal{N}(S) \longrightarrow E(K)$ (cf. 10.31) con la aplicación canónica $\mathcal{N}(S) \longrightarrow \mathcal{N}_s(k)$.

Vamos a relacionar esta reducción con la teoría clásica. Para ello consideramos el esquema $\mathrm{P}^2_S = \operatorname{Proy}(D[X,Y,Z])$. Por el teorema [E 4.28] tenemos una biyección natural $\mathrm{P}^2_S(S) \longrightarrow \mathrm{P}^2_K(K)$. Componiendo su inversa con la aplicación canónica $\mathrm{P}^2_S(S) \longrightarrow \mathrm{P}^2_k(k)$ obtenemos otra reducción $r' : \mathrm{P}^2_K(K) \longrightarrow \mathrm{P}^2_k(k)$. Ésta admite una interpretación clásica muy simple:

Un punto $x \in \mathrm{P}^2_K(K)$ está determinado por unas coordenadas homogéneas $[a,b,c]$ que podemos tomar en D. Más aún, multiplicando por una potencia adecuada de un primo de D, podemos suponer que una de ellas, por ejemplo, c, es una unidad en D. Por consiguiente, otro vector de coordenadas homogéneas es $[a',b',1]$, donde $a' = a/c$ y $b' = b/c$ están ambos en D.

Identificando $A^1_K = V(Z)$, el punto x es, en términos clásicos, el punto (a',b'). El homomorfismo de anillos $D[X,Y] \longrightarrow D$ determinado por la sustitución $X \mapsto a'$, $Y \mapsto b'$ induce a su vez un homomorfismo de esquemas

$$\sigma : S = \operatorname{Esp} D \longrightarrow \operatorname{Esp}(D[X,Y]) \longrightarrow \mathrm{P}^2_S\,.$$

Es claro que $\sigma_\eta = x$, mientras que σ_s, visto como punto de $A^2_k \subset \mathrm{P}^2_k$, es el punto de coordenadas $([a'],[b']) = [[a'],[b'],1] = [[a],[b],[c]]$.

En definitiva, en términos clásicos, la reducción $r' : \mathrm{P}^2_K(K) \longrightarrow \mathrm{P}^2_k(k)$ es la aplicación dada por $r'([a,b,c]) = [[a],[b],[c]]$, donde las coordenadas homogéneas se toman en D de modo que al menos una de ellas sea unitaria. En otras palabras, la reducción de un punto $x \in \mathrm{P}^2_K(K)$ es el punto de $\mathrm{P}^2_k(k)$ cuyas coordenadas homogéneas son las reducciones módulo $\mathfrak{p}$ de las coordenadas homogéneas de x.

Volviendo a la reducción $r : E(K) \longrightarrow \mathcal{N}_s(k)$ que hemos definido antes, podemos componerla con la aplicación $\mathcal{N}_s(k) \longrightarrow W_s(k)$ inducida por la contracción $\mathcal{N} \longrightarrow \mathcal{E} \longrightarrow W$, lo que nos da una tercera reducción $r_W : E(K) \longrightarrow W_s(k)$. Ahora observamos que W es una superficie fibrada determinada por una ecuación de Weierstrass con coeficientes en D, lo que nos da una inmersión cerrada $i : W \longrightarrow \mathrm{P}^2_S$. Cada $x \in E(K)$ se extiende a una sección $\sigma \in \mathcal{N}(S)$, de modo que las correspondientes secciones en $W(S)$ y $\mathrm{P}^2_S(S)$ determinan las reducciones $r_W(x)$ y $r'(i(x))$, respectivamente. Así pues, tenemos el diagrama conmutativo

$$\begin{array}{ccccc}
 & & E(K) & \longrightarrow & \mathrm{P}^2_K(K) \\
 & \overset{r}{\swarrow} & \downarrow{\scriptstyle r_W} & & \downarrow{\scriptstyle r'} \\
\mathcal{N}_s(k) & \longrightarrow & W_s(k) & \longrightarrow & \mathrm{P}^2_k(k)
\end{array}$$

La conmutatividad de la parte derecha se interpreta como que la reducción r_W es, en términos clásicos, la que a cada punto de $E(K)$ le asigna el punto que resulta de reducir módulo $\mathfrak{p}$ sus coordenadas homogéneas.[6] A su vez, la reducción r resulta ser un refinamiento natural de r_W.

Teorema 10.40 *Sea $S = \operatorname{Esp} D$, donde D es un anillo de valoración discreta con cuerpo de cocientes K y cuerpo de restos k, sea $\mathcal{N}$ su modelo de Néron. Entonces, la reducción $r : E(K) \longrightarrow \mathcal{N}_s(k)$ es un homomorfismo de grupos.*

Demostración: Si $T \longrightarrow S$ es cualquier cambio de base, la aplicación natural $\mathcal{N}(S) \longrightarrow \mathcal{N}(T)$ es un homomorfismo de grupos (esto se prueba fácilmente para cualquier esquema de grupos). Tomando $T = \operatorname{Esp} K$ obtenemos que $\mathcal{N}(S) \longrightarrow E(K)$ es un isomorfismo, y tomando $T = \operatorname{Esp} k$ obtenemos que $\mathcal{N}(S) \longrightarrow \mathcal{N}_s(k)$ es un homomorfismo. La reducción r es la composición del inverso del primero con el segundo. ∎

Definición 10.41 En las condiciones del teorema anterior, llamamos

$$E_0(K) = r^{-1}[\mathcal{N}_s^0(k)], \qquad E_1(K) = r^{-1}[\{o_k\}],$$

donde o_k es el elemento neutro de $\mathcal{N}_s(k)$. Obviamente $E_1(K) \subset E_0(K)$ son subgrupos de $E(K)$.

Hemos visto que la contracción $\rho : \mathcal{N} \longrightarrow W$ cumple que $\rho^{-1}[W_s^0] = \mathcal{N}_s^0$, por lo que la aplicación $u : \mathcal{N}_s(k) \longrightarrow W_s(k)$ cumple $u^{-1}[W_s^0(k)] = \mathcal{N}_s^0(k)$. Así pues, $E_0(K) = r_W^{-1}[W_s^0]$, es decir, que $E_0(K)$ puede verse también como el subgrupo de $E(K)$ formado por los puntos con reducción regular[7] en W_s^0.

Si consideramos a W^0 como esquema de grupos isomorfo a $\mathcal{N}^0$, entonces tenemos también un isomorfismo de grupos $\mathcal{N}_s^0(k) \cong W_s^0(k)$, del que se sigue que la restricción $r_W : E_0(K) \longrightarrow W_s^0$ es también un isomorfismo de grupos.

Por otra parte, de la propia definición se deduce que tenemos monomorfismos de grupos

$$E(K)/E_1(K) \longrightarrow \mathcal{N}_s(k), \qquad E_0(K)/E_1(K) \longrightarrow \mathcal{N}_s^0(k).$$

En particular, vemos que, si el cuerpo k es finito, los subgrupos $E_0(K)$ y $E_1(K)$ tienen índice finito en $E(K)$. Más aún, el índice de $E_0(K)$ en $E(K)$ es finito sin necesidad de que k lo sea.[8] Ello se debe a que tenemos un monomorfismo de grupos

$$E(K)/E_0(K) \longrightarrow \Phi_E(k).$$

En efecto, basta tener en cuenta que el homomorfismo de grupos algebraicos $\mathcal{N}_s \longrightarrow \Phi_E$ induce un homomorfismo de grupos

$$\mathcal{N}_s(k) \longrightarrow \Phi_E(k),$$

cuyo núcleo es $\mathcal{N}_s^0(k)$. El teorema siguiente recoge esto y un poco más:

[6] Es decir, que se trata de la reducción definida en [CE sección 6.2] (respecto de una ecuación de Weierstrass minimal de la curva elíptica.)

[7] Y, por consiguiente, es el mismo definido en [CE sección 6.2].

[8] Este hecho se enuncia sin demostración en [CE] tras el teorema [CE 6.24].

Teorema 10.42 *Sea D un anillo de valoración discreta con cuerpo de cocientes K y cuerpo de restos k, sea $\mathcal{N}$ su modelo de Néron y $\Phi_E = \pi_0(\mathcal{N}_s)$. Entonces, existen monomorfismos de grupos*

$$E_0(K)/E_1(K) \longrightarrow \mathcal{N}_s^0(k), \qquad E(K)/E_0(K) \longrightarrow \Phi_E(k).$$

Si D es completo, el primer monomorfismo es un isomorfismo. Si además k es finito, el segundo también lo es.

Demostración: Ya hemos probado la existencia de los monomorfismos. Si D es completo, el teorema 10.30 aplicado a $\mathcal{N}/S$ (donde $S = \operatorname{Esp} D$) nos da que todo $x \in \mathcal{N}_s(k)$ se extiende a un $\sigma : S \longrightarrow \mathcal{N}$ tal que $\sigma_s = x$. Es claro entonces que $\sigma_\eta \in E(K)$ cumple que $r(\sigma_\eta) = x$, luego la reducción $r : E(K) \longrightarrow \mathcal{N}_s(k)$ es suprayectiva, al igual que su restricción $E_0(K) \longrightarrow \mathcal{N}_s^0(k)$. Esto prueba a su vez la suprayectividad del primer monomorfismo.

Puesto que ya hemos visto que $r : E(K) \longrightarrow \mathcal{N}_s(k)$ es suprayectiva, para probar la suprayectividad del segundo monomorfismo basta ver que el homomorfismo $\mathcal{N}_s(k) \longrightarrow \Phi_E(k)$ es suprayectivo. Teniendo en cuenta el teorema 10.14, esto equivale a probar que cada componente conexa de $\mathcal{N}_s$ que es geométricamente conexa contiene un punto racional.

Esto se deduce de la tabla 8.1. En efecto, podemos descartar los casos en los que $\mathcal{E}_s$ tiene una única componente irreducible, ya que entonces $\Phi_E(k)$ es trivial. En todos los casos restantes salvo $\mathrm{I}_{2n,2}$, si C es la componente conexa y C' es la componente irreducible de $\mathcal{E}_s$ que la contiene, tenemos que $C' \cong \mathrm{P}^1_k$ y C es C' salvo a lo sumo dos puntos. Ahora bien, es claro que P^1_k tiene al menos tres puntos racionales, luego al menos uno de ellos está en C.

En el caso exceptuado, C puede ser también una cónica geométricamente regular C' menos un punto no racional. Basta probar que C' tiene al menos un punto racional. Esto es consecuencia de que k es finito. En efecto, si $\operatorname{car} k = 2$, el teorema 4.14 nos da que $C' \cong \mathrm{P}^1_k$.

Si $\operatorname{car} k \neq 2$, aplicamos 4.13 para representar $C' = V(aX^2 + bY^2 + cZ^2)$, con a, b, $c \in k$. La regularidad geométrica equivale a que $abc \neq 0$. Si k tiene q elementos, basta observar que los conjuntos

$$\{ax^2 \in k \mid a \in k\} \qquad \text{y} \qquad \{-by^2 - c \mid y \in k\}$$

tienen ambos $(q+1)/2$ elementos, luego existe un punto $(x, y, 1) \in k^3$ que cumple la ecuación $aX^2 + bY^2 + cZ^2 = 0$, es decir, que C' tiene un punto racional. ∎

Tercera parte

Aplicaciones

Capítulo XI

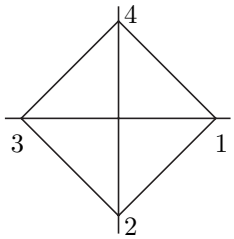
Caracteres de grupos

Exponemos en este capítulo una pequeña introducción a la teoría de caracteres de grupos, en la que incluimos poco más que lo imprescindible para definir, más adelante, el conductor de una curva elíptica. No obstante, en la última sección incluimos algunos resultados adicionales que no nos van a hacer falta, pero que conectan de forma natural con los resultados previos.

Una cosa es tener definido un grupo (por ejemplo, un grupo de unidades de un anillo, un grupo de Galois de una extensión de cuerpos, etc.) y otra muy distinta tener una representación clara de su estructura. A la hora de "comprender un grupo", resulta útil encontrar un grupo isomorfo lo más "concreto" posible. Un recurso clásico es tratar de expresar un grupo dado como grupo de permutaciones:

Ejemplo Si definimos el grupo diédrico de orden 8 como el grupo D_4 de las simetrías de un cuadrado, tendremos una representación más clara y manejable —que podemos incluso tomar como definición— si observamos que es isomorfo al subgrupo siguiente del grupo Σ_4 de las permutaciones de 4 elementos (que podemos identificar con los cuatro vértices del cuadrado):

$$D_4 = \{1, (1,2,3,4), (1,3)(2,4), (4,3,2,1), (1,3), (2,4), (1,2)(3,4), (1,4)(2,3)\}.$$



Las tres primeras (sin contar a 1) se corresponden con los giros de 90°, 180° y 270°, las dos siguientes son las simetrías respecto de las diagonales y las dos últimas son las simetrías respecto de las mediatrices de los lados. Por ejemplo, a partir de esta representación de D_4 es fácil ver que, si llamamos $\sigma = (1,2,3,4)$ y $\tau = (1,3)$, entonces

$$D_4 = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\} = \langle \sigma, \tau \rangle .$$

Además, el producto en D_4 puede calcularse a partir de estas expresiones sin más que tener en cuenta que $\sigma^4 = \tau^2 = 1$ y que $\tau\sigma = \sigma^{-1}\tau$. ∎

Sin embargo, la interpretación de D_4 como el grupo de las simetrías de un cuadrado nos proporciona otra representación concreta del mismo, como un grupo de matrices. En efecto, podemos identificar cada simetría del cuadrado con una aplicación lineal en $\mathbb{R}^2$ y ésta a su vez con su matriz en la base canónica:

Ejemplo El giro de 90° en $\mathbb{R}^2$ y la simetría respecto al eje Y son, respectivamente, las aplicaciones lineales determinadas por las matrices

$$\sigma = \begin{pmatrix} \cos\frac{2\pi}{4} & \operatorname{sen}\frac{2\pi}{4} \\ -\operatorname{sen}\frac{2\pi}{4} & \cos\frac{2\pi}{4} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \tau = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Se comprueba fácilmente que las matrices $1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau$ son distintas dos a dos, así como que satisfacen las relaciones $\sigma^4 = \tau^2 = 1$, $\tau\sigma = \sigma^{-1}\tau$, de donde se sigue que las ocho matrices son el subgrupo generado por σ y τ, y que sus elementos son todas las simetrías del cuadrado (la identidad, los tres giros y las cuatro simetrías propiamente dichas). Esto nos da una representación (o una definición) alternativa de D_4 como grupo de matrices (como el subgrupo generado por las matrices σ y τ).

Una forma sencilla de comprobar que D_4 como grupo de permutaciones es isomorfo a D_4 como grupo de matrices es observar que si identificamos el conjunto $\{1,2,3,4\}$ con los puntos de $X = \{(1,0),(0,-1),(-1,0),(0,1)\}$ (de acuerdo con la numeración de la figura), entonces, las permutaciones σ y τ son las restricciones a X de los automorfismos de $\mathbb{R}^2$ determinados por σ y τ, por lo que, en general, si identificamos cada matriz de D_4 con el automorfismo que determina en $\mathbb{R}^2$ (respecto de la base canónica), un isomorfismo entre D_4 como grupo de automorfismos y D_4 como grupo de permutaciones viene dado por la restricción $\phi \mapsto \phi|_X$. ∎

Ejemplo Si cambiamos $n = 4$ por $n = 3$ en el ejemplo anterior, obtenemos una representación matricial del grupo de simetrías de un triángulo, que tiene seis elementos y es, por consiguiente, isomorfo al grupo Σ_3 de permutaciones de tres elementos. Los generadores son

$$\sigma = \begin{pmatrix} \cos\frac{2\pi}{4} & \operatorname{sen}\frac{2\pi}{3} \\ -\operatorname{sen}\frac{2\pi}{3} & \cos\frac{2\pi}{3} \end{pmatrix} = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{pmatrix}, \quad \tau = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Se comprueba fácilmente que las seis matrices $1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau$ son distintas dos a dos, así como que $\sigma^3 = \tau^2 = 1$, $\tau\sigma = \sigma^{-1}\tau$, de donde se sigue que el grupo $\langle\sigma,\tau\rangle$ tiene orden 6. ∎

A primera vista, podría dudarse de si es más útil representar un grupo finito como grupo de permutaciones o como grupo de matrices, pero sucede que las representaciones matriciales dan lugar a una potente herramienta cuyas posibilidades superan con creces a las que ofrecen las representaciones por grupos de permutaciones. En este capítulo estudiaremos únicamente los aspectos básicos de la parte más simple de dicha teoría.

11.1 Representaciones lineales de grupos

Aunque los grupos D_4 y Σ_3 que hemos considerado en los ejemplos precedentes tenían una interpretación geométrica —como grupos de simetrías— que nos llevaba de forma natural a una representación matricial, podemos plantearnos la posibilidad de representar cualquier grupo abstracto (aunque aquí sólo consideraremos grupos finitos) en forma de grupo de matrices. Esta idea se plasma en la definición siguiente:

Definición 11.1 Una *representación matricial* de *grado* $n \geq 1$ de un grupo finito G sobre un cuerpo K es un homomorfismo de grupos $\rho : G \longrightarrow \mathrm{LG}(n, K)$, donde el grupo *lineal general* $\mathrm{LG}(n, K)$ es el grupo de las matrices inversibles de orden $n \times n$ con coeficientes en K.

Notemos que la definición no exige que ρ sea inyectivo. (En tal caso se dice que la representación es *fiel*.) En general, si N es el núcleo de ρ, tenemos que ρ induce una representación fiel del grupo cociente G/N.

En los ejemplos precedentes hemos calculado una representación fiel de grado 2 del grupo D_4 sobre $\mathbb{Q}$ y otra de Σ_3 sobre $\mathbb{R}$.

A la hora de estudiar las representaciones matriciales, es útil tener en cuenta que las matrices pueden identificarse con automorfismos de espacios vectoriales. Ello nos lleva a la definición siguiente:

Definición 11.2 Una *representación lineal* de *grado* $n \geq 1$ de un grupo finito G es un homomorfismo $\rho : G \longrightarrow \mathrm{Aut}_K(V)$, donde V es un espacio vectorial de dimensión n sobre un cuerpo K.

Si $\rho : G \longrightarrow \mathrm{Aut}(V)$ es una representación lineal de un grupo G, escribiremos a menudo $v\sigma = \rho(v)(\sigma)$. En estos términos, el hecho de que $\rho(\sigma)$ sea un automorfismo de V y que ρ sea un homomorfismo de grupos equivale a las relaciones

$$(v + w)\sigma = v\sigma + w\sigma, \qquad (\alpha v)\sigma = \alpha(v\sigma), \qquad (v\sigma)\tau = v(\sigma\tau),$$

donde v, $w \in V$, σ, $\tau \in G$, $\alpha \in K$.

La relación entre las representaciones matriciales y las representaciones lineales es evidente: toda representación matricial ρ de grado n sobre un cuerpo K determina una representación lineal sobre cualquier espacio vectorial V de dimensión n sobre K respecto a una base B de V prefijada, sin más que asignar a cada $\sigma \in G$ el automorfismo de V que tiene matriz $\rho(\sigma)$ en la base B.

Recíprocamente, toda representación lineal ρ en un espacio vectorial V de dimensión n sobre un cuerpo K determina una representación matricial de grado n para cada base B de V, sin más que asignar a cada $\sigma \in G$ la matriz de $\rho(\sigma)$ en la base B.

Ahora damos una definición de isomorfismo de representaciones que vuele irrelevante la arbitrariedad en la elección de las bases:

Definición 11.3 Diremos que dos representaciones lineales $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$, para $i = 1, 2$, son *isomorfas* (donde V_1 y V_2 son espacios vectoriales sobre un mismo cuerpo K) si existe un isomorfismo $\phi : V_1 \longrightarrow V_2$ de espacios vectoriales tal que $\rho_2 = \rho_1 \circ \bar{\phi}$, donde $\bar{\phi} : \mathrm{Aut}(V_1) \longrightarrow \mathrm{Aut}(V_2)$ es el isomorfismo de grupos dado por $\bar{\phi}(f) = \phi^{-1} f \phi$ (o, equivalentemente, si ϕ cumple que $\phi(v\sigma) = \phi(v)\sigma$ para todo $v \in V_1$ y todo $\sigma \in G$.)

Dos representaciones matriciales $\rho_i : G \longrightarrow \mathrm{LG}(n, K)$ son *isomorfas* si existe una matriz $M \in \mathrm{LG}(n, K)$ tal que, para todo $\sigma \in G$, se cumple la relación $\rho_2(\sigma) = M^{-1}\rho_1(\sigma)M$.

Es inmediato que dos representaciones matriciales isomorfas dan lugar a representaciones lineales isomorfas independientemente de los espacios vectoriales y las bases elegidas, así como que dos representaciones lineales isomorfas dan lugar a representaciones matriciales isomorfas independientemente de las bases elegidas.

A continuación vamos a mostrar una tercera estructura equivalente a la de representación matricial y a la de representación lineal. Se basa en la definición siguiente:

Definición 11.4 Si G es un grupo finito y K es un cuerpo, llamaremos $K[G]$ al espacio vectorial sobre K de base G, que en el que consideraremos la estructura de K-álgebra determinada por el producto siguiente:

$$(\sum_{\sigma\in G} \alpha_\sigma \sigma)(\sum_{\tau\in G} \beta_\tau \tau) = \sum_{\sigma,\tau\in G} \alpha_\sigma \beta_\tau \sigma\tau.$$

Es evidente que el producto así definido es bilineal y que extiende al producto de G. Teniendo esto en cuenta, se comprueba sin dificultad que cumple todas las propiedades necesarias para que $K[G]$ sea ciertamente una K-álgebra.

Si $\rho : G \longrightarrow \mathrm{Aut}(V)$ es una representación lineal, podemos dotar a V de estructura de $K[G]$-módulo (por la derecha) mediante el producto dado por

$$v(\sum_{\sigma\in G} \alpha_\sigma \sigma) = \sum_{\sigma\in G} \alpha_\sigma \rho(\sigma)(v).$$

Notemos que el producto $v\sigma$ según esta definición coincide con el producto $v\sigma = \rho(\sigma)(v)$ que habíamos definido. Recíprocamente, si V es un $K[G]$-módulo de dimensión finita sobre K, podemos definir una acción $\rho : G \longrightarrow \mathrm{Aut}(V)$ mediante $\rho(\sigma)(v) = v\sigma$.

De este modo, tenemos una correspondencia entre las representaciones lineales de grado n de G y los $K[G]$-módulos (por la derecha) de dimensión n sobre K. Es inmediato que dos representaciones son isomorfas si y sólo si los $K[G]$-módulos correspondientes son isomorfos. Más concretamente, un isomorfismo $f : V_1 \longrightarrow V_2$ entre dos K-espacios vectoriales es un isomorfismo entre dos representaciones lineales de G si y sólo si es un isomorfismo entre los $K[G]$-módulos asociados.

Observemos ahora que si L/K es una extensión de cuerpos, $\mathrm{LG}(n,K)$ es un subgrupo de $\mathrm{LG}(n,L)$, por lo que toda representación matricial de un grupo G sobre K puede considerarse también como representación sobre L. Esto tiene un equivalente en términos de representaciones lineales:

Definición 11.5 Si $\rho : G \longrightarrow \mathrm{Aut}(V)$ es una representación lineal de un grupo G y L/K es una extensión de cuerpos, entonces $V_L = L \otimes_K V$ es un L-espacio vectorial y tenemos un monomorfismo de grupos $\mathrm{Aut}(V) \longrightarrow \mathrm{Aut}(V_L)$ dado por $\alpha \mapsto i \otimes \alpha$, donde $i : K \longrightarrow L$ es la inclusión. Definimos la *extensión de escalares* $\rho^L : G \longrightarrow \mathrm{Aut}(V_L)$ como la composición de ρ con este monomorfismo, que claramente es una representación lineal de G sobre K del mismo grado que ρ.

Concretamente, si $v_1, \ldots, v_n$ es una K-base de V, entonces $1 \otimes v_1, \ldots, 1 \otimes v_n$ es una L-base de V_L, y la representación matricial de ρ en la primera base es la misma que la de ρ_L en la segunda.

En términos de módulos tenemos un isomorfismo natural $L[G] \cong L \otimes_K K[G]$, y ρ^L está asociada a la estructura natural de $L[G]$-módulo en V_L dada por

$$(\alpha \otimes v)(\beta \otimes \sigma) = (\alpha\beta) \otimes v\sigma.$$

Veamos un par de ejemplos generales de representaciones:

Definición 11.6 Si G es un grupo finito, llamaremos *representación trivial* de grado n de G sobre el cuerpo K a la representación matricial $\rho : G \longrightarrow \mathrm{LG}(n,K)$ dada por $\rho(\sigma) = I_n$ para todo $\sigma \in G$. Sus representaciones lineales asociadas son las representaciones en espacios vectoriales V de dimensión n que cumplen $v\sigma = v$ para todo $v \in V$ y todo $\sigma \in G$.

Definición 11.7 Si G es un grupo finito, llamaremos *representación regular* de G a la representación asociada a la estructura de $K[G]$-módulo de $K[G]$. Claramente es fiel y su grado es el orden de G.

Ahora veamos cómo podemos construir nuevas representaciones a partir de unas dadas:

Definición 11.8 Si $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$, para $i = 1, 2$, son dos representaciones lineales de G, definimos su *suma directa* como la representación

$$\rho_1 \oplus \rho_2 : G \longrightarrow \mathrm{Aut}(V_1 \oplus V_2)$$

asociada a la suma directa de los $K[G]$-módulos $V_1 \oplus V_2$. Obviamente, se trata de la representación dada por $(v_1 + v_2)\sigma = v_1\sigma + v_2\sigma$, donde $v_1\sigma$ se calcula con ρ_1 y $v_2\sigma$ con ρ_2.

Es claro que podemos definir igualmente la suma directa de cualquier número finito de representaciones de G. El grado de la suma directa es la suma de los grados.

Definición 11.9 Si $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$, para $i = 1, 2$, son dos representaciones lineales de G, definimos su *producto tensorial* como la representación

$$\rho_1 \otimes \rho_2 : G \longrightarrow \mathrm{Aut}(V_1 \otimes_K V_2)$$

asociada al $K[G]$-módulo $V_1 \otimes_K V_2$. Obviamente, se trata de la representación determinada por $(v_1 \otimes v_2)\sigma = (v_1\sigma) \otimes (v_2\sigma)$. El grado del producto tensorial es el producto de los grados.

Definición 11.10 Si $\rho : G \longrightarrow \mathrm{Aut}(V)$ es una representación de G, llamaremos *subrepresentaciones* de ρ a las representaciones $\rho : G \longrightarrow \mathrm{Aut}(W)$ asociadas a los $K[G]$-submódulos W de V.

Observemos que para que un subespacio vectorial $W \subset W$ sea un $K[G]$-submódulo es suficiente con que $W\sigma \subset W$, para todo $\sigma \in G$.

Veamos ya el primer teorema sobre representaciones que, siendo sencillo, no es trivial:

Teorema 11.11 *Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación de G, y sea W un $K[G]$-submódulo de V. Entonces existe otro $K[G]$-submódulo W^0 tal que $V = W \oplus W^0$.*

Demostración: Sea W' cualquier subespacio vectorial de V que cumpla $V = W \oplus W'$, sea $p : V \longrightarrow W$ la proyección y sea $p^0 : V \longrightarrow W$ la aplicación lineal dada por

$$p^0(v) = \frac{1}{|G|} \sum_{\sigma \in G} p(v\sigma^{-1})\sigma.$$

Si $w \in W$, entonces $p(w\sigma^{-1})\sigma = (w\sigma^{-1})\sigma = w$, luego $p^0(w) = w$. Si llamamos W^0 al núcleo de p^0, es claro que $V = W \oplus W^0$. Por otra parte,

$$p^0(v\tau^{-1})\tau = \frac{1}{|G|} \sum_{\sigma \in G} p(v\tau^{-1}\sigma^{-1})\sigma\tau = p^0(v).$$

Esto implica que W^0 es un $K[G]$-submódulo, pues si $p^0(v) = 0$, entonces

$$p^0(v\tau)\tau^{-1} = p^0(v) = 0,$$

luego $p^0(v\tau) = 0$ y, por lo tanto, $v\tau \in W^0$. ∎

Definición 11.12 Diremos que una representación $\rho : G \longrightarrow \mathrm{Aut}(V)$ es *irreducible* si V no tiene más $K[G]$-submódulos que los triviales: 0 y V.

Por el teorema anterior, si una representación no es irreducible, se descompone en suma directa de dos subrepresentaciones no triviales. Es claro entonces que toda representación puede descomponerse en suma directa de representaciones irreducibles $V = W_1 \oplus \cdots \oplus W_n$. La descomposición no es única, en el sentido de que podemos elegir los submódulos W_i de formas distintas, pero

más adelante veremos que la descomposición es única salvo isomorfismo, en el sentido de que dos descomposiciones cualesquiera de un mismo $K[G]$-módulo V han de tener el mismo número de sumandos y que, debidamente ordenados, cada sumando de una descomposición es isomorfo al sumando correspondiente de la otra.

Terminamos con una observación sobre el álgebra $K[G]$. Obviamente, es conmutativa si y sólo si el grupo G es abeliano. En general, el *centro* de un anillo A se define como el subanillo

$$Z(A) = \{a \in A \mid ab = ba \text{ para todo } b \in A\}.$$

Vamos a calcular el centro de $K[G]$. Para ello recordamos que dos elementos $\tau_1, \tau_2 \in G$ se dicen si existe un $\sigma \in G$ tal que $\tau_2 = \sigma^{-1}\tau_1\sigma$. La conjugación es una relación de equivalencia en G. Representaremos por $\mathrm{cl}_G(\tau)$ a la clase de conjugación de τ en G y por $\mathrm{cl}(G)$ al conjunto de todas las clases de conjugación de G.

Es obvio que un elemento

$$x = \sum_{\sigma\in G} \alpha_\sigma \sigma \in K[G]$$

está en el centro de $K[G]$ si y sólo si conmuta con todos los elementos $\tau \in G$, es decir, si cumple que $\tau x = x\tau$ o, equivalentemente, $\tau x \tau^{-1} = x$. Explícitamente:

$$\sum_{\sigma\in G} \alpha_\sigma \tau\sigma\tau^{-1} = \sum_{\sigma\in G} \alpha_\sigma \sigma.$$

Teniendo en cuenta que $\sigma \mapsto \tau\sigma\tau^{-1}$ es biyectiva con inversa $\sigma \mapsto \tau^{-1}\sigma\tau$, esto equivale a que

$$\sum_{\sigma\in G} \alpha_{\tau^{-1}\sigma\tau} \sigma = \sum_{\sigma\in G} \alpha_\sigma \sigma,$$

lo cual equivale a que la función $\sigma \mapsto \alpha_\sigma$ sea constante sobre las clases de conjugación de G. Por consiguiente:

Teorema 11.13 *Si G es un grupo finito, definimos, para cada clase de conjugación $c \in \mathrm{cl}(G)$, el elemento*

$$e_c = \sum_{\sigma\in c} \sigma.$$

Entonces, el centro de $K[G]$ está formado por los elementos de la forma

$$\sum_{c\in \mathrm{cl}(G)} \alpha_c e_c, \qquad \alpha_c \in K,$$

es decir, se trata del subespacio vectorial que tiene por base los elementos e_c.

11.2 Caracteres

Recordemos que la traza[1] de una matriz cuadrada $A = (a_{ij})$ se define como

$$\mathrm{Tr}(A) = \sum_i a_{ii}.$$

La traza es invariante por semejanza, es decir, que, si M es una matriz regular, se cumple que $\mathrm{Tr}(M^{-1}AM) = \mathrm{Tr}(A)$. En particular, si V es un espacio vectorial y $f \in \mathrm{Aut}(V)$, podemos definir la traza $\mathrm{Tr}(f)$ como la traza de la matriz de f en cualquier base.

Definición 11.14 Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación de un grupo finito G en un K-espacio vectorial V. Llamaremos *carácter* asociado a ρ a la función $\chi_\rho : G \longrightarrow K$ dada por $\chi_\rho(\sigma) = \mathrm{Tr}(\rho(\sigma))$. Los caracteres de las representaciones de G se llaman también caracteres de G. Un carácter es *irreducible* si está asociado a una representación irreducible.

Observemos que, si ρ tiene grado n, entonces $\rho(1)$ es la identidad en V y su matriz asociada en cualquier base es I_n, luego $\chi_\rho(1) = n$.

Otro hecho obvio es que

$$\chi_\rho(\sigma^{-1}\tau\sigma) = \mathrm{Tr}(\rho(\sigma)^{-1}\rho(\tau)\rho(\sigma)) = \mathrm{Tr}(\rho(\tau)) = \chi_\rho(\tau).$$

En otras palabras: los caracteres son constantes sobre las clases de conjugación de G.

Ejemplo El grupo D_4 tiene 5 clases de conjugación:

$$\mathrm{cl}(D_4) = \{\{1\}, \{\sigma, \sigma^3\}, \{\sigma^2\}, \{\tau, \sigma^2\tau\}, \{\sigma\tau, \sigma^3\tau\}\},$$

y se comprueba sin dificultad que el carácter χ asociado a la representación lineal que hemos construido en la introducción es el determinado por la tabla:

	1	σ	σ^2	τ	$\sigma\tau$
χ	2	0	-2	0	0

■

Ejercicio: Calcular el carácter asociado a la representación de Σ_3 construida en la introducción.

El teorema siguiente muestra que la suma y el producto de caracteres es de nuevo un carácter.

Teorema 11.15 *Sean $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$, para $i = 1, 2$, dos representaciones de un grupo G y sean χ_i sus caracteres correspondientes. Entonces el carácter de $\rho_1 \oplus \rho_2$ es $\chi_1 + \chi_2$, y el carácter de $\rho_1 \otimes \rho_2$ es $\chi_1\chi_2$.*

[1] Definición 6.38 de mi libro de Geometría.

DEMOSTRACIÓN: Si fijamos bases B_i de V_i y llamamos $\bar{\rho}_i(\sigma)$ a la matriz de $\rho_i(\sigma)$ en la base B_i, es claro que la matriz de $(\rho_1 \oplus \rho_2)(\sigma)$ en la base $B_1 \cup B_2$ de $V_1 \oplus V_2$ es

$$\begin{pmatrix} \bar{\rho}_1(\sigma) & 0 \\ 0 & \bar{\rho}_2(\sigma) \end{pmatrix},$$

y la traza de esta matriz es $\chi_1(\sigma) + \chi_2(\sigma)$.

Si $B_1 = \{v_i\}$, $B_2 = \{w_j\}$, $\bar{\rho}_1(\sigma) = (a_{ij})$, $\bar{\rho}_2(\sigma) = (b_{ij})$, entonces

$$(\rho_1 \otimes \rho_2)(\sigma)(v_i \otimes w_j) = \rho_1(\sigma)(v_i) \otimes \rho_2(\sigma)(v_j)$$

$$= \sum_k a_{ki} v_k \otimes \sum_l b_{lj} w_l = \sum_{kl} a_{ki} b_{lj} v_k \otimes w_l.$$

La matriz $(\overline{\rho_1 \otimes \rho_2})(\sigma)$ en la base $B_1 \otimes B_2$ tiene una fila y una columna para cada elemento $v_k \otimes w_l$. Según el cálculo que acabamos de hacer, el elemento que está en la fila y en la columna correspondientes a $v_i \otimes w_j$ es $a_{ii} b_{jj}$, por lo que la traza es

$$\sum_{i,j} a_{ii} b_{jj} = \chi_1(\sigma)\chi_2(\sigma).$$

■

Vamos a ver que las representaciones están completamente determinadas por sus caracteres, al menos bajo ciertas hipótesis adicionales:

NOTA: *Hasta el final de esta sección sobrentenderemos que el cuerpo K sobre el que consideramos las representaciones es algebraicamente cerrado y de característica* 0.

No suponemos simplemente $K = \mathbb{C}$ porque vamos a probar que la teoría general sobre un cuerpo K en estas condiciones puede reducirse al caso complejo. Más concretamente, el hecho de que K tenga característica 0 se traduce en que $\mathbb{Q} \subset K$ y, como K es algebraicamente cerrado, contiene a la clausura algebraica $\mathbb{A}$ de $\mathbb{Q}$. Probaremos que todas las representaciones matriciales de G en K son isomorfas a representaciones sobre $\mathbb{A}$.

Teorema 11.16 *Si $\rho : G \longrightarrow \mathrm{Aut}(V)$ es una representación y $\sigma \in G$, entonces V admite una base formada por vectores propios de $\rho(\sigma)$, y los valores propios son raíces de la unidad.*

DEMOSTRACIÓN: Restringiendo ρ al subgrupo generado por σ, podemos suponer que G está generado por σ. Como K es algebraicamente cerrado, el automorfismo $\rho(\sigma)$ tiene al menos un valor propio $\alpha_1 \in K$ (una raíz de su polinomio característico), Sea $v_1 \in V$ un vector propio asociado a α_1, de modo que $v_1\sigma = \alpha v_1$ y, en general, $v_1\sigma^n = \alpha^n v_1$. Así pues, $W_1 = \langle v_1 \rangle$ es un subespacio invariante. Por 11.11 podemos descomponer $V = W_1 \oplus V_1$, donde V_1 es también un subespacio invariante.

Repitiendo el mismo razonamiento con V_1 podemos encontrar un subespacio invariante $W_2 = \langle v_2 \rangle$ y una descomposición $V = W_1 \oplus W_2 \oplus V_2$. Tras un número

finito de pasos llegamos a una descomposición $V = W_1 \oplus \cdots \oplus W_n$ en subespacios invariantes de la forma $W_i = \langle v_i \rangle$, donde cada v_i es obviamente un vector propio de $\rho(\sigma)$.

La matriz de $\rho(\sigma)$ en esta base es diagonal, y los elementos de la diagonal son sus valores propios α_i. Como existe un $n \geq 1$ tal que $\sigma^n = 1$, ha de ser $\alpha_i^n = 1$, luego los valores propios α_i son raíces de la unidad. ∎

En general no es posible elegir una base de V tal que la matriz de $\rho(\sigma)$ sea diagonal simultáneamente para todo $\sigma \in G$, pero, como la traza $\chi(\sigma)$ se puede calcular a partir de la matriz de $\rho(\sigma)$ en cualquier base, concluimos que

$$\chi(\sigma) = \epsilon_1 + \cdots + \epsilon_n,$$

donde los números $\epsilon_i \in K$ son raíces de la unidad y, en particular, son enteros algebraicos (es decir, que son raíces de polinomios mónicos con coeficientes enteros). Conviene destacar este hecho:

Teorema 11.17 *Los valores que toman los caracteres de los grupos finitos son enteros algebraicos.*

En particular, los caracteres pueden verse como aplicaciones $\chi : G \longrightarrow \mathbb{A}$ (aunque todavía no podemos asegurar que las representaciones matriciales que los generan tengan necesariamente sus coeficientes en $\mathbb{A}$). Observemos que en $\mathbb{A} \subset \mathbb{C}$ podemos considerar la conjugación compleja, que representaremos con una barra, como es habitual.

Teorema 11.18 *Si $\chi : G \longrightarrow \mathbb{A}$ es un carácter de un grupo finito G, entonces, para todo $\sigma \in G$, se cumple que $\chi(\sigma^{-1}) = \overline{\chi(\sigma)}$.*

Demostración: Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación que genere el carácter dado. Según 11.16, podemos elegir una base de V en la que $\rho(\sigma)$ admite una matriz diagonal (a_{ij}) cuya diagonal está formada por raíces de la unidad, que son elementos de $\mathbb{A}$ de módulo 1. Entonces

$$\chi(\sigma^{-1}) = \sum_i \alpha_{ii}^{-1} = \sum_i \bar{\alpha}_{ii} = \overline{\chi(\sigma)}.$$

∎

Como tercera aplicación de 11.16 mostramos que un carácter determina el núcleo de la representación que lo genera:

Definición 11.19 Si $\chi : G \longrightarrow \mathbb{A}$ es un carácter de un grupo finito G, llamaremos *núcleo* de χ al conjunto

$$\mathrm{N}(\chi) = \{\sigma \in G \mid \chi(\sigma) = \chi(1)\}.$$

Teorema 11.20 *Si $\rho : G \longrightarrow \mathrm{Aut}(G)$ es una representación de un grupo finito G y χ es el carácter que determina, entonces el núcleo de χ es el núcleo de ρ.*

DEMOSTRACIÓN: Evidentemente, $\sigma \in G$ está en el núcleo de ρ si y sólo si $\rho(\sigma) = I_n$, donde n es el grado de la representación, luego, en tal caso, se cumple que $\chi(\sigma) = n = \chi(1)$. Recíprocamente, si $\chi(\sigma) = n$, sabemos que, en una base adecuada, $\rho(\sigma)$ se corresponde con una matriz diagonal y $\chi(\sigma) = \epsilon_1 + \cdots + \epsilon_n$ es la suma de dicha diagonal. Los ϵ_i pueden verse como números complejos de módulo 1, luego la parte real de cada uno de ellos es ≤ 1. Para que la suma dé n es necesario que todas las partes reales sean 1, lo cual implica que $\epsilon_i = 1$ y, por consiguiente, que $\rho(\sigma) = I_n$, de modo que σ está en el núcleo de ρ. ∎

Definición 11.21 Si G es un grupo finito, N es un subgrupo normal, para cada carácter $\chi : G/N \longrightarrow \mathbb{A}$ de G/N definimos el carácter $\hat{\chi} : G \longrightarrow \mathbb{A}$ dado por $\hat{\chi}(\sigma) = \chi(\sigma N)$.

Se trata ciertamente de un carácter porque si $\rho : G/N \longrightarrow \mathrm{Aut}(V)$ es la representación que determina χ, entonces la composición $G \longrightarrow G/N \longrightarrow \mathrm{Aut}(V)$ es una representación de G que genera $\hat{\chi}$.

Es claro que χ es irreducible si y sólo si lo es $\hat{\chi}$. Además, tenemos que $N \leq \mathrm{N}(\hat{\chi})$. Recíprocamente, es claro que todo carácter ψ de G que cumpla $N \leq \mathrm{N}(\psi)$ es de la forma $\psi = \hat{\chi}$, para cierto carácter $\chi : G/N \longrightarrow \mathbb{A}$.

En vista de esto, en lo sucesivo identificaremos los caracteres de un grupo cociente G/N con los caracteres de G cuyo núcleo contiene a N.

Las propiedades fundamentales de los caracteres se deducen del teorema siguiente:

Teorema 11.22 (Lema de Schur) *Sean $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$, para $i = 1, 2$ dos representaciones irreducibles de un grupo finito G y sea $f : V_1 \longrightarrow V_2$ un homomorfismo de $K[G]$-módulos. Si las representaciones no son isomorfas, se cumple que $f = 0$ y, si $V_1 = V_2$ y $\rho_1 = \rho_2$, entonces existe un $\alpha \in K$ tal que $f(v) = \alpha v$, para todo $v \in V_1$.*

DEMOSTRACIÓN: Si $f \neq 0$, el núcleo de V_1 ha de ser un $K[G]$-submódulo distinto de V_1, luego ha de ser trivial, y la imagen ha de ser un $K[G]$-submódulo no trivial de V_2, luego ha de ser todo V_2. Esto prueba que f es un isomorfismo y las representaciones son isomorfas.

Si suponemos que ambas representaciones son la misma, sea $\alpha \in K$ un valor propio de f (aquí usamos que K es algebraicamente cerrado). Sea $f' : V_1 \longrightarrow V_1$ la aplicación lineal dada por $f'(v) = f(v) - \alpha v$. Es claro que es un homomorfismo de $K[G]$-módulos que y su núcleo no es trivial (porque contiene a los vectores propios asociados a α) luego, por la parte ya probada, $f' = 0$, luego $f(v) = \alpha v$ para todo $v \in V_1$. ∎

Para extraer consecuencias del lema de Schur conviene introducir la notación siguiente:

Definición 11.23 Si G es un grupo finito, representamos por K^G al conjunto de funciones $\phi : G \longrightarrow K$. Definimos en K^G la forma bilineal simétrica

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{\sigma \in G} \phi(\sigma)\psi(\sigma^{-1}).$$

Teorema 11.24 (Relaciones de ortogonalidad) *Si χ_1 y χ_2 son caracteres irreducibles de un grupo finito G, entonces*

$$\langle \chi_1, \chi_2 \rangle = \begin{cases} 1 & si\ \chi_1 = \chi_2, \\ 0 & si\ \chi_1 \neq \chi_2. \end{cases}$$

DEMOSTRACIÓN: Sean $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$ representaciones que generen los caracteres χ_i. Sea $h : V_1 \longrightarrow V_2$ una aplicación lineal arbitraria y sea $h^0 : V_1 \longrightarrow V_2$ la aplicación lineal dada por

$$h^0(v) = \frac{1}{|G|} \sum_{\sigma \in G} h(v\sigma)\sigma^{-1}.$$

Se cumple que h^0 es un homomorfismo de $K[G]$-módulos, pues

$$h^0(v\tau) = \frac{1}{|G|} \sum_{\sigma \in G} h(v\tau\sigma)\sigma^{-1} = \left(\frac{1}{|G|} \sum_{\sigma \in G} h(v\tau\sigma)(\tau\sigma)^{-1} \right) \tau = h^0(v)\tau.$$

Fijemos bases de ambos espacios vectoriales, sean $(r^1_{ij}(\sigma))$, $(r^2_{ij}(\sigma))$ las matrices de $\rho_i(\sigma)$ en las bases respectivas y sean (x_{ij}), (x^0_{ij}) las matrices de h y h^0, respectivamente. Entonces,

$$x^0_{ij} = \frac{1}{|G|} \sum_{\sigma,k,l} r^1_{i,k}(\sigma) x_{kl} r^2_{lj}(\sigma^{-1}).$$

Si $\chi_1 \neq \chi_2$, las representaciones no son isomorfas, luego, según el lema de Schur, ha de ser $h^0 = 0$, cualquiera que sea la aplicación h de partida. Así pues, el miembro derecho de la igualdad anterior ha de ser nulo cualesquiera que sean los valores de x_{kl}. Si hacemos $x_{ij} = 1$ y $x_{kl} = 0$ cuando $(k,l) \neq (i,j)$, nos queda que

$$\frac{1}{|G|} \sum_{\sigma \in G} r^1_{i,i}(\sigma) r^2_{jj}(\sigma^{-1}) = 0$$

y, sumando para todo i, j, queda que

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{\sigma \in G} \chi_1(\sigma)\chi_2(\sigma^{-1}) = 0.$$

Tomemos ahora $\rho_1 = \rho_2$. Entonces el lema de Schur nos da que $h^0(v) = \alpha v$ para todo $v \in V_1$. El valor de α depende de h, y podemos calcularlo. Para ello observamos que

$$n\alpha = \mathrm{Tr}(h^0) = \frac{1}{|G|} \sum_{\sigma \in G} \mathrm{Tr}(\rho_1(\sigma) \circ h \circ \rho_2(\sigma^{-1})) = \frac{1}{|G|} \sum_{\sigma \in G} \mathrm{Tr}(h) = \mathrm{Tr}(h),$$

luego $\alpha = (1/n)\,\mathrm{Tr}(h)$. En el caso $i \neq j$, tomando igualmente $x_{ij} = 1$ y $x_{kl} = 0$ cuando $(k,l) \neq (i,j)$, obtenemos igualmente que

$$\frac{1}{|G|} \sum_{\sigma \in G} r^1_{i,i}(\sigma) r^1_{jj}(\sigma^{-1}) = 0.$$

En cambio, para $i = j$, la misma elección de x_{kl} hace que $\mathrm{Tr}(h) = 1$, luego

$$\frac{1}{n} = \frac{1}{|G|}\sum_{\sigma\in G} r^1_{i,i}(\sigma)r^1_{jj}(\sigma^{-1}).$$

Al sumar para todo i y todo j, la igualdad $i = j$ se da n veces, luego sumamos n veces la última ecuación y llegamos a que

$$\langle\chi_1,\chi_1\rangle = \frac{1}{|G|}\sum_{\sigma\in G}\chi_1(\sigma)\chi_1(\sigma^{-1}) = 1.$$

■

En realidad, la prueba del teorema anterior contiene más información que la que indica su enunciado, puesto que hemos probado que $\langle\chi_1,\chi_2\rangle = 0$, no bajo la hipótesis de que $\chi_1 \neq \chi_2$, sino bajo la hipótesis de que las representaciones ρ_1 y ρ_2 no eran isomorfas. Por consiguiente, si dos representaciones irreducibles no son isomorfas, sus caracteres χ_1 y χ_2 han de ser distintos o, de lo contrario, cumplirían que $\langle\chi_1,\chi_2\rangle = 1$, mientras que hemos visto que $\langle\chi_1,\chi_2\rangle = 0$.

En otras palabras, tenemos que dos representaciones irreducibles de un grupo G son isomorfas si y sólo si determinan el mismo carácter. Enseguida probaremos que esto es cierto aunque las representaciones no sean irreducibles, pero para ello conviene probar antes lo siguiente:

Teorema 11.25 *Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación de G, sea ϕ su carácter y sea $V = W_1 \oplus \cdots \oplus W_m$ una descomposición de V en subespacios invariantes irreducibles. Para cada carácter irreducible χ de G, el número de subespacios W_i que determinan una representación con carácter χ es $\langle\phi,\chi\rangle$.*

Demostración: Sea χ_i el carácter de la subrepresentación asociada a W_i. Entonces $\phi = \chi_1 + \cdots + \chi_m$, luego $\langle\phi,\chi\rangle = \langle\chi_1,\chi\rangle + \cdots + \langle\chi_m,\chi\rangle$, y las relaciones de ortogonalidad implican que este valor es el número de índices i tales que $\chi_i = \chi$. ■

Dicho de otro modo, si una representación tiene carácter ϕ, es necesariamente la suma directa de tantas representaciones irreducibles de carácter χ como indica el producto $\langle\phi,\chi\rangle$. Así pues:

Teorema 11.26 *Dos representaciones de un grupo finito G son isomorfas si y sólo si determinan el mismo carácter.*

Concluimos también que todo carácter ϕ se descompone de forma única como combinación lineal

$$\phi = n_1\chi_1 + \cdots + n_m\chi_m$$

de caracteres irreducibles con coeficientes enteros $n_i \geq 0$. Además,

$$\langle\phi,\phi\rangle = n_1^2 + \cdots + n_m^2,$$

luego ϕ es irreducible si y sólo si $\langle\phi,\phi\rangle = 1$.

Ejemplo El carácter χ que hemos calculado para el grupo D_4 es irreducible, pues

$$\langle \chi, \chi \rangle = \frac{1}{8} \sum_{\sigma \in G} \chi(\sigma)^2 = \frac{1}{8}(4+4) = 1.$$

■

Vamos a probar que el número de caracteres irreducibles es finito. Para ello consideramos la representación regular $\rho : G \longrightarrow \mathrm{Aut}(K[G])$. Llamemos r_G a su carácter.

Fijemos $\tau \in G$. Si $\tau \neq 1$ la matriz de $\rho(\tau)$ respecto de la base G tiene en la fila correspondiente a σ un único 1 situado en la columna correspondiente a $\sigma\tau \neq \sigma$, y ceros en los demás lugares, luego la diagonal es nula y, por consiguiente $r_G(\tau) = 0$. Concluimos que el carácter regular viene dado por

$$r_G(\tau) = \begin{cases} g & \text{si } \tau = 1, \\ 0 & \text{si } \tau \neq 1, \end{cases}$$

donde g es el orden de G.

Ahora, si χ es cualquier carácter irreducible de G, tenemos que

$$\langle r_G, \chi \rangle = \chi(1).$$

Por lo tanto, si $r_G = n_1\chi_1 + \cdots + n_h\chi_h$ es la descomposición de r_G en suma de caracteres irreducibles, los caracteres χ_i resultan ser todos los caracteres irreducibles de G, y $n_i = \chi_i(1)$ es el grado de χ_i. Teniendo en cuenta que $\langle r_G, r_G \rangle = g$, tenemos probado el teorema siguiente:

Teorema 11.27 *Un grupo finito G tiene un número finito de caracteres irreducibles $\chi_1, \ldots, \chi_h$, cuyos grados n_i verifican la relación*

$$n_1^2 + \cdots + n_h^2 = |G|.$$

Ejemplo El grupo D_4 tiene cinco clases de conjugación, luego cinco caracteres irreducibles, $\chi_1, \chi_2, \chi_3, \chi_4, \chi_5$, de los cuales conocemos dos: el carácter trivial $\chi_1 = 1$ y el calculado en la página 362 (al que numeraremos como χ_5). Los tres que faltan tienen grados n_i que han de cumplir $1 + n_2^2 + n_3^2 + n_4^2 + 4 = 8$, luego los tres han de ser de grado 1. ■

Si aplicamos el teorema 11.27 al caso $K = \mathbb{A}$, vemos que G tiene h representaciones irreducibles sobre $\mathbb{A}$, con caracteres χ_i, cuyos grados al cuadrado suman $|G|$. Si ahora K es un cuerpo arbitrario (algebraicamente cerrado de característica 0), cada una de las representaciones irreducibles de G sobre $\mathbb{A}$ determina por extensión de escalares (definición 11.5) una representación sobre K con la misma representación matricial asociada, por lo que tiene el mismo grado y, más aún, el mismo carácter. Como la relación $\langle \chi_i, \chi_i \rangle = 1$ no depende del cuerpo considerado, vemos que las extensiones de las representaciones de G sobre $\mathbb{A}$ siguen siendo irreducibles sobre K y, como sus grados siguen sumando $|G|$, no puede haber más representaciones irreducibles de G sobre K.

Si, por último, tenemos en cuenta que toda representación es suma directa de representaciones irreducibles, tenemos probado el teorema siguiente:

Teorema 11.28 *Toda representación de un grupo G sobre un cuerpo K es isomorfa a la extensión de escalares de una representación ρ de G sobre $\mathbb{A}$. Además, la extensión ρ^K es irreducible si y sólo si lo es ρ. En particular, los caracteres (irreducibles) de G sobre K coinciden con sus caracteres (irreducibles) sobre $\mathbb{A}$.*

Por consiguiente, a partir de aquí podríamos trabajar exclusivamente en el caso $K = \mathbb{A}$ sin pérdida de generalidad, pero nos será más cómodo aún trabajar en el caso $K = \mathbb{C}$.

11.3 Caracteres complejos

Para trabajar con caracteres complejos es más natural sustituir la forma bilineal $\langle\ ,\ \rangle$ por el siguiente producto escalar:

Definición 11.29 Si G es un grupo finito, definimos en el espacio vectorial $\mathbb{C}^G$ el producto escalar dado por

$$(\phi, \psi) = \frac{1}{|G|} \sum_{\sigma \in G} \phi(\sigma)\overline{\psi(\sigma)}.$$

Observemos que es ciertamente un producto escalar, es decir, que cumple las propiedades[2]

a) $(\phi, \psi) = \overline{(\psi, \phi)}$,

b) $(\phi + \psi, \chi) = (\phi, \chi) + (\psi, \chi), \quad (\phi, \psi + \chi) = (\phi, \psi) + (\phi, \chi)$

c) $(\alpha\phi, \psi) = \alpha(\phi, \psi), \quad (\phi, \alpha\psi) = \bar{\alpha}(\phi, \psi)$

d) $(\phi, \phi) \geq 0$ y $(\phi, \phi) = 0$ si y sólo si $\phi = 0$,

para todo ϕ, ψ, $\chi \in \mathbb{C}^G$ y todo $\alpha \in \mathbb{C}$.

Por otra parte, el teorema 11.18 prueba que, si $\phi, \psi \in \mathbb{C}^G$ son caracteres de G, entonces $\langle \phi, \psi \rangle = (\phi, \psi)$. Ahora observamos que en la sección anterior sólo hemos usado la forma bilineal $\langle\ ,\ \rangle$ sobre caracteres, por lo que todos los resultados de la sección anterior son válidos igualmente cambiando la forma bilineal $\langle\ ,\ \rangle$ por el producto escalar $(\ ,\ )$.

Para trabajar con funciones arbitrarias de $\mathbb{C}^G$ es más práctico el producto escalar.

Definición 11.30 Si G es un grupo finito, una *función de clases* en G es una aplicación $f : G \longrightarrow \mathbb{C}$ tal que $f(\rho^{-1}\tau\rho) = f(\tau)$ para todo par de elementos $\tau, \rho \in G$, es decir, una función que es constante en cada clase de conjugación de G. Llamaremos $F(G) \subset \mathbb{C}^G$ al subespacio vectorial formado por todas las funciones de clases.

[2]Véase la definición 1.1 de mi libro de Análisis.

Tras la definición 11.14 hemos probado que los caracteres de G son funciones de clases. Tenemos un isomorfismo natural $K^G \cong K[G]$ de espacios vectoriales que identifica cada función $\phi \in K^G$ con el elemento

$$\sum_{\sigma\in G} \phi(\sigma)\sigma \in K[G].$$

De acuerdo con el teorema 11.13, este isomorfismo hace corresponder $F(G)$ con el centro de $\mathbb{C}[G]$.

Probamos ahora una nueva consecuencia del lema de Schur, de la que extraeremos a su vez numerosas consecuencias sobre los caracteres de un grupo finito.

Teorema 11.31 *Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación irreducible de grado n y carácter χ, y sea $\phi \in F(G)$ una función de clases, que podemos identificar con*

$$x = \sum_{\sigma\in G} \phi(\sigma)\sigma \in Z(\mathbb{C}[G]).$$

Entonces, para todo $v \in V$, se cumple que

$$vx = \frac{|G|}{n}(\phi, \overline{\chi})v.$$

Demostración: Como x está en el centro de $\mathbb{C}[G]$, es claro que la aplicación lineal $f : V \longrightarrow V$ dada por $f(v) = vx$ es un homomorfismo de $\mathbb{C}[G]$-módulos, luego el lema de Schur implica que existe un $\alpha \in \mathbb{C}$ tal que $f(v) = \alpha v$, para todo $v \in V$. Sólo hemos de calcular α. Para ello usamos la linealidad de la traza:

$$n\alpha = \mathrm{Tr}(f) = \sum_{\sigma\in G} \phi(\sigma)\,\mathrm{Tr}(\sigma) = \sum_{\sigma\in G} \phi(\sigma)\chi(\sigma) = |G|(\phi, \overline{\chi}).$$

■

La primera consecuencia es la siguiente:

Teorema 11.32 *Si G es un grupo finito, sus caracteres irreducibles forman una base (ortonormal) del espacio $F(G)$ de las funciones de clases.*

Demostración: Sean $\chi_1, \ldots, \chi_h$ los caracteres irreducibles de G. Las relaciones de ortogonalidad implican que son linealmente independientes, luego sólo hemos de probar que generan H. Para ello basta probar que la dimensión de H es h y, a su vez, para ello basta probar que los conjugados $\overline{\chi}_1, \ldots, \overline{\chi}_h$ generan H. Notemos que $(\overline{\chi}_i, \overline{\chi}_j) = (\chi_j, \chi_i)$, luego los conjugados también son ortonormales.

Tomamos $\psi \in H$ y consideramos la función de clases

$$\phi = \psi - \sum_{i=1}^{h} (\psi, \overline{\chi}_i)\overline{\chi}_i,$$

que tiene la propiedad de que $(\phi, \overline{\chi}_i) = 0$ para todo i. Sólo hemos de probar que esto implica que $\phi = 0$. Sea $x \in Z(\mathbb{C}[G])$ el elemento correspondiente a ϕ a través del isomorfismo natural.

Consideremos una representación $\rho : G \longrightarrow \mathrm{Aut}(V)$. Si es irreducible, el teorema anterior nos da que $vx = 0$, para todo $v \in V$. Si no es irreducible, llegamos a la misma conclusión descomponiéndolo en suma directa de submódulos irreducibles.

Vamos a aplicar esto al caso en que $V = \mathbb{C}[G]$, es decir, a la representación regular de G, y para $v = 1$. Entonces,

$$0 = 1x = \sum_{\sigma \in G} \phi(\sigma)\sigma,$$

luego $\phi = 0$. ∎

Es evidente que la dimensión de $F(G)$ es igual al número de clases de conjugación de G, luego:

Teorema 11.33 *El número de caracteres irreducibles de un grupo G es igual a su número de clases de conjugación.*

Si $\chi_1, \ldots, \chi_h$ son los caracteres irreducibles de un grupo G, tenemos que toda función de clases f se expresa de forma única como

$$f = \sum_{i=1}^{h} (f, \chi_i)\chi_i,$$

luego la condición necesaria y suficiente para que una función de clases $f \neq 0$ sea un carácter es que (f, χ_i) sea un número natural para todo i.

En las condiciones de 11.31, consideremos la aplicación $T : Z(\mathbb{C}[G]) \longrightarrow \mathbb{C}$ dada por

$$T(x) = \frac{|G|}{n}(\phi, \overline{\chi}).$$

Según 11.25, el homomorfismo $V \longrightarrow V$ dado por $v \mapsto vx$ es la homotecia de razón $T(x)$. Como $(vx)y = v(xy)$, concluimos que la homotecia de razón $T(xy)$ es la composición de la homotecia de razón $T(x)$ seguida de la homotecia de razón $T(y)$ o, más simplemente: $T(xy) = T(x)T(y)$. Es obvio que T conserva la suma, de modo que es un homomorfismo de anillos (conmutativos y unitarios). Con esto podemos probar:

Teorema 11.34 *Los grados de las representaciones irreducibles de un grupo G dividen al orden de G.*

Demostración: Según 11.13, si $\mathrm{cl}(G) = \{c_1, \ldots, c_h\}$, el centro de $\mathbb{C}[G]$ tiene por base los elementos de la forma

$$e_i = \sum_{\sigma \in c_i} \sigma.$$

Es claro que $cd \in \langle c_1, \ldots, c_h\rangle_{\mathbb{Z}}$, luego el álgebra $\mathbb{Z}[c_1, \ldots, c_h]$ es un $\mathbb{Z}$-módulo finitamente generado, lo que prueba ([AC 3.58]) que los c_i son enteros sobre $\mathbb{Z}$.

Si χ es un carácter irreducible de G, tenemos que

$$x = \sum_{\sigma\in G} \overline{\chi}(\sigma)\sigma = \sum_{i=1}^{h} \overline{\chi}(\sigma_i)e_i$$

donde hemos elegido $\sigma_i \in c_i$. Como $\overline{\chi}(\sigma_i)$ es un entero algebraico, concluimos que x es entero sobre $\mathbb{Z}$, luego $T(x) \in \mathbb{C}$ es un entero algebraico. Explícitamente:

$$T(x) = \frac{|G|}{n}(\overline{\chi}, \overline{\chi}) = \frac{|G|}{n}(\chi, \chi) = \frac{|G|}{n}.$$

Como es un entero algebraico y un número racional, concluimos que es entero, y así, $n \mid |G|$. ∎

Los teoremas 11.27 y 11.33 nos dan una caracterización de los grupos abelianos:

Teorema 11.35 *Un grupo finito G es abeliano si y sólo si todos sus caracteres irreducibles tienen grado* 1.

Demostración: Sea g el orden de G y h su número de clases. Es claro que G es abeliano si y sólo si $g = h$. Si $n_1, \ldots, n_h$ son los grados de los caracteres irreducibles de G, sabemos que

$$n_1^2 + \cdots + n_h^2 = g,$$

luego $g = h$ si y sólo si $n_i = 1$ para todo i. ∎

Observemos que $\mathrm{LG}(1, \mathbb{C}) \cong \mathbb{C}^*$ y el isomorfismo puede verse como el que a cada matriz le asigna su traza, luego una representación matricial de grado 1 de un grupo G puede verse como un homomorfismo de grupos $G \longrightarrow \mathbb{C}^*$, que se identifica a su vez con su carácter. En definitiva, los caracteres de grado 1 de un grupo finito G son simplemente los homomorfismos de grupos[3] $\chi : G \longrightarrow \mathbb{C}^*$.

Ejemplo Nos faltaba calcular los caracteres de grado 1 del grupo D_4. Observemos que el centro de D_4 es $Z(D_4) = \{1, \sigma^2\}$. (El centro de un grupo está formado por los elementos cuya clase de conjugación es trivial.) El cociente $D_4/Z(D_4)$ es abeliano, luego tiene cuatro caracteres de grado 1, que son, por lo tanto, los tres caracteres que buscamos, más el trivial.

Concretamente, $D_4/Z(D_4) \cong C_2 \times C_2$, sus elementos tienen todos orden 2, luego sus caracteres tienen que tomar valores en $\mathbb{C}^*$ iguales a ± 1. Teniendo esto en cuenta es fácil calcular la *tabla de caracteres* irreducibles de D_4:

D_4	1	σ	σ^2	τ	$\sigma\tau$
χ_1	1	1	1	1	1
χ_2	1	1	1	−1	−1
χ_3	1	−1	1	1	−1
χ_4	1	−1	1	−1	1
χ_5	2	0	−2	0	0

[3]En particular, los caracteres irreducibles de los grupos abelianos finitos coinciden con los caracteres definidos, por ejemplo, en 11.12 de mi libro de Teoría de números.

Notemos que podríamos haber calculado χ_5 a partir de los otros caracteres sin necesidad de conocer la representación que lo genera. Basta tener en cuenta que $r_G = \chi_1 + \chi_2 + \chi_3 + \chi_4 + 2\chi_5$ y que r_G toma siempre el valor 0 salvo en 1. ∎

Ejemplo En $Q = \mathbb{R}^4$ es posible definir una estructura de anillo de división conocida como el álgebra de los cuaterniones.[4] Si llamamos $1, i, j, k$ a la base canónica de $\mathbb{R}^4$, el producto de Q está completamente determinado por las relaciones

$$i^2 = j^2 = k^2 = -1, \quad ij = k, \quad ji = -k, \quad jk = i, \quad kj = -i, \quad ki = j, \quad ik = -j.$$

Se sigue entonces que el conjunto $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ es un subgrupo del grupo de unidades de Q, conocido como el grupo cuaternio. Tiene cinco clases de conjugación:

$$\mathrm{cl}(Q_8) = \{\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}\}$$

y el cociente $Q_8/\{\pm 1\} \cong C_2 \times C_2$ nos da cuatro caracteres de grado 1 análogos a los que hemos obtenido para D_4 en el ejemplo anterior. Esto implica que el quinto carácter ha de tener grado 2 y, teniendo en cuenta que puede calcularse a partir del carácter regular de Q_8, concluimos que la tabla de caracteres de Q_8 es idéntica a la de D_4 (biyectando adecuadamente las clases de conjugación), a pesar de que ambos grupos no son isomorfos. ∎

Ejercicio: Calcular la tabla de caracteres de Σ_3.

Terminamos con otra consecuencia del teorema 11.31:

Teorema 11.36 *Sea G un grupo finito y sean $\chi_1, \ldots, \chi_h$ sus caracteres irreducibles. Si V es un $\mathbb{C}[G]$-módulo y llamamos V_i a la suma de todos sus $\mathbb{C}[G]$-submódulos irreducibles de carácter χ_i, se cumple que*

$$V = \bigoplus_{i=1}^{h} V_i.$$

Equivalentemente: podemos encontrar distintas descomposiciones de V en suma directa de $\mathbb{C}[G]$-submódulos irreducibles, pero, si en cada una de ellas agrupamos todos los sumandos correspondientes al mismo carácter χ_i, el módulo V_i que obtenemos es independiente de la descomposición de partida.

Demostración: Llamemos n_i al grado de χ_i. Consideremos el elemento

$$x = \frac{n_i}{|G|} \sum_{\sigma \in G} \overline{\chi_i(\sigma)}\sigma \in Z(\mathbb{C}[G])$$

[4]En la sección 1.4 de mi libro de Álgebra está construido el anillo de división de los cuaterniones racionales. El álgebra de los cuaterniones se obtiene sin más que cambiar $\mathbb{Q}$ por $\mathbb{R}$ en toda la construcción.

y llamemos $p_i : V \longrightarrow V$ a la aplicación lineal dada por $v \mapsto vx$. Como $x \in Z(\mathbb{C}[G])$, se trata, de hecho, de un homomorfismo de $\mathbb{C}[G]$-módulos.

Si W es un $\mathbb{C}[G]$-submódulo irreducible de V, la restricción $p_i|_W : W \longrightarrow W$ es también la multiplicación por x, y podemos aplicar el teorema 11.31, según el cual $p_i|_W$ es la homotecia de razón

$$\frac{n_i}{n}(\overline{\chi}_i, \overline{\chi}) = \frac{n_i}{n}(\chi, \chi_i),$$

donde χ es el carácter de W y n su grado. Así pues, $p_i|_W = 0$ si $\chi \neq \chi_i$ y $p_i|_W$ es la identidad si $\chi = \chi_i$. Esto implica que la imagen de p_i es V_i, que $p_i : V \longrightarrow V_i$ se restringe a la identidad en V_i y que es nula sobre cada V_j con $j \neq i$. Es obvio que V es la suma de los V_i y la existencia de estas proyecciones implica que la suma es directa. ∎

11.4 Caracteres inducidos

Si G es un grupo finito y H es un subgrupo, podemos considerar a $\mathbb{C}[H]$ como subespacio vectorial de $\mathbb{C}[G]$, lo que, a su vez, nos permite considerar a $\mathbb{C}[G]$ como $\mathbb{C}[H]$-módulo. Esto nos lleva a la definición siguiente:

Definición 11.37 Sea G un grupo finito y H un subgrupo. Consideremos una representación lineal $\rho : H \longrightarrow \mathrm{Aut}(W)$. Llamaremos *representación inducida* ρ^G a la representación de G asociada al $\mathbb{C}[G]$-módulo $W \otimes_{\mathbb{C}[H]} \mathbb{C}[G]$. Si ψ es el carácter de ρ, llamaremos *carácter inducido* ψ^G al carácter de G asociado a ρ^G.

Es obvio que, si $H \leq K \leq G$ y ψ es un carácter de H, entonces $(\psi^K)^G = \psi^G$.

Vamos a ver que ψ^G puede calcularse directamente a partir de ψ sin necesidad de conocer la representación que lo genera. Para ello conviene introducir la notación siguiente:

Definición 11.38 Sea G un grupo finito y H un subgrupo de G. Si ϕ es una función de clases en H, llamaremos $\phi^0 : G \longrightarrow \mathbb{C}$ a la función dada por

$$\phi^0(\sigma) = \begin{cases} \phi(\sigma) & \text{si } \sigma \in H, \\ 0 & \text{si } \sigma \notin H. \end{cases}$$

En estos términos, los caracteres inducidos se calculan como indica el teorema siguiente:

Teorema 11.39 *Sea G un grupo finito y H un subgrupo y sea R un sistema de representantes de las clases de congruencia por la derecha de G módulo H. Entonces, si ψ es un carácter de H, para todo $\sigma \in G$ se cumple que*

$$\psi^G(\sigma) = \sum_{\tau \in R} \psi^0(\tau\sigma\tau^{-1}) = \frac{1}{|H|} \sum_{\tau \in G} \psi^0(\tau\sigma\tau^{-1}).$$

DEMOSTRACIÓN: Sea $\rho : H \longrightarrow \mathrm{Aut}(W)$ la representación que determina el carácter dado ψ. Tenemos que cada $\sigma \in G$ se expresa de forma única como $\sigma = h\tau$, con $\tau \in R$. Es claro entonces que

$$\mathbb{C}[G] = \bigoplus_{\tau\in R} \mathbb{C}[H]\tau.$$

Por consiguiente, ψ^G es el carácter de

$$V = W \otimes_{\mathbb{C}[H]} \mathbb{C}[G] = \bigoplus_{\tau\in R} W\tau.$$

Fijado $\sigma \in G$, para cada $\tau \in R$, podemos expresar $\tau\sigma = h\tau_\sigma$, con $\tau_\sigma \in R$ y $h \in H$. De este modo, $(W\tau)\sigma = W\tau_\sigma$. Si fijamos una base B de W, la unión de los trasladados $B\tau$, con $\tau \in R$, es una base de V. Para calcular la traza de $\rho^G(\sigma)$ en esta base observamos que, si $\tau_\sigma \neq \tau$, las filas de la matriz de $\rho^G(\tau)$ correspondientes a los vectores de B^τ tienen ceros en la diagonal. Por el contrario, si $\tau_\sigma = \tau$, las suma de la diagonal de las filas correspondientes a $B\tau$ es la traza de $\rho^G(\sigma)|_{W\tau}$. Así pues:

$$\psi^G(\sigma) = \sum_{\tau\in R_\sigma} \mathrm{Tr}(\rho^G(\sigma)|_{W\tau}),$$

donde $R_\sigma = \{\tau \in R \mid \tau_\sigma = \tau\}$. Observemos que $\tau_\sigma = \tau$ equivale a que $\tau\sigma = h\tau$, es decir, que $\tau\sigma\tau^{-1} \in H$. Por último, observamos que el isomorfismo $f : W \longrightarrow W\tau$ dado por $f(w) = w\tau$ cumple

$$f(w\tau\sigma\tau^{-1}) = w\tau\sigma = f(w)\sigma.$$

Esto significa que $\rho^G(\sigma)|_{W\tau}$ se identifica a través de f con $\rho(\tau\sigma\tau^{-1})$, luego

$$\mathrm{Tr}(\rho^G(\sigma)|_{W\tau}) = \mathrm{Tr}(\rho(\tau\sigma\tau^{-1})) = \psi(\tau\sigma\tau^{-1}) = \psi^0(\tau\sigma\tau^{-1}).$$

Con esto obtenemos la primera fórmula del enunciado. La segunda se sigue de la primera debido a que, si $\tau \in R$ cumple $\tau\sigma\tau^{-1} \in H$, entonces, para cada $h \in H$ tenemos que $\tau' = h\tau \in G$ cumple $\tau'\sigma\tau'^{-1} \in H$ y $\psi(\tau'\sigma\tau'^{-1}) = \psi(\tau\sigma\tau^{-1})$ y, recíprocamente, todo $\tau' \in G$ que cumple $\tau'\sigma\tau'^{-1} \in H$ es de la forma $\tau' = h\tau$, para un único $\tau \in R$ tal que $\tau\sigma\tau^{-1} \in H$. En definitiva, cada sumando de la primera fórmula se corresponde con $|H|$ sumandos idénticos en la segunda. ∎

En particular, tenemos la relación entre los grados:

$$\psi^G(1) = |G : H|\psi(1).$$

Definición 11.40 Sea G un grupo finito, sea H un subgrupo de G y sea R un sistema de representantes de las clases de congruencia por la derecha de G módulo H. Para cada función de clases $\phi : H \longrightarrow \mathbb{C}$, definimos $\phi^G : G \longrightarrow \mathbb{C}$ mediante

$$\phi^G(\sigma) = \sum_{\tau\in R} \phi^0(\tau\sigma\tau^{-1}) = \frac{1}{|H|}\sum_{\tau\in G} \phi^0(\tau\sigma\tau^{-1}).$$

Hemos visto que si ϕ es un carácter de H, entonces ϕ^G es un carácter de G. En general, se cumple que ϕ^G es una función de clases de G. Esto se comprueba directamente sin dificultad o, alternativamente, basta observar que la aplicación $\phi \mapsto \phi^G$ es $\mathbb{C}$-lineal y que toda función de clases es combinación lineal de caracteres.

Notemos que también hay una forma natural (y mucho más simple) de pasar de un carácter de G a un carácter de H:

Definición 11.41 Sea G un grupo finito y H un subgrupo de G. Si ϕ es una función de clases de G, llamaremos ϕ_H a su restricción a H, que es también una función de clases en H, y es un carácter si ϕ lo es.

Entre estas dos operaciones hay una relación sencilla:

Teorema 11.42 (Reciprocidad de Frobenius) *Sea G un grupo finito y H un subgrupo. Sean $\phi : H \longrightarrow \mathbb{C}$ y $\psi : G \longrightarrow \mathbb{C}$ funciones de clases. Entonces*

$$(\phi, \psi_H) = (\phi^G, \psi).$$

Demostración: Basta realizar un cálculo directo:

$$(\phi^G, \psi) = \frac{1}{|G|}\sum_{\sigma\in G}\phi^G(\sigma)\overline{\psi(\sigma)} = \frac{1}{|G|}\,\frac{1}{|H|}\sum_{\sigma,\tau\in G}\phi^0(\tau\sigma\tau^{-1})\overline{\psi(\sigma)}$$

$$= \frac{1}{|G|}\,\frac{1}{|H|}\sum_{\sigma',\tau\in G}\phi^0(\sigma')\overline{\psi(\tau^{-1}\sigma'\tau)} = \frac{1}{|G|}\,\frac{1}{|H|}\sum_{\sigma',\tau\in G}\phi^0(\sigma')\overline{\psi(\sigma')}$$

$$= \frac{1}{|H|}\sum_{\sigma'\in H}\phi(\sigma')\overline{\psi(\sigma')} = (\phi, \psi_H).$$

■

Ejemplo Vamos a calcular la tabla de caracteres de Σ_4. El grupo tiene cinco clases de conjugación (una para cada tipo de descomposición en producto de ciclos disjuntos), luego Σ_5 tiene cinco caracteres irreducibles, $\chi_1, \chi_2, \chi_3, \chi_4, \chi_5$. Por simplificar la exposición damos ya la tabla y a continuación explicamos cómo se obtiene:

Σ_4	1	(ab)	(abc)	$(abcd)$	$(ab)(cd)$
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	1	-1

Tomamos como χ_1 el carácter trivial, con lo que podemos rellenar con unos la primera fila de la tabla.

El grupo Σ_4 contiene al grupo alternado A_4 como subgrupo normal, y el cociente tiene orden 2, por lo que induce un carácter no trivial de grado 1 que

es el homomorfismo $\chi_2 : \Sigma_4 \longrightarrow \mathbb{C}$ que toma el valor 1 sobre A_4 y el valor -1 sobre los elementos que no están en A_4. Esto nos da la segunda fila de la tabla.

Sea $H = \Sigma_3$, que podemos identificar con el subgrupo de Σ_4 formado por las permutaciones que dejan fijo al 4. Si llamamos 1_H al carácter trivial de H, tenemos que $(1_H^G, 1_G) = (1_H, 1_H) = 1$, luego $1_H^G - 1_G$ es un carácter de G, y su grado es 3. Vamos a calcularlo y veremos que es irreducible.

Un sistema de representantes de las clases módulo Σ_3 es claramente

$$R = \{1, (1,4), (2,4), (3,4)\}.$$

Como 1_H toma siempre el valor 1, tenemos que

$$1_H^G(\sigma) = \sum_{\tau \in R} 1_H^0(\tau\sigma\tau^{-1})$$

es simplemente el número de conjugados de σ por elementos de R que pertenecen a Σ_3, es decir, que fijan al 4. Por ejemplo, para calcular $1_H^G((1,2))$ observamos que

$$(1,2)^1 = (1,2), \quad (1,2)^{(1,4)} = (4,2), \quad (1,2)^{(2,4)} = (1,4), \quad (1,2)^{(3,4)} = (1,2),$$

por lo que $1_H^G((1,2)) = 2$. De este modo se calcula:

	1	(ab)	(abc)	$(abcd)$	$(ab)(cd)$
1_H^G	4	2	1	0	0
χ_4	3	1	0	-1	-1

donde hemos llamado $\chi_4 = 1_H^G - 1$. Ya hemos justificado que es un carácter. Para comprobar que es irreducible calculamos:

$$(\chi_4, \chi_4) = \frac{1}{24}(3^2 + 6 \cdot 1^2 + 6 \cdot (-1)^2 + 3 \cdot (-1)^2) = 1.$$

Esto nos da la cuarta fila de la tabla. La quinta fila es el carácter $\chi_5 = \chi_2\chi_4$, que también es irreducible porque $(\chi_5, \chi_5) = 1$.

Nos falta calcular χ_3. El teorema 11.27 nos da que tiene grado 2, luego podemos calcular χ_3 despejando en la ecuación

$$r_G = \chi_1 + \chi_2 + 2\chi_3 + 3\chi_4 + 3\chi_5.$$

Esto completa la tabla. ∎

Otra fórmula de interés que relaciona funciones de clase inducidas y restricciones es la siguiente:

Teorema 11.43 *Sea G un grupo finito y H un subgrupo. Sean $\phi : H \longrightarrow \mathbb{C}$ y $\psi : G \longrightarrow \mathbb{C}$ funciones de clases. Entonces $(\phi \cdot \psi_H)^G = \phi^G \cdot \psi$.*

DEMOSTRACIÓN: Para cada $\sigma \in G$, tenemos que

$$(\phi \cdot \psi_H)^G(\sigma) = \frac{1}{|H|}\sum_{\tau\in G}\phi^0(\tau\sigma\tau^{-1})\psi_H^0(\tau\sigma\tau^{-1})$$

$$= \frac{1}{|H|}\sum_{\tau\in G}\phi^0(\tau\sigma\tau^{-1})\psi(\sigma) = \phi^G(\sigma)\psi(\sigma).$$

■

Ahora necesitamos un resultado técnico:

Teorema 11.44 *Sea G un grupo finito y N un subgrupo normal, sea χ un carácter irreducible de G tal que χ_N sea suma de al menos dos caracteres distintos. Entonces existe un subgrupo $N \leq H < G$ y un carácter irreducible ψ de H tal que $\chi = \psi^G$.*

DEMOSTRACIÓN: Sea V un $\mathbb{C}[G]$-módulo asociado a χ, de modo que χ_N está asociado a V como $\mathbb{C}[N]$-módulo. Sea

$$V = \bigoplus_{i=1}^{h} V_i$$

la descomposición de V como $\mathbb{C}[N]$-módulo dada por el teorema 11.36. Por hipótesis, la suma tiene al menos dos sumandos no nulos.

En general, si W es un $\mathbb{C}[N]$-submódulo de V y $\sigma \in G$, se cumple que $W\sigma$ es también un $\mathbb{C}[N]$-submódulo, pues, si $n \in N$, se cumple que

$$W\sigma n = W(\sigma n\sigma^{-1})\sigma = W\sigma,$$

pues $\sigma n\sigma^{-1} \in N$. Además, si W tiene carácter χ_i, el carácter de $W\sigma$ es

$$\chi^\sigma(n) = \chi(\sigma n\sigma^{-1}),$$

que depende únicamente de χ y σ. Es claro que si W es irreducible, también lo es $W\sigma$, luego vemos que la multiplicación por σ transforma todos los submódulos irreducibles de un mismo V_i (es decir, todos los submódulos con un mismo carácter χ_i, en submódulos de un mismo V_j, por lo que $V_i\sigma = V_j$.

Fijemos un índice i_0 tal que $V_{i_0} \neq 0$ y sea $H = \{\sigma \in H \mid V_{i_0}\sigma = V_{i_0}\}$. Claramente, $N \leq H < G$. La segunda desigualdad es estricta porque, de lo contrario, V_{i_0} sería un $\mathbb{C}[G]$-submódulo de V, pero V es irreducible, luego sería $V = V_{i_0}$, cuando, por hipótesis, hay al menos dos sumandos no nulos.

Sea ψ el carácter de H asociado a $W = V_{i_0}$. Para probar que $\chi = \psi^G$ basta ver que, si R es un sistema de representantes de las clases de congruencia por la derecha de G módulo H, se cumple que

$$V = \bigoplus_{\tau\in R} W\tau,$$

pues esto implica que $V \cong W \times_{\mathbb{C}[H]} \mathbb{C}[G]$.

Si $\tau_1, \tau_2 \in R$ y $W\tau_1 = W\tau_2$, entonces $\tau_1\tau_2^{-1} \in H$, luego $\tau_1 = \tau_2$. Esto implica que cada $W\tau = V_{i_0}\tau$ con $\tau \in R$ es un V_i, luego la suma de los $W\tau$ es directa (porque lo es la de los V_i). Además, dicha suma directa es un $\mathbb{C}[G]$-submódulo de V, luego es todo V. ∎

Definición 11.45 Recordemos que un grupo finito G es resoluble si existe una serie de subgrupos

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

en la que cada cociente G_i/G_{i-1} es abeliano. Se dice que G es *superresoluble* si existe una serie análoga en la que cada G_i es normal en G y cada cociente G_i/G_{i-1} es cíclico.

Es inmediato que los subgrupos y los cocientes de un grupo superresoluble son superresolubles, pues si $N \trianglelefteq G$, podemos considerar la serie

$$1 = G_0N/N \trianglelefteq G_1N/N \trianglelefteq \cdots \trianglelefteq G_nN/N = G/N$$

en la que todos los términos cumplen $G_iN/N \trianglelefteq G/N$ y tenemos un epimorfismo

$$G_i/G_{i-1} \longrightarrow (G_iN/N) \,/\, (G_{i-1}N/N),$$

luego los cocientes también son cíclicos.

Similarmente, si $H \leq G$, consideramos la serie

$$1 = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \cdots \trianglelefteq G_n \cap H = H,$$

donde ahora tenemos monomorfismos

$$(G_i \cap H)/(G_{i-1} \cap H) \longrightarrow G_i/G_{i-1}.$$

Sólo necesitaremos una propiedad elemental de los grupos superresolubles:

Teorema 11.46 *Si G es un grupo finito superresoluble no abeliano, entonces existe un subgrupo normal abeliano N que cumple $Z(G) \lhd N \lhd G$ (donde $Z(G)$ es el centro de G).*

Demostración: El cociente $G/Z(G) \neq 1$ es superresoluble, luego podemos considerar el primer término no trivial $N/Z(G) \trianglelefteq G/Z(G)$ de una serie según la definición de grupo superresoluble. Así, se cumple que $Z(G) \lhd N \trianglelefteq G$ y $N/Z(G)$ es cíclico. Es claro entonces que N es abeliano, luego $N \neq G$. ∎

Teorema 11.47 *Si G es un grupo finito superresoluble, todo carácter irreducible de G está inducido por un carácter de grado 1 de un subgrupo de G.*

Demostración: Razonando por inducción, podemos suponer que el teorema es cierto para todo grupo de orden estrictamente menor que $|G|$. Sea χ un

carácter irreducible de G. Podemos suponer que χ es fiel, es decir, que la representación $\rho : G \longrightarrow \mathrm{Aut}(V)$ que lo genera es inyectiva, pues, si tuviera núcleo $N \neq 1$, podríamos ver a χ como carácter de G/N, luego habría un subgrupo $H/N \leq G/N$ y un carácter ψ de grado 1 en H/N tal que $\chi = \psi^G$.

También podemos suponer que G no es abeliano, pues en caso contrario χ ya tiene grado 1 y no hay nada que probar.

Por el teorema anterior, existe un subgrupo $Z(G) \lhd N \lhd G$. Como ρ es un monomorfismo, tenemos que $\rho[N] \lhd Z(\rho[G])$. Por consiguiente, no todos los automorfismos en $\rho[N]$ son homotecias (ya que las homotecias conmutan con todos los automorfismos), luego $\chi|_N$ ha de ser suma de al menos dos caracteres irreducibles distintos. (En caso contrario, como N es abeliano, $\chi|_N$ sería múltiplo de un único carácter de grado 1, y $\rho[N]$ constaría únicamente de homotecias.)

El teorema 11.44 nos da que $\chi = \psi^G$, para cierto carácter irreducible ψ de un subgrupo $H < G$. Como H también es superresoluble, podemos aplicar la hipótesis de inducción para concluir que $\psi = \phi^H$, para cierto carácter ϕ de grado 1, luego también $\chi = \phi^G$. ∎

11.5 El teorema de Brauer

La finalidad de esta sección es demostrar el teorema siguiente:

Teorema 11.48 (Brauer) *Si G es un grupo finito, todo carácter de G se expresa como combinación lineal con coeficientes enteros de caracteres inducidos por caracteres de grado* 1.

Para probarlo empezamos introduciendo el concepto siguiente:

Definición 11.49 Diremos que un grupo finito H es *p-elemental,* donde p es un número primo, si puede expresase como producto directo $H = C \times P$, donde C es un grupo cíclico de orden primo con p y P es un p-grupo (un grupo de orden potencia de p). Un grupo H es *elemental* si es p-elemental para algún primo p.

Todo grupo cíclico finito es p-elemental para todo primo p, pues se descompone como producto de grupos cíclicos de órdenes potencias de primos, y basta agrupar todos los factores que sean p-grupos por una parte, y todos los que no lo sean por otra.

Teorema 11.50 *Todo grupo finito elemental es superresoluble.*

Demostración: Veamos primero que todo p-grupo P es superresoluble. Podemos razonar por inducción sobre el orden de P. Si P es abeliano es evidente. En caso contrario, usamos[5] que $1 < Z(P) < P$. Por hipótesis de inducción $P/Z(P)$ es superresoluble y $Z(P)$ también lo es, por ser abeliano. Al

[5]Teorema 5 del apéndice del Capítulo V de mi libro de Geometría.

enlazar una serie de $Z(P)$ con una serie de $P/Z(P)$ según la definición de grupo superresoluble, obtenemos una serie que cumple la definición para P, porque los subgrupos de $Z(P)$ son normales en P.

Por último, si $H = C \times P$ es p-elemental y

$$1 = P_0 \trianglelefteq P_1 \trianglelefteq \cdots \trianglelefteq P_n = P$$

es una serie según la definición de grupo superresoluble, la serie

$$1 \trianglelefteq C \times P_0 \trianglelefteq C \times P_1 \trianglelefteq \cdots \trianglelefteq C \times P_n = H$$

cumple la definición de grupo superresoluble para H. ∎

Ahora podemos reducir la prueba del teorema de Brauer al resultado siguiente:

Teorema 11.51 *Si G es un grupo finito, todo carácter de G se expresa como combinación lineal con coeficientes enteros de caracteres inducidos desde subgrupos elementales.*

En efecto, de este teorema se sigue el teorema de Brauer, ya que si tenemos

$$\chi = n_1\phi_1^G + \cdots + n_r\phi_r^G,$$

donde cada ϕ_i es un carácter de un subgrupo elemental $H_i \leq G$, descomponiendo cada ϕ_i en suma de caracteres irreducibles podemos suponer que cada ϕ_i es irreducible y, como H_i es superresoluble, el teorema 11.47 nos da que ϕ_i está inducido a su vez por un carácter de grado 1, luego lo mismo vale para ϕ_i^G. ∎

Para tratar con combinaciones lineales enteras de caracteres conviene introducir el concepto siguiente:

Definición 11.52 Si G es un grupo finito y $\chi_1, \ldots, \chi_h$ son sus caracteres irreducibles, llamaremos $R(G) = \mathbb{Z}\chi_1 \oplus \cdots \oplus \mathbb{Z}\chi_h$ al subgrupo generado por los caracteres χ_i en el espacio $F(G)$ de las funciones de clase de G. A sus elementos los llamaremos *caracteres virtuales* de G.

Como los caracteres irreducibles son una base del $\mathbb{C}$-espacio vectorial $F(G)$ de las funciones de clases de G, es claro que también son una base de $R(G)$ como $\mathbb{Z}$-módulo. También es obvio que todo carácter virtual se expresa de forma única como diferencia de dos caracteres. Como el producto de caracteres es un carácter, tenemos que $R(G)$ es un subanillo de $F(G)$.

El teorema 11.51 es consecuencia, a su vez, del teorema siguiente:

Teorema 11.53 *Sea G un grupo finito y sea V_p el subgrupo de $R(G)$ generado por los caracteres inducidos desde subgrupos p-elementales de G. Entonces el cociente $R(G)/V_p$ es finito y su orden es primo con p.*

En efecto, si admitimos este resultado, sólo tenemos que probar que $R(G)$ es la suma V de los subgrupos V_p, para todo primo p. Como $V_p \leq V \leq R(G)$, tenemos que el cociente $R(G)/V$ es finito, y su orden es primo con p, para todo primo p, luego ha de ser $R(G) = V$. ∎

Observemos ahora que, si H es un subgrupo de G, el teorema 11.43 implica que el subgrupo de $R(G)$ generado por los caracteres inducidos desde H es un ideal de $R(G)$, y V_p es la suma de estos ideales cuando H recorre los subgrupos p-elementales de G. Por consiguiente, V_p es también un ideal de $R(G)$. Veamos ahora que 11.53 es consecuencia del teorema siguiente:

Teorema 11.54 *Sea G un grupo finito de orden $|G| = p^i m$, donde $p \nmid m$, y sea V_p el subgrupo de $R(G)$ generado por los caracteres inducidos desde subgrupos p-elementales de G. Entonces $m \in V_p$.*

En efecto, $R(G)$ es un $\mathbb{Z}$-módulo finitamente generado, luego $R(G)/V_p$ también lo es. Por consiguiente, es producto de un número finito de grupos cíclicos.

Si $m \in V_p$, como éste es un ideal, tenemos que $m\phi \in V_p$ para todo $\phi \in R(G)$, lo que significa que todos los elementos de $R(G)/V_p$ tienen orden divisor de m. Por consiguiente, $R(G)/V_p$ es producto de un número finito de grupos cíclicos finitos de orden primo con p, y esto prueba 11.53. ∎

Consideremos ahora el anillo D de los enteros ciclotómicos de orden g, es decir, la $\mathbb{Z}$-subálgebra de $\mathbb{C}$ generada por las raíces g-ésimas de la unidad. Se trata de un $\mathbb{Z}$-módulo libre de rango finito. Fijemos una base $D = \langle \omega_1, \ldots, \omega_c \rangle_{\mathbb{Z}}$ tal que $\omega_1 = 1$. Vamos a trabajar en el producto tensorial $D \otimes_{\mathbb{Z}} R(G)$.

Como $R(G)$ es el $\mathbb{Z}$-módulo libre que tiene por base los caracteres irreducibles $\chi_1, \ldots, \chi_h$ de G, tenemos, por una parte, que $D \otimes_{\mathbb{Z}} R(G)$ es el D-módulo libre generado por los elementos $1 \otimes \chi_i$. Podemos identificarlo con el D-submódulo generado por $\chi_1, \ldots, \chi_h$ en el espacio $F(G)$ de las funciones de clases de G (de modo que identificamos cada $1 \otimes \chi_i$ con χ_i). Así, $R(G)$ es el conjunto de elementos de $D \otimes_{\mathbb{Z}} R(G)$ cuyas coordenadas en la base $1 \otimes \chi_i$ (o χ_i) son enteras.

Por otra parte, $D \otimes_{\mathbb{Z}} R(G)$ es también el $R(G)$-módulo libre de base $\omega_i \otimes 1$, y los elementos de $R(G)$ son los que en esta base tienen todas las coordenadas nulas excepto la de $\omega_1 \otimes 1 = 1 \otimes 1$.

Es claro entonces que $(D \otimes_{\mathbb{Z}} V_p) \cap R(G) = V_p$. (Un elemento de la intersección es un elemento de $D \otimes_{\mathbb{Z}} R(G)$ cuyas coordenadas en la base $\omega_i \otimes 1$ están en V_p y son todas nulas menos la de $\omega_1 \otimes 1$.) Por consiguiente, para probar 11.54 basta ver que $m \in D \otimes_{\mathbb{Z}} V_p$.

El hecho de que $R(G)$ sea un subanillo de $F(G)$ y que V_p sea un ideal, implica inmediatamente que $D \otimes_{\mathbb{Z}} R(G)$ también es un subanillo de $F(G)$ y que $D \otimes_{\mathbb{Z}} V_p$ es un ideal de $D \otimes_{\mathbb{Z}} V_p$.

Teorema 11.55 *Sea G un grupo de orden g y sea $\phi : G \longrightarrow g\mathbb{Z}$ una función de clases que toma valores múltiplos de g. Entonces ϕ es combinación lineal con coeficientes en D de caracteres inducidos por caracteres de subgrupos cíclicos de G.*

DEMOSTRACIÓN: Podemos expresar $\phi = g\psi$, donde $\psi : G \longrightarrow \mathbb{Z}$ es otra función de clases. Para cada subgrupo cíclico $C \leq G$, definimos la función de clases $\theta_C : C \longrightarrow \mathbb{Z}$ mediante

$$\theta_C(x) = \begin{cases} |C| & \text{si } x \text{ genera } C, \\ 0 & \text{en otro caso.} \end{cases}$$

Si $C(G)$ es el conjunto de todos los subgrupos cíclicos de G, tenemos que

$$\sum_{C\in C(G)} \theta_C^G(x) = \sum_{y\in G} \sum_{C\in C(G)} \frac{\theta_C^0(yxy^{-1})}{|C|} = \sum_{g\in G} 1 = g.$$

Por lo tanto,

$$\phi = g\psi = \sum_{C\in C(G)} \theta_C^G\psi = \sum_{C\in C(G)} (\theta_C\psi_C)^G.$$

Falta probar que la función de clases $\eta_C = \theta_C\psi_C$ es combinación lineal con coeficientes en D de caracteres de C. Ciertamente, como toda función de clases, es combinación lineal de los caracteres irreducibles de C. Si χ es uno de ellos, su coeficiente en la combinación lineal es (η_C, χ) y, en efecto, se cumple que

$$(\eta_C, \chi) = \frac{1}{|C|} \sum_{\sigma\in C} \theta_C(\sigma)\psi(\sigma)\overline{\chi(\sigma)} = \sum_{\sigma} \psi(\sigma)\chi(\sigma^{-1}) \in D$$

donde en el último sumatorio σ recorre los generadores de C. El resultado está en D porque los caracteres de C y de G toman valores en D. (Precisamente para esto hemos introducido D en sustitución de $\mathbb{Z}$.) ∎

Puesto que todo grupo cíclico es p-elemental, el teorema anterior implica, en particular, que $\phi \in D \otimes_{\mathbb{Z}} V_p$.

Con esto podemos reducir el teorema de Brauer al resultado siguiente:

Teorema 11.56 *En las condiciones previas al teorema anterior, existe una función de clases $\psi : G \longrightarrow \mathbb{Z}$ tal que $\psi \in D \otimes_{\mathbb{Z}} V_p$ y, para todo $x \in G$, se cumple que $p \nmid \psi(x)$.*

En efecto, dada una función ψ en estas condiciones, si $g = p^i m$, llamemos N al orden del grupo de unidades de $\mathbb{Z}/p^i\mathbb{Z}$, de modo que $k^N \equiv 1 \pmod{p^i}$, para todo entero k primo con p. En particular, $\psi(x)^N \equiv 1 \pmod{p^i}$, para todo $x \in G$, luego la función de clases $m(\psi^N - 1)$ toma valores enteros múltiplos de g.

Por el teorema 11.55, tenemos que $m(\psi^N - 1) \in D \otimes_{\mathbb{Z}} V_p$. Por otra parte, $\psi \in D \otimes_{\mathbb{Z}} V_p$, y éste es un ideal de $D \otimes_{\mathbb{Z}} R(G)$, luego también $m\psi^N \in D \otimes_{\mathbb{Z}} V_p$, con lo que concluimos que $m \in D \otimes_{\mathbb{Z}} V_p$, y ya hemos visto que esto implica el teorema de Brauer. ∎

Tenemos pendiente demostrar 11.56.

Si G es un grupo finito y sea p un número primo. Diremos que $x \in G$ es un *p-elemento* si su orden es potencia de p, y es un *p'-elemento* si su orden es primo con p.

En general, si el orden de x es $m = p^i m'$, donde $p \nmid m'$, existen $u, v \in \mathbb{Z}$ tales que $up^i + vm' = 1$, con lo que $x_p = x^{vm'}$, $x_{p'} = x^{up^i}$ cumplen que

$$x = x_p x_{p'} = x_{p'} x_p, \quad x_p^{p^i} = x_{p'}^{m'} = 1,$$

es decir, que todo $x \in G$ puede descomponerse como producto de un p-elemento y un p'-elemento, a los que llamaremos, respectivamente, *p-componente* y *p'-componente* de x.

Necesitaremos este resultado técnico:

Teorema 11.57 *En las condiciones anteriores, sea $\psi : G \longrightarrow \mathbb{Z}$ una función de clases que cumpla $\psi \in D \otimes_{\mathbb{Z}} R(G)$. Si $x \in G$ y $x_{p'}$ es su p'-componente, entonces $\psi(x) \equiv \psi(x_{p'})$ (mód p)*

Demostración: Sea $C = \langle x \rangle$, de modo que $x_{p'} \in C$. Observamos que $\psi_C \in D \otimes_{\mathbb{Z}} R(C)$, luego no perdemos generalidad si suponemos que G está generado por x. Tenemos, pues, que

$$\psi = \sum_i d_i \chi_i,$$

con $d_i \in D$ y donde los caracteres irreducibles χ_i tienen todos grado 1 (porque G es abeliano), luego son homomorfismos de grupos $\chi_i : G \longrightarrow D^*$. Si $q = p^i$ es el orden de la p-componente de x, tenemos que $x^q = x_{p'}^q$, luego $\chi_i(x)^q = \chi_i(x_{p'})^q$. Por consiguiente:

$$\psi(x)^q = \left(\sum_i d_i \chi_i(x)\right)^q \equiv \sum_i d_i \chi_i(x)^q = \sum_i d_i \chi_i(x_{p'})^q$$

$$\equiv \left(\sum_i d_i \chi_i(x_{p'})\right)^q = \psi(x_{p'})^q \text{ (mód } p),$$

donde las congruencias son módulo el ideal generado por p en D. Ahora bien, como los extremos son enteros, concluimos que

$$\psi(x)^q \equiv \psi(x_{p'})^q \text{ (mód } p)$$

en $\mathbb{Z}$ y, como q es potencia de p, esto equivale a que $\psi(x) \equiv \psi(x_{p'})$ (mód p). ∎

Con esto estamos en condiciones de construir una función ψ en las condiciones del teorema 11.56. Para ello partimos de un sistema de representantes $\{x_i\}_i$ de las clases de conjugación de G formadas por p'-elementos. Sea $C_G(x_i)$ el centralizador en G de x_i, es decir, el subgrupo formado por los elementos que conmutan con x_i, sea P_i un p-subgrupo de Sylow[6] de $C_G(x_i)$, es decir, un p-subgrupo cuyo orden sea la mayor potencia de p que divide al orden de $C_G(x_i)$ y sea $C_i = \langle x_i \rangle$.

[6]Véase el apéndice del Capítulo V de mi libro de Geometría

Como los elementos de C_i conmutan con los de P_i, tenemos que $H_i = C_iP_i$ es un subgrupo de G y, como $C_i \cap P_i = 1$ (porque el orden de C_i es primo con el orden de P_i), concluimos que el producto $H_i = C_i \times P_i$ es directo, luego H_i es un subgrupo p-elemental de G.

Sea $\phi_i : C_i \longrightarrow \mathbb{Z}$ la función de clases dada por

$$\phi_i(x) = \begin{cases} |C_i| & \text{si } x = x_i, \\ 0 & \text{si } x \neq x_i. \end{cases}$$

Se cumple que $\phi_i \in R(C_i)$, pues, al expresar ϕ_i como combinación lineal de los caracteres de C_i, el coeficiente de cada carácter χ es

$$(\phi_i, \chi) = \overline{\chi(x_i)} = \chi(x_i^{-1}) \in D.$$

Definimos ahora $\psi_i : H_i \longrightarrow \mathbb{Z}$ mediante $\psi_i(x, y) = \phi_i(x)$, donde $x \in C_i$, $y \in P_i$. Viendo a C_i como cociente de H_i, tenemos que las funciones de clase de C_i determinan funciones de clase de H_i, y ψ_i es precisamente la función determinada por ϕ_i. Es claro entonces que $\psi_i \in D \otimes_{\mathbb{Z}} R(H_i)$ (porque ψ_i es combinación lineal con coeficientes en D de los caracteres de H_i determinados por los caracteres de C_i). Por consiguiente, $\psi_i^G \in D \otimes_{\mathbb{Z}} V_p$.

Por la propia definición de la función inducida por una función de clases es inmediato que ψ_i^G toma valores enteros. Vamos a probar que

$$\psi_i^G(x_i) \not\equiv 0 \ (\text{mód } p), \qquad \psi_i^G(x_j) = 0 \quad \text{para } j \neq i.$$

En efecto, si $y \in G$ cumple que $yx_jy^{-1} \in H_i$, entonces, como se trata de un p'-elemento, ha de ser $yx_jy^{-1} \in C_i$ y, para $j \neq i$, ha de ser $yx_jy^{-1} \neq x_i$, luego $\psi_i(yx_jy^{-1}) = \phi_i(yx_jy^{-1}) = 0$, y esto implica que $\phi_i^G(x_j) = 0$.

Por el contrario, el conjunto de los $y \in G$ tales que $yx_iy^{-1} = x_i$ es precisamente el centralizador $C_G(x_i)$, luego

$$\psi_i^G(x_i) = \frac{1}{|H_i|} \sum_{y \in G} \psi_i^0(y^{-1}x_iy) = \frac{|C_G(x_i)||C_i|}{|C_i||P_i|} = \frac{|C_G(x_i)|}{|P_i|},$$

que no es divisible entre p porque P_i es un p-subgrupo de Sylow del centralizador.

Ahora es fácil ver que la función

$$\psi = \sum_i \psi_i^G$$

cumple el teorema 11.56, pues, ciertamente $\psi \in D \otimes_{\mathbb{Z}} V_p$, toma valores enteros y, para todo $x \in G$, el teorema 11.57 nos da que $\psi(x) \equiv \psi(x_{p'})$ (mód p) y, a su vez, la p'-componente $x_{p'}$ está en la clase de conjugación de un x_i, luego

$$\psi(x) \equiv \psi(x_{p'}) = \psi(x_i) = \psi_i^G(x_i) \not\equiv 0 \ (\text{mód } p).$$

Esto prueba 11.56 y, por consiguiente, termina la demostración del teorema de Brauer. ∎

11.6 Caracteres en grupos cociente

Ya hemos visto que cada carácter de un grupo cociente G/N (y, más en general, cada función de clases) induce un carácter (o una función de clases) en G mediante $\phi_G(\sigma) = \phi(\sigma N)$. Ahora vamos a definir una correspondencia en sentido inverso análoga a la definición de los caracteres inducidos.

Para ello observamos que la representación $\rho : G \longrightarrow \mathbb{C}[G/N]$ dada por $\rho(\sigma)(N\tau) = N\tau\sigma$ determina en $\mathbb{C}[G/N]$ una estructura natural de $\mathbb{C}[G]$-módulo que nos permite dar la definición siguiente:

Definición 11.58 Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación lineal de un grupo finito G y sea N un subgrupo normal. Definimos la representación $\rho^{G/N}$ del grupo cociente G/N como la asociada al $\mathbb{C}[G/N]$-módulo $V \otimes_{\mathbb{C}[G]} \mathbb{C}[G/N]$. Si χ es el carácter de ρ, llamaremos $\chi^{G/N}$ al carácter de $\rho^{G/N}$.

Vamos a ver cómo calcular $\chi^{G/N}$ a partir de χ sin necesidad de considerar las representaciones correspondientes.

Llamemos V^N al subespacio de V fijado por los elementos de N. El hecho de que N sea un subgrupo normal implica que V^N es un $\mathbb{C}[G]$-submódulo de V, y la representación $G \longrightarrow \mathrm{Aut}(V^N)$ tiene a N en su núcleo, luego induce una representación de G/N o, lo que es lo mismo, podemos considerar a V^N como $\mathbb{C}[G/N]$-módulo de forma natural.

Consideremos a aplicación lineal $p : V \longrightarrow V^N$ dada por

$$p(v) = \frac{1}{|N|}\sum_{n\in N} vn.$$

Es inmediato comprobar que es un homomorfismo de $\mathbb{C}[G]$-módulos, que su imagen es ciertamente V^N y que se restringe a la identidad en V^N, luego, llamando W al núcleo de p, tenemos que $V = V \oplus W$, donde W es también un $\mathbb{C}[G]$-módulo.

La proyección p induce una aplicación lineal $f : V \otimes_{\mathbb{C}[G]} \mathbb{C}[G/N] \longrightarrow V^N$ dada por $f(v \otimes N\sigma) = p(v)\sigma$, que es claramente un homomorfismo de $\mathbb{C}[G/N]$-módulos y es, de hecho, un isomorfismo, pues admite como inversa a la aplicación g dada por $g(v) = v \otimes N1$.

Así pues, $\chi^{G/N}$ es también el carácter de la representación de G/N inducida por la restricción de ρ a V^N. Vamos a usar esta representación para calcular explícitamente $\chi^{G/N}$. Para cada $\sigma \in G$, definimos

$$x_\sigma = \frac{1}{|N|}\sum_{n\in N} n\sigma \in \mathbb{C}[G].$$

Es claro entonces que, si $v \in V$, se cumple que $vx_\sigma = p(v)\sigma$. Por consiguiente, $vx_\sigma = v\sigma$ para todo $v \in V^N$, mientras que $vx_\sigma = 0$ si $v \in W$. Esto significa que, fijando una base de V que sea unión de una base de V^N y otra de

W, vemos que la multiplicación por x_σ es un endomorfismo de V que tiene la misma traza que la restricción de $\rho(\sigma)$ a V^N. Equivalentemente:

$$\chi^{G/N}(N\sigma) = \mathrm{Tr}(x_\sigma) = \frac{1}{|N|}\sum_{n\in N}\chi(n\sigma).$$

Para enunciar la conclusión a la que hemos llegado conviene dar primero la definición siguiente:

Definición 11.59 Sea G un grupo finito y N un subgrupo normal. Para cada función de clases $\phi : G \longrightarrow \mathbb{C}$, definimos la función de clases $\phi^{G/N} : G/N \longrightarrow \mathbb{C}$ mediante

$$\phi^{G/N}(N\sigma) = \frac{1}{|N|}\sum_{n\in N}\phi(n\sigma).$$

En estos términos hemos probado lo siguiente:

Teorema 11.60 *Si χ es un carácter de un grupo finito G y N es un subgrupo normal, entonces el carácter $\chi^{G/N}$ de G/N definido en* 11.58 *coincide con la función de clases de la definición anterior.*

O, dicho de otro modo, si χ es un carácter, $\chi^{G/N}$ también lo es.

A continuación probamos una fórmula análoga a la reciprocidad de Frobenius para caracteres inducidos:

Teorema 11.61 *Sea G un grupo finito, sea N un subgrupo normal, y sean $\phi : G \longrightarrow \mathbb{C}$, $\psi : G/N \longrightarrow \mathbb{C}$ funciones de clases. Entonces*

$$(\phi, \psi_G) = (\phi^{G/N}, \psi).$$

Demostración: Notemos que, por claridad, hemos representado por ψ_G la función ψ vista como función de G (que usualmente representamos también por ψ). Se trata de una comprobación rutinaria:

$$(\phi^{G/N}, \psi) = \frac{1}{|G:N|}\sum_{N\sigma\in G/N}\phi^{G/N}(N\sigma)\overline{\psi(N\sigma)}$$

$$= \frac{1}{|G|}\sum_{N\sigma\in G/N}\sum_{n\in N}\phi(n\sigma)\overline{\psi_G(n\sigma)} = \frac{1}{|G|}\sum_{\sigma\in G}\phi(\sigma)\overline{\psi_G(\sigma)} = (\phi, \psi_G).$$

■

11.7 Complementos

En esta sección demostraremos algunos resultados adicionales sobre caracteres de grupos que no nos serán necesarios después.

Caracteres de productos directos Vamos a determinar los caracteres de un producto directo de grupos $G = G_1 \times G_2$. Observemos que, como $G_1 \cong G/G_2$, podemos considerar a cada carácter χ de G_1 como un carácter de G. Concretamente, entendiendo que $\chi(g_1g_2) = \chi(g_1)$. Lo mismo es válido para los caracteres de G_2.

Teorema 11.62 *Sea $G = G_1 \times G_2$ un producto directo de grupos. Si χ_i es un carácter irreducible de G_i, entonces $\chi_1\chi_2$ es un carácter irreducible de G, y todo carácter irreducible de G es de esta forma.*

DEMOSTRACIÓN: Sabemos que $\chi_1\chi_2$ es un carácter de G, aunque, en general, el producto de caracteres irreducibles no tiene por qué ser irreducible. No obstante, multiplicando las ecuaciones

$$(\chi_1,\chi_1) = \frac{1}{|G_1|}\sum_{g_1\in G_1}|\chi_1(g_1)|^2 = 1, \quad (\chi_2,\chi_2) = \frac{1}{|G_2|}\sum_{g_2\in G_2}|\chi_2(g_2)|^2 = 1,$$

obtenemos que $(\chi_1\chi_2, \chi_1\chi_2) = 1$, luego $\chi_1\chi_2$ es irreducible.

Si $\chi_1^i, \ldots, \chi_{h_i}^i$ son los caracteres irreducibles de G_i, es claro que los caracteres $\chi_k^1\chi_l^2$ son distintos dos a dos, pues el producto determina los factores por restricción. Sabemos que

$$\sum_k \chi_k^1(1)^2 = |G_1|, \quad \sum_l \chi_l^2(1)^2 = |G_2|,$$

y multiplicando ambas ecuaciones obtenemos que

$$\sum_{k,l}(\chi_k^1\chi_l^2)(1)^2 = |G|,$$

luego G no puede tener más caracteres irreducibles. ∎

En particular, descomponiendo un grupo abeliano como producto de grupos cíclicos, podemos determinar fácilmente todos sus caracteres irreducibles. Sólo tenemos que observar que los caracteres irreducibles de un grupo cíclico $G = \langle\sigma\rangle$ de orden n son los homomorfismos $\chi : G \longrightarrow \mathbb{C}^*$ determinados por que $\chi(\sigma)$ es una raíz n-sima de la unidad. Hay n raíces posibles que dan lugar a los n caracteres irreducibles de G.

El grado de un carácter irreducible Hemos probado que el grado de un carácter irreducible de un grupo finito G debe dividir al orden de G. Este resultado puede mejorarse.

Teorema 11.63 *Si G es un grupo finito, el grado de cualquier carácter irreducible de G divide al índice $|G : Z(G)|$.*

DEMOSTRACIÓN: Sea $g = |G|$ y $c = |Z(G)|$. Consideremos una representación irreducible $\rho : G \longrightarrow \mathrm{Aut}(V)$ de grado n. Si $\sigma \in Z(G) \subset Z(\mathbb{C}[G])$, el

teorema 11.31 nos dice que $\rho(\sigma)$ es una homotecia en V de razón $\lambda(\sigma)$, de modo que $\lambda : Z(G) \longrightarrow \mathbb{C}^*$ es un homomorfismo de grupos.

Fijemos ahora un número natural $m \geq 1$ y consideremos el grupo G^m (el producto directo de G por sí mismo m veces). Si χ es el carácter de ρ, podemos considerar en G^m el carácter χ^m, que, según hemos visto en la sección anterior, es irreducible, y está asociado a la representación

$$\rho^m : G^m \longrightarrow V \otimes_{\mathbb{C}[G]} \cdots \otimes_{\mathbb{C}[G]} V$$

dada por[7] $\rho^m(\sigma_1, \ldots, \sigma_m)(v_1 \otimes \cdots \otimes v_m) = v_1\sigma_1 \otimes \cdots \otimes v_m\sigma_m$. Por consiguiente, si $(\sigma_1, \ldots, \sigma_m) \in \mathbb{Z}(G)^m$, tenemos que $\rho^m(\sigma_1, \ldots, \sigma_m)$ es la homotecia de razón $\lambda(\sigma_1 \cdots \sigma_m)$.

Consideremos el subgrupo H de $Z(G)^m$ formado por los elementos que cumplen $\sigma_1 \cdots \sigma_m = 1$. Tenemos que H está en el núcleo de ρ^m, luego podemos ver a ρ^m como representación de G^m/H. El teorema 11.34 implica que el grado de ρ^m, que es n^m, divide el orden de este cociente, que es g^m/c^{m-1}. Así pues, existe un $k \in \mathbb{Z}$ tal que $kn^m = g^m/c^{m-1}$ o, lo que es lo mismo, $(g/cn)^m \in c^{-1}\mathbb{Z}$, para todo $m \in \mathbb{Z}$.

Esto implica que $\mathbb{Z}[g/cn] \subset c^{-1}\mathbb{Z}$, luego la $\mathbb{Z}$-álgebra $\mathbb{Z}[g/cn]$ es un $\mathbb{Z}$-módulo finitamente generado, luego g/cn es un entero algebraico y un número racional, luego $g/cn \in \mathbb{Z}$, luego $n \mid g/c = |G : Z(G)|$. ∎

El teorema 11.44 nos permite refinar más la cota:

Teorema 11.64 *Si G es un grupo finito y N es un subgrupo normal abeliano, entonces el grado de todo carácter irreducible de G divide al índice $|G : N|$.*

Demostración: Razonando por inducción, podemos suponer que el teorema es cierto para todo grupo de orden menor que $|G|$. Sea χ un carácter irreducible de G y supongamos que χ_N se descompone en suma de al menos dos caracteres irreducibles distintos. Entonces, por 11.44, existe un subgrupo $N \leq H < G$ tal que $\chi = \psi^G$, para cierto carácter ψ de H. Por hipótesis de inducción $\psi(1) \mid |H : N|$, luego

$$\chi(1) = \psi^G(1) = |G : H|\,\psi(1) \mid |G : N|.$$

Supongamos ahora que $\chi_N = n\psi$, para cierto carácter irreducible ψ de N, que será de grado 1, porque N es abeliano. Sea $\rho : G \longrightarrow \mathrm{LG}(n, \mathbb{C})$ una representación matricial que genere a χ, consideremos $G' = \rho[G] \leq \mathrm{LG}(n, \mathbb{C})$ y sea $N' = \rho[N]$. Tenemos un epimorfismo $G/N \longrightarrow G'/N'$, luego

$$|G' : N'| \,\Big|\, |G : N|.$$

El hecho de que $\chi_N = n\psi$ se traduce en que las matrices de N' son de la forma ϵI_n, luego $N' \leq Z(G')$. La inclusión $G' \longrightarrow \mathrm{LG}(n, \mathbb{C})$ es una representación de G' de grado n, luego el teorema anterior nos da que $n \mid |G' : N'| \,\Big|\, |G : N|$. ∎

[7] Con más detalle, al considerar a χ como carácter del i-ésimo factor, su representación asociada es la dada por $G^m \xrightarrow{p_i} G \xrightarrow{\rho} \mathrm{Aut}(V)$, y el producto tensorial de estas representaciones de G^m es el indicado.

Subgrupos normales El teorema 11.20 nos permite reconocer el núcleo de un carácter a partir de la tabla de caracteres de un grupo. Obviamente, los núcleos de caracteres son subgrupos normales. Los demás subgrupos normales de un grupo dado pueden calcularse a partir de la tabla de caracteres sin más que tener en cuenta que son intersecciones de núcleos:

Teorema 11.65 *Todo subgrupo normal de un grupo finito es la intersección de los núcleos de los caracteres irreducibles que lo contienen.*

DEMOSTRACIÓN: Es trivial: sea G un grupo y N un subgrupo normal. Los caracteres irreducibles que contienen a N en su núcleo son los caracteres irreducibles de G/N, luego todo se reduce a probar que la intersección de los núcleos de todos los caracteres irreducibles de un grupo dado es trivial, pero ello se debe a que dicha intersección es el núcleo de la representación regular, que es fiel. ∎

Recordemos que el subgrupo derivado de un grupo G es el menor subgrupo G' tal que el cociente G/G' es abeliano.

Teorema 11.66 *El subgrupo derivado de un grupo finito es la intersección de los núcleos de los caracteres irreducibles de grado* 1*.*

DEMOSTRACIÓN: Si un carácter irreducible $\chi : G \longrightarrow \mathbb{C}$ cumple $G' \leq \mathrm{N}(\chi)$, entonces χ es un carácter irreducible de G/G' y, como el cociente es abeliano, χ tiene grado 1. Recíprocamente, si χ tiene grado 1, entonces es un homomorfismo $\chi : G \longrightarrow \mathbb{C}^*$, luego $G/\mathrm{N}(\chi)$ es abeliano y, por consiguiente, $G' \leq \mathrm{N}(\chi)$. ∎

En particular, el número de caracteres de grado 1 de un grupo finito G es igual al índice $|G : G'|$.

También podemos calcular el centro de un grupo a partir de su tabla de caracteres. Para ello definimos el *centro* de un carácter $\chi : G \longrightarrow \mathbb{C}$ como el conjunto

$$Z(\chi) = \{\sigma \in G \mid |\chi(\sigma)| = \chi(1)\}.$$

Teorema 11.67 *Sea G un grupo finito.*

a) Si χ es un carácter de G asociado a una representación $\rho : G \longrightarrow \mathrm{Aut}(V)$, entonces

$$Z(\chi) = \{\sigma \in G \mid \rho(\sigma) \text{ es una homotecia }\}.$$

b) $Z(\chi)$ es un subgrupo de G y $Z(\chi)/\mathrm{N}(\chi)$ es cíclico.

c) $Z(G)$ es la intersección de los centros de todos los caracteres irreducibles de G.

d) Si χ es un carácter irreducible y fiel de G, entonces $Z(G) = Z(\chi)$.

DEMOSTRACIÓN: a) Dado $\sigma \in G$, sabemos que, eligiendo una base en V, podemos suponer que la matriz asociada al automorfismo $\rho(\sigma)$ es diagonal y $\chi(\sigma) = \epsilon_1 + \cdots + \epsilon_n$ es la suma de dicha diagonal. Además, todos los ϵ_i tienen módulo 1.

Tenemos que $\sigma \in Z(\chi)$ si y sólo si $|\epsilon_1 + \cdots + \epsilon_n| = n$, y es fácil ver que esto ocurre sí y sólo si todos los ϵ_i son iguales, es decir, si y sólo si $\rho(\sigma)$ es una homotecia de razón ϵ.

b) Ahora es inmediato que $Z(\chi)$ es un subgrupo de G. Más aún, si llamamos $\lambda(\sigma)$ a la razón de la homotecia $\rho(\sigma)$, tenemos que $\lambda : Z(\chi) \longrightarrow \mathbb{C}^*$ es un homomorfismo de grupos cuyo núcleo es $\mathrm{N}(\chi)$, $Z(\chi)/\mathrm{N}(\chi)$ es isomorfo a un subgrupo finito de $\mathbb{C}^*$, luego ha de ser cíclico.

c) Si χ es irreducible, el teorema 11.31 implica que $Z(G) \leq Z(\chi)$. Por otra parte, como $\rho[Z(\chi)]$ está formado por homotecias, $\rho[Z(\chi)] \leq Z(\rho[G])$. Teniendo en cuenta el isomorfismo natural $\rho[G] \cong G/\mathrm{N}(\chi)$, vemos que

$$Z(\chi)/\mathrm{N}(\chi) \leq Z(G/\mathrm{N}(\chi)).$$

Si σ pertenece a los centros de todos los caracteres irreducibles de G y $\tau \in G$, se cumple que $\sigma\tau\sigma^{-1}\tau^{-1} \in \mathrm{N}(\chi)$, y esto vale para todo carácter irreducible χ, luego $\sigma\tau\sigma^{-1}\tau^{-1} = 1$, lo que implica que $\sigma \in Z(G)$.

d) Si χ es un carácter irreducible y fiel de G, en c) hemos probado que $Z(\chi) \leq Z(G)$, y también la inclusión opuesta, luego $Z(G) = Z(\chi)$. ∎

En particular, vemos que una condición necesaria para que un grupo G pueda tener un carácter irreducible y fiel es que $Z(G)$ sea cíclico. Hay ejemplos que muestran que no es suficiente.

Capítulo XII

Curvas de Tate

En este capítulo presentaremos una técnica para estudiar las curvas elípticas con reducción multiplicativa sobre un cuerpo métrico discreto y completo. Se trata de una representación analítica debida a Tate, análoga a la teoría clásica para curvas elípticas complejas desarrollada en el capítulo X de [CE].

Recordemos, que si $R \subset \mathbb{C}$ es un *retículo complejo* (es decir, el $\mathbb{Z}$-módulo generado por dos números complejos linealmente independientes sobre $\mathbb{R}$), el cociente $T = \mathbb{C}/R$ admite una estructura natural de superficie de Riemann. Cada retículo R tiene asociada su *función $\wp$ de Weierstrass,* dada por

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in R\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right),$$

que es una función meromorfa en $\mathbb{C}$ con polos en los puntos de R, los cuales son, además, periodos de $\wp$, por lo que ésta induce una función meromorfa $\wp : T \longrightarrow \mathbb{C}^\infty$ con un único polo en 0. Por otra parte, para $n \geq 2$, definimos

$$G_n = \sum_{\omega \in R\setminus\{0\}} \frac{1}{\omega^n}.$$

(La serie converge para $n \geq 2$, y es nula cuando n es impar.) En estos términos ([CE 10.14]), la función $\wp$ satisface la ecuación diferencial

$$\wp'^2 = 4\wp^3 - 60G_4\wp - 140G_6.$$

De aquí se sigue ([CE 10.17]) que si llamamos $E_R/\mathbb{C}$ a la curva elíptica definida por la ecuación $Y^2 = 4X^3 - g_2X - g_3$ (donde $g_2 = 60G_4$ y $g_3 = 140G_6$), la aplicación $\phi : T \longrightarrow E_R(\mathbb{C})$ dada por

$$\phi(P) = \begin{cases} (\wp(P), \wp'(P)) & \text{si } P \neq 0, \\ O & \text{si } P = 0, \end{cases}$$

(donde O es el punto infinito de E_R) es un isomorfismo de grupos (y una transformación conforme si consideramos en $E_R(\mathbb{C})$ la estructura natural de superficie de Riemann).

Por último, sucede que toda curva elíptica $E/\mathbb{C}$ es isomorfa a una curva $E_R/\mathbb{C}$ para un cierto retículo R.

En este capítulo obtendremos resultados análogos cambiando $\mathbb{C}$ por un cuerpo métrico discreto y completo K. Nos interesará especialmente el caso en que K es un *cuerpo local*, es decir, una extensión finita del cuerpo $\mathbb{Q}_p$ de los números p-ádicos, para un primo p. Dedicamos la primera sección a recordar aspectos más concretos del caso complejo y reformularlos ligeramente para que puedan ser traducidos al caso local.

12.1 Curvas elípticas complejas

A la hora de obtener resultados análogos para $\mathbb{Q}_p$ de los hechos que acabamos de recordar, el primer obstáculo con el que nos encontramos es que $\mathbb{Q}_p$ no posee subgrupos discretos no triviales. En efecto, si $R \subset \mathbb{Q}_p$ es un subgrupo y $x \in R$ es no nulo, entonces $p^n x \in R$ y

$$\lim_n p^n x = 0,$$

luego 0 es un punto de acumulación de R. Esto impide, por ejemplo, dotar a $\mathbb{Q}_p/R$ de una estructura topológica razonable. Para resolver este problema vamos a ver que, en el caso complejo, podemos hacer las cosas de una forma ligeramente distinta.

En primer lugar, recordamos que toda curva elíptica puede ser parametrizada a partir de un retículo de la forma $R_\tau = \mathbb{Z} + \tau\mathbb{Z}$, donde τ pertenece al semiplano

$$H = \{\tau \in \mathbb{C} \mid \operatorname{Im}\tau > 0\}.$$

Ello se debe a que, si $E_\tau/\mathbb{C}$ es la curva elíptica asociada a R_τ y llamamos $j(\tau)$ a su invariante, la función $j : H \longrightarrow \mathbb{C}$ (la función modular de Klein) es suprayectiva ([CE 12.3]).

La aplicación $u = e^{2\pi i z}$ induce un isomorfismo de grupos $\mathbb{C}/\mathbb{Z} \cong \mathbb{C}^*$ que hace corresponder τ con $q = e^{2\pi i\tau}$. Por consiguiente, este isomorfismo induce a su vez un isomorfismo $\mathbb{C}/R_\tau \cong \mathbb{C}^*/q^{\mathbb{Z}}$, donde, obviamente, estamos llamando

$$q^{\mathbb{Z}} = \{q^n \mid n \in \mathbb{Z}\},$$

que es un subgrupo discreto de $\mathbb{C}^*$. Notemos que la condición $\operatorname{Im}\tau > 0$ equivale a $|q| < 1$. Así pues, resulta que toda curva elíptica compleja puede parametrizarse desde $\mathbb{C}^*$ módulo el subgrupo discreto $q^{\mathbb{Z}}$, y sucede que todo $q \in \mathbb{Q}_p^*$ con $|q| < 1$ determina también un subgrupo discreto $q^{\mathbb{Z}} \subset \mathbb{Q}_p^*$, por lo que será expresando en estos términos los resultados del caso complejo como podremos traducirlos al caso local. De ello nos ocuparemos en la sección siguiente. Aquí vamos a describir las parametrizaciones en términos de $\mathbb{C}^*/q^{\mathbb{Z}}$.

Para cada $\tau \in H$, llamamos $\wp(z;\tau)$, a la función de Weierstrass asociada al retículo R_τ, e, igualmente, llamamos $G_n(\tau)$ a la constante correspondiente

(que ahora pasa a ser una función de τ). El resultado fundamental es que las funciones $G_n(\tau)$ resultan ser holomorfas. El teorema [CE 10.30] nos da su desarrollo en serie de Fourier, que, en términos de $q = e^{2\pi i\tau}$, resulta ser un desarrollo en serie de potencias:

$$G_{2k}(\tau) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n,$$

donde ζ es la función dseta de Riemann y σ_k es la función aritmética

$$\sigma_k(n) = \sum_{d|n} d^k.$$

En la prueba del teorema [CE 10.30] está implícita la convergencia en el disco unitario $|q| < 1$ de la serie de potencias

$$s_k(q) = \sum_{n=1}^{\infty}\sigma_k(n)q^n$$

cuando k es impar, pero, como $\sigma_k(n) < \sigma_{k+1}(n)$, todas las series s_k son convergentes. Observemos que

$$s_k(q) = \sum_{n=1}^{\infty}\sum_{d|n} d^k q^n = \sum_{d=1}^{\infty} d^k \sum_{m=1}^{\infty} q^{md} = \sum_{d=1}^{\infty}\frac{d^k q^d}{1-q^d} = \sum_{n=1}^{\infty}\frac{n^k q^n}{1-q^n}.$$

Para que la reagrupación de los sumandos sea válida, hay que probar que la serie definida por $d^k q^n$ es absolutamente convergente, es decir, que converge (con una cierta ordenación) cuando q es un número real $0 < q < 1$. Ahora bien, teniendo en cuenta que

$$\lim_n \sigma_k(n)q^n = 0,$$

es fácil probar que la serie converge a $s_k(q)$ cuando se ordenan sus términos empezando por todos los que tienen $n = 1$, seguidos de los que tienen $n = 2$, etc. (Dado $\epsilon > 0$, tomamos n suficientemente grande como para que las sumas parciales de $s_k(q)$ disten de la suma total menos de $\epsilon/2$ y además $\sigma_k(n)q^n < \epsilon/2$.)

En particular, evaluando la función dseta, obtenemos que

$$g_2(\tau) = 60G_4(\tau) = \frac{(2\pi i)^4}{12}(1 + 240s_3(q)),$$

$$g_3(\tau) = 140G_6(\tau) = \frac{(2\pi i)^6}{216}(-1 + 504s_5(q)).$$

Por otra parte, antes del teorema [CE 10.33] obtuvimos la expresión

$$\frac{1}{(2\pi i)^2}\wp(z;\tau) = \frac{1}{12} + \frac{u}{(1-u)^2} + \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} nq^{nm}(u^n + u^{-n} - 2),$$

donde aquí hemos llamado $u = e^{2\pi iz}$. La expresión es válida si $0 < \operatorname{Im} z < \operatorname{Im}\tau$, lo cual equivale a $0 < |q| < |u| < 1$. Observemos ahora que, para $|x| < 1$, tenemos que

$$\frac{x}{(1-x)^2} = x\,\frac{d}{dx}\left(\frac{1}{1-x}\right) = \sum_{n=1}^{\infty} nx^n.$$

Aplicando dos veces esta identidad resulta que

$$\frac{1}{(2\pi i)^2}\wp(z;\tau) = \frac{1}{12} + \sum_{m=0}^{\infty}\frac{q^m u}{(1-q^m u)^2} + \sum_{m=1}^{\infty}\frac{q^m u^{-1}}{(1-q^m u^{-1})^2} - 2\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n}.$$

De aquí llegamos a su vez a la identidad

$$\frac{1}{(2\pi i)^2}\wp(z;\tau) = \frac{1}{12} + \sum_{n\in\mathbb{Z}}\frac{q^n u}{(1-q^n u)^2} - 2s_1(q).$$

En principio, hemos probado esto para $|q| < |u| < 1$. Ahora demostramos que la identidad es cierta en todo $\mathbb{C}^* \setminus q^{\mathbb{Z}}$:

Teorema 12.1 *Sea $\tau \in \mathbb{C}$ tal que $\operatorname{Im}\tau > 0$, sea $R = \mathbb{Z} + \tau\mathbb{Z}$ y $q = e^{2\pi i\tau}$. Entonces, la serie*

$$F(u) = \sum_{n\in\mathbb{Z}}\frac{q^n u}{(1-q^n u)^2}$$

converge absoluta y uniformemente en los compactos de $\mathbb{C}^* \setminus q^{\mathbb{Z}}$ a una función meromorfa en $\mathbb{C}^*$ tal que, para todo $z \in \mathbb{C} \setminus R$ y llamando $u = e^{2\pi iz}$, se cumple

$$\frac{1}{(2\pi i)^2}\wp(z;\tau) = \frac{1}{12} + \sum_{n\in\mathbb{Z}}\frac{q^n u}{(1-q^n u)^2} - 2s_1(q).$$

Demostración: Basta probar la convergencia, pues ya hemos probado que la identidad es válida en un abierto de $\mathbb{C} \setminus R$, luego lo será en todo $\mathbb{C} \setminus R$ por el principio de prolongación analítica. Notemos que los denominadores sólo se anulan en puntos de $q^{\mathbb{Z}}$, luego todos los sumandos son funciones holomorfas en $\mathbb{C}^* \setminus q^{\mathbb{Z}}$. Si probamos que la convergencia es uniforme en compactos, la suma será también holomorfa. Para cada $n > 0$, tenemos que

$$\left|\frac{q^{-n}u}{(1-q^{-n}u)^2}\right| + \left|\frac{q^n u}{(1-q^n u)^2}\right| = \frac{|u||q|^n}{|q^n-u|^2} + \frac{|u||q|^n}{|1-q^n u|^2}.$$

Puesto que $|q| < 1$, es claro que existen $c > 0$ y $n_0 \in \mathbb{N}$ independientes de q y tales que el miembro derecho está acotado por $c\,|q|^n$ para todo $u \in C$ y todo $n \geq n_0$. El criterio de mayoración de Weierstrass implica que la serie converge absoluta y uniformemente en C. ∎

Derivando respecto de z en la identidad del teorema anterior (y teniendo en cuenta que $u' = 2\pi iu$), concluimos que

$$\frac{1}{(2\pi i)^3}\wp'(z;\tau) = \sum_{n\in\mathbb{Z}}\frac{q^n u(1+q^n u)}{(1-q^n u)^3}.$$

Notemos que la serie del miembro derecho (como función de u) es u por la derivada de la serie del teorema anterior, luego también define una función meromorfa en $\mathbb{C}^*$ con polos (a lo sumo) en $q^{\mathbb{Z}}$.

Las funciones $\wp$ y $\wp'$ satisfacen la ecuación de E_τ:

$$Y^2 = 4X^3 - g_2X - g_3.$$

Se trata de una ecuación de Weierstrass clásica, pero no lo que nosotros hemos definido como ecuación de Weierstrass. Vamos a transformarla en una ecuación de Weierstrass mediante un cambio de variables que, además, elimine los factores $2\pi i$ de las fórmulas que hemos encontrado para $\wp$, $\wp'$, g_2 y g_3, así como los denominadores 12 y 216 que nos han aparecido. El cambio oportuno es:

$$\frac{1}{(2\pi i)^2}X = X' + \frac{1}{12},$$

$$\frac{1}{(2\pi i)^3}Y = 2Y' + X'.$$

Es fácil ver que este cambio transforma la ecuación en

$$Y^2 + XY = X^3 + a_4X + a_6,$$

donde

$$a_4(\tau) = -\frac{1}{4}\,\frac{1}{(2\pi i)^4}g_2(\tau) + \frac{1}{48} = -5s_3(q),$$

$$a_6(\tau) = -\frac{1}{4}\,\frac{1}{(2\pi i)^6}g_3(\tau) - \frac{1}{48}\,\frac{1}{(2\pi i)^4}g_2(\tau) + \frac{1}{1728} = -\frac{5s_3(q) + 7s_5(q)}{12}.$$

Llamaremos $E_q/\mathbb{C}$ a la curva elíptica definida por la ecuación de Weierstrass anterior. El cambio de variables induce un isomorfismo $E_\tau \cong E_q$.

Por otra parte, aplicando el cambio de variables a las funciones $\wp$ y $\wp'$ concluimos que la ecuación de E_q es satisfecha por las funciones

$$X(u,q) = \frac{1}{(2\pi i)^2}\wp(u,q) - \frac{1}{12} = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q),$$

$$Y(u,q) = \frac{1}{2}\left(\frac{1}{(2\pi i)^3}\wp'(u,q) - X(u,q)\right) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + s_1(q).$$

Con esto tenemos casi probado el teorema siguiente:

Teorema 12.2 *Sea $q \in \mathbb{C}^*$ tal que $|q| < 1$. Las series*

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q), \quad Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + s_1(q)$$

definen funciones (de u) meromorfas en $\mathbb{C}^*$ con polos en los puntos de $q^{\mathbb{Z}}$, y satisfacen la ecuación de Weierstrass

$$Y^2 + XY = X^3 + a_4X + a_6,$$

donde

$$a_4(q) = -5s_3(q), \qquad a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12}.$$

Además, las funciones X e Y inducen funciones meromorfas en el toro complejo $\mathbb{C}^*/q^{\mathbb{Z}}$ con un único polo en $u = 1$ y, si $E_q/\mathbb{C}$ es la curva elíptica definida por la ecuación de Weierstrass, la aplicación $\phi : \mathbb{C}^*/q^{\mathbb{Z}} \longrightarrow E_q(\mathbb{C})$ dada por

$$\phi(u) = \begin{cases} (X(u,q), Y(u,q)) & \text{si } u \neq 1, \\ O & \text{si } u = 1, \end{cases}$$

(donde O es el punto infinito de E_q) es un isomorfismo de grupos (y una transformación conforme si consideramos en $E_q(\mathbb{C})$ la estructura natural de superficie de Riemann).

Demostración: Se trata de una mera reformulación del teorema [CE 10.17] que hemos citado al principio del capítulo. Podemos tomar un $\tau \in \mathbb{C}$ tal que $\operatorname{Im}\tau > 0$ y $q = e^{2\pi i\tau}$. Sea $R = \mathbb{Z} + \tau\mathbb{Z}$.

La proyección canónica $\mathbb{C}^* \longrightarrow \mathbb{C}^*/q^{\mathbb{Z}}$ es localmente inyectiva, por lo que induce una estructura de superficie de Riemann en $\mathbb{C}^*/q^{\mathbb{Z}}$. Podemos considerar a $\mathbb{C}^*/q^{\mathbb{Z}}$ como un toro complejo, pues el isomorfismo $\mathbb{C}/R \cong \mathbb{C}^*/q^{\mathbb{Z}}$ dado por $z \mapsto e^{2\pi iz}$ es una transformación conforme. Lo que hemos probado es que, a través de esta transformación, las funciones de Weierstrass $\wp(z;\tau)$ y $\wp'(z;\tau)$ se corresponden con funciones meromorfas de $\mathbb{C}^*/q^{\mathbb{Z}}$ que, tras un cambio de variables lineal, se convierten en X e Y. Así, las aplicaciones inducidas por $\wp$, $\wp'$ y X, Y, junto con el isomorfismo $E_\tau \cong E_q$ dado por el cambio de variables, dan lugar a un diagrama conmutativo

$$\begin{array}{ccc} \mathbb{C}/R & \longrightarrow & E_\tau(\mathbb{C}) \\ \downarrow & & \downarrow \\ \mathbb{C}^*/q^{\mathbb{Z}} & \longrightarrow & E_q(\mathbb{C}) \end{array}$$

∎

Más aún, puesto que sabíamos que toda curva elíptica $E/\mathbb{C}$ es isomorfa a una de la forma $E_\tau/\mathbb{C}$, también podemos afirmar que toda curva elíptica es isomorfa a una de la forma $E_q/\mathbb{C}$, luego puede ser parametrizada desde $\mathbb{C}^*/q^{\mathbb{Z}}$ a través de las funciones X, Y.

Vamos a relacionar el discriminante $\Delta(\tau)$ y el invariante $j(\tau)$ de la ecuación clásica

$$Y^2 = 4X^3 - g_2X - g_3$$

con el discriminante $\Delta(q)$ y el invariante $j(q)$ de la ecuación dada por el teorema anterior. Recordemos que, por definición,

$$\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau), \qquad j = \frac{1728\, g_2^3(\tau)}{g_2^3(\tau) - 27g_3^2(\tau)}.$$

En las ecuaciones con las que hemos calculado a_4 y a_6 a partir de g_2 y g_3 podemos despejar

$$g_2 = \frac{(2\pi i)^4}{12}(1 - 48a_4) = \frac{(2\pi i)^4}{12}c_4,$$

$$g_3 = \frac{(2\pi i)^6}{216}(72a_4 - 864a_6 - 1) = \frac{(2\pi i)^6}{216}c_6,$$

donde c_4 y c_6 son las constantes asociadas a la ecuación de Weierstrass de E_q. Por consiguiente,

$$\Delta(\tau) = \frac{(2\pi i)^{12}}{12^3}(c_4^3 - c_6^2) = (2\pi i)^{12}\Delta(q),$$

$$j(\tau) = \frac{(12)^3 g_2(\tau)^3}{\Delta(\tau)} = \frac{c_4^3}{\Delta(q)} = j(q).$$

Ahora, los teoremas [CE 10.31], [CE 12.17] y [CE 10.32] nos dan que

$$\Delta(q) = \sum_{n=1}^{\infty} \tau(n)q^n = q\prod_{n=1}^{\infty}(1 - q^n)^{24},$$

$$j(q) = \frac{1}{q} + \sum_{n=0}^{\infty} c(n)q^n,$$

donde los coeficientes $\tau(n)$ y $c(n)$ son enteros.

Observemos que todas las series que hemos obtenido tienen coeficientes enteros salvo, en principio, la que define a

$$a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12} = -\sum_{n=1}^{\infty}\sum_{d|n}\frac{5d^3 + 7d^5}{12}q^n.$$

Ahora bien, es fácil ver que $12 \mid (5d^3 + 7d^5)$. (Basta razonar que esta expresión es divisible entre 3 y entre 4 tomando congruencias módulo 3 y 4, respectivamente.) Por consiguiente, la serie de potencias que define a $a_6(q)$ también tiene coeficientes enteros.

12.2 La curva de Tate

En esta sección K será un cuerpo métrico discreto y completo. Notemos que la serie

$$s_k(q) = \sum_{n=1}^{\infty}\sigma_k(n)q^n = \sum_{n=1}^{\infty}\frac{n^k q^n}{1 - q^n}$$

converge cuando $|q| < 1$. En efecto, ambas series convergen porque sus respectivos términos generales convergen a 0, y la igualdad entre ambas se demuestra por el mismo argumento que en el caso complejo.

Definición 12.3 Sea K un cuerpo métrico discreto y completo. Para cada $q \in K^*$ tal que $|q| < 1$, definimos la *curva de Tate* como la curva E_q/K definida por la ecuación de Weierstrass

$$Y^2 + XY = X^3 + a_4(q)X + a_6(q),$$

donde

$$a_4(q) = -5s_3(q), \quad a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12}.$$

En principio, no descartamos que K pueda tener característica 2 o 3, pero, al igual que en el caso complejo, la expresión que define a a_6 puede reducirse a una serie de potencias con coeficientes enteros (sin el denominador 12), y así hay que entender la definición de $a_6(q)$. En particular, $|a_4(q)| \leq 1$, $|a_6(q)| \leq 1$, es decir, la ecuación tiene coeficientes enteros.

Consideremos ahora las series formales de potencias que definen a $a_4(q)$ y $a_6(q)$, a las que daremos el mismo nombre, pero ahora $a_4(q)$, $a_6(q) \in \mathbb{Z}[[q]]$. El cuerpo de cocientes $\mathbb{Q}((q))$ está formado por las series de la forma

$$s = \sum_{n=m}^{\infty} a_n q^n, \qquad m \in \mathbb{Z},\ a_n \in \mathbb{Q},$$

y es un cuerpo valorado con la valoración dada por $v(s) = m$, donde m es el menor entero tal que $a_m \neq 0$.

El discriminante $\Delta(q)$ es un polinomio en $a_4(q)$, $a_6(q)$ con coeficientes enteros, por lo que podemos verlo también como serie $\Delta(q) \in \mathbb{Z}[[q]]$. Veamos ahora que la identidad

$$\Delta(q) = \sum_{n=1}^{\infty} \tau(n) q^n,$$

que en principio tenemos probada como igualdad de funciones holomorfas en el disco unitario complejo, es válida también como identidad en $\mathbb{Z}[[q]]$. En efecto, teniendo en cuenta que la suma y el producto de series formales convergentes converge a la suma y el producto de las series de partida, tenemos que el miembro izquierdo es una serie formal que converge a la función holomorfa $\Delta(q)$, y lo mismo vale para el miembro derecho, pero si dos series formales convergen a la misma función holomorfa, es que son iguales.

Más aún, también podemos considerar la identidad

$$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

como una identidad en $\mathbb{Z}[[q]]$. En primer lugar observamos que el producto es convergente, pues, si llamamos P_n al producto parcial n-simo, como

$$(1 + q^n)^{24} = 1 + q^n + \cdots$$

resulta que $v(P_n - P_{n-1}) \geq n$, y esto prueba que la sucesión $\{P_n\}_n$ es de Cauchy, luego convergente. Se trata, pues, de una sucesión de series finitas que converge

formalmente a una serie de potencias y también converge uniformemente en un disco del plano complejo a la función holomorfa dada por la serie $\Delta(q)$. Esto implica que la sucesión $\{P_n^{(i)}/i!\}_n$ es, por una parte, finalmente constante igual al coeficiente i-ésimo del límite formal y, por otra, converge al coeficiente i-ésimo de $\Delta(q)$ (porque si una sucesión de funciones holomorfas converge casi uniformemente, la sucesión de sus derivadas converge a la derivada del límite). Así pues, el límite formal coincide con la serie de potencias $\Delta(q)$.

Similarmente, podemos considerar la serie $c_4(q) \in \mathbb{Z}[[q]]$, así como

$$j(q) = \frac{c_4(q)}{\Delta(q)} \in \mathbb{Q}((q)),$$

que es una serie de Laurent que converge en el disco unitario (menos en 0) a la función holomorfa $j(q)$. Una vez más, la identidad

$$j(q) = \frac{1}{q} + \sum_{n=0}^{\infty} c(n)q^n$$

es válida en $\mathbb{Q}((q))$, pues ambos miembros son series de Laurent que convergen a la misma función meromorfa en el disco unitario, luego deben coincidir.

Con esto ya podemos probar:

Teorema 12.4 *Sea K un cuerpo métrico discreto y completo y $q \in K^*$ tal que $|q| < 1$. Entonces, la curva de Tate E_q/K es una curva elíptica con discriminante e invariante dados por*

$$\Delta(q) = \sum_{n=1}^{\infty} \tau(n)q^n = q\prod_{n=1}^{\infty}(1-q^n)^{24},$$

$$j(q) = \frac{1}{q} + \sum_{n=0}^{\infty} c(n)q^n,$$

donde los coeficientes $\tau(n)$ y $c(n)$ son enteros, los mismos que los de las expresiones análogas en $\mathbb{C}$.

Demostración: Hemos visto que las identidades son válidas en $\mathbb{Q}((q))$ y, al tener coeficientes enteros, todas las series convergen trivialmente en q, luego tenemos las identidades correspondientes en K. En particular, el desarrollo de $\Delta(q)$ en producto infinito prueba que $\Delta(q) \neq 0$, pues, más concretamente, es claro que $|\Delta(q)| = |q|$. Esto prueba que E_q es una curva elíptica. ∎

Recordemos ahora que, según [GA 5.27] y [GA 5.28], el valor absoluto de K se extiende de forma única a cada extensión finita de K, que resulta ser también un cuerpo métrico discreto y completo. Por consiguiente, el valor absoluto de K se extiende también de forma única a la clausura algebraica $\bar{K}$ de K, que es también un cuerpo métrico, aunque puede verse que no es discreto ni completo.

Teniendo esto en cuenta, vamos a probar que las series

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q), \quad Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + s_1(q)$$

convergen en todo punto $u \in \bar{K} \setminus q^{\mathbb{Z}}$, donde $\bar{K}$ es la clausura algebraica de K.

La condición $u \in \bar{K} \setminus q^{\mathbb{Z}}$ es la necesaria para que todos los sumandos estén definidos, y es claro que el término general tiende a 0. Esto prueba que las series convergen en $K(u)$ (porque es completo), luego convergen al mismo límite en $\bar{K}$. (No podíamos razonar directamente con $\bar{K}$ porque no es completo.)

Observemos ahora que las series satisfacen las ecuaciones funcionales

$$X(u,q) = X(qu,q) = X(u^{-1},q),$$

$$Y(u,q) = Y(qu,q), \quad Y(u^{-1},q) = -Y(u,q) - X(u,q).$$

En efecto, la primera ecuación para X es inmediata, para la segunda, multiplicamos el numerador y el denominador del término general (con u^{-1} en lugar de u) por $q^{-2n}u^2$ y obtenemos una reordenación de la serie evaluada en u. La primera ecuación para Y también es inmediata y, para la segunda, multiplicamos el numerador y el denominador del término general de Y por $(q^{-n}u)^3$ y comparamos con la suma de ambas series.

En particular, vemos que $X(q^n u,q) = X(u,q)$, $Y(q^n u,q) = Y(u,q)$ para todo $n \in \mathbb{Z}$. En efecto, para exponentes negativos tenemos, por ejemplo, que

$$X(q^{-n}u,q) = X(q^n u^{-1},q) = X(u^{-1},q) = X(u,q),$$

y con Y se razona análogamente. En otras palabras, X e Y son funciones periódicas, que inducen funciones sobre el cociente $\bar{K}^*/q^{\mathbb{Z}}$ definidas salvo en 1.

Veamos ahora que X e Y cumplen la ecuación de Tate, es decir:

$$Y(u,q)^2 + X(u,q)Y(u,q) = X(u,q)^3 + a_4(q)X(u,q) + a_6(q).$$

Para ello contamos con que esta ecuación se cumple siempre que q es un número complejo de módulo $0 < |q| < 1$ y $u \in \mathbb{C} \setminus q^{\mathbb{Z}}$. En particular, fijado $u \in \mathbb{C}^* \setminus \{1\}$, tenemos que la ecuación se cumple para $|q| < r = \min\{|u|, |u|^{-1}\}$.

Observemos en primer lugar que, si $n > 0$, cada término

$$t_n(T,q) = \frac{q^n T}{(1-q^n T)^2}$$

puede verse como un elemento del anillo $\mathbb{Z}[T][[q]]$, pues el denominador es una unidad de este anillo (porque su término independiente es una unidad en $\mathbb{Z}[T]$. Para índices negativos tenemos que

$$t_{-n}(T,q) = \frac{q^{-n}T}{(1-q^{-n}T)^2} = \frac{q^n T}{(q^n - T)^2},$$

y podemos considerarlo como una serie en $\mathbb{Z}[T]_T[[q]]$, donde hemos localizado respecto de T para que el término independiente del denominador sea una unidad de $\mathbb{Z}[T]_T$. Mas aún, en ambos casos tenemos que $v(t_n(T,q)) = |n|$, luego

la serie definida por estos términos converge en $\mathbb{Z}[T]_T[[q]]$. Por consiguiente, podemos definir

$$X(T,q) = \sum_{n\in\mathbb{Z}} \frac{q^n T}{(1-q^n T)^2} - 2s_1(q) = \frac{T}{(1-T)^2} + \sum_{n=1}^{\infty} P_n(T)q^n \in \mathbb{Q}(T)[[q]],$$

donde $P_n(T) \in \mathbb{Z}[T]_T$. En general, los coeficientes de $X(T,q)$ son funciones racionales de $\mathbb{Q}(T)$ cuyos denominadores son divisibles a lo sumo entre T y $T-1$.

Fijemos ahora un $u \in \mathbb{C}^* \setminus \{1\}$. Es claro que la serie formada por las series formales $t_n(u,q) \in \mathbb{C}[[q]]$ (más el término $-2s_1(q)$) converge formalmente a la serie $X(u,q) \in \mathbb{C}[[q]]$ que resulta de sustituir T por u en cada coeficiente de $X(T,u)$.

Por otra parte, podemos ver los términos $t_n(u,q)$ como funciones holomorfas en el disco $D(0,r)$, y la serie que definen converge absoluta y casi uniformemente en dicho disco, pues, si $|q| \le r' < r$, podemos acotar $|t_n(q)| \le c|q|^{|n|} \le cr^{|n|}$, donde la constante c no depende de q, y basta aplicar el criterio de mayoración de Weierstrass.

Así pues, podemos ver a $X(u,q)$ como una función holomorfa en $D(0,r)$ que es límite casi uniforme de una serie de funciones holomorfas cuyas series de Taylor convergen formalmente en $\mathbb{C}[[q]]$. Esto implica que $X(u,q) \in \mathbb{C}[[q]]$ es la serie de Taylor de la función holomorfa $X(u,q)$.

Similarmente razonamos que podemos considerar

$$Y(T,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n T)^2}{(1-q^n T)^3} + s_1(q) = \frac{T^2}{(1-T)^3} + \sum_{n=1}^{\infty} Q_n(T)q^n \in \mathbb{Q}(T)[[q]],$$

con $Q(T) \in \mathbb{Z}[T]_T$ de modo que la serie $Y(u,q)$ converge en $D(0,r)$.

A su vez, esto nos permite considerar la ecuación de Weierstrass como una igualdad en $\mathbb{C}[[q]]$. Llevando todos sus términos a un mismo miembro, es una ecuación de la forma $S(u,q) = 0$, para cierta serie $S(u,q) \in \mathbb{C}[[q]]$ que resulta de sustituir T por u en una serie $S(T,q) \in \mathbb{Q}(T)[[q]]$ cuyos coeficientes son funciones racionales en $\mathbb{Q}(T)$ cuyos denominadores son divisibles a lo sumo entre T y $T-1$.

Ahora bien, sabemos que $S(u,q) = 0$ para todo $q \in D(0,r)$, lo que implica que la serie de potencias $S(u,q)$ es idénticamente nula para todo u, es decir, que los coeficientes de $S(T,q)$ son funciones racionales de $\mathbb{C}(T)$ que se anulan en todo $u \in \mathbb{C}^* \setminus \{1\}$, luego son idénticamente nulos. Así pues, $S(T,q) = 0$ o, lo que es lo mismo, la ecuación de Weierstrass se cumple en $\mathbb{Q}(T)[[q]]$.

Por último, tomamos $q \in K$ y $u \in \bar{K} \setminus q^{\mathbb{Z}}$. Claramente[1] $S(u,q) = 0$, y esto equivale a que $X(u,q)$ e $Y(u,q)$ satisfacen la ecuación de Weierstrass.

[1]Si K tiene característica prima p, observamos primero que el hecho de que $S(T,q)$ sea idénticamente nula en $\mathbb{Q}(T)[[q]]$ implica que también lo es en $k(T)[[q]]$, donde $k = \mathbb{Z}/p\mathbb{Z}$, teniendo en cuenta que todos los coeficientes de $S(T,q)$ son funciones de $\mathbb{Q}(T)$ con coeficientes enteros y denominadores de la forma $T^i(T-1)^j$.

Definición 12.5 Sea K un cuerpo métrico discreto y completo y $q \in K^*$ tal que $|q| < 1$. La *aplicación de Tate* es la aplicación $\phi : \bar{K}^* \longrightarrow E_q(\bar{K})$ dada por

$$\phi(u) = \begin{cases} (X(u,q), Y(u,q)) & \text{si } u \notin q^{\mathbb{Z}}, \\ \mathrm{O} & \text{si } u \in q^{\mathbb{Z}}, \end{cases}$$

donde O es el punto infinito de E_q/K.

El paso siguiente es demostrar que ϕ es un homomorfismo de grupos. Para ello tomamos u_1, $u_2 \in \bar{K}^*$ y llamamos $u_3 = u_1u_2$, $P_i = \phi(u_i)$, con lo que hemos de probar que $P_3 = P_1 + P_2$.

Esto es evidente si $u_1 \in q^{\mathbb{Z}}$, pues entonces $P_1 = O$ y $P_3 = P_2 = O + P_2$, y lo mismo sucede si $u_2 \in q^{\mathbb{Z}}$. Así pues, podemos suponer que u_1, $u_2 \notin q^{\mathbb{Z}}$.

Supongamos ahora que $u_3 \in q^{\mathbb{Z}}$, con lo que hemos de probar que $P_1 + P_2 = O$. Tenemos que $u_2 = u_1^{-1}q^m$, luego

$$X(u_2,q) = X(u_1,q), \quad Y(u_2,q) = -Y(u_1,q) - X(u_1,q).$$

Según [CE 2.21], ésta es precisamente la relación que ha de darse entre las coordenadas de dos puntos P_1 y P_2 para que sea $P_2 = -P_1$.

A partir de aquí suponemos que u_1, u_2, $u_3 \notin q^{\mathbb{Z}}$, con lo que los tres puntos P_i son finitos, digamos $P_i = (x_i, y_i)$. (En otras palabras, llamamos $x_i = X(u_i, q)$, $y_i = Y(u_i, q)$.) Supongamos además que $x_1 \neq x_2$. Entonces, según [CE 2.21], la relación $P_3 = P_1 + P_2$ equivale a

$$(x_2 - x_1)^2 x_3 = (y_2 - y_1)^2 + (y_2 - y_1)(x_2 - x_1) - (x_1 + x_2)(x_2 - x_1)^2,$$

$$(x_2 - x_1)y_3 = -(y_2 - y_1 + x_2 - x_1)x_3 - (y_1x_2 - y_2x_1).$$

Si (tras pasar todos los términos al mismo miembro) sustituimos en estas ecuaciones

$$x_1 = X(T_1,q), \quad x_2 = X(T_2,q), \quad x_3 = X(T_1T_2,q),$$

$$y_1 = Y(T_1,q), \quad y_2 = Y(T_2,q), \quad y_3 = Y(T_1T_2,q),$$

obtenemos dos series $E_1(T_1, T_2, q)$, $E_2(T_1, T_2, q) \in \mathbb{Q}(T_1, T_2)[[q]]$ cuyos coeficientes son funciones racionales de $\mathbb{Q}(T_1, T_2)$ con coeficientes enteros y cuyos denominadores contienen a lo sumo los factores T_1, T_2, $T_1 - 1$, $T_2 - 1$, $T_1T_2 - 1$. Basta probar que ambas series son idénticamente nulas. Para ello observamos que, si fijamos u_1, $u_2 \in \mathbb{C}^* \setminus \{1\}$ tales que $u_3 = u_1u_2 \neq 1$, las series de potencias $X(u_i, q)$, $Y(u_i, q)$ convergen cuando q varía en un disco $D(0, r)$, para cierto r suficientemente pequeño y las sumas satisfacen las dos ecuaciones precedentes, luego las series $E_i(u_1, u_2, q) \in \mathbb{C}[[q]]$ son idénticamente nulas. Como esto vale para (casi) todos los números complejos u_1 y u_2, esto implica que las series $E_i(T_1, T_2, q)$ son idénticamente nulas.

Nos falta considerar el caso en que $x_1 = x_2$. Observemos que una curva elíptica contiene a lo sumo dos puntos con la misma coordenada x y, cuando hay dos, uno es el opuesto del otro. Así pues, nos falta probar que se cumple $\phi(u_1u_2) = \phi(u_1) + \phi(u_2)$ cuando $\phi(u_1) = \pm\phi(u_2)$. Terminaremos la prueba gracias al siguiente hecho elemental:

Teorema 12.6 *Sea $\phi : G \longrightarrow H$ una aplicación de un grupo (multiplicativo) G en un grupo (aditivo) H tal que $\phi(u_1u_2) = \phi(u_1) + \phi(u_2)$ siempre que u_1, $u_2 \in G$ cumplen $\phi(u_1) \neq \pm\phi(u_2)$. Si ϕ toma infinitos valores, entonces es un homomorfismo.*

DEMOSTRACIÓN: Dados u_1, $u_2 \in G$, podemos tomar $u \in G$ tal que $\phi(u)$ sea distinto de

$$\pm\phi(u_1), \quad -\phi(u_1) \pm \phi(u_2), \quad \pm\phi(u_1u_2).$$

Entonces $\phi(uu_1) = \phi(u) + \phi(u_1) \neq \pm\phi(u_2)$, luego

$$\phi(u) + \phi(u_1) + \phi(u_2) = \phi(uu_1) + \phi(u_2) = \phi(uu_1u_2) = \phi(u) + \phi(u_1u_2),$$

luego $\phi(u_1) + \phi(u_2) = \phi(u_1u_2)$. ∎

Para aplicar este teorema, sólo hemos de probar que la aplicación de Tate toma infinitos valores en $E_q(\bar{K})$. Ahora bien, la expresión

$$X(T,q) = \frac{T}{(1-T)^2} + \sum_{n=1}^{\infty} P_n(T)q^n$$

muestra que si $t \in K$ cumple $|t| < 1$, entonces $|P_n(1+t)| \leq 1$ (pues el denominador de P_n es de la forma T^i), luego

$$X(1+t,q) = \frac{1+t}{t^2} + \cdots$$

donde los puntos suspensivos representan un entero, luego $|X(1+t,q)| = |t|^{-2}$, luego los puntos $\phi(1+t^n)$, para $n = 1, 2, \ldots$ son distintos dos a dos.

El teorema siguiente recoge los hechos básicos sobre la aplicación de Tate:

Teorema 12.7 *Sea K un cuerpo métrico discreto y completo y $q \in K^*$ tal que $|q| < 1$. Entonces, la aplicación de Tate induce un isomorfismo de grupos $\phi : \bar{K}^*/q^{\mathbb{Z}} \longrightarrow E_q(\bar{K})$ compatible con la acción del grupo de Galois $G(\bar{K}/K)$, es decir, que para todo $\sigma \in G(\bar{K}/K)$ y todo $u \in \bar{K}$, se cumple que $\phi(u^\sigma) = \phi(u)^\sigma$.*

DEMOSTRACIÓN: Acabamos de probar que ϕ es un homomorfismo de grupos y, por la propia definición, es inmediato que su núcleo es $q^{\mathbb{Z}}$, luego induce un monomorfismo en $\bar{K}^*/q^{\mathbb{Z}}$. La suprayectividad no es fácil de probar, de modo que dedicaremos toda la sección siguiente a demostrarla.

La última propiedad se debe a que los automorfismos conservan el valor absoluto,[2] luego son continuos y "atraviesan" las series infinitas. ∎

[2]Esto es debido a la unicidad de la extensión, ya que, dado $\sigma \in G(\bar{K}/K)$, podríamos definir $|x|^* = |\sigma(x)|$ y tendríamos otro valor absoluto en $\bar{K}$ que extendería al de K, luego ha de ser $|\sigma(x)| = |x|$.

12.3 La suprayectividad de la aplicación de Tate

Tal y como hemos indicado en la prueba del teorema 12.7, dedicamos esta sección a terminarla, demostrando que la aplicación de Tate es suprayectiva. En realidad vamos a probar algo ligeramente más fuerte: si L/K es una extensión finita y $P \in E_q(L)$, entonces existe un $u \in L^*$ tal que $\phi(u) = P$. (Notemos que todo $P \in E_q(\bar{K})$ está en $E_q(L)$, para cierta extensión finita L/K. Lo que probamos es más fuerte porque demostramos que P tiene una antiimagen precisamente en L^* y no sólo en $\bar{K}^*$.)

Notemos que la curva E_q y la aplicación de Tate ϕ no se alteran si cambiamos K por L, por lo que no perdemos generalidad si suponemos que $L = K$, con lo cual, lo que hemos de probar es que la aplicación $\phi : K^* \longrightarrow E_q(K)$ es suprayectiva.

En realidad probaremos todavía más que esto: llamemos

$$D = \{u \in K \mid |u| \leq 1\}$$

al anillo de enteros de K, sea $\mathfrak{m} = (\pi)$ su ideal maximal, sea $k = D/\mathfrak{m}$ el cuerpo de restos y sea v la valoración en K asociada a π. Llamamos

$$D^* = \{u \in D \mid |u| = 1\}$$

al grupo de las unidades de D y consideramos su subgrupo

$$D_1^* = \{u \in D \mid u \equiv 1 \ (\text{mód } \mathfrak{m})\}.$$

Observemos que el homomorfismo natural $D^* \longrightarrow K^*/q^{\mathbb{Z}}$ es inyectivo, luego podemos considerar $D_1^* \subset D^* \subset K^*/q^{\mathbb{Z}}$. Vamos a probar que la aplicación de Tate induce un isomorfismo $\phi : K^*/q^{\mathbb{Z}} \longrightarrow E_q(K)$ que hace corresponder estos subgrupos con los subgrupos $E_{q,1}(K) \subset E_{q,0}(K) \subset E_q(K)$, respectivamente.

Para empezar notamos que la serie que define $s_k(q)$ muestra que $q \mid s_k(q)$, luego también $q \mid a_4(q)$, $a_6(q)$. A su vez, esto implica que

$$v(c_4(q)) = v(1 - 48a_4(q)) = 0,$$

y el teorema [CE 6.4] nos permite concluir que la ecuación de Tate es minimal. Por consiguiente, los grupos $E_{q,1}(K)$ y $E_{q,0}(K)$ pueden calcularse reduciendo módulo $\mathfrak{m}$ la propia ecuación de Tate. La reducción es la curva sobre k dada por la ecuación

$$Y^2 + XY = X^3.$$

Según el teorema 8.24, vemos que tiene un nodo, que es racional, pues en la prueba se ve que esto depende del polinomio $T^2+a_1T-a_2 = T^2+T = T(T+1)$, que tiene sus raíces en k. En otras palabras, las curvas de Tate tienen siempre reducción multiplicativa racional.

El punto singular de la reducción es el punto de coordenadas $(0,0)$, y los puntos de $E_q(K)$ que se reducen a $(0,0)$ son los que pueden expresarse en la forma $[\pi u, \pi v, \epsilon]$, con $u, v \in D$, $\epsilon \in D^*$. Equivalentemente, son los puntos (x, y)

con $v(x), v(y) \geq 1$, luego $E_{q,0}(K)$ está formado por O y por los puntos (x, y) tales que $v(x) \leq 0$ o $v(y) \leq 0$.

Similarmente, los puntos finitos que se reducen a $[0, 1, 0]$ son los de la forma $[\pi u, \epsilon, \pi v]$, con $u, v \in D$, $\epsilon \in D^*$. Así pues, $E_{q,1}(K)$ está formado por O y los puntos finitos (x, y) tales que $v(y) < 0$.

Las series de Laurent que hemos encontrado para $X(u, q)$ e $Y(u, q)$ muestran que

$$X(u,q) \in \frac{u}{(1-u)^2} + \mathfrak{m}, \quad Y(u,q) \in \frac{u^2}{(1-u)^3} + \mathfrak{m},$$

de donde se sigue inmediatamente que $\phi[D^*] \subset E_{q,0}(K)$ y que $\phi[D_1^*] \subset E_{q,1}(K)$.

El teorema [CE 6.16] afirma que la aplicación $E_{q,1}(K) \longrightarrow \mathfrak{m}$ dada por

$$(x, y) \mapsto -\frac{x}{y}, \qquad O \mapsto 0$$

es biyectiva. (El teorema afirma que, de hecho, es un isomorfismo de grupos cuando en $\mathfrak{m}$ consideramos la estructura de grupo inducida por el grupo formal de E_q, pero no necesitamos esto.) Por otra parte, tenemos una biyección obvia $\mathfrak{m} \longrightarrow D_1^*$ dada por $t \mapsto 1 + t$. Consideramos la composición

$$\mathfrak{m} \longrightarrow D_1^* \xrightarrow{\phi} E_{q,1}(K) \longrightarrow \mathfrak{m},$$

que es la aplicación dada por

$$t \mapsto -\frac{X(1+t,q)}{Y(1+t,q)}, \qquad 0 \mapsto 0.$$

Como hemos compuesto ϕ con dos aplicaciones biyectivas, si la composición es suprayectiva, ϕ también lo será.

Si en el desarrollo en serie de Laurent

$$X(T,q) = \frac{T}{(1-T)^2} + \sum_{n=1}^{\infty} P_n(T) q^n$$

cambiamos T por $1 + T$ obtenemos

$$X(1+T,q) = \frac{1+T}{T^2} + \sum_{n=1}^{\infty} P_n(1+T) q^n,$$

donde $P_n(1 + T)$ es una función racional cuyo denominador es de la forma $(1 + T)^i$. Como $1 + T$ es una unidad en $\mathbb{Z}[[T]]$, podemos desarrollar

$$P_n(1+T) = \sum_{m=0}^{\infty} c_{mn} T^m,$$

con c_{mn} en $\mathbb{Z}$ (o en el cuerpo primo de K), y así, como serie formal en $K[[T]]$,

$$X(1+T) = \frac{1+T}{T^2} + \sum_{n=1}^{\infty}\sum_{m=0}^{\infty} c_{mn} T^m q^n = \frac{1+T}{T^2} + \sum_{m=0}^{\infty}\sum_{n=1}^{\infty} c_{mn} q^n T^m$$

$$= T^{-2}(1 + T + T^2 \sum_{m=0}^{\infty} \alpha_{m+2} T^m) = T^{-2}(1 + \sum_{m=1}^{\infty} \alpha_m T^m),$$

con $\alpha_m \in D$. Esta serie converge para todo $t \in \mathfrak{m}$.

Similarmente obtenemos una serie de Laurent

$$Y(1+T) = -T^{-3}(1 + \sum_{m=1}^{\infty} \beta_m T^m),$$

para ciertos $\beta_m \in D$. La serie entre paréntesis tiene inversa en $D[[T]]$, la cual tendrá término independiente igual a 1. Por lo tanto,

$$-\frac{X(1+T,q)}{Y(1+T,q)} = T(1 + \sum_{m=1}^{\infty} \gamma_m T^m),$$

para ciertos $\gamma_m \in D$. Todo se reduce a probar que la aplicación $\mathfrak{m} \longrightarrow \mathfrak{m}$ dada por

$$t \mapsto t(1 + \sum_{m=1}^{\infty} \gamma_m t^m)$$

es suprayectiva, y esto es consecuencia inmediata del teorema [CE 5.6], donde se construye una serie $G(T) = T(1 + \cdots)$ inversa de la serie dada.

Con esto tenemos probado que $\phi : D_1^* \longrightarrow E_{q,1}(K)$ es biyectiva. Estudiamos ahora el homomorfismo

$$\bar{\phi} : D^*/D_1^* \longrightarrow E_{q,0}(K)/E_{q,1}(K)$$

inducido por ϕ. Puesto que $D^* = D \setminus \mathfrak{m}$, es claro que $D^*/D_1^* \cong k^*$ y, por [CE 6.8], tenemos un isomorfismo

$$E_{q,0}(K)/E_{q,1}(K) \cong \tilde{E}_q(k),$$

donde $\tilde{E}_q(k)$ es el grupo de puntos racionales regulares de la reducción de E_q módulo $\mathfrak{m}$. Nuevamente, si probamos que la composición

$$k^* \longrightarrow D^*/D_1^* \xrightarrow{\bar{\phi}} E_{q,0}(K)/E_{q,1}(K) \longrightarrow \tilde{E}_q(k)$$

es suprayectiva, tendremos que $\bar{\phi}$ también lo será.

Ahora bien, es fácil ver que dicha composición es

$$a \mapsto \left(\frac{a}{(1-a)^2}, \frac{a^2}{(1-a)^3}\right), \qquad 1 \mapsto O.$$

En efecto, todo $a \in k^* \setminus \{1\}$ es de la forma $a = [u]$, para cierto $u \in D$ tal que $1 - u \in D^*$. Al aplicar ϕ obtenemos $(X(u,q), Y(u,q))$. Por último hemos de calcular la reducción de este punto módulo $\mathfrak{m}$, y antes hemos visto que, este par es congruente módulo $\mathfrak{m}$ con

$$\left(\frac{u}{(1-u)^2}, \frac{u^2}{(1-u)^3}\right),$$

luego la aplicación tiene la forma indicada. Ahora es fácil ver que es suprayectiva, pues una antiimagen para un punto (x, y) es $a = y^2/x^3$. En efecto, tenemos

que (x, y) cumple la ecuación $y^2 + xy = x^3$, luego no puede ser $x = 0$ (ya que entonces (x, y) sería el punto singular $(0, 0)$). Usando la ecuación se comprueba sin dificultad que la imagen de a es ciertamente (x, y).

Ahora consideramos el diagrama conmutativo siguiente, con filas exactas:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & D_1^* & \longrightarrow & D^* & \longrightarrow & k^* & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle \phi} & & \downarrow & & \\ 0 & \longrightarrow & E_{q,1}(K) & \longrightarrow & E_{q,0}(K) & \longrightarrow & \tilde{E}_{q,r}(k) & \longrightarrow & 0 \end{array}$$

Hemos probado que las dos flechas verticales de los extremos son isomorfismos, luego ϕ también lo es. Esto implica a su vez que el homomorfismo inducido por ϕ entre los cocientes

$$\tilde{\phi} : K^*/D^*q^{\mathbb{Z}} \longrightarrow E_q(K)/E_{q,0}(K)$$

es inyectivo. Si probamos que es suprayectivo, un diagrama conmutativo análogo nos dará que el homomorfismo $\phi : K^*/q^{\mathbb{Z}} \longrightarrow E_q(K)$ es biyectivo.

Ahora bien, si $v(q) = m$, es claro que el homomorfismo

$$K^*/D^*q^{\mathbb{Z}} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

inducido por $u \mapsto v(u)$ es un isomorfismo. Así pues, como $\tilde{\phi}$ es inyectiva y su dominio tiene m elementos, para que sea suprayectiva basta probar que $|E_q(K)/E_{q,0}(K)| \leq m$.

Para ello aplicamos el teorema 10.42, que nos acota este índice por $|\Phi_{E_q}(k)|$, es decir, por el número de componentes irreducibles con puntos racionales del modelo de Néron de E_q. Ahora bien, sabemos que E_q tiene reducción multiplicativa racional, luego la fibra cerrada de su modelo regular minimal es de tipo $\mathrm{I_n}$ donde, según el algoritmo de Tate, $n = v(\Delta)$ y, entonces $|\Phi_{E_q}(k)| = n$.

Ahora tenemos en cuenta que el desarrollo de $\Delta(q)$ en producto infinito del teorema 12.4 implica que $n = v(\Delta) = v(q) = n$, y esto termina la prueba.

El teorema siguiente recoge los hechos adicionales que hemos probado, más allá de lo enunciado en el teorema 12.7:

Teorema 12.8 *Sea K un cuerpo métrico discreto y completo, sea D su anillo de enteros, sea D^* su grupo de unidades, sea $\mathfrak{m}$ su ideal maximal, sea k su cuerpo de restos y sea*

$$D_1^* = \{u \in D^* \mid u \equiv 1 \ (\text{mód } \mathfrak{m})\}.$$

Entonces, para cada $q \in K^*$ tal que $|q| < 1$, la curva de Tate E_q/K tiene reducción multiplicativa racional, y la aplicación de Tate determina un isomorfismo

$$\phi : K^*/q^{\mathbb{Z}} \longrightarrow E_q(K)$$

que hace corresponder los subgrupos $D_1^* \subset D^* \subset K^*/q^{\mathbb{Z}}$ con los subgrupos $E_{q,1}(K) \subset E_{q,0}(K) \subset E_q(K)$. Por consiguiente, si $n = v(q)$,

$$E_q(K)/E_{q,0}(K) \cong \mathbb{Z}/n\mathbb{Z}, \qquad E_{q,0}(K)/E_{q,1}(K) \cong k^*.$$

12.4 Curvas con reducción multiplicativa

En la sección primera hemos visto que toda curva elíptica $E/\mathbb{C}$ es isomorfa a una curva $E_\tau/\mathbb{C}$ asociada a un retículo complejo, de modo que puede ser parametrizada (con las funciones de Weierstrass) desde un toro complejo. Si sustituimos $\mathbb{C}$ por un cuerpo métrico discreto y completo K, el resultado análogo es falso, es decir, no toda curva elíptica E/K es isomorfa (ni siquiera sobre $\bar{K}$) a una curva de Tate E_q. Por ejemplo, una condición necesaria es que E/K tenga reducción multiplicativa racional. En esta sección demostraremos que la condición también es suficiente

Empecemos observando que el desarrollo en serie del invariante de E_q muestra que

$$|j(q)| = \frac{1}{|q|} > 1.$$

Ahora demostramos que $j(q)$ toma todos los valores posibles que satisfacen esta condición necesaria:

Teorema 12.9 *Sea K un cuerpo métrico discreto y completo, sea $\alpha \in \bar{K}$ tal que $|\alpha| > 1$. Entonces existe un único $q \in K(\alpha)$ tal que $j(q) = \alpha$.*

Demostración: La idea es aplicar el teorema [CE 5.6], pero no podemos aplicarlo directamente a la serie de $j(q)$. Ésta es de la forma

$$j(q) = \frac{1}{q}(1 + c(0)q + c(1)q^2 + \cdots),$$

donde los coeficientes son enteros. La serie entre paréntesis tiene inversa en $\mathbb{Z}[[q]]$, luego

$$f(q) = \frac{1}{j(q)} = q + c_2q^2 + \cdots,$$

donde los coeficientes c_i son también enteros. A esta serie sí que podemos aplicarle el teorema [CE 5.6], que nos da otra serie $g(q) = q + d_2q^2 + \cdots$ tal que $f(g(q)) = q$. Como $|1/\alpha| < 1$, podemos calcular $q = g(1/\alpha) \in K(\alpha)$ (es decir, que la serie converge en $1/\alpha$). Además, $|q| = |1/\alpha| < 1$ y

$$\frac{1}{j(q)} = f(q) = f(g(1/\alpha)) = \frac{1}{\alpha},$$

luego $j(q) = \alpha$.

Para probar la unicidad, supongamos que $j(q) = j(q')$, con $|q| < 1$, $|q'| < 1$. Entonces $f(q) = f(q')$, luego

$$0 = f(q) - f(q') = q - q' + c_2(q^2 - q'^2) + \cdots,$$

y es claro que podemos sacar factor común $q - q'$, de modo que

$$0 = |f(q) - f(q')| = |q - q'||1 + c_2(q + q') + \cdots\ | = |q - q'|,$$

luego $q = q'$. ∎

Observemos que una curva elíptica E/K tiene mala reducción si y sólo si su discriminante minimal cumple $|\Delta| < 1$ y, por 8.24, la reducción será multiplicativa si y sólo si $|c_4| = 1$. Esto implica que $|j(E)| = |c_4^3/\Delta| > 1$. Así pues, toda curva elíptica E/K con reducción multiplicativa es isomorfa sobre $\bar{K}$ a una curva de Tate. Vamos a investigar bajo qué condiciones podemos asegurar que el isomorfismo está definido sobre K. El teorema siguiente nos ayudará en casi todos los casos:

Teorema 12.10 *Sea E/K una curva elíptica definida sobre un cuerpo de característica distinta de 2 o 3 y supongamos que $j(E) \neq 0, 1728$. Definimos*

$$\gamma(E/K) = -c_4/c_6 \in K^*/K^{*2}.$$

Entonces $\gamma(E/K)$ es independiente de la ecuación de Weierstrass de E/K con la que se calcula y, si E'/K es otra curva elíptica que cumpla $j(E') \neq 0, 1728$, se cumple que $E/K \cong E'/K$ si y sólo si $j(E) = j(E')$ y $\gamma(E/K) = \gamma(E'/K)$.

Demostración: En característica distinta de 2 o 3 se cumple la relación $\Delta = (c_4^3 - c_6^2)/1728$, luego

$$j(E) = \frac{c_4^3}{\Delta} = \frac{1728c_4^3}{c_4^3 - c_6^2},$$

así, las condiciones $j(E) \neq 0, 1728$ equivalen a que (para cualquier ecuación de Weierstrass) $c_4 \neq 0 \neq c_6$, condiciones necesarias para la definición de $\gamma(E/K)$.

Si consideramos dos ecuaciones de Weierstrass, los nuevos c_4 y c_6 están relacionados con los iniciales según las fórmulas $u^4c_4' = c_4$, $u^6c_6' = c_6$, para cierto $u \in K^*$. Por lo tanto,

$$\frac{c_4'}{c_6'} = u^2\,\frac{c_4}{c_6} \equiv \frac{c_4}{c_6} \text{ (mód } K^{*2}).$$

Esto prueba que $\gamma(E/K)$ está bien definido. Es obvio que si $E/K \cong E'/K$, entonces $j(E) = j(E')$ y $\gamma(E/K) = \gamma(E'/K)$. Para probar el recíproco, en virtud del teorema [CE 2.7], la hipótesis sobre la característica de K nos permite considerar ecuaciones de Weierstrass de la forma

$$Y^2 = X^3 + a_4X + a_6, \qquad Y^2 = X^3 + a_4'X + a_6'.$$

Así,

$$j(E) = 1728\,\frac{4a_4^3}{4a_4^3 + 27a_6^2} = 1728\frac{4(a_4^3/a_6^2)}{4(a_4^3/a_6^2) + 27},$$

luego, llamando $v = a_4^3/a_6^2$, la hipótesis $j(E) = j(E')$ implica que

$$\frac{v}{4v + 27} = \frac{v'}{4v' + 27},$$

de donde se sigue inmediatamente que $v = v'$, es decir, que

$$\frac{a_4^3}{a_6^2} = \frac{a_4'^3}{a_6'^2}.$$

Por otra parte, tenemos que $c_4 = -48a_4$, $c_6 = -864a_6$, luego la hipótesis $\gamma(E/K) = \gamma(E'/K)$ implica que

$$\frac{2a_4}{a_6} \equiv \frac{c_4}{c_6} \equiv \frac{c'_4}{c'_6} \equiv \frac{2a'_4}{a'_6} \text{ (mód } K^{*2}).$$

Por consiguiente, existe un $t \in K^*$ tal que $a_4a'_6 = t^2a'_4a_6$. Entonces, sustituyendo en la relación $a_4^3a_6'^2 = a_4'^3a_6^2$ obtenemos que $a'_4 = t^4a_4$ y, multiplicando las dos ecuaciones llegamos a que $a'_6 = t^6a_6$. Esto significa que el cambio de variables $X = t^2X'$, $Y = t^3Y'$ transforma la primera ecuación en la segunda, luego $E/K \cong E'/K$. ∎

Nota No es difícil adaptar la prueba del teorema anterior al caso en que K tiene característica 3, pero en característica 2 sucede que $\gamma(E/K)$ siempre vale 1, por lo que el resultado ya no es cierto. ∎

Ahora es inmediato el refinamiento siguiente de [CE 2.9]:

Teorema 12.11 *Si dos curvas elípticas E/K y E'/K tienen el mismo invariante $j \neq 0, 1728$, existe una extensión cuadrática L/K tal que $E_L/L \cong E'_L/L$.*

Demostración: Si $\operatorname{car} K \neq 2, 3$, basta tomar

$$L = K\left(\sqrt{\tfrac{\gamma(E/K)}{\gamma(E'/K)}}\right),$$

que es una extensión cuadrática de K bien definida porque los invariantes están definidos módulo K^{*2}. Es claro entonces que $\gamma(E_L/K) = \gamma(E'_L/L)$, luego el teorema anterior nos da el isomorfismo indicado.

Si $\operatorname{car} K = 2, 3$ basta examinar la prueba del teorema [CE 2.9] para comprobar que, tanto en el caso $\operatorname{car} K = 3$ y $j \neq 0$, como en el caso $\operatorname{car} K = 2$ y $j \neq 0$, el cambio de variables que determina el isomorfismo requiere a lo sumo una extensión cuadrática para estar definido sobre el cuerpo dado. ∎

Los invariantes 0 y 1728 que hemos descartado no deben preocuparnos, pues en cualquier cuerpo métrico discreto tienen valor absoluto ≤ 1. Ahora podemos probar el teorema fundamental:

Teorema 12.12 (Tate) *Sea K un cuerpo métrico discreto y completo de característica distinta de 2 o 3, sea E/K una curva elíptica tal que $|j(E)| > 1$ y sea $\gamma(E/K) \in K^*/K^{*2}$ el invariante definido en el teorema* 12.10*.*

a) Existe un único $q \in K^*$ con $|q| < 1$ tal que $E_{\bar{K}} \cong E_{q\bar{K}}$.

b) Las afirmaciones siguientes son equivalentes:

1. *$E/K \cong E_q/K$.*
2. *$\gamma(E/K) = 1$.*
3. *E tiene reducción multiplicativa racional.*

DEMOSTRACIÓN: Por el teorema 12.9 existe un único $q \in K^*$ con $|q| < 1$ tal que $j(q) = j(E)$, lo que implica que E_q es la única curva de Tate isomorfa a E (sobre $\bar{K}$). En vista del teorema anterior, para probar la equivalencia entre b1 y b2 basta probar que $\gamma(E_q/K) = 1$. Para E_q tenemos que

$$c_4(q) = 1 - 48a_4(q) = 1 + 240s_3(q),$$

$$c_6(q) = -1 + 72a_4(q) - 864a_6(q) = -1 + 504s_5(q).$$

Hemos de probar que

$$\frac{1 + 240s_3(q)}{1 - 504s_5(q)}$$

es un cuadrado en K^*. De hecho, vamos a probar que, si $\alpha \in K^*$ cumple $|\alpha| < 1$, entonces $1 + 4\alpha \in K^*$, lo que implica que tanto el numerador como el denominador de la fracción anterior son cuadrados.

Para ello recordamos[3] que el desarrollo en serie de Taylor de la función holomorfa $(1 + z)^{-1/2}$ alrededor de $z = 0$ es

$$(1 + z)^{-1/2} = \sum_{n=0}^{\infty} \binom{-1/2}{n} z^n,$$

donde

$$\binom{-1/2}{n} = \frac{\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)\left(-\frac{5}{2}\right)\cdots\left(-\frac{2n-1}{2}\right)}{n!} = \frac{(-1)^n}{4^n}\binom{2n}{n},$$

luego

$$(1 + 4z)^{-1/2} = \sum_{n=0}^{\infty} (-1)^n \binom{2n}{n} z^n.$$

Si llamamos $F(z) \in \mathbb{Z}[[z]]$ a la serie dada por el miembro derecho, la igualdad

$$(1 + 4z)F(z)^2 = 1,$$

válida para todo $z \in D(0, 1/4)$ implica que la identidad es cierta formalmente en el anillo $\mathbb{Z}[[z]]$, y la serie converge en todo $\alpha \in K^*$ con $|\alpha| < 1$, luego tenemos que $1 + 4\alpha = (1/F(\alpha))^2$, como queríamos probar.

Obviamente, si $E/K \cong E_q/K$, entonces E tiene reducción multiplicativa racional (porque sabemos que E_q la tiene. Así pues, sólo hemos de probar que b3 implica b2.

De acuerdo con el algoritmo de Tate, si E/K tiene reducción multiplicativa, admite una ecuación de Weierstrass tal que

$$\pi \mid a_3, a_4, a_6, \quad \pi \mid b_4, b_6, \quad \pi \nmid b_2.$$

Por lo tanto,

$$\gamma(E/K) = -\frac{c_4}{c_6} = \frac{b_2^2 - 24b_4}{b_2^3 - 36b_2b_4 + 216b_6} = \frac{1}{b_2}\,\frac{1 - 24\frac{b_4}{b_2^2}}{1 - 36\frac{b_4}{b_2^2} + 216\frac{b_6}{b_2^3}}.$$

[3]Véase mi libro de Funciones de variable compleja, al final de la sección 3.3

Teniendo en cuenta que $|b_4/b_2^2| < 1$ y $|b_6/b_2^3| < 1$, el numerador y el denominador de la segunda fracción son cuadrados en K^*, pues ambos son de la forma $1 + 4\alpha$ con $|\alpha| < 1$. Así pues,

$$\gamma(E/K) = 1/b_2 \equiv b_2 \text{ (mód } K^{*2}).$$

Ahora bien, que la reducción de E/K sea racional equivale a que el polinomio $T^2 + \bar{a}_1 T - \bar{a}_2$ tenga raíces simples en k. El lema de Hensel[4] implica que estas raíces han de ser de la forma $\bar{\alpha}$, $\bar{\beta}$, donde α y β son raíces del polinomio $T^2 + a_1 T - a_2$. Así pues, este polinomio tiene raíces simples en K, luego su discriminante, que es precisamente b_2, es un cuadrado en K^*. Esto prueba que $\gamma(E/K) = 1$. ∎

Aunque el caso que nos va interesar es el de las curvas elípticas definidas sobre cuerpos de característica 0, lo cierto es que la restricción sobre la característica en el teorema anterior se puede eliminar. Para ello conviene observar un hecho general:

Teorema 12.13 *Sea K un cuerpo métrico completo y discreto. Si una curva elíptica E/K admite una ecuación de Weierstrass de la forma*

$$Y^2 + XY = X^3 + a_4 X + a_6,$$

donde $v(a_4), v(a_6) \geq 1$, entonces es isomorfa a una única curva de Tate.

Demostración: Se comprueba inmediatamente que el invariante de E cumple $|j(E)| > 1$, luego existe una única curva de Tate E_q/K con el mismo invariante, la cual cumple una ecuación de la forma

$$Y^2 + XY = X^3 + a_4' X + a_6'.$$

Como $E_{\bar{K}} \cong E_{q,\bar{K}}$, existen $u, r, s, t \in \bar{K}$ tales que una ecuación se transforma en la otra mediante un cambio de variables del tipo descrito en el teorema 4.23. Las relaciones que proporciona dicho teorema se reducen a

(1)	$1 + s = u$	(5)	$1 + 12r = u^2$
(2)	$-s + 3r - s^2 = 0$	(6)	$b_4 + r + 6r^2 = u^4 b_4'$
(3)	$r + 2t = 0$	(7)	$c_4 = u^4 c_4'$
(4)	$a_4 - t - rs + 3r^2 - 2st = u^4 a_4'$	(8)	$c_6 = u^6 c_6'$

Si $\operatorname{car} K = 2$, la primera ecuación nos da $u = 1$, la tercera $r = 0$, la segunda $s = 0, 1$ y la cuarta que $t \in K$, luego el cambio de variables determina un isomorfismo definido sobre K.

Si $\operatorname{car} K = 3$, la segunda ecuación nos da que $s = 0, -1$, la primera que $u = \pm 1$, la sexta nos da que $r \in K$ y la tercera que $t \in K$, con lo que llegamos a la misma conclusión.

Si $\operatorname{car} K \neq 2, 3$, las dos últimas ecuaciones nos dan que u^4, $u^6 \in K$, luego $u^2 \in K$. La quinta nos da que $r \in K$, la primera que $s \in K$ y la tercera que $t \in K$, y concluimos igualmente. ∎

[4]Teorema 5.20 de mi libro de Geometría algebraica o, alternativamente, por el teorema 7.18 de mi libro de Teoría de números, cuya prueba es mucho más simple.

Teorema 12.14 *Una curva elíptica E/K definida sobre un cuerpo métrico discreto y completo es isomorfa a una curva de Tate si y sólo si tiene reducción multiplicativa racional.*

DEMOSTRACIÓN: Sabemos que las curvas elípticas con reducción multiplicativa cumplen la condición $|j(E)| > 1$, luego, en el caso en que $\operatorname{car} K \neq 2, 3$, el teorema 12.12 prueba que E/K es isomorfa a una (única) curva de Tate. Ahora vamos a dar un argumento alternativo que es válido en cualquier característica:

Según el algoritmo de Tate, una curva elíptica con reducción multiplicativa racional (es decir, una curva de tipo $\mathrm{I_n}$, con $n \geq 1$) admite una ecuación de Weierstrass minimal tal que $v(a_3), v(a_4), v(a_6) \geq 1$ y $v(b_2) = v(a_1^2 + 4a_2) \neq 0$. Además, el polinomio $T^2 + \bar{a}_1 T + \bar{a}_2$ tiene raíces simples en el cuerpo de restos k.

Si $\operatorname{car} k \neq 2$, tomamos $t \in K$ tal que $a_2 + 2t = 0$ y el cambio de variables correspondiente (según el teorema 4.23) nos transforma la ecuación en otra que cumple las mismas condiciones anteriores y además $a_3 = 0$.

Si $\operatorname{car} k = 2$, entonces $v(a_1) = 0$, luego podemos tomar un $r \in K$ entero tal que $a_3 + ra_1 = 0$, con lo que el cambio de variables correspondiente nos da igualmente $a_3 = 0$ y se siguen cumpliendo todas las condiciones indicadas.

Ahora aplicamos el lema de Hensel (véase el final de la prueba de 12.12), según el cual existe un $s \in K$ entero tal que $s^2 + a_1 s - a_2 = 0$, con lo que el cambio correspondiente nos da una ecuación de Weierstrass en las condiciones del teorema anterior, el cual nos da la conclusión. ∎

Observemos ahora que las curvas con reducción multiplicativa no son las únicas que cumplen $|j(E)| > 1$. Por ejemplo, si $\operatorname{car} k > 3$, el teorema 9.1 muestra que las curvas que cumplen $|j(E)| > 1$ son exactamente las que tienen reducción de tipo $\mathrm{I_n}$, $\mathrm{I_{n,2}}$, $\mathrm{I_n^*}$ o $\mathrm{I_{n,2}^*}$, para $n \geq 1$, que cumplen, más concretamente, $v(j(E)) = -n$.

Más aún, si $\operatorname{car} k = 3$, sigue siendo cierto que en estos cuatro casos se cumple $v(j(E)) = -n$, pues en las condiciones del paso 2 del algoritmo de Tate tenemos que $v(b_2) = v(c_4) = 0$, luego $v(j(E)) = -v(\Delta) = -n$, y en las condiciones del paso 7 tenemos que $v(b_2) = 1$, $v(c_4) = 2$ y $v(j(E)) = 6 - v(\Delta) = -n$.

Definición 12.15 Sea K un cuerpo métrico discreto y completo. Diremos que una curva elíptica E/K tiene *potencialmente buena reducción* (resp. *potencialmente reducción multiplicativa*) si existe una extensión finita L/K tal que E_L/L tiene buena reducción (resp. reducción multiplicativa).

El teorema siguiente, que es una consecuencia inmediata de 12.11, muestra que las curvas E/K que cumplen $|j(E)| > 1$ son precisamente las curvas con reducción multiplicativa potencial:

Teorema 12.16 *Sea E/K una curva elíptica sobre un cuerpo métrico discreto y completo tal que $|j(E)| > 1$. Sea E_q/K la única curva de Tate que cumple $j(E_q) = j(E)$. Entonces existe una extensión cuadrática L/K de manera que $E_L/L \cong E_q/L$. (Y, en particular, E_L/L tiene reducción multiplicativa racional.)*

Conviene observar que, de acuerdo con la demostración de 12.11, en el caso en que $\operatorname{car} K \neq 2, 3$, la extensión necesaria es $L = K(\sqrt{\gamma(E/K)})$.

Aunque no tiene que ver con curvas de Tate, probamos a continuación un teorema análogo para el caso de buena reducción potencial, que es esencialmente [CE 6.13] y [CE 6.14], pero añadiremos una precisión que necesitaremos en el capítulo siguiente.

Teorema 12.17 *Sea E/K una curva elíptica sobre un cuerpo métrico discreto y completo de característica 0 tal que $|j(E)| \leq 1$. Entonces existe una extensión L/K de grado $|L : K| \mid 24$ tal que la curva E_L/L tiene buena reducción. Si la característica del cuerpo de restos es $\neq 2$, la cota sobre el grado puede rebajarse a 12.*

Demostración: Recordemos ([CE 2.15]) que, para cada $\lambda \in \bar{K}$, $\lambda \neq 0, 1$, la *curva de Legendre* asociada a λ es la curva elíptica E_λ de ecuación

$$Y^2 = X(X-1)(X-\lambda),$$

cuyo discriminante es $\Delta = 16\lambda^2(\lambda-1)^2$ y su invariante es

$$j(E_\lambda) = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}.$$

Supongamos que el cuerpo de restos k cumple $\operatorname{car} k \neq 2$ y tomemos como λ una solución de la ecuación

$$2^8(\lambda^2-\lambda+1)^3 - j(E)\lambda^2(\lambda-1)^2 = 0.$$

Claramente, $\lambda \neq 0, 1$, por lo que podemos considerar la curva E_λ, definida sobre el cuerpo $L_0 = K(\lambda)$. Sea L/L_0 una extensión arbitraria. Como $j(E)$ es entero en K y 2^8 es una unidad, es claro que λ es entero en L, luego la ecuación que define a E_λ tiene coeficientes enteros. Por otra parte, λ cumple también la reducción de la ecuación, de donde se sigue que $\bar{\lambda} \neq 0, 1$, luego $\bar{\Delta} \neq 0$, luego E_λ tiene buena reducción en L.

En principio, $|L_0 : K| \mid 6$ y, si $j(E) \neq 0, 1728$, el teorema 12.11 nos da una extensión L/L_0 de grado 2 (o tal vez 1) tal que $E_L/L \cong E_\lambda$. Así pues, tenemos que $|L : K| \mid 12$ y E_L/L tiene buena reducción.

Si $j(E) = 0$, la ecuación que determina λ se reduce a $\lambda^2 - \lambda + 1 = 0$, luego $|L_0 : K| \mid 2$, y la prueba del teorema [CE 2.9] muestra que podemos tomar una extensión L/L_0 de grado $|L : L_0| \mid 6$ tal que $E_L/L \cong E_\lambda$. Nuevamente, $|L : K| \mid 12$.

Si $j(E) = 1728$, entonces $\lambda = -1, 1/2, 2 \in K$, luego $L_0 = K$ y la prueba de [CE 2.9] nos muestra que podemos tomar $|L : K| \mid 4$.

Si la característica del cuerpo de restos es 2, razonamos igualmente con las *curvas de Deuring* ([CE 2.17]) D_α, definidas por ecuaciones de la forma $Y^2 + \alpha XY + Y = X^3$, y que cumplen

$$\Delta = \alpha^3 - 27, \qquad j = \frac{\alpha^3(\alpha^3-24)^3}{\alpha^3-27}.$$

Para $j(E) \neq 0, 1728$ tenemos que $|L_0 : K| \mid 12$ y $|L : L_0| \mid 2$.

Si $j(E) = 0$ podemos tomar $\alpha = 0$, con lo que $L_0 = K$ y $|L : L_0| \mid 6$.

Si $j(E) = 1728$, entonces $|L_0 : K| \mid 6$, $|L : L_0| \mid 4$ (porque la ecuación se reduce a $\alpha^6 - 36\alpha^3 + 216$). ∎

Recapitulando, tenemos lo siguiente:

Teorema 12.18 *Sea K un cuerpo métrico discreto y completo y sea E/K una curva elíptica.*

a) E/K tiene potencialmente buena reducción si y sólo si $|j(E)| \leq 1$.

b) E/K tiene potencialmente reducción multiplicativa si y sólo si $|j(E)| > 1$.

c) Si E/K tiene reducción buena o multiplicativa, tiene el mismo tipo de reducción en cualquier extensión de K.

Demostración: El apartado c) lo hemos probado en la sección 9.8. Notemos que al analizar las reducciones de tipo $\mathrm{I_n}$ o $\mathrm{I_{n,2}}$ no hemos usado la hipótesis de que el grado de ramificación de la extensión no sea divisible entre la característica del cuerpo de restos.

Los dos teoremas anteriores[5] nos dan una implicación de a) y b), respectivamente y, como los casos son mutuamente excluyentes (por el apartado c), tenemos también las implicaciones opuestas. ∎

En las condiciones del teorema 12.16, el isomorfismo $E_q/L \cong E_L/L$ induce isomorfismos

$$L^*/q^{\mathbb{Z}} \cong E_q(L) \cong E(L).$$

Podemos describir $E(K)$ a través de este isomorfismo:

Teorema 12.19 *Sea E/K una curva elíptica definida sobre un cuerpo métrico discreto y completo K de modo que $|j(E)| > 1$, sea $q \in K$ tal que $j(E_q) = j(E)$. Supongamos que E_q y E no son isomorfas sobre K, y sea L/K una extensión cuadrática tal que $E_q/L \cong E_L/L$. Entonces*

$$E(K) \cong \{u \in L^*/q^{\mathbb{Z}} \mid \mathrm{N}_K^L(u) \in q^{\mathbb{Z}}/q^{2\mathbb{Z}}\}.$$

Demostración: La norma es un homomorfismo $\mathrm{N}_K^L : L^* \longrightarrow K^*$ y, como $q \in K$, se cumple que $\mathrm{N}_K^L(q) = q^2$, luego la norma induce un homomorfismo $\mathrm{N}_K^L : L^*/q^{\mathbb{Z}} \longrightarrow K^*/q^{2\mathbb{Z}}$.

Tomemos un isomorfismo $\psi : E_q \longrightarrow E_L$ y sea $\sigma \in G(L/K)$ el automorfismo no trivial. Observemos que σ induce un automorfismo de $\operatorname{Esp} L$ definido sobre K, el cual induce a su vez automorfismos $\bar{\sigma} : E_{qL} \longrightarrow E_{qL}$ y $\bar{\sigma} : E_L \longrightarrow E_L$. A su vez, podemos definir $\psi^\sigma : E_q \longrightarrow E_L$ mediante $\psi^\sigma = \bar{\sigma} \circ \psi \circ \bar{\sigma}^{-1}$. Se cumple

[5] Notemos que la hipótesis sobre la característica de K en el teorema anterior sólo la hemos usado para acotar el grado de la extensión, pero no es necesaria para asegurar la buena reducción potencial.

que $\psi = \psi^\sigma$ si y sólo si ψ está definido[6] sobre K. Por consiguiente, podemos afirmar que $\psi^\sigma \neq \psi$. Por consiguiente, $\psi^\sigma \circ \psi^{-1}$ es un automorfismo no trivial de E_q.

Ahora bien, según [CE 2.12], la curva E_q tiene sólo dos automorfismos, y el que no es la identidad ha de ser el automorfismo que determina el punto opuesto en la estructura de variedad abeliana. Así pues, para cada $P \in E_q(L)$, se cumple que $\psi^{-1}(\psi^\sigma(P)) = -P$, o también $\psi^\sigma(P) = -\psi(P)$, donde hemos usado que ψ es un isomorfismo de grupos.

Por otra parte, se cumple[7] que $\psi^\sigma(P) = \psi(P^\sigma)^{\sigma^{-1}}$, donde los exponentes del segundo miembro corresponden a la acción natural de σ sobre $E_q(L)$ y $E(L)$. Así pues, $\psi(P^\sigma) = -\psi(P)^\sigma$, donde hemos usado que el automorfismo asociado al opuesto de la estructura de variedad abeliana de E_L/L está definido sobre K.

Por último, teniendo en cuenta que $q \in K$, el teorema 12.7 nos da que el isomorfismo $\phi : L^*/q^{\mathbb{Z}} \longrightarrow E_q(L)$ cumple $\phi(u^\sigma) = \phi(u)^\sigma$.

Uniendo todo esto vemos que, para todo $u \in L^*$, se cumple

$$\psi(\phi(u)) \in E(K) \Leftrightarrow \psi(\phi(u))^\sigma = \psi(\phi(u)) \Leftrightarrow -\psi(\phi(u)^\sigma) = \psi(\phi(u))$$

$$\Leftrightarrow \psi(-\phi(u^\sigma)) = \psi(\phi(u)) \Leftrightarrow \phi((u^\sigma)^{-1}) = \phi(u) \Leftrightarrow uu^\sigma \in q^{\mathbb{Z}} \Leftrightarrow \mathrm{N}_K^L(u) \in q^{\mathbb{Z}}.$$

La conclusión es ahora inmediata. ∎

[6] Obviamente, esto puede enunciarse en un contexto mucho más general (véase [CE 1.9] para la versión clásica). En términos de esquemas, tomando los abiertos finitos de ambas curvas, se trata de probar que un isomorfismo de L-álgebras $\psi : A \otimes_K L \longrightarrow B \otimes_K L$ tal que $\psi(x^\sigma) = \psi(x)^\sigma$ para todo $x \in A \otimes_K L$, está inducido por un isomorfismo de K-álgebras $A \longrightarrow B$. A su vez, basta ver que $\psi(a \otimes 1) \in B \otimes 1$ para todo $a \in A$. En el caso cuadrático la prueba es muy simple: si $1, \alpha$ es una K-base de L y $\sigma(\alpha) = u + v\alpha$, con $u, v \in K$, entonces $\psi(a \otimes 1) = b \otimes 1 + c \otimes \alpha$ cumple $\psi(a \otimes 1) = \psi(a \otimes 1)^\sigma$, es decir, $b \otimes 1 + c \otimes \alpha = b \otimes 1 + cu \otimes 1 + cv \otimes \alpha$, lo que implica claramente $c = 0$.

[7] Esto se debe a que, a través del isomorfismo natural $K[X, Y] \otimes_K L \cong L[X, Y]$, el automorfismo inducido por σ cumple $\sigma(X - a) = X - \sigma(a)$, luego el automorfismo que σ induce sobre la K-álgebra $K[x, y]$ asociada al abierto afín de los puntos finitos de E/L hace corresponder cada punto racional $(x - a, y - b)$ con $(x - \sigma(a), y - \sigma(b))$.

Capítulo XIII

Subgrupos de torsión

Si E/K es una curva elíptica y $m \geq 1$ un número natural, llamamos

$$E[m] = \{P \in E(\bar{K}) \mid mP = O\}$$

al subgrupo de $E(\bar{K})$ formado por los puntos de torsión de orden divisible entre m. Según las observaciones tras la definición [CE 3.9], si m no divide a la característica de K, se cumple que $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.

Cada $\sigma \in G(\bar{K}/K)$ induce un automorfismo de grupos $\sigma : E(\bar{K}) \longrightarrow E(\bar{K})$ que se restringe a un automorfismo $E[m] \longrightarrow E[m]$. Más precisamente, tenemos un homomorfismo de grupos $\rho_m : G(\bar{K}/K) \longrightarrow \mathrm{Aut}(E[m])$.

En este capítulo estudiaremos la relación entre estos homomorfismos ρ_m y el tipo de reducción de E/K, bajo el supuesto de que K es un cuerpo métrico discreto completo. Antes vamos a observar que los resultados que obtengamos se podrán aplicar al estudio de las curvas elípticas definidas sobre cuerpos numéricos (es decir, extensiones finitas de $\mathbb{Q}$).

Si K es un cuerpo numérico, E/K es una curva elíptica y $\mathfrak{p}$ es un ideal primo del anillo D de los enteros algebraicos de K, entonces el tipo de reducción de E sobre $\mathfrak{p}$, es decir, la fibra correspondiente a $\mathfrak{p}$ en el modelo regular minimal $\mathcal{E}/S$ de E/K sobre $S = \mathrm{Esp}\, D$, es el mismo que el tipo de reducción de E/K sobre $\mathrm{Esp}\, D_\mathfrak{p}$, puesto que el modelo regular minimal correspondiente es la superficie $\mathcal{E} \times_S \mathrm{Esp}\, D_\mathfrak{p}$, que tiene la misma fibra cerrada. Así pues, a efectos de estudiar el tipo de reducción de E/K módulo $\mathfrak{p}$, no perdemos generalidad si suponemos que D es un anillo de valoración discreta.

Sea ahora $K_\mathfrak{p}$ la compleción de K respecto de la valoración $v_\mathfrak{p}$ y sea $D_\mathfrak{p}$ su anillo de enteros. Tenemos que $K_\mathfrak{p}$ un cuerpo métrico discreto y completo y la curva $E_{K_\mathfrak{p}}/K_\mathfrak{p}$ tiene el mismo tipo de reducción que E/K. Esto es consecuencia de los dos hechos siguientes:

a) La valoración $v_\mathfrak{p}$ de $K_\mathfrak{p}$ extiende a la valoración de K asociada a $\mathfrak{p}$.

b) El cuerpo de restos $D_\mathfrak{p}/\mathfrak{p}$ coincide con $D/\mathfrak{p}$. (Esto hace que, además de conservarse el tipo de reducción se conserve también el subtipo.)

En efecto, basta considerar el algoritmo de Tate: fijamos una ecuación de Weierstrass minimal de E/K que cumpla las condiciones de uno de los pasos del algoritmo, y observamos que dichas condiciones se siguen cumpliendo si consideramos la ecuación como asociada a $E_{K_\mathfrak{p}}$, pues sólo dependen del valor que toma $v_\mathfrak{p}$ sobre las constantes asociadas a la ecuación y de la existencia de raíces en el cuerpo de restos k o en su clausura algebraica $\bar{k}$ de ciertos polinomios derivados también de la ecuación.

No está de más señalar que, al pasar de la curva E/K a su compleción $E_{K_\mathfrak{p}}/K_\mathfrak{p}$, no se alteran los grupos $E[m]$, pues claramente $E[m] \subset E_{K_\mathfrak{p}}[m]$ y ambos grupos tienen m^2 elementos, luego son iguales.

Por otra parte, aunque no vamos a necesitar este hecho, es fácil ver que la restricción determina un monomorfismo $G(\bar{K}_\mathfrak{p}/K_\mathfrak{p}) \longrightarrow G(\bar{K}/K)$, de modo que los homomorfismos locales $\rho_m : G(\bar{K}_\mathfrak{p}/K_\mathfrak{p}) \longrightarrow \mathrm{Aut}(E[m])$ para cada primo $\mathfrak{p}$ son restricciones del homomorfismo global $\rho_m : G(\bar{K}/K) \longrightarrow \mathrm{Aut}(E[m])$, que, de este modo, contiene toda la información local que extraeremos en las secciones siguientes.

De este modo, el caso principal al que pretendemos aplicar los resultados de este capítulo es el caso de las curvas elípticas E/K definidas sobre un *cuerpo local* K, es decir, sobre una extensión finita de un cuerpo $\mathbb{Q}_p$ de números p-ádicos (o, lo que es lo mismo, la compleción de un cuerpo numérico respecto de uno de sus divisores primos no arquimedianos). Se trata, pues, de cuerpos métricos discretos y completos de característica 0 con cuerpo de restos finito. No obstante, veremos que nos conviene trabajar en un contexto ligeramente más general:

NOTA: *A lo largo de este capítulo, y mientras no se indique lo contrario, se sobrentenderá que K es un cuerpo métrico discreto y completo de característica 0 cuyo cuerpo de restos es perfecto de característica p.*

13.1 Preliminares sobre cuerpos métricos

Necesitamos recordar algunos hechos sobre la aritmética de los cuerpos métricos discretos y completos.[1] Tal y como ya hemos recordado al principio de la sección 9.8, si K'/K es una extensión de grado n, entonces K' es también un cuerpo métrico discreto y completo, y su valoración cumple la relación $v_{K'}|_K = ev_K$, para cierto $e \geq 1$ llamado índice de ramificación de K'/K. La extensión de cuerpos de restos k'/k es finita, y su grado f se llama grado de inercia de K'/K. Además, se cumple la relación $n = ef$.

Recordemos que cada valor absoluto de K se extiende de forma única[2] a K', para cada extensión finita K'/K, luego podemos extenderlo a toda la clausura

[1] Todos los hechos que no demostraremos aquí están probados en mi libro de Teoría de cuerpos de clases, en lo sucesivo [CC], si bien figuran allí como requisitos previos, y no dependen de la teoría de cuerpos de clases propiamente dicha.

[2] En [CC] se prueban resultados más generales. Una prueba particularizada al caso local está en [GA 5.27].

algebraica $\bar{K}$ y, en particular, a cualquier extensión algebraica de K (que se convierte así en un cuerpo métrico, no necesariamente discreto ni completo).

Si la extensión K'/K es finita de Galois, la unicidad de la extensión implica que cada $\sigma \in G(K'/K)$ conserva el valor absoluto, luego cumple $\sigma[E'] = E'$ y $\sigma[\mathfrak{p}'] = \mathfrak{p}'$, por lo que induce un k-automorfismo $\bar{\sigma} \in G(k'/k)$. Como k es perfecto, la extensión k'/k es separable y por [CC 1.39] es de Galois, y además tenemos un epimorfismo de grupos[3]

$$G(K'/K) \longrightarrow G(k'/k).$$

El núcleo de este epimorfismo se llama *grupo de inercia* de la extensión, y es claramente

$$G_0(K'/K) = \{\sigma \in G(K'/K) \mid v(\sigma(\alpha) - \alpha) \geq 1 \text{ para todo } \alpha \in D'\}.$$

En particular, vemos que $|G_0(K'/K)| = e$.

Las extensiones que cumplen $e = 1$ se llaman no ramificadas, y el teorema [CC 2.36] nos da sus propiedades fundamentales: Las extensiones no ramificadas son finitas de Galois,[4] y el epimorfismo natural $G(K'/K) \longrightarrow G(k'/k)$ es un isomorfismo. Más aún, la aplicación $K' \mapsto k'$ biyecta las extensiones finitas no ramificadas de K con las extensiones finitas de k.

Hay que precisar en qué consiste esta biyección. Si L/K es una extensión algebraica, el valor absoluto de K se extiende a L de forma única, por lo que podemos considerar igualmente su anillo de enteros

$$E = \{\alpha \in K \mid |\alpha| \leq 1\},$$

que es un anillo local con un único ideal maximal $\mathfrak{m}$ (no necesariamente finitamente generado) y que no es sino el anillo de los elementos de L enteros sobre D. Si consideramos, en particular una clausura algebraica $\bar{K}$ de K, entonces $\bar{k} = E/\mathfrak{m}$ resulta ser[5] una clausura algebraica de k, y, para cada extensión algebraica L/K, tenemos un monomorfismo natural $E/\mathfrak{m} \longrightarrow \bar{k}$, de modo que podemos considerar a todos los cuerpos de restos de todas las extensiones algebraicas de K como subcuerpos de $\bar{k}$. Es en este sentido en el que podemos afirmar que la aplicación $K' \mapsto k'$ biyecta las extensiones no ramificadas de K con las extensiones finitas de k.

Todavía podemos precisar esto un poco más: Según [CC 2.35], el producto de extensiones no ramificadas es una extensión no ramificada, y las extensiones intermedias de una extensión no ramificada son no ramificadas. Por lo tanto, si llamamos K_{nr} a la unión de todas las extensiones finitas de K no ramificadas,

[3] El grupo de descomposición $G_{\mathfrak{P}}$ que aparece en [CC 1.39] es todo $G(K'/K)$ en el caso local, porque K' sólo tiene un ideal primo.

[4] Notemos que [CC 2.36] está enunciado en un contexto más general. En nuestro caso, hemos de tener en cuenta que K es separable y que todas las extensiones finitas de k son de Galois.

[5] Véanse las observaciones previas a [CC 2.32].

tenemos que K_{nr}/K es una extensión infinita de Galois y que una extensión finita K'/K es no ramificada si y sólo si $K' \subset K_{\mathrm{nr}}$.

Esto nos permite definir llamar *extensiones no ramificadas* de K a todos los cuerpos intermedios (finitos o no) de la extensión K_{nr}/K. Para el caso de extensiones finitas, esta definición coincide con la que ya teníamos.

Observemos que, si K'/K es una extensión finita, la valoración de K' no extiende a la de K en sentido estricto (extiende a ev_K), pero sí lo hace si la extensión es no ramificada. Por consiguiente, es claro que la valoración de K se extiende de forma única a una valoración en K_{nr}, luego K_{nr} es también un cuerpo métrico discreto (lo cual no es cierto para extensiones algebraicas arbitrarias). En particular, su anillo de enteros D_{nr} es un anillo de valoración discreta, y su cuerpo de restos es la unión de todas las extensiones finitas de k, luego es $\bar{k}$, la clausura algebraica de k (que coincide con la clausura algebraica del cuerpo de p elementos).

El cuerpo K_{nr} no es completo, pero podemos formar su compleción $\hat{K}_{\mathrm{nr}}$, que es un cuerpo métrico discreto y completo con el mismo cuerpo de restos $\bar{k}$. Como $\bar{k}$ es algebraicamente cerrado, resulta que $\hat{K}_{\mathrm{nr}}$ no tiene extensiones no ramificadas. Veamos algunos hechos básicos:

Teorema 13.1 *Si K'/K es una extensión finita, entonces*

$$K'_{\mathrm{nr}} = K'K_{\mathrm{nr}}, \quad \hat{K}'_{\mathrm{nr}} = K'\hat{K}_{\mathrm{nr}} \quad y \quad |K'_{\mathrm{nr}} : K_{\mathrm{nr}}| = |\hat{K}'_{\mathrm{nr}} : \hat{K}_{\mathrm{nr}}| = e.$$

Si la extensión K'/K es de Galois, entonces $K'_{\mathrm{nr}}/K_{\mathrm{nr}}$ y $\hat{K}'_{\mathrm{nr}}/\hat{K}_{\mathrm{nr}}$ también lo son, y la restricción induce isomorfismos

$$G(\hat{K}'_{\mathrm{nr}}/\hat{K}_{\mathrm{nr}}) \cong G(K'_{\mathrm{nr}}/K_{\mathrm{nr}}) \cong G_0(K'/K).$$

Demostración: Si L/K es una extensión finita no ramificada, entonces $K'L/K'$ también lo es (por [CC 2.35]), luego $K'L \subset K'_{\mathrm{nr}}$ y esto prueba que $K'K_{\mathrm{nr}} \subset K'_{\mathrm{nr}}$. Recíprocamente, si L'/K' es una extensión no ramificada, consideramos la única extensión no ramificada L/K tal que el cuerpo de restos de L es el de L'. Entonces $K'L/K'$ es una extensión no ramificada (de nuevo por [CC 2.35]) y su cuerpo de restos contiene al de L', luego [CC 2.36] nos da que $K' \subset L' \subset K'L$, pero la segunda extensión cumple $e = f = 1$, luego $L' = K'L \subset K'K_{\mathrm{nr}}$ y, por consiguiente, $K'_{\mathrm{nr}} = K'K_{\mathrm{nr}}$.

La igualdad $\hat{K}'_{\mathrm{nr}} = K'\hat{K}_{\mathrm{nr}}$ se sigue de que el miembro derecho es un cuerpo métrico completo que contiene a K'_{nr} como subconjunto denso, luego es la compleción de K'_{nr}.

Si e es índice de ramificación de $K'_{\mathrm{nr}}/K_{\mathrm{nr}}$, tenemos que $v_{K'_{\mathrm{nr}}}|_{K_{\mathrm{nr}}} = ev_{K_{\mathrm{nr}}}$, y restringiendo esta relación a K, vemos que e es también el índice de ramificación de K'/K. Como el grado de inercia de $K'_{\mathrm{nr}}/K_{\mathrm{nr}}$ ha de ser $f = 1$, concluimos que $|K'_{\mathrm{nr}} : K_{\mathrm{nr}}| = e$. El mismo argumento se aplica a las compleciones.

Si K'/K es de Galois, es claro que $K'K_{\rm nr}/K_{\rm nr}$ también lo es, y esto implica a su vez que $K'\hat{K}_{\rm nr}/K_{\rm nr}$ también lo es. Es claro que la restricción induce monomorfismos entre los grupos de Galois

$$G(\hat{K}'_{\rm nr}/\hat{K}_{\rm nr}) \longrightarrow G(K'_{\rm nr}/K_{\rm nr}) = G_0(K'_{\rm nr}/K_{\rm nr}) \longrightarrow G_0(K'/K).$$

Como todos los grupos tienen el mismo orden, son isomorfismos. ∎

Para cada extensión finita no ramificada K'/K, tenemos un isomorfismo natural $G(K'/K) \cong G(k'/k)$ (pues el grupo de inercia tiene orden $e = 1$). Estos isomorfismos inducen claramente un isomorfismo $G(K_{\rm nr}/K) \cong G(\bar{k}/k)$.

Definimos el *grupo de inercia (absoluto)* de K como el grupo $I_K = G(\bar{K}/K_{\rm nr})$, de modo que $G(K_{\rm nr}/K) \cong G(\bar{K}/K)/I_K$, y el isomorfismo anterior está inducido por el homomorfismo natural $G(\bar{K}/K) \longrightarrow G(\bar{k}/k)$, que resulta, por tanto, ser un epimorfismo de núcleo I_K.

Más aún, es claro que una extensión algebraica L/K es no ramificada si y sólo si $I_K \subset G(\bar{K}/L)$, es decir, si y sólo si el grupo de inercia I_K actúa trivialmente sobre L. La relación entre el grupo de inercia absoluto y los grupos de inercia de extensiones finitas es la siguiente:

Teorema 13.2 *Si K'/K es una extensión finita de Galois, entonces*

$$G_0(K'/K) = G(K'/K' \cap K_{\rm nr}) \cong I_K/I_{K'}.$$

Demostración: Sea L/K la extensión no ramificada cuyo cuerpo de restos sea el de K'. Según [CC 2.36] tenemos que $K \subset L \subset K'$, y es claro que L ha de ser la mayor extensión no ramificada de K contenida en K', es decir, que $L = K' \cap K_{\rm nr}$. Obviamente, es una extensión de Galois de K. Además, $|L : K| = f$ luego $|K' : L| = e$. (Aquí e y f son los correspondientes a la extensión de partida.) Tenemos un diagrama conmutativo

$$\begin{array}{ccc} G(K'/K) & \longrightarrow & G(k'/k) \\ \downarrow & \nearrow & \\ G(L/K) & & \end{array}$$

luego la restricción se restringe a $G_0(K'/K) \longrightarrow G_0(L/K) = 1$, luego

$$G_0(K'/K) \subset G(K'/L)$$

y ambos grupos tienen orden e, luego tenemos la primera igualdad del enunciado: $G_0(K'/K) = G(K'/K' \cap K_{\rm nr})$. Para la segunda basta observar que la restricción

$$I_K = G(\bar{K}/K_{\rm nr}) \longrightarrow G(K'K_{\rm nr}/K_{\rm nr}) \longrightarrow G(K'/(K' \cap K_{\rm nr})) = G_0(K'/K)$$

es claramente suprayectiva, y su núcleo es

$$G(\bar{K}/K_{\rm nr}) \cap G(\bar{K}/K') = G(\bar{K}/K'K_{\rm nr}) = G(\bar{K}/K'_{\rm nr}) = I_{K'}.$$

∎

Recordemos que una extensión finita K'/K de cuerpos métricos discretos se dice *dominadamente ramificada* si su índice de ramificación e no es divisible entre la característica p del cuerpo de restos. En caso contrario se dice que es *libremente ramificada.* En particular, las extensiones no ramificadas son dominadamente ramificadas. Es inmediato que si una extensión K'/K es dominadamente ramificada, también lo son las extensiones $K'_{\rm nr}/K_{\rm nr}$ y $\hat{K}'_{\rm nr}/\hat{K}_{\rm nr}$.

Teorema 13.3 *Si el cuerpo de restos k es algebraicamente cerrado, para cada número natural e no divisible entre* $\operatorname{car} k$*, existe una única extensión dominadamente ramificada K'/K de grado e. Además, la extensión es de Galois y el grupo $G(K'/K)$ es cíclico.*

Demostración: Si K'/K es una extensión dominadamente ramificada, el teorema [CE 2.44] nos da que $K' = K(\pi)$, donde π es raíz de un polinomio de la forma $X^n - \rho$, donde $n = e$ es el grado de la extensión.

Sea ω una raíz n-sima primitiva de la unidad y consideremos la extensión $K' = K(\omega)$. El teorema [CC 3.13] nos da que el diferente de K'/K divide a $n\omega^{n-1}$, luego el teorema [CC 3.22] nos da que el discriminante divide a $\mathrm{N}(n\omega^{n-1}) = n^n$, luego el primo de K no divide al discriminante y, según [CC 3.23], esto implica que la extensión K'/K es no ramificada. Esto sólo es posible si $K' = K$, de modo que K contiene a las raíces n-simas de la unidad. Por consiguiente, K' contiene a todos los conjugados de π y la extensión K'/K es de Galois.

Como la extensión K'/K tiene grado n, el polinomio $X^n - \rho$ ha de ser irreducible, luego todos los elementos de la forma $\omega^i\pi$ han de ser conjugados de π. Por consiguiente, para cada $i \in \mathbb{Z}$ existe un único $\sigma_i \in G(K'/K)$ tal que $\sigma_i(\rho) = \omega^i\rho$, y la aplicación $i \mapsto \sigma_i$ induce un isomorfismo de grupos $\mathbb{Z}/n\mathbb{Z} \longrightarrow G(K'/K)$. Así pues, la extensión es cíclica.

Por último, si K' y L son dos extensiones de K dominadamente ramificadas y de grado n, el teorema [CC 2.45] nos da que $K'L/K$ también es dominadamente ramificada, luego $G(K'L/K)$ es cíclico, luego tiene un único subgrupo H de índice n, luego K' y L son ambos iguales al cuerpo fijado por H.

Para probar la existencia basta tomar $K' = K(\sqrt[n]{\pi})$, donde π es primo en (el anillo de enteros de) K. El criterio de irreducibilidad de Eisenstein prueba que el polinomio $X^n - \pi$ es irreducible en $K[X]$, luego la extensión K'/K tiene grado n, por lo que es dominadamente ramificada. ∎

Decíamos al principio del capítulo que, dada una curva elíptica E/K, nuestro objetivo era relacionar los homomorfismos

$$\rho_m : G(\bar{K}/K) \longrightarrow \mathrm{Aut}(E[m])$$

con el tipo de reducción de E/K. Ahora podemos precisar esto un poco más. En realidad vamos a relacionar el tipo de reducción de E/K con la acción del grupo de inercia I_K sobre los grupos de torsión, es decir, con las restricciones $\rho_m : I_K \longrightarrow \mathrm{Aut}(E[m])$. Veamos ahora que, con este fin, no perdemos generalidad si suponemos que el cuerpo de restos k es algebraicamente cerrado.

En efecto, dada una curva elíptica E/K, consideramos el cuerpo K_{nr}, que es un cuerpo métrico discreto. Aunque no es completo, es el cuerpo de cocientes de su anillo de enteros, D_{nr}, que es un anillo de valoración discreta, cuyo cuerpo de restos es $\bar{k}$, la clausura algebraica del cuerpo de restos de K.

Por consiguiente, podemos considerar la reducción de $E_{K_{\mathrm{nr}}}/K_{\mathrm{nr}}$, que resulta ser del mismo tipo (aunque no necesariamente del mismo subtipo) que la de E/K. En efecto, basta tener el cuenta que la valoración de K_{nr} extiende a la de K y razonar con el algoritmo de Tate exactamente igual a como hemos hecho en la introducción a este capítulo:

Tomamos una ecuación de Weierstrass minimal de E/K que satisfaga las condiciones de uno de los pasos del algoritmo, y vemos que sigue cumpliéndolas como ecuación de $E_{K_{\mathrm{nr}}}/K_{\mathrm{nr}}$, pues éstas sólo dependen del valor que toma la valoración v sobre las constantes asociadas a la ecuación, y sobre la multiplicidad de las raíces en $\bar{k}$ de ciertos polinomios derivados también de ella. Lo que puede variar es el subtipo de la reducción, pues el subtipo es 2 o 3 cuando ciertos polinomios de $k[X]$ no tienen todas sus raíces en k, cosa que ya no sucede cuando cambiamos k por $\bar{k}$. Así pues, si el tipo de reducción de E/K tiene subtipo 2 o 3, sobre K_{nr} tendremos el mismo tipo de reducción pero con subtipo 1 (es decir, sin subíndice de subtipo).

Por otra parte, tenemos la igualdad $E[m] = E_{K_{\mathrm{nr}}}[m]$, pues claramente tenemos una inclusión y ambos tienen el mismo orden m^2.

Además, como K_{nr} no admite extensiones no ramificadas, tenemos que $(K_{\mathrm{nr}})_{\mathrm{nr}} = K_{\mathrm{nr}}$, luego $I_{K_{\mathrm{nr}}} = G(\bar{K}_{\mathrm{nr}}/K_{\mathrm{nr}}) = G(\bar{K}/K_{\mathrm{nr}}) = I_K$, luego la acción de $I_{K_{\mathrm{nr}}}$ sobre los grupos $E_{K_{\mathrm{nr}}}[m]$ es la misma que la de I_K sobre los grupos $E[m]$ (literalmente la misma, puesto que se trata de los mismos grupos con otros nombres).

Al cambiar K por K_{nr} hemos perdido la completitud, pero ahora podemos considerar a su vez la compleción $\hat{K}_{\mathrm{nr}}$, que resulta ser un cuerpo métrico discreto y completo con cuerpo de restos algebraicamente cerrado. Tal y como hemos razonado en la introducción a este capítulo, el tipo de reducción de $E_{K_{\mathrm{nr}}}/K_{\mathrm{nr}}$ es el mismo que el de $E_{\hat{K}_{\mathrm{nr}}}/\hat{K}_{\mathrm{nr}}$ y, obviamente, los grupos de torsión $E[m]$ siguen siendo los mismos.

Veamos ahora que $\bar{K}\hat{K}_{\mathrm{nr}}$ es una clausura algebraica de $\hat{K}_{\mathrm{nr}}$. En efecto, si $L = \hat{K}_{\mathrm{nr}}(\alpha)$ es una extensión finita de $\hat{K}_{\mathrm{nr}}$, sea $f \in \hat{K}_{\mathrm{nr}}[X]$ el polinomio mínimo de α. Por [CC 2.18], si $g \in K_{\mathrm{nr}}[X]$ es un polinomio (mónico) cuyos coeficientes estén lo suficientemente próximos a los de f, entonces g es irreducible en $\hat{K}_{\mathrm{nr}}[X]$ (luego también en $K_{\mathrm{nr}}[X]$) y, si $\beta \in \bar{K}$ es una raíz de g, se cumple que

$$L = \hat{K}_{\mathrm{nr}}(\alpha) = \hat{K}_{\mathrm{nr}}(\beta) \subset \bar{K}\hat{K}_{\mathrm{nr}}.$$

Así pues, éste último cuerpo contiene a todas las extensiones finitas de $\hat{K}_{\mathrm{nr}}$ y es una extensión algebraica de $\hat{K}_{\mathrm{nr}}$, luego es su clausura algebraica.

Ahora es fácil ver que la restricción $G(\bar{K}\hat{K}_{\mathrm{nr}}/\hat{K}_{\mathrm{nr}}) \longrightarrow G(\bar{K}/K_{\mathrm{nr}}) = I_K$ es un isomorfismo de grupos. En efecto, es inyectivo porque el valor absoluto

de $\hat{K}_{\rm nr}$ tiene extensión única a la clausura algebraica, lo cual implica que los automorfismos son continuos, y $\bar{K}$ es denso en $\bar{K}\hat{K}_{\rm nr}$ (pues su clausura contiene a $K_{\rm nr}$, luego también a la compleción $\hat{K}_{\rm nr}$).

Veamos ahora la suprayectividad: tomamos $\sigma \in G(\bar{K}/K_{\rm nr})$. Sea $L/\hat{K}_{\rm nr}$ una extensión finita. Según hemos visto, es de la forma $L = \hat{K}_{\rm nr}(\beta)$, para cierto $\beta \in \bar{K}$ cuyo polinomio mínimo en $K_{\rm nr}[X]$ es también irreducible en $\hat{K}_{\rm nr}[X]$. Esto implica que todos los conjugados de β sobre $K_{\rm nr}$ siguen siendo conjugados sobre $\hat{K}_{\rm nr}$. Por consiguiente, $\sigma|_{K_{\rm nr}(\beta)} : K_{\rm nr}(\beta) \longrightarrow \bar{K}$ se extiende de forma única a un $\hat{K}_{\rm nr}$-monomorfismo $\sigma_L : L \longrightarrow \bar{K}\hat{K}_{\rm nr}$. (Para definir $\sigma_L(\beta) = \sigma(\beta)$ necesitábamos que β y $\sigma(\beta)$ siguieran siendo conjugados sobre $\hat{K}_{\rm nr}$.)

La unicidad permite unir todas estas extensiones en un único $\hat{K}_{\rm nr}$-monomorfismo $\bar{\sigma} : \bar{K}\hat{K}_{\rm nr} \longrightarrow \bar{K}\hat{K}_{\rm nr}$ que extiende a σ y que es un automorfismo porque tiene por inverso a la extensión de σ^{-1}.

El cuerpo de restos de $\hat{K}_{\rm nr}$ sigue siendo algebraicamente cerrado, luego $\hat{K}_{\rm nr}$ no tiene extensiones no ramificadas, luego $I_{\hat{K}_{\rm nr}} = G(\bar{K}\hat{K}_{\rm nr}/\hat{K}_{\rm nr})$.

Puesto que el isomorfismo $I_{\hat{K}_{\rm nr}} \cong I_{K_{\rm nr}} \cong I_K$ es simplemente la restricción, es claro que la acción de $I_{\hat{K}_{\rm nr}}$ sobre los grupos $E[m]$ es la misma que la de I_K. Más precisamente, tenemos diagramas conmutativos:

$$\begin{array}{ccc} I_{\hat{K}_{\rm nr}} & \xrightarrow{\rho_m} & \mathrm{Aut}(E[m]) \\ \downarrow & \nearrow_{\rho_m} & \\ I_K & & \end{array}$$

que expresan que, si $P \in E[m]$, entonces P^σ es el mismo si consideramos que $\sigma \in I_{\hat{K}_{\rm nr}}$ o si lo identificamos con su restricción a $\bar{K}$.

En resumen, las curvas E/K y $E_{\hat{K}_{\rm nr}}/\hat{K}_{\rm nr}$ tienen el mismo tipo de reducción (aunque no necesariamente el mismo subtipo) y las acciones de los grupos de inercia $I_{\hat{K}_{\rm nr}} \cong I_K$ sobre los grupos $E[m]$ se corresponden a través del isomorfismo natural dado por la restricción.

13.2 Módulos de Tate

Pasamos ya a estudiar la acción del grupo de inercia I_K sobre los subgrupos de torsión $E[m]$, tal y como hemos explicado anteriormente. Empezaremos recordando la construcción de los módulos de Tate de una curva elíptica, aunque aquí vamos a necesitar estudiarlos en un contexto ligeramente más general:

Si A es un grupo abeliano y $m \geq 1$, definimos

$$A[m] = \{x \in A \mid mx = 0\}.$$

Si l es un número primo, consideramos los homomorfismos $A[l^{n+1}] \longrightarrow A[l^n]$ dados por $x \mapsto lx$, con los que podemos formar el límite inverso

$$T_l(A) = \varprojlim_n A[l^n].$$

Observemos que $A[l^n]$ tiene una estructura natural de $\mathbb{Z}/l^n\mathbb{Z}$ módulo, por lo que, considerando el anillo de los enteros l-ádicos como límite inverso

$$\mathbb{Z}_l = \varprojlim_n \mathbb{Z}/l^n\mathbb{Z}$$

(respecto de los epimorfismos $\mathbb{Z}/l^{n+1}\mathbb{Z} \longrightarrow \mathbb{Z}/l^n\mathbb{Z}$ dados por $m \mapsto lm$), podemos dotar a $T_l(A)$ de una estructura natural de $\mathbb{Z}_l$-módulo. Por último, definimos

$$V_l(A) = T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l,$$

que es un espacio vectorial sobre el cuerpo $\mathbb{Q}_l$ de los números l-ádicos.

Observemos ahora que un homomorfismo $\alpha : A \longrightarrow B$ entre grupos abelianos se restringe a homomorfismos $A[l^n] \longrightarrow B[l^n]$ compatibles con la multiplicación por l. Éstos determinan, por tanto, un homomorfismo entre sistemas inversos, el cual induce un homomorfismo de $\mathbb{Z}_l$-módulos $T_l(\alpha) : T_l(A) \longrightarrow T_l(B)$, el cual induce a su vez una aplicación $\mathbb{Q}_l$-lineal $V_l(\alpha) : V_l(A) \longrightarrow V_l(B)$. Esto significa que T_l y V_l son funtores. El teorema siguiente prueba que son exactos por la izquierda:

Teorema 13.4 *Si* $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ *es una sucesión exacta de grupos abelianos, la sucesión*

$$0 \longrightarrow T_l(A) \longrightarrow T_l(B) \longrightarrow T_l(C)$$

también es exacta. Una condición suficiente para que $T_l(\beta)$ *sea suprayectivo es que el grupo* A *sea* l*-divisible, es decir, que todo* $x \in A$ *sea de la forma* $x = ly$*, para cierto* $y \in A$*.*

Demostración: Es fácil ver que las sucesiones

$$0 \longrightarrow A[l^n] \longrightarrow B[l^n] \longrightarrow C[l^n]$$

son exactas. Si llamamos $C'[l^n] = \beta[B[l^n]] \subset C[l^n]$, tenemos sucesiones exactas

$$0 \longrightarrow A[l^n] \longrightarrow B[l^n] \longrightarrow C'[l^n] \longrightarrow 0,$$

y los grupos $C'[l^n]$ definen igualmente un sistema inverso. El teorema [AC 4.5] nos da una sucesión exacta

$$0 \longrightarrow T_l(A) \longrightarrow T_l(B) \longrightarrow \varprojlim_n C'[l^n].$$

El último módulo es un submódulo de $T_l(C)$, luego tenemos una sucesión exacta

$$0 \longrightarrow T_l(A) \longrightarrow T_l(B) \longrightarrow T_l(C),$$

donde es fácil ver que el segundo homomorfismo no es sino $T_l(\beta)$.

Supongamos ahora que A es l-divisible y veamos que la sucesión

$$0 \longrightarrow A[l^n] \longrightarrow B[l^n] \longrightarrow C[l^n] \longrightarrow 0$$

es exacta. En efecto, si $z \in C[l^n]$, existe un $y \in B$ tal que $\beta(y) = z$. Entonces $\beta(l^n y) = 0$, luego existe un $x \in A$ tal que $\alpha(x) = l^n y$. Por la divisibilidad, existe $x' \in A$ tal que $x = l^n x'$, y así $l^n(y - \alpha(x')) = 0$, luego $y' = y - \alpha(x') \in B[l^n]$ y $\beta(y') = \beta(y) = z$.

Por otra parte, la divisibilidad implica también que el límite inverso asociado a A es suprayectivo, luego [AC 4.5] implica ahora que la sucesión

$$0 \longrightarrow T_l(A) \longrightarrow T_l(B) \longrightarrow T_l(C) \longrightarrow 0$$

es exacta. ∎

Una observación elemental es que, si A es finito, entonces $T_l(A) = 0$. En efecto, la sucesión $A[l^n]$ se vuelve finalmente constante, luego un $x \in T_l(A)$ es una sucesión (x_n) en la que, para $n \geq n_0$, se cumple que $x_n \in A[l^n] = A[l^{n_0}]$, por lo que $x_n = l^{n_0} x_{n+n_0} = 0$, luego $x = 0$.

Si E/K es una curva elíptica, definimos $E[m]$, $T_l(E)$ y $V_l(E)$ como los correspondientes al grupo $E(\bar{K})$. Sabemos que $E[l^n] \cong \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$, de donde se sigue ([CE 3.21]) que[6] $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$, por lo que $V_l(E)$ es un $\mathbb{Q}_l$-espacio vectorial de dimensión 2.

Como la acción de $G(\bar{K}/K)$ respeta la multiplicación por l, es claro que induce una acción sobre $T_l(E)$ y ésta, a su vez, otra sobre $V_l(E)$. Más precisamente: tenemos un homomorfismo de grupos natural

$$\rho : G(\bar{K}/K) \longrightarrow \mathrm{Aut}_{\mathbb{Q}_p} V_l(E).$$

A continuación mostramos cómo estos homomorfismos determinan si E/K tiene reducción buena, multiplicativa o aditiva. Para ello damos la definición siguiente:

Definición 13.5 Sea E/K una curva elíptica, para cada primo $l \neq p$, llamamos $V_l(E)^{I_K}$ al subespacio vectorial de $V_l(E)$ formado por los puntos fijados por el grupo de inercia I_K. Llamaremos

$$\epsilon(E/K) = \dim_{\mathbb{Q}_l}(V_l(E)/V_l(E)^{I_K}) = 2 - \dim_{\mathbb{Q}_l} V_l(E)^{I_K}.$$

En principio, tenemos que $\epsilon(E/K)$ depende de l, pero el teorema siguiente muestra, en particular, que no es así:

Teorema 13.6 *Si E/K es una curva elíptica, se cumple que*

$$\epsilon(E/K) = \begin{cases} 0 & \text{si } E/K \text{ tiene buena reducción,} \\ 1 & \text{si } E/K \text{ tiene reducción multiplicativa,} \\ 2 & \text{si } E/K \text{ tiene reducción aditiva.} \end{cases}$$

[6] Conviene destacar que el isomorfismo no es canónico, es decir, que sólo está definido en función de la elección arbitraria de una base en $T_l(E)$.

DEMOSTRACIÓN: De las observaciones finales de la sección precedente se sigue inmediatamente que $\epsilon(E/K) = \epsilon(E_{\hat{K}_{\rm nr}}/\hat{K}_{\rm nr})$, así como que el tipo de reducción de E/K coincide con el de $E_{\hat{K}_{\rm nr}}/\hat{K}_{\rm nr}$. Por consiguiente, no perdemos generalidad si suponemos que el cuerpo de restos k es algebraicamente cerrado. En particular, tenemos entonces que $I_K = G(\bar{K}/K)$.

Consideremos las sucesiones exactas

$$0 \longrightarrow E_0(K) \longrightarrow E(K) \longrightarrow E(K)/E_0(K) \longrightarrow 0,$$

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \tilde{E}_r(k) \longrightarrow 0,$$

donde $\tilde{E}_r(k)$ es el conjunto de puntos regulares de la reducción de $\tilde{E}/k$.

Sabemos que el cociente $E(K)/E_0(K)$ es finito por 10.42, luego, según hemos visto, su módulo de Tate es nulo. Por consiguiente, la primera sucesión exacta nos da un isomorfismo $T_l(E_0(K)) \cong T_l(E(K))$ que, a su vez, induce un isomorfismo $V_l(E_0(K)) \cong V_l(E(K))$.

Por otra parte, el grupo $E_1(K)$ no tiene elementos de orden l por [CE 6.19], y esto implica obviamente que $T_l(E_1(K)) = 0$. Más aún, en la demostración del teorema [CE 6.19], teniendo a su vez en cuenta la de [CE 5.16], en la cual se basa, se ve que la multiplicación por $l \neq p$ es un isomorfismo en $E_1(K)$, por lo que se trata de un grupo divisible, y así, la segunda sucesión exacta nos proporciona un isomorfismo $T_l(E_0(K)) \cong T_l(\tilde{E}_r(k))$, que a su vez induce un isomorfismo $V_l(E_0(K)) \cong V_l(\tilde{E}_r(k))$.

Combinando ambos isomorfismos obtenemos que $V_l(E(K)) \cong V_l(\tilde{E}_r(k))$. Ahora bien, la inclusión $E(K) \subset E(\bar{K})$ induce monomorfismos

$$E(K)[l^n] \longrightarrow E[l^n],$$

que a su vez inducen un monomorfismo $T_l(E(K)) \longrightarrow T_l(E)$, que a su vez induce un monomorfismo $V_l(E(K)) \longrightarrow V_l(E)$. Puesto que $I_K = G(\bar{K}/K)$, los puntos de $E(K)[l^n]$ son los puntos de $E[l^n]$ fijados por I_K, luego $T_l(E(K))$ es el subespacio de $T_l(E)$ fijado por I_K, lo que implica claramente[7] que

$$V_l(E(K)) = V_l(E)^{I_K}.$$

En definitiva, tenemos que

$$\epsilon(E/K) = 2 - \dim_{\mathbb{Q}_l} V_l(E)^{I_K} = 2 - \dim_{\mathbb{Q}_l}(V_l(\tilde{E}_r(k))).$$

Ahora observamos que si E/K tiene buena reducción, entonces $\tilde{E}/k$ es una curva elíptica, luego $\tilde{E}_r(k) = \tilde{E}(k)$ y $V_l(\tilde{E}_r(k)) = T_l(\tilde{E}) \cong \mathbb{Q}_l^2$ (por [CE 3.21], ya que $l \neq p$). Por otra parte, la unicidad que proporcionan los teoremas 10.22 y 10.23, implica que si E/K tiene reducción multiplicativa[8], entonces $\tilde{E}_r(k) \cong k^*$ y, si la reducción es aditiva, $\tilde{E}_r(k) \cong k^+$.

[7] Un elemento de $V_l(E)$ es de la forma x/s, con $x \in T_l(E)$ y $s \in \mathbb{Z}_l$, por lo que se cumple $(x/s)^\sigma = x^\sigma/s = x/s$ si y sólo si $x^\sigma = x$, si y sólo si $x \in T_l(E(K))$, si y sólo si $s \in V_l(E(K))$.

[8] Aquí es donde usamos que k es algebraicamente cerrado: la reducción multiplicativa será necesariamente racional.

Es claro que $k^*[l^n]$ es el grupo de las raíces de la unidad de orden divisible entre p^n, luego $k^*[l^n] \cong \mathbb{Z}/l^n\mathbb{Z}$, lo que implica que $V_l(k^*) \cong \mathbb{Q}_l$. Por otra parte, usando una vez más que $l \neq p$, vemos que $k^+[l^n] = 0$, luego $V_l(k^+) = 0$. En resumen:

$$\dim_{\mathbb{Q}_l}(V_l(\tilde{E}_r(k))) = \begin{cases} 2 & \text{si } E/K \text{ tiene buena reducción,} \\ 1 & \text{si } E/K \text{ tiene reducción multiplicativa,} \\ 0 & \text{si } E/K \text{ tiene reducción aditiva,} \end{cases}$$

y esto implica inmediatamente la igualdad del enunciado. ∎

Así pues, vemos que el tipo de reducción (buena, multiplicativa o aditiva) de E/K está determinado por la acción del grupo de inercia I_K sobre $V_l(E)$. Veamos una aplicación:

Teorema 13.7 *Si $\phi : E_1 \longrightarrow E_2$ es una isogenia no nula entre dos curvas elípticas sobre K, entonces $\epsilon(E_1/K) = \epsilon(E_2/K)$, de modo que ambas curvas tienen el mismo tipo de reducción (buena, multiplicativa o aditiva) sobre K.*

Demostración: El núcleo de ϕ es un subgrupo finito de E_1. Pongamos que tiene r elementos y tomemos un primo l que no divida a r y que sea distinto de la característica del cuerpo de restos de k. Es claro que ϕ se restringe a un homomorfismo de grupos $\phi_n : E_1[l^n] \longrightarrow E_2[l^n]$. El orden del núcleo de ϕ_n ha de dividir a l^{2n} y a r, luego ha de ser trivial. Como ambos grupos tienen el mismo orden, ϕ_n es un isomorfismo.

Por otra parte, el hecho de que ϕ esté definido sobre K implica inmediatamente que es compatible con la acción de $G(\bar{K}/K)$ en ambos grupos, es decir, que para todo $\sigma \in G(\bar{K}/K)$ y todo $P \in E_1[l^n]$ se cumple que $\phi_n(P^\sigma) = \phi_n(P)^\sigma$.

Es claro entonces que los isomorfismos ϕ_n inducen un isomorfismo de módulos $T_l(E_1) \longrightarrow T_l(E_2)$, que a su vez induce un isomorfismo de espacios vectoriales $\bar{\phi} : V_l(E_1) \longrightarrow V_l(E_2)$ compatible con la acción del grupo de Galois. En particular, $\bar{\phi}[V_l(E_1)^{I_K}] = V_l(E_2)^{I_K}$, luego $\epsilon(E_1/K) = \epsilon(E_2/K)$. ∎

Más en general, si K es un cuerpo numérico, $\mathfrak{p}$ es un ideal primo de su anillo de enteros, $K_\mathfrak{p}$ es la compleción de K respecto de la valoración de $\mathfrak{p}$ y $\phi : E_1 \longrightarrow E_2$ es una isogenia no nula entre dos curvas elípticas definidas sobre K, entonces ϕ induce una isogenia no nula $\phi_{K_\mathfrak{p}} : E_{1K_\mathfrak{p}} \longrightarrow E_{2K_\mathfrak{p}}$, por lo que $\epsilon(E_1/K_\mathfrak{p}) = \epsilon(E_2/K_\mathfrak{p})$. De acuerdo con la discusión que hemos realizado en la introducción de este capítulo, esto implica que E_1 y E_2 tienen el mismo tipo de reducción respecto de cada primo de K.

13.3 El criterio de Néron-Ogg-Shafarevich

Según hemos visto en la sección anterior, una curva elíptica E/K tiene buena reducción si y sólo si $\epsilon(E/K) = 0$, si y sólo si $V_l(E)^{I_K} = V_l(E)$, si y sólo si el grupo de inercia I_K fija al espacio vectorial $V_l(E)$, para cualquier primo $l \neq p$, y esto equivale claramente a que I_K fije al módulo de Tate $T_l(E)$ para cualquier primo $l \neq p$. Esto es una parte del llamado criterio de Néron-Ogg-Shafarevich,

que nos da además otras equivalencias directamente en términos de los grupos de torsión $E[m]$:

Teorema 13.8 (Criterio de Néron–Ogg–Shafarevich) *Para toda curva elíptica E/K, las condiciones siguientes son equivalentes:*

a) E tiene buena reducción sobre K.

b) El grupo de inercia I_K actúa trivialmente sobre el módulo de Tate $T_l(E)$ para algún primo $l \neq p$ (o para todo primo $l \neq p$).

c) El grupo de inercia I_K actúa trivialmente sobre $E[m]$, para todo $m \geq 2$ primo con p.

d) El grupo de inercia I_K actúa trivialmente sobre $E[m]$, para infinitos valores de m primos con p.

DEMOSTRACIÓN: Hemos visto que a) $\Leftrightarrow$ b), y es claro que b) $\Rightarrow$ c) $\Rightarrow$ d). Veamos, pues, que d) $\Rightarrow$ a). No perdemos generalidad si suponemos que el cuerpo de restos k es algebraicamente cerrado, de modo que $I_K = G(\bar{K}/K)$.

Por el teorema 10.42 sabemos que el índice $|E(K) : E_0(K)|$ es finito. Tomemos un número natural m que cumpla las propiedades siguientes:

a) m es primo con p,

b) $m > |E(K) : E_0(K)|$,

c) I_K actúa trivialmente sobre $E[m]$.

Ahora consideramos las sucesiones exactas

$$0 \longrightarrow E_0(K) \longrightarrow E(K) \longrightarrow E(K)/E_0(K) \longrightarrow 0,$$

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow E_r(k) \longrightarrow 0.$$

Por c) tenemos que $E[m] \subset E(K)$. Sabemos que $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Para cada primo $q \mid m$, sea q^e la mayor potencia de q que divide a m. Podemos tomar un subgrupo $\langle P\rangle \times \langle Q\rangle$ de $E[m]$ de orden $q^e \times q^e$. Si tuviéramos que $q^{e-1}P \notin E_0(K)$ o $q^{e-1}Q \notin E_0(K)$ (pongamos el primer caso), entonces la primera sucesión exacta inyectaría $\langle P\rangle$ en el cociente $E(K)/E_0(K)$, con lo que el índice $|E(K) : E_0(K)|$ sería múltiplo de q^e. Por b) esto no puede ocurrir para todo primo q, luego existe un primo $q \mid m$ tal que $q^{e-1}P \in E_0(K)$ y $q^{e-1}Q \in E_0(K)$. Así pues, el grupo $E_0(K)$ contiene un subgrupo isomorfo a $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Ahora consideramos la segunda sucesión exacta. Por [CE 6.19] sabemos que $E_1(K)$ no contiene elementos de orden q, luego $E_r(k)$ contiene un subgrupo isomorfo a $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Supongamos que E tiene mala reducción sobre K. Si la reducción fuera multiplicativa (multiplicativa racional, ya que k es algebraicamente cerrado), se cumpliría que $E_r(k) \cong k^*$, pero entonces los elementos de orden q en $E_r(k)$

formarían un subgrupo isomorfo a $\mathbb{Z}/q\mathbb{Z}$ (al grupo de las raíces q-ésimas de la unidad de k). Si la reducción fuera aditiva, sería $E_r(k) \cong k$ y no habría elementos de torsión. Así pues, E ha de tener buena reducción sobre K. ∎

En principio, con este resultado hemos sustituido una condición sobre la acción del grupo de inercia sobre los módulos de Tate (o sobre uno de ellos) por una condición que afecta a infinitos grupos $E[m]$. Vamos a ver que, para curvas con buena reducción potencial, la condición puede expresarse en términos de un único grupo $E[m]$.

Teorema 13.9 *Si E/K es una curva elíptica tal que $|j(E)| \leq 1$. Entonces, las afirmaciones siguientes son equivalentes:*

a) E tiene buena reducción sobre K.

b) I_K actúa trivialmente sobre $E[m]$ para todo $m \geq 1$ primo con p.

c) I_K actúa trivialmente sobre $E[m]$, para algún $m \geq 3$ primo con p.

Demostración: Sólo hay que probar que c) ⇒ a). Según el teorema 12.18, la hipótesis sobre el invariante se traduce en que la curva tiene potencialmente buena reducción, es decir, que existe una extensión finita L/K tal que E_L/L tiene buena reducción. Sea l el mayor primo que divide a m y llamemos

$$l' = \begin{cases} l & \text{si } l > 2, \\ 4 & \text{si } l = 2. \end{cases}$$

Como $m \geq 3$, tenemos que $l' \mid m$, luego $E[l'] \subset E[m]$, luego I_K actúa trivialmente sobre $E[l']$.

Consideremos ahora el grupo de inercia $G_0(L/K) = I_K/I_L$. El teorema anterior nos da que I_L actúa trivialmente en $T_l(E)$, luego $G_0(L/K)$ actúa sobre $T_l(E)$. En otras palabras, tenemos un homomorfismo

$$\rho : G_0(L/K) \longrightarrow \mathrm{Aut}_{\mathbb{Z}_l} T_l(E).$$

Explícitamente, cada $x \in T_l(E)$ es una sucesión $x = (P_n)$ con $P_n \in E[l^n]$ de modo que $P_n = lP_{n+1}$ y, para cada $\sigma \in I_K$, tenemos que $x^\sigma = (P_n^\sigma)$.

Más en general, si fijamos una base x, y de $T_l(E)$ sobre $\mathbb{Z}_l$, cada automorfismo $u : T_l(E) \longrightarrow T_l(E)$ (como $\mathbb{Z}_l$-módulo) está determinado por las imágenes $u(x) = ax + by$, $u(y) = cx + dy$ o, equivalentemente, por la matriz

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{LG}(\mathbb{Z}_l).$$

Si $z \in T_l(E)$ tiene coordenadas $z = z_1 x + z_2 y$, entonces las coordenadas de $u(z)$ son

$$(z_1, z_2) \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (az_1 + cz_2, bz_1 + dz_2),$$

luego, por la definición de la estructura de $\mathbb{Z}_l$-módulo en $T_l(E)$, tenemos que $u(z)_n = (a_n z_{1,n} + c_n z_{2,n}, b_n z_{1,n} + d_n z_{2,n})$, donde $a_n, b_n, c_n, d_n \in \mathbb{Z}/l^n\mathbb{Z}$ son los restos módulo l^n de a, b, c, d.

Por consiguiente, si llamamos $u_n : E[l^n] \longrightarrow E[l^n]$ al automorfismo definido por la matriz

$$\begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \in \mathrm{LG}(\mathbb{Z}/n\mathbb{Z}),$$

tenemos que $u(z) = (u_n(z_n))$. Observemos que las aplicaciones $u \mapsto u_n$ son homomorfismos $\mathrm{Aut}_{\mathbb{Z}_l}(T_l(E)) \longrightarrow \mathrm{Aut}_{\mathbb{Z}}(E[l^n])$. En estos términos, hemos visto que la composición

$$G_0(L/K) \xrightarrow{\rho} \mathrm{Aut}_{\mathbb{Z}_l}(T_l(E)) \longrightarrow \mathrm{Aut}_{\mathbb{Z}}(E[l'])$$

es la acción natural de $G_0(L/K)$ (o, equivalentemente, de I_K) sobre $E[l']$, y sabemos que esta acción es trivial. Por consiguiente, la imagen por ρ de $G_0(L/K)$ es un subgrupo finito del núcleo del segundo homomorfismo. Si probamos que dicho núcleo no tiene más subgrupo finito que el subgrupo trivial, concluiremos que la imagen de ρ es trivial, es decir, que I_K actúa trivialmente sobre $T_l(E)$, lo cual, según el teorema anterior, equivale a que E tenga buena reducción sobre K.

Equivalentemente, sólo nos queda probar que el grupo

$$H = \{A \in \mathrm{LG}(\mathbb{Z}_l) \mid A \equiv I_2 \ (\mathrm{mód}\ l')\}$$

no tiene elementos no triviales de orden finito. (Aquí es donde necesitamos que sea $l' = 4$ si $l = 2$, pues si fuera $l' = 2$, una matriz de orden finito sería $-I_2$.)

Supongamos, pues, que H contiene una matriz A de orden finito $\neq 1$. No perdemos generalidad si suponemos que tiene orden primo p. Podemos considerar entonces el polinomio mínimo $\mathrm{pol.min}\, A \in \mathbb{Q}_l[X]$, que divide a $X^p - 1$ y también al polinomio característico, el cual cumple

$$\mathrm{pol.car}\, A \equiv \mathrm{pol.car}\, I_2 = (X-1)^2 \ (\mathrm{mód}\ l').$$

Si $\mathrm{pol.min}\, A$ tiene grado 2, entonces coincide con el polinomio característico, con lo que $\mathrm{pol.car}A \mid X^p - 1$ (en $\mathbb{Q}_l[X]$, luego en $\mathbb{Z}_l[X]$) y, por consiguiente, $(X-1)^2 \mid X^p - 1$ en $(\mathbb{Z}/l\mathbb{Z})[X]$. Esto sólo es posible si $p = l = 2$. Entonces

$$\mathrm{pol.car}\, A = \mathrm{pol.min}\, A = X^2 - 1 \not\equiv (X-1)^2 \ (\mathrm{mód}\ 4),$$

luego este caso no puede darse.

Si $\mathrm{pol.min}\, A$ tiene grado 1, no puede ser $X-1$, pues sería $A = I_2$, luego divide al polinomio ciclotómico $c_p(X)$. Por consiguiente, $c_p(X)$ y $\mathrm{pol.car}\, A$ tienen un factor común en $\mathbb{Q}_l[X]$, luego también en $\mathbb{Z}_l[X]$, y podemos tomarlo mónico. Concluimos como antes que $c_p(X)$ es divisible entre $X-1$ en $(\mathbb{Z}/l\mathbb{Z})[X]$, con lo que, nuevamente, $X^p - 1$ tiene una raíz doble en dicho cuerpo, y eso nos lleva también al caso $p = l = 2$. Ahora tendría que ser $\mathrm{pol.min}\, A = X + 1$, pero entonces $A = -I_2 \notin H$, luego este caso tampoco puede darse. ∎

Observemos que el teorema anterior no puede ser cierto para curvas arbitrarias (sin exigir que tengan buena reducción potencial), pues, si así fuera, bastaría tomar una extensión finita L/K tal que $E[m] \subset E(L)$ para un $m \geq 3$ cualquiera, para concluir que E_L/L tiene buena reducción. De este modo, resultaría que todas las curvas elípticas tendrían potencialmente buena reducción.

Las condiciones del teorema anterior (y las de 13.8) son especialmente simples si el cuerpo de restos es algebraicamente cerrado. Entonces $I_K = G(\bar{K}/K)$, por lo que la condición de que I_K deje invariante a $E[m]$ es equivalente a que $E[m] \subset E(K)$.

En otros términos, si llamamos $K(E[m])$ a la adjunción a K de los cuerpos $K(P)$ de los puntos $P \in E[m]$ (o, en términos clásicos, la adjunción de las coordenadas de los puntos $P \in E[m]$ vistos como puntos racionales de $E(\bar{K})$), tenemos que $K(E[m])/K$ es una extensión finita de Galois (porque $G(\bar{K}/K)$ permuta los puntos de $E[m]$), y la condición de que I_K deje invariante a $E[m]$ equivale a que deje invariante a $K(E[m])$, es decir, a que la extensión $K(E[m])/K$ sea no ramificada. Si k es algebraicamente cerrado, esto equivale a su vez a que $K(E[m]) = K$.

Para curvas con buena reducción potencial, los cuerpos $K(E[m])$ no son tantos como parecen:

Teorema 13.10 *Supongamos que una curva elíptica E/K cumple $|j(E)| \leq 1$ y que el cuerpo de restos de K es algebraicamente cerrado de característica p.*

a) Existe una mínima extensión L/K tal que, para toda extensión finita K'/K, la curva $E_{K'}/K'$ tiene buena reducción si y sólo si $L \subset K'$.

b) Se cumple que $L = K(E[m])$, para cualquier natural $m \geq 3$ primo con p. En particular, la extensión L/K es finita de Galois.

c) Si $p \neq 2$, entonces $|L : K(E[2])| \,\big|\, 2$.

Demostración: Por el teorema anterior, la curva $E_{K'}/K'$ tiene buena reducción si y sólo si $E[m] \subset E(K')$, lo que equivale a que $K(E[m]) \subset K'$, para cualquier $m \geq 3$ prefijado primo con p.

Aplicando esto a m' y a $K' = K(E[m'])$, concluimos que $E_{K'}/K'$ tiene buena reducción, y aplicando el mismo hecho a m y K', obtenemos la inclusión $K(E[m]) \subset K(E[m'])$. Intercambiando los papeles llegamos a la inclusión opuesta, luego todos los cuerpos $K(E[m])$ son una misma extensión L de K y cumple a). La extensión L/K es de Galois porque los K-automorfismos permutan los puntos de $E[m]$. Con esto quedan probados a) y b).

Para probar c) llamamos $L_0 = K(E[2])$ y tomamos una ecuación de Weierstrass de E/K de la forma $Y^2 = X^3 + a_2X^2 + a_4X + a_6$, con $a_i \in K$ enteros. Es fácil ver que los tres puntos finitos de $E[2]$ son los que en $E(\bar{K})$ tienen coordenadas $(\alpha, 0)$, donde $\alpha \in \bar{K}$ es una raíz del miembro derecho de la ecuación. Como los tres puntos están en $E(L_0)$, concluimos que la ecuación factoriza como

$$Y^2 = (X - a)(X - b)(X - c), \qquad a, b, c \in L_0.$$

Un cambio de variables $X = X' + c$ nos permite suponer que $c = 0$, con lo que la ecuación se reduce a

$$Y^2 = X(X-a)(X-b).$$

Si llamamos $L' = L_0(\sqrt{a})$, el cambio de variables $X = aX'$, $Y = (\sqrt{a})^3 Y'$ pone la ecuación en forma de Legendre:

$$Y^2 = X(X-1)(X-\lambda),$$

y el mismo argumento de 12.17 prueba que $E_{L'}$ tiene buena reducción, luego ha de ser $L_0 \subset L \subset L'$, y esto implica que $|L : L_0| \mid 2$. ∎

En las condiciones del teorema anterior, de acuerdo con el teorema 12.17, sabemos que $|L : K| \mid 24$, e incluso $|L : K| \mid 12$ si $p \neq 2$. En particular, vemos que la extensión L/K es dominadamente ramificada siempre que $p \neq 2, 3$. El interés de la ramificación dominada es que reduce la condición de buena reducción a una divisibilidad de grados en lugar de una inclusión de cuerpos. Vamos a enunciarlo sin exigir que el cuerpo de restos sea algebraicamente cerrado:

Teorema 13.11 *Sea E/K una curva elíptica tal que $|j(E)| \leq 1$ y sea p la característica del cuerpo de restos de K.*

a) Si $m \geq 3$ es un número natural primo con p, el índice de ramificación e_0 de la extensión $K(E[m])/K$ es independiente de m, y cumple $e_0 \mid 24$. Si $p \neq 2$, entonces $e_0 \mid 12$.

b) Si $p \nmid e_0$ (en particular si $p \neq 2, 3$), entonces, para cada extensión finita K'/K, se cumple que $E_{K'}$ tiene buena reducción si y sólo si su índice de ramificación es múltiplo de e_0.

Demostración: Por el teorema 13.1 sabemos que si K'/K es cualquier extensión finita, el índice de ramificación de K'/K coincide con el de $\hat{K}'_{\mathrm{nr}}/\hat{K}_{\mathrm{nr}}$, el cual coincide a su vez con el grado $|\hat{K}'_{\mathrm{nr}} : \hat{K}_{\mathrm{nr}}|$. Teniendo en cuenta que el tipo de reducción de $E_{K'}$ coincide con el de $E_{\hat{K}'_{\mathrm{nr}}}$, así como que

$$\widehat{K(E[m])}_{\mathrm{nr}} = \hat{K}_{\mathrm{nr}}(E[m]),$$

es claro que podemos sustituir K por $\hat{K}_{\mathrm{nr}}$, con lo que podemos suponer que el cuerpo de restos es algebraicamente cerrado. El apartado a) es, entonces, consecuencia inmediata de las observaciones previas al teorema. Para probar b) basta observar que $E_{K'}$ tiene buena reducción si y sólo si $L = K(E[m]) \subset K'$, si y sólo si $L \subset K'_d$, donde K'_d es la máxima extensión dominadamente ramificada de K contenida en K', cuyo grado es el mayor natural primo con p que divide al grado $|K' : K|$ (teorema [CC 2.46]). Teniendo en cuenta el teorema 13.3, la inclusión $K \subset L \subset K'_d$ equivale a que $e_0 = |L : K| \;\big|\; |K'_d : K|$ (pues si se da la divisibilidad, entonces el grupo de Galois $G(K'_d/K)$ tiene un subgrupo de índice d, cuyo cuerpo fijado ha de ser necesariamente L), y esto equivale a que $e_0 \mid |K' : K|$. ∎

Ahora es inmediato que, si $p \neq 2, 3$, el índice de ramificación e_0 considerado en el teorema anterior coincide con el valor de m determinado por la tabla del teorema 9.3 en función del tipo de reducción de E/K (donde no hemos de considerar los tipos $\mathrm{I_n}$ ni $\mathrm{I_n^*}$, para $n > 0$, pues tienen potencialmente reducción multiplicativa).

13.4 El carácter de Artin

En esta sección hacemos un paréntesis para estudiar más a fondo las extensiones libremente ramificadas. Nos apoyaremos fuertemente en la teoría de la ramificación expuesta en el capítulo X de [CC]. Empezamos recordando los conceptos y hechos básicos:

Si K'/K es una extensión finita de Galois, definimos sus *grupos de ramificación* como los grupos[9]

$$G_i(K'/K) = \{\sigma \in G(K'/K) \mid v(\sigma(\alpha) - \alpha) \geq i + 1 \text{ para todo } \alpha \in D'\},$$

donde D' es el anillo de enteros de K'. Observemos que $G_{-1}(K'/K) = G(K'/K)$ y que $G_0(K'/K)$ es el grupo de inercia que ya habíamos definido.

En [CC] se expone la teoría de la ramificación para el caso de los cuerpos numéricos y el de los cuerpos locales (sus compleciones, las extensiones finitas de los cuerpos $\mathbb{Q}_p$ de números p-ádicos) para mostrar más fácilmente la relación entre ambos casos, pero es inmediato comprobar que todo lo dicho en el caso p-ádico es válido igualmente —sin cambio alguno en las demostraciones[10]— en el contexto en el que venimos trabajando en todo este capítulo, es decir, para cuerpos métricos completos discretos de característica 0 con cuerpo de restos perfecto de característica prima p. Por consiguiente, en esta sección seguimos trabajando en este mismo contexto.

El teorema [CC 10.4] afirma que todos los grupos $G_i(K'/K)$ son subgrupos normales de $G(K'/K)$, y que existe un i tal que $G_i(K'/K) = 1$. Así pues, forman una serie

$$1 = G_i \trianglelefteq G_{i-1} \trianglelefteq \cdots \trianglelefteq G_0 \trianglelefteq G(K'/K).$$

Si descomponemos el índice de ramificación $e = p^s e_0$, donde $p \nmid e_0$, sabemos que $g_0 = e$, y el teorema [CC 10.5] nos da que $g_1 = p^s$, de modo que $G_1(K'/K)$ es el p-subgrupo de Sylow del grupo de inercia $G_0(K'/K)$. En particular, la extensión K'/K es dominadamente ramificada si y sólo si $G_1(K'/K) = 1$.

[9] En [CC 10.1] están definidos en un contexto más general. En el caso local, el grupo de descomposición $G_{\mathfrak{P}}$ es todo el grupo de Galois $G(K'/K)$.

[10] El teorema [CC 10.6] no es válido en este contexto general porque se apoya en que el cuerpo de restos es finito, pero no vamos a necesitar este hecho ni se usa en los teorema siguientes de [CC]. Podría parecer que la prueba de [CC 10.5] usa también la finitud del cuerpo de restos, pero no es cierto: sólo requiere el hecho de que todo subgrupo finito del grupo multiplicativo de un cuerpo es cíclico (pues, si el grupo tiene orden n, ha de ser el grupo de las raíces n-simas de la unidad, que es cíclico).

Si $D' = D[\alpha_1, \ldots, \alpha_n]$, es fácil ver que

$$G_i(K'/K) = \{\sigma \in G(K'/K) \mid v(\sigma(\alpha_j) - \alpha_j) \geq i+1 \text{ para } j = 1, \ldots, n\}.$$

Con esto podemos probar:

Teorema 13.12 *Si K'/K es una extensión finita de Galois, el isomorfismo natural (dado por la restricción)*

$$G(\hat{K}'_{\mathrm{nr}}/\hat{K}_{\mathrm{nr}}) \longrightarrow G_0(K'/K)$$

se restringe a isomorfismos entre los grupos de ramificación de ambas extensiones.

DEMOSTRACIÓN: Sea $K'' = K_{\mathrm{nr}} \cap K'$, de modo que tenemos la igualdad de cuerpos de restos $k'' = k'$. Según el teorema [CC 3.11], si $\alpha \in K''$ cumple $k'' = k[\bar{\alpha}]$ y π es cualquier primo en K', entonces $D' = D[\alpha, \pi]$, mientras que $\hat{D}'_{\mathrm{nr}} = \hat{D}_{\mathrm{nr}}[\pi]$. Ahora basta aplicar la observación previa al teorema, teniendo en cuenta que, como $\alpha \in K_{\mathrm{nr}}$, todos los elementos de $G(\hat{K}'_{\mathrm{nr}}/\hat{K}_{\mathrm{nr}})$ fijan a α. ∎

Esto nos permitirá reducir muchas pruebas al caso en que el cuerpo de restos es algebraicamente cerrado.

El teorema [CC 3.12] nos da que existe un $\alpha \in D'$ tal que $D' = D[\alpha]$ y, por consiguiente,

$$G_i(K'/K) = \{\sigma \in G(K'/K) \mid v_{K'}(\sigma(\alpha) - \alpha) \geq i+1\}.$$

De aquí se sigue que la función $i_{K'/K} : G(K'/K) \longrightarrow \mathbb{N} \cup \{\infty\}$ dada por

$$i_{K'/K}(\sigma) = v_{K'}(\alpha^\sigma - \alpha).$$

es independiente de la elección del generador $\alpha \in D'$, pues es igual al máximo número natural i tal que $\sigma \in G_{i-1}(K'/K)$. En términos de esta función, tenemos que[11]

$$G_i(K'/K) = \{\sigma \in G(K'/K) \mid i_{K'/K}(\sigma) \geq i+1\}.$$

El hecho de que $G_i(K'/K) = 1$ para i suficientemente grande se traduce en que

$$i_{K'/K}(\sigma) = \infty \quad \text{si y sólo si} \quad \sigma = 1.$$

Similarmente, el hecho de que los grupos de ramificación sean normales en $G(K'/K)$ se traduce en que

$$i_{K'/K}(\tau^{-1}\sigma\tau) = i_{K'/K}(\sigma), \qquad \text{para todo } \sigma, \tau \in G(K'/K).$$

Otra propiedad elemental es la siguiente:

$$i_{K'/K}(\sigma\tau) \geq \min\{i_{K'/K}(\sigma), i_{K'/K}(\tau)\}.$$

[11] En virtud de [CC 10.3], también podemos calcular la función $i_{K'/K}$ con $\alpha = \pi$, donde π es un primo de K', aunque no genere el anillo de enteros.

En efecto:

$$i_{K'/K}(\sigma\tau) = v(\alpha^{\sigma\tau} - \alpha) = v(\alpha^{\sigma\tau} - \alpha^\sigma + \alpha^\sigma - \alpha)$$
$$\geq \min\{v(\alpha^{\sigma\tau} - \alpha^\sigma), v(\alpha^\sigma - \alpha)\} = \min\{i_{K'/K}(\tau), i_{K'/K}(\sigma)\}.$$

■

El teorema [CC 10.16] se traduce en una propiedad más de la función $i_{K'/K}$:

Teorema 13.13 *Sea $k \subset L \subset K$ una cadena de extensiones de Galois de cuerpos locales. Entonces, para cada $\sigma \in G(L/k)$, se cumple que*

$$i_{L/k}(\sigma|_L) = \frac{1}{e_{K/L}} \sum_{\tau \in G(K/L)} i_{K/k}(\tau\sigma).$$

Demostración: Sea α (resp. β) un generador del anillo de enteros de K (resp. de L) sobre el anillo de enteros de k. El teorema [CC 10.16] afirma que

$$v_L(\sigma(\beta) - \beta) = \sum_{\tau \in G(K/L)} v_L((\tau\sigma)(\alpha) - \alpha),$$

y esto equivale a que

$$e_{K/L}\, i_{L/k}(\sigma|_L) = \sum_{\tau \in G(K/L)} i_{K/k}(\tau\sigma).$$

■

De aquí en adelante L/K será una extensión finita de Galois, llamaremos $G = G(L/K)$ a su grupo de Galois y $G_i = G_i(L/K)$ a sus grupos de ramificación. Representaremos por g y g_i sus órdenes respectivos.

La función $i_{L/K} : G \longrightarrow \mathbb{N} \cup \{\infty\}$ que acabamos de definir es una función de clases en G excepto por el hecho de que no está definida en $\sigma = 1$. Vamos a corregir esto:

Definición 13.14 La *función de Artin* $a_{L/K} : G(L/K) \longrightarrow \mathbb{Z}$ es la función dada por

$$a_{L/K}(\sigma) = -f\, i_{L/K}(\sigma) \quad \text{si } \sigma \neq 1, \quad a_{L/K}(1) = f \sum_{\sigma \neq 1} i_{L/K}(\sigma),$$

donde f es el grado de inercia de la extensión L/K.

Es claro que $a_{L/K}$ es una función de clases en $G(L/K)$. Hemos definido $a_{L/K}(1)$ para que se cumpla que

$$\sum_{\sigma \in G} a_{L/K}(\sigma) = 0,$$

es decir, que[12] $(a_{L/K}, 1) = 0$.

[12]De este modo, si una función de clases ϕ coincide con $a_{L/K}$ salvo quizá para $\sigma = 1$ y cumple $(\phi, 1) = 0$, entonces $\phi = a_{L/K}$.

El valor $a_{L/K}(1)$ tiene una interpretación aritmética. Para obtenerla observamos que $i_{L/K}$ toma el valor i sobre los elementos de $G_{i-1}\setminus G_i$, luego, si $g_t = 1$, tenemos que

$$\sum_{\sigma\neq 1} i_{L/K}(\sigma) = (g_0 - g_1) + 2(g_1 - g_2) + 3(g_2 - g_3) + \cdots + t(g_{t-1} - 1)$$

$$= g_0 + g_1 + \cdots + g_{t-1} - t = \sum_{i=0}^{\infty}(g_i - 1).$$

El teorema [CC 10.11] nos da inmediatamente el resultado siguiente:

Teorema 13.15 *Si $\mathfrak{D}_{L/K}$ es el diferente de la extensión L/K, entonces*

$$a_{L/K}(1) = f v_L(\mathfrak{D}_{L/K}).$$

De la propia definición de la función de Artin se sigue que, $a_{L/K} = 0$ si y sólo si la extensión L/K es no ramificada. El propósito central de esta sección es demostrar el teorema siguiente:

Teorema 13.16 *Si L/K es es ramificada, la función $a_{L/K}$ es un carácter del grupo de Galois $G(L/K)$.*

Como $a_{L/K}$ es una función de clases, el teorema 11.32 nos da que es combinación lineal de los caracteres irreducibles de G, y el coeficiente de cada carácter χ es $(a_{L/K}, \chi)$. Teniendo en cuenta que $a_{L/K} \neq 0$, basta probar que estos coeficientes son números naturales. Observamos que

$$(a_{L/K}, \chi) = \frac{1}{g}\sum_{\sigma\in G} a_{L/K}(\sigma)\chi(\sigma^{-1}) = \frac{1}{g}\sum_{\sigma\in G}\chi(\sigma)\, a_{L/K}(\sigma^{-1})$$

$$= \frac{1}{g}\sum_{\sigma\in G}\chi(\sigma)\,\overline{a_{L/K}(\sigma)} = (\chi, a_{L/K}),$$

donde hemos usado que $a_{L/K}(\sigma^{-1}) = a_{L/K}(\sigma) = \overline{a_{L/K}(\sigma)}$.

Para cada función de clases ϕ de G, definimos

$$f(\phi) = (\phi, a_{L/K}).$$

El teorema 13.16 quedará probado si demostramos que $f(\chi)$ es un número natural para todo carácter χ de G.

Para cada $i \geq 0$, llamamos r_{G_i} al carácter regular del grupo de ramificación i-ésimo G_i. Sabemos que en la descomposición de r_{G_i} en suma de caracteres irreducibles aparece cada carácter irreducible con multiplicidad igual a su grado. Por consiguiente, $u_i = r_{G_i} - 1_{G_i}$ es también un carácter de G_i, salvo que sea $G_i = 1$, en cuyo caso $u_i = 0$. Esto sucede para todo i suficientemente grande.

Teorema 13.17 *En las condiciones anteriores, se cumple que*

$$a_{L/K} = \sum_{i=0}^{\infty}\frac{g_i}{g_0}\,u_i^G.$$

DEMOSTRACIÓN: Tenemos que

$$u_i^G(\sigma) = \frac{1}{g_i}\sum_{\tau\in G} u_i^0(\tau\sigma\tau^{-1}).$$

Teniendo en cuenta que G_i es un subgrupo normal en G y que $u_i(\sigma) = -1$ para todo $\sigma \neq 1$, es claro que

$$u_i^G(\sigma) = \begin{cases} \frac{g(g_i-1)}{g_i} & \text{si } \sigma = 1 \\ -g/g_i & \text{si } \sigma \in G_i \setminus \{1\}, \\ 0 & \text{si } \sigma \in G \setminus G_i. \end{cases}$$

Por lo tanto,

$$\frac{g_i}{g_0}u_i^G(\sigma) = \begin{cases} f(g_i-1) & \text{si } \sigma = 1 \\ -f & \text{si } \sigma \in G_i \setminus \{1\}, \\ 0 & \text{si } \sigma \in G \setminus G_i. \end{cases}$$

Así, si $\sigma \in G_k \setminus G_{k+1}$, la suma para todo i es igual a

$$-f(k+1) = -fi_{L/K}(\sigma) = a_{L/K}(\sigma).$$

Ahora observamos que

$$\sum_{\sigma\in G} u_i^G(\sigma) = 0,$$

y lo mismo vale si sumamos para todo i. Como $a_{L/K}$ cumple también que $(a_{L/K}, 1) = 0$, también se tiene la igualdad para $\sigma = 1$. ∎

De aquí extraemos varias consecuencias. En primer lugar, vemos que $g_0 a_{L/K}$ es un carácter de G. Por consiguiente, si χ es un carácter de G, se cumple que $(\chi, g_0 a_{L/K})$ es un número natural. Equivalentemente:

Teorema 13.18 *Si χ es un carácter de G, se cumple que $f(\chi)$ es un número racional ≥ 0.*

Para cada función de clases ϕ en G, definimos

$$\phi(G_i) = \frac{1}{g_i}\sum_{\sigma\in G_i} \phi(\sigma).$$

En estos términos se cumple lo siguiente:

Teorema 13.19 *Si ϕ es una función de clases en G, entonces*

$$f(\phi) = \sum_{i=0}^{\infty} \frac{g_i}{g_0}(\phi(1) - \phi(G_i)).$$

DEMOSTRACIÓN: Basta tener en cuenta que

$$(\phi, u_i^G) = (\phi|_{G_i}, u_i) = \phi(1) - \phi(G_i).$$

∎

Teorema 13.20 *Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación de G con carácter χ, y sea V^{G_i} el subespacio formado por los elementos de V fijados por cada elemento de G_i. Entonces*

$$f(\chi) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \dim(V/V^{G_i}).$$

DEMOSTRACIÓN: Observemos que V^{G_1} es el $\mathbb{C}[G_i]$-submódulo de V asociado al carácter trivial 1_{G_i} en la descomposición dada por el teorema 11.36. Por consiguiente, su dimensión es la multiplicidad de 1_{G_i} en $\chi|_{G_i}$, es decir:

$$\dim V^{G_i} = (\chi|_{G_i}, 1_{G_i}) = \chi(G_i).$$

Por otra parte, $\dim V = \chi(1)$, con lo que $\dim V/V^{G_i} = \chi(1) - \chi(G_i)$ y basta aplicar el teorema anterior. ∎

Seguidamente reformulamos el teorema 13.13:

Teorema 13.21 *Sea $K \subset K' \subset L$ una cadena de extensiones de Galois. Llamemos $N = G(L/K')$, de modo que $G/N \cong G(K'/K)$. Entonces,*

$$a_{K'/K} = a_{L/K}^{G/N}.$$

DEMOSTRACIÓN: Tomemos un $\sigma \in G$, de modo que $\sigma|_{K'}$ se identifica con $N\sigma \in G/N$. De acuerdo con 11.59, la igualdad $a_{K'/K}(N\sigma) = a_{L/K}^{G/H}(N\sigma)$ equivale a

$$a_{K'/K}(N\sigma) = \frac{1}{n_{L/K'}} \sum_{n\in N} a_{L/K}(n\sigma).$$

Si $\sigma \notin N$, esto equivale a su vez a que

$$-f_{K'/K}\, i_{K'/K}(\sigma|_{K'}) = \frac{1}{e_{L/K'} f_{L/K'}} \sum_{n\in N} (-f_{L/K}) i_{L/K}(n\sigma),$$

lo cual, simplificando, se reduce a

$$i_{K'/K}(\sigma|_{K'}) = \frac{1}{e_{L/K'}} \sum_{n\in N} i_{L/K}(n\sigma),$$

que es precisamente lo que afirma el teorema 13.13. Falta probar la igualdad cuando $\sigma|_{K'} = 1$, pero ésta es consecuencia inmediata de que

$$(a_{L/K}^{G/N}, 1_{G/N}) = (a_{L/K}, 1_G) = 0.$$

∎

Ahora relacionamos la función $a_{L/K}$ con $a_{L/K'}$.

Teorema 13.22 *Sea $K \subset K' \subset L$ una cadena de extensiones tal que L/K es de Galois y sea $H = G(L/K')$. Entonces*

$$a_{L/K}|_H = v_K(\Delta_{K'/K}) r_H + f_{K'/K}\, a_{L/K'},$$

donde $\Delta_{K'/K}$ es el discriminante de K'/K y r_H es el carácter regular de H.

DEMOSTRACIÓN: Si $\sigma \in G$ cumple $\sigma \neq 1$, entonces

$$a_{L/K}(\sigma) = -f_{L/K}\, i_{L/K}(\sigma), \quad a_{L/K'}(\sigma) = -f_{L/K'}\, i_{L(K')}(\sigma), \quad r_H(\sigma) = 0.$$

Además, un generador del anillo de enteros de L sobre el anillo de enteros de K lo genera también sobre el anillo de enteros de K', luego $i_{L/K}(\sigma) = i_{L/K'}(\sigma)$. Ahora es claro que la igualdad del enunciado se cumple para σ. Falta considerar el caso $\sigma = 1$. Teniendo en cuenta el teorema 13.15, la igualdad que hemos de probar es equivalente a

$$f_{L/K}\, v_L(\mathcal{D}_{L/K}) = |L : K'| v_K(\Delta_{K'/K}) + f_{K'/K} f_{L/K'}\, v_L(\mathcal{D}_{L/K'}).$$

Según [CC 3.22], el discriminante de una extensión es la norma del diferente, lo cual implica que

$$v_K(\Delta_{L/K}) = f_{L/K}\, v_L(\mathcal{D}_{L/K}), \qquad v_{K'}(\Delta_{L/K'}) = f_{L/K'}\, v_L(\mathcal{D}_{L/K'}).$$

Así pues, la ecuación que hemos de probar equivale a

$$v_K(\Delta_{L/K}) = |L : K'| v_K(\Delta_{K'/K}) + f_{K'/K}\, v_{K'}(\Delta_{L/K'}).$$

A su vez, esta fórmula equivale al teorema [CC 3.24]. ∎

Como consecuencia:

Teorema 13.23 *Sea $K \subset K' \subset L$ una cadena de extensiones tal que L/K es de Galois. Sea $H = G(L/K')$. Entonces, para todo carácter ψ de H,*

$$f(\psi^G) = v_K(\Delta_{K'/K})\psi(1) + f_{K'/K} f(\psi).$$

DEMOSTRACIÓN: Hay que entender que la última f de la fórmula es la función correspondiente a la extensión L/K'.

$$\begin{aligned} f(\psi^G) = (\psi^G, a_{L/K}) = (\psi, a_{L/K}|_H) &= v_K(\Delta_{K'/K})(\psi, r_H) + f_{K'/K}(\psi, a_{L/K'}) \\ &= v_K(\Delta_{K'/K})\psi(1) + f_{K'/K}\, f(\psi). \end{aligned}$$

∎

Ahora consideramos la función $\phi_{L/K}$ definida en [CC 10.18]:

Teorema 13.24 *Sea χ un carácter de grado 1 en G y sea $c(\chi)$ el mayor número natural tal que $\chi|_{G_{c(\chi)}} \neq 1$. (Si $\chi = 1_G$, tomamos $c(\chi) = -1$.) Entonces,*

$$f(\chi) = \phi_{L/K}(c(\chi)) + 1.$$

DEMOSTRACIÓN: Si $i \leq c(\chi)$, entonces $\chi(G_i) = (\chi|_{G_i}, 1) = 0$ (porque $\chi|_{G_i}$ tiene grado 1, luego es irreducible). Por lo tanto, $\chi(1) - \chi(G_i) = 1$. Si $i > c(\chi)$, entonces $\chi(G_i) = 1$, luego $\chi(1) - \chi(G_i) = 0$. El teorema 13.19 nos da que

$$f(\chi) = \sum_{i=0}^{c(\chi)} \frac{g_i}{g_0} = \phi(c(\chi)) + 1.$$

Teorema 13.25 *Sea χ un carácter de grado 1 en G, sea N su núcleo y sea K' su cuerpo fijado. Sea $c'(\chi)$ el mayor número natural tal que $(G/N)_{c'(\chi)} \neq 1$. Entonces $f(\chi) = \phi_{K'/K}(c'(\chi)) + 1$ es un número natural.*

DEMOSTRACIÓN: El teorema [CC 10.19] afirma que

$$(G/N)_i = G_{\psi_{L/K'}(i)}N/N,$$

donde $\psi_{L/K'}$ es la función de Hasse (la inversa de $\phi_{L/K'}$). Por tanto, $(G/N)_i = 1$ equivale a que $G_{\psi_{L/K'}(i)} \leq N$, es decir, a que $\chi|_{G_{\psi_{L/K'}(i)}} = 1$. Por consiguiente, $c(\chi) = \psi_{L/K'}(c'(\chi))$ o, equivalentemente, $c'(\chi) = \phi_{L/K'}(c(\chi))$. El teorema anterior y [CC 10.20] nos dan que

$$f(\chi) = \phi_{L/K}(c(\chi)) + 1 = \phi_{K'/K}(\phi_{L/K'}(c(\chi))) + 1 = \phi_{K'/K}(c'(\chi)) + 1.$$

Por último, la extensión K'/K es abeliana, luego podemos aplicar el teorema [CC 10.25]: el número natural $c'(\chi)$ cumple que $G(K'/K)_{c'(\chi)} \neq 1$ y $G(K'/K)_{c'(\chi)+1} = 1$, luego es un vértice de la función $\phi_{K'/K}$, luego $\phi_{K'/K}(c'(\chi))$ es un vértice de $\psi_{K'/K}$, luego es un número entero ≥ -1. (La función $\psi_{K'/K}$ es lineal hasta -1, luego su primer vértice es ≥ -1.) ∎

Finalmente estamos en condiciones de demostrar el teorema 13.16:

Hemos de probar que $f(\chi)$ es un número natural para todo carácter χ de G. Por el teorema 13.18 sabemos que $f(\chi)$ es un número racional ≥ 0, luego sólo necesitamos probar que es entero. Por el teorema de Brauer 11.48, podemos expresar

$$\chi = \sum_i n_i \psi_i^G,$$

donde $n_i \in \mathbb{Z}$ y cada ψ_i es un carácter de grado 1 en un cierto subgrupo H_i de G. Por consiguiente, basta probar que $f(\psi_i^G)$ es entero. Por 13.23, basta probar que $f(\psi_i)$ es entero, lo que equivale a suponer que χ tiene grado 1. En tal caso basta aplicar el teorema anterior. ∎

A partir del carácter de Artin podemos definir otro que, de hecho, es el que nos va a interesar:

Definición 13.26 Si L/K es una extensión finita de Galois, definimos la *función de Swan* $s_{L/K} : G(L/K) \longrightarrow \mathbb{Z}$ como la función dada por

$$s_{L/K} = a_{L/K} - u_0^G = \sum_{i=1}^{\infty} \frac{g_i}{g_0}\, u_i^G,$$

donde $u_i = r_{G_i} - 1_{G_i}$. (Véase el teorema 13.17.)

Explícitamente:

$$s_{L/K}(\sigma) = \begin{cases} f(1 - i(\sigma)) & \text{si } \sigma \in G_0 \setminus 1, \\ 0 & \text{si } \sigma \in G \setminus G_0, \end{cases}$$

y $s_{L/K}(1)$ está determinado por la relación $(s_{L/K}, 1_G) = 0$, que se cumple porque $(a_{L/K}, 1_G) = 0$ y $(u_0^G, 1_G) = (u_0, 1_{G_0}) = 0$.

Es claro entonces que $s_{L/K} = 0$ si y sólo si $G_1 = 1$, es decir, si la extensión L/K es dominadamente ramificada. En caso contrario es una función de clases no nula. Consideremos un carácter irreducible χ de G, y observemos que

$$(s_{L/K}, \chi) = \sum_{i=1}^{\infty} \frac{g_i}{g_0} (u_i^G, \chi) = \sum_{i=1}^{\infty} \frac{g_i}{g_0} (u_i, \chi_{G_i}) \geq 0.$$

Por otra parte, $(s_{L/K}, \chi) = (a_{L/K}, \chi) - (u_0^G, \chi) \in \mathbb{Z}$, puesto que $a_{L/K}$ y u_0^G son caracteres. Concluimos que $(s_{L/K}, \chi)$ es un número natural para todo χ, luego $s_{L/K}$ es un carácter de G, el *carácter de Swan* de la extensión L/K.

13.5 El invariante de Swan

Dada una curva elíptica E/K, el carácter de Swan que acabamos de definir permite definir una medida $\delta(E/K)$ de la ramificación libre de las extensiones $K(E[m])/K$, pero para ello tendríamos que utilizar mucha más teoría de representaciones de grupos que la que hemos desarrollado en el capítulo XI. En su lugar, definiremos $\delta(E/K)$ sin hacer referencia al carácter de Swan y mostraremos sólo parcialmente la relación entre ambos conceptos.

Definición 13.27 Sea E/K una curva elíptica, sea l un primo distinto de la característica p del cuerpo de restos de K. Definimos el *invariante de Swan* de E/K como

$$\delta(E/K) = \sum_{i=1}^{\infty} \frac{g_i}{g_0} \dim_{\mathbb{Z}/l\mathbb{Z}}(E[l]/E[l]^{G_i}),$$

donde $G_i = G_i(K(E[l])/K)$, $g_i = |G_i|$ y $E[l]^{G_i}$ es el subespacio vectorial de $E[l]$ fijado por todos los elementos de G_i.

El resultado principal que probaremos en esta sección es el teorema siguiente:

Teorema 13.28 *Si E/K es una curva elíptica, el invariante $\delta(E/K)$ es un número natural independiente del primo l con que se calcula.*

Del teorema 13.12 se sigue inmediatamente que $\delta(E/K) = \delta(E_{\hat{K}_{\mathrm{nr}}}/\hat{K}_{\mathrm{nr}})$, lo que nos permite restringirnos al caso en que el cuerpo de restos k es algebraicamente cerrado sin pérdida de generalidad.

Antes de entrar en la demostración de 13.28 probaremos algunos resultados sobre $\delta(E/K)$. En primer lugar probamos que $\delta(E/K)$ depende únicamente de la ramificación libre de las extensiones $K(E[l])/K$:

Teorema 13.29 *Si E/K es una curva elíptica, para cada primo $l \neq p$, se cumple que $\delta(E/K) = 0$ si y sólo si la extensión $K(E[l])/K$ es dominadamente ramificada.*

DEMOSTRACIÓN: Es claro que $\delta(E/K) = 0$ (para un l) si y sólo si G_1 actúa trivialmente sobre $E[l]$, si y sólo si G_1 actúa trivialmente sobre $K(E[l])$, si y sólo si $G_1 = 1$, si y sólo si la extensión $K(E[l])/K$ es dominadamente ramificada. ∎

Ahora probamos que, para calcular $\delta(E/K)$, podemos sustituir $K(E[l])$ por cualquier extensión dominadamente ramificada:

Teorema 13.30 *Dada una curva elíptica E/K y un primo $l \neq p$, llamemos $L_0 = K(E[l])$ y sea $K \subset L_0 \subset L$ de modo que L/K es finita de Galois y L/L_0 es dominadamente ramificada.*[13] *Entonces,*

$$\delta(E/K) = \sum_{i=1}^{\infty} \frac{g_i}{g_0} \dim_{\mathbb{Z}/l\mathbb{Z}}(E[l]/E[l]^{G_i}),$$

donde $G_i = G_i(L/K)$ y $g_i = |G_i|$.

DEMOSTRACIÓN: Llamemos $G_i^0 = G_i(L_0/K)$ y $g_i^0 = |G_i^0|$. En principio, $\delta(E/K)$ está definido en términos de los grupos G_i^0. Hemos de probar que podemos reemplazarlos por los G_i.

Observemos que la restricción $G(L/K) \longrightarrow G(L_0/K)$ tiene núcleo $G(L/L_0)$, que es primo con p, luego se restringe a un isomorfismo $r : G_1 \longrightarrow G_1^0$.

Como la extensión L/L_0 es dominadamente ramificada, su índice de ramificación es $e = g_0/g_0^0$ y, para $x \geq 0$, su función de Hasse viene es simplemente $\psi(x) = ex$ (véase [CC 10.18]). Según [CC 10.19], tenemos que

$$G_x^0 = G_{\psi(x)}H/H,$$

donde $H = G(L/L_0)$ y $G_x = G_{\{x\}}$, donde $\{x\}$ es el menor natural mayor o igual que x. En otros términos, $G_x^0 = r[G_{ex}]$. Más explícitamente, si la sucesión de grupos de ramificación de L_0/K es

$$G_1^0 = \cdots = G_{v_1}^0 > G_{v_1+1}^0 = \cdots = G_{v_2}^0 > G_{v_2+1} = \cdots$$

entonces la de L/K es

$$G_1 = \cdots = G_{ev_1} > G_{ev_1+1} = \cdots = G_{ev_2} > G_{ev_2+1} = \cdots,$$

de modo que $G_{v_i}^0$ está formado por las restricciones de los elementos de G_{ev_i}. Así pues, llamando $v_0 = 0$ y agrupando los sumandos iguales en el sumatorio del enunciado, tenemos que éste es igual a

$$\sum_i \frac{g_{ev_i}(ev_i - ev_{i-1})}{g_0} \dim_{\mathbb{Z}/l\mathbb{Z}}(E[l]/E[l]^{G_{ev_i}})$$

$$= \sum_i \frac{g_{v_i}^0(v_i - v_{i-1})}{g_0^0} \dim_{\mathbb{Z}/l\mathbb{Z}}(E[l]/E[l]^{G_{v_i}^0}) = \delta(E/K),$$

donde hemos usado que $g_{ev_i} = g_{v_i}^0$ y que $E[l]^{G_{ev_i}} = E[l]^{G_{v_i}^0}$. ∎

[13] En realidad esta hipótesis no es necesaria.

Ahora mostramos el efecto de cambiar el cuerpo base, siempre mediante una extensión dominadamente ramificada:

Teorema 13.31 *Si L/K es una extensión dominadamente ramificada y su índice de ramificación es e, entonces, para toda curva elíptica E/K y todo primo $l \neq p$, se cumple que $\delta(E_L/L) = e\,\delta(E/K)$.*

Demostración: Llamemos $L_0 = K(E[l])$, con lo que $LL_0 = L(E[l])$. La extensión LL_0/L_0 es dominadamente ramificada, luego el teorema anterior nos da que $\delta(E/K)$ puede calcularse con los grupos de ramificación de LL_0/K. Por otra parte, $\delta(E_L/L)$ se calcula, por definición, con los grupos de ramificación de LL_0/L. Ahora tenemos una cadena de extensiones $K \subset L \subset LL_0$ en la que la primera es dominadamente ramificada. Esto implica que

$$G_1(LL_0/K) \subset G(LL_0/L).$$

El teorema [CC 10.2] nos da entonces que

$$G_i(LL_0/L) = G_i(LL_0/K) \cap G(LL_0/L) = G_i(LL_0/K).$$

Así pues, la expresión dada por el teorema anterior para $\delta(E/K)$ coincide con la definición de $\delta(E_L/L)$ excepto por el término g_0, que es diferente para ambas extensiones y, concretamente, tenemos $g_0(LL_0/K) = eg_0(LL_0/L)$. Esto implica la relación del enunciado. ∎

En particular vemos que las extensiones no ramificadas no alteran el valor de $\delta(E/K)$.

Pasemos ya a probar el teorema 13.28. En primer lugar consideraremos el caso en que la curva E/K tiene buena reducción potencial. El teorema 13.10 nos dice que todos los cuerpos $K(E[l])$ son un mismo cuerpo L, salvo quizá $L_0 = K(E[2])$, que, en cualquier caso, cumple que $|L : L_0| \,\big|\, 2$.

Para que $l = 2$ sea un primo admisible ha de ser $p \neq 2$, y entonces la extensión L/L_0 es dominadamente ramificada, luego el teorema 13.30 nos da que $\delta(E/K)$ para $l = 2$ puede calcularse igualmente con los grupos de ramificación de L en lugar de con los de L_0.

Si la extensión L/K es dominadamente ramificada, entonces $\delta(E/K) = 0$ para cualquier primo l con el que se calcule. En particular esto sucede si E/K tiene buena reducción (pues entonces L/K es trivial) o si $p > 3$ (por 13.10). Supongamos, pues, que L/K tiene ramificación libre. En particular estamos suponiendo que la reducción de E/K es aditiva.

Veamos que, en estas condiciones, $E(K)[l] = 0$. Tratamos aparte el caso en que $l = 2$. Tal y como hemos explicado en la prueba de 13.10, la curva E/K admite una ecuación de Weierstrass de la forma

$$Y^2 = X^3 + a_2X^2 + a_4X + a_6,$$

de modo que los puntos de $E[2]$ distintos del neutro son los puntos de $E(\bar{K})$ de coordenadas $(\alpha, 0)$, donde α es una raíz del miembro derecho de la ecuación. Si

uno de ellos está en $E(K)$, tras un cambio de variables pasa a tener coordenadas $(0,0)$, y la ecuación de Weierstrass se reduce a $Y^2 = X(X^2 + a_2X + a_4)$. De aquí se sigue que $|L_0 : K| \,\big|\, 2$, luego $|L : K| \,\big|\, 4$, contradicción.

Pasamos ahora al caso en que $l > 3$. Para ello consideramos las sucesiones exactas

$$0 \longrightarrow E_0(K) \longrightarrow E(K) \longrightarrow E(K)/E_0(K) \longrightarrow 0,$$

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow E_r(k) \longrightarrow 0.$$

que ya consideramos en la prueba del teorema 13.8. Según el teorema 10.42, el orden del grupo $E(K)/E_0(K)$ divide al número de componentes conexas de la fibra cerrada del modelo de Néron de E/K que, para los tipos correspondientes a reducción aditiva, es 1, 2, 3 o 4. Por consiguiente, todo $P \in E(K)[l]$ tiene imagen trivial en $E(K)/E_0(K)$, luego está en $E_0(K)$. A su vez, su imagen en $E_r(k) = k^+$ es trivial, pues k^+ no contiene elementos de torsión, luego $P \in E_1(K)$, pero, por [CE 6.19], sabemos que $E_1(K)[l] = 0$.

En realidad podemos afirmar algo más fino: como L es la menor extensión de K donde E tiene buena reducción, si $K \subset K' \subsetneq L$, se cumple que $E_{K'}$ sigue teniendo reducción aditiva y L es también la menor extensión de K' donde $E_{K'}$ tiene buena reducción, luego el argumento precedente se aplica a $E_{K'}$ y nos permite concluir que $E(K')[l] = 0$.

Aplicamos esto a los cuerpos K_i fijados por los grupos de ramificación G_i, de modo que $E[l]^{G_i} \neq 0$ si y sólo si $E(K_i)[l] \neq 0$, si y sólo si $K_i = L$, si y sólo si $G_i = 1$, en cuyo caso $E[l]^{G_i} = E[l]$. En definitiva, llegamos así a que

$$\delta(E/K) = \sum_i \frac{2g_i}{g_0},$$

donde la suma recorre los índices i tales que $g_i \neq 1$. En particular, vemos que $\delta(E/K)$ es independiente de la elección de l.

Recordemos que estamos suponiendo que el cuerpo de restos de K es algebraicamente cerrado, por lo que $G(\bar{K}/L) = I_L$. Como E_L/L tiene buena reducción, el teorema 13.6 nos da que $G(\bar{K}/L)$ actúa trivialmente sobre $T_l(E)$, luego la acción de $G(\bar{K}/K)$ sobre $T_l(E)$ induce una acción

$$G(L/K) \longrightarrow \mathrm{Aut}(V_l(E)),$$

que es una representación de $G(L/K)$ sobre el cuerpo $\mathbb{Q}_l$. Llamemos χ_l a su carácter.

Si $G_i \neq 1$, entonces su cuerpo fijado K_i está estrictamente contenido en L, luego la reducción de E_{K_i}/K_i es aditiva, y 13.6 nos da que $V_l(E)^{G_i} = 0$.

Consideramos ahora $V = \bar{\mathbb{Q}}_l \otimes_{\mathbb{Q}_l} V_l(E)$ con la estructura natural de $\bar{\mathbb{Q}}_l[G]$-módulo, que determina una representación de G sobre el cuerpo $\bar{\mathbb{Q}}_l$ con el mismo carácter χ_l. Veamos que que $V^{G_i} = 0$ siempre que $G_i \neq 1$. Para ello consideramos la representación matricial $\rho : G_i \longrightarrow \mathrm{LG}(2, \mathbb{Q}_l)$ asociada a una base de $V_l(E)$. Si fuera $V^{G_i} \neq 0$, el sistema de ecuaciones $(x, y)(\rho(\sigma) - I_2) = (0, 0)$, para

$\sigma \in G_i$, tendría una solución no trivial en $\bar{\mathbb{Q}}_l$, pero, al ser un sistema de ecuaciones lineales con coeficientes en $\mathbb{Q}_l$, tendría también una solución no trivial en $\mathbb{Q}_l$, lo que implicaría que $V_l(E)^{G_i} \neq 0$.

Al ser $\bar{Q}_l$ algebraicamente cerrado, podemos afirmar que $(1, \chi_l|_{G_i}) = 0$ luego, llamando r_{G_i} al carácter regular de G_i y $u_i = r_{G_i} - 1$, tenemos también que

$$(u_i^G, \chi_l) = (u_i, \chi_{lG_i}) = (r_{G_i}, \chi_{lG_i}) = \chi_l(1) = 2.$$

Por el contrario, si $G_i = 1$, entonces $u_i = 0$ y $(u_i^G, \chi_l) = 0$. Esto nos da la siguiente expresión para el invariante de Swan:

$$\delta(E/K) = \sum_{i=1}^{\infty} \frac{g_i}{g_0}(u_i^G, \chi_l) = (s_{L/K}, \chi_l),$$

que es ciertamente un número natural, pues el carácter de Swan $s_{L/K}$ es un carácter de G (o la función nula).

Con esto queda probado el teorema 13.28 para curvas con buena reducción potencial. Para abordar el caso de la reducción multiplicativa potencial necesitamos estudiar los cuerpos $K(E[m])$ en este contexto. Nos apoyaremos en las curvas de Tate:

Sea $q \in K$ tal que $|q| < 1$ y consideremos la curva de Tate E_q/K. Tenemos un isomorfismo de grupos

$$\bar{K}/q^{\mathbb{Z}} \longrightarrow E_q(\bar{K}).$$

Sea m un número natural primo con p, sea $\zeta \in \bar{K}$ una raíz m-sima primitiva de la unidad y $Q \in \bar{K}$ una raíz m-sima de q. Se cumple que $\langle\zeta\rangle \cap \langle Q\rangle = 1$, pues si $\zeta^i = Q^j$, entonces $\zeta^{im} = q^j$ y, como $|\zeta| = 1$, $|q| < 1$, ha de ser $i = j = 0$. Es claro entonces que $\langle\zeta, Q\rangle \cong (\mathbb{Z}/m\mathbb{Z}) \times \mathbb{Z}$, y que

$$\langle\zeta, Q\rangle / q^{\mathbb{Z}} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

Por consiguiente, el isomorfismo de Tate se restringe a un monomorfismo

$$\langle\zeta, Q\rangle / q^{\mathbb{Z}} \longrightarrow E[m].$$

Como ambos grupos tienen m^2 elementos, se trata de un isomorfismo.

Llamemos $L = K(\zeta, Q)$. El isomorfismo de Tate se restringe a un isomorfismo $L/q^{\mathbb{Z}} \longrightarrow E(L)$, de donde se sigue que $K(E[m]) \subset L$. Como $p \nmid m$, la extensión ciclotómica $K(\zeta)/K$ es no ramificada, y la extensión $L/K(\zeta)$ es dominadamente ramificada por [CC 2.44], luego la extensión completa L/K es dominadamente ramificada, y lo mismo le sucede a $K(E[m])/K$.

En el caso general, si E/K es una curva elíptica con reducción multiplicativa potencial, es decir, tal que $|j(E)| > 1$, el teorema 12.16 nos da una extensión cuadrática (o trivial) L/K tal que E_L/L es una curva de Tate.

Por la parte ya probada, sabemos que $L(E[m])/L$ es una extensión no ramificada. Si E/K tiene reducción multiplicativa, la extensión L/K es trivial o

bien no ramificada (según que la reducción sea multiplicativa racional o irracional, aunque el segundo caso no puede darse si suponemos que el cuerpo de restos es algebraicamente cerrado), por consiguiente, la extensión $L(E[m])/K$ es dominadamente ramificada, y lo mismo sucede si $p = 3$ (pues entonces L/K es a, lo sumo, dominadamente ramificada).

Ahora podemos reunir los casos básicos en los que $\delta(E/K)$ es trivial:

Teorema 13.32 *Para toda curva elíptica E/K, se cumple que $\delta(E/K) = 0$ en los casos siguientes:*

a) La característica del cuerpo de restos es $p > 3$.

b) E/K tiene buena reducción o reducción multiplicativa.

c) E/K tiene potencialmente reducción multiplicativa y $p > 2$.

DEMOSTRACIÓN: Fijado un primo $l \neq p$, acabamos de ver que la extensión $K(E[l])/K$ es dominadamente ramificada cuando E/K tiene reducción multiplicativa y cuando tiene reducción multiplicativa potencial y $p > 2$. Si E/K tiene buena reducción, entonces la extensión $K(E[l])/K$ es no ramificada, luego también tenemos que $\delta(E/K) = 0$. Sólo nos falta considerar el caso en que E/K tenga buena reducción potencial y $p > 3$, en cuyo caso basta considerar el teorema 13.11. ∎

Así pues, para probar el teorema 13.28 sólo nos falta considerar el caso en que E/K tiene reducción aditiva potencialmente multiplicativa y $p = 2$. En este caso hemos visto que el índice de ramificación de cada extensión $K(E[m])/K$ puede ser divisible entre 2, pero no entre 4, ya que $K(E[m])$ está contenido en la cadena de extensiones $K \subset L \subset L(E[m])$, donde la primera es cuadrática y la segunda tiene ramificación dominada.

Veamos que $\delta(E/K)$ es un número natural. Llamemos $L = K(E[l])$. Podemos suponer que el cuerpo de restos de K es algebraicamente cerrado, con lo que $G(L/K) = G_0(L/K)$.

Si la extensión L/K es dominadamente ramificada, entonces $\delta(E/K) = 0$ y hemos terminado. En caso contrario, tenemos que $G_1(L/K)$ tiene orden 2. Por otra parte, el cociente $G(L/K)/G_1(L/K)$ es cíclico, por [CC 10.5].

Sea σ un generador del cociente y sea $G_1(L/K) = \{1, \tau\}$. Entonces, todo elemento de $G(L/K)$ es de la forma $\sigma^i\tau^j$, y se cumple que $\sigma\tau = \tau\sigma$ porque $G_1(L/K) \trianglelefteq G(L/K)$, luego $\sigma^{-1}\tau\sigma = \tau$. Esto implica que $G(L/K)$ es un grupo abeliano, y el teorema [CC 10.9] nos da entonces que g_0 divide a todos los índices i tales que $G_i > G_{i+1}$. Esto significa que, si en la definición de $\delta(E/K)$ agrupamos todos los sumandos correspondientes a grupos G_i iguales, el número de sumandos de cada grupo es múltiplo de g_0, por lo que cada uno de dichos grupos es un número natural, y $\delta(E/K)$ también lo es.

Consideremos ahora dos primos impares $l_1 \neq l_2$. Vamos a probar que la definición de δ con l_1 coincide con la definición con l_2. Sea $q \in K^*$ tal que

$|q| < 1$ y $j(E_q) = j(E)$. Observemos que K contiene a las raíces de la unidad de orden $l_1 l_2$, porque la extensión ciclotómica de orden $l_1 l_2$ es no ramificada y K no tiene extensiones no ramificadas. Por consiguiente, si α es una raíz del polinomio $X^{l_1 l_2} - q$, la extensión $K(\alpha)/K$ es finita de Galois (puesto que contiene a todas las demás raíces, que resultan de multiplicar α por las raíces de la unidad), y es dominadamente ramificada por [CC 2.44].

Si cambiamos K por $K(\alpha)$, de acuerdo con el teorema 13.31, estamos multiplicando $\delta(E/K)$ por el grado $|K(\alpha) : K|$ (tanto para el cálculo con l_1 como para el cálculo con l_2), luego, para probar la igualdad, podemos suponer que K contiene a las raíces de q de índice l_1 y l_2.

Hemos visto que, a través de la aplicación de Tate, los puntos de $E_q[l_i]$ se corresponden con productos ζQ^j, donde $\zeta \in K^*$ es una raíz l_i-ésima de la unidad, y $Q \in K^*$ es una raíz l_i-ésima de q. Por consiguiente $E_q[l_i] \subset E_q(K)$, para $i = 1, 2$.

Consideremos de nuevo la extensión cuadrática L/K dada por 12.16, para la cual $E_L \cong E_{qL}$. Como estamos suponiendo que E tiene reducción aditiva y E_{qL} tiene reducción multiplicativa, la extensión ha de ser ramificada. El isomorfismo implica que $E[l_i] \subset E(L)$.

Por otra parte, 12.19 implica que $E(K)[l_i] = 0$. En efecto, cada $P \in E[l_i]$ es la imagen por el isomorfismo $E_{qL} \cong E_L$ de un punto $P' \in E_q[m]$, y éste es la imagen por la aplicación de Tate de un punto de la forma $\zeta Q^j \in K^*$, donde ζ es una raíz l_i-ésima de la unidad y Q es una raíz l_i-ésima de q. Según 12.19, se cumple que $P \in E(K)$ si y solo si $\mathrm{N}(\zeta Q^j) = \zeta^2 Q^{2j} \in q^{\mathbb{Z}}$.

Ahora bien, si $\zeta^2 Q^{2j} = q^m$, elevando a l_i vemos que $q^{2j} = q^{l_1 m}$, luego $l_1 m = 2j$, luego la igualdad original es $\zeta^2 = 1$, luego $\zeta = 1$ (porque l_i es impar). Además $l_i \mid m$, con lo que el punto original es $\zeta Q^j \cong 1$ (mód $q^{\mathbb{Z}}$), que corresponde al elemento neutro de $L^*/q^{\mathbb{Z}}$, luego P es el elemento neutro de $E[l_i]$.

Esto implica que $K \subsetneq K(E[l_i]) \subset L$, luego $L = K(E[l_1]) = K(E[l_2])$. Además, $G(L/K) = G_1(L/K)$ cumple que $E[l_i]^{G_1} = 0$. Por último, si

$$G_1 = \cdots = G_v > G_{v+1} = 1,$$

entonces $\delta(E/K) = 2v$, tanto para l_1 como para l_2. Esto termina la prueba del teorema 13.28. ∎

Teorema 13.33 *Si $\phi : E_1 \longrightarrow E_2$ es una isogenia no nula entre dos curvas elípticas sobre K, entonces $\delta(E_1/K) = \delta(E_2/K)$.*

Demostración: Por 13.7 sabemos que ambas curvas tienen el mismo tipo de reducción, así como que éste variará de igual modo tras una extensión de constantes. Por consiguiente, si una tiene potencialmente buena reducción, lo mismo le sucederá a la otra, y en tal caso, la menor extensión L/K tal que E_{iL}/L tiene buena reducción es la misma para ambas. En la prueba del teorema 13.28 hemos visto que $E[l]^{G_i} = 0$ si y sólo si $G_i \neq 1$, de donde se sigue inmediatamente la igualdad de los invariantes.

Consideremos ahora el caso en que ambas curvas tienen reducción multiplicativa potencial. No perdemos generalidad si suponemos que el cuerpo de restos

de k es algebraicamente cerrado. En virtud del teorema 13.31, podemos sustituir K por cualquier extensión dominadamente ramificada, pues esto modificará del mismo modo los invariantes de ambas curvas.

Sea $q_i \in K$ tal que $j(E_{q_i}) = j(E_i)$. Igual que hemos hecho en la prueba del teorema 13.28, podemos extender K de modo que contenga las raíces l-ésimas de q_i. Sea L/K la extensión cuadrática tal que $T_{q_1} \cong E_{1L}$. Entonces $E_{2,L}$ tiene también reducción multiplicativa (necesariamente racional), luego también se cumple que $T_{q_2} \cong E_{2,L}$, y en la prueba del teorema 13.28 hemos visto que, en estas circunstancias, se cumple que $K(E_1[l]) = L = K(E_2[l])$, así como que $E_1[l]^{G_1} = 0 = E_2[l]^{G_1}$. De aquí se sigue inmediatamente la igualdad de los invariantes. ∎

13.6 El conductor de una curva elíptica

Conviene reunir en un único término los dos invariantes $\epsilon(E/K)$ y $\delta(E/K)$ que hemos asociado a una curva elíptica:

Definición 13.34 Si E/K es una curva elíptica, definimos el *exponente del conductor* de E/K como

$$f(E/K) = \epsilon(E/K) + \delta(E/K).$$

Los teoremas 13.6 y 13.32 se combinan en el teorema siguiente:

Teorema 13.35 *Sea E/K una curva elíptica y sea p la característica del cuerpo de restos de K.*

a) E/K tiene buena reducción si y sólo si $f(E/K) = 0$.

b) E/K tiene reducción multiplicativa si y sólo si $f(E/K) = 1$.

c) E/K tiene reducción aditiva si y sólo si $f(E/K) \geq 2$.

Además, en el último caso, se cumple $f(E/K) = 2$ siempre que $p > 3$.

Similarmente, los teoremas 13.7 y 13.33 se combinan en el teorema siguiente:

Teorema 13.36 *Si $\phi : E_1 \longrightarrow E_2$ es una isogenia no nula entre dos curvas elípticas sobre K, entonces $f(E_1/K) = f(E_2/K)$.*

Ahora podemos reunir la información local contenida en los exponentes $f(E/K)$ en el concepto global de conductor, definido para curvas elípticas sobre cuerpos de cocientes de dominios de Dedekind (no necesariamente locales):

Definición 13.37 Sea K el cuerpo de cocientes de un dominio de Dedekind D de característica 0 y tal que, para cada divisor primo $\mathfrak{p}$ de D, el cuerpo de restos $k_\mathfrak{p} = D/\mathfrak{p}$ sea perfecto. Si E/K es una curva elíptica, para cada primo $\mathfrak{p}$ de D podemos considerar la compleción $K_\mathfrak{p}$ de K, que es un cuerpo métrico

completo de característica 0 con cuerpo de restos perfecto, así como la curva elíptica $E_{K_\mathfrak{p}}$, que —tal y como hemos razonado al principio del capítulo— tiene el mismo tipo (y subtipo) de reducción que E/K sobre $\mathfrak{p}$. Definimos

$$f_\mathfrak{p}(E/K) = f(E_{K_\mathfrak{p}}/K_\mathfrak{p}).$$

En virtud de los teoremas 8.22 y 13.35, tenemos que $f_\mathfrak{p}(E/K) = 1$ salvo a lo sumo para un número finito de primos, por lo que podemos definir el *conductor* de E/K sobre D como el ideal de D dado por

$$\mathfrak{f}(E/K) = \prod_\mathfrak{p} \mathfrak{p}^{f_\mathfrak{p}(E/K)}.$$

Es claro que el teorema 13.36 es válido también globalmente: dos curvas elípticas isógenas (sobre un dominio de Dedekind) tienen el mismo conductor.

Aparentemente, el cálculo del conductor (o, más concretamente, el cálculo de los exponentes del conductor en primos con cuerpo de restos de característica 2 o 3) es complicado, porque exige calcular invariantes de Swan, que dependen de los grupos de ramificación de ciertas extensiones de cuerpos. Sin embargo, en la práctica el cálculo es muy simple gracias a la llamada *fórmula de Ogg,* según la cual, si E/K es una curva elíptica y $\mathcal{E}/S$ es su modelo regular minimal, entonces

$$v_\mathfrak{p}(\Delta_\mathfrak{p}) = f_\mathfrak{p}(E/K) + m_\mathfrak{p} - 1,$$

donde $\Delta_\mathfrak{p}$ es el discriminante minimal de E/K en $\mathfrak{p}$ y $m_\mathfrak{p}$ es el número de componentes irreducibles de la fibra cerrada $\mathcal{E}_\mathfrak{p}$ contadas con su multiplicidad (de modo que, por ejemplo, los tipos I_0^*, $\mathrm{I}_{0,1}^*$ y $\mathrm{I}_{0,2}^*$ tienen todos $m = 5$).

Así pues, el conductor de una curva elíptica puede calcularse con el algoritmo de Tate. La fórmula de Ogg no es fácil de probar. El lector puede comprobarla trivialmente para primos con cuerpo de restos de característica $p > 3$. Sólo tiene que combinar la tabla del teorema 9.1 para calcular $v_\mathfrak{p}(\Delta_\mathfrak{p})$ y la tabla 8.1 que nos da el valor de $m_\mathfrak{p}$ para cada tipo de reducción. Naturalmente, éste es precisamente el caso en que la fórmula carece de interés, pues si $p > 3$ tenemos que $f_\mathfrak{p}(E/K) = \epsilon_\mathfrak{p}(E/K)$ se calcula trivialmente sin necesidad de la fórmula.

Esto nos permite concebir al invariante de Swan $\delta(E/K)$ como la corrección de $\epsilon(E/K)$ necesaria para que la fórmula de Ogg sea válida también cuando $p = 2, 3$.

El nombre de "fórmula de Ogg" no parece muy afortunado: Tate la había constatado ya para $p > 3$, Ogg publicó una demostración válida cuando $p = 3$, pero incompleta en el caso $p = 2$, y la primera demostración general se debe a Saito, aunque aquí no estamos en condiciones de exponerla.

Bibliografía

[1] Kunz, E. *Introducction to Commutative Algebra and Algebraic Geometry.* Birkhäuser, Boston, 1991.

[2] Liu, Q. *Algebraic Geometry and Arithmetic Curves.* Oxford University Press, 2002.

[3] Matsumura, H. *Commutative Algebra.* Benjamin, New York, 1980.

[4] Matsumura, H. *Commutative ring theory.* Cambridge University Press, 1986.

[5] Ogg, A.P. *Elliptic Curves and Wild Ramification,* Amer. J. Math. 89 (1967), 1–21.

[6] Serre, J.P. *Local Fields,* Springer, New York, 1979.

[7] Serre, J.P. *Linear Representations of Finite Groups,* Springer, New York, 1977.

[8] Silverman, J. *Advanced Topics in the Arithmetic of Elliptic Curves,* Grad. Text Math., 151, Springer, New York, 1994.

[9] Waterhouse, W.C. *Introduction to Affine Group Schemes.* Springer, New York, 1979.

Índice de Materias

analíticamente no ramificado, 63
anillo de coeficientes, 33
anulador, 193
Artin (función de), 438

birracional
    aplicación, 183
    equivalencia, 202
    homomorfismo, 190

carácter, 362
    virtual, 381
Castelnuovo (criterio de), 213
catenario
    anillo, 53
    esquema, 55
centro, 186, 361
    de un carácter, 390
conductor, 452
    exponente del, 451
conjugados, 361
constructible, 17
contracción, 189
corte transversal, 171
cuasiexcelente (anillo), 88
cuerpo de coeficientes, 31
curva, 99
cúspide, 259

Dedekind (esquema de), 126
descomposición primaria, 4
desingularización, 190
    canónica, 192
    minimal, 221
dominación, 202

elemental (grupo), 380
elevación, 23
elíptica (curva), 124
equicaracterístico, 30
esquema de grupos, 326
excelente
    anillo, 87
    esquema, 90
explosión, 136, 140

fielmente plano, 15

G (propiedad), 80
grado, 106
grado (de una representación), 357
grupo
    aditivo, 327
    de inercia, 423
    multiplicativo, 327
gráfica, 183, 184

intersección (número de), 170, 176
irreducible (representación), 360

J (propiedad), 70, 72
jacobiana (matriz), 40
jacobiano (criterio), 100

lugar excepcional, 183

minimal (superficie), 217
modelo, 128
    de Weierstrass, 131
        minimal, 253
    regular minimal, 219
multiplicidad, 104

Nagata (anillo de), 59
nodo, 260

normal (anillo), 11
Néron (modelo de), 345
Néron–Ogg–Shafarevich (criterio), 431
núcleo (de un carácter), 364

Ogg, fórmula de, 452

primario (submódulo), 3

racional (aplicación), 183
reducción, 258, 350
    potencialmente buena o multiplicativa, 415
relativamente minimal (superficie), 204
representación
    fiel, 357
    inducida, 374
    irreducible, 360
    lineal, 357
    matricial, 357
    regular, 359
    trivial, 359

Schur (lema de), 365
Selmer (curva de), 159
semilocal (anillo), 8
separable (álgebra), 312
suave, 23, 48
subrepresentación, 360
sucesión canónica, 192
superficie
    aritmética, 126
    fibrada, 126
superresoluble (grupo), 379
Swan
    función de, 443
    invariante de, 444

tangencia, 171
Tate
    aplicación de, 404
    curva de, 400
Teorema chino del resto, 8
transformada estricta, 152
transformada total, 184

universalmente catenario
    anillo, 53
    esquema, 55

valoración normal, 186

Weierstrass
    ecuación de, 119
    modelo de, 131