El teorema de Kronecker-Weber

Artur TRAVESA

Seminari de Teoria de Nombres (UB-UAB-UPC)

CSIC, Madrid
Septiembre de 2008

Índice general

Introducción

El sintagma nominal "teoría de números" es una perífrasis de la palabra "aritmética", de manera que las dos expresiones tienen el mismo significado. En efecto, desde el punto de vista etimológico, la palabra aritmética deriva de la latina *arithmetica* que, a su vez, proviene del griego *ἀριθμητική τέχνη* (literalmente, arte numérico), derivada del adjetivo *ἀριθμητικός* (relativo al número), y, éste, del substantivo *ἀριθμός* (número). Así, pues, la aritmética es el estudio de los números.

Para hacer ese estudio de los números se utilizan métodos y técnicas diferentes que, a su vez, dan lugar a diversas ramas de la aritmética: la teoría algebraica de números, la teoría analítica, la probabilística, la heurística y computacional, la geometría aritmética, ... Para ser precisos, este curso es fundamentalmente un curso de *teoría algebraica de números algebraicos*, aunque en su desarrollo aparecerán también números no algebraicos y en algunas partes se utilizarán técnicas no propiamente algebraicas.

La teoría algebraica de números tiene dos objetivos principales: por un lado, la construcción de una teoría general de los cuerpos de números algebraicos que permita su clasificación completa y la descripción de su aritmética y, por el otro, el estudio de las aplicaciones de esta teoría general a cuestiones concretas: por ejemplo, ecuaciones diofánticas, multiplicación compleja de funciones abelianas i elípticas, integración de diferenciales algebraicas, teorías de codificación y criptografía, ...

Su estudio se basa en diversas teorías y metodologías (la teoría de Galois, la de la ramificación, el análisis complejo, el análisis p-ádico, ...) y usa herramientas diferentes (funciones analíticas, curvas elípticas, formas modulares, variedades abelianas, ...). Algunas de estas técnicas y herramientas se utilizarán en este curso; concretamente, algunas que permiten la consecución del objetivo que nos proponemos de manera natural: una demostración del

Teorema de Kronecker-Weber sobre el cuerpo de los números racionales.

El teorema de Kronecker-Weber se sabe demostrar de maneras diversas; una de las más corrientes es obtenerlo a partir de la teoría de cuerpos de clases. Otra, también muy extendida, es obtenerlo a partir de su análogo local; es decir, a partir del teorema sobre los cuerpos de los números p-ádicos, para todo número primo p.

Obtener el teorema de Kronecker-Weber a partir de la teoría de cuerpos de clases implica, óbviamente, establecer previamente esta teoría; y esto queda fuera del alcance de un primer curso de teoría algebraica de números. Obtenerlo a partir de su análogo local, si bien es posible en un primer curso de teoría algebraica de números, no es lo más razonable en un curso de quince o dieciséis horas, en el cual parece más adecuado trabajar los métodos más básicos de la teoría antes que los más elaborados o específicos.

Por suerte, entre las distintas posibilidades para obtener este teorema, hay una tercera que permite introducir algunos objetos y algunas técnicas básicas de la teoría algebraica de números y dar una demostración completa en un tiempo relativamente corto: consiste en establecer y usar una parte de la teoría de la ramificación superior. Y esta es la que hemos elegido; así, el teorema de Kronecker-Weber puede servir como primer ejemplo y a la vez como motivación de la teoría de cuerpos de clases o de otros aspectos de la teoría de la ramificación.

Y, a la vez, saber que existe un análogo local que se puede obtener en pocas horas más, puede servir de motivación para continuar el estudio de la teoría algebraica de números en sus aspectos locales.

Capítulo 1

Ley de reciprocidad cuadrática

1.1. Teoría de Galois

Sea $L|K$ una extensión finita de cuerpos. El grupo de los automorfismos de L que dejan fijos los elementos de K se llama el grupo de Galois de la extensión $L|K$ y se denota por $\mathrm{Gal}\,(L|K)$; es un grupo finito de orden menor o igual que el grado de la extensión. Se dice que la extensión $L|K$ es de Galois cuando se satisface la igualdad; equivalentmente, cuando la extensión es normal y separable. Una extensión de Galois $L|K$ se llama abeliana (respectivamente cíclica, resoluble, nilpotente) cuando el grupo de Galois $\mathrm{Gal}\,(L|K)$ es un grupo abeliano (respectivamente cíclico, resoluble, nilpotente).

Si $L|K$ es una extensión de Galois y K' es un subcuerpo de L que contiene K, la extensión $L|K'$ también es una extensión de Galois y el grupo $\mathrm{Gal}\,(L|K')$ es un subgrupo de $\mathrm{Gal}\,(L|K)$; una condición necesaria y suficiente para que la extensión $K'|K$ sea de Galois es que $\mathrm{Gal}\,(L|K')$ sea un subgrupo normal de $\mathrm{Gal}\,(L|K)$; en este caso, el grupo de Galois de la extensión $K'|K$ se identifica de manera natural con el grupo cociente $\mathrm{Gal}\,(L|K)\,/\mathrm{Gal}\,(L|K')$, puesto que se tiene la sucesión exacta de grupos

$$1 \longrightarrow \mathrm{Gal}\,(L|K') \xrightarrow{inc} \mathrm{Gal}\,(L|K) \xrightarrow{res} \mathrm{Gal}\,(K'|K) \longrightarrow 1$$

en donde res es el morfismo dado por restricción a K' de los automorfismos de L i inc es la inclusión como subconjunto. Por otro lado, hay una correspondencia biyectiva entre el conjunto de los subcuerpos K' de L que contienen

K y el conjunto de los subgrupos de $\mathrm{Gal}\,(L|K)$; esta correspondencia se obtiene asignando a cada cuerpo K' el grupo $\mathrm{Gal}\,(L|K')$. Recíprocamente, a cada subgrupo $H \subseteq \mathrm{Gal}\,(L|K)$ le corresponde el cuerpo L^H formado por los elementos de L que son fijos por todos los automorfismos de H.

Sean $L_1|K$ y $L_2|K$ dos extensiones de Galois finitas dentro de una misma clausura algebraica del cuerpo K. La extensión composición $L_1L_2|K$ y la extensión intersección $L_1 \cap L_2|K$ son entonces extensiones de Galois; el grupo de Galois de la composición se puede identificar con un subgrupo del grupo producto $\mathrm{Gal}\,(L_1|K) \times \mathrm{Gal}\,(L_2|K)$. Esta identificación se hace asignando a cada K-automorfismo σ de L_1L_2 la pareja de automorfismos que se obtiene por restricción de σ a cada uno de los cuerpos L_i. Además, el grupo de Galois $\mathrm{Gal}\,(L_1L_2|L_1 \cap L_2)$ es isomorfo de manera natural al producto $\mathrm{Gal}\,(L_1|L_1 \cap L_2) \times \mathrm{Gal}\,(L_2|L_1 \cap L_2)$. De esta manera obtenemos una sucesión exacta

$$1 \longrightarrow \mathrm{Gal}\,(L_1|L_1 \cap L_2) \times \mathrm{Gal}\,(L_2|L_1 \cap L_2) \longrightarrow \mathrm{Gal}\,(L_1L_2|K) \longrightarrow$$

$$\longrightarrow \mathrm{Gal}\,(L_1 \cap L_2|K) \longrightarrow 1.$$

En particular, si $L_1 \cap L_2 = K$, entonces las extensiones $L_1|K$, L_2/K son linealmente disjuntas y el grupo de Galois $\mathrm{Gal}\,(L_1L_2|K)$ es isomorfo al producto de los grupos $\mathrm{Gal}\,(L_1|K)$ y $\mathrm{Gal}\,(L_2|K)$.

Por otro lado, si $L|K$ es una extensión de Galois y $K'|K$ es una extensión cualquiera, entonces la extensión $LK'|K'$ es de Galois y $\mathrm{Gal}\,(LK'|K')$ es un subgrupo de $\mathrm{Gal}\,(L|K)$. En cambio, el hecho de que dos extensiones $K'|K$ y $L|K'$ sean de Galois no implica que la extensión $L|K$ también lo sea.

1.2. Cuerpos ciclotómicos

Consideremos una clausura algebraica $\overline{\mathbb{Q}}$ del cuerpo $\mathbb{Q}$ de los números racionales y sea $\zeta \in \overline{\mathbb{Q}}$ una raíz primitiva n-ésima de la unidad. La extensión $\mathbb{Q}(\zeta)|\mathbb{Q}$ se llama la n-ésima extensión ciclotómica de $\mathbb{Q}$; es una extensión de Galois y su grupo de Galois se identifica de manera natural con el grupo multiplicativo de los elementos inversibles del anillo $\mathbb{Z}/n\mathbb{Z}$. En efecto, si σ es un automorfismo de $\mathbb{Q}(\zeta)$, entonces $\sigma(\zeta)$ ha de ser también una raíz primitiva n-ésima de la unidad y, por tanto, de la forma $\sigma(\zeta) = \zeta^{\chi(\sigma)}$, donde

$\chi(\sigma)$ es un número entero definido módulo n y coprimo con n que no depende de la elección de la raíz primitiva ζ; eso permite definir una aplicación $\mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q}) \xrightarrow{\chi} (\mathbb{Z}/n\mathbb{Z})^*$ que resulta ser un isomorfismo de grupos. Por tanto, la extensión $\mathbb{Q}(\zeta)|\mathbb{Q}$ es abeliana.

Análogamente, si k es un cuerpo cualquiera y $\zeta \in \overline{k}$ es una raíz primitiva n-ésima de la unidad, también $k(\zeta)|k$ es una extensión abeliana; en este caso, el morfismo $\mathrm{Gal}\,(k(\zeta)|k) \xrightarrow{\chi} (\mathbb{Z}/n\mathbb{Z})^*$ es inyectivo, aunque no necesariamente exhaustivo.

Pongamos $n = p^r n'$, con $r \geq 0$, $n' \geq 1$ un número entero, y p un número primo que no divide n'. Entonces $\zeta^{n'}$ es una raíz primitiva p^r-ésima de la unidad y $\mathbb{Q}(\zeta^{n'})|\mathbb{Q}$ es una subextensión de $\mathbb{Q}(\zeta)|\mathbb{Q}$. El isomorfismo χ, definido para cada número entero positivo n, es compatible con los morfismos de restricción y de reducción

$$\mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q}) \xrightarrow{res} \mathrm{Gal}\left(\mathbb{Q}(\zeta^{n'})|\mathbb{Q}\right),$$

$$(\mathbb{Z}/n\mathbb{Z})^* \xrightarrow{red} (\mathbb{Z}/p^r\mathbb{Z})^*,$$

de manera que hay un diagrama conmutativo de morfismos de grupos abelianos

$$\begin{array}{ccc} \mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q}) & \xrightarrow{\chi} & (\mathbb{Z}/n\mathbb{Z})^* \\ res \downarrow & & \downarrow red \\ \mathrm{Gal}\left(\mathbb{Q}(\zeta^{n'})|\mathbb{Q}\right) & \xrightarrow{\chi} & (\mathbb{Z}/p^r\mathbb{Z})^*. \end{array}$$

Por otra parte, la extensión $\mathbb{Q}(\zeta)|\mathbb{Q}$ es la composición de las extensiones linealmente disjuntas $\mathbb{Q}(\zeta^{p^r})|\mathbb{Q}$ y $\mathbb{Q}(\zeta^{n'})|\mathbb{Q}$ y, por tanto, para los grupos de Galois se tiene que $\mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q}) \simeq \mathrm{Gal}\left(\mathbb{Q}(\zeta^{p^r})|\mathbb{Q}\right) \times \mathrm{Gal}\left(\mathbb{Q}(\zeta^{n'})|\mathbb{Q}\right)$. Eso permite en muchos casos reducir el estudio de los cuerpos ciclotómicos al caso de los engendrados por raíces primitivas de la unidad de orden potencia de un número primo.

Una de las propiedades importantes de las extensiones ciclotómicas de $\mathbb{Q}$ viene reflejada en el siguiente

Teorema 1.2.1. (Kronecker-Weber) *Sea $K|\mathbb{Q}$ una extensión abeliana finita. Entonces, existe una raíz de la unidad ζ tal que K es un subcuerpo del cuerpo ciclotómico $\mathbb{Q}(\zeta)$.*

Uno de los objetivos de este curso es dar una demostración de este teorema.

1.3. Períodos de Gauss

Sean p un número primo impar y ζ una raíz primitiva p-ésima de la unidad. El grupo de Galois $\mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q})$ es cíclico de orden $p-1$, de manera que hay una correspondencia biyectiva entre el conjunto de las subextensiones de la extensión ciclotómica $\mathbb{Q}(\zeta)|\mathbb{Q}$ y el conjunto de los divisores positivos d de $p-1$. El objetivo inmediato es dar un elemento primitivo para cada uno de los subcuerpos de $\mathbb{Q}(\zeta)$; es decir, dar un generador de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$.

Sea g un generador del grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})^*$. Entonces, el automorfismo σ de $\mathbb{Q}(\zeta)$ definido por la fórmula $\sigma(\zeta) := \zeta^g$ es un generador del grupo $\mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q})$. Por comodidad de escritura, para todo número entero i pondremos $\zeta_i := \zeta^{g^i}$. La demostración del resultado siguiente no presenta ninguna dificultad.

Lema 1.3.1. *Sean i, j números enteros cualesquiera. Entonces,*

$$\zeta_i = \zeta_j \iff i \equiv j \pmod{p-1}; \qquad \sigma^j(\zeta_i) = \zeta_{i+j}. \square$$

Definición 1.3.2. Sea n un divisor cualquiera de $p-1$. Para todo número entero i, $0 \le i \le n-1$, llamaremos i-ésimo n-período de ζ relativo a g al elemento de $\mathbb{Q}(\zeta)$

$$\eta_i := \sum_{j=0}^{d-1} \sigma^{jn}(\zeta_i) = \sum_{j=0}^{d-1} \zeta_{i+jn},$$

donde $d := (p-1)/n$.

Individualmente, los n-períodos dependen de la elección de ζ y de g. El resultado siguiente precisa mejor de qué forma se produce esa dependencia.

Proposición 1.3.3. *El conjunto $\{\eta_0, \eta_1, \ldots, \eta_{n-1}\}$ no depende ni de la elección del generador g de $(\mathbb{Z}/p\mathbb{Z})^*$ ni de la elección de la raíz primitiva p-ésima de la unidad ζ. Además, el período η_0 tampoco depende de la elección de g, y los diferentes η_i son los n-períodos η_0' associados a las diferentes raíces primitivas p-ésimas de la unidad ζ'.*

Demostración: Puesto que n divide al orden de $G := (\mathbb{Z}/p\mathbb{Z})^*$, los exponentes g^{i+jn} de ζ en el n-período η_i forman una clase lateral de G módulo el subgrupo $\langle g^n \rangle$; y puesto que G es cíclico, este subgrupo no depende del

generador g elegido en G. Por tanto, las clases laterales tampoco dependen de g. Esto demuestra que el período η_0 y el conjunto $\{\eta_0, \eta_1, \ldots, \eta_{n-1}\}$ no dependen de cual sea el generador g de G.

Por otro lado, si cambiamos ζ por otra raíz primitiva p-ésima de la unidad ζ', podemos escrivir $\zeta' = \zeta^{g^\alpha}$ para un cierto entero α; entonces, para todo entero i, $0 \leq i \leq n-1$, es

$$\eta_i' = \sum_{j=0}^{d-1} \zeta'_{i+jn} = \sum_{j=0}^{d-1} \zeta_{\alpha+i+jn} = \eta_{\alpha+i}.$$

Por tanto, los períodos η_i se pueden obtener como los períodos η_0 asociados a las diferentes raíces primitivas p-ésimas de la unidad. □

Sea, ahora, $K|\mathbb{Q}$ una subextensión de $\mathbb{Q}(\zeta)|\mathbb{Q}$. El grado $n := [K : \mathbb{Q}]$ es un divisor de $p-1$ y K es el cuerpo fijo por el único subgrupo $H \subseteq \mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q})$ de índice n. Por tanto, el cuerpo K está generado sobre $\mathbb{Q}$ por los coeficientes del polinomio irreducible de ζ sobre el cuerpo K (cf. el ejercicio siguiente).

Ejercicio 1.3.4. Sea $L|k$ una extensión de Galois de cuerpos y sea $\theta \in L$ un elemento primitivo de la extensión. Entonces, todo subcuerpo $K \subseteq L$ que contiene k se obtiene a partir de k al adjuntar los coeficientes del polinomio $\mathrm{Irr}(\theta, K)$.

Ahora bien, H es el grupo $\langle \sigma^n \rangle$, de manera que

$$\mathrm{Irr}(\zeta, K) = \prod_{\tau \in H} (X - \tau(\zeta)) = \prod_{j=0}^{d-1} \left(X - \sigma^{jn}(\zeta)\right),$$

donde $d := (p-1)/n$; los coeficientes de este polinomio son los valores de los polinomios simétricos elementales en los elementos $x_j := \sigma^{jn}(\zeta) = \zeta_{jn}$, $0 \leq j \leq d-1$; es decir, los coeficientes son los números algebraicos $s_k := s_k(x_0, x_1, \ldots, x_{d-1})$, $1 \leq k \leq d$.

El cuerpo generado sobre $\mathbb{Q}$ por (los valores de) los polinomios simétricos elementales $s_k(x_0, x_1, \ldots, x_{d-1})$ es el mismo que el engendrado por (los valores de) los polinomios de Newton $t_k := t_k(x_0, x_1, \ldots, x_{d-1}) := \sum_{j=0}^{d-1} x_j^k$ (cf. [B-M-T, ej.50]). Estos últimos son exactamente los n-períodos de ζ relativos a un cierto

generador g' de $(\mathbb{Z}/p\mathbb{Z})^*$: en efecto, puesto que $1 \leq k < p$, el número entero k es una unidad de $(\mathbb{Z}/p\mathbb{Z})^*$ y se puede escribir en la forma $k = g^i$ para un cierto número entero i; entonces, $t_k = \eta_i$. Por tanto, $K \subseteq \mathbb{Q}(\eta_0, \eta_1, \ldots, \eta_{n-1})$. Por otro lado, de la definición de los períodos es claro que $\sigma^n(\eta_i) = \eta_i$, de manera que $\eta_i \in K$, ya que K es el cuerpo fijo por $\langle \sigma^n \rangle$. Eso demuestra la igualdad $K = \mathbb{Q}(\eta_0, \eta_1, \ldots, \eta_{n-1})$.

Finalmente, se satisface la igualdad $\sigma^j(\eta_i) = \eta_{i+j}$, para toda pareja de enteros i, j; por tanto, los períodos η_i son todos conjugados; puesto que $\mathbb{Q}(\eta_i) \subseteq \mathbb{Q}(\zeta)$, la extensión $\mathbb{Q}(\eta_i)|\mathbb{Q}$ es de Galois (y abeliana), de manera que $K = \mathbb{Q}(\eta_i)$. Hemos demostrado, pues, el siguiente

Teorema 1.3.5. *Sean p un número primo impar, ζ una raíz primitiva p-ésima de la unidad, $K \subseteq \mathbb{Q}(\zeta)$ un subcuerpo cualquiera y $n := [K : \mathbb{Q}]$ el grado. Entonces, para todo entero i, $0 \leq i \leq n-1$, podemos escribir $K = \mathbb{Q}(\eta_i)$, donde η_i denota el i-ésimo n-período de ζ relativo a cualquier generador del grupo $(\mathbb{Z}/p\mathbb{Z})^*$.*

Observación 1.3.6. La parte final de esta demostración se puede hacer de manera más sencilla (cf. [vdW, chap.VIII,§ 4]; pero hemos hecho ésta porque de ella se obtiene una generalización inmediata al caso en que la raíz de la unidad ζ es de orden potencia de p.

En particular, y puesto que p es impar, podemos pensar en la única subextensión cuadrática $K|\mathbb{Q}$ de $\mathbb{Q}(\zeta_p)|\mathbb{Q}$. ¿Podemos describir este cuerpo fácilmente? La respuesta a esa pregunta es el objetivo de las secciones siguientes.

1.4. Caracteres de Dirichlet

Sea G un grupo abeliano finito. El grupo $\widehat{G} := \mathrm{Hom}(G, \mathbb{C}^*)$ se llama el grupo dual o de los caracteres (complejos) de G. Si $\chi : G \longrightarrow \mathbb{C}^*$ es un carácter, su imagen está formada por raíces de la unidad, ya que G es de orden finito. Aún más, si n denota el exponente del grupo abeliano G (si se quiere, el generador positivo del ideal anulador del $\mathbb{Z}$-módulo G), entonces la imagen de χ está formada por raíces n-ésimas de la unidad.

Proposición 1.4.1. *Sea G un grupo abeliano finito. Aleshores G es isomorfo (no canónicamente) a $\widehat{G}$ y es canónicamente isomorfo a $\widehat{\widehat{G}}$.*

Demostración: Cf. [B-M-T, ej.265]. □

Proposición 1.4.2. (Relaciones de ortogonalidad de los caracteres) *Sea G un grupo abeliano finito y sea g su orden. Entonces:*

$$\sum_{\sigma\in G}\chi(\sigma)=\begin{cases} g & si\ \chi=1,\\ 0 & si\ \chi\neq 1,\end{cases}\qquad \chi\in\widehat{G},$$

$$\sum_{\chi\in\widehat{G}}\chi(\sigma)=\begin{cases} g & si\ \sigma=1,\\ 0 & si\ \sigma\neq 1,\end{cases}\qquad \sigma\in G.$$

Demostración: Cf. [B-M-T, ej.266] □

Proposición 1.4.3. *Sea $0\longrightarrow G'\longrightarrow G\longrightarrow G''\longrightarrow 0$ una sucesión exacta de grupos abelianos finitos. Entonces, la sucesión $1\longrightarrow\widehat{G''}\longrightarrow\widehat{G}\longrightarrow\widehat{G'}\longrightarrow 1$ que se obtiene al aplicar el functor $\mathrm{Hom}(*,\mathbb{C}^*)$ es exacta.*

Demostración: Ejercicio. □

Observación 1.4.4. En lugar de utilizar $\mathbb{C}^*$ podríamos haber utilizado cualquier cuerpo algebraicamente cerrado de característica cero; en particular, $\overline{\mathbb{Q}}$. Aún más, puesto que la imagen está formada por raíces de la unidad, es suficiente que el cuerpo que se toma contenga todas esas raíces de la unidad. Por otro lado, si p es un número primo que no divide al orden del grupo G, podemos tomar $\overline{\mathbb{F}}_p$ en lugar de $\mathbb{C}$ y los resultados son los mismos.

Por comodidad de escritura, conviene escribir $G(n)$ para designar el grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$ de los elementos inversibles del anillo $\mathbb{Z}/n\mathbb{Z}$.

Definición 1.4.5. Se llaman caracteres de Dirichlet módulo n los caracteres (complejos) de $G(n)$.

Sea χ un carácter de Dirichlet módulo n. Para todo múltiplo m de n disponemos de un morfismo exhaustivo de grupos $G(m)\xrightarrow{red}G(n)$ dado por reducción y, por tanto, podemos pensar χ como un carácter de Dirichlet módulo m en la forma $G(m)\xrightarrow{red}G(n)\longrightarrow\mathbb{C}^*$.

Proposición 1.4.6. *Sea $\chi: G(n)\longrightarrow\mathbb{C}^*$ un carácter de Dirichlet módulo n. Supongamos que existen dos divisores d_1 y d_2 de n tales que χ es la composición de cada uno de los morfismos de reducción $G(n)\xrightarrow{red}G(d_i)$ con un*

carácter de Dirichlet $\chi_i : G(d_i) \longrightarrow \mathbb{C}^*$. *Sea* d *el máximo común divisor de* d_1 *y* d_2. *Entonces, existe un carácter de Dirichlet módulo* d, χ', *tal que* χ *es la composición de* χ' *con el morfismo de reducción* $G(n) \xrightarrow{red} G(d)$.

Demostración: Podemos suponer que n divide al producto $d_1 d_2$ (o, si se quiere, que n es el mínimo común múltiplo de d_1 y d_2). Puesto que χ_i está definido módulo d_i, para todo entero a primo con n y tal que $a \equiv 1 \pmod{d_i}$ es $\chi(a) = \chi_i(a) = 1$. Hay que ver que si $a \equiv 1 \pmod{d}$ y a es primo con n, entonces $\chi(a) = 1$. Pero el subgrupo de $G(n)$ generado por la reunión de los subgrupos $\{a \in G(n) : a \equiv 1 \pmod{d_i}\}$, $i = 1$, 2, es el subgrupo $\{a \in G(n) : a \equiv 1 \pmod{d}\}$. En efecto, si escribimos $d = \lambda_1 d_1 + \lambda_2 d_2$, y si $a = 1 + \alpha d$, obtenemos que $a = 1 + \alpha\lambda_1 d_1 + \alpha\lambda_2 d_2 = (1 + \alpha\lambda_1 d_1)(1 + \alpha\lambda_2 d_2) - \alpha^2 \lambda_1 \lambda_2 d_1 d_2 \equiv (1 + \alpha\lambda_1 d_1)(1 + \alpha\lambda_2 d_2) \pmod{n}$; y si a es primo con n, también $1 + \alpha\lambda_i d_i$ ha de ser primo con n. Puesto que χ es trivial sobre cada uno de los subgrupos $\{a \in G(n) : a \equiv 1 \pmod{d_i}\}$, χ ha de ser trivial sobre el subgrupo $\{a \in G(n) : a \equiv 1 \pmod{d}\}$. Esto acaba la demostración. □

Corolario 1.4.7. *Sea* χ *un carácter de Dirichlet módulo* n. *Existe el menor número natural* f *divisor de* n *tal que* χ *es la composición de un carácter de Dirichlet módulo* f *con el morfismo de reducción* $G(n) \xrightarrow{red} G(f)$. □

Definición 1.4.8. Este menor número entero $f \geq 1$ se llama el conductor del carácter χ. Los caracteres de Dirichlet módulo n de conductor exactamente n se llaman caracteres de Dirichlet primitivos módulo n.

A menudo conviene pensar los caracteres de Dirichlet módulo n como aplicaciones de $\mathbb{Z}/n\mathbb{Z}$ e, incluso, como aplicaciones de $\mathbb{Z}$. Esto se puede hacer extendiendo a $\mathbb{Z}/n\mathbb{Z}$ la aplicación $\chi : G(n) \longrightarrow \mathbb{C}^*$ por la fórmula $\chi(a) := 0$ si $a \in \mathbb{Z}/n\mathbb{Z}$ no es inversible; y se extiende a $\mathbb{Z}$ simplemente componiendo con la aplicación de reducción $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, de manera que $\chi(a) = 0$ para todo número entero a tal que $\mathrm{mcd}(a, n) > 1$. Si se considera el caso en que χ es primitivo, entonces la igualdad $\chi(a) = 0$ se produce "tan poco" como es possible; solamente cuando a tiene factores primos comunes con el conductor. Cuando hablemos de un carácter de Dirichlet sin especificar su conductor ni su módulo de definición lo consideraremos siempre primitivo.

Así, solamente hay un carácter de Dirichlet trivial, χ_1; vale 1 sobre todos los números enteros; es el carácter de conductor 1.

Podemos multiplicar caracteres de Dirichlet. En efecto, si χ_1, χ_2 son caracteres de Dirichlet de conductores f_1, f_2, podemos definir el carácter producto $\chi_1\chi_2$ de la manera siguiente: consideremos, en primer lugar, el morfismo de grupos $\omega : G(\text{mcm}(f_1, f_2)) \longrightarrow \mathbb{C}^*$ definido por $\omega(a) := \chi_1(a)\chi_2(a)$. Entonces, ω es un carácter de Dirichlet y definimos $\chi_1\chi_2$ como el carácter primitivo asociado a ω. Esto permite hablar del grupo de los caracteres de Dirichlet, grupo que tiene como elemento neutro el carácter trivial. Además, el inverso de un carácter χ es el que se obtiene al componer χ con la conjugación compleja $\mathbb{C}^* \longrightarrow \mathbb{C}^*$; en efecto, para tota raíz de la unidad, ζ, se satisface que $\overline{\zeta} = \zeta^{-1}$, donde la barra indica el número complejo conjugado. En particular, un carácter y su inverso tienen el mismo conductor.

Ejercicio 1.4.9. Sean χ_1, χ_2 caracteres de Dirichlet primitivos de conductores respectivos f_1 y f_2. Supongamos que $\text{mcd}(f_1, f_2) = 1$. Entonces, el producto $\chi_1\chi_2$ es un carácter de Dirichlet de conductor $f_1 f_2$.

1.5. Símbolo de Legendre

Uno de los ejemplos más importantes de caracteres de Dirichlet lo proporciona el estudio de los cuadrados de los cuerpos finitos $\mathbb{F}_p$, con p un número primo impar.

La aplicación ${\mathbb{F}_p}^* \xrightarrow{\left(\frac{*}{p}\right)} \{\pm 1\} \subset \mathbb{C}^*$ definida por $\left(\frac{a}{p}\right) := 1$ si a es el cuadrado de un elemento de ${\mathbb{F}_p}^*$, $\left(\frac{a}{p}\right) = -1$ si a no es un cuadrado en $\mathbb{F}_p$, es un morfismo de grupos. se llama el símbolo de Legendre y es un carácter cuadrático de Dirichlet de conductor p.

En efecto, el núcleo de este morfismo es el subgrupo de los cuadrados de ${\mathbb{F}_p}^*$; por tanto, un subgrupo de índice 2 (el morfismo $\mathbb{F}_p^* \longrightarrow \mathbb{F}_p^{*2}$ de elevar al cuadrado tiene núcleo $\{\pm 1\}$, que es de cardinal 2 si $p \neq 2$). En consecuencia, el símbolo de Legendre $\left(\frac{*}{p}\right)$ no es el carácter trivial y está definido módulo el número primo impar p; esto implica que su conductor es p. Y, claramente, el cuadrado de este carácter es el carácter trivial.

Esto se traduce en las propiedades siguientes para el símbolo de Legendre:

$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, para todo par de números enteros a, b;

$\left(\frac{a^2}{p}\right) = 1$, para todo número entero a no divisible por p; y

$\left(\frac{a}{p}\right) = 0$, para todo número entero a divisible por p.

Proposición 1.5.1. (Criterio de Euler) *Sea p un número primo impar. Para todo número entero a se satisface la congruencia* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Demostración: Sea $b \in \overline{\mathbb{F}}_p$ un elemento tal que $b^2 = a$ (en $\overline{\mathbb{F}}_p$). Puesto que los elementos de ${\mathbb{F}_p}^*$ son las raíces del polinomio $X^{p-1} - 1$ en $\overline{\mathbb{F}}_p$, tenemos que $a^{p-1} = 1$ y que $a^{\frac{p-1}{2}} = \pm 1$. Por tanto, decir que a es un cuadrado de $\mathbb{F}_p$ es equivalente a decir que $b^{p-1} = 1$; pero $b^{p-1} = 1$ equivale a $a^{\frac{p-1}{2}} = 1$. Por tanto, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. □

Corolario 1.5.2. *Sea p un número natural primo impar. Entonces:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, \text{ si } p \equiv 1 \pmod 4, \\ -1, \text{si } p \equiv 3 \pmod 4, \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, \text{ si } p \equiv \pm 1 \pmod 8, \\ -1, \text{si } p \equiv \pm 3 \pmod 8. \end{cases}$$

Demostración: La cuestión relativa al símbolo $\left(\frac{-1}{p}\right)$ es inmediata. Por otro lado, podemos considerar $\zeta \in \overline{\mathbb{F}}_p$ una raíz primitiva de orden 8 de la unidad y poner $b := \zeta + \zeta^{-1}$. Puesto que $\zeta^4 = -1$, tenemos que $\zeta^2 + \zeta^{-2} = 0$ y $b^2 = (\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2 = 2$. Por tanto, $\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = b^{p-1}$.

Por otro lado, puesto que estamos trabajando en un cuerpo de característica p y ζ es de orden 8, disponemos de la igualdad $b^p = \zeta^p + \zeta^{-p} = \zeta^r + \zeta^{-r}$, donde r es cualquier número entero tal que $r \equiv p \pmod 8$. Si $r = \pm 1$, entonces $b^p = \zeta + \zeta^{-1} = b$, de donde $b^{p-1} = 1$. Y si $r = \pm 5$, entonces $b^p = \zeta^5 + \zeta^{-5} = -(\zeta + \zeta^{-1}) = -b$, de donde $b^{p-1} = -1$. Esto acaba la demostración. □

1.6. Sumas de Gauss

Consideremos un carácter de Dirichlet primitivo módulo n, χ, una raíz primitiva n-ésima de la unidad, $\zeta \in \mathbb{C}$, y un número entero arbitrario, N.

Definición 1.6.1. Llamaremos N-ésima suma de Gauss para χ relativa a ζ al elemento de $\mathbb{Q}(\zeta)$ dado por la expresión

$$G(\chi, N) := \sum_{a \mod n} \chi(a)\zeta^{aN}.$$

Cuando la raíz de la unidad considerada sea $\zeta := \exp(\frac{2\pi i}{n})$ hablaremos de la suma de Gauss normalizada y la denotaremos $g(\chi, N)$.

El cálculo de la N-ésima suma de Gauss se puede reducir al de la primera.

Proposición 1.6.2. *Sea χ un carácter de Dirichlet primitivo módulo n y sea $\zeta \in \mathbb{C}$ una raíz primitiva n-ésima de la unidad. Entonces, para todo número entero N se satisface la igualdad*

$$G(\chi, N) = \overline{\chi(N)}G(\chi, 1),$$

donde $\overline{\chi(N)}$ indica el número complejo conjugado de $\chi(N)$.

Demostración: Supongamos, en primer lugar, que $\mathrm{mcd}(N, n) = 1$. En este caso, N es inversible módulo n y podemos escribir la igualdad

$$G(\chi, N) = \sum_{a \mod n} \chi(aNN^{-1})\zeta^{aN};$$

puesto que χ es multiplicativo y $\chi(N^{-1}) = \overline{\chi(N)}$, incluso la podemos escribir en la forma $G(\chi, N) = \sum_{a \mod n} \overline{\chi(N)}\chi(aN)\zeta^{aN}$; y puesto que la multiplicación por N en el conjunto $(\mathbb{Z}/n\mathbb{Z})^*$ es una aplicación biyectiva, obtenemos la igualdad que queríamos ver: $G(\chi, N) = \overline{\chi(N)}G(\chi, 1)$.

Consideremos ahora el caso contrario. Sea $d := \mathrm{mcd}(N, n) > 1$ y escribamos $N = N'd$, $n = n'd$, de manera que $\mathrm{mcd}(N', n') = 1$. Puesto que $\chi(N) = 0$, es suficiente ver que $G(\chi, N) = 0$. Podemos escribir la igualdad $G(\chi, N) = \sum_{a \mod n} \chi(a)\zeta^{adN'}$. Podemos suponer que $0 \leq a < n$ y hacer la

división entera de a por n' en la forma $a = n'q+r$, de manera que $0 \leq r < n'$ y $0 \leq q < d$. Esto da la igualtat $G(\chi, N) = \sum_{r \mod n'} \zeta^{rdN'} \sum_{q \mod d} \chi(n'q + r)$, ya que $\zeta^{n'qdN'} = 1$.

Puesto que χ es un carácter primitivo módulo n, no puede ser que el núcleo del morfismo de reducción $G(n) \xrightarrow{red} G(n')$ esté incluído en el núcleo de χ; por tanto, existe un elemento $c \in G(n)$, $c \equiv 1 \pmod{n'}$, tal que $\chi(c) \neq 1$. Entonces, para cada valor fijo de r el subconjunto de $G(n)$ formado por los elementos $cn'q+cr$ con $0 \leq q < d$ es el mismo que el formado por los elementos $n'q+r$ y, por tanto, se obtiene la igualdad $\sum_{q \mod d} \chi(n'q+r) = \sum_{q \mod d} \chi(cn'q+cr)$. De este hecho se deduce que $G(\chi, N) = \sum_{r \mod n'} \zeta^{rdN'} \sum_{q \mod d} \chi(n'q+r) = \sum_{r \mod n'} \zeta^{rdN'} \sum_{q \mod d} \chi(cn'q+cr) = \chi(c)G(\chi, N)$. Y, puesto que $\chi(c) \neq 1$, que $G(\chi, N) = 0$. □

El resultado siguiente nos da información sobre el valor de las sumas de Gauss.

Proposición 1.6.3. *Sea χ un carácter de Dirichlet primitivo módulo n y sea $\zeta \in \mathbb{C}$ una raíz n-ésima primitiva de la unidad. Entonces, para todo número entero N primo con n se satisface la igualdad $|G(\chi, N)| = \sqrt{n}$.*

Demostración: Puesto que $\mcd(N, n) = 1$, podemos escribir $|G(\chi, N)| = |G(\chi, 1)|$. Calculemos:

$$\begin{aligned} |G(\chi,1)|^2 &= G(\chi,1)\overline{G(\chi,1)} = \\ &= G(\chi,1) \sum_{a \mod n} \overline{\chi(a)}\zeta^{-a} = \\ &= \sum_{a \mod n} G(\chi,a)\zeta^{-a} = \\ &= \sum_{a \mod n} \sum_{b \mod n} \chi(b)\zeta^{a(b-1)} = \\ &= \sum_{b \mod n} \chi(b) \sum_{a \mod n} \zeta^{a(b-1)}. \end{aligned}$$

Si $b \not\equiv 1 \pmod{n}$, entonces $\sum_{a \mod n} \zeta^{a(b-1)} = 0$, ya que es la suma de los n

primeros términos de una progresión geométrica de razón $\zeta^{b-1} \neq 1$ y tal que el producto del último término por la razón es igual al primer término. Y si $b \equiv 1 \pmod{n}$, entonces $\zeta^{a(b-1)} = 1$, de manera que obtenemos la igualdad $|G(\chi, 1)|^2 = \chi(1)n = n$. □

Para el caso de los caracteres cuadráticos podemos afinar un poco más. En efecto, el resultado siguiente nos será de utilidad en la próxima sección.

Corolario 1.6.4. *Supongamos que χ es un carácter cuadrático de Dirichlet, primitivo módulo n. Entonces, $G(\chi, 1)^2 = \chi(-1)n$.*

Demostración: De nuevo podemos calcular

$$G(\chi,1)^2 = G(\chi,1) \sum_{a \mod n} \chi(a)\zeta^a = \\ = \sum_{a \mod n} G(\chi,a)\zeta^a,$$

ya que $\chi(a) = \overline{\chi(a)}$. Por tanto,

$$G(\chi,1)^2 = \sum_{a \mod n} \sum_{b \mod n} \chi(b)\zeta^{a(b+1)} = \\ = \sum_{b \mod n} \chi(b) \sum_{a \mod n} \zeta^{a(b+1)}.$$

Podemos repetir el razonamiento de la proposición anterior cambiando $b-1$ por $b+1$ y obtendremos la igualdad buscada. □

1.7. Cuerpos cuadráticos

Sea $K|\mathbb{Q}$ una extensión cuadrática; es decir, de grado $[K : \mathbb{Q}] = 2$. Si x es un elemento de K no racional, entonces $K = \mathbb{Q}(x)$ y x es raíz de una ecuación irreducible de grado 2 de coeficientes racionales. Si escribimos esta ecuación en la forma $aX^2 + bX + c = 0$, obtenemos que x es uno de los dos números algebraicos $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. Puesto que a y b son números racionales, $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{b^2 - 4ac})$. Quitando denominadores y cuadrados, obtenemos que K es de la forma $\mathbb{Q}(\sqrt{D})$, donde D es un número entero

libre de cuadrados; es decir, $D = -1$ o bien $\pm D$ es un producto de números primos diferentes.

Claramente, la extensión $K|\mathbb{Q}$ es una extensión de Galois abeliana y, según el teorema de Kronecker-Weber, debe haber una raíz de la unidad, ζ, tal que $\sqrt{D} \in \mathbb{Q}(\zeta)$. El objetivo de esta sección es demostrar este hecho de manera independiente. Para ello, comencemos considerando un número primo impar p y una raíz primitiva p-ésima de la unidad $\zeta \in \mathbb{C}$. El primer paso consiste en encontrar las subextensiones cuadráticas de $\mathbb{Q}(\zeta)|\mathbb{Q}$.

Proposición 1.7.1. *Sea* $S := \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right)\zeta^a$ *la primera suma de Gauss para el carácter de Legendre* $\left(\frac{*}{p}\right)$. *Entonces,* $S^2 = \left(\frac{-1}{p}\right)p$.

Demostración: Basta con aplicar el último corolario de la seción anterior al carácter de Legendre módulo p. □

Definición 1.7.2. Sea p un natural primo impar. Escribiremos p^* para el número $\left(\frac{-1}{p}\right)p$.

Observemos que siempre es $p^* \equiv 1 \pmod 4$.

Corolario 1.7.3. *Sea* p *un número primo impar y sea* ζ_p *una raíz primitiva* p*-ésima de la unidad. Entonces* $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$. □

Es decir, para los cuerpos cuadráticos $\mathbb{Q}(\sqrt{p^*})$ se satisface el teorema de Kronecker-Weber.

Por otro lado, es claro que $i = \sqrt{-1}$ es una raíz cuarta primitiva de la unidad, de manera que para $\mathbb{Q}(i)$ se satisface el teorema de Kronecker-Weber. Además, puesto que $\mathbb{Q}(\sqrt{-p^*})$ es un subcuerpo de la composición de los dos cuerpos $\mathbb{Q}(\sqrt{p^*})$ y $\mathbb{Q}(i)$, y puesto que la composición de cuerpos ciclotómicos es un cuerpo ciclotómico, para las extensiones cuadráticas $\mathbb{Q}(\sqrt{p})|\mathbb{Q}$ y $\mathbb{Q}(\sqrt{-p})|\mathbb{Q}$, donde p es un número primo impar, se satisface el teorema de Kronecker-Weber.

Por otro lado, una raíz primitiva 8-ésima de la unidad es el número complejo $\zeta_8 := \frac{1+i}{\sqrt{2}}$, de manera que, puesto que $i \in \mathbb{Q}(\zeta_8)$, también $\sqrt{2}$ y $\sqrt{-2}$

son elementos de $\mathbb{Q}(\zeta_8)$ y para los cuerpos $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{-2})$ se satisface el teorema.

Finalmente, si $D = \pm p_1 p_2 \cdots p_r$ es la descomposición de D como producto de números primos, se satisface la inclusión

$$\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{p_1^*}, \sqrt{p_2^*}, \ldots, \sqrt{p_r^*})$$

y, puesto que para cada uno de los cuerpos $\mathbb{Q}(\sqrt{p_i^*})$ se satisface el teorema, lo mismo sucede con el cuerpo $\mathbb{Q}(\sqrt{D})$.

Dicho de otra manera, hemos demostrado el siguiente

Teorema 1.7.4. *Sea D un número entero libre de cuadrados. Entonces $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\zeta)$ donde $\zeta \in \mathbb{C}$ es una raíz primitiva $4|D|$-ésima de la unidad.* □

1.8. Congruencias cuadráticas

Tal como lo hemos definido, el símbolo de Legendre da información sobre la resolubilidad de congruencias cuadráticas módulo un número primo impar p. En efecto, la congruencia $ax^2 + bx + c \equiv 0 \pmod{p}$, $a \not\equiv 0 \pmod{p}$, tiene solución cuando su discriminante $\Delta := b^2 - 4ac$ es un cuadrado módulo p; es decir, cuando $\left(\frac{\Delta}{p}\right) \neq -1$. Aún más, el número de soluciones de la congruencia es $1 + \left(\frac{\Delta}{p}\right)$.

Podríamos preguntarnos qué sucede cuando cambiamos el número primo p por un número entero cualquiera $N > 1$. En este caso, todavía nos puede ayudar el símbolo de Legendre. Consideremos una congruencia cuadrática

$$ax^2 + bx + c \equiv 0 \pmod{N}. \tag{1.8.1}$$

Sea $N = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ la descomposición de N en factores primos diferentes p_i, y supongamos que el coeficiente dominante a no es divisible por ninguno de los primos p_i. Si la congruencia 1.8.1 tiene solución, entonces

$$ax^2 + bx + c \equiv 0 \pmod{p_i^{n_i}} \tag{1.8.2}$$

tiene solución para cada valor de i; recíprocamente, el teorema chino del resto nos permite asegurar que si la congruencia 1.8.2 tiene exactamente k_i soluciones diferentes módulo $p_i^{n_i}$, entonces la congruencia 1.8.1 tiene exactamente $k_1 k_2 \cdots k_r$ soluciones diferentes módulo N. De manera que el problema consiste en determinar el número de soluciones de cada una de las congruencias 1.8.2. Por tanto, reducimos la dificultad del problema a la resolución de congruencias de la forma

$$ax^2 + bx + c \equiv 0 \pmod{p^n} \tag{1.8.3}$$

donde p es un número primo, a no es divisible por p y n es un número natural cualquiera.

Proposición 1.8.1. *Sean p un número primo (que puede ser 2), $f(X) := aX^2 + bX + c$ un polinomio de coeficientes enteros a, b, c, tal que a no es divisible por p, y supongamos que un número entero $x = x_1$, $0 \leq x < p$, es una solución simple de la congruencia $f(X) \equiv 0 \pmod{p}$. Entonces, para todo entero $n \geq 2$ existe un número entero x_n, $0 \leq x_n < p^n$, y solamente uno tal que $x_n \equiv x_{n-1} \pmod{p^{n-1}}$ y $f(x_n) \equiv 0 \pmod{p^n}$.*

Demostración: Haremos la demostración por inducción sobre n. El caso $n = 1$ es la hipótesis. Supongamos que x_n es un número entero para el cual se satisfacen las condiciones del enunciado. Escribamos $f(x_n) = p^n z_n$; puesto que queremos que sea $x_{n+1} \equiv x_n \pmod{p^n}$, hay que determinar todos los valores de α_n, definidos módulo p, de manera que para $x_{n+1} := x_n + \alpha_n p^n$ se satisfaga $f(x_{n+1}) \equiv 0 \pmod{p^{n+1}}$. Ahora bien, para todo x_{n+1} de la forma $x_n + \alpha_n p^n$ se satisface la congruencia $f(x_{n+1}) \equiv z_n p^n + f'(x_n)\alpha_n p^n \pmod{p^{n+1}}$, de manera que demostrar que $f(x_{n+1}) \equiv 0 \pmod{p^{n+1}}$ equivale a demostrar que $z_n + f'(x_n)\alpha_n \equiv 0 \pmod{p}$. Por otro lado, decir que la raíz x de $f(X) \equiv 0 \pmod{p}$ es simple es equivalente a decir que $f'(x) \not\equiv 0 \pmod{p}$; así, por hipótesis de inducción, $f'(x_n) \equiv f'(x) \not\equiv 0 \pmod{p}$. Eso nos permite asegurar que la congruencia lineal $z_n + f'(x_n)\alpha_n \equiv 0 \pmod{p}$ tiene exactamente una solución α_n, como queríamos demostrar. □

Corolario 1.8.2. *Sean p un número primo impar y a, b, c números enteros tales que a no es divisible por p. Si $\left(\dfrac{b^2 - 4ac}{p}\right) = 1$, entonces, para cada número natural $n \geq 1$, la congruencia cuadrática $aX^2 + bX + c \equiv 0 \pmod{p^n}$ tiene exactamente dos soluciones $\pmod{p^n}$.* □

Observación 1.8.3. La única congruencia cuadrática módulo 2 que tiene raíces simples es la congruencia $X^2 + X \equiv 0 \pmod 2$. Por tanto, si una congruencia cuadrática módulo 2^n se reduce a la congruencia $X^2 + X \equiv 0 \pmod 2$, entonces tiene exactamente dos soluciones $\pmod{2^n}$ para todo número entero n.

De esta manera, obtenemos un criterio sencillo para saber el número de soluciones de todas las congruencias $f(X) := aX^2 + bX + c \equiv 0 \pmod N$ tales que $\mathrm{mcd}(a, N) = 1$ y $f(X)$ es separable $\pmod p$ para todo número primo p que divide N.

1.9. Ley de reciprocidad cuadrática

Uno de los resultados de teoría de números del cual se han publicado más demostraciones diferentes y que aún hoy es objeto de estudio es la ley de reciprocidad cuadrática. El objetivo de esta sección es dar una demostración de esa ley. Para ello, convendrá considerar ciertas sumas de Gauss en característica impar ℓ.

Hemos visto más arriba que si p es un número primo impar, consideramos una raíz primitiva p-ésima de la unidad $\zeta \in \mathbb{C}$ y ponemos $S := \sum_{a \bmod p} \left(\frac{a}{p}\right)\zeta^a$, entonces es $S^2 = \left(\frac{-1}{p}\right)p$. Este resultado también es válido si cambiamos $\mathbb{C}$ por $\overline{\mathbb{F}}_\ell$, para cualquier primo impar $\ell \neq p$.

En efecto, podemos repetir el cálculo:

$$\begin{aligned} S^2 &= \sum_{a \bmod p} \sum_{b \bmod p} \left(\frac{ab}{p}\right)\zeta^{a+b} = \sum_{a\neq 0 \bmod p} \sum_{b \bmod p} \left(\frac{ab}{p}\right)\zeta^{a+b} = \\ &= \sum_{a\neq 0 \bmod p} \sum_{c \bmod p} \left(\frac{a^2c}{p}\right)\zeta^{a(1+c)} = \sum_{a\neq 0 \bmod p} \sum_{c \bmod p} \left(\frac{c}{p}\right)\zeta^{a(1+c)} = \\ &= \sum_{c \bmod p} \left(\frac{c}{p}\right) \sum_{a\neq 0 \bmod p} \zeta^{a(1+c)}. \end{aligned}$$

Si $1 + c \not\equiv 0 \pmod p$, entonces ζ^{1+c} es aún una raíz primitiva p-ésima de

la unidad en $\overline{\mathbb{F}}_\ell$ y $\sum_{a\neq 0 \mod p} \zeta^{a(1+c)} = -1$; y si $1+c \equiv 0 \pmod p$, entonces $\sum_{a\neq 0 \mod p} \zeta^{a(1+c)} = p-1$. Eso hace que

$$S^2 = -\sum_{1+c\neq 0 \mod p} \left(\frac{c}{p}\right) + \left(\frac{-1}{p}\right)(p-1) = \left(\frac{-1}{p}\right)p.$$

Lema 1.9.1. *Con las notaciones anteriores se satisface la fórmula* $S^{\ell-1} = \left(\frac{\ell}{p}\right)$.

DEMOSTRACIÓN: Puesto que trabajamos en característica impar ℓ, podemos escribir

$$\begin{aligned} S^\ell &= \sum_{a \mod p} \left(\frac{a}{p}\right)\zeta^{a\ell} = \\ &= \sum_{a \mod p} \left(\frac{a\ell^{-1}}{p}\right)\zeta^{a} = \\ &= \left(\frac{\ell^{-1}}{p}\right) \sum_{a \mod p} \left(\frac{a}{p}\right)\zeta^{a} = \\ &= \left(\frac{\ell^{-1}}{p}\right) S = \\ &= \left(\frac{\ell}{p}\right) S. \end{aligned}$$

Puesto que $S^2 \neq 0$, podemos simplificar S y obtenemos la igualdad buscada. □

Teorema 1.9.2. (Ley de reciprocidad cuadrática) *Sean p, ℓ números primos impares. Entonces,* $\left(\frac{\ell}{p}\right) = \left(\frac{p}{\ell}\right)(-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}$.

DEMOSTRACIÓN: Si $\ell = p$ el resultado es trivial. Por otro lado, recordemos que si tenemos un número entero a, y si $z \in \overline{\mathbb{F}}_\ell$ es tal que $z^2 = a$, entonces $\left(\frac{a}{\ell}\right) = z^{\ell-1}$. Podemos aplicar este hecho para calcular el símbolo de Legendre

$\left(\dfrac{\left(\dfrac{-1}{p}\right)p}{\ell}\right)$ en el caso $\ell \neq p$ en la forma

$$\left(\frac{\left(\frac{-1}{p}\right)p}{\ell}\right) = S^{\ell-1} = \left(\frac{\ell}{p}\right).$$

Pero sabemos que $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, de manera que obtenemos la igualdad

$$\left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2}\,\frac{\ell-1}{2}}\left(\frac{p}{\ell}\right)$$

que queríamos demostrar. □

Más adelante veremos otra demostración de este teorema.

Una aplicación inmediata de la ley de reciprocidad cuadrática es el cálculo efectivo del símbolo de Legendre. En efecto, la mejor manera de veurlo es con un ejemplo. Supongamos que queremos calcular el símbolo

$$\left(\frac{34569284994927}{1602961}\right).$$

Lo primero que hay que hacer es calcular el resto de 34569284994927 módulo el primo 1602961; eso da sin ninguna dificultad

$$\begin{aligned}\left(\frac{34569284994927}{1602961}\right) = \left(\frac{1188715}{1602961}\right) = \left(\frac{5\cdot 11\cdot 21613}{1602961}\right) = \\ = \left(\frac{5}{1602961}\right)\left(\frac{11}{1602961}\right)\left(\frac{21613}{1602961}\right).\end{aligned}$$

Apliquemos la ley de reciprocidad cuadrática. Puesto que $1602961 \equiv 1 \pmod 4$, los factores $(-1)^{\frac{p-1}{2}\,\frac{\ell-1}{2}}$ son triviales y podemos escribir:

$$\begin{aligned}\left(\frac{34569284994927}{1602961}\right) = \left(\frac{1602961}{5}\right)\left(\frac{1602961}{11}\right)\left(\frac{1602961}{21613}\right) = \\ = \left(\frac{1}{5}\right)\left(\frac{8}{11}\right)\left(\frac{3599}{21613}\right).\end{aligned}$$

Ahora, $\left(\frac{1}{5}\right) = 1$ y $\left(\frac{8}{11}\right) = \left(\frac{2}{11}\right) = -1$, ya que $8 = 2 \cdot 2^2$ y $11 \equiv 3 \pmod 8$; puesto que $3599 = 59 \cdot 61$, obtenemos

$$\left(\frac{34569284994927}{1602961}\right) = -\left(\frac{59}{21613}\right)\left(\frac{61}{21613}\right) = -\left(\frac{21613}{59}\right)\left(\frac{21613}{61}\right),$$

ya que $21613 \equiv 1 \pmod 4$. Finalmente, $21613 \equiv 19 \pmod{59}$ y $21613 \equiv 19 \pmod{61}$; por tanto:

$$\left(\frac{34569284994927}{1602961}\right) = -\left(\frac{19}{59}\right)\left(\frac{19}{61}\right) = \left(\frac{59}{19}\right)\left(\frac{61}{19}\right),$$

ya que $59 \equiv 19 \equiv 3 \pmod 4$; y, puesto que $19 \equiv 3 \pmod 8$,

$$\left(\frac{34569284994927}{1602961}\right) = \left(\frac{2}{19}\right)\left(\frac{4}{19}\right) = \left(\frac{2}{19}\right) = -1.$$

1.10. Símbolo de Jacobi

Los símbolos de Legendre vienen asociados a los números primos impares p. A fin de evitar la descomposición en factores primos en el cálculo de este símbolo, introduciremos el símbolo de Jacobi.

Sea P un número entero positivo impar. Para todo número entero a, definimos el símbolo de Jacobi $\left(\frac{a}{P}\right)$ de la manera siguiente:

sea $P := p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ la descomposición de P en factores primos. Cada uno de los números primos p_i es un número primo impar y podemos definir

$$\left(\frac{a}{P}\right) := \left(\frac{a}{p_1}\right)^{n_1}\left(\frac{a}{p_2}\right)^{n_2} \cdots \left(\frac{a}{p_r}\right)^{n_r},$$

como producto de símbolos de Legendre. El símbolo definido de esta manera se llama el símbolo de Jacobi y se satisfacen las propiedades siguientes:

(1) si $\mathrm{mcd}(a, P) > 1$, entonces $\left(\frac{a}{P}\right) = 0$;

(2) si $\mathrm{mcd}(a, P) = 1$, entonces $\left(\frac{a}{P}\right) = \pm 1$;

(3) si P_1, P_2, P son números enteros positivos impares y a_1, a_2, a son números enteros cualesquiera, entonces $\left(\frac{a}{P_1P_2}\right) = \left(\frac{a}{P_1}\right)\left(\frac{a}{P_2}\right)$ y $\left(\frac{a_1a_2}{P}\right) = \left(\frac{a_1}{P}\right)\left(\frac{a_2}{P}\right)$; y

(4) si $a \equiv a' \pmod{P}$, entonces $\left(\frac{a}{P}\right) = \left(\frac{a'}{P}\right)$.

La demostración de estas propiedades es inmediata a partir de la definición y de las del símbolo de Legendre. Además, se satisface también la ley de reciprocidad cuadrática.

Proposición 1.10.1. *Sean P_1, P_2 números enteros positivos impares. Entonces,* $\left(\frac{P_1}{P_2}\right) = (-1)^{\frac{P_1-1}{2}\frac{P_2-1}{2}}\left(\frac{P_2}{P_1}\right)$.

Demostración: Para hacer la demostración basta factorizar P_1 y P_2 y aplicar la ley de reciprocidad cuadrática para el símbolo de Legendre. El resultado final se deduce del siguiente

Lema 1.10.2. *Sea $P := p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$ la descomposición en factores primos de un número entero impar P. Pongamos $\varepsilon(P) := \frac{P-1}{2}$. Entonces,*

$$(-1)^{\varepsilon(P)} = \prod_i (-1)^{\varepsilon(p_i)n_i}.$$

Demostración: Si P_1, P_2 son números enteros impares, entonces

$$(P_1-1)(P_2-1) = P_1P_2 - P_1 - P_2 + 1 = (P_1P_2-1) - (P_1-1) - (P_2-1),$$

y puesto que $(P_1-1)(P_2-1) \equiv 0 \pmod 4$, se obtiene que $P_1P_2 - 1 \equiv (P_1-1)+(P_2-1) \pmod 4$; por tanto, $(-1)^{\varepsilon(P_1P_2)} = (-1)^{\varepsilon(P_1)}(-1)^{\varepsilon(P_2)}$. □

Este mismo lema nos permite escribir el valor del símbolo $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$. Análogamente, $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$, ya que si $\omega(P) := \frac{P^2-1}{8}$, entonces $(-1)^{\omega(P_1P_2)} = (-1)^{\omega(P_1)}(-1)^{\omega(P_2)}$.

En efecto. Puesto que P_i es impar, $P_i^2 \equiv 1 \pmod 8$; y puesto que

$$(P_1^2-1)(P_2^2-1) = (P_1P_2)^2 - 1 - (P_1^2-1) - (P_2^2-1),$$

se tiene que $(P_1P_2)^2 - 1 \equiv (P_1^2 - 1) + (P_2^2 - 1) \pmod{8^2}$; por tanto, $(-1)^{\omega(P_1P_2)} = (-1)^{\omega(P_1)}(-1)^{\omega(P_2)}$.

El símbolo de Jacobi permite simplificar el cálculo de los símbolos de Legendre. Si P es un número primo impar, para todo número entero a el símbolo de Jacobi y el de Legendre $\left(\frac{a}{P}\right)$ coinciden. Por tanto, podemos evitar la descomposición en factores primos en el cálculo del símbolo de Legendre: basta separar los factores 2 del numerador antes de invertir el símbolo.

Veámoslo, como en la sección anterior, en el cálculo de

$$\left(\frac{34569284994927}{1602961}\right).$$

Igual que antes, obtenemos

$$\left(\frac{34569284994927}{1602961}\right) = \left(\frac{1188715}{1602961}\right).$$

Aplicando la ley de reciprocidad cuadrática,

$$\left(\frac{34569284994927}{1602961}\right) = \left(\frac{1602961}{1188715}\right),$$

y, reduciendo el numerador módulo el denominador,

$$\left(\frac{34569284994927}{1602961}\right) = \left(\frac{414246}{1188715}\right).$$

Ahora tenemos dos posibilidades. O bien separar los factores 2 del numerador y calcular el símbolo de Jacobi $\left(\frac{2}{1188715}\right)$ si el número de factores 2 que hemos podido sacar es impar, o bien restar el denominador del numerador y calcular el símbolo $\left(\frac{-1}{1188715}\right)$ a fin de obtener un símbolo con numerador y denominador impares positivos. Lo haremos de la primera forma, ya que eso producirá un numerador menor y, por tanto, los cálculos posteriores se harán con números de menos cifras. Eso da

$$\left(\frac{34569284994927}{1602961}\right) = -\left(\frac{207123}{1188715}\right),$$

ya que $1188715 \equiv 3 \pmod 8$. Puesto que $1188715 \equiv 207123 \equiv 3 \pmod 4$, la ley de reciprocidad da

$$\left(\frac{34569284994927}{1602961}\right) = \left(\frac{1188715}{207123}\right) = \left(\frac{153100}{207123}\right).$$

Ahora es claro un factor 10^2 en el numerador, y 5 no divide el denominador; por tanto, podemos eliminar este factor y obtenemos

$$\left(\frac{34569284994927}{1602961}\right) = \left(\frac{1531}{207123}\right) = -\left(\frac{207123}{1531}\right),$$

ya que $207123 \equiv 1531 \equiv 3 \pmod 8$. Reduciendo de nuevo:

$$\left(\frac{34569284994927}{1602961}\right) = -\left(\frac{438}{1531}\right) = -\left(\frac{2}{1531}\right)\left(\frac{219}{1531}\right) = \left(\frac{219}{1531}\right).$$

Reiterando el proceso:

$$\begin{aligned}\left(\frac{34569284994927}{1602961}\right) &= -\left(\frac{1531}{219}\right) = -\left(\frac{217}{219}\right) = \\ &= -\left(\frac{219}{217}\right) = -\left(\frac{2}{217}\right) = -1.\end{aligned}$$

1.11. Símbolo de Kronecker

Otro ejemplo muy importante de carácter de Dirichlet es el dado por el símbolo de Kronecker. Esta sección se dedica a su introducción y estudio; más adelante servirá para describir cómodamente las leyes de descomposición de los números primos en los cuerpos cuadráticos.

Observemos que $(\mathbb{Z}/4\mathbb{Z})^*$ es un grupo de orden 2; por tanto, solamente hay dos caracteres de Dirichlet módulo 4; uno de ellos es el carácter trivial y el otro es el carácter cuadrático $(-1)^{\varepsilon(*)}$, primitivo módulo 4, definido en la sección anterior al hablar del símbolo de Jacobi.

Análogamente, solamente hay cuatro caracteres de Dirichlet módulo 8. Dos de ellos, no primitivos, son los inducidos por los caracteres de Dirichlet módulo 4: el carácter trivial y el carácter $(-1)^{\varepsilon(*)}$. Los otros dos también son cuadráticos, ya que el grupo $(\mathbb{Z}/8\mathbb{Z})^*$ es de exponente 2; uno de ellos

es el carácter $(-1)^{\omega(*)}$, que también ha aparecido al hablar del símbolo de Jacobi; el otro, en consecuencia, es el producto de los otros dos caracteres no triviales: $(-1)^{\varepsilon(*)+\omega(*)}$.

Hemos visto, también, que si p es un número primo impar, entonces el carácter de Legendre $\left(\frac{*}{p}\right)$ es el único carácter cuadrático de conductor p.

Sea $d := \ell_1\ell_2\cdots\ell_r$ un producto de números naturales primos impares diferentes, que puede ser $d = 1$. El producto de los caracteres de Legendre $\left(\frac{*}{\ell_i}\right)$, es decir, el carácter de Jacobi $\left(\frac{*}{d}\right)$, es un carácter cuadrático de Dirichlet definido módulo d, el trivial si $d = 1$. Si lo multiplicamos por la potencia $\varepsilon(d)$-ésima del único carácter primitivo módulo 4, $(-1)^{\varepsilon(*)}$, obtenemos un carácter cuadrático de Dirichlet definido módulo $4d$. Es el carácter cuadrático de Dirichlet $\chi_d := (-1)^{\varepsilon(d)\varepsilon(*)}\left(\frac{*}{d}\right)$ y se llama el d-ésimo carácter de Kronecker.

A partir de este carácter podemos definir tres caracteres más:

$$\chi_{-d} := (-1)^{\varepsilon(*)}\chi_d,$$

$$\chi_{2d} := (-1)^{\omega(*)}\chi_d,$$

$$\chi_{-2d} := (-1)^{\varepsilon(*)}(-1)^{\omega(*)}\chi_d.$$

Son caracteres cuadráticos de Dirichlet definidos módulo $4d$, $8d$ y $8d$, respectivamente. se llaman los caracteres de Kronecker.

Proposición 1.11.1. *Sea D un número entero libre de cuadrados. Entonces, χ_D es el único carácter cuadrático de Dirichlet módulo $4|D|$ tal que para todo número natural primo impar p que no divide D es $\chi_D(p) = \left(\frac{D}{p}\right)$.*

Demostración: Sea $d := \ell_1\ell_2\cdots\ell_r$ la descomposición en factores primos de la parte positiva impar de D. La ley de reciprocidad cuadrática para el símbolo de Jacobi $\left(\frac{*}{d}\right)$ permite demostrar en seguida que para el carácter de Kronecker χ_D se satisface la propiedad enunciada. En efecto,

$$\chi_d(p) = (-1)^{\varepsilon(d)\varepsilon(p)}\left(\frac{p}{d}\right) = \left(\frac{d}{p}\right);$$

por tanto, también

$$\chi_{-d}(p) = (-1)^{\varepsilon(p)}\chi_d(p) = (-1)^{\varepsilon(p)}\left(\frac{d}{p}\right) = \left(\frac{-d}{p}\right),$$

$$\chi_{2d}(p) = (-1)^{\omega(p)}\chi_d(p) = (-1)^{\omega(p)}\left(\frac{d}{p}\right) = \left(\frac{2d}{p}\right),$$

y

$$\chi_{-2d}(p) = (-1)^{\varepsilon(p)}(-1)^{\omega(p)}\chi_d(p) = (-1)^{\varepsilon(p)}(-1)^{\omega(p)}\left(\frac{d}{p}\right) = \left(\frac{-2d}{p}\right).$$

Resta demostrar la unicidad.

Para ello, supongamos que χ es un carácter cuadrático de Dirichlet definido módulo $4|D|$ para el cual se satisface la propiedad y consideremos $\psi := \chi\chi_D^{-1}$. Entonces, ψ es un carácter de Dirichlet definido módulo $4|D|$ para el cual y para todo natural primo impar p que no divide D se satisface que $\psi(p) = 1$. Puesto que ψ es multiplicativo, también se satisface que $\psi(a) = 1$ para todo número natural impar a primo con D; es decir, para todo número natural a primo con $4D$. Eso demuestra que $\chi = \chi_D$. □

Proposición 1.11.2. *Sea D un número entero libre de cuadrados y sea d la parte impar positiva de su descomposición en factores primos. El conductor del carácter de Kronecker χ_D es exactamente $4|D|$, excepto en el caso $D \equiv 1 \pmod 4$ en que el conductor es d.*

Demostración: Puesto que el carácter de Legendre $\left(\frac{*}{\ell_i}\right)$ es primitivo de conductor ℓ_i, el carácter $\psi := \left(\frac{*}{\ell_1}\right)\left(\frac{*}{\ell_2}\right)\cdots\left(\frac{*}{\ell_r}\right)$ es primitivo de conductor $\ell_1\ell_2\cdots\ell_r$. Puesto que el carácter de Kronecker es el producto de ψ por caracteres de conductores potencia de 2, basta estudiar el conductor de los otros factores.

Si $D = d \equiv 1 \pmod 4$, para obtener χ_D se multiplica ψ por el carácter trivial, ya que $(-1)^{\varepsilon(D)\varepsilon(*)} = 1$. Y si $D = -d \equiv 1 \pmod 4$, también se multiplica ψ por el carácter trivial, ya que $(-1)^{\varepsilon(D)\varepsilon(*)}(-1)^{\varepsilon(*)} = 1$. En los otros casos, o bien ψ se multiplica por el carácter primitivo de conductor 4, en el caso $D \equiv 3 \pmod 4$ o bien se multiplica por uno de los dos caracteres primitivos de conductor 8, en el caso en que D es par. □

La proposición siguiente generaliza el hecho que los únicos caracteres cuadráticos de Dirichlet de conductor primo impar son los caracteres de Legendre.

Proposición 1.11.3. *Sea χ un carácter cuadrático de Dirichlet primitivo. Entonces, existe un número entero D libre de cuadrados tal que χ es el carácter de Kronecker χ_D, considerado definido módulo su conductor.*

Para la demostración, usaremos una serie de resultados previos.

Lema 1.11.4. *Sea f el conductor de un carácter cuadrático de Dirichlet y supongamos que f es impar. Entonces, f es libre de cuadrados.*

Demostración: Sea χ un carácter cuadrático de Dirichlet definido módulo un número impar n y sea n' el producto de los números primos impares diferentes que dividen n. Si demostramos que todos los elementos $a \in G(n)$ para los que se satisface la congruencia $a \equiv 1 \pmod{n'}$ son cuadrados en $G(n)$, entonces habremos acabado ya que, por ser χ cuadrático, es $\chi(b) = \pm 1$ para todo $b \in G(n)$ y, por tanto, $\chi(b^2) = 1$; eso nos permite asegurar que χ se puede definir módulo n', de manera que su conductor, que es un divisor de n', es libre de cuadrados.

Ahora bien, si $a \in G(n)$ es un cuadrado módulo n', lo es módulo ℓ para todo número primo ℓ que divide n y, puesto que el polinomio $X^2 - a$ es separable módulo ℓ, las congruencias $X^2 - a \equiv 0 \pmod{\ell^k}$ tienen solución para cada valor de k. Por tanto, la congruencia $X^2 - a \equiv 0 \pmod{n}$ tiene solución y a es un cuadrado en $G(n)$. □

Lema 1.11.5. *Sea f el conductor de un carácter cuadrático de Dirichlet. Entonces, f es libre del factor 2^4.*

Demostración: La demostración es parecida a la del lema anterior. Si $r \geq 3$, entonces $G(2^r)/G(2^r)^2 \simeq G(8) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; por tanto, el subgrupo de los cuadrados de $G(2^r)$ es un subgrupo de índice 4. Además, si a es un cuadrado de $G(2^r)$, entonces $a \equiv 1 \pmod{8}$. Por otro lado, el subgrupo formado por los elementos $a \in G(2^r)$ tales que $a \equiv 1 \pmod{8}$ también es de índice 4; por tanto, los dos subgrupos son iguales. Eso implica que, en el caso $r \geq 3$, podemos rebajar los factores 2^r de n hasta 2^3. □

Lema 1.11.6. *El conductor de un carácter de Dirichlet (cuadrático o no) no es nunca de la forma $2f$ con f impar.*

DEMOSTRACIÓN: Puesto que si f es impar, entonces $G(2f) \simeq G(f)$. □

Vamos a demostrar, ahora, la proposición. Sea f el conductor del carácter χ y supongamos que f es impar. El grupo de los caracteres cuadráticos de Dirichlet definidos módulo f es isomorfo al grupo $G(f)/G(f)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^r$, donde r es el número de factores primos diferentes que dividen f. Por otro lado, los caracteres cuadráticos de $G(f)$ que reducen a los caracteres de Legendre $\left(\frac{*}{\ell}\right)$, para ℓ un número primo que divide f, forman un sistema de generadores libres del grupo de los caracteres cuadráticos de $G(f)$; en consecuencia, χ es un producto de estos caracteres. Si alguno de los caracteres de Legendre no apareciese en este producto, el conductor no podría ser f; por tanto, χ es el producto de estos caracteres de Legendre. Y este producto es el carácter de Kronecker χ_D para $D = \pm f$ con el signo elegido de manera que χ_D tenga conductor f.

En el caso que f es exactamente divisible per 4, hay que añadir el carácter $(-1)^{\varepsilon(*)}$ en el razonamiento anterior; eso da para χ el carácter de Kronecker χ_{-D}, con D elegido igual que antes. Y en el caso que f es divisible por 8 hay que añadir el carácter $(-1)^{\omega(*)}$ o el carácter $(-1)^{\omega(*)}(-1)^{\varepsilon(*)}$. Los detalles se dejan al lector. □

Capítulo 2

Enteros de los cuerpos de números

La riqueza de la aritmética de $\mathbb{Z}$ queda completamente escondida en punto consideramos su cuerpo de fracciones, $\mathbb{Q}$. Por tanto, si queremos estudiar la aritmética de un cuerpo de números, K, será bueno buscar algún anillo que lo tenga como cuerpo de fracciones y que, a la vez, tenga buenas propiedades de divisibilidad.

Los anillos que se utilizan usualmente son anillos que tienen algunas de las buenes propiedades de divisibilidad del anillo $\mathbb{Z}$; pero, en general, no son anillos tan agradables como $\mathbb{Z}$.

2.1. Elementos enteros sobre un anillo

El anillo $\mathbb{Z}[i]$ de los números enteros de Gauss es uno de los anillos más conocidos; sus elementos son los números complejos de la forma $a+bi$, donde a y b son números enteros; su cuerpo de fracciones es el cuerpo ciclotómico $\mathbb{Q}(i)$.

Observemos que si $\alpha := a + bi$ es un número entero de Gauss, entonces $\alpha \in \mathbb{Q}(i)$ es raíz del polinomio mónico de coeficientes enteros $(X-a)^2+b^2 \in \mathbb{Z}[X]$. Recíprocamente, si un elemento $\alpha := a+bi \in \mathbb{Q}(i)$, a, $b \in \mathbb{Q}$, es raíz de un polinomio mónico de coeficientes enteros, entonces es un número entero de Gauss; es decir, a y b son enteros.

En efecto; sea $f(X) \in \mathbb{Z}[X]$ un polinomio mónico y sea $\alpha := a+bi \in \mathbb{Q}(i)$, a, $b \in \mathbb{Q}$, una raíz de $f(X)$. Puesto que $f(X) \in \mathbb{R}[X]$, el conjugado de α, $\overline{\alpha} := a - bi$, también es una raíz de $f(X)$. Por tanto, el polinomio $f(X)$ es divisible por $(X - \alpha)(X - \overline{\alpha}) = (X - a)^2 + b^2$. Por el lema de Gauss, este polinomio mónico tiene coeficientes enteros; es decir, $2a \in \mathbb{Z}$ y $a^2 + b^2 \in \mathbb{Z}$. En consecuencia, $(2b)^2 \in \mathbb{Z}$, de manera que $2b \in \mathbb{Z}$. Escribamos $a = A/2$, $b = B/2$, con A, $B \in \mathbb{Z}$; de $a^2 + b^2 \in \mathbb{Z}$ resulta que $A^2 + B^2 \equiv 0 \pmod 4$; puesto que en $\mathbb{Z}/4\mathbb{Z}$ la suma de dos cuadrados solamente es nula cuando los dos cuadrados son nulos, ha de ser $A^2 \equiv B^2 \equiv 0 \pmod 4$, de manera que A, $B \in 2\mathbb{Z}$. Eso nos asegura que a, $b \in \mathbb{Z}$, como queríamos demostrar.

Este hecho se puede resumir diciendo que los números enteros de Gauss son exactamente los números de $\mathbb{Q}(i)$ que son raíces de polinomios mónicos de coeficientes enteros.

Definición 2.1.1. Sea B un anillo y sea $A \subseteq B$ un subanillo. Un elemento $b \in B$ se llama entero sobre A si b es raíz de un polinomio mónico de coeficientes en A. La extensión de anillos $B|A$ se llama entera si todo elemento de B es entero sobre A.

Proposición 2.1.2. *Sea $B|A$ una extensión de anillos y sea $b \in B$. Las propiedades siguientes son equivalentes:*

(a) b es entero sobre A;

(b) el anillo $A[b]$ es un A-módulo finitamente generado;

(c) existe un subanillo C de B que contiene A y b y que es un A-módulo finitamente generado; y

(d) existe un $A[b]$-submódulo finitamente generado y fiel de B. □

Corolario 2.1.3. *Sean A un anillo y $\{a_1, a_2, \ldots, a_n\}$ elementos de un anillo extensión $B|A$ tales que para $0 \leq i < n$ el elemento a_{i+1} es entero sobre el anillo $A[a_1, a_2, \ldots, a_i]$. Entonces, el anillo $A[a_1, a_2, \ldots, a_n]$ es un A-módulo finitamente generado.* □

Corolario 2.1.4. *Sea B un anillo y sea $A \subseteq B$ un subanillo. El conjunto de los elementos $b \in B$ que son enteros sobre A es un subanillo de B que contiene A.* □

Corolario 2.1.5. *Sean $C|B$ i $B|A$ extensiones enteras de anillos. Entonces, la extensión $C|A$ es una extensión entera.* □

Definición 2.1.6. Sea $B|A$ una extensión de anillos. El subanillo de B formado por los elementos que son enteros sobre A se llama la clausura entera de A en B. Se dice que A es íntegramente cerrado en B si A es su propia clausura entera en B. Un dominio de integridad A se llama íntegramente cerrado si coincide con su propia clausura entera en su cuerpo de fracciones.

Nos interesa, sobre todo, el caso de dominios de integridad. Los ejemplos más sencillos de anillos íntegramente cerrados los dan los resultados siguientes.

Proposición 2.1.7. *Sea $B|A$ una extensión de anillos y sea C la clausura entera de A en B. Entonces, C es íntegramente cerrado en B.* □

Proposición 2.1.8. *Sea A un dominio factorial. Entonces, A es íntegramente cerrado.* □

Corolario 2.1.9. *Sea A un dominio principal. Entonces, A es íntegramente cerrado.* □

Proposición 2.1.10. *Sea A un dominio íntegramente cerrado y sea $S \subseteq A$ un subconjunto multiplicativamente cerrado de A. Entonces, el anillo localizado de A en S, $S^{-1}A$, es íntegramente cerrado.* □

Es evidente que, en el caso de un cuerpo, una extensión entera es una extensión algebraica. Por otro lado, es un ejercicio sencillo demostrar que si $A \subseteq B$ son dominios y la extensión $B|A$ es entera, condición necesaria y suficiente para que A sea un cuerpo es que B lo sea. La propiedad siguiente es útil para determinar si un elemento es entero.

Proposición 2.1.11. *Sean A un dominio de integridad, K el cuerpo de fracciones de A, $L|K$ una extensión algebraica, $b \in L$ un elemento cualquiera, y $f(X) := \mathrm{Irr}(b, K)$ el polinomio mónico irreductible de $K[X]$ que tiene b como raíz. Supongamos que A es íntegramente cerrado. Entonces, condición necesaria y suficiente para que b sea entero sobre A es que $f(X) \in A[X]$.*

Demostración: Podemos suponer que la extensión $L|K$ es normal. Sea $g(X) \in A[X]$ una ecuación de dependencia entera de b. Puesto que $f(X)$

es el polinomio irreducible de $K[X]$ de grado menor que tiene b como raíz y $g(X)$ es un polinomio de $K[X]$ que tiene b como raíz, $f(X)$ divide $g(X)$ en $K[X]$. Eso implica que las raíces de $f(X)$ también lo son de $g(X)$, de manera que todas las raíces de $f(X)$ son elementos de L enteros sobre A. Por tanto, los polinomios simétricos elementales de estas raíces son enteros sobre A. Pero estos polinomios simétricos elementales son los coeficientes de $f(X)$ y, por tanto, los coeficientes de $f(X)$ son elementos de K que son enteros sobre A; puesto que A es íntegramente cerrado, el polinomio $f(X)$ tiene los coeficientes en $A[X]$. □

2.2. Enteros de los cuerpos de números

Se llama cuerpo de números todo cuerpo K de característica cero tal que la extensión $K|\mathbb{Q}$ es finita.

Definición 2.2.1. Un número entero algebraico es un elemento de $\overline{\mathbb{Q}}$ que es entero sobre $\mathbb{Z}$. Si K es un cuerpo de números, la clausura entera de $\mathbb{Z}$ en K se llama el anillo de los enteros de K. Es el anillo formado por todos los elementos de K que son enteros algebraicos.

El primer objetivo de esta sección es calcular los anillos de enteros de los cuerpos cuadráticos. Sea, pues, D un número entero libre de cuadrados. El anillo $\mathbb{Z}[\sqrt{D}]$ es un subanillo del cuerpo cuadrático $K := \mathbb{Q}(\sqrt{D})$ que es entero sobre $\mathbb{Z}$; por tanto, si $\mathcal{O}_K$ designa el anillo de los enteros del cuerpo K, se tiene la inclusión $\mathbb{Z}[\sqrt{D}] \subseteq \mathcal{O}_K$. El recíproco no es cierto en general. En efecto, se satisface el resultado siguiente.

Proposición 2.2.2. *Sea D un número entero libre de cuadrados. El anillo de los enteros del cuerpo $K := \mathbb{Q}(\sqrt{D})$ es el anillo $\mathcal{O}_K = \mathbb{Z}[\omega]$, donde $\omega = \sqrt{D}$ si $D \not\equiv 1 \pmod 4$ y $\omega = \dfrac{D+\sqrt{D}}{2}$ si $D \equiv 1 \pmod 4$.*

Demostración: La demostración es una generalización directa del cálculo que hemos hecho para el caso del anillo $\mathbb{Z}[i]$ de los números enteros de Gauss. Sean a, $b \in \mathbb{Q}$ tales que $a + b\sqrt{D} \in \mathcal{O}_K$. El conjugado $a - b\sqrt{D}$ de $a + b\sqrt{D}$ también es un entero de K, de manera que la suma y el producto de estos dos elementos son elementos enteros de K. Pero son racionales y, puesto que

$\mathbb{Z}$ es íntegramente cerrado, son enteros. Eso nos permite asegurar que $2a$, $a^2 - Db^2 \in \mathbb{Z}$. Por tanto, $4a^2 - 4Db^2 \in 4\mathbb{Z}$ y $4Db^2 \in \mathbb{Z}$. Ahora, puesto que D es libre de cuadrados, $2b$ ha de ser entero, ya que si tuviese algún denominador, D no podría llevar su cuadrado a $\mathbb{Z}$. Por tanto, $A := 2a$, $B := 2b \in \mathbb{Z}$ y $A^2 - DB^2 \in 4\mathbb{Z}$. Además, si $D \not\equiv 1 \pmod 4$, entonces $A^2 - DB^2 \in 4\mathbb{Z}$ solamente se puede dar si A y B son pares; de manera que en este caso a, $b \in \mathbb{Z}$ y $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$. Pero en el caso $D \equiv 1 \pmod 4$ puede ser que A y B sean a la vez impares; eso nos permite asegurar que $\mathcal{O}_K$ está formado por elementos $(A + B\sqrt{D})/2$ tales que A, B son enteros de la misma paridad. En particular, puesto que $\dfrac{D + \sqrt{D}}{2} \in \mathcal{O}_K$ (es raíz del polinomio $X^2 - DX + \dfrac{D(D-1)}{4} \in \mathbb{Z}[X]$), se satisface que $\mathcal{O}_K = \mathbb{Z}[\dfrac{D + \sqrt{D}}{2}]$. □

En particular, $\mathbb{Z}[i]$ es el anillo de los números enteros del cuerpo ciclotómico $\mathbb{Q}(i)$. Es bien conocido que este anillo es un anillo principal, ya que es euclídeo. Esta propiedad no es en absoluto una propiedad general de los anillos de los enteros de los cuerpos de números. En efecto, veremos en seguida que hay ejemplos de anillos de enteros de cuerpos de números, incluso de cuerpos cuadráticos, que no son principales; de hecho, ni tan solo factoriales.

Ejemplo 2.2.3. Consideremos el anillo $\mathbb{Z}[\sqrt{-5}]$. Es el anillo de los enteros del cuerpo cuadrático $\mathbb{Q}(\sqrt{-5})$. Veamos que no es factorial.

Observemos que $21 = (4 + \sqrt{-5})(4 - \sqrt{-5}) = 3 \cdot 7$; estas son dos descomposiciones en factores irreducibles en el anillo $\mathbb{Z}[\sqrt{-5}]$ del número 21; y son esencialmente diferentes. En efecto, ninguno de los elementos $4 \pm \sqrt{-5}$, 3 y 7 es un elemento unitario del anillo $\mathbb{Z}[\sqrt{-5}]$ y ninguno de estos elementos es un elemento asociado de ningún otro. Eso se puede ver, por ejemplo, teniendo en cuenta que si α es un elemento inversible, entonces la norma $\mathrm{N}(\alpha)$ es un elemento inversible de $\mathbb{Z}$, ya que es un número entero algebraico de $\mathbb{Q}$ y $\mathrm{N}(\alpha)\mathrm{N}(\alpha^{-1}) = \mathrm{N}(1) = 1$. Puesto que $\mathrm{N}(4 \pm \sqrt{-5}) = 21$, $\mathrm{N}(3) = 9$, y $\mathrm{N}(7) = 49$, ninguno de estos elementos es una unidad del anillo $\mathbb{Z}[\sqrt{-5}]$. Por otro lado, si alguno de estos elementos fuese asociado de algún otro, ambos deberían tener, salvo quizás el signo, la misma norma; pero eso solamente sucede con los dos elementos $4 \pm \sqrt{-5}$, que tampoco son asociados ya que, por ejemplo, su cociente no es entero sobre $\mathbb{Z}$.

Resta ver que estos elementos son irreducibles. Si alguno de ellos no lo

fuese, su norma debería descomponer; pero para $\alpha \in \mathbb{Z}[\sqrt{-5}]$, no puede ser $\mathrm{N}(\alpha) = \pm 3$ ni $\mathrm{N}(\alpha) = \pm 7$, ya que las ecuaciones $\mathrm{N}(a + b\sqrt{-5}) = a^2 + 5b^2 = \pm 3, \pm 7$ no tienen soluciones a, $b \in \mathbb{Z}$. En consecuencia, el anillo $\mathbb{Z}[\sqrt{-5}]$ no puede ser un anillo factorial.

Por otro lado, hay anillos de enteros de cuerpos cuadráticos que son principales pero que no son euclídeos para ninguna elección de la aplicación grado.

Ejemplo 2.2.4. Sea $A := \mathbb{Z}[\theta]$, $2\theta := 1 + \sqrt{-19}$, el anillo de los enteros de $\mathbb{Q}(\sqrt{-19})$. Entonces, el anillo A es principal pero no es euclídeo para ninguna elección de la aplicación grado.

Una demostración completa de este hecho se puede encontrar indicada en el libro [B-M-T, ex.24].

2.3. Anillos de Dedekind

El objetivo de esta sección es dar las propiedades algebraicas más elementales de los anillos de los enteros de los cuerpos de números.

Proposición 2.3.1. *Sean A un dominio noetheriano e íntegramente cerrado, K el cuerpo de fracciones de A, $L|K$ una extensión finita y separable, y B la clausura entera de A en L. Entonces, B es un A-módulo finitamente generado.*

Demostración: Observemos, en primer lugar, que podemos elegir una K-base de L formada por elementos $b_1, b_2, \ldots, b_n \in B$. En efecto, sea $b \in L$ y sean $a_0, a_1, \ldots, a_{n-1} \in K$ tales que $a_0 + a_1 b + a_2 b^2 + \cdots + a_{n-1} b^{n-1} + b^n = 0$; sea $a \in A$ un denominador común de todos los coeficientes a_i; entonces, $a_0 a^n, a_1 a^{n-1}, \ldots, a_{n-1} a \in A$ y

$$a_0 a^n + a_1 a^{n-1}(ab) + \cdots + a_{n-1} a (ab)^{n-1} + (ab)^n = 0$$

es una ecuación de dependencia entera de ab sobre A. Por tanto, podemos multiplicar cada elemento de una K-base de L por un elemento de A para obtener una K-base de L formada por elementos de B.

Por otro lado, puesto que la extensión $L|K$ es finita y separable, la forma bilineal traza, $\mathrm{T}_{L|K}$, es no degenerada y podemos considerar la K-base de

L dual de la base $b_1, b_2, \ldots, b_n$ respecto de esta forma bilineal (cf. [B-M-T, ex.85]); sea $\beta_1, \beta_2, \ldots, \beta_n \in L$ esta base dual y sea $d \in A$, $d \neq 0$, un elemento tal que $d\beta_j \in B$ para todo β_j. Entonces, B es un A-submódulo del A-módulo libre y finitamente generado $M := d^{-1}(Ab_1 + \cdots + Ab_n) \subseteq L$. En efecto; sea $b \in B$ y escribámoslo en la forma $b = \alpha_1 b_1 + \cdots + \alpha_n b_n$ con los coeficientes $\alpha_i \in K$; puesto que $\mathrm{T}_{L|K}(b_i\beta_j) = \delta_{ij}$, obtenemos que $d\alpha_j = \mathrm{T}_{L|K}(db\beta_j) \in A$, ya que $db\beta_j \in B$ y la traza es la suma de los conjugados, que son enteros. Por tanto, $db \in Ab_1 + \cdots + Ab_n$, como queríamos demostrar.

Ahora, puesto que A es noetheriano, $B \subseteq M$ y M es un A-módulo finitamente generado, obtenemos que B es un A-módulo finitamente generado. □

Corolario 2.3.2. *Sean A un dominio principal, K el cuerpo de fracciones de A, $L|K$ una extensión finita y separable, $n := [L : K]$ el grado, y B la clausura entera de A en L. Entonces, B es un A-módulo libre de rango n.*

Demostración: Es bien conocido que si B es un módulo finitamente generado y sin torsión sobre un dominio de ideales principales, entonces B es un A-módulo libre. La proposición anterior nos asegura que B es un A-módulo finitamente generado; y la cuestión relativa a la torsión es inmediata, ya que B es un dominio de integridad. Finalmente, una A-base de B es también una K-base de L, ya que L es el cuerpo de fracciones de B. Por tanto, B es A-libre de rango $[L : K]$. □

Corolario 2.3.3. *El anillo de los enteros de un cuerpo de números es un $\mathbb{Z}$-módulo libre de rango finito.* □

Así, el anillo de los enteros de un cuerpo de números es un dominio noetheriano, íntegramente cerrado y de dimensión 1, ya que la extensión $A|\mathbb{Z}$ es entera y $\mathbb{Z}$ es de dimensión 1.

Definición 2.3.4. Llamaremos anillo de Dedekind a todo dominio de integridad noetheriano, íntegramente cerrado y de dimensión 1; es decir, un anillo noetheriano íntegro, íntegramente cerrado, que no es un cuerpo y tal que todo ideal primo no nulo es maximal.

Corolario 2.3.5. *El anillo de los enteros de un cuerpo de números es un anillo de Dedekind.* □

2.4. El grupo de ideales

Los anillos de Dedekind y, en particular, los anillos de enteros de los cuerpos de números, no son, en general, principales. De todas maneras, en un anillo de Dedekind todo ideal no nulo descompone de manera única como producto de ideales primos no nulos. Eso hace que el estudio de su aritmética (y, en consecuencia, de la aritmética de su cuerpo de fracciones) sea viable.

Definición 2.4.1. Sea A un dominio de integridad. Un ideal fraccionario de A es un A-submódulo $\mathfrak{a}$ del cuerpo de fracciones K de A tal que existe un elemento $a \in A$, $a \neq 0$, de manera que $a\mathfrak{a} \subseteq A$.

Por ejemplo, todo ideal de A es un ideal fraccionario. Los ideales de A también se llaman, por ello, los ideales enteros de A.

Definición 2.4.2. Un ideal fraccionario se llama principal si es de la forma aA con $a \in K$.

Claramente, los ideales fraccionarios principales no nulos de A forman un grupo abeliano respecto la multiplicación de ideales; el inverso de un ideal fraccionario principal aA es el ideal fraccionario principal $a^{-1}A$. Pero ésta no es la única propiedad interesante de los ideales fraccionarios de los anillos de Dedekind. De hecho, el conjunto de todos los ideales fraccionarios no nulos de un anillo de Dedekind es un grupo respecto la multiplicación de A-submódulos de K y el conjunto de los ideales fraccionarios principales no nulos es un subgrupo del grupo de todos los ideales fraccionarios. El objetivo de esta sección es demostrar este hecho, y también hacer el estudio de los ideales fraccionarios de los anillos de Dedekind.

Proposición 2.4.3. *Sea A un dominio de integridad. Todo A-submódulo finitamente generado $\mathfrak{a}$ del cuerpo de fracciones K de A es un ideal fraccionario.*

Demostración: Sea $a_1, a_2, \ldots, a_r$ un sistema finito de generadores de $\mathfrak{a}$ y sea $a \in A$ un denominador común de todos los elementos a_i. Entonces, $a\mathfrak{a} \subseteq A$. □

Proposición 2.4.4. *Sea A un dominio noetheriano. El conjunto de los ideales fraccionarios de A coincide con el conjunto de los A-submódulos finitamente generados del cuerpo de fracciones K. Con mayor precisión, todo ideal*

fraccionario es de la forma $a\mathfrak{a}$*, donde* $a \in K$ *y* $\mathfrak{a} \subseteq A$ *es un ideal entero de* A*.*

DEMOSTRACIÓN: Ya hemos visto que todo A-submódulo finitamente generado de K es un ideal fraccionario. Recíprocamente, supongamos que $\mathfrak{b} \subseteq K$ es un ideal fraccionario y sea $b \in A$ tal que $b\mathfrak{b} \subseteq A$. Entonces, $\mathfrak{b} \subseteq b^{-1}A$; puesto que $b^{-1}A$ es finitamente generado (de hecho, es principal) y A es noetheriano, el A-submódulo $\mathfrak{b}$ de $b^{-1}A$ ha de ser finitamente generado.

Por otro lado, si escribimos $\mathfrak{b} = \langle b_1, b_2, \ldots, b_r \rangle$, con $b_i \in K$, y si $a \in A$ es un denominador común de los elementos $b_1, b_2, \ldots, b_r$, entonces $\mathfrak{b} = a^{-1}\mathfrak{a}$, donde $\mathfrak{a} := \langle ab_1, ab_2, \ldots, ab_r \rangle$ es un ideal entero de A. □

Teorema 2.4.5. *Sea* A *un anillo de Dedekind. Entonces, el conjunto de los ideales fraccionarios no nulos de* A *es un grupo abeliano libre respecto la multiplicación de* A*-submódulos del cuerpo de fracciones* K *de* A*. Los ideales primos no nulos de* A *forman un sistema de generadores libres de este grupo. Además, condición necesaria y suficiente para que un ideal* $\mathfrak{a}$ *de* A *sea divisible por un ideal* $\mathfrak{b}$ *de* A *es que* $\mathfrak{a} \subseteq \mathfrak{b}$*.*

DEMOSTRACIÓN: Haremos la demostración de este teorema en diversas etapas.

Lema 2.4.6. *Sea* A *un anillo noetheriano y sea* $\mathfrak{a} \subseteq A$ *un ideal no nulo de* A*. Entonces, existen ideales primos no nulos* $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r \subseteq A$ *tales que* $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$*.*

DEMOSTRACIÓN: Si no fuese así, el conjunto $\mathcal{C}$ formado por los ideales no nulos de A que no contienen ningún producto de ideales primos no nulos sería un conjunto no vacío. Por ser A noetheriano, este conjunto ha de tener elementos maximales para la inclusión de ideales. Sea $\mathfrak{a}$ un elemento maximal de $\mathcal{C}$. El ideal $\mathfrak{a}$ no puede ser un ideal primo de A, ya que pertenece a $\mathcal{C}$; por tanto, existen elementos $a_1, a_2 \in A$ $a_1, a_2 \notin \mathfrak{a}$, tales que $a_1a_2 \in \mathfrak{a}$. Entonces, cadas uno de los ideales $\mathfrak{b}_i := \mathfrak{a} + a_iA$, $i = 1, 2$, contiene un producto de ideales primos de A y $\mathfrak{b}_1\mathfrak{b}_2 \subseteq \mathfrak{a}$. Pero entonces, $\mathfrak{a}$ contiene un producto de ideales primos: el ideal producto de los productos de ideales primos que contienen a los ideales $\mathfrak{b}_i$. Esta contradicción acaba la demostración. □

Lema 2.4.7. *Sea* A *un anillo de Dedekind y sea* $\mathfrak{p} \subseteq A$ *un ideal primo no nulo. Entonces,* $\mathfrak{p}$ *es un ideal fraccionario inversible; es decir, existe un ideal fraccionario* $\mathfrak{p}^{-1}$ *de* A *tal que* $\mathfrak{p}\mathfrak{p}^{-1} = A$*.*

DEMOSTRACIÓN: Sea $\mathfrak{p}^{-1} := (A : \mathfrak{p}) = \{x \in K : x\mathfrak{p} \subseteq A\}$, donde K designa el cuerpo de fracciones de A. Se trata de ver que $\mathfrak{p}\mathfrak{p}^{-1} = A$; comprobemos, en primer lugar, que $A \subsetneq \mathfrak{p}^{-1}$. Tomemos un elemento no nulo $a \in \mathfrak{p}$; en virtud del lema anterior, podemos elegir un número entero r minimal respecto a la propiedad que el ideal principal aA contenga un producto de r ideales primos no nulos de A, pongamos $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq aA$. Entonces, puesto que $\mathfrak{p}$ es un ideal primo, $\mathfrak{p}$ ha de contener alguno de los primos $\mathfrak{p}_i$, digamos $\mathfrak{p}_1$; y puesto que $\mathfrak{p}_1$ es maximal, ha de ser $\mathfrak{p}_1 = \mathfrak{p}$. Por otro lado, $\mathfrak{p}_2 \cdots \mathfrak{p}_r \nsubseteq aA$ ya que r es minimal; por tanto, existe un elemento $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ tal que $b \notin aA$. Entonces, $ba^{-1} \in \mathfrak{p}^{-1}$ (ya que $b\mathfrak{p} = b\mathfrak{p}_1 \subseteq aA$) pero $ba^{-1} \notin A$, como queríamos ver.

De la inclusión trivial $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq A$, y del hecho que $\mathfrak{p}$ es un ideal maximal, deducimos que $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$ o bien $\mathfrak{p}\mathfrak{p}^{-1} = A$. Veamos que la primera igualdad no puede ser y habremos acabado. Si fuese $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$, entonces todo elemento de $\mathfrak{p}^{-1}$ dejaría invariante el A-submódulo finitamente generado $\mathfrak{p}$ de K; por tanto, el ideal fraccionario $\mathfrak{p}^{-1}$ habría de estar formado por elementos enteros sobre A; y, puesto que A es íntegramente cerrado, eso querría decir que $\mathfrak{p}^{-1} \subseteq A$; contradicción. □

Lema 2.4.8. *Sea A un anillo de Dedekind. Entonces, todo ideal fraccionario no nulo $\mathfrak{a}$ de A es inversible. Además, el inverso de $\mathfrak{a}$ es el ideal fraccionario $\mathfrak{a}^{-1} := (A : \mathfrak{a}) = \{x \in K : x\mathfrak{a} \subseteq A\}$.*

DEMOSTRACIÓN: Puesto que A es un anillo noetheriano, la proposición 2.4.4 nos asegura que todo ideal fraccionario de A es el producto de un elemento a de K por un ideal entero $\mathfrak{a}$ de A; puesto que los ideales fraccionarios principales son inversibles, para ver que un ideal fraccionario $\mathfrak{a}$ es inversible podemos suponer que es un ideal entero. Así, es suficiente demostrar que todo ideal entero no nulo $\mathfrak{a} \subseteq A$ es inversible.

Si no fuese así, y de nuevo por la noetherianidad, podríamos elegir un ideal entero no nulo $\mathfrak{a} \subseteq A$ maximal entre los no inversibles. Puesto que los ideales maximales de A son inversibles, $\mathfrak{a}$ no es un ideal maximal de A y existe un ideal maximal $\mathfrak{p}$ de A tal que $\mathfrak{a} \subsetneq \mathfrak{p}$. Entonces, $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = A$. Puesto que el inverso de $\mathfrak{p}$ contiene elementos no enteros sobre A y puesto que $\mathfrak{a}$ es un A-submódulo finitamente generado de K, no puede ser $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$; es decir, $\mathfrak{a}\mathfrak{p}^{-1}$ es un ideal de A que contiene $\mathfrak{a}$ estrictamente. Por la maximalidad de $\mathfrak{a}$, el ideal $\mathfrak{a}\mathfrak{p}^{-1}$ es un ideal fraccionario inversible; si multiplicamos por $\mathfrak{p}$ que es inversible, obtenemos que $\mathfrak{a}$ es un ideal inversible.

Resta ver que el inverso de $\mathfrak{a}$ es $(A : \mathfrak{a})$. Pero eso es claro; si $a \in \mathfrak{a}^{-1}$, es claro que $a \in (A : \mathfrak{a})$; recíprocamente, si $a \in (A : \mathfrak{a})$, entonces $a\mathfrak{a} \subseteq A$, de manera que $a\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$ y, puesto que $1 \in A = \mathfrak{a}\mathfrak{a}^{-1}$, ha de ser $a \in \mathfrak{a}^{-1}$. Eso acaba la demostración. □

Acabamos de probar que el conjunto formado por los ideales fraccionarios no nulos de A es un grupo respecto la multiplicación de ideales fraccionarios. Si demostramos que todo ideal entero no nulo descompone de manera única como producto de ideales primos de A ya habremos acabado, ya que todo ideal fraccionario es de la forma $a^{-1}\mathfrak{a}$ para un cierto elemento $a \in A$ y un cierto ideal entero $\mathfrak{a} \subseteq A$.

El conjunto de los ideales no nulos de A que no admiten una descomposición como producto de ideales primos no nulos es el conjunto vacío; en efecto, en caso contrario, tendría un elemento maximal $\mathfrak{a} \subseteq A$; si $\mathfrak{p}$ es un ideal maximal de A que contiene $\mathfrak{a}$, puesto que $\mathfrak{p}$ es inversible, ha de ser $\mathfrak{a} \subsetneq \mathfrak{p}$; entonces, $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = A$, de manera que podemos repetir el razonamiento de antes: $\mathfrak{a}\mathfrak{p}^{-1}$ es un ideal entero de A que no puede coincidir con $\mathfrak{a}$ ya que $\mathfrak{p}^{-1}$ contiene elementos no enteros sobre A y $\mathfrak{a}$ es un A-submódulo finitamente generado de K; por tanto, $\mathfrak{a}\mathfrak{p}^{-1}$ admite descomposición como producto de ideales primos; si multiplicamos por $\mathfrak{p}$ obtenemos una descomposición de $\mathfrak{a}$ como producto de ideales primos de A.

Resta ver la unicidad. Pero esto es fácil, ya que disponemos de la multiplicación por los inversos de los ideales primos no nulos de A. Si $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$, el ideal $\mathfrak{q}_1$ es un ideal primo que contiene un producto de ideales primos; por tanto, contiene algún $\mathfrak{p}_i$, digamos $\mathfrak{p}_i = \mathfrak{p}_1$. La maximalidad nos permite asegurar que $\mathfrak{q}_1 = \mathfrak{p}_1$; si multiplicamos por el inverso de $\mathfrak{p}_1$, obtenemos la igualdad $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$, con menos factores, y la prueba se acaba fácilmente por un argumento recursivo. □

Definición 2.4.9. El grupo de los ideales fraccionarios no nulos del anillo de Dedekind A se llama el grupo de ideales de A (o el grupo de ideales de K cuando el anillo A es claro). El grupo cociente de este grupo de ideales por el subgrupo de los ideales fraccionarios principales se llama el grupo de clases de ideales de A (o de K). Se acostumbra a designar por $\mathrm{Cl}(A)$.

De hecho, se dispone de la sucesión exacta de grupos abelianos

$$1 \longrightarrow A^* \longrightarrow K^* \longrightarrow \mathbf{I}(A) \longrightarrow \mathrm{Cl}(A) \longrightarrow 1,$$

donde $\mathbf{I}(A)$ designa el grupo de los ideales fraccionarios no nulos de A y A^* el grupo de los elementos inversibles del anillo A.

2.5. Factorialidad y principalidad

Una consecuencia inmediata de la definición del grupo de clases de ideales de un anillo de Dedekind es el resultado siguiente.

Corolario 2.5.1. *Sea A un anillo de Dedekind. Condición necesaria y suficiente para que el anillo A sea un anillo principal es que el grupo de clases de ideales de A sea trivial.* □

Esta condición caracteriza cuando un anillo de Dedekind es principal. Podemos decir que el grupo $\mathrm{Cl}(A)$ es una medida de cuánto se aparta el anillo A de ser un anillo principal. De todas maneras, aunque todavía no sabemos casi nada del grupo de clases de ideales de un anillo de Dedekind, podemos dar alguna condición suficiente para que un anillo de Dedekind sea principal.

El hecho que los ideales primos de un anillo de Dedekind formen un sistema de generadores del grupo de ideales y el hecho que el producto de ideales principales es un ideal principal nos permiten escribir inmediatamente que si todos los ideales primos de un anillo de Dedekind A son principales, entonces A es un anillo principal. Incluso más, podemos demostrar el resultado siguiente.

Proposición 2.5.2. *Sea A un anillo de Dedekind. Supongamos que A tiene solamente un número finito de ideales primos. Entonces, A es un anillo principal.*

Demostración: Sean $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ todos los ideales primos no nulos de A. Fijado uno de ellos, digamos $\mathfrak{p} = \mathfrak{p}_1$, podemos elegir $a \in \mathfrak{p}$ de manera que $a \notin \mathfrak{p}^2$; el sistema de congruencias

$$\begin{cases} x \equiv a & \mod \mathfrak{p} \\ x \equiv 1 & \mod \mathfrak{p}_i,\ i > 1, \end{cases}$$

tiene solución en A en virtud del teorema chino del resto. Y una solución x de este sistema es un generador del ideal $\mathfrak{p}$, ya que en la descomposición en

producto de ideales primos del ideal principal xA no puede aparecer ningún primo $\mathfrak{p}_i \neq \mathfrak{p}$ ni tampoco $\mathfrak{p}^2$; y el ideal xA no es todo el anillo A ya que $x \in \mathfrak{p}$ porque para x se safisface la primera ecuación.

En consecuencia, todo ideal primo de A es un ideal principal y, por tanto, A es un anillo principal. □

Proposición 2.5.3. *Sea A un anillo de Dedekind y supongamos que el grupo de clases de ideales de A es finitamente generado. Entonces, existe un elemento $a \in A$, $a \neq 0$, tal que el anillo $A[a^{-1}]$ es un anillo de Dedekind principal.*

Demostración: Notemos, en primer lugar, que cualquier localizado de un anillo de Dedekind es un anillo de Dedekind. En efecto, si S es un conjunto multiplicativamente cerrado de un anillo de Dedekind A, entonces el anillo $S^{-1}A$ es un dominio noetheriano, es íntegramente cerrado y es de dimensión 1; por tanto, es un anillo de Dedekind.

Para demostrar la proposición, sean $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r \subseteq A$ ideales primos tales que sus clases generen $\mathrm{Cl}(A)$ y sea $a \neq 0$ un elemento $a \in \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_r$. Entonces, el anillo $A[a^{-1}]$ es el localizado de A en las potencias de a y, por tanto, las extensiones de los ideales $\mathfrak{p}_i$ coinciden con todo el anillo $A[a^{-1}]$. Por otro lado, la asignación $\mathfrak{a} \mapsto \mathfrak{a}A[a^{-1}]$ define un morfismo exhaustivo de grupos entre los grupos de ideales fraccionarios no nulos de los anillos A y $A[a^{-1}]$; su núcleo está formado por los ideales fraccionarios de A que contienen alguna potencia de a. Además, los ideales fraccionarios principales de A van a parar a ideales fraccionarios principales de $A[a^{-1}]$, de manera que el grupo $\mathrm{Cl}(A)$ se aplica exhaustivamente en el grupo $\mathrm{Cl}(A[a^{-1}])$. Puesto que las imágenes de un sistema de generadores forman un sistema de generadores, y puesto que los ideales $\mathfrak{p}_i$ se aplican en el ideal unidad, el grupo $\mathrm{Cl}(A[a^{-1}])$ es el grupo trivial. □

Seguidamente se trata de caracterizar cuando un anillo de Dedekind es factorial. En concreto, se trata de demostrar el resultado siguiente.

Proposición 2.5.4. *Sea A un anillo de Dedekind. Condición necesaria y suficiente para que A sea factorial es que sea principal.*

Demostración: Supongamos que A es un anillo de Dedekind factorial y que $\mathfrak{p} \subseteq A$ es un ideal primo no nulo; hemos de ver que $\mathfrak{p}$ es un ideal principal. Sea $a \neq 0$ un elemento de $\mathfrak{p}$; puesto que A es factorial, este elemento

a admite una factorización $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, $\alpha_i \geq 1$, como producto de elementos irreducibles diferentes p_i de A. Puesto que $\mathfrak{p}$ es primo, alguno de los elementos irreducibles p_i ha de ser un elemento de $\mathfrak{p}$. Entonces, el ideal principal generado por p_i es un ideal primo, ya que A es un anillo factorial, y está incluído en $\mathfrak{p}$; puesto que en A todo ideal primo no nulo es maximal, ha de ser $\mathfrak{p} = p_i A$. $\square$

Capítulo 3

Ramificación

Este capítulo se dedica al estudio de extensiones de anillos de Dedekind y del comportamiento de los ideales primos en estas extensiones. Comencemos por repasar los conceptos y las propiedades de la traza y la norma.

3.1. Normas y trazas

Sea $L|K$ una extensión finita de cuerpos. Para todo elemento $\theta \in L$ podemos definir una aplicación K-lineal $\mathfrak{m}_\theta : L \longrightarrow L$ por la fórmula $\mathfrak{m}_\theta(\theta') := \theta\theta'$, para todo $\theta' \in L$. Si elegimos una K-base de L, $\{\theta_1, \theta_2, \ldots, \theta_n\}$, la aplicación lineal $\mathfrak{m}_\theta$ tiene asociada una matriz $(a_{i,j}) \in \mathcal{M}_n(K)$, donde $\mathcal{M}_n(K)$ indica el espacio vectorial de las matrices cuadradas de n filas y n columnas y coeficientes en K. El polinomio característico de la matriz $(a_{i,j})$ no depende de la base elegida. En particular, la traza, $\mathrm{T}_{L|K}(\theta) := \mathrm{tr}(a_{i,j}) = \sum_{i=1}^{n} a_{i,i}$, y el determinante, $\mathrm{N}_{L|K}(\theta) := \det(a_{i,j})$, no dependen de la base.

Definición 3.1.1. Las aplicaciones $\mathrm{T}_{L|K} : L \longrightarrow K$ y $\mathrm{N}_{L|K} : L \longrightarrow K$ definidas por las fórmulas $\mathrm{T}_{L|K}(\theta) := \mathrm{tr}(a_{i,j}) = \sum_{i=1}^{n} a_{i,i}$, y $\mathrm{N}_{L|K}(\theta) := \det(a_{i,j})$, se llaman, respectivamente, la traza y la norma de la extensión $L|K$.

Listemos a continuación las propiedades más elementales de estas aplicaciones $\mathrm{T}_{L|K}$ y $\mathrm{N}_{L|K}$.

Proposición 3.1.2. *Sean $\theta, \theta_1, \theta_2 \in L$ y $\alpha \in K$. Entonces:*

(a) $\mathrm{T}_{L|K}(\theta_1 + \theta_2) = \mathrm{T}_{L|K}(\theta_1) + \mathrm{T}_{L|K}(\theta_2)$;

(b) $\mathrm{T}_{L|K}(\alpha\theta) = \alpha \mathrm{T}_{L|K}(\theta)$;

(c) $\mathrm{N}_{L|K}(\theta_1\theta_2) = \mathrm{N}_{L|K}(\theta_1)\mathrm{N}_{L|K}(\theta_2)$; *y*

(d) $\mathrm{N}_{L|K}(\alpha\theta) = \alpha^n \mathrm{N}_{L|K}(\theta)$,

donde $n := [L : K]$ es el grado de la extensión $L|K$. □

Los resultados siguientes nos proporcionan una manera cómoda para calcular la traza y la norma.

Proposición 3.1.3. *Sean $L|K$ una extensión finita de cuerpos, $\theta \in L$ un elemento cualquiera, s el grado de separabilidad de la extensión $L|K$, σ_1, σ_2, ..., σ_s las K-inclusiones diferentes de L en una clausura algebraica de K, y p^i el grado de inseparabilidad de la extensión $L|K$. Entonces,*

$$\mathrm{T}_{L|K}(\theta) = p^i \left(\sigma_1(\theta) + \cdots + \sigma_s(\theta)\right)$$
$$\mathrm{N}_{L|K}(\theta) = \left(\sigma_1(\theta) \cdots \sigma_s(\theta)\right)^{p^i}.$$

En particular, si la extensión $L|K$ no es separable, entonces $\mathrm{T}_{L|K} = 0$.

Demostración: Supongamos, en primer lugar, que θ es un elemento primitivo de la extensión $L|K$. Sean $f(X) := \mathrm{Irr}(\theta, K)$ el polinomio mónico irreducible de $K[X]$ que tiene θ por raíz y $g(X)$ el polinomio característico de la multiplicación $\mathfrak{m}_\theta$. Puesto que $g(\mathfrak{m}_\theta) = 0$, también $g(\theta) = 0$ y el polinomio $f(X)$ divide el polinomio $g(X)$. Además, los dos polinomios $f(X)$ y $g(X)$ tienen el mismo grado, $n := sp^i$, y ambos son mónicos; por tanto, coinciden. Eso nos permite asegurar que $\mathrm{T}_{L|K}(\theta)$ es la suma de los n conjugados de θ y que $\mathrm{N}_{L|K}(\theta)$ es el producto de los n conjugados de θ, ya que las raíces del polinomio irreductible de θ sobre K son los s conjugados diferentes, $\sigma_j(\theta)$, contados p^i veces cada uno.

En el caso general, si θ no es un elemento primitivo, aún podemos considerar el subcuerpo $K' := K(\theta)$ de L. Si elegimos una K-base de K' y una K'-base de L cualesquiera, los productos forman una K-base de L y la matriz de la multiplicación por θ en L en esta base se puede escribir en forma de matriz diagonal de cajas idénticas a la matriz de la multiplicación por θ

en K'. Por tanto, el polinomio característico de la multiplicación por θ en la extensión $L|K$ es la potencia $[L : K']$-ésima del polinomio característico de la multiplicación por θ en la extensión $K'|K$; en particular, la traza $\mathrm{T}_{L|K}(\theta)$ es el producto $[L : K']\mathrm{T}_{K'|K}(\theta)$ y la norma $\mathrm{N}_{L|K}(\theta)$ es la potencia $\big(\mathrm{N}_{K'|K}(\theta)\big)^{[L:K']}$. Para acabar la demostración, basta tener en cuenta que las s K-inmersiones diferentes de L se distribuyen, según los valores que toman sobre θ, en tantas clases de equivalencia como el grado de separabilidad de la extensión $K'|K$, y que todas las clases tienen cardinal igual al grado de separabilidad de la extensión $L|K'$. □

Proposición 3.1.4. *Sean $L|K'$ y $K'|K$ extensiones finitas de cuerpos. Entonces, para todo $\theta \in L$ se satisfacen las fórmulas de transitividad $\mathrm{T}_{L|K}(\theta) = \mathrm{T}_{K'|K}\big(\mathrm{T}_{L|K'}(\theta)\big)$ y $\mathrm{N}_{L|K}(\theta) = \mathrm{N}_{K'|K}\big(\mathrm{N}_{L|K'}(\theta)\big)$. Es decir, como aplicaciones, $\mathrm{T}_{L|K} = \mathrm{T}_{K'|K} \circ \mathrm{T}_{L|K'}$ y $\mathrm{N}_{L|K} = \mathrm{N}_{K'|K} \circ \mathrm{N}_{L|K'}$.*

Demostración: Basta tener en cuenta que las K-inmersiones de L son las extensiones diferentes a L de las K-inmersiones de K' y de qué manera se obtienen a partir de las K'-inmersiones de L. □

La forma lineal traza nos permite definir de manera natural, ya que L es una K-álgebra, una aplicación bilineal $\mathrm{T}_{L|K} : L \times L \longrightarrow K$ por la fórmula $(a, b) \mapsto \mathrm{T}_{L|K}(ab)$. Puesto que L es conmutativo, la forma bilineal es simétrica. El resultado que sigue ya ha sido usado en un par de ocasiones.

Proposición 3.1.5. *Sea $L|K$ una extensión finita de cuerpos y consideremos $T_{L|K} : L \times L \longrightarrow K$ la forma bilineal simétrica definida por $(x, y) \mapsto \mathrm{T}_{L|K}(xy)$. Para que la extensión $L|K$ sea separable es condición necesaria y suficiente que la forma $\mathrm{T}_{L|K}$ sea no degenerada; es decir, que de la igualdad $\mathrm{T}_{L|K}(xy) = 0$ para todo $y \in L$ se deduzca que $x = 0$.*

Demostración: Supongamos, en primer lugar, que la extensión $L|K$ es separable y sea θ un elemento primitivo de la extensión. El conjunto $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$, donde $n := [L : K]$ designa el grado de la extensión $L|K$, es una K-base de L. Sea $D := (d_{i,j})$ la matriz de la forma bilineal $\mathrm{T}_{L|K}$ en esta base; es decir, $d_{i,j} := \mathrm{T}_{L|K}(\theta^{i-1}\theta^{j-1})$. Hay que ver que la matriz D es no singular; es decir, que $\det D \neq 0$.

Para ello, consideremos la matriz de Vandermonde

$$V = V(\theta_1, \theta_2, \ldots, \theta_n) := \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \theta_1 & \theta_2 & \ldots & \theta_n \\ \theta_1^2 & \theta_2^2 & \ldots & \theta_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1^{n-1} & \theta_2^{n-1} & \ldots & \theta_n^{n-1} \end{pmatrix},$$

donde los elementos θ_i son los diferentes conjugados de $\theta_1 := \theta$. La traza de θ es la suma de los conjugados, $\theta_1 + \cdots + \theta_n$; análogamente, para todo número entero k, la traza de θ^k es la suma de sus conjugados, $\theta_1^k + \cdots + \theta_n^k$. Eso implica que la matriz D es el producto $D = VV^t$ de V por su matriz transpuesta; por tanto, el determinante de D es el cuadrado del determinante de la matriz V, que es no nulo ya que los elementos θ_i, θ_j son diferentes para $i \neq j$.

Recíprocamente, ya hemos visto que si la extensión $L|K$ no es separable, entonces $\mathrm{T}_{L|K} = 0$. □

3.2. Extensiones de anillos de Dedekind

En algunas aplicaciones, los anillos de Dedekind son extensiones de otros anillos de Dedekind. Concretamente, en el caso de los cuerpos de números, el anillo de los enteros de un cuerpo de números L, extensión de K, es la clausura entera en L del anillo de los enteros de K. Este resultado es más general.

Proposición 3.2.1. *Sean A un anillo de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión finita y B la clausura entera de A en L. Entonces, B es un anillo de Dedekind.*

Demostración: El anillo B es íntegramente cerrado, ya que es una clausura entera, y es de dimensión 1, ya que A lo es y la extensión $B|A$ es entera. Resta ver la noetherianidad.

Sea $K' \subseteq L$ la clausura separable de K en L. Eso quiere decir que la extensión $K'|K$ es separable y la extensión $L|K'$ es puramente inseparable. Sea A' la clausura entera de A en K'; entonces, B también es la clausura

entera de A' en L. Ello hace que podamos hacer la prueba de la proposición en dos etapas y con una hipótesis suplementaria para cada una de ellas: en primer lugar, podemos suponer que la extensión $L|K$ es separable; y después, que la extensión $L|K$ es puramente inseparable. Y, en el caso separable, la noetherianidad queda asegurada por la proposición 2.3.1.

Supongamos, pues, que la extensión $L|K$ es puramente inseparable. Puesto que es finita, existe un número entero q, potencia de la característica, de manera que $L^q \subseteq K$. Consideremos el cuerpo M, extensión de L, definido por la condición $M^q = K$; es decir, $x \in M \Longleftrightarrow x^q \in K$. La clausura entera, C, de A en M es el anillo definido por la condición $x \in C \Longleftrightarrow x^q \in A$. El morfismo de cuerpos $M \longrightarrow K$ definido por $x \mapsto x^q$ es un isomorfismo y, en consecuencia, su restricción $C \longrightarrow A$ también es un isomorfismo; por tanto, el anillo C es un anillo de Dedekind. De aquí deduciremos la noetherianidad de B.

Sea $\mathfrak{a}$ un ideal no nulo de B y sea $\mathfrak{A}$ su extensión al anillo C; puesto que C es un anillo de Dedekind, el ideal $\mathfrak{A}$ es inversible y su inverso es el ideal fraccionario $(C : \mathfrak{A})$. Eso nos permite asegurar que existen elementos $a_i \in \mathfrak{a}$ y elementos $c_i \in (C : \mathfrak{A})$ tales que $\sum_i a_i c_i = 1$. Elevando a q, obtenemos la igualdad $\sum_i a_i a_i^{q-1} c_i^q = 1$, que tiene coeficientes $b_i := a_i^{q-1} c_i^q \in L$, ya que $a_i \in \mathfrak{a}$ y $c_i \in M$. Aún más, $b_i \mathfrak{a} \subseteq c_i^q \mathfrak{a}^q \subseteq C$, ya que $c_i \in (C : \mathfrak{A})$ y $\mathfrak{a} \subseteq \mathfrak{A}$. Por tanto, $b_i \mathfrak{a} \subseteq C \cap L = B$, de manera que $b_i \in (B : \mathfrak{a})$; ahora, la igualdad $\sum_i a_i c_i = 1$ implica que $\mathfrak{a}(B : \mathfrak{a}) = B$ y, en consecuencia, el ideal $\mathfrak{a}$ es un ideal inversible de B.

Dicho de otra manera, hemos probado que todo ideal no nulo de B es inversible. Pero eso ya implica que B es un anillo noetheriano; en efecto, sea $\mathfrak{a} \subseteq B$ un ideal no nulo; podemos elegir elementos $a_1, a_2, \ldots, a_r \in \mathfrak{a}$ y elementos $b_1, b_2, \ldots, b_r \in (B : \mathfrak{a})$ tales que $\sum_{i=1}^{r} a_i b_i = 1$; en este caso, $\{a_1, a_2, \ldots, a_r\}$ es un sistema de generadores de $\mathfrak{a}$, ya que si $a \in \mathfrak{a}$, entonces $ab_i \in B$ y $\sum_{i=1}^{r} a_i a b_i = a$. Así, todo ideal de B es finitamente generado. □

3.3. Índice de ramificación y grado residual

Sean A un anillo de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión finita y B la clausura entera de A en L. En la sección anterior hemos visto que B también es un anillo de Dedekind. En particular, si $\mathfrak{p} \subseteq A$ es un ideal primo no nulo de A, su extensión a B, $\mathfrak{p}B$, es un ideal no nulo que no es todo el anillo B porque la extensión $B|A$ es entera. Por tanto, el ideal $\mathfrak{p}B$ descompone en producto de ideales primos de B de manera única.

Sea $\mathfrak{p}B = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$ esta descomposición en factores primos; eso quiere decir que los ideales $\mathfrak{P}_i$, $1 \leq i \leq g$, son ideales primos no nulos y diferentes de B y que $e_i \geq 1$ son enteros.

Definición 3.3.1. Se llama índice de ramificación de $\mathfrak{P}_i$ sobre $\mathfrak{p}$ el número entero e_i. Se acostumbra a designar por $e(\mathfrak{P}_i|\mathfrak{p})$ o por $e_{\mathfrak{P}_i|\mathfrak{p}}$.

Observemos que podemos partir de un ideal primo $\mathfrak{P} \subseteq B$, considerar su contracción $\mathfrak{p} := \mathfrak{P} \cap A$ en A y después mirar cual es el exponente de $\mathfrak{P}$ en la descomposición de $\mathfrak{p}B$ en ideales primos de B; eso siempre da un exponente $e(\mathfrak{P}|\mathfrak{p}) \geq 1$ ya que $\mathfrak{P} \supseteq \mathfrak{p}B$ y, por tanto, $\mathfrak{P}$ es un ideal primo que divide el ideal $\mathfrak{p}B$.

Definición 3.3.2. Sea $\mathfrak{p}$ un ideal primo no nulo del anillo de Dedekind A. El anillo cociente, $A/\mathfrak{p}$, es un cuerpo, ya que $\mathfrak{p}$ es un ideal maximal de A. Se llama el cuerpo residual de A en $\mathfrak{p}$.

Consideremos, ahora, los cuerpos residuales de A en $\mathfrak{p}$ y de B en $\mathfrak{P}$. El morfismo de anillos $A \xrightarrow{inc} B$ dado por la inclusión de A en B da lugar por paso al cociente a un morfismo de los cuerpos residuales $A/\mathfrak{p} \longrightarrow B/\mathfrak{P}$, ya que $\mathfrak{P} \cap A = \mathfrak{p}$. Eso nos permite asegurar que el cuerpo residual de B en $\mathfrak{P}$ es un cuerpo extensión del cuerpo residual de A en $\mathfrak{p}$.

Proposición 3.3.3. *Sean A un anillo de Dedekind, K el cuerpo de fracciones de A, $L|K$ una extensión finita, B la clausura entera de A en L, $\mathfrak{P}$ un ideal primo no nulo de B, y $\mathfrak{p} := \mathfrak{P} \cap A$ su contracción a A. Entonces, la extensión de los cuerpos residuales $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ es una extensión finita de grado $[B/\mathfrak{P} : A/\mathfrak{p}] \leq [L : K]$.*

Demostración: Comencemos por hacer un proceso de localización con la finalidad de hacer que el anillo A sea principal. Para ello, sea $S := A - \mathfrak{p}$ el

complementario del ideal primo $\mathfrak{p}$ de A y consideremos los anillos localizados $S^{-1}A$ y $S^{-1}B$. Los localizados de anillos de Dedekind son anillos de Dedekind, de manera que $S^{-1}A$ es aún un anillo de Dedekind; además, $S^{-1}A$ solamente tiene un ideal maximal: el ideal $\mathfrak{p}S^{-1}A$; por tanto, en virtud de la proposición 2.5.2, el anillo $S^{-1}A$ es un anillo de Dedekind principal. Por otro lado, el anillo $S^{-1}B$ es la clausura entera de $S^{-1}A$ en L y, puesto que la localización y el paso al cociente conmutan, aún tenemos isomorfismos $A/\mathfrak{p} \simeq S^{-1}A/\mathfrak{p}S^{-1}A$ y $B/\mathfrak{P} \simeq S^{-1}B/\mathfrak{P}S^{-1}B$. Además, se satisface la igualdad $\mathfrak{P}S^{-1}B \cap S^{-1}A = \mathfrak{p}S^{-1}A$. Estas consideraciones hacen que podamos suponer, a la hora de hacer la demostración, que el ideal $\mathfrak{p}$ es un ideal principal.

Sea, pues, $\pi \in \mathfrak{p}$ un generador de $\mathfrak{p}$. Supongamos que en $B/\mathfrak{P}$ tenemos un conjunto $\{b_i + \mathfrak{P}\}_i$ formado por elementos $A/\mathfrak{p}$-linealmente independientes, donde $b_i \in B$; entonces, el conjunto $\{b_i\}_i$ es un conjunto de elementos de B linealmente independientes. En efecto, si tuviésemos una relación no trivial de dependencia lineal $\sum_i a_i b_i = 0$ con $a_i \in K$, podríamos quitar denominadores de los a_i y suponer que $a_i \in A$ para todo i; y después de dividir por una potencia adecuada de π, podríamos suponer que alguno de los elementos a_i no pertenece al ideal primo $\mathfrak{p}$; reduciendo esta ecuación módulo $\mathfrak{P}$, obtendríamos una relación de dependencia lineal de los elementos $b_i + \mathfrak{P}$ de coeficientes en $A/\mathfrak{p}$, alguno de ellos no nulo.

Dicho de otra manera, elementos $A/\mathfrak{p}$-linealmente independientes de $B/\mathfrak{P}$ provienen de elementos K-linealmente independientes de L, de manera que el grado de la extensión residual en $\mathfrak{P}$ es menor o igual que el grado de la extensión $L|K$. □

Definición 3.3.4. El grado $[B/\mathfrak{P} : A/\mathfrak{p}]$ se llama el grado residual en $\mathfrak{P}$ de la extensión de anillos $B|A$. Cuando no hay confusión posible sobre cual es el anillo A (y, en consecuencia, B) también se habla del grado residual de $L|K$ en $\mathfrak{P}$. Se acostumbra a designar por $f(\mathfrak{P}|\mathfrak{p})$ o por $f_{\mathfrak{P}|\mathfrak{p}}$.

Una propiedad muy importante y, a la vez, de demostración inmediata, es la multiplicatividad de los índices de ramificación y de los grados residuales en cadenas de extensiones finitas. Concretamente, se satisface el resultado siguiente.

Proposición 3.3.5. *Sean A un anillo de Dedekind, K su cuerpo de fracciones, $K'|K$ y $L|K'$ extensiones finitas, A' la clausura entera de A en K',*

B la clausura entera de A' en L, $\mathfrak{P} \subseteq B$ un ideal primo no nulo de B, $\mathfrak{P}' := \mathfrak{P} \cap A'$ su contracción a A' y $\mathfrak{p} := \mathfrak{P} \cap A = \mathfrak{P}' \cap A$ la contracción a A de $\mathfrak{P}$ y de $\mathfrak{P}'$. Entonces se satisfacen las fórmulas:

$$\begin{aligned} e(\mathfrak{P}|\mathfrak{p}) &= e(\mathfrak{P}|\mathfrak{P}')e(\mathfrak{P}'|\mathfrak{p}), \\ f(\mathfrak{P}|\mathfrak{p}) &= f(\mathfrak{P}|\mathfrak{P}')f(\mathfrak{P}'|\mathfrak{p}), \\ g(\mathfrak{p}) &= \sum_{\mathfrak{P}' \cap A = \mathfrak{p}} g(\mathfrak{P}'). \square \end{aligned}$$

Definición 3.3.6. Sean $B|A$ una extensión finita y entera de anillos de Dedekind, $\mathfrak{P} \subseteq B$ un ideal primo de B y $\mathfrak{p} := \mathfrak{P} \cap A$ su contracción a A. Se dice que la extensión $B|A$ es ramificada en $\mathfrak{P}$ cuando la extensión residual en $\mathfrak{P}$ no es separable o bien $e(\mathfrak{P}|\mathfrak{p}) > 1$; se dice que la extensión $B|A$ es ramificada en $\mathfrak{p}$ cuando hay algún ideal primo $\mathfrak{P}$ en B tal que $\mathfrak{P}^2$ divide $\mathfrak{p}B$ o bien la extensión residual en $\mathfrak{P}$ no es separable. Se dice que la extensión $B|A$ es no ramificada en $\mathfrak{P} \subseteq B$ cuando la extensión residual $B|\mathfrak{P}$ de $A|\mathfrak{p}$ es separable y $e(\mathfrak{P}|\mathfrak{p}) = 1$. Se dice que la extensión $B|A$ es no ramificada en el primo $\mathfrak{p} \subseteq A$ cuando es no ramificada en todo ideal primo $\mathfrak{P} \subseteq B$ que divide $\mathfrak{p}$.

3.4. La fórmula $\sum e_i f_i = n$

Acabamos de ver que a cada extensión finita y entera, $B|A$, de anillos de Dedekind le podemos asociar tres familias importantes de invariantes: las familias $\{e(\mathfrak{P}|\mathfrak{p})\}_{\mathfrak{P}}$, de los índices de ramificación de los ideals primos no nulos $\mathfrak{P} \subseteq B$; $\{f(\mathfrak{P}|\mathfrak{p})\}_{\mathfrak{P}}$, de los grados residuales; y $\{g(\mathfrak{p})\}_{\mathfrak{p}}$, de los números de ideales primos de B que dividen los ideales primos no nulos $\mathfrak{p} \subseteq A$. Se trata, seguidamente, de demostrar una relación, quizás la más importante, entre estos invariantes.

Proposición 3.4.1. *Sean A un anillo de Dedekind, K el cuerpo de fracciones de A, $L|K$ una extensión finita, $n := [L : K]$ el grado, B la clausura entera de A en L y $\mathfrak{p}$ un ideal primo no nulo de A. Sea $\mathfrak{p}B = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_g^{e_g}$ la descomposición de $\mathfrak{p}B$ en factores primos en B. Entonces, se satisface la desigualdad*

$$\sum_{i=1}^{g} e_i f_i \leq n.$$

La suma $\sum_{i=1}^{g} e_i f_i$ *es la dimensión de* $B/\mathfrak{p}B$ *como* $A/\mathfrak{p}$*-espacio vectorial.*

DEMOSTRACIÓN: Sea $S := A - \mathfrak{p}$. Entonces, el anillo $S^{-1}A$ es un anillo de Dedekind principal y local con ideal maximal $\mathfrak{p}S^{-1}A$. El anillo $S^{-1}B$ es la clausura entera de $S^{-1}A$ en L, los ideales $\mathfrak{P}_i S^{-1}B$ son los ideales primos de $S^{-1}B$, se satisface la descomposición $\mathfrak{p}S^{-1}B = \mathfrak{P}_1^{e_1} S^{-1}B \cdots \mathfrak{P}_g^{e_g} S^{-1}B$, y se tienen isomorfismos $A/\mathfrak{p} \simeq S^{-1}A/\mathfrak{p}S^{-1}A$ y $B/\mathfrak{P}_i \simeq S^{-1}B/\mathfrak{P}_i S^{-1}B$. Por tanto, e igual que en la demostración de la proposición 3.3.3, podemos suponer que A es un anillo de Dedekind local (y, por tanto, principal). Con esta hipótesis suplementaria, el anillo de Dedekind B solamente tiene un número finito de ideales primos y, en consecuencia, es principal. Por tanto, podemos razonar de la manera siguiente. En primer lugar, el teorema chino del resto nos permite escribir el isomorfismo de anillos

$$B/\mathfrak{p}B \simeq \prod_{i=1}^{g} B/\mathfrak{P}_i^{e_i}.$$

Por tanto, si demostramos que $B/\mathfrak{P}_i^{e_i}$ tiene dimensión $e_i f_i$ sobre $A/\mathfrak{p}$, obtendremos el valor de la suma $\sum_{i=1}^{g} e_i f_i$ como la dimensión de $B/\mathfrak{p}B$. Aunque el anillo $B/\mathfrak{P}_i^{e_i}$ no es, en general, un $B/\mathfrak{P}_i$-espacio vectorial, sus ideales $\mathfrak{P}_i^a/\mathfrak{P}_i^{e_i}$, $0 \leq a \leq e_i - 1$, forman una cadena de cocientes $\mathfrak{P}_i^a/\mathfrak{P}_i^{a+1}$ que son $B/\mathfrak{P}_i$-espacios vectoriales de dimensión 1 (la multiplicación por la potencia a-ésima de un generador de $\mathfrak{P}_i$ define un isomorfismo de $B/\mathfrak{P}_i$ en $\mathfrak{P}_i^a/\mathfrak{P}_i^{a+1}$). Para acabar la demostración de la segunda propiedad basta tener en cuenta que el $A/\mathfrak{p}$-espacio vectorial $B/\mathfrak{P}_i$ es de dimensión f_i.

Resta demostrar que la dimensión de $B/\mathfrak{p}B$ como $A/\mathfrak{p}$-espacio vectorial es menor o igual que el grado $[L : K]$. Claramente, el anillo $B/\mathfrak{p}B$ es un $A/\mathfrak{p}A$-espacio vectorial, y $\mathfrak{p}B \cap A = \mathfrak{p}$; sea $\{b_i\}_i$ un conjunto de elementos de B tales que sus clases $b_i + \mathfrak{p}B$ sean $A/\mathfrak{p}$-linealmente independientes. Si tuviésemos una relación no trivial de dependncia lineal $\sum_i a_i b_i = 0$ en L con los coeficientes $a_i \in K$, multiplicando (o dividiendo) por una potencia adecuada de un generador π del ideal $\mathfrak{p}$ podríamos suponer que todos los coeficientes a_i son de A y que alguno de ellos no es del ideal $\mathfrak{p}$; la reducción de esta igualdad módulo el ideal $\mathfrak{p}B$ daría una relación no trivial de dependencia

lineal de los elementos $b_i + \mathfrak{p}B$. Eso nos permite asegurar que la dimensión de $B/\mathfrak{p}B$ como $A/\mathfrak{p}$-espacio vectorial no puede superar la dimensión de L como K-espacio vectorial. Esto acaba la demostración. □

Observación 3.4.2. Si en esta demostración el anillo $S^{-1}B$ es un $S^{-1}A$-módulo finitamente generado (por ejemplo, cuando B es un A-módulo finitamente generado), entonces la dimensión de $B/\mathfrak{p}B$ como $A/\mathfrak{p}$-espacio vectorial y el grado $[L : K]$ coinciden.

En efecto, el lema de Nakayama nos permite asegurar que un sistema minimal de generadores de $S^{-1}B$ como $S^{-1}A$-módulo da lugar, por reducción, a una $A/\mathfrak{p}$-base de $B/\mathfrak{p}B$; y en la demostración de la proposición hemos visto que estos elementos son K-linealmente independientes de L. Sea $\{b_1, b_2, \ldots, b_n\}$ un sistema minimal de generadores de $S^{-1}B$ como $S^{-1}A$-módulo. Puesto que $L = S^{-1}BK$, si $b \in L$ es un elemento cualquiera, entonces existe $a \in S^{-1}A$ tal que $ab \in S^{-1}B$; por tanto, ab pertenece al K-subespacio vectorial de L generado por los elementos b_i, de manera que b ha de pertenecer a este subespacio. Eso demuestra que un sistema minimal de generadores de $S^{-1}B$ como $S^{-1}A$-módulo es automáticamente una K-base de L. Por tanto, las dos dimensiones coinciden.

Dicho de otra manera, hemos demostrado una de las implicaciones del resultado siguiente.

Proposición 3.4.3. *Mantengamos las mismas notaciones que en la proposición anterior y pongamos $S := A - \mathfrak{p}$. Entonces, condición necesaria y suficiente para que la dimensión de $B/\mathfrak{p}B$ como $A/\mathfrak{p}$-espacio vectorial coincida con el grado $[L : K]$ es que el anillo $S^{-1}B$ sea un $S^{-1}A$-módulo finitamente generado.*

Demostración: Solamente resta ver la necesidad de la condición. De nuevo podemos suponer que A es principal; en este caso, ya hemos visto que un conjunto $\{b_1, b_2, \ldots, b_r\}$ de elementos de B que den una base del cociente $B/\mathfrak{p}B$ sobre $A/\mathfrak{p}$ es automáticamente un conjunto de elementos de L que son K-linealmente independientes. Puesto que estamos suponiendo que las dos dimensiones son iguales, eso implica que $\{b_1, b_2, \ldots, b_r\}$ es una K-base de L. Veamos que es un sistema de generadores de B como A-módulo y habremos acabado. Si $b \in B$, podemos escribir $b = \sum_{i=1}^{r} a_i b_i$ con $a_i \in K$; si algún

coeficiente a_i no fuese de A, multiplicando por una potencia positiva adecuada de un generador π de $\mathfrak{p}$, obtendríamos una igualdad $\pi^k b = \sum_{i=1}^{r} (\pi^k a_i) b_i$ con los coeficientes $\pi^k a_i \in A$, alguno d'ellos inversible; Esta igualdad daría, por reducción módulo $\mathfrak{p}B$ una relación no trivial de dependencia lineal de los elementos b_i en $B/\mathfrak{p}B$, contradiciendo el hecho que los elementos b_i son una $A/\mathfrak{p}$-base de $B/\mathfrak{p}B$. □

Observación 3.4.4. En particular, la condición de generación finita de la proposición se satisface en el caso en que la extensión $L|K$ sea separable; por ejemplo, en el caso de los anillos de enteros de los cuerpos de números.

Corolario 3.4.5. *Sean A un anillo de Dedekind, K el cuerpo de fracciones de A, $L|K$ una extensión finita, $n := [L : K]$ el grado, B la clausura entera de A en L, y $\mathfrak{p}$ un ideal primo no nulo de A. Sea $\mathfrak{p}B = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$ la descomposición de $\mathfrak{p}B$ en factors primos en B. Supongamos, además, que la extensión $L|K$ es separable o bien que $S^{-1}B$ es un $S^{-1}A$-módulo finitamente generado (para $S := A - \mathfrak{p}$). Entonces se satisface la igualdad*

$$\sum_{i=1}^{g} e_i f_i = [L : K]. \square$$

3.5. El caso galoisiano

Un cas muy importante por sus aplicaciones prácticas es el caso en que la extensión de los cuerpos de fracciones es una extensión de Galois. En este caso, las propiedades generales adquieren una forma más sencilla y son más fáciles de utilizar. Esta sección se dedica a hacer el estudio en este caso particular.

Supongamos, pues, que A es un anillo de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión finita, $n := [L : K]$ el grado, y B la clausura entera de A en L. Supongamos que la extensión $L|K$ es una extensión de Galois y sea $G := \mathrm{Gal}\,(L|K)$ su grupo de Galois.

Proposición 3.5.1. *Consideremos un ideal primo no nulo $\mathfrak{p} \subseteq A$. Entonces, el grupo de Galois G opera transitivamente y de manera natural en el conjunto de los ideales primos $\mathfrak{P}$ de B que dividen $\mathfrak{p}$.*

DEMOSTRACIÓN: En efecto, si $\sigma \in G$ es un K-automorfismo de L, entonces la imagen $\sigma(b)$ de un elemento $b \in B$ es un elemento de B, ya que $\sigma(b)$ es un conjugado de b sobre K y, por tanto, es raíz del mismo polinomio mónico irreducible de coeficientes en A que tiene b por raíz. Por tanto, σ es un A-automorfismo de B. Ahora, la imagen por un isomorfismo de un ideal primo es un ideal primo; por tanto, G opera en el conjunto de los ideales primos de B; y si $\mathfrak{P} \cap A = \mathfrak{p}$, entonces, $\sigma(\mathfrak{P}) \cap A = \mathfrak{p}$, ya que A (y, por tanto, $\mathfrak{p}$) es fijo elemento a elemento por σ. Por tanto, G opera en el conjunto de los ideales primos de B que dividen un ideal primo dado $\mathfrak{p}$ en A. Resta ver que esta acción es transitiva.

Para ello, sean $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_s$, $s \leq g$, los diferentes ideales primos de B conjugados de $\mathfrak{P}_1 := \mathfrak{P}$. Supongamos que $s < g$. Claramente, G permuta los ideales $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ y también permuta los ideales $\mathfrak{P}_{s+1}, \ldots, \mathfrak{P}_g$; el producto $\mathfrak{P}_1 \cdots \mathfrak{P}_s$ no está incluído en ningún $\mathfrak{P}_i$ para $i > s$, de manera que existe $b \in \mathfrak{P}_1 \cdots \mathfrak{P}_s$ tal que $b \notin \mathfrak{P}_i$ para todo i, $s < i \leq g$. Entonces, $\mathrm{N}_{L|K}(b) = \prod_{\sigma \in G} \sigma(b)$ es un elemento del producto $\mathfrak{P}_1 \cdots \mathfrak{P}_s$ y también de A; por tanto, de la intersección, que está incluída en $\mathfrak{P} \cap A = \mathfrak{p}$; es decir, $\mathrm{N}_{L|K}(b) \in \mathfrak{p}$. En consecuencia, $\mathrm{N}_{L|K}(b) \in \mathfrak{P}_i$, de manera que para algún $\sigma \in G$ es $\sigma(b) \in \mathfrak{P}_i$, ya que $\mathfrak{P}_i$ es un ideal primo de B y $\sigma(b) \in B$ para todo $\sigma \in G$. Pero, entonces, $b \in \sigma^{-1}(\mathfrak{P}_i)$, de manera que $\sigma^{-1}(\mathfrak{P}_i)$ es uno de los ideales $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$, que son los únicos que pueden contener b. Eso contradice el hecho que $s < g$. □

La fórmula $\sum_{i=1}^{g} e_i f_i = n$ del caso separable admite una expressión más sencilla en el caso galoisiano.

Proposición 3.5.2. *Supongamos que la extensión $L|K$ es de Galois. Entonces, todos los ideales primos $\mathfrak{P} \subseteq B$ que dividen el ideal primo $\mathfrak{p} \subseteq A$ tienen el mismo índice de ramificación y el mismo grado residual; es decir, $e := e(\mathfrak{P}|\mathfrak{p})$ y $f := f(\mathfrak{P}|\mathfrak{p})$ no dependen del ideal primo $\mathfrak{P}$ de B que divide $\mathfrak{p}$. Además, se satisface la fórmula $n = efg$, donde g es el número de ideales primos de B que dividen el ideal $\mathfrak{p}$.*

DEMOSTRACIÓN: Si $g > 1$, sean $\mathfrak{P} \neq \mathfrak{P}'$ dos ideales primos de B que dividen el ideal primo $\mathfrak{p}$ de A y sea $\sigma \in G$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Entonces, σ define un isomorfismo de $B/\mathfrak{P}$ en $B/\mathfrak{P}'$ que restringe a la identidad sobre $A/\mathfrak{p}$; por tanto, los grados residuales de $\mathfrak{P}$ y de $\mathfrak{P}'$ coinciden. Análogamente, puesto

que $\sigma(\mathfrak{p}B) = \mathfrak{p}B$, la descomposición de $\mathfrak{p}B$ como producto de ideales primos de B se transforma por σ en ella misma; eso quiere decir que los exponentes de $\mathfrak{P}$ y de $\mathfrak{P}'$ en esta descomposición han de coincidir; es decir, que los índices de ramificación de $\mathfrak{P}$ y de $\mathfrak{P}'$ son iguales. Si ahora aplicamos la fórmula $\sum_{i=1}^{g} e_i f_i = n$, teniendo en cuenta que todos los e_i coinciden y que todos los f_i también, obtenemos la fórmula $n = efg$ del enunciado. □

Definición 3.5.3. Sea $\mathfrak{P} \subseteq B$ un ideal primo no nulo de B y sea $\mathfrak{p} := \mathfrak{P} \cap A$ su contracción a A. El subgrupo de isotropía de $\mathfrak{P}$, $D(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}$, se llama el grupo de descomposición del primo $\mathfrak{P}$ en la extensión de Galois $B|A$.

Supongamos, ahora, que $\mathfrak{P}'$ es otro ideal primo de B que divide $\mathfrak{p}$. En virtud de la proposición 3.5.1, existe un automorfismo $\sigma \in G$ tal que $\mathfrak{P}' = \sigma(\mathfrak{P})$. En consecuencia, el grupo de descomposición de $\mathfrak{P}'$ es conjugado del grupo de descomposición de $\mathfrak{P}$; concretamente, $D(\mathfrak{P}'|\mathfrak{p}) = \sigma^{-1}D(\mathfrak{P}|\mathfrak{p})\sigma$. Además, el índice de $D(\mathfrak{P}|\mathfrak{p})$ en G es el número de ideales primos de B que dividen $\mathfrak{p}$; es decir, $D(\mathfrak{P}|\mathfrak{p})$ es un subgrupo de G de índice $g(\mathfrak{p})$; equivalentmente, el orden del grupo de descomposición es el producto $e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})$.

Proposición 3.5.4. *Supongamos que la extensión $L|K$ es de Galois. Sea $\mathfrak{P} \subseteq B$ un ideal primo no nulo y sea $\mathfrak{p} := \mathfrak{P} \cap A$ su contracción. Entonces, la extensión residual $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ es una extensión normal; además, hay un morfismo exhaustivo de grupos $D(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}\,((B/\mathfrak{P})|(A/\mathfrak{p}))$.*

Demostración: Sea $b \in B$ un representante de una clase cualquiera $b + \mathfrak{P} \in B/\mathfrak{P}$. Consideremos el polinomio de $L[X]$ $f(X) := \prod_{\sigma\in G}(X - \sigma(b))$; las raíces del polinomio $f(X)$ son los diferentes conjugados de b contados cada uno tantas veces como el grado de la extensión $L|K(b)$, de manera que el polinomio $f(X)$ es la potencia $[L : K(b)]$-ésima del polinomio $\mathrm{Irr}(b, K)$; por tanto, $f(X)$ es un polinomio mónico de coeficientes en $A[X]$. La reducción módulo $\mathfrak{P}$ del polinomio $f(X)$ es un polinomio de coeficientes en $A/\mathfrak{p}$ que tiene por raíces las clases $\sigma(b)+\mathfrak{P} \in B/\mathfrak{P}$; por tanto, descompone en factores lineales en $B/\mathfrak{P}$; en consecuencia, el polinomio $\mathrm{Irr}(b + \mathfrak{P}, A/\mathfrak{p})$, que es un divisor de aquel, también descompone en factores lineales en $B/\mathfrak{P}$. Eso nos dice que todos los conjugados sobre $A/\mathfrak{p}$ de todos los elementos de $B/\mathfrak{P}$ son

elementos de $B/\mathfrak{P}$; por tanto, la extensión $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ es una extensión normal.

Por otro lado, sea $\sigma \in D(\mathfrak{P}|\mathfrak{p})$; es decir, un A-automorfismo de B que deja $\mathfrak{P}$ invariante. Por paso al cociente, σ define un $A/\mathfrak{p}$-automorfismo de $B/\mathfrak{P}$; es decir, un elemento del grupo de Galois de la extensión $A/\mathfrak{p} \subseteq B/\mathfrak{P}$. De esta manera se obtiene un morfismo de grupos $D(\mathfrak{P}|\mathfrak{p}) \xrightarrow{\pi} \mathrm{Gal}\,(B/\mathfrak{P}|A/\mathfrak{p})$. Queremos probar que π es exhaustivo. Para ello, comencemos por recordar que un $A/\mathfrak{p}$-automorfismo de $B/\mathfrak{P}$ queda determinado de manera única por su acción sobre un elemento primitivo de la clausura separable de $A/\mathfrak{p}$ en $B/\mathfrak{P}$; es decir, que dar un elemento de $\mathrm{Gal}\,(B/\mathfrak{P}|A/\mathfrak{p})$ equivale a dar un conjugado sobre $A/\mathfrak{p}$ de un tal elemento primitivo.

Sea, pues, $\overline{b} \in B/\mathfrak{P}$ un tal elemento primitivo; podemos elegir $b \in B$ de manera que $b \equiv \overline{b} \pmod{\mathfrak{P}}$ y que $b \in \sigma^{-1}(\mathfrak{P})$ para todo $\sigma \in G - D(\mathfrak{P}|\mathfrak{p})$; por ejemplo, un elemento que satisfaga simultáneamente las congruencias

$$\begin{aligned} b &\equiv \overline{b} \pmod{\mathfrak{P}}, \\ b &\equiv 0 \pmod{\sigma^{-1}(\mathfrak{P})}, \text{ para todo } \sigma \in G - D(\mathfrak{P}|\mathfrak{p}). \end{aligned}$$

Si consideramos el polinomio $f(X) := \prod_{\sigma \in G} (X - \sigma(b))$, las raíces no nulas de su reducción módulo $\mathfrak{P}$ son de la forma $\sigma(b) + \mathfrak{P}$ con $\sigma \in D(\mathfrak{P}|\mathfrak{p})$; eso dice que todos los conjugados de $\overline{b} + \mathfrak{P}$ sobre $A/\mathfrak{p}$ son las reducciones módulo $\mathfrak{P}$ de conjugados $\sigma(b)$ de b sobre A. Es decir, dada una $A/\mathfrak{p}$-inmersión de $B/\mathfrak{P}$, entonces existe un elemento $\sigma \in D(\mathfrak{P}|\mathfrak{p})$ que la tiene por reducción módulo $\mathfrak{P}$. Eso demuestra la exhaustividad de π. $\square$

Definición 3.5.5. Sea $\mathfrak{P} \subseteq B$ un ideal primo no nulo de B y sea $\mathfrak{p} := \mathfrak{P} \cap A$ su contracción a A. El núcleo del morfismo $D(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}\,(B/\mathfrak{P}|A/\mathfrak{p})$, es decir, el subgrupo $I(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in D(\mathfrak{P}|\mathfrak{p}) : \sigma(b) - b \in \mathfrak{P} \text{ para todo } b \in B\}$ de $D(\mathfrak{P}|\mathfrak{p})$ se llama el grupo de inercia del primo $\mathfrak{P}$ en la extensión de Galois $B|A$.

En particular, el grupo de inercia es un subgrupo normal del grupo de descomposición y su cociente es el grupo de Galois de la extensión residual. Puesto que esta extensión residual es normal, el orden de su grupo de Galois es exactamente su grado de separabilidad. Dicho de otra manera, el índice del grupo de inercia en el grupo de descomposición es el grado de separabilidad de la extensión residual. Más adelante, volveremos al estudio de los grupos de descomposición y de inercia.

3.6. Discriminante

El estudio de los ideales primos que ramifican en una extensión finita y entera de anillos de Dedekind $B|A$ se puede hacer, en el caso separable, con la ayuda de un invariante asociado a la extensión de manera natural y que sirve para determinar el conjunto de los ideales primos de A que ramifican en la extensión $B|A$: el discriminante. El objetivo de esta sección es definir y estudiar algunas de sus propiedades.

Sean, pues, A un dominio íntegramente cerrado, K su cuerpo de fracciones, $L|K$ una extensión finita y separable, $n := [L : K]$ el grado de la extensión, y B la clausura entera de A en L. Ya hemos visto en la sección primera que el hecho que la extensión $L|K$ sea separable es equivalente al hecho que la forma bilineal $\mathrm{T}_{L|K}$ sea no degenerada. Este hecho es capital para las propiedades del discriminante.

Definición 3.6.1. Sea $\{b_1, b_2, \ldots, b_n\}$ una K-base arbitraria de L. Llamaremos discriminante de $\{b_1, b_2, \ldots, b_n\}$ al determinante $\det\big(\mathrm{T}_{L|K}(b_i b_j)\big)$ de la matriz de la forma bilineal traza en esta base. Puesto que la forma bilineal $\mathrm{T}_{L|K}$ es no degenerada, el discriminante es un elemento de K^*. Escribiremos $D(b_1, b_2, \ldots, b_n) := \det\big(\mathrm{T}_{L|K}(b_i b_j)\big)$. Si $b_1, b_2, \ldots, b_n$ son elementos de B, entonces $D(b_1, b_2, \ldots, b_n) \in A$, ya que $\mathrm{T}_{L|K}(b_i b_j) \in A$ para toda pareja de elementos $b_i, b_j \in B$.

Consideremos una nueva base $\{b'_1, b'_2, \ldots, b'_n\}$ dada a partir de la base $\{b_1, b_2, \ldots, b_n\}$ por multiplicación por una matriz P en la forma

$$\begin{pmatrix} b'_1 \\ b'_2 \\ \vdots \\ b'_n \end{pmatrix} = P \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

Entonces, se satisface la igualdad $D(b'_1, b'_2, \ldots, b'_n) = \det P^2 D(b_1, b_2, \ldots, b_n)$, ya que hacemos un cambio de base a una forma bilineal. Por tanto, los discriminantes de bases diferentes coinciden módulo cuadrados de K^*.

Definición 3.6.2. Llamaremos discriminante de la extensión $B|A$ el ideal de A generado por los discriminantes $D(b_1, b_2, \ldots, b_n)$, cuando los conjuntos $\{b_1, b_2, \ldots, b_n\}$ recorren todas las posibles K-bases de L formadas por elementos de B. Lo designaremos con el símbolo $\Delta(B|A)$.

Lema 3.6.3. *Sea $\{b_1, b_2, \ldots, b_n\}$ una K-base de L formada por elementos de B. El ideal extensión $D(b_1, b_2, \ldots, b_n)B$ está incluído en el A-módulo libre $Ab_1 \oplus Ab_2 \oplus \cdots \oplus Ab_n$.*

DEMOSTRACIÓN: En efecto, dado $b \in B$ podemos escribir $b = \sum_{i=1}^{n} a_i b_i$ con los coeficientes $a_i \in L$; al multiplicar por b_j obtenemos las expresiones $bb_j = \sum_{i=1}^{n} a_i b_i b_j$ y, al tomar trazas, $\mathrm{T}_{L|K}(bb_j) = \sum_{i=1}^{n} a_i \mathrm{T}_{L|K}(b_i b_j)$. Puesto que $bb_j, b_i b_j \in B$, sus trazas pertenecen a A y la regla de Cramer para la resolución de sistemas de ecuaciones lineales nos permite asegurar que los coeficientes a_i se obtienen como el cociente de un determinante formado por elementos de A por el determinante de la matriz $(\mathrm{T}_{L|K}(b_i b_j))$; por tanto, $a_i \in \dfrac{1}{D(b_1, b_2, \ldots, b_n)} A \subseteq K$. Eso demuestra la segunda parte. □

La propiedad que demostraremos a continuación hace referencia al caso en que B sea un A-módulo libre.

Proposición 3.6.4. *Supongamos que B es un A-módulo libre y que el conjunto $\{b_1, b_2, \ldots, b_n\}$ es una A-base de B. Entonces, $\Delta(B|A)$ es el ideal principal generado por $D(b_1, b_2, \ldots, b_n)$.*

DEMOSTRACIÓN: Si $\{b'_1, b'_2, \ldots, b'_n\}$ es otra K-base de L formada por elementos de B, puesto que $\{b_1, b_2, \ldots, b_n\}$ es una A-base de B, existe una matriz $(a_{i,j}) \in \mathcal{M}_n(A)$, no necesariamente invertible en A, y la matriz de la forma $\mathrm{T}_{L|K}$ en esta nueva base es el producto $(a_{i,j})\left(\mathrm{T}_{L|K}(b_i b_j)\right)(a_{j,i})$. Por tanto, $D(b'_1, b'_2, \ldots, b'_n) = \det(a_{i,j})^2 D(b_1, b_2, \ldots, b_n)$ pertenece al ideal generado por $D(b_1, b_2, \ldots, b_n)$. □

En segundo lugar, veremos que el discriminante se comporta bien por localización. Concretamente, si $S \subseteq A$ es un conjunto multiplicativamente cerrado, entonces $S^{-1}A$ es un dominio íntegramente cerrado con cuerpo de fracciones K y $S^{-1}B$ es la clausura entera de $S^{-1}A$ en L. Por tanto, tiene sentido hablar del discriminante $\Delta(S^{-1}B/S^{-1}A)$.

Proposición 3.6.5. *Sea S un subconjunto multiplicativamente cerrado de A. Entonces, se satisface la igualdad $\Delta(S^{-1}B/S^{-1}A) = S^{-1}\Delta(B/A)$.*

DEMOSTRACIÓN: La inclusión $S^{-1}\Delta(B/A) \subseteq \Delta(S^{-1}B/S^{-1}A)$ es clara, ya que si $\{b_1, b_2, \ldots, b_n\}$ es una K-base de L formada por elementos de B,

también es una K-base de L formada por elementos de $S^{-1}B$; por tanto, $\Delta(B|A) \subseteq \Delta(S^{-1}B|S^{-1}A)$; en consecuencia, $S^{-1}\Delta(B|A) \subseteq \Delta(S^{-1}B|S^{-1}A)$.

Por otro lado, si $\{b_1, b_2, \ldots, b_n\}$ es una K-base de L formada por elementos de $S^{-1}B$, podemos multiplicar todos los elementos b_i por un elemento conveniente $s \in S$ de manera que $sb_i \in B$; entonces, $D(sb_1, sb_2, \ldots, sb_n) \in \Delta(B|A)$ y de la igualdad $D(sb_1, sb_2, \ldots, sb_n) = s^{2n}D(b_1, b_2, \ldots, b_n)$, se deduce inmediatamente que $D(b_1, b_2, \ldots, b_n) \in S^{-1}\Delta(B|A)$. Eso demuestra la otra inclusión. □

Finalmente, vamos a ver una propiedad que facilitará el cálculo del discriminante en algunos casos particulares importantes.

Proposición 3.6.6. *Sea $\theta \in L$ un elemento primitivo de la extensión $L|K$ y sea $f(X) := \mathrm{Irr}(\theta, K)$ el polinomio mónico irreducible de $K[X]$ que tiene θ por raíz. Entonces,*

$$D(1, \theta, \theta^2, \ldots, \theta^{n-1}) = (-1)^{n(n-1)/2}\mathrm{N}_{L|K}(f'(\theta)),$$

donde $f'(X)$ denota el polinomio derivado del polinomio $f(X)$.

Demostración: Podemos escribir $f(X) = (X - \theta_1)\cdots(X - \theta_n)$ donde $\theta_1, \ldots, \theta_n$ son los n conjugados diferentes de $\theta =: \theta_1$. Al derivar la igualdad y substituir en θ_i obtenemos las igualdades

$$f'(\theta_i) = \prod_{j \neq i}(\theta_i - \theta_j)$$

que, una vez multiplicadas, dan la fórmula

$$\prod_{i=1}^{n} f'(\theta_i) = \prod_{i=1}^{n}\prod_{j \neq i}(\theta_i - \theta_j).$$

Puesto que el polinomio $f'(X)$ tiene coeficientes en el cuerpo K, la norma $\mathrm{N}_{L|K}(f'(\theta))$ puede ser calculada como el producto $\mathrm{N}_{L|K}(f'(\theta)) = \prod_{i=1}^{n} f'(\theta_i)$ de los conjugados de $f'(\theta)$. Por otro lado, el discriminante se puede calcular en la forma $D(1, \theta, \ldots, \theta^{n-1}) = \det(\theta_i^{j-1})^2$, como ya ha sido probado anteriormente al caracterizar las extensiones separables por la no degeneración de la

forma bilineal traza. Por tanto, y puesto que el determinante de la matriz de Vandermonde

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \theta_1 & \theta_2 & \dots & \theta_n \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1^{n-1} & \theta_2^{n-1} & \dots & \theta_n^{n-1} \end{pmatrix}$$

es el producto $\prod_{i=2}^{n}\prod_{j<i}(\theta_i - \theta_j)$, obtenemos la igualdad

$$D(1,\theta,\dots,\theta^{n-1}) = \prod_{i=2}^{n}\prod_{j<i}(\theta_i-\theta_j)^2 = (-1)^{n(n-1)/2}\prod_{i=1}^{n}\prod_{j\neq i}(\theta_i-\theta_j)$$

que, combinada con la que da la norma de $f'(\theta)$, hace el resultado evidente. □

Un ejemplo importante de discriminante es el discriminante de las sucesivas potencias de una raíz de la unidad; este discriminante lo usaremos más adelante.

Proposición 3.6.7. *Sea $\zeta_n \in \mathbb{C}$ una raíz primitiva n-ésima de la unidad. Entonces,*

$$D(1,\zeta_n,\zeta_n^2,\dots,\zeta_n^{\varphi(n)-1}) = (-1)^{\varphi(n)(\varphi(n)-1)/2} n^{\frac{\varphi(n)}{\prod_{p|n} p^{\varphi(n)/(p-1)}}}.$$

Demostración: La demostración que haremos está basada en el conocimiento de los polinomios ciclotómicos $\Phi_n(X)$; concretamente en las dos fórmulas siguientes:

$$\Phi_n(X) = \prod_{d|n}(X^d-1)^{\mu(n/d)},$$

para todo número natural n, y donde μ denota la función de Möbius, y

$$\Phi_{n'}(X)\Phi_{n'p}(X) = \Phi_{n'}(X^p),$$

siempre que p sea un número natural primo que no divida n'. Los casos $n = 1$ y $n = 2$ no tienen ninguna dificultad; por tanto, podemos suponer que $n > 2$.

Al derivar la primera de estas fórmulas y substituir en ζ_n se obtiene la expresión

$$\Phi_n'(\zeta_n) = \zeta_n^{-1} n \prod_{d|n,\, d\neq n}(\zeta_n^d - 1)^{\mu(n/d)}.$$

La proposición 3.6.6 ya da el signo enunciado, de manera que basta calcular la norma $\mathrm{N}_n(\Phi_n'(\zeta_n))$, donde ponemos N_n para indicar la norma de la extensión $\mathbb{Q}(\zeta_n)|\mathbb{Q}$. El hecho que la norma sea multiplicativa, así como su transitividad para cadenas de extensiones, nos legitiman a escribir consecutivamente las igualdades

$$\begin{aligned}
\mathrm{N}_n(\Phi_n'(\zeta_n)) &= \mathrm{N}_n(\zeta_n)^{-1} n^{\varphi(n)} \prod_{d|n,\, d\neq n} \mathrm{N}_n(\zeta_n^d - 1)^{\mu(n/d)} \\
&= \mathrm{N}_n(\zeta_n)^{-1} n^{\varphi(n)} \prod_{d|n,\, d\neq n} \mathrm{N}_n(\zeta_{n/d} - 1)^{\mu(n/d)} \\
&= \mathrm{N}_n(\zeta_n)^{-1} n^{\varphi(n)} \prod_{d|n,\, d\neq 1} \mathrm{N}_n(\zeta_d - 1)^{\mu(d)} \\
&= \mathrm{N}_n(\zeta_n)^{-1} n^{\varphi(n)} \prod_{d|n,\, d\neq 1} \mathrm{N}_d(\zeta_d - 1)^{\mu(d)\varphi(n)/\varphi(d)}.
\end{aligned}$$

Observemos, en primer lugar, que para todo número natural $n > 2$ es $\mathrm{N}_n(\zeta_n) = 1$, ya que el inverso de cada conjugado de ζ también es un conjugado de ζ y son diferentes. Por otro lado, puesto que $d \neq 1$, es $\zeta_d \neq 1$ y $\mathrm{N}_d(\zeta_d - 1) \neq 0$. Si d es divisible por el cuadrado de un número primo, entonces $\mu(d) = 0$ y el factor $\mathrm{N}_d(\zeta_d - 1)^{\mu(d)\varphi(n)/\varphi(d)}$ vale 1. Por tanto, el producto se extiende a los números naturales $d \neq 1$ diferentes de n que son libres de cuadrados.

Ahora, podemos observar que $\mathrm{N}_d(\zeta_d - 1) = (-1)^{\varphi(d)}\mathrm{N}_d(1 - \zeta_d)$, de manera que los factores del producto son $\mathrm{N}_d(1 - \zeta_d)^{\mu(d)\varphi(n)/\varphi(d)}$, ya que el signo es $(-1)^{\mu(d)\varphi(n)} = 1$, porque $\varphi(n)$ es par para todo $n > 2$. De esta manera obtenemos la expresión

$$\mathrm{N}_n(\Phi_n'(\zeta_n)) = n^{\varphi(n)} \prod_{d|n,\, d\neq 1} \mathrm{N}_d(1 - \zeta_d)^{\mu(d)\varphi(n)/\varphi(d)},$$

el producto extendido a todos los números naturales d libres de cuadrados y diferentes de 1 que dividen n.

De la segunda de las fórmulas generales para los polinomios ciclotómicos que hemos escrito se deduce que $\Phi_d(1) = 1$ para todo número natural d divisible por dos o más primos diferentes; en efecto, puesto que $1 \in \mathbb{Q}$, 1 no puede ser raíz de ningún polinomio ciclotómico $\Phi_d(X)$, de manera que de la igualdad $\Phi_{n'}(1)\Phi_{n'p}(1) = \Phi_{n'}(1)$ es deduce que $\Phi_{n'p}(1) = 1$. Por otro lado, para todo número natural primo p que divide n se satisface la igualdad

$\mathrm{N}_p(1-\zeta_p) = \Phi_p(1) = p$, ya que $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$. Llevando estos cálculos a la fórmula anterior obtenemos la fórmula que queríamos probar. □

3.7. Discriminante y ramificación

En esta sección se trata de ver qué relación tiene el discriminante con la ramificación. Para ello, nos poondremos en la situación en que A es un anillo de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión finita y separable, $n := [L : K]$ el grado de la extensión, y B la clausura entera de A en L. Entonces, el ideal discriminante $\Delta(B|A)$ descompone de manera única como producto de ideales primos no nulos de A. Se trata de probar que el conjunto de los ideales primos de A que ramifican en B está formado exactamente por los ideales primos que dividen el discriminante.

Comencemos por estudiar un poco más de cerca el comportamiento local del discriminante y de la ramificación. Sea $\mathfrak{p} \subseteq A$ un ideal primo no nulo y sea $S := A - \mathfrak{p}$. Entonces, $S^{-1}\mathfrak{p} := \mathfrak{p}S^{-1}A$ es un ideal primo de $S^{-1}A$ y, en virtud de la proposición 3.6.4, condición necesaria y suficiente para que $\Delta(B|A) \subseteq \mathfrak{p}$ es que $\Delta(S^{-1}B|S^{-1}A) \subseteq S^{-1}\mathfrak{p}$. Por otro lado, $S^{-1}A$ es un anillo de Dedekind local y $S^{-1}B$ es la clausura entera de $S^{-1}A$ en L; además, si $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ es la descomposición de $\mathfrak{p}B$ en B, la descomposición de $\mathfrak{p}S^{-1}B$ en $S^{-1}B$ es $\mathfrak{p}S^{-1}B = (S^{-1}\mathfrak{P}_1)^{e_1} \cdots (S^{-1}\mathfrak{P}_g)^{e_g}$ y la extensión residual $S^{-1}A/S^{-1}\mathfrak{p} \subseteq S^{-1}B/S^{-1}\mathfrak{P}_i$ es la extensión $A/\mathfrak{p} \subseteq B/\mathfrak{P}_i$; por tanto, condición necesaria y suficiente para que el ideal $\mathfrak{p} \subseteq A$ ramifique en B es que el ideal $S^{-1}\mathfrak{p} \subseteq S^{-1}A$ ramifique en $S^{-1}B$. Pero, ahora, los anillos $S^{-1}A$ y $S^{-1}B$ son anillos de Dedekind principales y $S^{-1}B$ es un $S^{-1}A$-módulo libre de rango n; de manera que el ideal discriminante $\Delta(S^{-1}B|S^{-1}A)$ es principal y generado por el discriminante de una $S^{-1}A$-base de $S^{-1}B$.

Estas consideraciones hacen que podamos suponer de entrada que A es un anillo de Dedekind principal y local y que $\mathfrak{p}$ es el único ideal primo no nulo de A. Si $\{b_1, b_2, \ldots, b_n\}$ es una A-base de B, entonces es una K-base de L y $\{b_1 + \mathfrak{p}B, b_2 + \mathfrak{p}B, \ldots, b_n + \mathfrak{p}B\}$ es una $A/\mathfrak{p}$-base de $B/\mathfrak{p}B$. Esto ya ha sido probado en el transcurso de la sección 4.

Sea $b \in B$ un elemento cualquiera. La multiplicación por b define una aplicación A-lineal $\mathfrak{m}_b : B \longrightarrow B$ que, en la A-base $\{b_1, b_2, \ldots, b_n\}$ de B ad-

mite una matriz $(a_{i,j}) \in \mathcal{M}_n(A)$. La reducción módulo $\mathfrak{p}B$ de esta aplicación lineal da lugar a la aplicación $A/\mathfrak{p}A$-lineal $\overline{\mathfrak{m}}_b : B/\mathfrak{p}B \longrightarrow B/\mathfrak{p}B$ de multiplicación por $b+\mathfrak{p}B$ en $B/\mathfrak{p}B$, que tiene matriz $(a_{i,j}+\mathfrak{p}) \in \mathcal{M}_n(A/\mathfrak{p}A)$ en la $A/\mathfrak{p}$-base $\{b_1+\mathfrak{p}B, b_2+\mathfrak{p}B, \ldots, b_n+\mathfrak{p}B\}$ de $B/\mathfrak{p}B$. En particular, se satisface la igualdad $\mathrm{T}_{L|K}(b)+\mathfrak{p} = \mathrm{tr}(\overline{\mathfrak{m}}_b)$, de manera que la reducción módulo $\mathfrak{p}$ del discriminante $D_{B|A}(b_1, b_2, \ldots, b_n)$ es el determinante $\overline{D}(b_1, b_2, \ldots, b_n) := \det[\mathrm{tr}((b_i+\mathfrak{p}B)(b_j+\mathfrak{p}B))]$.

Puesto que $\Delta(B|A)$ es generado por $D(b_1, b_2, \ldots, b_n)$, decir que $\Delta(B|A) \subseteq \mathfrak{p}$ equivale a decir que $D(b_1, b_2, \ldots, b_n) \in \mathfrak{p}$, o sea, que $\overline{D}(b_1, b_2, \ldots, b_n) = 0$ en $A/\mathfrak{p}$. Por tanto, hay que probar que condición necesaria y suficiente para que $\mathfrak{p}$ ramifique en B es que $\overline{D}(b_1, b_2, \ldots, b_n) = 0$ en $A/\mathfrak{p}$. Para ello, sea $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ la descomposición de $\mathfrak{p}B$ en ideales primos de B. El teorema chino del resto nos legitima a escribir la descomposición

$$B/\mathfrak{p}B \simeq \bigoplus_{i=1}^{g} B/\mathfrak{P}_i^{e_i}$$

de $B/\mathfrak{p}B$ como suma directa de subespacios vectoriales sobre $A/\mathfrak{p}$. Podemos considerar una $A/\mathfrak{p}$-base de $B/\mathfrak{p}B$ construída reuniendo bases de los sumandos $B/\mathfrak{P}_i^{e_i}$; si $\theta \in B/\mathfrak{p}B$ es un elemento cualquiera y $\theta = \theta_1 + \cdots + \theta_g$ es la descomposición de θ en sumandos $\theta_i \in B/\mathfrak{P}_i^{e_i}$, la matriz de la multiplicación por θ en $B/\mathfrak{p}B$ en esta nueva base se expresa en forma de matriz de cajas en la diagonal, cada una de ellas correspondiente a la matriz de la multiplicación por θ_i en la base que hemos tomado en $B/\mathfrak{P}_i^{e_i}$ para construir por reunión la base de $B/\mathfrak{p}B$. En particular, esto nos permite asegurar que la traza de la aplicación lineal de multiplicación por θ en $B/\mathfrak{p}B$ es la suma de les trazas de las aplicaciones lineales de multiplicación por θ_i en cada $B/\mathfrak{P}_i^{e_i}$. En consecuencia, la matriz de les trazas de los productos toma la forma de una matriz de cajas en la diagonal donde cada una es la matriz de las trazas de los productos de los elementos de la base de $B/\mathfrak{P}_i^{e_i}$, ya que los productos de elementos de diferentes factores $B/\mathfrak{P}_i^{e_i}$ se anulan. Puesto que los determinantes de las matrices de una forma bilineal simétrica en dos bases diferentes son iguales salvo la multiplicación por el cuadrado del determinante de la matriz del cambio de base, y este determinante siempre es inversible, obtenemos la fórmula

$$\overline{D}(b_1, b_2, \ldots, b_n) = \det P^2 \prod_{i=1}^{g} \overline{D}_i,$$

donde $\overline{D}_i$ es el determinante de la matriz de las trazas de los productos de los elementos de la base que hemos elegido en $B/\mathfrak{P}_i^{e_i}$.

Supongamos que el ideal primo $\mathfrak{p}$ es no ramificado en B; es decir, que para $1 \leq i \leq g$ la extensión $A/\mathfrak{p} \subseteq B/\mathfrak{P}_i$ es separable y $e_i = 1$. Puesto que las extensiones $A/\mathfrak{p} \subseteq B/\mathfrak{P}_i$ son separables, los determinantes $\overline{D}_i$ son no nulos y obtenemos que $\overline{D}(b_1, b_2, \ldots, b_n) \neq 0$ en $A/\mathfrak{p}$, como queríamos ver. Recíprocamente, hay que ver que si $\mathfrak{p}$ ramifica en B, entonces $\overline{D}(b_1, b_2, \ldots, b_n) = 0$. Supongamos, primeramente, que $e_1 > 1$. Podemos elegir la $A/\mathfrak{p}$-base de $B/\mathfrak{P}_1^{e_1}$ completando bases en la filtración de $B/\mathfrak{P}_1^{e_1}$ dada por los ideales (y $A/\mathfrak{p}$-espacios vectoriales) $\mathfrak{P}_1^a/\mathfrak{P}_1^{e_1}$, $e_1 - 1 \geq a \geq 0$; el hecho que el primer vector de esta base sea nilpotente (su potencia e_1-ésima se anula) hace que la aplicación lineal de multiplicación por este elemento sea un endomorfismo nilpotente de $B/\mathfrak{P}_1^{e_1}$ y, por tanto, todos los valores propios sean nulos. Análogamente, los productos de este elemento por cualquier otro también son nilpotentes y lo mismo sucede con los endomorfismos de $B/\mathfrak{P}_1^{e_1}$ de multiplicación por estos productos; por tanto, las trazas de los productos son nulas y la matriz que sirve para calcular el determinante $\overline{D}_1$ tiene una columna de ceros. Por tanto, $\overline{D}_1 = 0$. Resta el caso en que todos los índices de ramificación sean triviales, pero que alguna de las extensiones $A/\mathfrak{p} \subseteq B/\mathfrak{P}_i$ no sea separable. En este caso, la forma traza en $B/\mathfrak{P}_i$ es la forma nula y $\overline{D}_i = 0$.

En resumen, hemos demostrado el resultado siguiente.

Proposición 3.7.1. *Sean A un anillo de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión finita y separable, B la clausura entera de A en L y $\mathfrak{p}$ un ideal primo no nulo de A. Condición necesaria y suficiente para que el ideal $\mathfrak{p}$ ramifique en la extensión $B|A$ es que el discriminante $\Delta(B|A)$ sea divisible por $\mathfrak{p}$.* □

3.8. El caso cuadrático

En el capítulo anterior hemos determinado exactamente el anillo de los enteros de todos los cuerpos cuadráticos. Ahora podemos determinar el discriminante y las leyes de descomposición de todos los ideales primos de $\mathbb{Z}$ en un cuerpo cuadrático. Comencemos por determinar el discriminante.

Proposición 3.8.1. *Sea D un número entero libre de cuadrados y sea $K := \mathbb{Q}(\sqrt{D})$. Entonces, el discriminante de la extensión $K|\mathbb{Q}$ es el número entero*

$4D$ *si* $D \not\equiv 1 \pmod 4$ *y es* D *si* $D \equiv 1 \pmod 4$.

Demostración: Puesto que $\mathbb{Z}$ es principal, el discriminante de la extensión cuadrática $K|\mathbb{Q}$ es el ideal principal generado por el discriminante $D(1,\omega)$ donde $\{1,\omega\}$ es la base del anillo de los enteros de K que hemos determinado anteriormente. Concretamente, si $D \not\equiv 1 \pmod 4$, podemos tomar $\omega = \sqrt{D}$. En este caso, la matriz de la forma bilineal traza es la matriz

$$\begin{bmatrix} \mathrm{T}(1) & \mathrm{T}(\sqrt{D}) \\ \mathrm{T}(\sqrt{D}) & \mathrm{T}(D) \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2D \end{bmatrix},$$

ya que el polinomio irreducible de $\sqrt{D}$ y, por tanto, el polinomio característico de la multiplicación por $\sqrt{D}$ en $\mathcal{O}_K$ es el polinomio $X^2 - D$. Ello hace que $D(1,\sqrt{D}) = 4D$, como queríamos demostrar.

En el caso $D \equiv 1 \pmod 4$, podemos tomar $2\omega = 1 + \sqrt{D}$ y repetir el cálculo que hemos hecho en el otro caso. Pero, con la finalidad de ver otra manera de calcular el discriminante, utilizaremos la fórmula

$$D(1,\omega,\ldots,\omega^{n-1}) = \det(\sigma_i(\omega^{j-1}))^2,$$

donde σ_i recorre el conjunto de las inmersiones diferentes de K en $\overline{\mathbb{Q}}$, que hemos obtenido en la demostración de la proposición 3.1.5 en la forma

$$D(1,\omega,\ldots,\omega^{n-1}) = \det V^2$$

donde $V = (\sigma_i(\omega^{j-1}))$ es la matriz de Vandermonde de los conjugados de ω. Calculemos:

$$D(1,\omega) = \det \begin{bmatrix} 1 & 1 \\ \dfrac{1+\sqrt{D}}{2} & \dfrac{1-\sqrt{D}}{2} \end{bmatrix}^2 = (-\sqrt{D})^2 = D. \square$$

En consecuencia, los ideales primos de $\mathbb{Z}$ que ramifican en la extensión $K|\mathbb{Q}$ son los primos que dividen D y 2 si $D \not\equiv 1 \pmod 4$. Puesto que la extensión es de grado 2 y las extensiones residuales son separables, esto quiere decir que la extensión de estos primos es el cuadrado de un ideal primo de K. Poro otro lado, solamente quedan dos posibilidades para la descomposición de los otros primos de $\mathbb{Z}$ en K: o bien el primo de $\mathbb{Z}$ continúa siendo un ideal primo una vez extendido a K, y en este caso se dice que el primo es inerte,

o bien el primo descompone como producto de dos ideales primos diferentes de K; en este caso se dice que el primo descompone completamente.

El resultado siguiente explica como descomponen todos los primos de $\mathbb{Z}$ en la extensión cuadrática $\mathbb{Q}(\sqrt{D})|\mathbb{Q}$.

Proposición 3.8.2. *Sean D un número entero libre de cuadrados, $K := \mathbb{Q}(\sqrt{D})$, $\mathcal{O}_K$ el anillo de los enteros de K, y p un número natural primo. Si p divide el discriminante de la extensión cuadrática $K|\mathbb{Q}$, entonces, $p\mathcal{O}_K = \mathfrak{p}^2$, donde $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_K$ de grado residual 1; si $p \neq 2$ y D es un resto cuadrático módulo p, entonces $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, el producto de dos ideales primos diferentes de $\mathcal{O}_K$ de grado residual 1; si $p \neq 2$ y D no es un resto cuadrático módulo p, entonces $p\mathcal{O}_K$ es un ideal primo de $\mathcal{O}_K$ de grado residual 2. Finalmente, $2\mathcal{O}_K$ es el producto de dos ideales primos diferentes de $\mathcal{O}_K$ de grado residual 1 cuando $D \equiv 1 \pmod 8$ y $2\mathcal{O}_K$ es un ideal primo de $\mathcal{O}_K$ de grado residual 2 cuando $D \equiv 5 \pmod 8$.*

Demostración: El caso de los primos que ramifican es claro. Por tanto, podemos suponer que el ideal primo $p\mathbb{Z}$ no ramifica en el anillo $\mathcal{O}_K$ de los enteros de K. Comencemos por estudiar el caso $p \neq 2$. Hemos de estudiar la descomposición del anillo $\mathcal{O}_k/p\mathcal{O}_K$ como producto de cuerpos, ya que una condición necesaria y suficiente para que el ideal $p\mathcal{O}_K$ sea primo es que el anillo cociente $\mathcal{O}_K/p\mathcal{O}_K$ sea un cuerpo. De nuevo, el cálculo del anillo de los enteros de K da que el anillo $\mathcal{O}_K$, como grup abeliano, es la suma de los subgrupos $\mathbb{Z}$ y $\omega\mathbb{Z}$, ω como en la proposición anterior. En el caso $D \not\equiv 1 \pmod 4$, el anillo $\mathcal{O}_K/p\mathcal{O}_K$ es el anillo $\mathbb{Z}[\sqrt{D}]/p\mathbb{Z}[\sqrt{D}]$; y en el caso $D \equiv 1 \pmod 4$, si calculamos $\mathcal{O}_K/p\mathcal{O}_K$ podemos observar que este anillo también es el anillo $\mathbb{Z}[\sqrt{D}]/p\mathbb{Z}[\sqrt{D}]$, ya que, para $a, b \in \mathbb{Z}$ es $a + b\dfrac{1+\sqrt{D}}{2} \equiv a + (b+p)\dfrac{1+\sqrt{D}}{2} \pmod{p\mathcal{O}_K}$, de manera que si b es impar, entonces $b+p$ es par y $(b+p)\dfrac{1+\sqrt{D}}{2}$ es la suma de un número entero con un múltiplo entero de $\sqrt{D}$. Por tanto, hay que descomponer $\mathbb{Z}[\sqrt{D}]/p\mathbb{Z}[\sqrt{D}]$ como producto de cuerpos. Ahora bien,

$$\mathcal{O}_K/p\mathcal{O}_K \simeq \mathbb{Z}[\sqrt{D}]/p\mathbb{Z}[\sqrt{D}] \simeq \mathbb{Z}[X]/(p, X^2 - D) \simeq \mathbb{F}_p[X]/(X^2 - D);$$

por tanto, y puesto que el polinomio $X^2 - D$ es separable en $\mathbb{F}_p[X]$, el anillo cociente $\mathcal{O}_K/p\mathcal{O}_K$ es un cuerpo exactamente cuando el polinomio $X^2 - D$ es

irreducible en $\mathbb{F}_p[X]$, y descompone como producto de dos cuerpos isomorfos a $\mathbb{F}_p$ cuando el polinomio X^2-D tiene dos raíces diferentes en $\mathbb{F}_p$. Esto acaba el caso $p \neq 2$.

Para $p = 2$, basta considerar el caso $D \equiv 1 \pmod 4$, ya que en caso contrario 2 ramifica, en virtud de la proposición anterior. En este caso, ω admite como polinomio irreducible el polinomio $X^2 - X + \dfrac{1-D}{4}$, de manera que si b es la clase módulo 2 de $\dfrac{1-D}{4}$, entonces

$$\mathcal{O}_K/p\mathcal{O}_K \simeq \mathbb{Z}[X]/(2, X^2 - X + \frac{1-D}{4}) \simeq \mathbb{F}_2[X]/(X^2 - X + b).$$

Pero condición necesaria y suficiente para que el polinomio (separable) $X^2 - X + b$ sea irreducible en $\mathbb{F}_2[X]$ es que $b = 1$ en $\mathbb{F}_2$; y eso equivale a decir que $D \equiv 5 \pmod 8$. □

Corolario 3.8.3. *Las leyes de descomposición de los ideales primos de $\mathbb{Z}$ en el cuerpo cuadrático $K := \mathbb{Q}(\sqrt{D})$ vienen dadas por el carácter cuadrático de Kronecker, χ_D. Concretamente,*

$$\chi_D(p) = \begin{cases} 0, & \textit{si } p \textit{ ramifica}, \\ 1, & \textit{si } p \textit{ descompone completamente}, \\ -1, & \textit{si } p \textit{ es inerte}. \end{cases}$$

Demostración: Para el caso de los números primos impares p, basta recordar que el carácter de Kronecker χ_D es el único carácter cuadrático de Dirichlet definido módulo $4|D|$ tal que se satisface la igualdad $\chi_D(p) = \left(\dfrac{D}{p}\right)$ para todo número primo impar p. Y para el caso $p = 2$ basta observar que si $D \equiv 1 \pmod 4$, entonces el valor de $\chi_D(2)$ es dado exactamente por $(-1)^{\omega(D)}$. □

Una aplicación aritmética interesante de las leyes de descomposición de los ideales primos de $\mathbb{Z}$ en el anillo de los enteros de Gauss $\mathbb{Z}(i)$ es la obtención de aquellos enteros que son suma de dos cuadrados. En efecto, podemos demostrar muy fácilmente el teorema siguiente.

Teorema 3.8.4. *Sea $n \in \mathbb{Z}$ un entero positivo cualquiera. Condición necesaria y suficiente para que n sea la suma de los cuadrados de dos números enteros es que todos los números primos impares que dividen n con exponente impar sean de la forma $p \equiv 1 \pmod 4$.*

DEMOSTRACIÓN: En primer lugar, el anillo $\mathbb{Z}[i]$ de los enteros de Gauss es el anillo de los enteros de $\mathbb{Q}(i)$. Observemos que para $a, b \in \mathbb{Z}$ es $\mathrm{N}_{\mathbb{Q}(i)|\mathbb{Q}}(a+bi) = a^2 + b^2$, una suma de dos cuadrados, de manera que un entero n es suma de los cuadrados de dos números enteros exactamente cuando es norma de un elemento de $\mathbb{Z}[i]$. Por otro lado, es bien conocido que $\mathbb{Z}[i]$ es un anillo euclídeo y, por tanto, principal. Además, $i = \sqrt{-1}$ y $-1 \equiv 3 \pmod 4$, de manera que $\Delta(\mathbb{Z}[i]/\mathbb{Z}) = 4\mathbb{Z}$; por tanto $2\mathbb{Z}[i]$ es el cuadrado de un ideal primo de $\mathbb{Z}[i]$. Para p un número natural primo impar, condición necesaria y suficiente para que $p\mathbb{Z}[i]$ sea el producto de dos ideales primos diferentes de $\mathbb{Z}[i]$ es que $p \equiv 1 \pmod 4$, ya que el valor del carácter de Kronecker χ_{-1} en un primo impar p es exactamente $(-1)^{\varepsilon(p)}$. De esta manera, si $p \equiv 1 \pmod 4$, entonces, existen ideales primos $\mathfrak{p}_1, \mathfrak{p}_2$ en $\mathbb{Z}[i]$ tales que $p\mathbb{Z}[i] = \mathfrak{p}_1\mathfrak{p}_2$; si $a + bi$ es un generador de uno de estos ideales primos, ha de ser $\mathrm{N}(a+bi) = a^2+b^2 = p$, ya que $\mathrm{N}(a + bi)$ ha de ser un divisor no trivial de $\mathrm{N}(p) = p^2$. En consecuencia, si $p \equiv 1 \pmod 4$, y también si $p = 2 = 1^2 + 1^2 = \mathrm{N}(1 + i) = \mathrm{N}(1 - i)$, p es suma de los cuadrados de dos números enteros. Puesto que la norma es multiplicativa y todo cuadrado es suma de dos cuadrados, la condición del enunciado es suficiente.

Pero también es necesaria. Supongamos que n es la suma de los cuadrados de dos números enteros; es decir, la norma de un elemento $\alpha \in \mathbb{Z}[i]$. Sea $p \equiv 3 \pmod 4$ un número natural primo que divide n; entonces, el ideal $p\mathbb{Z}[i]$ es un ideal primo de $\mathbb{Z}[i]$ y el exponente de p en la descomposición en factors primos de $n = \mathrm{N}(\alpha)$ es dos veces el exponente de $p\mathbb{Z}[i]$ en la descomposición en primos del ideal $\alpha\mathbb{Z}[i]$, ya que $\mathrm{N}(p) = p^2$. □

3.9. El caso ciclotómico

Ya hemos comentado más arriba la importancia que tienen los cuerpos ciclotómicos. En esta sección se trata de hacer un estudio de algunas de sus propietades aritméticas. Concretamente, estudiaremos cuál es su anillo de enteros, cuál es su discriminante, y cuáles son las leyes de descomposición de los números primos en estos anillos.

Consideremos, pues, un número entero $n > 1$, una raíz primitiva n-ésima de la unidad $\zeta := \zeta_n$, el cuerpo ciclotómico $K := \mathbb{Q}(\zeta)$ y el anillo de los enteros de K, $A := \mathcal{O}_K$. Es bien conocido que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ y que el conjunto $1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(n)-1}$ es una $\mathbb{Q}$-base de $\mathbb{Q}(\zeta)$, donde φ designa la función de

Euler. Ya hemos calculado el discriminante $D(1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(n)-1})$; eso nos da información sobre el conjunto de los ideals primos de $\mathbb{Z}$ que ramifican en A.

Corolario 3.9.1. *Sea p un número natural primo que ramifica en $\mathbb{Q}(\zeta_n)$. Entonces, p divide n.*

Demostración: El discriminante de la extensión $\mathbb{Q}(\zeta)|\mathbb{Q}$ es el ideal principal generado por el discriminante de una $\mathbb{Z}$-base del anillo de los enteros de $\mathbb{Q}(\zeta)$. Puesto que $\zeta \in A$, el discriminante $D(1, \zeta, \ldots, \zeta^{\varphi(n)-1})$ es el producto del discriminante de esta base por el cuadrado del determinante de la matriz de los elementos ζ^i expresados en esta base; esta matriz es de coeficientes enteros y, por tanto, el discriminante de la extensión divide el ideal generado por $D(1, \zeta, \ldots, \zeta^{\varphi(n)-1})$. Por tanto, el discriminante de la extensión divide $n^{\varphi(n)}$. Puesto que los primos que ramifican dividen el discriminate, si p ramifica, entonces p ha de dividir n. □

Este resultado tiene un recíproco. Si n es un número natural impar, entonces $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$, de manera que al hablar de cuerpos ciclotómicos podemos suponer siempre que $n \not\equiv 2 \pmod 4$. En estas condiciones, los ideales primos de $\mathbb{Z}$ que ramifican en $\mathbb{Q}(\zeta)$ son exactamente los ideales $p\mathbb{Z}$ tales que p divide n. Para demostrarlo, comenzaremos por el caso en que n sea potencia de un número primo.

Proposición 3.9.2. *Supongamos que p es un número natural primo y que $n = p^r$, $r \geq 1$. Sea $\alpha := 1 - \zeta \in \mathbb{Q}(\zeta)$. Entonces:*

(i) El ideal principal αA es un ideal primo.

(ii) El grado residual de αA es 1.

(iii) El ideal pA es la potencia $\varphi(n)$-ésima del ideal primo αA.

Demostración: Puesto que las raíces de la unidad son números enteros algebraicos, es claro que $\zeta \in A$; por tanto, αA es un ideal entero de $\mathbb{Q}(\zeta)$. Sea $f(X) := \Phi_{p^r}(X)$ el polinomio ciclotómico; es bien conocido que

$$f(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = 1 + X^{p^{r-1}} + \cdots + X^{(p-1)p^{r-1}}.$$

Para todo número entero i se satisface la fórmula $u_i := \dfrac{1-\zeta^i}{1-\zeta} = 1+\zeta+\zeta^2+\cdots+\zeta^{i-1}$, de manera que $u_i \in A$; y si i no es divisible por p, intercanviando los papeles de ζ y ζ^i, obtenemos también que $u_i^{-1} \in A$, de manera que u_i es un elemento inversible de A. Esto hace que a partir de la igualdad $f(X) = \prod_{\mathrm{mcd}(i,p)=1} (X-\zeta^i)$ podamos escribir

$$p = f(1) = \prod_{\mathrm{mcd}(i,p)=1} (1-\zeta^i) = u(1-\zeta)^{\varphi(n)},$$

donde $u = \prod_{\mathrm{mcd}(i,p)=1} u_i$ es inversible en A. En particular, los elementos α y $1-\zeta^i$, $\mathrm{mcd}(i,p)=1$, son asociados (generan el mismo ideal) y el ideal pA es la potencia $\varphi(n)$-ésima del ideal principal αA. Puesto que $p\mathbb{Z}$ es un ideal primo de $\mathbb{Z}$ y la extensión $\mathbb{Q}(\zeta)|\mathbb{Q}$ es de Galois, la fórmula $efg = n$ nos permite asegurar que el ideal αA es un ideal primo de A de grado residual 1. □

Corolario 3.9.3. *Sea $n \not\equiv 2 \pmod 4$ un número natural, que escribiremos en la forma $n = p^r n'$, con $r \geq 0$ y $\mathrm{mcd}(p,n') = 1$, y sea $\mathfrak{P} \subseteq A$ un ideal primo de A que divide p. Entonces, $e(\mathfrak{P}|p\mathbb{Z}) = \varphi(p^r)$. En particular, condición necesaria y suficiente para que p ramifique en $\mathbb{Q}(\zeta)$ es que p divida n.*

Demostración: Podemos considerar las cadenas de cuerpos $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{n'}) \subseteq \mathbb{Q}(\zeta_n)$ y $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{p^r}) \subseteq \mathbb{Q}(\zeta_n)$. Acabamos de probar que la extensión $\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}$ solamente ramifica en el primo $p\mathbb{Z}$ y que el índice de ramificación es $\varphi(p^r)$; por tanto, la extensión $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ ramifica en $p\mathbb{Z}$ y el índice de ramificación de $p\mathbb{Z}$ es un múltiplo de $\varphi(p^r)$. Por otro lado, en virtud del corolario 3.9.1, la extensión $\mathbb{Q}(\zeta_{n'})|\mathbb{Q}$ no ramifica en ningún ideal primo de $\mathbb{Q}(\zeta_{n'})$ que divide $p\mathbb{Z}$; en consecuencia, si $\mathfrak{P}$ es un ideal primo de $\mathbb{Q}(\zeta_n)$ que contrae a $p\mathbb{Z}$, y si $\mathfrak{p}$ es la contracción de $\mathfrak{P}$ en $\mathbb{Q}(\zeta_{n'})$, entonces, $e(\mathfrak{P}|p\mathbb{Z}) = e(\mathfrak{P}|\mathfrak{p})$ divide el grado $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_{n'})] = \varphi(p^r)$. Por tanto, la igualdad $e(\mathfrak{P}|p\mathbb{Z}) = \varphi(p^r)$. □

A continuación determinaremos el grado residual de todos los ideales primos. Comenzaremos por demostrar el resultado siguiente.

Lema 3.9.4. *Sean ℓ un número natural primo que no divide n y $\mathfrak{l} \subseteq A$ un ideal primo que divide ℓA. Entonces, las clases residuales de las potencias $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ en el cuerpo residual $A/\mathfrak{l}$ son todas diferentes. Además, si $f := f(\mathfrak{l}|\ell)$ designa el grado residual en $\mathfrak{l}$, entonces $\ell^f \equiv 1 \pmod n$.*

DEMOSTRACIÓN: El polinomio $X^n - 1 \in \mathbb{Z}[X]$ es separable sobre $\mathbb{Z}$ y sobre $\mathbb{F}_\ell$, ya que ℓ no divide n. Por tanto, las reducciones módulo $\mathfrak{l}$ de las raíces diferentes de $f(X)$, $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$, han de ser raíces diferentes de $X^n - 1$ en $\overline{\mathbb{F}}_\ell$. Esto demuestra la primera afirmación. Por otro lado, el conjunto $\{\zeta^i \in A/\mathfrak{l} : 0 \leq i \leq n-1\}$ es un subgrupo de orden n de $(A/\mathfrak{l})^*$, que es de orden $\ell^f - 1$. Por tanto, n divide $\ell^f - 1$. □

Lema 3.9.5. *Sea ℓ un número natural primo que no divide n. Entonces, $A = \ell A + \mathbb{Z}[\zeta]$.*

DEMOSTRACIÓN: Hay que demostrar que para todo elemento $b \in A$ existe $b' \in \mathbb{Z}[\zeta]$ tal que $b - b' \in \ell A$. Pongamos $D := D(1, \zeta, \ldots, \zeta^{\varphi(n)-1})$; entonces, $D \in \mathbb{Z}$ y ℓ no divide D, ya que D divide una potencia de n. En consecuencia, D es inversible en $\mathbb{Z}/\ell\mathbb{Z}$; es decir, existe $D' \in \mathbb{Z}$ tal que $DD' \equiv 1 \pmod{\ell}$. Esto nos permite asegurar que $b \equiv DD'b \pmod{\ell A}$. Pero, en virtud del lema 3.6.3, $Db \in \mathbb{Z}[\zeta]$, de manera que $DD'b \in \mathbb{Z}[\zeta]$ y podemos tomar $b' = DD'b$. □

Corolario 3.9.6. *Sean ℓ un número natural primo que no divide n y f un número natural cualquiera tal que $\ell^f \equiv 1 \pmod{n}$. Entonces, para todo elemento $b \in A$ es $b^{\ell^f} - b \in \ell A$.*

DEMOSTRACIÓN: En efecto, acabamos de probar que existen $a_i \in \mathbb{Z}$ tales que $b - \sum_{i=1}^{\varphi(n)} a_i \zeta^i \in \ell A$. Puesto que $a_i \in \mathbb{Z}$, se satisfacen las congruencias $a_i^\ell \equiv a_i \pmod{\ell}$, de manera que $a_i^\ell - a_i \in \ell\mathbb{Z} \subseteq \ell A$; por tanto, $b^\ell - \sum_{i=1}^{\varphi(n)} a_i \zeta^{i\ell} \in \ell A$ y, por inducción, $b^{\ell^f} - \sum_{i=1}^{\varphi(n)} a_i \zeta^{i\ell^f} \in \ell A$. Por hipótesis, $\zeta^{\ell^f} = \zeta$, de manera que la última suma es b; por tanto, $b^{\ell^f} - b \in \ell A$ como queríamos probar. □

Proposición 3.9.7. *Sean ℓ un número natural primo que no divide n y f el número natural menor tal que $\ell^f \equiv 1 \pmod{n}$. Entonces,*

$$\ell A = \mathfrak{l}_1 \mathfrak{l}_2 \cdots \mathfrak{l}_g,$$

donde $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_g$ son ideales primos diferentes de A, de grados residuales $f(\mathfrak{l}_i|\ell\mathbb{Z}) = f$, y g es definido por la fórmula $fg = \varphi(n)$.

DEMOSTRACIÓN: Puesto que ℓ no divide n, la asignación $\zeta \mapsto \zeta^\ell$ define un automorfismo de $\mathbb{Q}(\zeta)$; pongamos F_ℓ. Entonces, para todo $b \in A$ es $F_\ell(b) - b^\ell \in \ell A$, ya que podemos elegir $a_i \in \mathbb{Z}$ tales que $b - \sum_{i=1}^{\varphi(n)} a_i \zeta^i \in \ell A$ y, en consecuencia, $F_\ell(b) \equiv \sum_i a_i \zeta^{i\ell} \equiv \sum_i a_i^\ell \zeta^{i\ell} \equiv \left(\sum_i a_i \zeta^i\right)^\ell \equiv b^\ell \pmod{\ell A}$. Por inducción, $F_\ell^f(b) - b^{\ell^f} \in \ell A$, de manera que, en virtud del corolario anterior, $F_\ell^f(b) - b \in \ell A$, para todo $b \in A$.

Por hipótesis, el orden del automorfismo $F_\ell \in \mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q})$ es exactamente f. Sean $\mathfrak{l}$ un ideal primo de A que divide ℓA y f_1 el grado residual de $\mathfrak{l}$. Esto nos dice que $A/\mathfrak{l}A$ es el cuerpo finito de ℓ^{f_1} elementos; por tanto, f_1 es el número natural no nulo menor tal que para todo elemento $b \in A$ se satisfce $b^{\ell^{f_1}} - b \in \mathfrak{l}$. Puesto que para f también se satisface, debe ser $f_1 \leq f$. Pero, por otro lado, puesto que $\zeta^{\ell^{f_1}} - \zeta \in \mathfrak{l}$ y las raíces de la unidad $1, \zeta, \ldots, \zeta^{n-1}$ son diferentes en $A/\mathfrak{l}$, debe ser $\ell^{f_1} \equiv 1 \pmod{n}$; esto demuestra la otra desigualdad: $f \leq f_1$. Por tanto, $f = f_1$, hecho que acaba la demostración. □

Podemos, por tanto, dar las leyes de descomposición de todos los ideales primos de $\mathbb{Z}$ en los cuerpos ciclotómicos $\mathbb{Q}(\zeta)$, $\zeta = \zeta_n$ una raíz primitiva n-ésima de la unidad.

Teorema 3.9.8. *Sean $n \not\equiv 2 \pmod 4$ un número natural, ζ una raíz primitiva n-ésima de la unidad, A el anillo de los enteros del cuerpo ciclotómico $\mathbb{Q}(\zeta)$ y $p \in \mathbb{Z}$ un número natural primo. La descomposición de $p\mathbb{Z}$ en A viene dada de la manera siguiente. Pongamos $n = p^r n'$ con $r \geq 0$ y $\mathrm{mcd}(p, n') = 1$; entonces*

$$pA = (\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_g)^e,$$

donde $e = \varphi(p^r)$, $\mathfrak{p}_i$ son ideales primos diferentes de A de grado residual el número entero positivo menor f tal que $p^f \equiv 1 \pmod{n'}$ y $fg = \varphi(n')$.

DEMOSTRACIÓN: Resta ver el caso $r \geq 1$. Podemos considerar la cadena de cuerpos $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{n'}) \subseteq \mathbb{Q}(\zeta_n)$ y tener en cuenta la multiplicatividad de los índices de ramificación y la de los grados residuales. Sea $\mathfrak{P} \subseteq A$ un ideal primo que divide p y sea $\mathfrak{p}$ su contracción al anillo de los enteros de $\mathbb{Q}(\zeta_{n'})$. Entonces, $f(\mathfrak{P}|\mathfrak{p}) = g(\mathfrak{p}) = 1$, ya que $e(\mathfrak{P}|\mathfrak{p}) = \varphi(p^r)$ es el grado de la extensión; por tanto, $f(\mathfrak{P}|p) = f(\mathfrak{p}|p)$ y podemos aplicar la proposición anterior. Y puesto que $e(\mathfrak{p}|p) = 1$, es $e(\mathfrak{P}|p) = \varphi(p^r)$. □

Vamos a hacer, ahora, el estudio de los anillos de los enteros.

Teorema 3.9.9. *Sean n un número entero, $\zeta := \zeta_n$ una raíz primitiva n-ésima de la unidad, y $K := \mathbb{Q}(\zeta)$ el n-ésimo cuerpo ciclotómico. Entonces, el anillo de los enteros de K es el anillo $\mathcal{O}_K = \mathbb{Z}[\zeta]$.*

Demostración: Sean $A := \mathcal{O}_K$ y $B := \mathbb{Z}[\zeta]$. Claramente, $\zeta \in A$, de manera que $B \subseteq A$ y hay que provar la igualdad. Comencemos por el caso $n = p^r$, donde p es un número natural primo y $r \geq 1$. Retomemos la notación de la proposición 3.9.2. Hemos demostrado que $B + \alpha A = A$; puesto que $\alpha \in B$, después de multiplicar por α y substituir, obtenemos la igualdad $B + \alpha^2 A = A$; y, por inducción, para todo número entero $s \geq 1$ es $B + \alpha^s A = A$. Ahora bien, también hemos visto que $D(1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(n)-1})A \subseteq B$ y que $D(1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(n)-1})$ es una potencia de p. Por tanto, para s suficientemente grande se satisface la inclusión $p^s A \subseteq B$; y puesto que pA es una potencia de αA, también $\alpha^s A \subseteq B$ para s suficientemente grande. Esto implica la igualdad $B = A$.

El caso general se puede probar por inducción sobre el número de primos diferentes que dividen n. Pongamos $n = p^r n'$ con p primo, $\mathrm{mcd}(p, n') = 1$, y $r \geq 1$, $\zeta' := \zeta_{n'}$ una raíz primitiva n'-ésima de la unidad, $K' := \mathbb{Q}(\zeta')$ y $A' = B' = \mathbb{Z}[\zeta']$ el anillo de los enteros de K' (hipótesis de inducción). Es claro que $\zeta^{n'}$ es una raíz primitiva p^r-ésima de la unidad y que $A'[\zeta^{n'}] = \mathbb{Z}[\zeta] \subseteq A$; hay que probar la igualdad. El discriminante $D(1, \zeta^{n'}, \zeta^{2n'}, \ldots, \zeta^{n'(\varphi(p^r)-1)})$ se puede calcular como el discriminante de la extensión $\mathbb{Q}(\zeta^{n'})|\mathbb{Q}$, ya que las extensiones $\mathbb{Q}(\zeta_{n'})|\mathbb{Q}$ y $\mathbb{Q}(\zeta^{n'})|\mathbb{Q}$ son linealmente disjuntas; por lo que hemos visto en el caso en que n es potencia de p, el discriminante $D(1, \zeta^{n'}, \zeta^{2n'}, \ldots, \zeta^{n'(\varphi(p^r)-1)})$ es una potencia de p en $\mathbb{Z}$ y, por tanto, una potencia p^k de p en A'. Igual que en la demostración del lema 3.6.3, obtenemos la inclusión $p^k A \subseteq A'[\zeta^{n'}]$ teniendo en cuenta la regla de Cramer. Por otro lado, puesto que la extensión $\mathbb{Q}(\zeta)|\mathbb{Q}(\zeta')$ es totalmente ramificada en todos los ideales primos $\mathfrak{P}$ de A que dividen $p\mathbb{Z}$ (es decir, sus índices de ramificación coinciden con el grado), los cuerpos residuales de A en $\mathfrak{P}$ y de A' en $\mathfrak{P} \cap A'$ coinciden para todo ideal primo $\mathfrak{P}$ de A que divide p. Sean $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ todos los ideales primos de A que dividen p y sean $\mathfrak{P}'_i := \mathfrak{P}_i \cap A'$ sus contracciones a A'. Se tienen igualdades $pA' = \mathfrak{P}'_1 \mathfrak{P}'_2 \cdots \mathfrak{P}'_g$ en A', ya que el número de ideales primos de A y de A' que dividen p es el mismo y $A'/\mathbb{Z}$ es no ramificada en p, y $(1 - \zeta^{n'})A = \mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_g$, ya que la potencia $\varphi(p^r)$-ésima de los dos ideales es el ideal pA. Esta última igualdad nos permite asegurar que

$A/(1-\zeta^{n'})A \simeq A'/\mathfrak{P}'_1\mathfrak{P}'_2\cdots\mathfrak{P}'_g$, en virtud del teorema chino del resto, de manera que $A = A'+(1-\zeta^{n'})A = A'[\zeta^{n'}]+(1-\zeta^{n'})A$. De nuevo por inducción teniendo en cuenta que $1-\zeta^{n'} \in A'[\zeta^{n'}]$, se obtiene que para todo número entero s suficientemente grande es $A = A'[\zeta^{n'}] + (1-\zeta^{n'})^s A$. Puesto que una potencia del ideal $(1-\zeta^{n'})A$ es el ideal pA, si tomamos s suficientemente grande, obtenemos la igualdad $A = A'[\zeta^{n'}]$, como queríamos demostrar. □

Como consecuencia de este resultado, el discriminante $\Delta(\mathbb{Z}[\zeta]|\mathbb{Z})$ es el determinante $D(1,\zeta,\ldots,\zeta^{\varphi(n)-1})$ que hemos calculado en la proposición 3.6.7. Obtenemos, por tanto, el resultado siguiente.

Corolario 3.9.10. *El discriminante de la extensión ciclotómica $\mathbb{Z}[\zeta]|\mathbb{Z}$, donde $\zeta = \zeta_n$ es una raíz primitiva n-ésima de la unidad, es dado por la fórmula*

$$\Delta(\mathbb{Z}[\zeta]/\mathbb{Z}) = (-1)^{\varphi(n)(\varphi(n)-1)/2}\frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}. \square$$

Observación 3.9.11. Esta fórmula se puede probar de otra manera usando unas ciertas fórmulas de transitividad del discriminante, que no hemos probado.

Una aplicación interesante de las leyes de descomposición de los números primos en los cuerpos ciclotómicos $\mathbb{Q}(\zeta_p)$, p un número primo, es una nueva demostración de la ley de reciprocidad cuadrática. Recordemos que si ζ es una raíz primitiva p-ésima de la unidad, p un número natural primo impar, entonces el único subcuerpo cuadrático de $\mathbb{Q}(\zeta)$ es el cuerpo $\mathbb{Q}(\sqrt{p^*})$, donde $p^* = (-1)^{\varepsilon(p)}p$. La parte principal de la demostración es el resultado siguiente.

Lema 3.9.12. *Sean p, ℓ, números naturales primos impares diferentes. Condición necesaria y suficiente para que ℓ descomponga como producto de dos ideales primos diferentes en $\mathbb{Q}(\sqrt{p^*})$ es que descomponga como producto de un número par de ideales primos diferentes en $\mathbb{Q}(\zeta)$.*

Demostración: Sean $K := \mathbb{Q}(\zeta)$, A su anillo de enteros, $K' := \mathbb{Q}(\sqrt{p^*})$, A' su anillo de enteros, $\mathfrak{L} \subseteq A$ un ideal primo que divide ℓ y $\mathfrak{l} := \mathfrak{L} \cap A'$ su contracción. La sucesión exacta de grupos de Galois

$$1 \longrightarrow \mathrm{Gal}\,(K|K') \longrightarrow \mathrm{Gal}\,(K|\mathbb{Q}) \longrightarrow \mathrm{Gal}\,(K'|\mathbb{Q}) \longrightarrow 1$$

da lugar, por restricción, a la sucesión de grupos de descomposición

$$1 \longrightarrow D(\mathfrak{L}|\mathfrak{l}) \longrightarrow D(\mathfrak{L}|\ell) \longrightarrow D(\mathfrak{l}|\ell) \longrightarrow 1.$$

Esta sucesión también es exacta. La única parte que merece un poco de comentario es la exhaustividad del morfismo $D(\mathfrak{L}|\ell) \longrightarrow D(\mathfrak{l}|\ell)$. Si $\sigma' \in D(\mathfrak{l}|\ell)$, entonces, existe $\sigma \in \mathrm{Gal}\,(K|\mathbb{Q})$ tal que la restricción de σ a K' es σ'; los ideales $\mathfrak{L}$ y $\sigma(\mathfrak{L})$ contraen ambos a $\mathfrak{l}$ en A', de manera que existe $\tau \in \mathrm{Gal}\,(K|K')$ tal que $\tau\sigma\mathfrak{L} = \mathfrak{L}$; por tanto, el automorfismo $\tau\sigma$ pertenece al grupo de descomposición $D(\mathfrak{L}|\mathfrak{l})$; finalmente, la imagen de $\tau\sigma$ en $D(\mathfrak{L}|\ell)$ se aplica sobre σ', ya que τ es la identidad en K'.

Sean g, g', g'' los índices de los grupos de descomposición $D(\mathfrak{L}|\ell)$, $D(\mathfrak{l}|\ell)$, $D(\mathfrak{L}|\mathfrak{l})$, respectivamente; es decir, los números de primos que dividen ℓ, ℓ, $\mathfrak{l}$, en las extensiones $K|\mathbb{Q}$, $K'|\mathbb{Q}$, y $K|K'$. La exactitud de las dos sucesiones anteriores demuestra que $g = g'g''$, de manera que si g' es par, también lo es g. Recíprocamente, supongamos que g es par. Teniendo en cuenta que los grupos de Galois y, por tanto, los grupos de descomposición, son grupos cíclicos, se deduce inmediatamente que $D(\mathfrak{L}|\ell)$ está incluído en el único subgrupo de $\mathrm{Gal}\,(K|\mathbb{Q})$ de índice 2, que es $\mathrm{Gal}\,(K|K')$, de manera que $D(\mathfrak{L}|\ell) = D(\mathfrak{L}|\mathfrak{l})$ y $D(\mathfrak{l}|\ell)$ es el grupo trivial; esto dice que $g' = 2$, como queríamos ver. □

Ahora podemos acabar fácilmente una demostración de la ley de reciprocidad cuadrática. La descripción de las leyes de descomposición de los primos en los cuerpos cuadráticos nos permite asegurar que una condición necesaria y suficiente para que ℓ descomponga como producto de dos ideales primos diferentes de A' es que $\left(\dfrac{p^*}{\ell}\right) = 1$; y el resultado que acabamos de probar admite la consecuencia siguiente.

Corolario 3.9.13. *Condición necesaria y suficiente para que ℓ descomponga completamente en A' es que* $\left(\dfrac{\ell}{p}\right) = 1$.

Demostración: Con las mismas notaciones que en la demostración del lema anterior podemos escribir que g es par si, y sólo si, el grado residual f de $\mathfrak{L}|\ell$ divide $(p-1)/2$; y esto último equivale a decir que $\ell^{(p-1)/2} \equiv 1 \pmod{p}$, vía la caracterización del grado residual de los primos en las extensiones ciclotómicas de $\mathbb{Q}$ que hemos dado más arriba. Pero en ${\mathbb{F}_p}^*$ los elementos ℓ que satisfacen la congruencia anterior son exactamente los cuadrados, ya que ${\mathbb{F}_p}^*$ es un grupo cíclico. Por tanto, ℓ descompone completamente en A' si, y sólo si, $\left(\dfrac{\ell}{p}\right) = 1$, por definición del símbolo de Legendre. □

Por tanto, obtenemos la equivalencia entre las propiedades $\left(\frac{p^*}{\ell}\right) = 1$ y $\left(\frac{\ell}{p}\right) = 1$; sólo hay que tener en cuenta el valor del símbolo $\left(\frac{-1}{\ell}\right)$. $\square$

Capítulo 4

Geometría de los números

Este capítulo se dedica a hacer el estudio de los grupos de las unidades y de los grupos de clases de ideales de los anillos de los enteros de los cuerpos de números. Antes de estudiar el concepto y algunas propiedades de las redes de $\mathbb{R}^n$ introduciremos el concepto de dominio fundamental para una acción de un grupo en un conjunto; especialmente en el caso de acciones continuas en espacios topológicos, que tienen aplicaciones importantes en otros temas de estudio de la teoría algebraica de números; concretamente, en el estudio de las curvas elípticas y las formas modulares.

4.1. Dominios fundamentales

Sean X un espacio topológico, G un grupo topológico y $G \times X \xrightarrow{h} X$ una acción continua de G en X; eso quiere decir que para todo elemento $\sigma \in G$ disponemos de una aplicación continua $h_\sigma : X \longrightarrow X$ de manera que $h_{\sigma\sigma'} = h_\sigma \circ h_{\sigma'}$ y que $h_1 = \mathrm{id}_X$, donde 1 denota el elemento neutro de G. En particular, la aplicación h_σ es un homeomorfismo con inverso $h_{\sigma^{-1}}$.

Definición 4.1.1. Se llama dominio fundamental de X para la acción h todo subespacio topológico $D \subseteq X$ que satisface las condiciones siguientes:

(i) D contiene un representante de cada una de las órbitas Gx, $x \in X$; y

(ii) si dos elementos diferentes de D son de la misma órbita, entonces están en la frontera de D.

Ejemplo 4.1.2. Consideremos $X := \mathbb{C}$ como espacio topológico, $G := \mathbb{Z}[i]$ como grupo topológico discreto, y la acción dada por traslación: $(a+bi, z) \mapsto a + bi + z$. Un dominio fundamental para esta acción es el paralelogramo $\{z \in \mathbb{C} : 0 \leq \Re(z) \leq 1,\ 0 \leq \Im(z) \leq 1\}$. También lo es el paralelogramo no compacto $\{z \in \mathbb{C} : 0 \leq \Re(z) < 1,\ 0 \leq \Im(z) < 1\}$.

Ejemplo 4.1.3. Más generalmente, sean $X = \mathbb{C}$, $G = \mathbb{Z} \times \mathbb{Z}$ considerado como grupo discreto y fijemos una $\mathbb{R}$-base $\{\omega_1, \omega_2\}$ de $\mathbb{C}$. Definimos la acción por la fórmula $((a, b), z) \mapsto a\omega_1 + b\omega_2 + z$. Un dominio fundamental para esta acción es el paralelogramo $D := \{z = a\omega_1 + b\omega_2 \in \mathbb{C} : a, b \in \mathbb{R},\ 0 \leq a \leq 1,\ 0 \leq b \leq 1\}$.

Observación 4.1.4. El cociente $\mathbb{C}/\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \simeq D/(\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2) \cap D$ es una superficie de Riemann compacta de género 1 (un toro); se llama la curva elíptica definida por la pareja ω_1, ω_2.

Ejemplo 4.1.5. Más generalmente aún, consideremos $X := \mathbb{R}^n$, $G := \mathbb{Z}^n$ y la acción dada a partir de una $\mathbb{R}$-base $\{e_1, \ldots, e_n\}$ de $\mathbb{R}^n$ por la fórmula de traslación $((a_1, \ldots, a_n), x) \mapsto x + \sum_{i=1}^{n} a_i e_i$. Un dominio fundamental para esta acción es el paralelepípedo fundamental $D = \{\sum_{i=1}^{n} a_i e_i : a_i \in \mathbb{R},\ 0 \leq a_i \leq 1\}$. También lo es el paralelepípedo no compacto $D = \{\sum_{i=1}^{n} a_i e_i : a_i \in \mathbb{R},\ 0 \leq a_i < 1\}$.

Ejemplo 4.1.6. Sea $X = \mathbb{H}$ el semiplano superior de Poincaré, $\mathbb{H} := \{z \in \mathbb{C} : \Re(z) > 0\}$ y sea $G = \mathbf{GL}_2{}^+(\mathbb{R})$, el grupo de las matrices cuadradas de rango 2 y coeficientes reales que tienen determinante positivo. Podemos definir una acción en $\mathbb{H}$ por la fórmula siguiente:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} z := \frac{az + b}{cz + d}.$$

Un dominio fundamental para esta acción es cualquier conjunto D formado por un solo elemento; en efecto, la acción es transitiva.

Ejercicio 4.1.7. El conjunto $D := \{z \in \mathbb{H} : -1/2 \leq \Re(z) \leq 1/2,\ |z| \geq 1\}$ es un dominio fundamental para la restricción de la acción anterior al subgrupo discreto $\mathbf{SL}_2(\mathbb{Z})$ de las matrices de coeficientes enteros y determinante 1.

4.2. Redes de $\mathbb{R}^n$

Nos interesará hablar de subgrupos discretos de $\mathbb{R}^n$; conviene tener a mano el resuldado siguiente.

Proposición 4.2.1. *Sea G un subgrupo discreto de $\mathbb{R}^n$. Entonces, G es un grupo abeliano libre de rango $r \leq n$.*

Demostración: Podemos elegir en G un conjunto de elementos $\{e_1, e_2, \ldots, e_r\}$ que sean $\mathbb{R}$-linealmente independientes de manera que r sea máximo; en particular, $r \leq n$. Consideremos el subconjunto $S := \{\sum_{i=1}^{n} a_i e_i : a_i \in \mathbb{R}, 0 \leq a_i \leq 1\}$. Puesto que S es un subconjunto compacto de $\mathbb{R}^n$ y G es discreto, el conjunto $S \cap G$ es finito. Se trata de demostrar que $S \cap G$ es un conjunto de generadores de G; de esta manera obtendremos que G es un grupo abeliano libre, ya que no tiene torsión por ser un subgrupo de $\mathbb{R}^n$ y todo grupo abeliano finitamente generado y sin torsión es libre.

Sea, pues, $x \in G$; podemos escribir x en la forma $x = \sum_{i=1}^{r} \alpha_i e_i$ con $\alpha_i \in \mathbb{R}$, ya que en caso contrario el conjunto $\{e_1, e_2, \ldots, e_r, x\}$ estaría formado por más de r elementos $\mathbb{R}$-linealmente independientes de G y r no sería máximo. Pongamos $y := x - \sum_{i=1}^{r} [\alpha_i] e_i = \sum_{i=1}^{r} (\alpha_i - [\alpha_i]) e_i$; puesto que $y, e_1, \ldots, e_r \in S \cap G$ y $x = y + \sum_{i=1}^{r} [\alpha_i] e_i$, resulta que $S \cap G$ genera G como grupo abeliano y G es finitamente generado.

Resta ver que el rango de G es menor o igual que n. Para todo número entero k y todo elemento $x \in G$ pongamos $x_k := kx - \sum_{i=1}^{r} [k\alpha_i] e_i = \sum_{i=1}^{r} (k\alpha_i - [k\alpha_i]) e_i$; como antes, $x_k \in S \cap G$ y, puesto que $S \cap G$ es finito, existen números enteros diferentes k, j tales que $x_k = x_j \in S \cap G$. La $\mathbb{R}$-independencia lineal de los elementos e_i y la última igualdad nos permiten asegurar que para todo índice i los coeficientes α_i son racionales, ya que $\alpha_i = (k-j)^{-1}([k\alpha_i] - [j\alpha_i])$. Esto implica que x pertenece al $\mathbb{Q}$-espacio vectorial generado por los elementos e_i. En particular, los elementos (en número finito) de $S \cap G$ son combinaciones lineales de los elementos e_i que tienen coeficientes racionales

y podemos considerar un denominador común $d \in \mathbb{Z}$, $d \neq 0$, de todos estos coeficientes; entonces, el grupo abeliano libre G es un subgrupo del grupo abeliano libre $\bigoplus_{i=1}^{r} d^{-1}\mathbb{Z}e_i$ de rango r; por tanto, el rango de G es menor o igual que r y, puesto que G contiene r elementos que son $\mathbb{R}$-linealmente independientes, los e_i, el grupo G es de rango r. □

Definición 4.2.2. Un subgrupo $G \subseteq \mathbb{R}^n$ se llama red de $\mathbb{R}^n$ si es un subgrupo discreto de rango n.

Sea G una red de $\mathbb{R}^n$; entonces G es un grupo topológico que actúa en $\mathbb{R}^n$ por translación: $(\sigma, x) \mapsto x + \sigma$ (cf. ejemplo 4.1.5 más arriba). El conjunto $D := \{\sum_{i=1}^{n} a_i e_i : 0 \leq a_i < 1\}$, donde $e_1, \ldots, e_n$ es una $\mathbb{Z}$-base de G, es un dominio fundamental para la acción de G en $\mathbb{R}^n$; se llama el paralelepípedo fundamental relativo a la base $\{e_1, \ldots, e_n\}$. Observemos que D es un subconjunto medible Lebesgue de $\mathbb{R}^n$; su medida $\mu(D)$ se llama la malla de la red G y se representa usualmente por $\mu(G)$. Por otro lado, no hay ninguna pareja de elementos de D que estén en la misma órbita para la acción de G; esta propiedad será útil en seguida.

Lema 4.2.3. *La malla de una red G de $\mathbb{R}^n$ no depende de la $\mathbb{Z}$-base elegida en G.*

Demostración: En efecto, un cambio de base en G es dado por una matriz $M \in \mathbf{GL}_n(\mathbb{Z})$; y la medida del nuevo paralelepípedo fundamental se obtiene a partir de la anterior multiplicando por el valor absoluto del determinante de M. Pero las matrices de $\mathbf{GL}_n(\mathbb{Z})$ son de determinante ± 1. □

Teorema 4.2.4. (Minkowski) *Sean G una red de $\mathbb{R}^n$ y X un subconjunto medible Lebesgue de $\mathbb{R}^n$ tal que $\mu(X) > \mu(G)$. Entonces, X contiene dos elementos diferentes x, y tales que $x \equiv y \pmod{G}$.*

Demostración: Sean $\{e_1, \ldots, e_n\}$ una $\mathbb{Z}$-base de G y D el paralelepípedo fundamental para $\mathbb{R}^n$ relativo a esta base. Por definición de dominio fundamental, los conjuntos $g + D$, $g \in G$, dan un recubrimiento de $\mathbb{R}^n$; este recubrimiento es disjunto en virtud de la elección de D. En consecuencia, los conjuntos $X \cap (g + D)$, $g \in G$, forman un recubrimiento disjunto de X. Por

otro lado, puesto que la medida de Lebesgue es invariante por translación (es la medida de Haar del grupo topológico localmente compacto $\mathbb{R}^n$), los conjuntos $g+D$ son medibles; por tanto, las intersecciones $X\cap(g+D)$ también son medibles y su medida coincide con la medida de sus transladados $(-g+X)\cap D$. De la igualdad $\mu(X)=\sum_{g\in G}\mu(X\cap(g+D))$, que se deduce del hecho que X es recubierto de manera disjunta por los conjuntos $X\cap(g+D)$, obtenemos que $\mu(X)=\sum_{g\in G}\mu((-g+X)\cap D)$, de manera que los conjuntos $(-g+X)\cap D$ no pueden ser disjuntos dos a dos, ya que su reunión es un subconjunto de D y estamos suponiendo que $\mu(G)=\mu(D)<\mu(X)$.

Por tanto, existen elementos diferentes $g,g'\in G$ tales que $(-g+X)\cap(-g'+X)\cap D$ es no vacío; es decir, existen elementos $x,y\in X$ tales que $x-g=y-g'$ y, entonces, $x-y=g-g'\in G$ y $x\neq y$ ya que $g\neq g'$. □

Corolario 4.2.5. *Sean G una red de $\mathbb{R}^n$ y $X\subseteq\mathbb{R}^n$ un subconjunto convexo, simétrico respecto al origen i medible Lebesgue. Supongamos que $\mu(X)>2^n\mu(G)$ o bien que X es compacto y $\mu(X)\geq 2^n\mu(G)$. Entonces, existe $x\in G\cap X$ tal que $x\neq 0$.*

Demostración: Supongamos que $\mu(X)>2^n\mu(G)$; entonces, el conjunto $Y:=\{x/2:x\in X\}$ también es medible Lebesgue y $\mu(Y)=2^{-n}\mu(X)>\mu(G)$, por hipótesis. En virtud del teorema de Minkowski, existen dos puntos diferentes $y_1,y_2\in Y$ tales que $y_2-y_1\in G$; el punto $x:=y_2-y_1$ es un punto no nulo de $X\cap G$, ya que X es convexo y simétrico respecto al origen, $2y_1,2y_2\in X$ y x es el punto medio de $2y_2$ y $-2y_1$.

En el caso en que supongamos que X es compacto y que $\mu(X)\geq 2^n\mu(G)$, para todo $\varepsilon>0$ podemos poner $X_\varepsilon:=(1+\varepsilon)X$, de manera que se satisfacen las mismas hipótesis con la mejora $\mu(X_\varepsilon)>\mu(G)$, y podemos aplicar a X_ε lo que acabamos de demostrar: para cada $\varepsilon>0$ existe un punto no nulo $x_\varepsilon\in G\cap X_\varepsilon$. Los conjuntos $X'_\varepsilon:=X_\varepsilon\cap G-\{0\}$ son no vacíos, compactos y discretos, de manera que son finitos y no vacíos; y la finitud de todos ellos implica que la intersección $\bigcap_{\varepsilon>0}X'_\varepsilon$ es no vacía. Finalmente, de la compacidad de X se deduce que la intersección es $X\cap G\neq\{0\}$, ya que $\bigcap_{\varepsilon>0}(1+\varepsilon)X=X$. Esto acaba la demostración. □

4.3. La inmersión canónica de un cuerpo de números

Sea K un cuerpo de números y sea $n := [K : \mathbb{Q}]$ su grado. Si consideramos una clausura algebraica $\overline{\mathbb{Q}}$ de $\mathbb{Q}$, entonces existen exactamente n maneras diferentes de pensar K como subcuerpo de $\overline{\mathbb{Q}}$; en efecto, puesto que $\mathbb{Q}$ es de característica cero, toda extensión de $\mathbb{Q}$ es separable, de manera que el grado de separabilidad de cualquier cuerpo extensión finita K (es decir, el número de maneras de incluir K en $\overline{\mathbb{Q}}$) coincide con el grado.

Por otro lado, podemos cambiar $\overline{\mathbb{Q}}$ por cualquier cuerpo que lo contenga y la propiedad no varía, ya que una $\mathbb{Q}$-inmersión de K ha de estar incluída en $\overline{K} = \overline{\mathbb{Q}}$; en particular, el número total de $\mathbb{Q}$-inmersiones de K en $\mathbb{C}$ es exactamente n.

Podemos pensar, aún, en las $\mathbb{Q}$-inmersiones de K en $\mathbb{R}$; puesto que $\mathbb{R} \subseteq \mathbb{C}$, es claro que el número de $\mathbb{Q}$-inmersiones de K en $\mathbb{R}$ es $r_1 \leq n$. Sea σ una inmersión de K en $\mathbb{C}$; si componemos con la conjugación compleja, $c : \mathbb{C} \longrightarrow \mathbb{C}$, dada por $c(a+bi) := a-bi$, para $a, b \in \mathbb{R}$, obtendremos otra $\mathbb{Q}$-inmersión $c\sigma$ de K en $\mathbb{C}$. Es claro que una condición necesaria y suficiente para que $\sigma = c\sigma$ es que $\sigma(K) \subseteq \mathbb{R}$. Eso nos permite asegurar que el número n de $\mathbb{Q}$-inmersiones diferentes de K en $\mathbb{C}$ se puede expresar en la forma $n = r_1 + 2r_2$, donde r_2 es el número de conjuntos $\{\sigma, c\sigma\}$ tals que $\sigma \neq c\sigma$.

A la vista de este hecho, y por comodidad, numeraremos las $\mathbb{Q}$-inmersiones de K en la forma $\sigma_1, \ldots, \sigma_{r_1}$, las *inmersiones reales*, y σ_{r_1+j}, $\sigma_{r_1+r_2+j} = c\sigma_{r_1+j}$, con $1 \leq j \leq r_2$, los pares de $\mathbb{Q}$-inmersiones *complejas conjugadas no reales* de K. Observemos que, de esta manera, el conocimiento de las inmersiones σ_i para $1 \leq i \leq r_1 + r_2$ ya determina unívocamente las otras.

Definición 4.3.1. El morfismo de anillos $K \xrightarrow{\sigma} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ definido por la asignación

$$x \mapsto (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x))$$

se llama la inmersión canónica de K. A menudo se acostumbra a identificar $\mathbb{C}$ con $\mathbb{R}^2$ (como $\mathbb{R}$-espacio vectorial); en este caso, la inmersión canónica se piensa en la forma $K \xrightarrow{\sigma} \mathbb{R}^n$.

La importancia y la utilidad de la inmersión canónica de K se ven bien en el resuldado siguiente.

Proposición 4.3.2. *Sea G un subgrupo abeliano libre de rango n de K. Entonces, la imagen de G por la inmersión canónica es una red de $\mathbb{R}^n$. Si $\{e_1, \dots, e_n\}$ es una $\mathbb{Z}$-base de G, la malla de la red $\sigma(G)$ es dada por la fórmula*

$$\mu(\sigma(G)) = 2^{-r_2} \left|\det(\sigma_i(e_j))\right| .$$

Demostración: Los vectores $\sigma(e_1), \dots, \sigma(e_n)$ generan la imagen $\sigma(G)$; si demostramos que son linealmente independientes, entonces sabremos que forman una $\mathbb{Z}$-base de $\sigma(G)$, de manera que $\sigma(G)$ es una red de $\mathbb{R}^n$ y $\sigma(e_1)$, $\dots$, $\sigma(e_n)$ son los vértices de un paralelepípedo fundamental; por tanto, podremos calcular la malla de esta red como el valor absoluto del determinante de los vectores $\sigma(e_j)$ expresados en la base "canónica" de $\mathbb{R}^n$. Ahora bien, los componentes del vector $\sigma(e_j)$ en la base canónica de $\mathbb{R}^n$ son exactamente los números $\sigma_i(e_j)$ para los r_1 componentes reales, y los pares $\Re(\sigma_i(e_j)), \Im(\sigma_i(e_j))$, para los componentes $\sigma_i(e_j)$ con $r_1 < i \leq r_1 + r_2$. Teniendo en cuenta que $\Re(\sigma_i(e_j)) = (\sigma_i(e_j) + \sigma_{i+r_2}(e_j))/2$, $\Im(\sigma_i(e_j)) = (\sigma_i(e_j) - \sigma_{i+r_2}(e_j))/2i$, y la linealidad del determinante respecto a las filas, el determinante a calcular es el producto del factor $(2i)^{-r_2}$ por el determinante $\det(\sigma_i(e_j))$; en efecto, para cada índice i, $1 \leq i \leq r_2$, podemos cambiar la fila formada por los componentes $\Re(\sigma_{r_1+i}(e_j))$ por la formada por los $\sigma_{r_1+i}(e_j)$; después, la formada por los componentes $\Im(\sigma_{r_1+i}(e_j))$ por la que consta de los $\sigma_{r_1+r_2+i}(e_j)/(-2i)$; y, finalmente, sacar factor común los r_2 factores $-1/2i = i/2$. Pero el determinante $\det(\sigma_i(e_j))$ es no nulo, ya que los elementos e_j son una $\mathbb{Q}$-base de K y la extensión $K|\mathbb{Q}$ es separable. Este cálculo demuestra, por tanto, que los vectores $\sigma(e_j)$ son $\mathbb{R}$-linealmente independientes y que la malla de la red es dada por la fórmula enunciada. □

Corolario 4.3.3. *Sea $\{e_1, \dots, e_n\}$ una $\mathbb{Z}$-base del anillo de los enteros del cuerpo de números K. Condición necesaria y suficiente para que el discriminante absoluto de K, $D(e_1, \dots, e_n)$, sea positivo es que el número r_2 de pares de inmersiones complejas conjugadas no reales de K sea par.*

Demostración: En efecto, el discriminante que hay que calcular es el cuadrado del determinante $\det(\sigma_i(e_j))$, donde $\sigma_i(e_j)$ son los diferentes conjugados de e_j; y en la demostración de la proposición anterior hemos visto que este determinante es el producto de un determinante de entradas reales por el producto de los factores $(-2i)^{r_2}$. Por tanto, el discriminante de los vectores e_j es un número real positivo multiplicado por $(-2i)^{2r_2}$; y este número es positivo cuando r_2 es par. □

Observación 4.3.4. En particular, este resultado proporciona una manera sencilla de comprobar el signo del discriminante de los cuerpos ciclotómicos.

El corolario siguiente da cuenta de las redes que nos serán más útiles; concretamente, ya hemos visto que el anillo $\mathcal{O}_K$ de los enteros de K es un $\mathbb{Z}$-submódulo libre de rango n de K. Lo mismo le sucede a todo ideal $\mathfrak{a} \subseteq \mathcal{O}_K$; es claro que es un $\mathbb{Z}$-submódulo sin torsión de $\mathcal{O}_K$ y que es finitamente generado, ya que $\mathbb{Z}$ es noetheriano y $\mathcal{O}_K$ es finitamente generado; por tanto, es un grupo abeliano libre de rango $\leq n$; puesto que para todo $a \in \mathfrak{a}$ no nulo se satisface la inclusión $a\mathcal{O}_K \subseteq \mathfrak{a}$ y $a\mathcal{O}_K \simeq \mathcal{O}_K$ como grupos abelianos, $\mathfrak{a}$ contiene un grupo abeliano libre de rango n y, en consecuencia, $\mathfrak{a}$ es un grupo abeliano libre de rango n.

Corolario 4.3.5. *Sean $\mathcal{O}_K$ el anillo de los enteros de un cuerpo de números K de grado $[K : \mathbb{Q}] = n$, $\mathfrak{a} \subseteq \mathcal{O}_K$ un ideal no nulo de $\mathcal{O}_K$ y Δ el discriminante de una $\mathbb{Z}$-base de $\mathcal{O}_K$. Entonces, $\sigma(\mathcal{O}_K)$ y $\sigma(\mathfrak{a})$ son redes de $\mathbb{R}^n$ y sus mallas son dadas por las fórmulas:*

$$\mu(\sigma(\mathcal{O}_K)) = 2^{-r_2}|\Delta|^{1/2}, \text{ y}$$
$$\mu(\sigma(\mathfrak{a})) = 2^{-r_2}|\Delta|^{1/2}\mathcal{N}(\mathfrak{a}),$$

donde $\mathcal{N}(\mathfrak{a})$, la norma absoluta de $\mathfrak{a}$, es el cardinal del anillo finito $\mathcal{O}_K/\mathfrak{a}$.

Demostración: La cuestión relativa al anillo $\mathcal{O}_K$ es inmediata a partir de la proposición anterior. En efecto, si $\{e_1, \ldots, e_n\}$ es una $\mathbb{Z}$-base de $\mathcal{O}_K$, el discriminante $\Delta(\mathcal{O}_K/\mathbb{Z})$ es el ideal generado por el cuadrado del determinante de la matriz $(\sigma_i(e_j))$, de manera que la malla de la red solamente tiene en cuenta el valor absoluto de la raíz cuadrada del discriminante.

Por otro lado, la diferencia al considerar un ideal no nulo $\mathfrak{a}$ de $\mathcal{O}_K$ está en el hecho que $\mathfrak{a}$ es un subgrupo abeliano de $\mathcal{O}_K$ de índice $\mathcal{N}(\mathfrak{a})$. Puesto que la inmersión canónica es un morfismo inyectivo de anillos, esto implica que $\sigma(\mathfrak{a})$ es un subgrupo de índice $\mathcal{N}(\mathfrak{a})$ de $\sigma(\mathcal{O}_K)$; en consecuencia, podemos obtener un dominio fundamental para $\sigma(\mathfrak{a})$ haciendo la reunión disjunta de $\mathcal{N}(\mathfrak{a})$ transladados de un dominio fundamental para $\sigma(\mathcal{O}_K)$. Ello hace que la malla de $\sigma(\mathfrak{a})$ sea $\mathcal{N}(\mathfrak{a})$ veces la malla de $\sigma(\mathcal{O}_K)$; esto acaba la demostración. □

4.4. Finitud del grupo de clases de ideales

El grupo de clases de ideales de un anillo de Dedekind no es, en general, un grupo finito. Uno de los teoremas más importantes en el estudio de la teoría algebraica de números algebraicos es el que asegura esta finitud en el caso de los anillos de los enteros de los cuerpos de números. El objetivo de esta sección es establecer este teorema. Conviene comenzar por la demostración del resuldado siguiente.

Proposición 4.4.1. (La cota de Minkowski) *Sean K un cuerpo de números, $A := \mathcal{O}_K$ su anillo de enteros, $n := [K : \mathbb{Q}]$ el grado, r_1 el número de inmersiones reales de K, r_2 el número de pares de inmersiones complejas conjugadas no reales de K, Δ el discriminante absoluto de la extensión $A|\mathbb{Z}$; es decir, el generador positivo del ideal discriminante $\Delta(A|\mathbb{Z})$, y $\mathfrak{a} \subseteq A$ un ideal no nulo. Entonces, existe un elemento $a \in \mathfrak{a}$, $a \neq 0$, tal que su norma satisface la desigualdad*

$$|\mathrm{N}_{K|\mathbb{Q}}(a)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |\Delta|^{1/2} \mathcal{N}(\mathfrak{a}).$$

Demostración: Consideremos la inmersión canónica σ de K en $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Para todo número real positivo ε, el conjunto $X_\varepsilon \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ formado por los elementos $(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2})$ tales que $\sum_{i=1}^{r_1} |x_i| + 2\sum_{j=1}^{r_2} |z_j| \leq \varepsilon$ es compacto, convexo y simétrico respecto al origen; por tanto, es medible Lebesgue. El cálculo de su medida da

Lema 4.4.2. $\mu(X_\varepsilon) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{\varepsilon^n}{n!}$.

Demostración: El conjunto X_ε no solamente depende de ε, sino que también depende de las constantes r_1 y r_2 tales que $r_1 + 2r_2 = n$. Pongamos $m(r_1, r_2, \varepsilon) := \mu(X_\varepsilon)$. Calcularemos esta medida por inducción sobre las constantes r_1 y r_2. Claramente, $m(1, 0, \varepsilon) = 2\varepsilon$ y $m(0, 1, \varepsilon) = \dfrac{\pi\varepsilon^2}{4}$ ya que, en el primer caso, el conjunto es un segmento y, en el segundo, el conjunto es un círculo. El paso de r_1 a $r_1 + 1$ se puede hacer de la manera siguiente: X_ε es ahora un subconjunto de $\mathbb{R}^{r_1+1} \times \mathbb{C}^{r_2}$ y nos podemos fijar en el componente real de subíndice $r_1 + 1$; la medida $m(r_1 + 1, r_2, \varepsilon)$ se puede calcular, integrando "por rebanadas", como la integral

$$\int_{-\varepsilon}^{\varepsilon} m(r_1, r_2, \varepsilon - |x|)dx.$$

Por hipótesis de inducción, $m(r_1, r_2, \varepsilon - |x|) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{(\varepsilon - x)^{r_1+2r_2}}{(r_1+2r_2)!}$ que, llevado a la integral, da el valor $m(r_1, r_2, \varepsilon) = 2^{r_1+1}\left(\frac{\pi}{2}\right)^{r_2}\frac{\varepsilon^{r_1+1+2r_2}}{(r_1+1+2r_2)!}$, como había que ver. El paso de r_2 a r_2+1 se hace de manera parecida integrando sobre el disco $|z| \leq \varepsilon/2$; concretamente, hay que calcular la integral

$$\int_{|z|\leq\varepsilon/2} m(r_1, r_2, \varepsilon - 2|z|)d\mu(z),$$

donde $d\mu(z)$ denota la medida de Lebesgue de $\mathbb{C}$. Si hacemos el cambio de variables habitual a coordenadas polares, $z = \rho e^{i\theta}$, resulta que $d\mu(z) = \rho d\rho d\theta$ y hay que calcular la integral doble

$$\begin{aligned} m(r_1, r_2+1, \varepsilon) &= \int_0^{\varepsilon/2}\int_0^{2\pi} 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{(\varepsilon-2\rho)^{r_1+2r_2}}{(r_1+2r_2)!}\rho d\rho d\theta \\ &= 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{2\pi}{(r_1+2r_2)!}\int_0^{\varepsilon/2}(\varepsilon-2\rho)^{r_1+2r_2}\rho d\rho \\ &= 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2+1}\frac{\varepsilon^{r_1+2r_2+2}}{(r_1+2r_2+2)!}, \end{aligned}$$

después de calcular la última integral por partes. Esto acaba el cálculo de la medida del conjunto X_ε. □

A continuación, dado el ideal $\mathfrak{a}$, podemos elegir ε de manera que

$$\varepsilon^n = \left(\frac{4}{\pi}\right)^{r_2} n!|\Delta|^{1/2}\mathcal{N}(\mathfrak{a}),$$

donde Δ es el discriminante absoluto de la extensión $A|\mathbb{Z}$. Esto nos permite asegurar que la medida de X_ε es exactamente $\mu(X_\varepsilon) = 2^n\mu(\sigma(\mathfrak{a}))$. En virtud del teorema de Minkowski, existe un elemento no nulo $a \in \mathfrak{a}$ tal que $\sigma(a) \in X_\varepsilon$; el cálculo de la norma de a da $|\mathrm{N}_{K/\mathbb{Q}}(a)| = \prod_{i=1}^{r_1}|\sigma_i(a)|\prod_{j=1}^{r_2}|\sigma_{r_1+j}(a)|^2$ y la desigualdad de la media geométrica que

$$|\mathrm{N}_{K/\mathbb{Q}}(a)| \leq \left(\frac{1}{n}\sum_{i=1}^{r_1}|\sigma_i(a)| + \frac{2}{n}\sum_{j=1}^{r_2}|\sigma_{r_1+j}(a)|\right)^n,$$

que admite $\dfrac{\varepsilon^n}{n^n}$ como cota superior. El resuldado se deduce del hecho que $n = r_1 + 2r_2$. □

Corolario 4.4.3. *Con las mismas notaciones que en la proposición anterior, toda clase de ideales de A contiene un representante entero $\mathfrak{a}$ tal que su norma absoluta satisface la desigualdad*

$$\mathcal{N}(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |\Delta|^{1/2}.$$

Demostración: Puesto que toda clase de ideales contiene un representante entero, podemos tomar un representante entero $\mathfrak{b}$ de la clase inversa de la dada. Sea $a \in \mathfrak{b}$ un elemento para el cual se satisface la desigualdad de la proposición anterior. Puesto que $a \in \mathfrak{b}$, el ideal $\mathfrak{a} := a\mathfrak{b}^{-1}$ es entero y satisface el enunciado, ya que $\mathcal{N}(aA) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$. □

El resuldado principal que queremos demostrar en esta sección es el teorema de finitud del grupo de clases de ideales de los anillos de los enteros de los cuerpos de números.

Teorema 4.4.4. (Dirichlet) *Sea A el anillo de los enteros de un cuerpo de números K. Entonces, el grupo de clases de ideales del anillo A es finito.*

Demostración: Apliquemos la cota de Minkowski; toda clase de ideales contiene un ideal entero no nulo de norma acotada por una constante que sólo depende del cuerpo. Pero, para todo entero m, el conjunto de los ideales enteros no nulos $\mathfrak{a} \subseteq A$ tales que $\mathcal{N}(\mathfrak{a}) = m$ es un conjunto finito; en efecto, de $\#A/\mathfrak{a} = m$ se deduce inmediatamente que $m \in \mathfrak{a}$, de manera que $\mathfrak{a}$ divide el ideal mA. Así, de ideales de norma acotada sólo hay un número finito y, en consecuencia, sólo hay un número finito de clases de ideales. □

4.5. Teoremas de finitud

Una consecuencia importante de los resuldados de la sección anterior es el siguiente.

Teorema 4.5.1. (Hermite-Minkowski) *Sean $K \neq \mathbb{Q}$ un cuerpo de números, A el anillo de los enteros de K y Δ el generador positivo del ideal discriminante $\Delta(A|\mathbb{Z})$. Entonces, $\Delta > 1$. En particular, existe algún número primo p que ramifica en K.*

DEMOSTRACIÓN: La demostración de este teorema se puede hacer cómodamente a partir del resuldado siguiente.

Corolario 4.5.2. *Sea $n := [K : \mathbb{Q}]$ el grado de K. Entonces,*

$$\Delta \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}.$$

En particular, el cociente $\dfrac{n}{\log(\Delta)}$ está acotado superiormente por una constante independiente del cuerpo $K \neq \mathbb{Q}$.

DEMOSTRACIÓN: Puesto que para todo ideal entero no nulo $\mathfrak{a}$ es $\mathcal{N}(\mathfrak{a}) \geq 1$, el corolario 4.4.3 nos permite escribir la desigualdad $|\Delta|^{1/2} \geq \left(\frac{\pi}{4}\right)^{r_2} \frac{n^n}{n!}$; pero $\pi < 4$ y $2r_2 \leq n$, de manera que $|\Delta| \geq u_n := \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2}$. Ahora bien, la sucesión de término general u_n satisface las propiedades siguientes: $u_2 = \pi^2/4$ y $u_{n+1} \geq 3\pi u_n/4$, ya que el cociente u_{n+1}/u_n es la expresión $\frac{\pi}{4}\left(1 + \frac{1}{n}\right)^{2n}$, que está acotada inferiormente por $3\pi/4$ en virtud de la fórmula del binomio; por tanto, se obtiene la desigualdad $u_n \geq u_2\left(\frac{3\pi}{4}\right)^{n-2}$ que da la que queríamos demostrar.

Por otro lado, si tomamos logaritmos, obtendremos la cota uniforme del cociente $\dfrac{n}{\log|\Delta|}$. □

Ahora, la demostración del teorema de Hermite-Minkowski es inmediata si tenemos en cuenta que, para $n \geq 2$ es $\left(\frac{\pi}{3}\right)\left(\frac{3\pi}{4}\right)^{n-1} \geq \left(\frac{\pi}{3}\right)\left(\frac{3\pi}{4}\right) > 1$. □

Observación 4.5.3. Este resultado dista mucho de ser general. En efecto, veremos que hay cuerpos de números que tienen extensiones finitas (incluso abelianas) que son no ramificadas en todos los primos de su anillo de enteros. A pesar de todo, cualquier cuerpo de números tiene sólo un número finito de extensiones abelianas no ramificadas en todos los ideales primos de su anillo de enteros.

El resultado siguiente da información sobre la cantidad de cuerpos de números "pequeños" que pueden ramificar sólo en un conjunto dado de números primos.

Teorema 4.5.4. (Hermite) *Sea $D \in \mathbb{N}$ un número entero positivo cualquiera. El conjunto formado por los cuerpos de números que tienen discriminante absoluto acotado por D es un conjunto finito; es decir, si Δ_K denota el generador positivo del ideal discriminante de un cuerpo de números, entonces es $\Delta_K > D$ salvo, quizás, para un número finito de cuerpos de números K.*

Demostración: El corolario que hemos utilizado en la demostración del teorema de Hermite-Minkowski nos permite asegurar que el grado de un cuerpo de números está acotado superiormente por el logaritmo de una potencia fija de su discriminante; por tanto, es suficiente demostrar que el conjunto de los cuerpos de números que tienen grado y discriminante dados es un conjunto finito. Además, para n dado, sólo hay un número finito de pares de números naturales r_1, r_2 tales que $n = r_1 + 2r_2$; por tanto, podemos suponer, también, que r_1, r_2 son fijos. Supongamos, pues, que $n = r_1 + 2r_2$, y que K es un cuerpo de números de grado n y discriminante absoluto Δ que tiene exactamente r_1 inmersiones reales. Hay que ver que sólo podemos elegir K entre un número finito de cuerpos.

Consideremos el subconjunto $X \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ definido de la manera siguiente:

(a) si $r_1 > 0$, tomemos X como el producto de los discos de centro en el origen y radio $1/2$ en cada componente complejo no real, del intervalo $-1/2 \leq x \leq 1/2$ en cada factor $\mathbb{R}$ salvo el primero, y el intervalo centrado en el origen de longitud $2^n \left(\frac{2}{\pi}\right)^{r_2} |\Delta|^{1/2}$ en el primer componente;

(b) si $r_1 = 0$, tomemos X como el producto de discos de radio $1/2$ centrados en el origen de cada factor $\mathbb{C}$ salvo el primero, y el rectángulo definido por las condiciones $|z - \overline{z}| \leq 2^{n-1}\pi \left(\frac{2}{\pi}\right)^{r_2} |\Delta|^{1/2}$, $|z + \overline{z}| \leq 1/2$, en el primer componente $\mathbb{C}$.

En cualquier caso, el conjunto X es un producto de intervalos y discos cerrados, de manera que es compacto, simétrico respecto al origen y convexo, y el cálculo de la su medida da inmediatamente $\mu(X) = 2^{n-r_2}|\Delta|^{1/2} = 2^n \mu(\sigma(\mathcal{O}_K))$. Por tanto, existe un número entero no nulo $a \in A$ tal que

$\sigma(a) \in X$ Veamos que a es un elemento primitivo de la extensión $K|\mathbb{Q}$.

En efecto, los conjugados de a son los números $\sigma_i(a)$ y $\overline{\sigma_i(a)}$, contados tantas veces como el grado de la extensión $K|\mathbb{Q}(a)$. Para $i > 1$, los números $\sigma_i(a)$ y $\overline{\sigma_i(a)}$ son de módulo menor que 1 por construcción de X. Si tenemos en cuenta la fórmula $\mathrm{N}_{K/\mathbb{Q}}(a) = \prod_{i=1}^{n} \sigma_i(a)$, y tomamos módulos, observaremos que $|\sigma_1(a)| > 1$, ya que la norma de a es un número entero por ser a un entero algebraico no nulo. En particular, si $r_1 > 0$ obtenemos que $\sigma_1(a)$ es diferente de todos los demás conjugados, de manera que el grado de la extensión $K|\mathbb{Q}(a)$ es 1 y a es un elemento primitivo de K. Si $r_1 = 0$, el mismo argumento demuestra que es $|\sigma(a)| = |\overline{\sigma_1(a)}| > 1$, de manera que $\sigma_1(a)$ es diferente de todos los $\sigma_i(a)$ y de los $\overline{\sigma_i(a)}$ para $i > 1$; pero, por construcción de X, la parte real de $\sigma_1(a)$ tiene módulo menor o igual que $1/4$, de manera que $\sigma_1(a)$ no puede ser real ya que es de módulo > 1; en particular, también $\sigma_1(a)$ es diferente de $\overline{\sigma_1(a)}$ y, en consecuencia, a es un elemento primitivo de K.

Ahora ya estamos, ya que los conjugados de a son números complejos (o reales) acotados por construcción del conjunto X; por tanto, también son acotados los valores de los polinomios simétricos elementales construídos con estos números; puesto que estos valores son los coeficientes del polinomio $\mathrm{Irr}(a, \mathbb{Q})$, y estos coeficientes son números enteros, ya que a es un entero algebraico, sólo hay un número finito de posibilidades para el polinomio $\mathrm{Irr}(a, \mathbb{Q})$ y, en consecuencia, un número finito de posibilidades para el elemento primitivo a. □

Observación 4.5.5. Este resultado admite otras formulaciones interesantes. Por ejemplo, si fijamos un conjunto finito de números primos y un número entero $N > 1$, entonces el conjunto formado por los cuerpos de números de grado $n \leq N$ que no ramifican fuera de los primos fijados es, también, un conjunto finito.

4.6. El teorema de Dirichlet de las unidades

En esta sección se trata de hacer el estudio del grupo de las unidades de los cuerpos de números. Así como para el estudio de la estructura lineal ha ido bien la inmersión canónica de los cuerpos de números en $\mathbb{R}^n$, ahora conven-

drá hacer algo parecido; deberemos considerar alguna inmersión que tenga en cuenta la multiplicatividad del grupo. Eso se hace "tomando logaritmos".

Sean K un cuerpo de números, A el anillo de los enteros de K, r_1 el número de inmersiones reales de K, r_2 el de pares de inmersiones complejas conjugadas no reales, $n = r_1 + 2r_2$ el grado de la extensión, y designemos por U el grupo de los elementos inversibles de A.

La inmersión canónica de K en $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ es un morfismo de anillos; conviene tomar logaritmos en cada componente a fin de obtener un morfismo de grupos. Concretamente, consideremos la aplicación $\log : K^* \longrightarrow \mathbb{R}^{r_1+r_2}$ definida por la fórmula

$$u \mapsto (\log|\sigma_1(u)|, \ldots, \log|\sigma_{r_1}(u)|, \log|\sigma_{r_1+1}(u)|, \ldots, \log|\sigma_{r_1+r_2}(u)|).$$

Igual que en el caso de la inmersión canónica, nos olvidamos de la mitad de los componentes complejos no reales; ello es debido al hecho que si consideráse mos también los otros r_2 componentes no obtendríamos componentes diferentes de los anteriores, ya que el módulo de un número complejo coincide con el de su conjugado. Por otra parte, para $u, v \in K^*$ se satisface la igualdad $\log(uv) = \log(u) + \log(v)$, de manera que log es un morfismo del grupo multiplicativo K^* en el grupo aditivo $\mathbb{R}^{r_1+r_2}$. Se llama la inmersión logarítmica de K, en contraposición a la inmersión canónica. El teorema que se trata de probar es el siguiente.

Teorema 4.6.1. (Dirichlet) *El grupo de las unidades U de A es el producto del grupo de las raíces de la unidad de K, que es un grupo finito, por un grupo abeliano libre de rango $r := r_1 + r_2 - 1$.*

Demostración: Haremos la demostración de este teorema en diversas etapas. Acabamos de ver que la inmersión logarítmica es un morfismo de grupos.

Lema 4.6.2. *Sea H el hiperplano de $\mathbb{R}^{r+1}$ formado por los elementos $(x_1, \ldots, x_{r+1})$ tales que $x_1 + \cdots + x_{r_1} + 2x_{r_1+1} + \cdots + 2x_{r_1+r_2} = 0$. Entonces, $\log(U) \subseteq H$.*

Demostración: Puesto que las unidades de A son elementos de A de norma ± 1, resulta que para sus imágenes se satisface que

$$\sum_{i=1}^{r_1} \log|\sigma_i(u)| + 2\sum_{j=1}^{r_2} \log|\sigma_{r_1+j}(u)| = \sum_{i=1}^{r_1+2r_2} \log|\sigma_i(u)| = \log|\mathrm{N}_{K/\mathbb{Q}}(u)| = 0,$$

de manera que la imagen de U está incluída en H. □

Lema 4.6.3. *Para todo subconjunto compacto $X \subseteq \mathbb{R}^{r+1}$ el conjunto de los elementos $u \in U$ tales que $\log(u) \in X$ es finito. En particular, $\log(U)$ es un subgrupo discreto de $\mathbb{R}^{r+1}$.*

DEMOSTRACIÓN: Sea $X \subseteq \mathbb{R}^{r+1}$ un subconjunto compacto. Entonces, X es un conjunto acotado, de manera que si $u \in U$ es tal que $\log(u) \in X$, entonces los conjugados de u están acotados y la cota sólo depende de X. Por tanto, los polinomios simétricos elementales de los conjugados de u están acotados; es decir, los coeficientes (enteros) del polinomio irreducible de u sobre $\mathbb{Q}$ están acotados. Esto implica que sólo hay un número finito de posibilidades para estos polinomos y, en consecuencia, un número finito de elementos $u \in U$ tales que $\log(u) \in X$. □

Corolario 4.6.4. *El núcleo del morfismo $\log : U \longrightarrow \mathbb{R}^{r+1}$ está formado exactamente por las raíces de la unidad de K.*

DEMOSTRACIÓN: El núcleo de log es la antiimagen del compacto $\{0\}$, de manera que es un subgrupo finito de U. Por tanto, es un subgrupo finito del grupo multiplicativo de un cuerpo y, en consecuencia, es cíclico y formado por raíces de la unidad. Por otro lado, todas las raíces de la unidad de K son elementos inversibles de A y son números complejos de módulo 1; puesto que sus conjugados también son raíces de la unidad, también son de módulo 1 y, en consecuencia, pertenecen al núcleo de log. □

Puesto que H es isomorfo a $\mathbb{R}^r$ y $\log(U)$ es un subgrupo discreto de $\mathbb{R}^{r+1}$, hemos demostrado que el cociente de U por el subgrupo de las raíces de la unidad de K es (isomorfo a) un subgrupo discreto de $\mathbb{R}^r$; por tanto, un grupo abeliano libre de rango $\leq r$. En particular, si $r = 0$ ya hemos acabado la demostración y podemos suponer que $r \geq 1$. Sólo resta ver que la imagen $\log(U)$ es de rango exactamente r. Para ello, es suficiente demostrar que $\log(U)$ contiene r vectores linealmente independientes. Y, para ver este hecho, basta comprobar que si ω es una forma lineal no nula definida en H, entonces existe un elemento $u \in U$ tal que $\omega(\log(u)) \neq 0$; es decir, que $\log(U)$ no está incluído en el núcleo de ninguna forma lineal no nula. Por tanto, el resto de la prueba consiste en buscar esta unidad u.

Puesto que H es de dimensión r y ninguno de los componentes de H es nulo, la proyección de $\mathbb{R}^{r+1}$ en los primeros r componentes da un isomorfismo de H en $\mathbb{R}^r$; por tanto, una forma lineal en H se puede pensar definida por una fórmula $\omega(x_1, \ldots, x_r) = c_1x_1 + \cdots + c_rx_r$, donde $c_1, \ldots, c_r \in \mathbb{R}$ son

constantes que sólo dependen de la forma ω y no del punto $(x_1, \ldots, x_r) \in \mathbb{R}^r$. En particular, podemos pensar $\omega(\log(u))$ como la forma ω aplicada a los primeros r componentes de $\log(u)$.

Lema 4.6.5. *Sean $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2}$ números reales estrictamente positivos. Pongamos $\varepsilon_{r_1+r_2+j} := \varepsilon_{r_1+j}$ para $1 \leq j \leq r_2$ y supongamos que*

$$\varepsilon := \prod_{i=1}^{n} \varepsilon_i = \left(\frac{2}{\pi}\right)^{r_2} |\Delta|^{1/2}.$$

Entonces, existe $a \in A$, $a \neq 0$, tal que para todos los componentes $\log|\sigma_i(a)|$ se satisfacen las desigualdades

$$0 \leq \log(\varepsilon_i) - \log|\sigma_i(a)| \leq \log(\varepsilon)$$

y, además, $|\mathrm{N}_{K|\mathbb{Q}}(a)| \leq \varepsilon$.

Demostración: Consideremos el subconjunto $X \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ formado por los elementos $(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2})$ tales que $|x_i| \leq \varepsilon_i$, $1 \leq i \leq r_1$, y $|z_j| \leq \varepsilon_{r_1+j}$, $1 \leq j \leq r_2$. Claramente, X es un subconjunto compacto, convexo y simétrico respecto al origen, y su medida de Lebesgue es exactamente

$$\begin{aligned}
\mu(X) &= \prod_{i=1}^{r_1}(2\varepsilon_i) \prod_{j=1}^{r_2}(\pi\varepsilon_{r_1+j}^2) \\
&= 2^{r_1}\pi^{r_2}\varepsilon \\
&= 2^{r_1+r_2}|\Delta|^{1/2} \\
&= 2^{n-r_2}|\Delta|^{1/2} \\
&= 2^n\mu(\sigma(A)).
\end{aligned}$$

Por tanto, el teorema de Minkowski nos permite asegurar la existencia de un elemento no nulo $a \in A$ tal que $\sigma(a) \in X$; esto es decir que para los componentes $\sigma_i(a)$ se satisfacen las desigualdades $|\sigma_i(a)| \leq \varepsilon_i$, para $1 \leq i \leq n$. Puesto que a es un número entero algebraico no nulo, es $|\mathrm{N}_{K|\mathbb{Q}}(a)| \geq 1$, de manera que obtenemos las desigualdades

$$1 \leq |\mathrm{N}_{K/\mathbb{Q}}(a)| = \prod_{i=1}^{n} |\sigma_i(a)| \leq \varepsilon.$$

Por otro lado, si nos fijamos en un índice i obtenemos

$$|\sigma_i(a)|^{-1} = |\mathrm{N}_{K/\mathbb{Q}}(a)|^{-1} \prod_{j\neq i} |\sigma_j(a)| \leq |\mathrm{N}_{K/\mathbb{Q}}(a)|^{-1} \prod_{j\neq i} \varepsilon_j \leq \prod_{j\neq i} \varepsilon_j = \varepsilon\varepsilon_i^{-1}$$

que da $\varepsilon_i\varepsilon^{-1} \leq |\sigma_i(a)| \leq \varepsilon_i$ para $1 \leq i \leq n$. Tomando logaritmos, se obtienen las desigualdades deseadas. □

Aplicaremos este resultado de la manera siguiente: dada la forma lineal ω definida por la ecuación $\omega(x_1, \ldots, x_r) = c_1x_1 + \cdots + c_rx_r$, elegimos números reales positivos ε_i para los que se satisfagan las condiciones del lema y sea M un número real fijo tal que $M > \sum_{i=1}^{r} |c_i| \log(\varepsilon)$. Entonces, para el elemento $a \in A$ que proporciona el lema se satisface la desigualdad

$$\left| \omega(\log(a)) - \sum_{i=1}^{r} c_i \log(\varepsilon_i) \right| < M.$$

El final de la demostración consiste en tomar una sucesión de elementos $a_h \in A$ para los que se satisfagan las condiciones anteriores y alguna más. Concretamente, para todo número natural $h > 0$ podemos elegir los elementos ε_i, $1 \leq i \leq r$, del lema de manera que se satisfaga la igualdad $\sum_{i=1}^{r} c_i \log(\varepsilon_i) = 2hM$, ya que algún coeficiente c_i es no nulo; después, elegimos ε_{r+1} de manera que se satisfaga la condición del lema. El elemento a_h que nos proporciona el lema satisface la desigualdad $|\omega(\log(a_h)) - 2hM| < M$; es decir,

$$(2h-1)M < \omega(\log(a_h)) < (2h+1)M.$$

Esto produce una sucesión de números enteros algebraicos $a_h \in A$ para los que se satisfacen las desigualdades anteriores y, además, tienen la norma acotada por ε. En consecuencia, los ideales a_hA son todos de norma $\mathcal{N}(aA) \leq \varepsilon$; por tanto, son en número finito. Esto implica que existen números naturales diferentes h, k tales que $a_hA = a_kA$ y, por tanto, existe una unidad $u \in U$ tal que $a_k = ua_h$. Si suponemos que $h < k$, obtenemos las desigualdades $\omega(\log(a_h)) < (2h+1)M \leq (2k-1)M < \omega(\log(a_k))$, de manera que $\omega(\log(u)) = \omega(\log(a_k)) - \omega(\log(a_h)) > 0$, y obtenemos la unidad $u \in U$ tal que $\omega(\log(u)) \neq 0$ que deseábamos encontrar. □

Definición 4.6.6. Se llama sistema de unidades fundamentales de un cuerpo de números K todo conjunto $\{u_1, \ldots, u_r\}$ de unidades del anillo de los enteros de K tal que toda unidad $u \in U$ se expresa de manera única en la forma

$$u = \eta u_1^{m_1} \cdots u_r^{m_r},$$

donde η es una raíz de la unidad del cuerpo K y los m_i son números enteros.

Con esta definición, el teorema de Dirichlet de las unidades admite la formulación equivalente siguiente.

Corolario 4.6.7. *Todo cuerpo de números admite un sistema de unidades fundamentales* $u_1, \ldots, u_r \in U$. □

4.7. Unidades de los cuerpos cuadráticos

Un caso sencillo de cálculo de las unidades de un cuerpo de números es el caso de los cuerpos cuadráticos. Supongamos, pues, que D es un número entero libre de cuadrados y pongamos $K := \mathbb{Q}(\sqrt{D})$, A el anillo de los enteros de K, U el grupo de las unidades de A, y $W \subseteq U$ el grupo de las raíces de la unidad de K.

Proposición 4.7.1. *Si* $D < 0$*, es decir, si* K *es un cuerpo cuadrático imaginario, entonces* $U = W$*. Además,*

$$W = \begin{cases} \{1, -1\}, & \text{si } D \neq -1, -3, \\ \{1, -1, i, -i\}, & \text{si } D = -1, \\ \{1, -1, \rho, -\rho, \rho^2, -\rho^2\}, & \text{si } D = -3, \end{cases}$$

donde $\rho := \dfrac{-1 + \sqrt{-3}}{2}$ *es una raíz cúbica primitiva de la unidad.*

Demostración: En efecto, en el caso $D < 0$ no hay ninguna inmersión real de K, de manera que el rango del grupo de las unidades es $r = r_1 + r_2 - 1 = 0$, ya que de $2 = r_1 + 2r_2$ y $r_1 = 0$ se dedude que $r_2 = 1$ y, por tanto, que $r = 0$. En consecuencia, el grupo de las unidades no tiene parte libre y coincide con el grupo de las raíces de la unidad del cuerpo K.

Por otro lado, si K contiene una raíz n-ésima de la unidad ζ, entonces el grado de K es divisible por $\varphi(n)$, ya que $\mathbb{Q}(\zeta) \subseteq K$; las únicas posibilidades para que K sea de grado 2 son que $\varphi(n) = 1$ o $\varphi(n) = 2$; y eso sólo sucede para los valores $n \in \{1, 2, 3, 4, 6\}$. Puesto que para todo cuerpo de números es $\{\pm 1\} \subseteq W$, la proposición es inmediata. □

El caso $D > 0$ es más complicado; en efecto, en ese caso las dos inmersiones de K son reales, de manera que $r_1 = 2$, $r_2 = 0$ y el rango del grupo de las unidades de K es $r = 1$. Puesto que las únicas raíces de la unidad de $\mathbb{R}$ son ± 1, el grupo de las raíces de la unidad de K es $W = \{1, -1\}$. Esto significa que existe una unidad $u \in U$ tal que todas las unidades de A son los números $\pm u^m$, con $m \in \mathbb{Z}$. Además, podemos elegir u de manera que sea $u > 1$. En efecto, puesto que $-1 \in W$, podemos suponer que $u > 0$ y después, puesto que $u \in U$ equivale a $u^{-1} \in U$ y exactamente uno de los dos elementos es > 1, salvo que $u = 1$, podemos cambiar, si conviene, el generador u por u^{-1}. En definitiva, hemos probado el resultado siguiente.

Proposición 4.7.2. *Supongamos que $D > 0$. Entonces, el grupo W de las raíces de la unidad de $\mathbb{Q}(\sqrt{D})$ es el grupo $\{1, -1\}$. Existe una unidad $u > 1$ del anillo de los enteros de $\mathbb{Q}(\sqrt{D})$ tal que todas las demás unidades se escriben de manera única en la forma $\pm u^m$ con $m \in \mathbb{Z}$.* □

Esta unidad $u > 1$ es una unidad fundamental de $\mathbb{Q}(\sqrt{D})$; se llama **la** unidad fundamental; es la menor de todas las unidades $v > 1$ del anillo de los enteros de $\mathbb{Q}(\sqrt{D})$. Existen algoritmos para calcular esta unidad de manera explícita.

Proposición 4.7.3. *Sea $D > 0$ un número entero libre de cuadrados. La unidad fundamental de $\mathbb{Q}(\sqrt{D})$ es el número $u := \dfrac{a + b\sqrt{D}}{2}$ donde b es el menor número entero positivo tal que uno de los dos números $Db^2 \pm 4$ es un cuadrado y $a > 0$ es el número entero positivo tal que $a^2 = Db^2 \pm 4$ donde se toma el signo menos si las dos ecuaciones tienen solución. Además, la norma de la unidad fundamental u es exactamente el signo que hace que la ecuación tenga solución, y -1 si ambas tienen.*

Demostración: Pongamos $K := \mathbb{Q}(\sqrt{D})$ y sea $u > 1$ una unidad de A; podemos escribir u en la forma $u = \dfrac{a + b\sqrt{D}}{2}$ donde a, b son números enteros de la misma paridad y ambos pares si $D \not\equiv 1 \pmod 4$. Puesto que $D > 1$,

si $a, b > 0$, entonces $u > 1$; si $a, b < 0$, entonces $u < -1$; y si $ab < 0$, entonces $|u| < 1$. Por tanto, las unidades $u > 1$ de K se escriben en la forma $u = \dfrac{a + b\sqrt{D}}{2}$ con $a, b > 0$ números enteros de la misma paridad, ambos pares si $D \not\equiv 1 \pmod 4$. En particular, el cálculo de la norma de u da $\mathrm{N}(u) = \dfrac{a + b\sqrt{D}}{2} \dfrac{a - b\sqrt{D}}{2} = \dfrac{a^2 - Db^2}{4} = \pm 1$, de manera que la ecuación $a^2 - Db^2 = \pm 4$ tiene solución, con el signo igual a la norma de la unidad u. Además, la menor unidad $u > 1$ ha de ser la unidad fundamental. Resta ver, pues, que la menor unidad $u > 1$ se obtiene al tomar los menores números enteros $a, b > 0$ que satisfacen la ecuación $a^2 - Db^2 = \pm 4$.

Observemos que podemos escribir la ecuación en la forma $a^2 \mp 4 = Db^2$, de manera que al hacer b menor y mantener el signo también a es menor; además, si para algún valor de b les dos ecuaciones tienen solución, el menor valor de a corresponde a la ecuación con signo $+1$ y hay una unidad de norma -1; en este caso, la unidad fundamental es de norma -1, ya que la norma es multiplicativa. Finalmente, un sencillo cálculo demuestra que si tenemos números enteros $a, b, a', b' > 0$ tales que $b' < b$ y que $a^2 + 4 = Db^2$ y $a'^2 - 4 = Db'^2$, entonces también ha de ser $a' < a$. Así, el resultado queda demostrado completamente, ya que a valores menores de b corresponden valores menores de a. □

4.8. Ejemplos

El objetivo de esta sección es dar algunos ejemplos de aplicación de técnicas de este capítulo y de los anteriores al cálculo explícito de algunos invariantes de los anillos de los enteros de algunos cuerpos de números.

Ejemplo 4.8.1. Consideremos, en primer lugar, el cuerpo $K := \mathbb{Q}(\sqrt{-23})$.

Puesto que $-23 \equiv 1 \pmod 4$, el anillo de los enteros es el anillo $A := \mathbb{Z}[\omega]$ donde $2\omega = 1 + \sqrt{-23}$ y el discriminante absoluto es $\Delta = -23$. En particular, el único primo que ramifica es 23. Por otro lado, puesto que K es un cuerpo cuadrático imaginario, obtenemos inmediatamente el valor de las constantes $r_1 = 0$ y $r_2 = 1$; en particular, el grupo de las unidades de A es el grupo $\{1, -1\}$. Vamos a estudiar el grupo de clases de ideales, $H := \mathrm{Cl}(A)$.

La cota de Minkowski, $\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|\Delta|^{1/2}$, admite la acotación siguiente:

$$\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|\Delta|^{1/2} = \left(\frac{4}{\pi}\right) \frac{2!}{2^2}\sqrt{23} < \left(\frac{2}{\pi}\right)\sqrt{25} = \frac{10}{\pi} < 4,$$

de manera que cada clase de ideales tiene un representante de norma ≤ 3. En consecuencia, el grupo de clases de ideales, H, está generado por todos los ideales primos de A de norma 2 y de norma 3, si hay; estos ideales han de dividir los ideales $2A$ y $3A$. Pero las leyes de descomposición de los primos en los cuerpos cuadráticos nos permiten asegurar en seguida que $2A = \mathfrak{p}_2\mathfrak{p}_2'$ y que $3A = \mathfrak{p}_3\mathfrak{p}_3'$, donde $\mathfrak{p}_2$, $\mathfrak{p}_2'$, $\mathfrak{p}_3$, y $\mathfrak{p}_3'$ son ideales primos diferentes de A de grado residual 1, ya que $-23 \equiv 1 \pmod 8$ y $\left(\frac{-23}{3}\right) = 1$. Además, puesto que los productos $\mathfrak{p}_2\mathfrak{p}_2'$ y $\mathfrak{p}_3\mathfrak{p}_3'$ son ideales principales, el grupo de clases de ideales de A está generado por las clases de los ideales $\mathfrak{p}_2$ y $\mathfrak{p}_3$.

Por otro lado, $\mathrm{N}\left(\frac{1+\sqrt{-23}}{2}\right) = 6$, de manera que el ideal generado por este elemento es producto de un ideal de norma 2 y uno de norma 3; en consecuencia, o bien el producto $\mathfrak{p}_2\mathfrak{p}_3$ es principal, o bien lo es el producto $\mathfrak{p}_2\mathfrak{p}_3'$, de manera que el grupo de clases de ideales de A está generado por la clase del ideal $\mathfrak{p}_2$. Este ideal no puede ser principal, ya que para todo elemento $\alpha := \frac{a+b\sqrt{-23}}{2} \in A$ es $\mathrm{N}(\alpha) = \frac{a^2+23b^2}{4} \neq 2$; además, el elemento $\alpha := \frac{3+\sqrt{-23}}{2}$ es de norma $\mathrm{N}(\alpha) = 8$, de manera que el ideal αA es el producto de tres ideales primos de norma 2; esto da las posibilidades $\alpha A = \mathfrak{p}_2^3$, o bien $\alpha A = 2\mathfrak{p}_2$. La última es imposible, ya que lo contrario nos diría que $\mathfrak{p}_2$ es el ideal generado por el elemento $\frac{3+\sqrt{-23}}{4}$, que no es entero algebraico. Por tanto, el cubo del ideal $\mathfrak{p}_2$ es un ideal principal y, por tanto, el grupo de clases de ideales de A es un grupo cíclico de 3 elementos.

Ejemplo 4.8.2. El cuerpo $K := \mathbb{Q}(\theta)$, donde θ es una raíz del polinomio $f(X) := X^3 + X + 1$.

En primer lugar, el polinomio $f(X)$ es irreducible, ya que lo es módulo 2; por otro lado, puesto que todos los coeficientes no nulos son positivos, $f(X)$ no tiene ninguna raíz real positiva, y la regla de Descartes nos permite asegurar que tiene exactamente una raíz negativa; por tanto, $f(X)$ sólo tiene

una raíz real. En consecuencia, $r_1 = r_2 = r = 1$. El discriminante de las potencias de θ es exactameente -31. En efecto, de $\theta^3 + \theta + 1 = 0$ se obtiene sucesivamente que

$$\begin{gathered}\theta(\theta^2+1) = -1\\ \theta = \frac{-1}{\theta^2+1},\\ \theta^2 = \frac{1}{\theta^4+2\theta^2+1},\\ (\theta^2)^3 + 2(\theta^2)^2 + (\theta^2) - 1 = 0\end{gathered}$$

que, juntamente con las fórmulas

$$\begin{aligned}\theta^3 &= -\theta - 1, \text{ i}\\ \theta^4 &= -\theta^2 - \theta,\end{aligned}$$

permite obtener las trazas

$$\mathrm{T}(\theta) = 0, \quad \mathrm{T}(\theta^2) = -2, \quad \mathrm{T}(\theta^3) = -3, \quad \mathrm{T}(\theta^4) = 2,$$

de manera que el discriminante de las potencias de θ es el determinante

$$\begin{vmatrix} 3 & 0 & -2\\ 0 & -2 & -3\\ -2 & -3 & 2\end{vmatrix} = -31.$$

De aquí ya podemos deducir dos cosas importantes; por un lado, que el discriminante de la extensión es -31, ya que -31 es libre de cuadrados; por otro, puesto que el discriminante de las potencias de θ coincide con el discriminante del cuerpo, las potencias de θ han de formar una $\mathbb{Z}$-base del anillo de los enteros de K. En particular, el anillo de los enteros es $A := \mathbb{Z}[\theta]$. Por otro lado, podemos acotar la constante de Minkowski por $\dfrac{4}{\pi}\dfrac{3!}{3^3}\sqrt{31} < 2$, de manera que el anillo A es principal.

Las raíces de la unidad de K son exactamente 1 y -1, ya que podemos pensar que θ es real, de manera que $K \subseteq \mathbb{R}$. Resta calcular una unidad fundamental. Ya hemos visto más arriba que $\eta := 1 + \theta^2$ es una unidad de A; y es claro que es $\eta > 1$. Veremos que η es una unidad fundamental de A. Para ello, demostraremos un resuldado previo.

Lema 4.8.3. *Sea $K \subseteq \mathbb{R}$ un cuerpo cúbico tal que $r_1 = r_2 = 1$. Entonces, toda unidad positiva $u \in A$ es de norma 1 y, si $u > 1$ y Δ designa el*

discriminante absoluto de la extensión $A|\mathbb{Z}$, se satisface la desigualdad $|\Delta| < 4u^3 + 24$.

DEMOSTRACIÓN: La norma de una unidad y la norma de su inversa coinciden, de manera que podemos suponer que $u > 1$; puesto que $u \neq \pm 1$, u es un elemento primitivo de la extensión $K|\mathbb{Q}$, y su polinomio irreducible es de la forma $(X-u)(X-\alpha)(X-\overline{\alpha})$, donde $\alpha \in \mathbb{C}$ y $\overline{\alpha}$ designa el número complejo conjugado de α; ello es debido al hecho que $r_2 = 1$. La norma de u es, pues, el producto de los conjugados de u, de manera que es $\mathrm{N}(u) = u\alpha\overline{\alpha} > 0$; por tanto, ha de ser $\mathrm{N}(u) = 1$.

Puesto que el discriminante de las potencias de u es un múltiplo del discriminante de la extensión $A|\mathbb{Z}$, es suficiente demostrar que $|D(1, u, u^2)| \leq 4u^3 + 24$. Podemos escribir $u = r^2$, $\alpha = r^{-1}e^{ix}$, $\overline{\alpha} = r^{-1}e^{-ix}$, con $r, x \in \mathbb{R}$, $r > 0$, de manera que el discriminante de las potencias de u se puede calcular por la fórmula

$$\begin{aligned} D(1, u, u^2) &= \begin{vmatrix} 1 & 1 & 1 \\ r^2 & r^{-1}e^{ix} & r^{-1}e^{-ix} \\ r^4 & r^{-2}e^{2ix} & r^{-2}e^{-2ix} \end{vmatrix}^2 \\ &= \left(e^{2ix} - e^{-2ix} - (e^{ix} - e^{-ix})(r^3 + r^{-3})\right)^2 \\ &= \left(2i\sin(2x) - 2i(r^3 + r^{-3})\sin(x)\right)^2 \\ &= -4sin^2(x)\left(2\cos(x) - (r^3 + r^{-3})\right)^2. \end{aligned}$$

Consideremos la función $g : \mathbb{R} \longrightarrow \mathbb{R}$ definida por la fórmula

$$g(x) := 4sin(x)\,(cos(x) - a)\,,$$

donde $2a := r^3 + r^{-3}$. El valor absoluto del discriminante $D(1, u, u^2)$ es el cuadrado del valor en x de la función g, luego es suficiente demostrar que $|g(x)|^2 < 4u^3 + 24$ para todo número real x. Puesto que la función g es continua y periódica, tiene máximo y mínimo y el máximo de $|g(x)|^2$ es el cuadrado de uno de los extremos de g; por tanto, es suficiente probar que el cuadrado de estos extremos es menor que $4u^3 + 24$. Sea $x_0 \in \mathbb{R}$ un punto donde $g(x)$ tenga un extremo; entonces, la derivada de g ha de anularse en x_0, de manera que $\cos(x_0)$ ha de ser una raíz del polinomio $2t^2 - at - 1$; pongamos $t_0 := \cos(x_0)$. La igualdad $at_0 = 2t_0^2 - 1$ aplicada sucesivamente

da la cadena de igualdades

$$\begin{aligned}|g(x_0)|^2 &= 16\sin^2(x_0)\left(\cos(x_0)-a\right)^2\\ &= 16(1-t_0^2)\left(t_0^2-2at_0+a^2\right)\\ &= 16(1-t_0^2)\left(a^2+2-3t_0^2\right)\\ &= 16\left(a^2-t_0^4-t_0^2+1\right)\\ &= 4r^6+4r^{-6}+8-16t_0^4-16t_0^2+16\\ &= 4u^3+24+4\left(r^{-6}-4t_0^4-4t_0^2\right),\end{aligned}$$

de manera que es suficiente ver que $r^{-6} < 4t_0^2$. Ahora bien, si $t_0 \geq 0$, entonces $4t_0^2 = 2+2at_0 \geq 2$ y, puesto que $r^{-6} = u^{-3} < 1$, la desigualdad queda probada. Finalmente, si $t_0 < 0$, entonces $t_0 < \dfrac{-1}{2r^3} < 0$, ya que el valor del polinomio $2t^2 - at - 1$ en $\dfrac{-1}{2r^3}$ es $\dfrac{3(1-r^6)}{4r^6} < 0$ y el valor en t_0 es cero; al elevar al cuadrado obtenemos la desigualdad que deseábamos. □

Con este resuldado a nuestra disposición, podemos proceder a demostrar que η es la menor de las unidades de A que es > 1 y, por tanto, una unidad fundamental.

En primer lugar, se satisface la igualdad $\eta^3 = \eta^2 + 1$ (comprovación inmediata), que se obtiene al calcular el polinomio $\mathrm{Irr}(\eta, \mathbb{Q})$. Si aplicamos el lema, puesto que el discriminante absoluto de K es -31, toda unidad $u > 1$ de A y, en particular, la unidad fundamental $u > 1$ de A, satisface la desigualdad $31 < 4u^3 + 24$; es decir, $u^3 > 7/4$. Ahora bien, si fuese $\eta \geq 7/4$, obtendríamos la desigualdad contradictoria

$$\frac{7}{4} \leq \eta = \frac{\eta^3}{\eta^2} = 1 + \frac{1}{\eta^2} \leq 1 + \frac{16}{49} = \frac{65}{49} < \frac{70}{49} < \frac{70}{40} = \frac{7}{4}.$$

Por tanto, η no puede ser divisible por el cubo de u. Pero η es una potencia de u; si vemos que η no es el cuadrado de una unidad positiva, habremos obtenido $\eta = u$ y, en consecuencia, η es una unidad fundamental de A.

Puesto que $\eta = -\theta^{-1}$, obtenemos que $A = \mathbb{Z}[\eta]$, de manera que si η fuese un cuadrado, la ecuación $\eta = (a + b\eta + c\eta^2)^2$ habría de tener soluciones enteras a, b, c. Pero los números $1, \eta, \eta^2$ son $\mathbb{Q}$-linealmente independientes y la ecuación anterior se puede escribir en la forma

$$\eta = (a^2 + c^2 + 2bc) + (c^2 + 2ab)\eta + (c^2 + 2bc + 2ac + b^2)\eta^2,$$

si tenemos en cuenta la expresión de las potencias de η que se obtienen a partir de la igualdad $\eta^3 = \eta^2 + 1$; por tanto, se han de satisfacer las igualdades

$$\begin{aligned} a^2 + c^2 + 2bc &= 0 \\ c^2 + 2ab &= 1 \\ c^2 + 2bc + 2ac + b^2 &= 0. \end{aligned}$$

Esto nos enseña que c es impar y, después, que a y b también son impares; entonces, la reducción módulo 4 de la ecuación $c^2 + 2ab = 1$ lleva a contradicción. Por tanto, η no es el cuadrado de ningún elemento de A y esto acaba la prueba.

Capítulo 5

Ramificación superior

Este capítulo se dedica a hacer el estudio de los grupos de ramificación superior; antes, pero, haremos el estudio del diferente y de su relación con el discriminante y la ramificación. El estudio de estos conceptos será básico para la prueba del teorema de Kronecker-Weber que haremos.

5.1. El diferente

Hemos visto en el capítulo tercero que el discriminante es un invariante asociado a una extensión entera finita y separable de anillos de Dedekind y que determina los ideales primos del anillo base que ramifican en la extensión. En esta sección se trata de definir un invariante del anillo extensión que nos de la información de manera más precisa: concretamente, el diferente de la extensión da cuenta de los ideales del anillo extensión que son ramificados sobre su base.

Comencemos por considerar, igual que en el caso del discriminante, un dominio íntegramente cerrado A, su cuerpo de fracciones K, una extensión finita y separable $L|K$, y la clausura entera B de A en L o, más generalmente, un subanillo B de L tal que la extensión $B|A$ sea entera y que L sea el cuerpo de fracciones de B.

Definición 5.1.1. El codiferente $\mathcal{C}(B|A)$ es el subconjunto de L formado por todos los elementos $b \in L$ tales que $\mathrm{T}_{L|K}(bB) \subseteq A$.

Puesto que la extensión $B|A$ es entera y A es íntegramente cerrado, la traza de los elementos de B está en A, de manera que se satisface la inclusión $B \subseteq \mathcal{C}(B|A)$; por otro lado, es inmediato de la definición que $\mathcal{C}(B|A)$ es un B-submódulo de L; incluso más, es el mayor de los B-submódulos $M \subseteq L$ tales que $\mathrm{T}_{L|K}(M) \subseteq A$.

Proposición 5.1.2. *Con las notaciones e hipótesis precedentes, el ideal codiferente $\mathcal{C}(B|A)$ es un ideal fraccionario de B.*

Demostración: Si demostramos que $\mathcal{C}(B|A)$ está incluído en un B-submódulo finitamente generado de L, tomando un denominador común $b \in B$ de estos generadores obtendremos la inclusión $b\mathcal{C}(B|A) \subseteq B$ y habremos acabado. Por tanto, basta ver que $\mathcal{C}(B|A)$ está incluído en un B-submódulo finitamente generado de L y es suficiente demostrar que $\mathcal{C}(B|A)$ está incluído en un A-submódulo finitamente generado de L.

El cálculo que sigue ya ha sido usado anteriormente. Consideremos una K-base de L, $\{e_1, \ldots, e_n\}$, formada por elementos $e_i \in B$. Para todo elemento $b \in \mathcal{C}(B|A)$ podemos escribir una igualdad $b = a_1e_1 + \cdots + a_ne_n$ con los elementos a_i en K; si D denota el discriminante $D := D(e_1, \ldots, e_n) \in A$, puesto que la traza de los elementos be_j está en A por definición de $\mathcal{C}(B|A)$, obtenemos las relaciones $Da_i \in A$, de manera que $\mathcal{C}(B|A) \subseteq \bigoplus_{i=1}^{n} D^{-1}Ae_i$, que es un A-submódulo finitamente generado de L. $\square$

Observación 5.1.3. En el caso que B es la clausura entera de A en L, disponemos de una caracterización interesante del ideal codiferente. Puesto que la forma bilineal traza $\mathrm{T}_{L|K} : L \times L \longrightarrow K$ es no degenerada (recordemos que la extensión $L|K$ es separable por definición), la aplicación

$$L \xrightarrow{\varphi} \mathrm{Hom}_K(L, K), \qquad b \mapsto \mathrm{T}_{L|K}(b \cdot *),$$

es un isomorfismo de K-espacios vectoriales. Por definición del codiferente, la imagen de un elemento $b \in \mathcal{C}(B|A)$ define, por restricción, una aplicación A-lineal de B en A. De esta manera, obtenemos una aplicación A-lineal inyectiva $\mathcal{C}(B|A) \xrightarrow{\varphi} \mathrm{Hom}_A(B, A)$. Por otro lado, puesto que B es la clausura entera de A en L y A es íntegramente cerrado, todo elemento de L se puede escribir en la forma b/s, donde $b \in B$ y $s \in A$, $s \neq 0$. Eso permite extender de manera única toda aplicación A-lineal $B \xrightarrow{f} A$ a una aplicación K-lineal

$L \xrightarrow{f} K$; el isomorfismo $L \xrightarrow{\varphi} \mathrm{Hom}_K(L,K)$ nos proporciona un elemento $b \in L$ tal que $f = \mathrm{T}_{L|K}(b \cdot *)$; y este elemento b pertenece a $\mathcal{C}(B|A)$ por definición del codiferente. Por tanto, la aplicación $\mathcal{C}(B|A) \xrightarrow{\varphi} \mathrm{Hom}_A(B,A)$ es un isomorfismo.

En definitiva, hemos probado el resultado siguiente.

Proposición 5.1.4. *Supongamos que B es la clausura entera de A en L. Entonces, la aplicación*

$$\mathcal{C}(B|A) \xrightarrow{\varphi} \mathrm{Hom}_A(B,A), \qquad b \mapsto \mathrm{T}_{L|K}(b \cdot *),$$

es un isomorfismo de A-módulos. □

Definición 5.1.5. Se llama diferente de la extensión $B|A$ el ideal fraccionario inverso del ideal codiferente; es decir, el ideal $(B : \mathcal{C}(B|A))$. Se designa a menudo con el símbolo $\mathcal{D}(B|A)$, aunque también se usan los $\mathcal{D}_{B|A}$, o $\mathcal{D}(L|K)$ o $\mathcal{D}_{L|K}$ cuando no hay peligro de confusión sobre cuáles son los anillos que se tratan.

El diferente es un ideal entero no nulo de B, ya que $B \subseteq \mathcal{C}(B|A)$. En el caso que B sea un anillo de Dedekind, se satisface la igualdad $\mathcal{C}(B|A)\mathcal{D}(B|A) = B$, y el ideal diferente admite una factorización en ideales primos $\mathcal{D}(B|A) = \prod_{\mathfrak{P}} \mathfrak{P}^{d(\mathfrak{P})}$, donde los exponentes $d(\mathfrak{P})$ son números enteros no negativos, nulos para todos los ideales primos no nulos de B salvo, quizás, de los de un conjunto finito. El exponente $d(\mathfrak{P})$ se llama el exponente diferencial de $\mathfrak{P}$ sobre A. Una caracterización útil del diferente (y del codiferente) es la siguiente.

Proposición 5.1.6. *Sean A un anillo de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión finita y separable, B la clausura entera de A en L, y $\mathfrak{a} \subseteq K$, $\mathfrak{b} \subseteq L$, ideales fraccionarios no nulos. Las propiedades siguientes son equivalentes:*

(i) $\mathrm{T}_{L|K}(\mathfrak{b}) \subseteq \mathfrak{a}$;

(ii) $\mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathcal{C}(B|A)$;

(iii) $\mathfrak{b} \subseteq \mathfrak{a}\mathcal{C}(B|A)$;

(iii') $\mathcal{D}(B|A)\mathfrak{b} \subseteq \mathfrak{a}B$.

DEMOSTRACIÓN: La propiedad (i) equivale a la propiedad $\mathfrak{a}^{-1}\mathrm{T}_{L|K}(\mathfrak{b}) \subseteq A$, que lo es a $\mathrm{T}_{L|K}(\mathfrak{a}^{-1}\mathfrak{b}) \subseteq A$, en virtud de la linealidad de la traza; pero esta es (ii) por definición de codiferente. Las otras dos se obtienen por multiplicación. □

Igual que en el caso del discriminante, y para anillos de Dedekind, el ideal diferente se comporta bien por localización.

Proposición 5.1.7. *Sean A un anillo de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión finita y separable, B la clausura entera de A en L y S un subconjunto multiplicativamente cerrado de A. Entonces,*

$$\mathcal{D}(S^{-1}B|S^{-1}A) = S^{-1}\mathcal{D}(B|A).$$

DEMOSTRACIÓN: Claramente, es suficiente demostrar la propiedad para los ideales codiferente y invertir. Sea $b \in \mathcal{C}(B|A)$; entonces, $\mathrm{T}_{L|K}(bB) \subseteq A$ y, por la K-linealidad de la aplicación $\mathrm{T}_{L|K}$, también $\mathrm{T}_{L|K}(bS^{-1}B) \subseteq S^{-1}A$; por tanto, $b \in \mathcal{C}(S^{-1}B|S^{-1}A)$ y puesto que $\mathcal{C}(S^{-1}B|S^{-1}A)$ es un $S^{-1}B$-submódulo de L, también $S^{-1}\mathcal{C}(B|A) \subseteq \mathcal{C}(S^{-1}B|S^{-1}A)$. Resta ver la otra inclusión.

Sea $b \in \mathcal{C}(S^{-1}B|S^{-1}A)$; eso es decir que $\mathrm{T}_{L|K}(bS^{-1}B) \subseteq S^{-1}A$ y, por tanto, que $\mathrm{T}_{L|K}(bB) \subseteq S^{-1}A$. Puesto que la extensión $L|K$ es separable, A es noetheriano e íntegramente cerrado, y B es la clausura entera de A en L, ya sabemos que B es un A-módulo finitamente generado; de aquí se deduce que podemos elegir un elemento $s \in S$ tal que $\mathrm{T}_{L|K}(sbB) = s\mathrm{T}_{L|K}(bB) \subseteq A$, de manera que $sb \in \mathcal{C}(B|A)$ y, por tanto, $b \in S^{-1}\mathcal{C}(B|A)$. Esto acaba la prueba. □

Igual que para el caso de los índices de ramificación, los grados residuales, o las trazas y las normas, una de las fórmulas más útiles para los diferentes es la fórmula de la transitividtad para cadenas de extensiones.

Proposición 5.1.8. *Supongamos que A es un anillo de Dedekind, K su cuerpo de fracciones, $K'|K$ y $L|K'$ extensiones finitas y separables, y A' y B las clausuras enteras de A en K' y L, respectivamente. Entonces, se satisface la igualdad de ideales de B*

$$\mathcal{D}(B|A) = \mathcal{D}(B|A')\mathcal{D}(A'|A).$$

Demostración: A partir de la definición y usando la transitividad de las trazas, para todo ideal fraccionario no nulo $\mathfrak{b} \subseteq L$ podemos escribir la sucesión de propiedades equivalentes:

$$\begin{aligned}
\mathfrak{b} \subseteq \mathcal{C}(B|A') &\iff \mathrm{T}_{L|K'}(\mathfrak{b}) \subseteq A' \\
&\iff \mathcal{C}(A'|A)\mathrm{T}_{L|K'}(\mathfrak{b}) \subseteq \mathcal{C}(A'|A) \\
&\iff \mathrm{T}_{K'|K}(\mathcal{C}(A'|A)\mathrm{T}_{L|K'}(\mathfrak{b})) \subseteq A \\
&\iff \mathrm{T}_{K'|K}(\mathrm{T}_{L|K'}(\mathcal{C}(A'|A)\mathfrak{b})) \subseteq A \\
&\iff \mathrm{T}_{L|K}(\mathcal{C}(A'|A)\mathfrak{b}) \subseteq A \\
&\iff \mathcal{C}(A'|A)\mathfrak{b} \subseteq \mathcal{C}(B|A) \\
&\iff \mathfrak{b} \subseteq \mathcal{D}(A'|A)\mathcal{C}(B|A),
\end{aligned}$$

de manera que $\mathcal{C}(B|A') = \mathcal{D}(A'|A)\mathcal{C}(B|A)$; solamente resta pasar los codiferentes al otro lado de la igualdad. □

5.2. Relación entre el diferente y el discriminante

De la misma manera que el ideal discriminante se puede calcular a partir de fórmulas más o menos sencillas, también el diferente se puede calcular efectivamente; como mínimo, en algunos casos sencillos.

Definición 5.2.1. Sea A' un dominio de integridad y sea B la clausura entera de A' (en su cuerpo de fracciones). Se llama conductor de B en A' el conjunto de los elementos $b \in A'$ tales que $bB \subseteq A'$; es un ideal a la vez de A' y de B; de hecho, es el mayor de los ideales de A' que es un ideal de B. En particular, condición necesaria y suficiente para que sea $A' = B$ es que el conductor sea A'.

Proposición 5.2.2. *Supongamos que A es un dominio noetheriano íntegramente cerrado, K su cuerpo de fracciones, $L|K$ una extensión finita y separable, y B la clausura entera de A en L. Sea $b \in B$ un elemento primitivo de la extensión $L|K$ y pongamos $A' := A[b]$ y $f(X) := \mathrm{Irr}(b, K)$ el polinomio minimal de b sobre K. Entonces:*

(i) $f(X) \in A[X]$.

(ii) El codiferente $\mathcal{C}(A'|A)$ *es el ideal fraccionario de* A' *generado por* $\dfrac{1}{f'(b)}$.

(iii) Si A *es un anillo de Dedekind y* $\mathfrak{C}(B|A')$ *denota el conductor de* B *en* A'*, se satisface la igualdad de ideales* $f'(b)B = \mathfrak{C}(B|A')\mathcal{D}(B|A)$.

Demostración: El primer apartado es inmediato, ya que A es íntegramente cerrado y b es entero sobre A.

Para la segunda parte, observemos que, dado un elemento cualquiera $y \in L$, podemos escribir $y = g(b)$ para un cierto polinomio $g(X) \in K[X]$ de grado $\leq n-1$, ya que $\{1, b, b^2, \ldots, b^{n-1}\}$ es una K-base de L; si $b = b_1, b_2, \ldots, b_n$ son los diferentes conjugados de b sobre K, entonces podemos escribir

$$g(X) = \sum_{i=1}^{n} g(b_i) \frac{f(X)}{f'(b_i)(X - b_i)}, \tag{5.2.1}$$

ya que ambos son polinomios de grado $\leq n-1$ que toman el mismo valor en todos los b_i; y, si definimos la traza de un polinomio coeficiente a coeficiente, la expresión anterior se puede escribir en la forma

$$g(X) = \mathrm{T}_{L|K}\left(\frac{yf(X)}{f'(b)(X-b)}\right).$$

Esto nos permite demostrar en seguida la inclusión $\mathcal{C}(A'|A) \subseteq f'(b)^{-1}A'$. En efecto; si $x \in \mathcal{C}(A'|A)$, para $y := xf'(b)$ se satisface que $g(X) \in A[X]$, ya que los polinomios $\dfrac{f(X)}{X-b}$ tienen coeficientes en A' y $x \in \mathcal{C}(A'|A)$; por tanto, $xf'(b) = g(b) \in A'$, como queríamos ver.

Para probar la otra inclusión es suficiente demostrar que se satisfacen las igualdades $\mathrm{T}_{L|K}(b^{n-1}/f'(b)) = 1$, y $\mathrm{T}_{L|K}(b^j/f'(b)) = 0$, para $0 \leq j \leq n-2$, ya que estos elementos forman una A-base del A'-módulo $f'(b)^{-1}A'$. Pero si aplicamos la fórmula 5.2.1 de más arriba al elemento $y := b^{j+1}$, $0 \leq j \leq n-2$, obtenemos la identidad

$$X^{j+1} = \sum_{i=1}^{n} b_i^{j+1} \frac{f(X)}{f'(b_i)(X - b_i)}$$

que, haciendo $X = 0$ y teniendo en cuenta que $f(0) \neq 0$, da las fórmulas deseadas para $0 \leq j \leq n-2$; por otro lado, si $y = b^n$, las expresiones $(*)$ dan

$$X^n - f(X) = \sum_{i=1}^{n} b_i^n \frac{f(X)}{f'(b_i)(X - b_i)}.$$

Si hacemos $X = 0$ y cambiamos el signo, obtenemos las identidades

$$f(0) = f(0)\sum_{i=1}^{n} \frac{b_i^{n-1}}{f'(b_i)} = f(0)\mathrm{T}_{L|K}\left(\frac{b^{n-1}}{f'(b)}\right),$$

de manera que, al dividir por $f(0)$, obtenemos la igualdad que faltaba. Esto acaba la demostración del apartado (ii).

Para ver la última afirmación, observemos que $\mathcal{C}(B|A) \subseteq \mathcal{C}(A'|A) \subseteq f'(b)^{-1}A'$, en virtud de (ii) y de la definición del codiferente; por tanto, tenemos la inclusión $f'(b)\mathcal{C}(B|A) \subseteq A'$ y $f'(b)\mathcal{C}(B|A)$ es un ideal de B, de manera que, en virtud de la definición de conductor, $f'(b)\mathcal{C}(B|A) \subseteq \mathfrak{C}(B|A')$; es decir, la inclusión $f'(b)B \subseteq \mathfrak{C}(B|A')\mathcal{D}(B|A)$.

Resta ver la otra inclusión. Dados elementos arbitrarios $x \in \mathfrak{C}(B|A')$ y $y \in B$, el producto xy es un elemento de A'; por tanto, podemos aplicar el apartado (ii) y obtenemos que $\mathrm{T}(xy/f'(b)) \in A$, en virtud de la definición de codiferente. Por tanto, $x/f'(b) \in \mathcal{C}(B|A)$, de manera que $x\mathcal{D}(B|A) \subseteq f'(b)B$; esto acaba la prueba, ya que x es arbitrario. □

Corolario 5.2.3. *Con las mismas notaciones e hipótesis, si A es un anillo de Dedekind, entonces condición necesaria y suficiente para que $\mathcal{D}(B|A) = f'(b)B$ es que sea $B = A[b]$.* □

El resultado siguiente nos enseña la relación entre el diferente y la ramificación; en particular, nos enseña que el diferente es un invariante más fino que el discriminante respecto a este problema.

Proposición 5.2.4. *Sean A un anillo de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión finita y separable, B la clausura entera de A en L, $\mathfrak{P} \subseteq B$ un ideal primo no nulo de B, $\mathfrak{p} := \mathfrak{P} \cap A$ su contracción a A, $d(\mathfrak{P})$ el exponente diferencial de $\mathfrak{P}$ sobre A, y $e(\mathfrak{P}|\mathfrak{p})$ el índice de ramificación de $\mathfrak{P}$ sobre $\mathfrak{p}$. Entonces, $d(\mathfrak{P}) \geq e(\mathfrak{P}|\mathfrak{p}) - 1$. Además, para que se satisfaga la igualdad es condición necesaria y suficiente que*

(i) el índice de ramificación $e(\mathfrak{P}|\mathfrak{p})$ no sea divisible por la característica residual de $A/\mathfrak{p}$; y

(ii) la extensión residual $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ sea separable.

Demostración: Sea $S := A - \mathfrak{p}$; la proposición 5.1.7 nos enseña que el exponente diferencial de $\mathfrak{P}$ coincide con el exponente diferencial del ideal primo

$S^{-1}\mathfrak{P} \subseteq S^{-1}B$ sobre su contracción $S^{-1}\mathfrak{p} \subseteq S^{-1}A$; pero ahora tenemos la ventaja que $S^{-1}A$ es local principal, que $S^{-1}B$ es principal, y que los únicos ideales primos no nulos de $S^{-1}B$ son los ideales primos que contraen al único ideal primo no nulo de $S^{-1}A$. Además, tenemos igualdades $e(S^{-1}\mathfrak{P}_i|S^{-1}\mathfrak{p}) = e(\mathfrak{P}_i|\mathfrak{p})$ entre los índices de ramificación. Por tanto, podemos suponer de entrada que A es local principal; sean π un generador de este ideal, $\mathfrak{P} = \mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ los ideales primos de B que contraen a $\mathfrak{p}$, $e_i := e(\mathfrak{P}_i|\mathfrak{p})$ y $d_i := d(\mathfrak{P}_i)$ los exponentes diferenciales. Puesto que el codiferente de la extensión $B|A$ es el ideal fraccionario $\mathcal{C}(B|A) = \prod_{i=1}^{g} \mathfrak{P}_i^{-d_i}$, la desigualdad quedará probada si vemos que $\prod_{i=1}^{g} \mathfrak{P}_i^{1-e_i} \subseteq \mathcal{C}(B|A)$.

Sea $b \in \prod_{i=1}^{g} \mathfrak{P}_i^{1-e_i}$; entonces, $b\pi \in \prod_{i=1}^{g} \mathfrak{P}_i$, ya que $\pi B = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$; en consecuencia, para todo índice i se satisface la relación $b\pi \in \mathfrak{P}_i$. De aquí podemos concluir que $\mathrm{T}_{L|K}(b\pi) \in \mathfrak{p}$; en efecto, el hecho que $b\pi$ sea un elemento de todos los ideales primos que dividen $\mathfrak{p}$ se mantiene si cambiamos L por su clausura normal sobre K, de manera que todos los conjugados de $b\pi$ también están en todos los ideales primos que dividen $\mathfrak{p}$; por tanto, su traza, que es un elemento de A, pertenece a todos los ideales primos que dividen $\mathfrak{p}$; es decir, para todo índice i, se satisface la relación $\mathrm{T}_{L|K}(b\pi) \in A \cap \mathfrak{P}_i = \mathfrak{p} = \pi A$. En consecuencia, $\pi \mathrm{T}_{L|K}(b) = \mathrm{T}_{L|K}(b\pi) \in \pi A$ o, equivalentemente, $\mathrm{T}_{L|K}(b) \in A$; por tanto, y puesto que $\prod_{i=1}^{g} \mathfrak{P}_i^{1-e_i}$ es un B-submódulo de L, obtenemos que $b \in \mathcal{C}(B|A)$, como queríamos probar.

A continuación, se trata de caracterizar la igualdad. Para ello, supongamos que se satisfacen las propiedades (i) y (ii). Puesto que la extensión residual $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ es separable, existe un elemento $\overline{b} \in B/\mathfrak{P}$ tal que su traza es no nula en $A/\mathfrak{p}$; teniendo en cuenta que los ideales $\mathfrak{P}_i^{e_i}$, $i \geq 2$, son comaximales, podemos tomar un representante $b \in B$ de $\overline{b}$ de manera que para todo índice $i \geq 2$ sea $b \in \mathfrak{P}_i^{e_i}$. La clase residual módulo $\mathfrak{p}$ de la traza $\mathrm{T}_{L|K}(b)$ es $e_1 \mathrm{T}_{(B/\mathfrak{P})|(A/\mathfrak{p})}(\overline{b})$ (recordemos que la matriz de la multiplicación por $\overline{b}$ en el cociente $B/\mathfrak{p}B \simeq \prod_{i=1}^{g} B/\mathfrak{P}_i^{e_i}$ se puede tomar formada por cajas en la diagonal, e_i veces la caja de la multiplicación por la clase residual de b

en $B/\mathfrak{P}_i$ para cada índice i). La elección de $\overline{b}$ y la hipótesis (i) nos permiten asegurar que esta clase residual es no nula; por tanto, $\mathrm{T}_{L|K}(b) \notin \mathfrak{p} = \pi A$, de manera que $\mathrm{T}_{L|K}(b/\pi) = \pi^{-1}\mathrm{T}_{L|K}(b) \notin A$; en cambio, $b/\pi \in \mathfrak{P}_1^{-e_1}$, ya que $\pi \in \mathfrak{P}_1^{e_1}$ y $b \in B$. Esto dice que $b/\pi \notin \mathcal{C}(B|A)$, de manera que hemos construído un elemento de $\mathfrak{P}_1^{-e_1}$ que no es de $\mathcal{C}(B|A)$; dicho de otra manera, el exponente de $\mathfrak{P}$ en $\mathcal{C}(B|A)$ ha de ser estrictamente menor que e_1; por tanto, $d_1 = e_1 - 1$.

Recíprocamente, hay que demostrar que si alguna de las hipótesis (i) o (ii) no se satisface, entonces el exponente de $\mathfrak{P}$ en el diferente de la extensión satisface la desigualdad estricta $d_1 > e_1 - 1$. Para ello, tomemos un elemento cualquiera b del ideal fraccionario $\mathfrak{P}_1^{-e_1}\displaystyle\prod_{i\neq 1}\mathfrak{P}_i^{1-e_i}$; entonces, $b\pi \in \mathfrak{P}_i$ para todo índice $i \neq 1$ y la clase residual módulo $\mathfrak{p}$ de la traza $\mathrm{T}_{L|K}(b\pi)$ es el elemento $e_1\mathrm{T}_{(B/\mathfrak{P})|(A/\mathfrak{p})}(\overline{b}\overline{\pi})$, que es cero trivialmente si e_1 es múltiplo de la característica residual, y también si la extensión residual no es separable, ya que, en este caso, la traza es nula. Por tanto, $\pi\mathrm{T}_{L|K}(b) = \mathrm{T}_{L|K}(b\pi) \in \mathfrak{p} = \pi A$ y $\mathrm{T}_{L|K}(b) \in A$; por tanto, y puesto que $\mathfrak{P}_1^{-e_1}\displaystyle\prod_{i\neq 1}\mathfrak{P}_i^{1-e_i}$ es un B-submódulo de L, es $b \in \mathcal{C}(B|A)$, de manera que $\mathfrak{P}_1^{-e_1}\displaystyle\prod_{i\neq 1}\mathfrak{P}_i^{1-e_i} \subseteq \mathcal{C}(B|A)$ y $d_1 \geq e_1$. □

Corolario 5.2.5. *Los ideales primos de B que ramifican son exactamente los que dividen el diferente $\mathcal{D}(B|A)$.* □

Se trata de demostrar, finalmente, que el discriminante es la norma del diferente y de obtener, en consecuencia, una fórmula de transitividad para el discriminante.

Proposición 5.2.6. *Sean A un anillo de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión finita y separable y B la clausura entera de A en L. Entonces, $\Delta(B|A) = \mathrm{N}_{L|K}(\mathcal{D}(B|A))$.*

Demostración: Ejercicio. □

Corolario 5.2.7. *Sean A un anillo de Dedekind, K su cuerpo de fracciones, $K'|K$ y $L|K'$ extensiones finitas y separables, A' la clausura entera de A en K' y B la clausura entera de A (y de A') en L. Entonces,*

$$\Delta(B|A) = \Delta(A'|A)^{[L:K']}\mathrm{N}_{K'|K}(\Delta(B|A')).$$

DEMOSTRACIÓN: Basta tomar normas en la fórmula de transitividad del diferente y tener en cuenta la transitividad de la norma. □

5.3. Grupos de descomposición y de inercia

Ya hemos definido en el capítulo tercero los grupos de descomposición y de inercia. En esta sección se trata de hacer un estudio sistemático de esos grupos; en particular, de sus propiedades generales y de las de los cuerpos de descomposición y de inercia, que también introduciremos. Eso servirá de base para la definición y el estudio de los grupos de ramificación superior.

Sean A un anillo de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión finita, B la clausura entera de A en L, $\mathfrak{P} \subseteq B$ un ideal primo no nulo de B, y $\mathfrak{p} := \mathfrak{P} \cap A$ su contracción a A. Supongamos que la extensión $L|K$ es de Galois y sea $G := \mathrm{Gal}\,(L|K)$. Recordemos que el grupo de descomposición del ideal primo $\mathfrak{P}$ es el grupo $G_{-1}(\mathfrak{P}|\mathfrak{p}) := D(\mathfrak{P}|\mathfrak{p})$ formado por todos los automorfismos $\sigma \in G$ tales que $\sigma(\mathfrak{P}) = \mathfrak{P}$, y que el grupo de inercia de $\mathfrak{P}$ es el grupo $G_0(\mathfrak{P}|\mathfrak{p}) := I(\mathfrak{P}|\mathfrak{p})$ formado por los automorfismos $\sigma \in G_{-1}(\mathfrak{P}|\mathfrak{p})$ que actúan trivialmente en el cociente $B/\mathfrak{P}$; además, disponemos de una sucesión exacta de grupos

$$1 \longrightarrow G_0(\mathfrak{P}|\mathfrak{p}) \longrightarrow G_{-1}(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}\,((B/\mathfrak{P})|(A/\mathfrak{p})) \longrightarrow 1.$$

Comencemos por estudiar el comportamiento de estos grupos en cadenas de extensiones de Galois.

Proposición 5.3.1. *Con las mismas notaciones e hipótesis anteriores, supongamos que $K' \subseteq L$ es un subcuerpo de L que contiene K y sean A' la clausura entera de A en K' y $\mathfrak{P}' := \mathfrak{P} \cap A'$ la contracción de $\mathfrak{P}$ a A'. Entonces, los grupos de descomposición y de inercia de $\mathfrak{P}$ sobre su contracción $\mathfrak{P}'$ se obtienen cortando los grupos sobre $\mathfrak{p}$ con el grupo de Galois $\mathrm{Gal}\,(L|K')$; es decir, $G_i(\mathfrak{P}|\mathfrak{P}') = G_i(\mathfrak{P}|\mathfrak{p}) \cap \mathrm{Gal}\,(L|K')$, para $i = -1, 0$.*

DEMOSTRACIÓN: Es inmediata a partir de las definiciones. □

Si, además, la subextensión $K'|K$ también es de Galois, entonces tiene sentido considerar los grupos $G_i(\mathfrak{P}'|\mathfrak{p})$, $i = -1, 0$.

Proposición 5.3.2. *Supongamos que la extensión $K'|K$ también es de Galois. Entonces, hay un diagrama conmutativo*

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G_0(\mathfrak{P}|\mathfrak{P}') & \longrightarrow & G_0(\mathfrak{P}|\mathfrak{p}) & \longrightarrow & G_0(\mathfrak{P}'|\mathfrak{p}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G_{-1}(\mathfrak{P}|\mathfrak{P}') & \longrightarrow & G_{-1}(\mathfrak{P}|\mathfrak{p}) & \longrightarrow & G_{-1}(\mathfrak{P}'|\mathfrak{p}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{Gal}\left(\overline{L}|\overline{K}'\right) & \longrightarrow & \mathrm{Gal}\left(\overline{L}|\overline{K}\right) & \longrightarrow & \mathrm{Gal}\left(\overline{K}'|\overline{K}\right) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

que tiene las filas y las columnas exactas y donde $\overline{L}$, $\overline{K}$, $\overline{K}'$, designan los cuerpos residuales $B/\mathfrak{P}$, $A/\mathfrak{p}$, y $A'/\mathfrak{P}'$, respectivamente.

Demostración: La exactitud de las columnas es simultánea a la definición de los grupos de inercia (cf. Cap. 3, §5), y la exactitud de la tercera fila es la teoría de Galois finita aplicada a la cadena de extensiones residuales. Por otro lado, la comprobación de la conmutatividad del diagrama es inmediata. Si demostramos la exactitud de la segunda fila, la de la primera es un ejercicio trivial de hacer cuadrar diagramas. Y para ver esta exactitud, es suficiente demostrar la exhaustividad del morfismo $G_{-1}(\mathfrak{P}|\mathfrak{p}) \longrightarrow G_{-1}(\mathfrak{P}'|\mathfrak{p})$, ya que las otras partes de la demostración también son inmediatas a partir de la sucesión exacta

$$1 \longrightarrow \mathrm{Gal}\,(L|K') \longrightarrow \mathrm{Gal}\,(L|K) \longrightarrow \mathrm{Gal}\,(K'|K) \longrightarrow 1$$

que proporciona la teoría de Galois. Además, dado $\sigma' \in D(\mathfrak{P}'|\mathfrak{p})$, la sucesión exacta de la teoría de Galois nos proporciona una antiimagen $\sigma \in \mathrm{Gal}\,(L|K)$ de σ'; el elemento σ puede no pertenecer a $D(\mathfrak{P}|\mathfrak{p})$, pero transforma $\mathfrak{P}$ en un ideal primo $\sigma(\mathfrak{P})$ de B. Puesto que la imagen de σ en $\mathrm{Gal}\,(K'|K)$ deja $\mathfrak{P}'$ invariante, la restricción de $\sigma(\mathfrak{P})$ a A' también es $\mathfrak{P}'$, de manera que $\mathfrak{P}$ y $\sigma(\mathfrak{P})$ son conjugados por $\mathrm{Gal}\,(L|K')$; es decir, existe un elemento $\tau \in \mathrm{Gal}\,(L|K')$ tal que $\tau\sigma(\mathfrak{P}) = \mathfrak{P}$; en particular, obtenemos que $\tau\sigma \in G_{-1}(\mathfrak{P}|\mathfrak{p})$ y su imagen en $\mathrm{Gal}\,(K'|K)$ coincide con la imagen de σ, porque $\tau \in \mathrm{Gal}\,(L|K')$. Por tanto, hemos encontrado una antiimagen de σ en $G_{-1}(\mathfrak{P}|\mathfrak{p})$, como queríamos. □

Observación 5.3.3. A menudo se demuestra este resultado con la hipótesis adicional que la extensión residual $\overline{L}|\overline{K}$ es separable, de manera que, entonces, es de Galois; de hecho, esta hipótesis solamente ha sido usada en la demostración de la proposición cuando hemos hablado de la exactitud de la tercera fila del diagrama. Ahora bien, esta sucesión es exacta sin necesidad de la hipótesis de separabilidad. Para ver este hecho, observemos los siguientes: en primer lugar, para la definición de la sucesión basta que la extensión $\overline{K}'|\overline{K}$ sea normal; en segundo lugar, la exhaustividad del segundo morfismo solamente utiliza la normalidad de la extensión $\overline{L}|\overline{K}$ cuando aseguramos que una $\overline{K}$-inmersión de $\overline{L}$ que extienda un $\overline{K}$-automorfismo dado de $\overline{K}'$ es automáticamente un $\overline{K}$-automorfismo de $\overline{L}$; y, finalmente, el núcleo de este morfismo es exactamente el grupo de Galois $\mathrm{Gal}\left(\overline{L}|\overline{K}'\right)$, sin necesidad de ninguna propiedad de normalidad ni de separabilidad.

5.4. Cuerpos de descomposición y de inercia

Mantengamos las notaciones y las hipótesis de la sección anterior. Escribiremos D, I, para designar los grupos de descomposición y de inercia, respectivamente, del ideal $\mathfrak{P}$ sobre su contracción.

Definición 5.4.1. Los cuerpos fijos de L por los subgrupos $D := G_{-1}(\mathfrak{P}|\mathfrak{p})$, $I := G_0(\mathfrak{P}|\mathfrak{p})$, L^D, L^I, se llaman, respectivamente, el cuerpo de descomposición y el cuerpo de inercia en $\mathfrak{P}$.

De esta manera, obtenemos una sucesión de cuerpos $K \subseteq L^D \subseteq L^I \subseteq L$ tal que las extensiones $L|L^I$, $L|L^D$, y $L^I|L^D$ son extensiones de Galois con grupos respectivos $\mathrm{Gal}\left(L|L^I\right) = I$, $\mathrm{Gal}\left(L|L^D\right) = D$, y $\mathrm{Gal}\left(L^I|L^D\right) \simeq \mathrm{Gal}\left(\overline{L}|\overline{K}\right)$, el grupo de Galois de la extensión residual. En particular, obtenemos los grados de las extensiones: por un lado, si ponemos $e := e(\mathfrak{P}|\mathfrak{p})$ y $f := f(\mathfrak{P}|\mathfrak{p})$, entonces $[L : L^D] = ef = n/g$, ya que $g := g(\mathfrak{p})$ es el índice del grupo de isotropía de la acción de $\mathrm{Gal}\,(L|K)$ en el conjunto de los ideales primos de B que dividen $\mathfrak{p}$; es decir, el índice del grupo de descomposición D; en consecuencia, $[L^D : K] = g$. Por otro lado, el grado $[L^I : L^D]$ es el grado de separabilidad de la extensión residual $\overline{L}|\overline{K}$, ya que es una extensión normal y, por tanto, el orden de su grupo de Galois es el grado de separabilidad; en particular, si la extensión residual $\overline{L}|\overline{K}$ es de característica $p > 0$, y escribimos el grado de separabilidad en la forma $f_s = f_s(\mathfrak{P}|\mathfrak{p})$, obtenemos que el cociente

f/f_s es una cierta potencia p^i de p: el grado de inseparabilidad; con estas notaciones, podemos escribir los grados $[L^I : L^D] = f_s$, y, en consecuencia, $[L : L^I] = ep^i$. Estos grados hacen pensar en si el primo $\mathfrak{P}$ será totalmente ramificado en la extensión $L|L^I$, y si la contracción de $\mathfrak{P}$ al cuerpo L^D es un ideal primo que no descompone en la extensión $L|L^D$. Esto es, efectivamente, de esta manera.

Proposición 5.4.2. *Sean $\mathfrak{P}_I$ y $\mathfrak{P}_D$ las contracciones de $\mathfrak{P}$ a las clausuras enteras B_I, B_D, de A en L^I, L^D, respectivamente. Entonces:*

(i) $\mathfrak{P}$ es el único ideal primo de B que divide $\mathfrak{P}_I$ y $\mathfrak{P}_D$;

(ii) la extensión de $\mathfrak{P}_I$ a B es el ideal $\mathfrak{P}^e$, donde $e := e(\mathfrak{P}|\mathfrak{p})$ es el índice de ramificación de $\mathfrak{P}$ sobre $\mathfrak{p}$, y el grado residual $f(\mathfrak{P}|\mathfrak{P}_I)$ es el grado de inseparabilidad, p^i, de la extensión residual $(B/\mathfrak{P})|(A/\mathfrak{p})$; y

(iii) la extensión de $\mathfrak{P}_D$ a B_I es el ideal $\mathfrak{P}_I$, y el grado residual $f(\mathfrak{P}_I|\mathfrak{P}_D)$ es el grado de separabilidad, f_s, de la extensión residual $(B/\mathfrak{P})|(A/\mathfrak{p})$.

Demostración: El grupo de descomposición $D(\mathfrak{P}|\mathfrak{P}_D)$ coincide con el grupo $D(\mathfrak{P}|\mathfrak{p})$ porque la extensión $L|L^D$ es de Galois de grupo de Galois $D(\mathfrak{P}|\mathfrak{p})$; por tanto, la primera afirmación es inmediata. En particular, las otras dos propiedades son equivalentes. Si ahora aplicamos las dos proposiciones anteriores al cálculo de los grupos de descomposición y de inercia del primo $\mathfrak{P}_I$ en la extensión de Galois $L^I|L^D$, podemos mirar el diagrama conmutativo

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & I(\mathfrak{P}|\mathfrak{P}_I) & \longrightarrow & I(\mathfrak{P}|\mathfrak{P}_D) & \longrightarrow & I(\mathfrak{P}_I|\mathfrak{P}_D) & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & D(\mathfrak{P}|\mathfrak{P}_I) & \longrightarrow & D(\mathfrak{P}|\mathfrak{P}_D) & \longrightarrow & D(\mathfrak{P}_I|\mathfrak{P}_D) & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & \mathrm{Gal}\left(\overline{L}|\overline{L}^I\right) & \longrightarrow & \mathrm{Gal}\left(\overline{L}|\overline{L}^D\right) & \longrightarrow & \mathrm{Gal}\left(\overline{L}^I|\overline{L}^D\right) & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

y obtenemos inmediatamente las igualdades:

$$\begin{aligned} D(\mathfrak{P}|\mathfrak{P}_D) = D(\mathfrak{P}|\mathfrak{p}) &= \mathrm{Gal}\left(L|L^D\right), \\ I(\mathfrak{P}|\mathfrak{P}_D) = I(\mathfrak{P}|\mathfrak{p}) &= \mathrm{Gal}\left(L|L^I\right), \\ D(\mathfrak{P}|\mathfrak{P}_I) = I(\mathfrak{P}|\mathfrak{p}) &= \mathrm{Gal}\left(L|L^I\right), \\ I(\mathfrak{P}|\mathfrak{P}_I) = I(\mathfrak{P}|\mathfrak{p}) &= \mathrm{Gal}\left(L|L^I\right), \end{aligned}$$

de manera que $I(\mathfrak{P}_I|\mathfrak{P}_D)$ es trivial y el grupo de Galois de la extensión residual $(B_I/\mathfrak{P}_I)|(B_D/\mathfrak{P}_D)$ es isomorfo al grupo de Galois $\mathrm{Gal}\left(L^I|L^D\right)$; en particular, el grado residual $f(\mathfrak{P}_I|\mathfrak{P}_D)$ coincide con el grado de la extensión; es decir, este grado es f_s y $\mathfrak{P}_I$ es no ramificado sobre $\mathfrak{P}_D$. De aquí se dedude inmediatamente la validez de las propiedades (ii) y (iii). □

Observación 5.4.3. En general, el grupo de descomposición no es un subgrupo normal del grupo de Galois; pero si lo es, la descomposición de $\mathfrak{p}$ en B_D es dada por la fórmula

$$\mathfrak{p}B_D = \mathfrak{P}_{D,1} \cdots \mathfrak{P}_{D,g},$$

donde $\mathfrak{P}_{D,i}$, son ideales primos diferentes de B_D de grado residual $f(\mathfrak{P}_{D,i}|\mathfrak{p}) = 1$ y $g = g(\mathfrak{p})$ es el número de ideales primos de B que dividen $\mathfrak{p}$.

Demostración: En este caso, la extensión $L^D|K$ es de Galois y, por tanto, todos los ideales primos de B_D que dividen $\mathfrak{p}$ tienen el mismo índice de ramificación y el mismo grado residual; pero si nos fijamos en el ideal de B_D contracción de $\mathfrak{P}$, obtenemos que el índice de ramificación y el grado residual de $\mathfrak{P}$ sobre $\mathfrak{p}$ son los de $\mathfrak{P}$ sobre su contracción $\mathfrak{P} \cap B_D$; por tanto, el índice de ramificación y el grado residual de $\mathfrak{P} \cap B_D$ sobre $\mathfrak{p}$ son ambos triviales, es decir, iguales a 1, y el número de ideales primos de B que dividen $\mathfrak{P} \cap B_D$ también es 1, de manera que el número de ideales primos de B_D que dividen $\mathfrak{p}$ coincide con el número de ideales primos de B que dividen $\mathfrak{p}$. □

Podemos resumir estos hechos en el resultado siguiente.

Corolario 5.4.4. *Sean A un anillo de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión finita, B la clausura entera de A en L, $\mathfrak{P} \subseteq B$ un ideal primo no nulo de B, y $\mathfrak{p} := \mathfrak{P} \cap A$ su contracción a A. Supongamos que la extensión $L|K$ es de Galois y sean $D := G_{-1}(\mathfrak{P}|\mathfrak{p})$, $I := G_0(\mathfrak{P}|\mathfrak{p})$, los grupos de descomposición y de inercia de $\mathfrak{P}$ sobre $\mathfrak{p}$. Entonces, la extensión*

$L|K$ "rompe" en una extensión $L|L^I$ que es totalmente ramificada en $\mathfrak{P}$ de manera que $L^I|K$ es no ramificada en $\mathfrak{P}_I := \mathfrak{P} \cap B_I$. Además, la extensión $L^I|K$ también "rompe" en una extensión $L^I|L^D$ que es no ramificada en $\mathfrak{P}_I$ y tal que $\mathfrak{P}_D := \mathfrak{P}_I \cap B_D$ no descompone en B_I. Si la extensión $L^D|K$ es de Galois (es decir, si el grupo de descomposición es normal en $\mathrm{Gal}\,(L|K)$), entonces, el primo $\mathfrak{p}$ descompone completamente en la extensión $L^D|K$. $\square$

5.5. Automorfismo de Frobenius

El estudio de las extensiones de Galois finitas de cuerpos de números que son no ramificadas en un ideal primo conduce de manera natural a la introducción del automorfismo de Frobenius. Esta sección se dedica a su introducción y al estudio de sus propiedades.

Efectivamente, en el caso de los cuerpos de números, los cuerpos residuales de las extensiones son cuerpos finitos; por tanto, son extensiones cíclicas y, en particular, separables. Más generalmente, sean A un anillo de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión finita y de Galois, $G := \mathrm{Gal}\,(L|K)$ su grupo de Galois, B la clausura entera de A en L, $\mathfrak{P} \subseteq B$ un ideal primo no nulo, y $\mathfrak{p} := \mathfrak{P} \cap A$ su contracción a A, y supongamos que la extensión $B|A$ es no ramificada en $\mathfrak{P}$ y que el cuerpo residual $A/\mathfrak{p}$ es un cuerpo finito de q elementos y característica p.

En estas condiciones, el grupo de inercia $G_0(\mathfrak{P}|\mathfrak{p})$ es trivial y el grupo de descomposición $G_{-1}(\mathfrak{P}|\mathfrak{p})$ es isomorfo de manera natural al grupo de Galois de la extensión residual; por tanto, $G_{-1}(\mathfrak{P}|\mathfrak{p})$ es un grupo cíclico de orden $f := f(\mathfrak{P}|\mathfrak{p})$. Podemos considerar, pues, el automorfismo $F_{\mathfrak{P}} \in G_{-1}(\mathfrak{P}|\mathfrak{p})$ que pensado en el grupo de Galois de la extensión residual es el automorfismo de Frobenius; es decir, que $F_{\mathfrak{P}}$ está definido unívocamente por la condición

$$F_{\mathfrak{P}}(b) - b^q \in \mathfrak{P}$$

para todo elemento $b \in B$.

Definición 5.5.1. El automorfismo $F_{\mathfrak{P}} \in G_{-1}(\mathfrak{P}|\mathfrak{p})$ se llama el automorfismo de Frobenius asociado a $\mathfrak{P}$; es un generador del grupo de descomposición $G_{-1}(\mathfrak{P}|\mathfrak{p})$ y es de orden $f(\mathfrak{P}|\mathfrak{p})$. Se acostumbra a designar por $(\mathfrak{P}, B|A)$ o por $\left(\dfrac{B|A}{\mathfrak{P}}\right)$; cuando no hay duda sobre los anillos, también se suele escribir

$(\mathfrak{P}, L|K)$ y $\left(\dfrac{L|K}{\mathfrak{P}}\right)$.

Observemos que si $\mathfrak{P}$ es no ramificado sobre $\mathfrak{p}$, entonces $\sigma(\mathfrak{P})$ también es no ramificado sobre $\mathfrak{p}$ para todo elemento $\sigma \in \mathrm{Gal}\,(L|K)$; puesto que la extensión $L|K$ es de Galois, esto significa que para todo ideal primo de B que divide $\mathfrak{p}$ está definido el automorfismo de Frobenius.

Proposición 5.5.2. *Supongamos que $B|A$ es no ramificada en $\mathfrak{P}$, sea $\mathfrak{P}' \subseteq B$ otro ideal primo no nulo de B que divida $\mathfrak{p}$ y sea $\sigma \in \mathrm{Gal}\,(L|K)$ un automorfismo cualquiera tal que $\mathfrak{P}' = \sigma(\mathfrak{P})$. Entonces, se satisface la igualdad*

$$\left(\frac{B|A}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{B|A}{\mathfrak{P}}\right)\sigma^{-1}$$

en el grupo de Galois $\mathrm{Gal}\,(L|K)$.

Demostración: En efecto, ya sabemos que los grupos de descomposición son conjugados, ya que son los grupos de isotropía de la acción del grupo de Galois sobre el conjunto de los ideales primos de B que dividen $\mathfrak{p}$. Ahora, la demostración es una simple comprobación: los elementos $\left(\dfrac{B|A}{\sigma(\mathfrak{P})}\right)$ y $\sigma\left(\dfrac{B|A}{\mathfrak{P}}\right)\sigma^{-1}$ están ambos en el grupo de descomposición $G_{-1}(\sigma(\mathfrak{P})|\mathfrak{p})$ y satisfacen la condición de congruencia; por la unicidad del automorfismo de Frobenius, coinciden. □

Seguidamente, se trata de hacer el estudio del comportamiento del automorfismo de Frobenius para cadenas de extensiones de Galois no ramificadas.

Proposición 5.5.3. *Sean K' un subcuerpo de L que contiene K, A' la clausura entera de A en K', y $\mathfrak{P}' := \mathfrak{P} \cap A'$ la contracción de $\mathfrak{P}$ a A'. La extensión $L|K'$ es una extensión de Galois y también es no ramificada en $\mathfrak{P}$. Entonces, el automorfismo de Frobenius $\left(\dfrac{B|A'}{\mathfrak{P}}\right)$ es la potencia f'-ésima del automorfismo de Frobenius $\left(\dfrac{B|A}{\mathfrak{P}}\right)$, donde f' es el grado residual $f' := f(\mathfrak{P}'|\mathfrak{p})$. Si, además, la extensión $K'|K$ es de Galois, entonces la extensión $A'|A$ es no ramificada en $\mathfrak{P}'$ y el automorfismo de Frobenius $\left(\dfrac{K'|K}{\mathfrak{P}'}\right)$ es la restricción a* $\mathrm{Gal}\,(K'|K)$ *del automorfismo de Frobenius $\left(\dfrac{L|K}{\mathfrak{P}}\right)$.*

DEMOSTRACIÓN: Todos los automorfismos que intervienen en el enunciado están definidos y basta comprobar que se satisfacen las congruencias que definen los automorfismos de Frobenius. Y para ello, basta tener en cuenta cuáles son los cuerpos residuales (finitos). □

Observación 5.5.4. Supongamos, ahora, que tenemos dos extensiones de Galois $L_i|K$ tales que el cuerpo L es el cuerpo composición de los L_i; sean $\mathfrak{P}_i := \mathfrak{P} \cap B_i$, las restricciones de $\mathfrak{P}$ a la clausura entera B_i de A en L_i, $i = 1, 2$. Entonces, las extensiones $B_i|A$ son no ramificadas en $\mathfrak{P}_i$ y los automorfismos de Frobenius $\left(\frac{B|A}{\mathfrak{P}}\right)$ $\left(\frac{B_i|A}{\mathfrak{P}_i}\right)$ están definidos. Por otro lado, puesto que el grupo de Galois de la extensión $L|K$ se inyecta, por restricción en cada componente, en el producto cartesiano de los grupos de Galois $\mathrm{Gal}\,(L_i|K)$, podemos identificar $\mathrm{Gal}\,(L|K)$ con un subgrupo de $\mathrm{Gal}\,(L_1|K) \times \mathrm{Gal}\,(L_2|K)$. Con esta identificación, el automorfismo de Frobenius $\left(\frac{B|A}{\mathfrak{P}}\right)$ es la pareja $\left(\left(\frac{B_1|A}{\mathfrak{P}_1}\right), \left(\frac{B_2|A}{\mathfrak{P}_2}\right)\right)$.

El automorfismo de Frobenius da una caracterización muy sencilla de los ideales primos del anillo base que descomponen completamente. Recordemos que se dice que un ideal primo $\mathfrak{p} \subseteq A$ descompone completamente en un cuerpo L extensión de K cuando la extensión de $\mathfrak{p}$ a la clausura entera de A en L es el producto de tantos ideales primos diferentes como el grado $[L : K]$ de la extensión.

Corolario 5.5.5. *Supongamos que la extensión $L|K$ es de Galois y no ramificada en $\mathfrak{p}$. Condición necesaria y suficiente para que $\mathfrak{p}$ descomponga completamente en B es que para cualquier ideal primo $\mathfrak{P} \subseteq B$ que divida $\mathfrak{p}$ en B, el automorfismo de Frobenius $\left(\frac{B|A}{\mathfrak{P}}\right)$ sea trivial.*

DEMOSTRACIÓN: En efecto, el automorfismo de Frobenius es un generador del grupo de descomposición y condición necesaria y suficiente para que este grupo sea trivial es que el índice de ramificación y el grado residual de cualquier ideal primo $\mathfrak{p}$ sean ambos iguales a 1. Esta condición es equivalente a decir que el ideal primo $\mathfrak{p}$ descompone completamente. □

Corolario 5.5.6. *Supongamos que el cuerpo L es el cuerpo composición de dos subcuerpoos $L_i \subseteq L$, $i = 1, 2$, que contienen K, como en la observación*

anterior. Entonces, condición necesaria y suficiente para que $\mathfrak{p}$ *descomponga completamente en* L *es que descomponga completament en cada una de les extensiones* L_i/K*.*

Observación 5.5.7. En el caso que la extensión $L|K$ sea abeliana, el automorfismo de Frobenius $\left(\frac{L|K}{\mathfrak{P}}\right)$ no depende del ideal primo $\mathfrak{P}$ de B que divide $\mathfrak{p}$; en este caso, se acostumbra a designar por $\left(\frac{L|K}{\mathfrak{p}}\right)$ y se llama el automorfismo de Frobenius de $\mathfrak{p}$.

5.6. Grupos de ramificación superior

La herramienta básica de la demostración que haremos del teorema de Kronecker-Weber es el concepto y las propiedades de los grupos de ramificación superior. Estos grupos son una generalización natural del grupo de inercia, del cual son subgrupos y heredan algunas propiedades.

Sean A un anillo de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión de Galois finita, $G := \mathrm{Gal}\,(L|K)$ el grupo de Galois, y B la clausura entera de A en L. Recordemos que G actúa de manera natural en B y que lo hace transitivamente en el conjunto de los ideales primos $\mathfrak{P} \subseteq B$ que dividen un ideal primo dado $\mathfrak{p} \subseteq A$. Además, hemos definido el grupo de descomposición $G_{-1}(\mathfrak{P}|\mathfrak{p})$ de un ideal primo fijo $\mathfrak{P} \subseteq B$ sobre su contracción $\mathfrak{p} := \mathfrak{P} \cap A$, como el subgrupo de G formado por los elementos $\sigma \in G$ que dejan $\mathfrak{P}$ invariante; es decir, por los elementos $\sigma \in G$ que actúan en el anillo cociente $B/\mathfrak{P}$; análogamente, hemos definido el grupo de inercia $G_0(\mathfrak{P}|\mathfrak{p})$ como el conjunto de los elementos $\sigma \in G$ que actúan en el anillo cociente $B/\mathfrak{P}$ como la identidad; equivalentemente, los elementos $\sigma \in G_0$ tales que para todo elemento $b \in B$ se satisface que $\sigma(b) - b \in \mathfrak{P}$.

Definición 5.6.1. Sea $k \geq -1$ un número entero. El conjunto

$$G_k(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in G_{-1}(\mathfrak{P}|\mathfrak{p}) :\ \sigma(b) - b \in \mathfrak{P}^{k+1},\ \text{para todo } b \in B\}$$

formado por los elementos $\sigma \in G_{-1}(\mathfrak{P}|\mathfrak{p})$ que actúan trivialmente en el anillo cociente $B/\mathfrak{P}^{k+1}$, es un subgrupo normal de $G_{-1}(\mathfrak{P}|\mathfrak{p})$; se llama el k-ésimo grupo de ramificación de $\mathfrak{P}$ sobre $\mathfrak{p}$. En efecto, es el núcleo del morfismo de

grupos

$$G_{-1}(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Aut}_{A/\mathfrak{p}}(B/\mathfrak{P}^{k+1}).$$

Por comodidad de notación, escribiremos G_k en lugar de $G_k(\mathfrak{P}|\mathfrak{p})$.

Observación 5.6.2. Notemos que el subíndice k asociado al grupo es una unidad inferior al exponente de $\mathfrak{P}$ que utilizamos en el anillo cociente $B/\mathfrak{P}^{k+1}$ sobre el cual pedimos que la acción sea trivial. Por otro lado, la definición coincide con la dada previamente para los grupos de descomposición y de inercia y generaliza esta última. Además, para todo $k \geq -1$, el grupo G_{k+1} es un subgrupo de G_k, de manera que disponemos de una sucesión de subgrupos de G_{-1}

$$G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots \supseteq G_k \supseteq G_{k+1} \supseteq \ldots$$

Puesto que el anillo B es noetheriano, se satisface la propiedad $\bigcap_{k\geq -1} \mathfrak{P}^k = (0)$, de manera que, puesto que G_{-1} es finito, existe $n_0 \in \mathbb{Z}$ tal que para $k \geq n_0$ es $G_k = (1)$. Por tanto, los subgrupos G_k forman una cadena normal de G_{-1}.

De los grupos de ramificación nos interesan los cocientes G_k/G_{k+1}, que podemos formar en virtud de la definición. Ya sabemos que el grupo cociente G_{-1}/G_0 es isomorfo al grupo de Galois de la extensión residual $A/\mathfrak{p} \subseteq B/\mathfrak{P}$. Para estudiar la estructura de los cocientes para $k \geq 0$, comencemos por establecer el resultado siguiente.

Proposición 5.6.3. *Para todo número entero $k \geq 1$, los grupos cociente G_k/G_{k+1} son abelianos.*

Demostración: La demostración es una consecuencia elemental del estudio de los conmutadores $[\sigma, \tau] := \sigma\tau\sigma^{-1}\tau^{-1}$, para $\sigma \in G_k$, $\tau \in G_n$, $k, n \geq 0$. Se satisface el resultado siguiente.

Lema 5.6.4. *Con las notaciones anteriores, $[\sigma, \tau] \in G_{k+n}$.*

Demostración: Comencemos por ver que para todo $b \in \mathfrak{P}^{n+1}$ es $\sigma b - b \in \mathfrak{P}^{k+n+1}$. Para ello, es suficiente considerar elementos b de la forma $b := b_1 \cdot b_2 \cdot \cdots \cdot b_{n+1}$ tales que $b_j \in \mathfrak{P}$, ya que estos elementos generan $\mathfrak{P}^{n+1}$ como grupo abeliano aditivo. Podemos escribir la identidad

$$\sigma(b) - b = \sum_{j=1}^{n+1} \sigma(b_1) \ldots \sigma(b_{j-1})(\sigma(b_j) - b_j) b_{j+1} \ldots b_{n+1},$$

que muestra que el elemento $\sigma(b)-b$ pertenece a $\mathfrak{P}^{k+n+1}$, ya que $\sigma(b_j)-b_j \in \mathfrak{P}^{k+1}$ porque $b_j \in B$ y $\sigma \in G_k$. Análogamente, para todo $c \in \mathfrak{P}^{k+1}$ es $\tau(c)-c \in \mathfrak{P}^{k+n+1}$.

Tomemos, ahora, cualquier elemento $x \in B$ y pongamos $y := \sigma^{-1}\tau^{-1}(x)$, $b := \tau(y)-y$, y $c := \sigma(y)-y$. Por la elección de σ y τ, se satisfacen las propiedades $b \in \mathfrak{P}^{n+1}$, $c \in \mathfrak{P}^{k+1}$, de manera que $\sigma(b)-b, \tau(c)-c \in \mathfrak{P}^{k+n+1}$; restando, obtenemos que

$$\begin{aligned}\sigma(b)-b-\tau(c)+c &= \sigma(\tau(y)-y)-(\tau(y)-y)-\tau(\sigma(y)-y)+(\sigma(y)-y)\\ &= \sigma\tau(y)-\tau\sigma(y) \in \mathfrak{P}^{k+n+1};\end{aligned}$$

es decir, $[\sigma,\tau](x)-x \in \mathfrak{P}^{k+n+1}$. Por tanto, $[\sigma,\tau] \in G_{k+n}$. □

Ahora podemos acabar fácilmente la prueba de la proposición; basta tomar $n=k$ y obtenemos que $[\sigma,\tau] \in G_{2k}$; puesto que $k \geq 1$, es $2k \geq k+1$ y el grupo cociente G_k/G_{k+1} es abeliano. □

El resultado que proporciona esta proposición no es tan general como es posible. Sin embargo, en el caso de los cuerpos de números, los cuerpos residuales son finitos y, en consecuencia, las extensiones residuales son separables. A causa de este hecho, y que solamente trataremos el caso de los cuerpos de números, nos situaremos en la hipótesis restrictiva que la extensión residual $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ sea separable. En este caso, podemos demostrar el resultado siguiente, que no es válido en general.

Proposición 5.6.5. *Supongamos que la extensión residual en $\mathfrak{P}$ es separable. Entonces:*

(i) El cociente G_0/G_1 es isomorfo a un subgrupo (finito) del grupo multiplicativo $(B/\mathfrak{P})^*$; en particular, es cíclico de orden primo con la característica residual (si esta es positiva).

(ii) Para $k \geq 1$, los cocientes G_k/G_{k+1} son isomorfos a subgrupos (finitos) del grupo aditivo del cuerpo residual $B/\mathfrak{P}$; en particular, si $B/\mathfrak{P}$ es un cuerpo de característica $p>0$, los cocientes son p-grupos abelianos elementales; y si la característica residual es 0, los cocientes son triviales y $G_1=(0)$.

Demostración: Si localizamos en $S := A-\mathfrak{p}$, ni los grupos de ramificación ni los cuerpos residuales no cambian, de manera que podemos suponer que A y B son anillos principales. Sea $\pi \in \mathfrak{P}$ un generador del ideal $\mathfrak{P}$. Vamos

a definir morfismos de grupos abelianos $G_0 \longrightarrow (B/\mathfrak{P})^*$ y $G_k \longrightarrow B/\mathfrak{P}$. Dado $\sigma \in G_0$, el elemento $\sigma(\pi)$ también pertenece a $\mathfrak{P}$, ya que σ deja invariante $\mathfrak{P}$; pero no puede ser que $\sigma(\pi) \in \mathfrak{P}^2$ ya que, aplicando σ^{-1}, también sería $\pi \in \mathfrak{P}^2$; por tanto, existe $u_\sigma \in B$, $u_\sigma \notin \mathfrak{P}$, tal que $\sigma(\pi) = u_\sigma \pi$. Este elemento está unívocamente determinado por σ, por ejemplo, por ser B un dominio de integridad. Si ahora tomamos $\tau \in G_0$, la igualdad $\sigma(\pi) = u_\sigma \pi$ se transforma en $u_{\tau\sigma}\pi = \tau\sigma(\pi) = \tau(u_\sigma)u_\tau\pi$, de manera que $u_{\tau\sigma} = \tau(u_\sigma)u_\tau$. Si reducimos módulo $\mathfrak{P}$, puesto que $\tau \in G_0$, es $\tau(u_\sigma) \equiv u_\sigma \pmod{\mathfrak{P}}$, y, por tanto, $u_{\tau\sigma} \equiv u_\sigma u_\tau \pmod{\mathfrak{P}}$. De esta manera definimos una aplicación multiplicativa $G_0 \longrightarrow B/\mathfrak{P}$; puesto que $u_\sigma \in B$ y $u_\sigma \notin \mathfrak{P}$, la imagen está incluída en $(B/\mathfrak{P})^*$, de manera que se obtiene un morfismo de grupos. El núcleo de este morfismo está formado por los elementos $\sigma \in G_0$ tales que $u_\sigma \equiv 1 \pmod{\mathfrak{P}}$; es decir, tales que $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^2}$. Ahora bien, decir que $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^2}$ equivale a decir que para todo elemento $b \in B$ es $\sigma(b) \equiv b \pmod{\mathfrak{P}^2}$. En efecto, en el caso separable, el cuerpo residual en $\mathfrak{P}$ coincide con el cuerpo residual de B_I en $\mathfrak{P}_I := \mathfrak{P} \cap B_I$, y, por tanto, podemos escribir b en la forma $b = c + d$, para algunos elementos $c \in B_I$ y $d \in \mathfrak{P}$; puesto que $c \in B_I$ y $\sigma \in G_0$, es $\sigma(c) = c$, de manera que basta ver que $\sigma(d) \equiv d \pmod{\mathfrak{P}^2}$. Pero si escribimos $d = a\pi$, $a \in B$, entonces, $\sigma(d) - d = \sigma(a\pi) - a\pi = \sigma(a)(\sigma(\pi) - \pi) + \pi(\sigma(a) - a) \in \mathfrak{P}^2$, ya que $\sigma(\pi) - \pi \in \mathfrak{P}^2$, $\sigma(a) \in B$, y $\sigma(a) - a \in \mathfrak{P}$ por ser $\sigma \in G_0$. Dicho de otra manera, el núcleo del morfismo $G_0 \longrightarrow (B/\mathfrak{P})^*$ es exactamente G_1. Esto demuestra la primera parte.

La segunda parte se demuestra análogamente. Dado $\sigma \in G_k$, $k \geq 1$, $\sigma(\pi) - \pi \in \mathfrak{P}^{k+1}$, de manera que existe $u_\sigma \in B$, unívocamente determinado por σ, tal que $\sigma(\pi) - \pi = u_\sigma \pi^{k+1}$. Si ahora tomamos $\tau \in G_k$, la igualdad $\sigma(\pi) - \pi = u_\sigma \pi^{k+1}$ se transforma en

$$\begin{aligned} u_{\tau\sigma}\pi^{k+1} &= \tau\sigma(\pi) - \pi \\ &= \tau(\sigma(\pi) - \pi) + (\tau(\pi) - \pi) \\ &= \tau(u_\sigma \pi^{k+1}) + u_\tau \pi^{k+1} \\ &= \tau(u_\sigma)\tau(\pi)^{k+1} + u_\tau \pi^{k+1} \\ &= \tau(u_\sigma)(\pi + u_\tau \pi^{k+1})^{k+1} + u_\tau \pi^{k+1} \\ &= \pi^{k+1}(\tau(u_\sigma)(1 + u_\tau \pi^k)^{k+1} + u_\tau); \end{aligned}$$

si dividimos por π^{k+1}, obtenemos que $u_{\tau\sigma} \equiv \tau(u_\sigma) + u_\tau \pmod{\mathfrak{P}}$, ya que $k \geq 1$; y puesto que $\tau(u_\sigma) \equiv u_\sigma \pmod{\mathfrak{P}}$, porque $\tau \in G_0$, obtenemos que

$u_{\tau\sigma} \equiv u_\sigma + u_\tau \pmod{\mathfrak{P}}$. Si reducimos módulo $\mathfrak{P}$, obtenemos un morfismo aditivo de grupos $G_k \longrightarrow B/\mathfrak{P}$. El núcleo de este morfismo está formado por los elementos $\sigma \in G_k$ tales que $u_\sigma \equiv 0 \pmod{\mathfrak{P}}$; es decir, tales que $\sigma(\pi) - \pi \in \mathfrak{P}^{k+2}$. Ahora bien, decir que $\sigma(\pi) - \pi \in \mathfrak{P}^{k+2}$ equivale a decir que para todo elemento $b \in B$ es $\sigma(b) - b \in \mathfrak{P}^{k+2}$. En efecto; como antes, podemos escribir b en la forma $b = c + d$, para algunos elementos $c \in B_I$ y $d \in \mathfrak{P}$; puesto que $c \in B_I$ y $\sigma \in G_k \subseteq G_0$, es $\sigma(c) = c$, de manera que basta ver que $\sigma(d) - d \in \mathfrak{P}^{k+2}$. Pero si escribimos $d = a\pi$, $a \in B$, entonces, $\sigma(d) - d = \sigma(a\pi) - a\pi = \sigma(a)(\sigma(\pi) - \pi) + \pi(\sigma(a) - a) \in \mathfrak{P}^{k+2}$, ya que $\sigma(\pi) - \pi \in \mathfrak{P}^{k+2}$, por hipótesis, $\sigma(a) \in B$, y $\sigma(a) - a \in \mathfrak{P}^{k+1}$ por ser $\sigma \in G_k$. Dicho de otra manera, el núcleo del morfismo $G_k \longrightarrow B/\mathfrak{P}$ es exactamente G_{k+1}, como se quería demostrar. □

Corolario 5.6.6. *Supongamos que el cuerpo residual es de característica positiva p; entonces, G_1 es un p-grupo abeliano y el cociente G_0/G_1 es un grupo abeliano de orden no divisible por p.* □

Definición 5.6.7. Una extensión $B|A$ de anillos de Dedekind se llama moderadamente ramificada en un ideal primo no nulo $\mathfrak{P} \subseteq B$ cuando el índice de ramificación $e(\mathfrak{P}|\mathfrak{p})$ no es divisible por la característica residual en $\mathfrak{P}$; en caso contrario, se llama salvajemente ramificada. En el caso galoisiano, decir moderadamente ramificada en $\mathfrak{P}$ equivale a decir que el grupo de ramificación $G_1(\mathfrak{P}|\mathfrak{p})$ es trivial.

Corolario 5.6.8. *Supongamos que los cuerpos residuales son finitos. Entonces, el grupo de descomposición es un grupo resoluble.*

Demostración: En efecto, acabamos de probar que si la extensión residual es separable, entonces el grupo de inercia es resoluble, ya que la cadena de los grupos de ramificación G_k, $k \geq 0$, es abeliana; por otro lado, si la extensión residual es resoluble, puesto que el grupo cociente G_{-1}/G_0 es isomorfo al grupo de Galois de la extensión residual, la cadena G_k, $k \geq -1$, es abeliana; y este es el caso si los cuerpos residuales son finitos. □

5.7. El grupo de inercia moderada

En el caso de extensiones de Galois de cuerpos de números o, más generalmente, en que la extensión residual $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ es separable, podemos

considerar el cuerpo L^{G_1} fijo por el grupo G_1; entonces, la extensión totalmente ramificada en $\mathfrak{P}$, $L|L^I$, "rompe" en una extensión moderadamente ramificada $L^{G_1}|L^I$ y una extensión, $L|L^{G_1}$, totalmente ramificada de grado potencia de la característica residual. En particular, la ramificación total aún se puede estudiar por etapas: una moderadamente ramificada y una salvajemente ramificada.

Definición 5.7.1. El grupo G_0/G_1 se llama el grupo de inercia moderada en $\mathfrak{P}$; es un grupo de orden la parte libre de p del índice de ramificación $e(\mathfrak{P}|\mathfrak{p})$, donde p denota la característica residual.

Para uso posterior, conviene establecer el resultado siguiente.

Proposición 5.7.2. *Supongamos que el cuerpo residual $A/\mathfrak{p}$ es de cardinal finito q y de característica positiva p. El grupo de inercia moderada de la extensión $B|A$ en $\mathfrak{P}$, G_0/G_1, es un grupo cíclico de orden divisor de $q^f - 1$, donde $f := f(\mathfrak{P}|\mathfrak{p})$ denota el grado residual en $\mathfrak{P}$ de la extensión. Si suponemos que el grupo G_{-1}/G_1 es abeliano, entonces, el orden de G_0/G_1 es divisor de $q-1$.*

Demostración: La primera parte es inmediata, ya que el cociente G_0/G_1 se identifica con un subgrupo del grupo multiplicativo $(B/\mathfrak{P})^*$; veamos la segunda.

Igual que en la demostración de la proposición de más arriba, podemos suponer que A es local y, por tanto, que $\mathfrak{P}$ es un ideal principal; sea, pues, $\pi \in \mathfrak{P}$ un generador de $\mathfrak{P}$. Observemos que si $\sigma \in G_{-1}$, entonces $\sigma(\pi) = u_\sigma \pi$ para un cierto elemento entero $u_\sigma \in B$; en particular, ya hemos visto que si $\sigma \in G_0$, entonces $u_\sigma \notin \mathfrak{P}$ y la asignación de la clase residual de u_σ a σ, define el morfismo inyectivo de grupos $G_0/G_1 \longrightarrow (B/\mathfrak{P})^*$.

Puesto que el grupo cociente G_0/G_1 es cíclico, podemos considerar un elemento $\sigma \in G_0$ que genere el cociente G_0/G_1; se trata de demostrar que el orden de σ como automorfismo de G_0/G_1 es un divisor de $q-1$. Para ello, podemos considerar un elemento $\varphi \in G_{-1}$ tal que la reducción módulo $\mathfrak{P}$ del automorfismo $\varphi : B \longrightarrow B$ sea el automorfismo de Frobenius del cuerpo finito $B/\mathfrak{P}$ sobre $A/\mathfrak{p}$; recordemos que el automorfismo de Frobenius de $B/\mathfrak{P}$ es dado por la asignación $b \mapsto b^q$. En particular, podemos escribir $\sigma(\pi) = u_\sigma \pi$, $\varphi(\pi) = u_\varphi \pi$, y $\varphi\sigma\varphi^{-1}(\pi) = v\pi$, para ciertos elementos $u_\sigma, u_\varphi, v \in B$.

Con estas notaciones, podemos observar que se satisfacen las igualdades siguientes: por un lado, de la segunda se deduce inmediatamente que $\varphi^{-1}(\pi) = \varphi^{-1}(u_\varphi)^{-1}\pi$; por otro, la hipótesis que el cociente G_{-1}/G_1 es abeliano nos enseña que $u_\sigma - v \in \mathfrak{P}$, ya que la acción de los dos automorfismos $\varphi\sigma\varphi^{-1}$ y σ coincide módulo $\mathfrak{P}^2$, de manera que $\varphi\sigma\varphi^{-1}(\pi) - \sigma(\pi) \in \mathfrak{P}^2$; y podemos dividir por π. Finalmente, podemos escribir:

$$\begin{aligned}\varphi\sigma\varphi^{-1}(\pi) &= \varphi\sigma(\varphi^{-1}(u_\varphi)^{-1}\pi)\\ &= \varphi(\sigma\varphi^{-1}(u_\varphi)^{-1}u_\sigma\pi)\\ &= \varphi\sigma\varphi^{-1}(u_\varphi)^{-1}\varphi(u_\sigma)u_\varphi\pi;\end{aligned}$$

es decir, $v = \varphi\sigma\varphi^{-1}(u_\varphi)^{-1}\varphi(u_\sigma)u_\varphi$. Si tenemos en cuenta que $\sigma \in G_0$, obtenemos que σ es la identidad en $B/\mathfrak{P}$, de manera que

$$\begin{aligned}v &\equiv \varphi\varphi^{-1}(u_\varphi)^{-1}\varphi(u_\sigma)u_\varphi\\ &= \varphi(u_\sigma)\\ &= u_\sigma^q \pmod{\mathfrak{P}},\end{aligned}$$

por definición de φ. De aquí se deduce inmediatamente, ya que $u_\sigma \notin \mathfrak{P}$, que $u_\sigma^{q-1} \equiv 1 \pmod{\mathfrak{P}}$, de manera que σ es de orden divisor de $q-1$, como queríamos demostrar. □

5.8. Grupos de ramificación y diferente

El objetivo de esta sección es proporcionar una fórmula explícita para el cálculo del diferente de una extensión en algunos casos particulares importantes. Conviene establecer algunas propiedades de los grupos de ramificación respecto a cadenas de extensiones.

Proposición 5.8.1. *Sean A un anillo de Dedekind, K su cuerpo de fracciones, $L|K$ una extensión de Galois finita, B la clausura entera de A en L, $\mathfrak{P} \subseteq B$ un ideal primo no nulo de B, $\mathfrak{p} := \mathfrak{P} \cap A$ su contracción a A, $G := \mathrm{Gal}\,(L|K)$ el grupo de Galois, $H \subseteq G$ un subgrupo cualquiera de G, $K' := L^H$ el cuerpo fijo, $A' := B \cap K'$ la clausura entera de A en K' y $\mathfrak{P}' := \mathfrak{P} \cap A'$ la contracción de $\mathfrak{P}$ a A'. Entonces, los grupos de ramificación de $\mathfrak{P}$ sobre $\mathfrak{P}'$ se pueden calcular por la fórmula*

$$G_k(\mathfrak{P}/\mathfrak{P}') = G_k(\mathfrak{P}/\mathfrak{p}) \cap H.$$

DEMOSTRACIÓN: Inmediata a partir de la definición de los grupos de ramificación, ya que $H = \mathrm{Gal}\,(L|K')$. □

Corolario 5.8.2. *Si, además, el grupo H es uno de los grupos de ramificación, pongamos $G_k(\mathfrak{P}|\mathfrak{p})$, entonces, los grupos de ramificación $G_i(\mathfrak{P}|\mathfrak{P}')$ son exactamente el grupo $G_k(\mathfrak{P}|\mathfrak{p})$ para $0 \leq i \leq k$, y $G_i(\mathfrak{P}|\mathfrak{P}') = G_i(\mathfrak{P}|\mathfrak{p})$, para $i > k$.* □

Seguidamente se trata de hacer el cálculo de los exponentes del diferente en función de los órdenes de los grupos de ramificación. Para ello, nos situaremos en el caso local (cosa que podemos hacer siempre ya que el diferente y los grupos de ramificación se conservan por localización) y totalmente ramificado (cosa que podemos hacer si nos restringimos a la extensión dada por el grupo de inercia).

Proposición 5.8.3. *Con las mismas notaciones que en la proposición anterior, supongamos que A es un anillo de Dedekind local, que la extensión residual $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ es separable, y que la extensión $B|A$ es totalmente ramificada en $\mathfrak{P}$. Entonces, el exponente de $\mathfrak{P}$ en el diferente $\mathcal{D}(B|A)$ es dado por la suma finita*

$$\sum_{k\geq 0}(\#G_k(\mathfrak{P}/\mathfrak{p}) - 1).$$

DEMOSTRACIÓN: Puesto que la extensión es totalmente ramificada, $\mathfrak{P}$ es el único ideal primo de B que divide $\mathfrak{p}$, y puesto que A es local, los anillos A y B son principales. Elijamos un generador π de $\mathfrak{P}$ y sea $f(X) := \mathrm{Irr}(\pi, K)$ el polinomio mónico irreducible de $A[X]$ que tiene π como raíz. Aseguramos que en este caso π es un elemento primitivo de la extensión $L|K$ y $B = A[\pi]$.

En efecto, esto es una consecuencia del resultado más general que sigue.

Lema 5.8.4. *Con las mismas hipótesis y notaciones, $B = A[\pi]$ y el polinomio $f(X) := \mathrm{Irr}(\pi, K)$ es un polinomio de Eisenstein respecto al generador del ideal maximal $\mathfrak{p}$ de A.*

DEMOSTRACIÓN: Sea $e := e(\mathfrak{P}|\mathfrak{p}) = [L : K]$ el índice de ramificación, que coincide con el grado porque la extensión es totalmente ramificada y la extensión residual es separable. Comencemos por demostrar que los elementos

$$1, \pi, \pi^2, \ldots, \pi^{e-1}$$

son K-linealmente independientes; más generalmente, supongamos que tenemos una igualdad de la forma

$$b = a_0 + a_1\pi + \cdots + a_{e-1}\pi^{e-1},$$

con los elementos $a_i \in K$ y $b \in L$. Para todo índice i, $1 \leq i \leq e-1$, tal que a_i sea no nulo, sea $v_i \in \mathbb{Z}$ el exponente de la potencia exacta de $\mathfrak{p}$ que contiene el elemento a_i; esta potencia sólo es no negativa cuando $a_i \in A$ y, en caso contrario, el ideal $\mathfrak{p}^{v_i}$ sólo es un ideal fraccionario. Puesto que la extensión de $\mathfrak{p}$ al anillo B es el ideal $\mathfrak{P}^e$, y puesto que π es un generador de $\mathfrak{P}$, los elementos $a_i\pi^i$ tales que $a_i \neq 0$ pertenecen exactamente al ideal $\mathfrak{P}^{i+ev_i}$. Los exponentes son todos diferentes, ya que lo son módulo e; luego, la suma $a_0 + a_1\pi + \cdots + a_{e-1}\pi^{e-1}$ pertenece al ideal $\mathfrak{P}^t$ y no a $\mathfrak{P}^{t+1}$, donde t es el mínimo de los exponentes $i + ev_i$ tales que $a_i \neq 0$. En particular, si $b = 0$, ha de ser $a_i = 0$ para todo índice i, ya que 0 no pertenece a ninguna potencia positiva de $\mathfrak{P}$; esto nos dice que los elementos $1, \pi, \ldots, \pi^{e-1}$ son K-linealmente independientes.

Pero aún nos dice más; si $b \in A$, entonces t ha de ser un múltiplo no negativo de e, ya que la potencia exacta de $\mathfrak{P}$ que contiene b es e veces la potencia exacta de $\mathfrak{p}$ que contiene b en A. En particular, si $b \in A$, entonces $t \geq 0$ y t es divisible por e; por tanto, todos los v_i han de ser no negativos, y $b \in A[\pi]$; esto demuestra la igualdad $B = A[\pi]$.

Finalmente, ya hemos hecho notar que el polinomio $f(X)$ tiene coeficientes en A; además, puesto que las potencias $1, \pi, \pi^2, \ldots, \pi^{e-1}$ son K-linealmente independientes, $f(X)$ es un polinomio de grado e, ya que el grado no puede sobrepasar al de la extensión y ha de ser mayor o igual que e. Si ponemos $f(X) = X^e - (a_0 + a_1X + \cdots + a_{e-1}X^{e-1})$, obtenemos la igualdad $\pi^e = a_0 + a_1\pi + \cdots + a_{e-1}\pi^{e-1}$ con $a_i \in A$; puesto que π^e pertenece exactamente al ideal $\mathfrak{P}^e$, resulta que $t = e$, y esto sólo se consigue cuando $t = ev_0$, ya que, en caso contrario, t no es divisible por e. Dicho de otra manera, $v_0 = 1$, y $v_i \geq 1$ para todo índice $i \geq 1$ tal que $a_i \neq 0$; puesto que $\mathfrak{p}$ es principal, resulta que $a_0 \in \mathfrak{p} - \mathfrak{p}^2$ es un generador de $\mathfrak{p}$ y todos los demás coeficientes a_i pertenecen a $\mathfrak{p}$; es decir, $f(X)$ es un polinomio de Eisenstein respecto a $\mathfrak{p}$. □

En consecuencia, el conductor de B en $A[\pi]$ es trivial y, por tanto, el diferente de la extensión es el ideal, potencia de $\mathfrak{P}$, generado por $f'(\pi)$. Calculemos este ideal. Si consideramos la derivada en π del polinomio $f(X)$,

podemos escribir $f(X) = \prod_{\sigma \in G}(X - \sigma(\pi))$, de manera que $f'(\pi)$ es el producto

$$\begin{aligned} f'(\pi) &= \prod_{\sigma \neq 1}(\pi - \sigma(\pi)) \\ &= \prod_{k \geq 0} \prod_{\sigma \in G_k - G_{k+1}} (\pi - \sigma(\pi)), \end{aligned}$$

ya que $G_0 = G_{-1} = G$ porque la extensión es totalmente ramificada. Ahora, para $\sigma \in G_k$, $\sigma \notin G_{k+1}$, ha de ser $b - \sigma(b) \in \mathfrak{P}^{k+1}$ para todo elemento $b \in B$; en particular, $\pi - \sigma(\pi) \in \mathfrak{P}^{k+1}$; por otro lado, $\pi - \sigma(\pi) \notin \mathfrak{P}^{k+2}$, ya que en este caso, obtendríamos que $\sigma \in G_{k+1}$ como en la demostración de la proposición 5.6.5. Así, el exponent de $\mathfrak{P}$ en el diferente $\mathcal{D}(B|A) = f'(\pi)B$ es la suma

$$\begin{aligned} &\sum_{k \geq 0} \sum_{\sigma \in G_k - G_{k+1}} (k+1) \\ &= \sum_{k \geq 0} (k+1)(\#G_k - \#G_{k+1}) \\ &= \sum_{k \geq 0} (k+1)[(\#G_k - 1) - (\#G_{k+1} - 1)] \\ &= \sum_{k \geq 0} (\#G_k - 1), \end{aligned}$$

ya que G_k es trivial a partir de un lugar en adelante. Esto acaba la prueba. □

Capítulo 6

El teorema de Kronecker-Weber

Este capítulo se dedica a hacer la demostración del teorema de Kronecker-Weber, que ya ha sido enunciado en el primer capítulo. De hecho, es el punto culminante del curso y la "excusa"que hemos utilizado para hacer la introducción de los métodos generales de ramificación y geometría de los números que se suelen utilizar en la teoría algebraica de números.

6.1. El caso moderadamente ramificado

El objetivo de este capítulo es presentar una demostración completa del resultado siguiente.

Teorema 6.1.1. (Kronecker-Weber) *Sea $K|\mathbb{Q}$ una extensión abeliana. Entonces, existe una raíz de la unidad, ζ, tal que $K \subseteq \mathbb{Q}(\zeta)$.*

Recordemos que ya lo hemos demostrado en el caso en que la extensión $K|\mathbb{Q}$ sea cuadrática. Ahora conviene hacer la reducción de la prueba al caso de las extensiones cíclicas de grado potencia de un número primo. Concretamente, podemos comenzar por establecer el resultado siguiente.

Proposición 6.1.2. *Si el teorema de Kronecker-Weber se satisface para todas las extensiones cíclicas de grado potencia de primo, entonces se satisface para todas las extensiones abelianas.*

DEMOSTRACIÓN: Basta considerar que toda extensión abeliana descompone en producto linealmente disjunto de extensiones cíclicas de grado potencia de primo. Esto se deduce del hecho que todo grupo abeliano descompone en producto directo de p-subgrupos y estos en producto directo de subgrupos cíclicos; concretamente, supongamos que $G := \mathrm{Gal}\,(K|\mathbb{Q})$ descompone en producto $G := \prod_i G_i$, donde p_i es un número primo cualquiera y G_i es un p_i-grupo cíclico. Sea K_i el subcuerpo de K fijo por el subgrupo $\prod_{j\neq i} G_j$ de G; entonces, $K_i|\mathbb{Q}$ es una extensión cíclica de grado potencia de un número primo p_i; por hipótesis, existe una raíz de la unidad ζ_i tal que $K_i \subseteq \mathbb{Q}(\zeta_i)$. Sean $n_i \in \mathbb{Z}$ tales que ζ_i es una raíz primitiva n_i-ésima de la unidad, $n := \mathrm{mcm}\{n_i\}$ y ζ una raíz primitiva n-ésima de la unidad. Puesto que K es la composición de los cuerpos K_i, obtenemos que $K \subseteq \mathbb{Q}(\zeta)$, que es lo que se quería probar. □

Recordemos que toda extensión de $\mathbb{Q}$ ramifica en algún número primo. Ahora, se trata de hacer la reducción de la prueba del teorema de Kronecker-Weber al caso en que el conjunto de los números primos que ramifican consiste sólo en el primo que divide el grado; dicho de otra manera, podemos suponer que la extensión es cíclica de grado potencia de un número primo p y no ramificada en todo número primo ℓ diferente de p.

Efectivamente. Supongamos que $K|\mathbb{Q}$ es cíclica de grado potencia de un número primo p y que $\ell \neq p$ es un número primo que ramifica. Sea $\mathfrak{L}$ un ideal primo del anillo de los enteros del cuerpo K que divide ℓ; en particular, la extensión $K|\mathbb{Q}$ es moderadamente ramificada en $\mathfrak{L}$; es decir, el grupo de ramificación $G_1(\mathfrak{L}|\ell)$ es trivial. Puesto que el orden del grupo de inercia en $\mathfrak{L}$ es un divisor del grado, ha de ser una potencia de p, pongamos p^m; y puesto que el cuerpo residual de $\mathbb{Z}$ en ℓ es el cuerpo $\mathbb{F}_\ell$, el hecho que el cociente $G_{-1}(\mathfrak{L}|\ell)/G_1(\mathfrak{L}|\ell)$ sea abeliano nos permite asegurar que el orden del grupo de inercia divide $\ell - 1$; por tanto, $\ell \equiv 1 \pmod{p^m}$. Ahora bien, la extensión $\mathbb{Q}(\zeta_\ell)|\mathbb{Q}$ es cíclica, no ramificada fuera de ℓ y totalmente ramificada en ℓ; en consecuencia, existe un único subcuerpo $L \subseteq \mathbb{Q}(\zeta_\ell)$ tal que la extensión $L|\mathbb{Q}$ es cíclica, totalmente ramificada en ℓ, no ramificada fuera de ℓ y de grado p^m.

Consideremos el cuerpo composición KL. Puesto que las extensiones $K|\mathbb{Q}$ y $L|\mathbb{Q}$ son abelianas de grado potencia de p, también la composición $KL|\mathbb{Q}$

es una extensión abeliana de grado potencia de p, pongamos p^{n+t}, donde $t \leq m$ y $p^n := [K : \mathbb{Q}]$. Sean $\mathfrak{L}'$ un ideal primo del anillo de los enteros de KL que divida $\mathfrak{L}$, $I' := G_0(\mathfrak{L}'|\ell)$ el grupo de inercia de $\mathfrak{L}'$ sobre el primo ℓ, y $H := \mathrm{Gal}\,(L|\mathbb{Q}) \simeq \mathbb{Z}/p^m\mathbb{Z}$ el grupo de Galois.

El morfismo de restricción $\mathrm{Gal}\,(KL|\mathbb{Q}) \longrightarrow \mathrm{Gal}\,(K|\mathbb{Q})$ aplica el grupo de inercia I' en el grupo de inercia $G_0(\mathfrak{L}|\ell)$, de manera que se obtiene una inclusión $I' \subseteq G_0(\mathfrak{L}|\ell) \times H$, por vía de la identificación de $\mathrm{Gal}\,(KL|\mathbb{Q})$ con un subgrupo del producto $\mathrm{Gal}\,(K|\mathbb{Q}) \times \mathrm{Gal}\,(L|\mathbb{Q})$. Por otro lado, el orden del grupo de inercia I' es múltiplo de p^m, ya que el índice de ramificación de $\mathfrak{L}'$ sobre ℓ es divisible por el índice de ramificación de $\mathfrak{L}$ sobre ℓ; y, como antes, los grupos de ramificación superiores $G_i(\mathfrak{L}'|\ell)$, $i \geq 1$, son triviales, ya que la extensión es de grado potencia de p y p no divide la característica residual ℓ; por tanto, el grupo de inercia I' es cíclico. Además, el orden de los elementos del grupo producto $G_0(\mathfrak{L}|\ell) \times H$ es un divisor de p^m, ya que ambos grupos son cíclicos de orden p^m; puesto que el orden de I' es como mínimo p^m y I' es cíclico, el orden de I' es exactamente p^m. Así, si designamos por K' el subcuerpo de KL fijo por el subgrupo I', la extensión $K'|\mathbb{Q}$ es no ramificada en ℓ; y puesto que $L|\mathbb{Q}$ es totalmente ramificada en ℓ, ha de ser $K' \cap L = \mathbb{Q}$; por tanto, el subcuerpo $K'L \subseteq KL$ es de grado $[K'L : \mathbb{Q}] = [K' : \mathbb{Q}][L : \mathbb{Q}] = [KL : \mathbb{Q}]$, ya que el grado de la extensión $K'|\mathbb{Q}$ es el grado de la extensión $KL|\mathbb{Q}$ dividido por el índice de ramificación de $\mathfrak{L}'$ sobre ℓ, que es exactamente el mismo que el grado de la extensión $L|\mathbb{Q}$; en consecuencia, obtenemos la igualdad de cuerpos $K'L = KL$.

De esta manera, si demostramos que el cuerpo K' es ciclotómico, puesto que L también lo es, lo es su composición $K'L = KL$, de manera que el cuerpo K, siendo subcuerpo de un cuerpo ciclotómico, también es un cuerpo ciclotómico. Ahora, el cuerpo K' no ramifica en ℓ, por construcción, y sus primos de ramificación forman un subconjunto del conjunto de los primos de ramificación de la extensión $K|\mathbb{Q}$; puesto que el conjunto de primos de ramificación de la extensión $K|\mathbb{Q}$ es finito, podemos repetir el argumento y suponer que la extensión $K|\mathbb{Q}$ es no ramificada fuera de los ideales primos que dividen p.

En estos momentos podemos demostrar el teorema de Kronecker-Weber para el caso moderadamente ramificado. Pero podemos decir aún más.

Proposición 6.1.3. *Sea $K|\mathbb{Q}$ una extensión abeliana de grado potencia de un número primo p, $[K : \mathbb{Q}] = p^m$, que sólo ramifica en un primo $\ell \neq p$.*

Entonces, $\ell \equiv 1 \pmod{p^m}$*, la extensión* $K|\mathbb{Q}$ *es totalmente ramificada en* ℓ*, y* K *es el único subcuerpo de* $\mathbb{Q}(\zeta_\ell)$ *de grado* p^m*. En consecuencia, también, la extensión* $K|\mathbb{Q}$ *es cíclica.*

DEMOSTRACIÓN: Para la primera parte, podemos suponer que la extensión $K|\mathbb{Q}$ es cíclica de grado potencia de un número primo p. Sea ℓ un primo diferente de p que ramifica; acabamos de probar que $\ell \equiv 1 \pmod{p^m}$. Además, las extensiones $K|\mathbb{Q}$ y $L|\mathbb{Q}$ de la discusión anterior sólo ramifican en el primo ℓ; por tanto, la extensión $K'|\mathbb{Q}$ es no ramificada en todo primo; puesto que todo cuerpo de números $K' \neq \mathbb{Q}$ ramifica en algún primo, ha de ser $K' = \mathbb{Q}$; en consecuencia, $K \subseteq KL = K'L = L$ y L es el único subcuerpo de grado p^m de $\mathbb{Q}(\zeta_\ell)$. El final es claro; si no suponemos que la extensión $K|\mathbb{Q}$ es cíclica, podemos considerar K como la composición de extensiones cíclicas; cada una de ellas es un subcuerpo de $\mathbb{Q}(\zeta_\ell)$ de manera que K también. Puesto que la extensión $\mathbb{Q}(\zeta_\ell)|\mathbb{Q}$ es cíclica, hemos acabado. □

Corolario 6.1.4. *Sea* $K|\mathbb{Q}$ *una extensión abeliana y moderadamente ramificada en todos los ideales primos. Entonces, existe una raíz de la unidad* ζ *y* $K \subseteq \mathbb{Q}(\zeta)$*.*

DEMOSTRACIÓN: En virtud de la proposición 6.1.2, podem suposar que la extensión $K|\mathbb{Q}$ es cíclica. Por otro lado, la reducción sucessiva de K a K' en la discusión precedente a la proposición anterior permite suponer que el cuerpo K sólo ramifica en un ideal primo; y, en este caso, la proposición anterior acaba la prueba. □

Observación 6.1.5. En particular, si $K|\mathbb{Q}$ es una extensión abeliana, $\ell_1, \ldots, \ell_k$ los primos que ramifican, y si el grado de la extensión no es divisible por ninguno de los primos ℓ_i, entonces el cuerpo K es un subcuerpo del cuerpo ciclotómico $\mathbb{Q}(\zeta)$, donde ζ es una raíz n-ésima de la unidad para $n = \ell_1 \cdots \ell_k$.

6.2. El caso cíclico de grado potencia de un primo impar

Hemos visto que para establecer el teorema de Kronecker-Weber es suficiente demostrarlo para el caso de las extencions cíclicas de grado potencia de un número primo p y que sólo ramifican en p. Se trata de verlo en el caso

en que p es un primo impar. Necesitaremos el resultado siguiente en hipótesis más generales.

Proposición 6.2.1. *Sean p un número primo impar y $K|\mathbb{Q}$ una extensión abeliana de grado p^m que sólo ramifique en el primo p. Entonces, $K|\mathbb{Q}$ es totalmente ramificada en p y cíclica.*

DEMOSTRACIÓN: Sean $\mathfrak{P}$ un ideal primo del anillo de los enteros de K que divide p i $I := G_0(\mathfrak{P}|p)$ el grupo de inercia. El cuerpo fijo por I es un cuerpo extensión de $\mathbb{Q}$ que no ramifica en ningún ideal primo; por tanto, en virtud del teorema de Hermite-Minkowski $K^I = \mathbb{Q}$ y la extensión $K|\mathbb{Q}$ es totalmente ramificada en p; dicho de otra manera, el grupo de inercia es todo el grupo de Galois de la extensión. En particular, la extensión residual es trivial y el cuerpo residual de K en $\mathfrak{P}$ es $\mathbb{F}_p$. Puesto que conocemos la estructura de los cocientes sucesivos de los grupos de ramificación, podemos asegurar que el grupo de inercia coincide con el grupo de ramificación G_1, y que para todo número entero $k \geq 1$ el cociente G_k/G_{k+1} es un grupo abeliano trivial o cíclico de orden p. Por tanto, la extensión es totalmente ramificada en p. Para ver que la extensión es cíclica se trata de aplicar el resultado siguiente.

Lema 6.2.2. *Supongamos que $K|\mathbb{Q}$ es una extensión abeliana de grado p que sólo ramifica en p; entonces, el grupo de ramificación $G_2(\mathfrak{P}|p)$ es trivial.*

DEMOSTRACIÓN: Si localizamos en $S := \mathbb{Z} - p\mathbb{Z}$ podemos suponer que $\mathfrak{P}$ es un ideal principal, y podemos elegir un generador π de $\mathfrak{P}$. Sea $f(X) := \mathrm{Irr}(\pi, \mathbb{Q})$ el polinomio mónico irreducible de $\mathbb{Q}[X]$ que tiene π por raíz; de hecho, puesto que π es entero sobre $S^{-1}\mathbb{Z}$, $f(X) \in S^{-1}\mathbb{Z}[X]$. Puesto que la cadena de los grupos de ramificación es trivial a partir de un lugar en adelante, podemos considerar un número entero k tal que $G_k \neq (1)$ pero $G_{k+1} = (1)$; y puesto que $G_0 = G_1 \simeq \mathbb{Z}/p\mathbb{Z}$, ha de ser $k \geq 1$. Se trata de ver que $k = 1$.

Si consideramos la derivada en π del polinomio $f(X)$ obtenemos las relaciones $f'(\pi) \in \mathfrak{P}^{(k+1)(p-1)}$ y $f'(\pi) \notin \mathfrak{P}^{(k+1)(p-1)+1}$. En efecto, podemos escribir $f(X) = \prod_{\sigma \in G_k} (X - \sigma(\pi))$, de manera que $f'(\pi)$ es el producto $f'(\pi) = \prod_{\sigma \neq 1}(\pi - \sigma(\pi))$; pero puesto que $\sigma \in G_k$ y $\sigma \notin G_{k+1}$, ha de ser $b - \sigma(b) \in \mathfrak{P}^{k+1}$ para todo elemento b entero de K sobre $S^{-1}\mathbb{Z}$; en particular, $\pi - \sigma(\pi) \in \mathfrak{P}^{k+1}$;

por otro lado, $\pi - \sigma(\pi) \notin \mathfrak{P}^{k+2}$, ya que en este caso, obtendríamos que $\sigma \in G_{k+1}$ como en la demostración de la proposición 5.6.5. Ahora basta multiplicar por todos los automorfismos $\sigma \in G_k$, $\sigma \neq 1$. Por otro lado, podemos escribir una igualdad de la forma

$$f'(\pi) = p\pi^{p-1} + (p-1)a_{p-1}\pi^{p-2} + \cdots + 2a_2\pi + a_1,$$

donde los coeficientes a_j son elementos de $S^{-1}\mathbb{Z}$; es decir, son números racionales que tienen denominadores enteros no divisibles por p. Puesto que la extensión $K|\mathbb{Q}$ es totalmente ramificada y de grado p, la extensión de p es el ideal $\mathfrak{P}^p$, de manera que cada uno de los coeficientes a_j que sean no nulos es un elemento de una potencia $\mathfrak{P}^{pn_j}$ con $n_j \geq 0$. En particular, si v_j denota el exponente de $\mathfrak{P}$ que contiene el sumando $ya_j\pi^{j-1}$ pero tal que $ya_j\pi^{j-1} \notin \mathfrak{P}^{v_j+1}$, obtenemos que $v_j \equiv j-1 \pmod{p}$; en consecuencia, todos los sumandos no nulos están en potencias diferentes de $\mathfrak{P}$ y la suma está en la potencia que tiene el exponente v_j menor. En particular, obtenemos la desigualdad $(k+1)(p-1) \leq v_{p-1} = 2p-1$; puesto que $k \geq 1$ y $p > 2$, esto implica que $k = 1$, de manera que $G_2 = (1)$, como queríamos probar. □

Para hacer la demostración de la proposición, sabemos que $G = G_0 = G_1$; sea $k \geq 2$ tal que $G = G_k$ pero $G_{k+1} \subsetneq G_k$; el cociente G_k/G_{k+1} es un grupo abeliano cíclico de orden p. Puesto que G es un p-grupo abeliano finito, si no fuese cíclico debería tener más de dos subgrupos de índice p (como mínimo, habría de tener $p+1$); por tanto, es suficiente probar que G_{k+1} es el único subgrupo de G de índice p.

Supongamos que H fuese un subgrupo de índice p de G diferente de G_{k+1}; se trata de llegar a contradicción. Para ello, consideremos los cuerpos fijos K^H y $K^{G_{k+1}}$ y sean $\mathfrak{P}_H$ y $\mathfrak{P}_{k+1}$ las contracciones a estos cuerpos del ideal primo $\mathfrak{P}$ del anillo de los enteros de K. El cálculo de los grupos de ramificación de $\mathfrak{P}$ para estas extensiones se puede hacer de manera sencilla. Puesto que $\mathrm{Gal}\left(K|K^{G_{k+1}}\right) = G_{k+1}$, obtenemos las igualdades

$$G_i(\mathfrak{P}|\mathfrak{P}_{k+1}) = \begin{cases} G_i \cap G_{k+1} = G_{k+1} & \text{si } 0 \leq i \leq k+1, \\ G_i \cap G_{k+1} = G_i & \text{si } i > k+1; \end{cases}$$

$$G_i(\mathfrak{P}|\mathfrak{P}_H) = \begin{cases} G_i \cap H = H & \text{si } 0 \leq i \leq k, \\ G_i \cap H \subsetneq G_{k+1} & \text{si } i \geq k+1, \end{cases}$$

esta última igualdad porque $H \neq G_{k+1}$ y ambos son subgrupos de índice p de G. Estos cálculos nos permiten comparar los exponentes de $\mathfrak{P}$ en los

diferentes de las extensiones $K|K^H$ y $K|K^{G_{k+1}}$ de la manera siguiente:

$$\sum_{i\geq 0}(\#G_i \cap H - 1) < \sum_{i\geq 0}(\#G_i \cap G_{k+1} - 1),$$

ya que los k primeros sumandos son iguales, el $k+1$-ésimo satisface la desigualdad estricta, y los siguientes satisfacen la desigualdad $\leq$.

Por otro lado, el lema nos permite asegurar que el exponente del diferente de las extensiones $K^H|\mathbb{Q}$ y $K^{G_{k+1}}|\mathbb{Q}$ es el mismo, ya que los grupos G_0 y G_1 de las dos extensiones son cíclicos de orden p y los grupos G_2 son triviales. Si ahora consideramos el diferente de la extensión $K|\mathbb{Q}$ y calculamos el exponente de $\mathfrak{P}$ en esta extensión utilizando la fórmula de la transitividad del diferente para cadenas de extensiones obtenemos una contradicción, ya que la extensión a K de los ideales $\mathfrak{P}_H$ y $\mathfrak{P}_{k+1}$ es exactamente la misma, $\mathfrak{P}^{p^{m-1}}$, porque las extensiones son totalmente ramificadas de grado p^{m-1}. En consecuencia, ha de ser $H = G_{k+1}$ y G es cíclico. □

Proposición 6.2.3. *Sean p un primo impar y $K|\mathbb{Q}$ una extensión cíclica de grado p^m que sólo ramifique en p. Entonces, K es el único subcuerpo de $\mathbb{Q}(\zeta)$ de grado p^m, donde ζ es una raíz primitiva p^{m+1}-ésima de la unidad.*

Demostración: En efecto, sea K' el único subcuerpo de $\mathbb{Q}(\zeta)$ de grado p^m; entonces, las dos extensiones $K|\mathbb{Q}$ y $K'|\mathbb{Q}$ satisfacen las condiciones del enunciado; es decir, son cíclicas de grado p^m y sólo ramifican en p; por tanto, el cuerpo composición KK' es un cuerpo extensión abeliana de $\mathbb{Q}$ que sólo ramifica en p y de grado potencia de p; en virtud de la proposición anterior, ha de ser cíclico y de grado potencia de p; puesto que contiene dos cuerpos K y K' que tienen el mismo grado sobre $\mathbb{Q}$, ha de ser $K = K'$, como queríamos ver. □

6.3. El caso cíclico de grado potencia de 2

Hemos reducido la demostración del teorema de Kronecker-Weber al caso de las extensiones cíclicas de grado potencia de 2 que sólo ramifiquen en 2. Para acabar la prueba, comencemos por demostrar el resultado siguiente.

Proposición 6.3.1. *Sea $K|\mathbb{Q}$ una extensión abeliana de grado 2^m que sólo ramifique en 2 y supongamos que $K \subseteq \mathbb{R}$. Entonces, K es exactamente el*

subcuerpo real maximal $\mathbb{Q}(\zeta+\zeta^{-1})$ *del cuerpo* $\mathbb{Q}(\zeta)$*, donde* ζ *es una raíz primitiva* 2^{m+2}*-ésima de la unidad.*

Demostración: Sabemos que toda extensión cuadrática de $\mathbb{Q}$ es ciclotómica y que si sólo ramifica en 2 es uno de los tres cuerpos $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, o $\mathbb{Q}(\sqrt{-2})$, que son los tres únicos subcuerpos cuadráticos de $\mathbb{Q}(\zeta)$, donde ζ es una raíz primitiva $8=2^3$-ésima de la unidad; por tanto, el resultado es claro en el caso $m=1$, ya que $\mathbb{Q}(\sqrt{2})$ es el único de estos cuerpos que es real.

Supongamos, pues, que $m\geq 2$. Puesto que $K|\mathbb{Q}$ es abeliana de grado divisible por 2, K contiene un subcuerpo cuadrático; el hecho que el cuerpo K sea real y que la extensión $K|\mathbb{Q}$ sólo ramifique en 2 impone las mismas restricciones a este subcuerpo cuadrático; por tanto, K contiene el único cuerpo cuadrático real que sólo ramifica en 2. Esto implica que el grupo de Galois de la extensión $K|\mathbb{Q}$ sólo tiene un subgrupo de índice 2 y, en consecuencia, es cíclico.

Comparemos el cuerpo K con el cuerpo $L:=\mathbb{Q}(\zeta+\zeta^{-1})$. El cuerpo composición KL es un cuerpo real y la extensión $KL|\mathbb{Q}$ es abeliana, no ramificada fuera de 2 y de grado potencia de 2; acabamos de probar que la extensión $KL|\mathbb{Q}$ es cíclica; puesto que contiene K y L, que son del mismo grado sobre $\mathbb{Q}$, ha de ser $K=L$, como queríamos demostrar. □

Ahora podemos acabar la demostración del teorema de Kronecker-Weber.

Proposición 6.3.2. *Sea* $K|\mathbb{Q}$ *una extensión abeliana de grado* 2^m *y no ramificada fuera de* 2*. Entonces,* K *es uno de los tres subcuerpos* $\mathbb{Q}(\zeta^2)$*,* $\mathbb{Q}(\zeta+\zeta^{-1})$*,* $\mathbb{Q}(\zeta-\zeta^{-1})$ *del cuerpo ciclotómico* $\mathbb{Q}(\zeta)$*, donde* ζ *es una raíz primitiva* 2^{m+2}*-ésima de la unidad. Estos cuerpos son los únicos subcuerpos de* $\mathbb{Q}(\zeta)$ *de grado* 2^m *sobre* $\mathbb{Q}$*.*

Demostración: En efecto, el cuerpo composición de K y $\mathbb{Q}(i)$, $K(i)$, es un cuerpo extensión abeliana de $\mathbb{Q}$, no ramificada fuera de 2, y de grado potencia de 2, 2^n, con $n\leq m+1$. Sea $K(i)^+:=K(i)\cap\mathbb{R}$, el subcuerpo real maximal de $K(i)$; es un cuerpo real, no ramificado fuera de 2, y de grado 2^s, $s\leq n-1\leq m$, ya que $i\notin K(i)^+$; por tanto, $K(i)^+$ es subcuerpo de $\mathbb{Q}(\zeta+\zeta^{-1})$, que es el único cuerpo real que satisface estas condiciones. Para acabar, es suficiente demostrar que $K(i)$ es el cuerpo $K(i)^+(i)$ que, claramente, es un subcuerpo de $\mathbb{Q}(\zeta+\zeta^{-1})(i)=\mathbb{Q}(\zeta)$. Pero $K(i)^+(i)\subseteq K(i)$ y los dos cuerpos son de grado 2 sobre $K(i)^+$; por tanto, coinciden. □

6.4. Conductor de una extensión abeliana de $\mathbb{Q}$

Sea $K|\mathbb{Q}$ una extensión abeliana. El teorema de Kronecker-Weber nos permite asegurar la existencia de una raíz de la unidad ζ tal que $K \subseteq \mathbb{Q}(\zeta)$.

Definición 6.4.1. Se llama conductor de una extensión abeliana $K|\mathbb{Q}$ el menor entero positivo n tal que $K \subseteq \mathbb{Q}(\zeta_n)$, donde ζ_n es una raíz primitiva n-ésima de la unidad.

Observación 6.4.2. Si n es impar, entonces $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$, de manera que el conductor de una extensión abeliana de $\mathbb{Q}$ es un número natural $n \not\equiv 2 \pmod 4$.

El teorema de Kronecker-Weber admite una formulación más precisa. En efecto, podemos establecder fácilmente el resultado siguiente.

Teorema 6.4.3. (Kronecker-Weber) *Sea $K|\mathbb{Q}$ una extensión abeliana. Sean $p_1, p_2, \ldots, p_k$ los primos de $\mathbb{Z}$ que ramifican en K y pongamos $e_i := p_i^{r_i} e_i'$, con e_i' no divisible por p_i, el índice de ramificación de p_i, $1 \leq i \leq k$, en la extensión $K|\mathbb{Q}$. Entonces, el conductor n de K es dado por*

$$n = \begin{cases} p_1^{r_1+1} p_2^{r_2+1} \cdots p_k^{r_k+1}, & \text{si } p_i \neq 2 \text{ para todo índice } i, \\ 2^{\varepsilon} p_1^{r_1+1} p_2^{r_2+1} \cdots p_k^{r_k+1}, & \text{si } p_1 = 2, \end{cases}$$

donde $\varepsilon \in \{0, 1\}$.

Demostración: De hecho, este resultado está incluído en la sucesión de reducciones que hemos hecho de la prueba del teorema. En efecto, la reducción al caso de extensiones cíclicas de grado potencia de un primo se ha hecho tomando como conductor de K el mínimo común múltiplo de los conductores de los factores cíclicos; por otro lado, la reducción al caso salvajemente ramificado sólo añade una raíz $p_1 p_2 \cdots p_k$-ésima de la unidad, como máximo. Finalmente, en el caso $K|\mathbb{Q}$ cíclica, de grado potencia de p, y no ramificada fuera de p, hemos tomado una raíz primitiva p^{r+1}-ésima de la unidad, si $p \neq 2$, y $2^{r+2} = 2 \cdot 2^{r+1}$-ésima, si $p = 2$. Por tanto, el valor n dado en el enunciado es un múltiplo del conductor.

Por otro lado, si $m = p_1^{r_1} p_2^{r_2+1} \cdots p_k^{r_k+1}$, el índice de ramificación de p_1 en la extensión $\mathbb{Q}(\zeta_m)|\mathbb{Q}$ no es divisible por $p_1^{r_1}$, de manera que el conductor de K ha de ser divisible por $p_i^{r_i+1}$ para todo primo p_i que ramifique en K. □

El valor de ε se puede determinar en cada caso a partir de la sucesión de subcuerpos K' que se obtienen por el procedimiento descrito justo antes de la proposición 6.1.3. Sólo hay que notar que si ζ es una raíz primitiva 2^{m+2}-ésima de la unidad, y si $K = \mathbb{Q}(\zeta^2)$, entonces $\varepsilon = 0$, mientras que si $K = \mathbb{Q}(\zeta + \zeta^{-1})$ o $K = \mathbb{Q}(\zeta - \zeta^{-1})$, entonces $\varepsilon = 1$.

Corolario 6.4.4. *Sean $K|\mathbb{Q}$ una extensión abeliana, n su conductor, y ζ una raíz primitiva n-ésima de la unidad. Entonces, la extensión $\mathbb{Q}(\zeta)|K$ es moderadamente ramificada en todos los ideales primos del anillo de los enteros de K.*

Demostración: La potencia de un número primo p que divide el índice de ramificación $e_p(\mathbb{Q}(\zeta)|\mathbb{Q})$ es exactamente la misma que divide $e_p(K|\mathbb{Q})$; por tanto, si $\mathfrak{p}$ es un ideal primo del anillo de los enteros de K que divide p, el índice de ramificación de $\mathfrak{p}$ en $\mathbb{Q}(\zeta)|K$ no es divisible por p. □

Observación 6.4.5. Si K es un cuerpo de números y $L|K$ es una extensión abeliana, no es cierto en general que $L \subseteq K(\zeta)$ para ninguna raíz de la unidad ζ.

En efecto, consideremos el cuerpo $\mathbb{Q}(\alpha)$, donde $\alpha^3 - \alpha + 1 = 0$ y sea $K := \mathbb{Q}(\sqrt{-23})$. La extensión $K(\alpha)|K$ es cíclica de grado 3 y no ramifica en ningún ideal primo de K; pero $K(\alpha)$ no puede estar incluído en ningún cuerpo $K(\zeta)$ para raíces de la unidad ζ, ya que por ser $K \subseteq \mathbb{Q}(\zeta_{23})$, obtendríamos que $\mathbb{Q}(\alpha)$ sería un subcuerpo de $\mathbb{Q}(\zeta, \zeta_{23})$, de manera que $\mathbb{Q}(\alpha)|\mathbb{Q}$ sería una extensión abeliana; pero $\mathbb{Q}(\alpha)|\mathbb{Q}$ no es ni tan solo de Galois.

Capítulo 7

Ramificación en el caso infinito

El objetivo de este capítulo es hacer un resumen de las propiedades de la ramificación y escribirlas sin la hipótesis de finitud de las extensiones. Para ello, hemos de situarnos en el caso galoisiano y hay que repasar, en primer lugar, la teoría de Galois en el caso general, no necesariamente finito.

7.1. Teoría de Galois

Sea $L|K$ una extensión algebraica, no necesariamente finita, de cuerpos. Entonces, el cuerpo L es el límite inductivo (si se quiere, la reunión conjuntista) de todos los subcuerpos $K' \subseteq L$ tales que $K'|K$ es una extensión finita.

Definición 7.1.1. Se dice que la extensión $L|K$ es una extensión de Galois si es normal y separable.

En este caso, las extensiones de Galois finitas $K'|K$ tales que $K' \subseteq L$ forman un sistema cofinal del sistema de todas las subextensiones finitas de $L|K$; por tanto, el cuerpo L también es el límite inductivo de los subcuerpos $K' \subseteq L$ tales que $K'|K$ es una subextensión de Galois finita de $L|K$. Además, el grupo de Galois $\mathrm{Gal}\,(L|K)$ es el límite proyectivo de los grupos de Galois $\mathrm{Gal}\,(K'|K)$ para las subextensiones de Galois finitas $K'|K$ de $L|K$. Es decir, $\mathrm{Gal}\,(L|K)$ es un grupo profinito; por tanto, un grupo topológico que admite una base de entornos del elemento neutro formada por los grupos de Galois

$\mathrm{Gal}\,(L|K')$ donde $K'|K$ describe el conjunto de las subextensiones de Galois finitas de $L|K$. Los grupos $\mathrm{Gal}\,(L|K')$ son subgrupos normales de $\mathrm{Gal}\,(L|K)$. En particular, $\mathrm{Gal}\,(L|K)$ es un grupo topológico Hausdorff y compacto.

Recordemos el teorema fundamental de la teoría de Galois.

Teorema 7.1.2. *Sea $L|K$ una extensión de Galois cualquiera de cuerpos. Existe una aplicación biyectiva entre el conjunto de los subgrupos cerrados H de $\mathrm{Gal}\,(L|K)$ y el conjunto de los subcuerpos L' de L que contienen K dada por la asignación*

$$H \mapsto L' := L^H$$

con inversa dada por

$$L' \mapsto \mathrm{Gal}\,(L|L')\,.$$

Los subgrupos abiertos H se corresponden con los subcuerpos L' tales que la extensión $L'|K$ es finita. □

Ejemplo 7.1.3. El grupo de Galois absoluto de un cuerpo finito

Consideremos un cuerpo finito $K := \mathbb{F}_q$ de cardinal q y característica p. Es bien conocido que para todo número entero $n \geq 1$ el cuerpo $\mathbb{F}_q$ tiene una y sólo una extensión de grado n en una clausura algebraica fija $L := \overline{\mathbb{F}}_p$ de $\mathbb{F}_q$; es el cuerpo $\mathbb{F}_{q^n}$ formado por 0 y las raíces $(q^n - 1)$-ésimas de la unidad de $\overline{\mathbb{F}}_q$. En particular, la extensión $\mathbb{F}_{q^n}|\mathbb{F}_q$ es una extensión cíclica de grado n, generada por el automorfismo de Frobenius, $x \mapsto x^q$, de $\mathbb{F}_{q^n}$.

Por otro lado, esta misma asignación, para $x \in \overline{\mathbb{F}}_q$, define un elemento Frob_q de $\mathrm{Gal}\left(\overline{\mathbb{F}}_q|\mathbb{F}_q\right)$; se llama el automorfismo de Frobenius de la extensión $\overline{\mathbb{F}}_q|\mathbb{F}_q$. La restricción de Frob_q a $\mathbb{F}_{q^n}$ es el automorfismo de Frobenius de la extensión $\mathbb{F}_{q^n}|\mathbb{F}_q$. El cuerpo fijo por el subgrupo de $\mathrm{Gal}\left(\overline{\mathbb{F}}_q|\mathbb{F}_q\right)$ generado por Frob_q es el cuerpo $\mathbb{F}_q$, de manera que la adherencia de este subgrupo es todo el grupo de Galois. Dicho de otra manera, el grupo $\mathrm{Gal}\left(\overline{\mathbb{F}}_q|\mathbb{F}_q\right)$ es generado topológicamente por un sólo elemento, Frob_q.

Esto nos dice que el grupo de Galois $\mathrm{Gal}\left(\overline{\mathbb{F}}_q|\mathbb{F}_q\right)$ es (isomorfo a) el límite proyectivo de los grupos $\mathbb{Z}/n\mathbb{Z}$; es decir, $\mathrm{Gal}\left(\overline{\mathbb{F}}_q|\mathbb{F}_q\right) \simeq \widehat{\mathbb{Z}}$, la completación profinita de $\mathbb{Z}$.

Ejemplo 7.1.4. Fijemos un número primo impar p y, para todo número entero $n \geq 1$, consideremos una raíz primitiva p^n-ésima de la unidad, $\eta_n := \zeta_{p^n}$. Sea $K_n := \mathbb{Q}(\eta_n)$ y pongamos $L := K_\infty$ el cuerpo reunión de los cuerpos K_n.

El grupo de Galois de cada una de les extensiones $K_n|\mathbb{Q}$ es un grupo cíclico de orden $(p-1)p^{n-1}$ generado por un automorfismo de K_n determinado unívocamente por su acción sobre η_n. Además, η_{n+1}^p es un elemento primitivo de la extensión $K_n|\mathbb{Q}$, de manera que el morfismo natural dado por restricción,

$$\mathrm{Gal}\,(K_{n+1}|\mathbb{Q}) \longrightarrow \mathrm{Gal}\,(K_n|\mathbb{Q})\,,$$

aplica un generador en un generador. En consecuencia, el grupo de Galois de la extensión $K_\infty|\mathbb{Q}$ es isomorfo al límite proyectivo de los grupos abelianos $(\mathbb{Z}/p^{n+1}\mathbb{Z})^* \simeq \mathbb{Z}/p^n\mathbb{Z}\times\mathbb{Z}/(p-1)\mathbb{Z}$; es decir, es isomorfo al grupo abeliano ${\mathbb{Z}_p}^*$ formado por los elementos inversibles del anillo $\mathbb{Z}_p$, límite proyectivo de los anillos $\mathbb{Z}/p^{n+1}\mathbb{Z}$. Dicho de otra manera, $\mathrm{Gal}\,(K_\infty|\mathbb{Q})$ es isomorfo al producto cartesiano $\mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$.

En estos ejemplos se observa que el cuerpo L es el límite inductivo de una familia numerable de subcuerpos $K' \subseteq L$ tales que $K'|K$ es una extensión finita. Aún más, en estos ejemplos se puede demostrar que L es la reunión de una sucesión numerable de tales subcuerpos. Pero esto no es cierto en general; por ejemplo, podemos considerar una cantidad no numerable de elementos algebraicamente independientes X_i sobre un cuerpo k y formar el cuerpo de fracciones K del anillo de polinomios en estas indeterminadas y coeficientes en k. Se trata de ver que si L es una clausura algebraica de K, entonces no existe ninguna familia numerable de subcuerpos $K_n \subseteq L$ tales que $K_n|K$ sea una extensión finita y L sea el límite inductivo de la familia de cuerpos K_n. Por ejemplo, este es el caso si tomamos $k = \mathbb{Q}$ y $L = \mathbb{C}$.

En efecto, el límite inductivo de una familia numerable de extensiones finitamente generadas de un cuerpo K es un cuerpo numerablemente generado sobre K, mientras que la extensión $L|K$ no puede ser numerablemente generada ya que ha de contener todas las raíces m-ésimas de todas las indeterminadas X_i para todos los números enteros $m \geq 2$, y éstas generan una subextensión de L que no es numerablemente generada sobre K.

Esta observación hará que, a partir de ahora, restrinjamos el estudio a situaciones más llanas.

7.2. Grupos de descomposición y de inercia

Sean A un dominio íntegramente cerrado de dimensión 1, K su cuerpo de fracciones, $L|K$ una extensión de Galois, no necesariamente finita, y B la clausura entera de A en L. En particular, B es un dominio de integridad íntegramente cerrado y de dimensión 1, ya que es una extensión entera de un anillo de dimensión 1. En general, sin embargo, y aunque A sea un anillo de Dedekind, B puede no ser un anillo de Dedekind. Para ver esto, daremos un ejemplo concreto.

Fijemos un número primo p y consideremos, para todo número entero $n \geq 1$, una raíz primitiva p^n-ésima de la unidad, η_n, la sucesión de cuerpos $K_n := \mathbb{Q}(\eta_n)$, y pongamos K_∞ la reunión de esta cadena de cuerpos. El anillo de los enteros de cada uno de los cuerpos $\mathbb{Q}(\eta_n)$ es el anillo $A_n := \mathbb{Z}[\eta_n]$ y la clausura entera de $\mathbb{Z}$ en K_∞ es el anillo A_∞, reunión de los anillos A_n. Por otro lado, sea $\mathfrak{P}_n$ el ideal de A_n generado por el elemento $1 - \eta_n$; es el único ideal primo de A_n que divide p. El ideal $\mathfrak{P}_\infty$ de A_∞ generado por todos los elementos $1-\eta_n$ es, pues, la reunión de todos los ideales $\mathfrak{P}_n$; en consecuencia, $\mathfrak{P}_\infty$ no es el ideal total de A_∞ y es un ideal maximal con cuerpo residual $\mathbb{F}_p$, que es el cuerpo residual de $\mathfrak{P}_n$ en A_n para todo n. Ahora bien, el ideal primo $\mathfrak{P}_\infty$ coincide con su potencia p-ésima, ya que el ideal generado por $1 - \eta_n$ es la potencia p-ésima del ideal generado por $1 - \eta_{n+1}$ en el anillo A_{n+1}. En consecuencia, en A_∞ no hay descomposición única de los ideales como producto de ideales primos no nulos y A_∞ no puede ser un anillo de Dedekind.

Volvamos a la situación general. A pesar de que los anillos A y B no sean anillos de Dedekind, dado un ideal primo no nulo $\mathfrak{P} \subseteq B$, si ponemos $\mathfrak{p} := \mathfrak{P} \cap A$ su contracción a A, el ideal $\mathfrak{p}$ es un ideal primo no nulo de A y podemos, aún, definir los grupos de descomposición y de inercia de $\mathfrak{P}$ sobre $\mathfrak{p}$ por las fórmulas

$$G_{-1}(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in \mathrm{Gal}\,(L|K) : \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

$$G_0(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in G_{-1}(\mathfrak{P}|\mathfrak{p}) : \sigma \text{ actúa trivialmente en el cociente } B/\mathfrak{P}\}.$$

En particular, esta definición se aplica en el caso en que el anillo A es la clausura entera de $\mathbb{Z}$ en un cuerpo extensión algebraica de $\mathbb{Q}$, no necesariamente finita, y también en el caso de un anillo simetrizado de este anillo respecto de cualquier sistema multiplicativamente cerrado. Estas situaciones son las que nos interesan de manera especial.

A partir de ahora, y para lo que resta de este capítulo, dada una extensión de Galois $L|K$ de manera que K es el cuerpo de fracciones de un dominio íntegramente cerrado de dimensión 1, supondremos que la extensión $L|K$ se puede escribir como el límite inductivo de una familia numerable de subextensiones finitas $K'|K$ de $L|K$. En este caso, podemos elegir una sucesión (numerable) de subextensiones de Galois finitas $K_n|K$ de $L|K$ tales que para todo número natural n es $K_n \subseteq K_{n+1}$ y el cuerpo L es la reunión de la cadena de cuerpos K_n; en particular, esto lo podremos hacer siempre que el cuerpo L sea numerable; por ejemplo, un cuerpo de números algebraicos, no necesariamente finito sobre $\mathbb{Q}$.

Igual que en el caso finito, podemos escribir el resultado siguiente.

Lema 7.2.1. *Sea $\mathfrak{p}$ un ideal primo cualquiera del anillo A. Entonces, el grupo de Galois $\mathrm{Gal}\,(L|K)$ actúa transitivamente en el conjunto de los ideales primos $\mathfrak{P}$ de B que dividen $\mathfrak{p}$; es decir, tales que $\mathfrak{P} \cap A = \mathfrak{p}$.*

Demostración: Sean $\mathfrak{P}, \mathfrak{P}' \subseteq B$ ideales primos de B que tengan la misma contracción a A, $\mathfrak{p} := \mathfrak{P} \cap A = \mathfrak{P}' \cap A$. Elijamos una sucesión de subextensiones de Galois finitas $K_n|K$ de $L|K$ tales que $K_0 = K$, $K_n \subseteq K_{n+1}$ para todo $n \geq 0$, y $L = \bigcup_{n\geq 0} K_n$; para todo número entero $n \geq 0$ denotemos por A_n la clausura entera de A en K_n y sean $\mathfrak{P}_n := \mathfrak{P} \cap A_n$ y $\mathfrak{P}'_n := \mathfrak{P}' \cap A_n$ las contracciones de $\mathfrak{P}$ y $\mathfrak{P}'$ al anillo A_n. Puesto que la extensión $K_n|K$ es de Galois finita, existe $\sigma_n \in \mathrm{Gal}\,(K_n|K)$ tal que $\sigma_n(\mathfrak{P}_n) = \mathfrak{P}'_n$; ésto se ha enunciado en el capítulo tercero con la hipótesis suplementaria que el anillo A es de Dedekind, pero esta hipótesis no se ha utilizado; de hecho, sólo se ha utilizado que el anillo A es un dominio íntegramente cerrado. Si demostramos que podemos elegir esta sucesión de manera que cada σ_n sea la restricción de σ_{n+1} al cuerpo K_n ya habremos acabado; en efecto, en este caso, existe un automorfismo $\sigma \in \mathrm{Gal}\,(L|K)$ tal que la restricción de σ a cada uno de los cuerpos K_n es el automorfismo σ_n, ya que $\mathrm{Gal}\,(L|K)$ es el límite proyectivo de los grupos de Galois $\mathrm{Gal}\,(K_n|K)$; entonces, el ideal primo de B, $\sigma(\mathfrak{P})$, es la reunión de los ideales $\mathfrak{P}'_n = \sigma_n(\mathfrak{P}_n)$; por tanto, $\sigma(\mathfrak{P}) = \mathfrak{P}'$, como había que demostrar.

Veamos, pues, que podemos elegir los automorfismos σ_n de manera que la restricción de σ_{n+1} al cuerpo K_n sea el automorfismo σ_n y que $\sigma_{n+1}(\mathfrak{P}_{n+1}) = \mathfrak{P}'_{n+1}$. Para ello, dado σ_n, sea $\tau_{n+1} \in \mathrm{Gal}\,(K_{n+1}|K)$ una extensión cualquiera de σ_n al cuerpo K_{n+1}; entonces, τ_{n+1} transforma el ideal primo $\mathfrak{P}_{n+1}$ en un

cierto ideal primo $\tau_{n+1}(\mathfrak{P}_{n+1})$ de A_{n+1}; puesto que $\tau_{n+1}(\mathfrak{P}_{n+1})$ y $\mathfrak{P}'_{n+1}$ son ideales primos de A_{n+1} que contraen al ideal primo $\mathfrak{P}'_n$ de A_n y la extensión $K_{n+1}|K_n$ es de Galois finita, existe un elemento $\rho_{n+1} \in \mathrm{Gal}\,(K_{n+1}|K_n)$ tal que $\rho_{n+1}(\tau_{n+1}(\mathfrak{P}_{n+1})) = \mathfrak{P}'_{n+1}$; entonces, podemos tomar $\sigma_{n+1} := \rho_{n+1} \circ \tau_{n+1} \in \mathrm{Gal}\,(K_{n+1}|K_n)$ y este automorfismo extiende σ_n, ya que τ_{n+1} lo extiende y ρ_{n+1} es la identidad en K_n, y manda el ideal $\mathfrak{P}_{n+1}$ al ideal $\mathfrak{P}'_{n+1}$; ésto es lo que había que demostrar. □

Proposición 7.2.2. *Sean A un dominio íntegramente cerrado de dimensión 1, K su cuerpo de fracciones, $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq K_{n+1} \subseteq \ldots$ una cadena de extensiones de Galois $K_n|K$, $L := \bigcup_{n\geq 0} K_n$ la reunión de la cadena, B la clausura entera de A en L, $\mathfrak{P} \subseteq B$ un ideal primo no nulo de B, y $\mathfrak{p} := \mathfrak{P} \cap A$ su contracción a A. Entonces:*

(i) la extensión residual $B/\mathfrak{P}|A/\mathfrak{p}$ es una extensión algebraica normal de cuerpos;

(ii) los grupos de descomposición y de inercia $G_{-1}(\mathfrak{P}|\mathfrak{p})$ y $G_0(\mathfrak{P}|\mathfrak{p})$ son subgrupos cerrados de $\mathrm{Gal}\,(L|K)$; y

(iii) la sucesión natural de morfismos de grupos topológicos

$$1 \longrightarrow G_0(\mathfrak{P}|\mathfrak{p}) \longrightarrow G_{-1}(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}\,(B/\mathfrak{P}|A/\mathfrak{p}) \longrightarrow 1$$

es exacta.

Demostración: Sean $A_n := B \cap K_n$ y $\mathfrak{P}_n := \mathfrak{P} \cap A_n$, para todo $n \geq 0$. Entonces, $B = \bigcup_{n\geq 0} A_n$, $\mathfrak{P} = \bigcup_{n\geq 0} \mathfrak{P}_n$, y $B/\mathfrak{P} = \bigcup_{n\geq 0}(A_n/\mathfrak{P}_n)$; en consecuencia, la extensión residual $B/\mathfrak{P}|A/\mathfrak{p}$ es algebraica y normal, el grupo de descomposición $G_{-1}(\mathfrak{P}|\mathfrak{p})$ es el límite proyectivo de los grupos de descomposición $G_{-1}(\mathfrak{P}_n|\mathfrak{p})$ y el grupo de inercia $G_0(\mathfrak{P}|\mathfrak{p})$ es el límite proyectivo de los grupos de inercia $G_0(\mathfrak{P}_n|\mathfrak{p})$; en particular, ambos son subgrupos cerrados de $\mathrm{Gal}\,(L|K)$. Por otro lado, disponemos de diagramas conmutativos con las filas exactas

$$\begin{array}{ccccccccc}
1 & \to & G_0(\mathfrak{P}_{n+1}|\mathfrak{p}) & \longrightarrow & G_{-1}(\mathfrak{P}_{n+1}|\mathfrak{p}) & \longrightarrow & \mathrm{Gal}\left(\dfrac{A_{n+1}}{\mathfrak{P}_{n+1}}|\dfrac{A}{\mathfrak{p}}\right) & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & G_0(\mathfrak{P}_n|\mathfrak{p}) & \longrightarrow & G_{-1}(\mathfrak{P}_n|\mathfrak{p}) & \longrightarrow & \mathrm{Gal}\left(\dfrac{A_n}{\mathfrak{P}_n}|\dfrac{A}{\mathfrak{p}}\right) & \to & 1,
\end{array}$$

donde los morfismos verticales son dados por restricción; por tanto, por paso al límite proyectivo, la sucesión

$$1 \longrightarrow G_0(\mathfrak{P}|\mathfrak{p}) \longrightarrow G_{-1}(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}\,(B/\mathfrak{P}|A/\mathfrak{p}) \longrightarrow 1$$

es exacta de grupos profinitos. □

Definición 7.2.3. Diremos que el ideal primo $\mathfrak{P}$ es no ramificado sobre su contracción $\mathfrak{p}$ si el grupo de inercia $G_0(\mathfrak{P}|\mathfrak{p})$ es trivial; eso equivale a decir que todos los ideales $\mathfrak{P}_n$ son no ramificados sobre $\mathfrak{p}$. Análogamente, diremos que $\mathfrak{P}$ es totalmente ramificado si el grupo de inercia $G_0(\mathfrak{P}|\mathfrak{p})$ es todo el grupo de Galois $\mathrm{Gal}\,(L|K)$; eso equivale a decir que los ideales primos $\mathfrak{P}_n$ son totalmente ramificados sobre $\mathfrak{p}$.

7.3. Extensiones abelianas no finitas de $\mathbb{Q}$

En esta sección nos situaremos en el caso en que el cuerpo base es el cuerpo $\mathbb{Q}$ de los números racionales. Se trata de resumir las propiedades de las extensiones abelianas de $\mathbb{Q}$.

Sea p un número primo y sea $\mu(p^\infty)$ el grupo de todas las raíces de la unidad de una clausura algebraica fija de $\mathbb{Q}$ que son de orden potencia de p. El cuerpo $\mathbb{Q}(\mu(p^\infty))$ es un cuerpo extensión abeliana de $\mathbb{Q}$ de grupo de Galois isomorfo al grupo abeliano

$$\begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \varprojlim \mathbb{Z}/p^n\mathbb{Z}, & \text{si } p \neq 2, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \varprojlim \mathbb{Z}/2^n\mathbb{Z}, & \text{si } p = 2. \end{cases}$$

Es una extensión totalmente ramificada en p y no ramificada fuera de p. De hecho, es el cuerpo extensión abeliana maximal de $\mathbb{Q}$ que es no ramificada fuera de p.

Más generalmente, si S es un conjunto cualquiera de números primos, el cuerpo composición $\mathbb{Q}_{ab}^S := \prod_{p \in S} \mathbb{Q}(\mu(p^\infty))$ es la extensión abeliana maximal de $\mathbb{Q}$ no ramificada en todo primo $\ell \notin S$; su grupo de Galois es isomorfo al producto de los grupos de Galois de las extensiones $\mathbb{Q}(\mu(p^\infty))|\mathbb{Q}$ para $p \in S$; es decir,

$$\mathrm{Gal}\left(\mathbb{Q}_{ab}^S|\mathbb{Q}\right) \simeq \begin{cases} \prod_{p\in S} \mathbb{Z}/(p-1)\mathbb{Z} \times \prod_{p\in S} \mathbb{Z}_p, & \text{si } 2 \notin S, \\ \mathbb{Z}/2\mathbb{Z} \times \prod_{p\in S} \mathbb{Z}/(p-1)\mathbb{Z} \times \prod_{p\in S} \mathbb{Z}_p, & \text{si } 2 \in S. \end{cases}$$

En general, pues, el grupo de Galois de la extensión abeliana maximal de $\mathbb{Q}$ no ramificada fuera de un conjunto fijado de primos no es un grupo finitamente generado, ya que los grupos $\mathbb{Z}_p$ no son grupos numerables; pero, en cambio, si S es finito, el grupo de Galois de la extensión $\mathbb{Q}_{ab}^S|\mathbb{Q}$ es un grupo topológico finitamente generado; en efecto, el producto de los grupos $\mathbb{Z}_p$ para $p \in S$ es un grupo procíclico (es decir, límite proyectivo de grupos cíclicos) y, en consecuencia, es generado topológicamente por un único elemento; en consecuencia, el número de generadores topológicos de $\mathrm{Gal}\left(\mathbb{Q}_{ab}^S|\mathbb{Q}\right)$ es $\leq \#S + 1$.

Más generalmente, dados un cuerpo de números K, extensión finita de $\mathbb{Q}$, y un conjunto finito S de ideales primos del anillo de los enteros de K, se puede hablar de la extensión maximal de K no ramificada fuera de S, $K^S|K$, y de la extensión abeliana maximal de K no ramificada fuera de S, $K_{ab}^S|K$; son extensiones de Galois del cuerpo K; nos podemos preguntar sobre la generación finita o no del grupo de Galois de estas extensiones. En general, no se conoce aún la respuesta a esta pregunta. De hecho, el grupo $G_S^{ab} := \mathrm{Gal}\left(K_{ab}^S|K\right)$ es el abelianizado del grupo $G_S := \mathrm{Gal}\left(K^S|K\right)$, de manera que el hecho de tener información sobre este último puede arrojar luz sobre qué sucede para G_S. Y en el caso en que el grupo G_S sea finitamente generado como grupo topológico, aún surge la cuestión de dar cotas buenas para el número de generadores; y mejor si estas cotas sólo dependen del cuerpo K y del cardinal del conjunto S. Esta pregunta es la que hemos respondido en el caso abeliano sobre $\mathbb{Q}$ para todo conjunto finito S de números primos.

Bibliografía

[A] Artin, Michael: *Algebra*. Prentice Hall, 1991. ISBN: 0-13-004763-5.

[A-M] Atiyah, Michael Francis; Macdonald, Ian Grant: *Introducción al álgebra conmutativa*. Traducción del original *Introduction to Commutative Algebra*. Reverté, Barcelona, 1973. ISBN: 84-291-5008-0.

[B-M-T] Bayer, Pilar; Montes, Jesús; Travesa, Artur: *Problemes d'Àlgebra*. Publicacions de la Universitat de Barcelona; col. Materials docents, n. 7. Barcelona, 1990. ISBN: 84-7875-361-3.

[Gr] Greenberg, Marvin: An elementary proof of the Kronecker-Weber theorem. *Amer. Math. Monthly* **81** (1974), p. 601-607; correction, **82** (1975), p. 803.

[Hi] Hilbert, David: *The Theory of Algebraic Nuber Fields*. Traducción inglesa del original *Die Theorie der algebraischen Zahlkörper*, conocido usualmente como el "Zahlbericht". Springer Verlag, Berlin, 1998. ISBN: 3-540-62779-0.

[Ja] Janusz, Gerald: *Algebraic Number Fields*. PAM 55, Academic Press, New York, 1973. ISBN: 0-12-380250-4.

[Kr] Kronecker, Leopoldt: Über die algebraisch auflösbaren Gleichungen. *Monatsber. K. Preuss. Akad. Wiss.* Berlin, 1853, p. 365-374. *Mathematische Werke*, vol. 4, p. 3-11. Chelsea, New York, 1968.

[La] Lang, Serge: *Algebraic Number Theory*. Adisson Wesley Pub. Com., Reading, 1970. ISBN: 0-201-04201-0.

[Ne] Neukirch, Jürgen: *Algebraic Number Theory*. GMW 322, Springer Verlag, Berlin, 1999. ISBN: 3-540-65399-6.

[Ri] Ribenboim, Paulo: *Algebraic Numbers*. Wiley-Interscience, New York, 1972. ISBN: 0-471-71804-8.

[Se] Serre, Jean-Pierre: *Cours d'Arithmétique*. Presses Universitaires de France, 1970. 2a. ed., 1977.

[Sp] Speiser, Andreas: Zerlegungsgruppe. *J. reine angew. Math.*, **149** (1919), p. 174-188.

[vdW] van der Waerden, Bartel Leendert: *Algebra*, vol. 1. Frederick Ungar Pub. Co. New York, 1970. ISBN: 0-8044-4950-3.

[Wa] Washington, Lawrence C.: *Introduction to cyclotomic fields*, GTM 83, Springer Verlag, New York, 1982. ISBN: 0-387-90622-3.

[We] Weber, Heinrich: Theorie der Abel'schen Zahlkörper. *Acta Math.*, **8** (1896), p. 193-263.