Teoría de Números Algebraicos

Ángel del Río Mateos

December 14, 2022

Este documento contiene los apuntes que he utilizado durante varios años para explicar Teoría de Números Álgebraicos en la asignatura de Teoría de Números del Máster en Matemática Avanzada. Para la elaboración de estos alumnos he utilizado diversos textos entre los que habría que destacar los siguientes:

- Z.I. Borevich, I.R. Shafarevich, Academic Press 1966.
- G.J. Janusz, Algebraic Number Fields, Academic Press 1973.
- D.A. Marcus, Number Fields, Springer 1977.
- P. Samuel, Algebraic Theory of Numbers, Houghton-Mifflin, Boston 1977.

Los conocimientos que damos por supuestos son los correspondientes a un grado en matemáticas en especial los de álgebra lineal, estructuras algebraicas básicas (grupos, anillos y cuerpos) y Teoría de Galois. Los siguientes textos, que se pueden descargar de mi página web `um.es/adelrio` o haciendo click en el hipervínculo, contienen algunos de estos contenidos:

[AB] Á. del Río, J.J. Simón, A. del Valle. Algebra Básica

[GA] Á. del Río. Grupos y Anillos

[EA] Á. del Río. Ecuaciones algebraicas

También supondremos una familiaridad elemental con el concepto de módulo sobre un anillo. Salvo que se diga lo contrario todos los anillos se supondrá que son conmutativos.

ADVERTENCIAS IMPORTANTES: El autor no es un especialista en Teoría de Números, más bien un aficionado a ella. Además estos apuntes están lejos de ser "presentables", es decir, están llenos de erratas e incluso errores. No sé si algún día tendré tiempo para revisarlos con la calma necesaria para que se puedan convertir en "presentables". Espero que aún así puedan resultar útiles a alguien.

Contenidos

Capítulo 1

Preliminares

En este capítulo vamos a repasar algunos conceptos y resultados que damos por conocidos.

1.1 Grupos abelianos finitamente generados

En esta sección recordamos algunas propiedades básicas de los grupos abelianos finitamente generados. Comenzamos recordando que todo grupo cíclico infinito es isomorfo al grupo aditivo $\mathbb{Z}$ y todo grupo cíclico finito de orden n es isomorfo a $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

Para enteros positivos $n_1, \ldots, n_k$ vamos a utilizar $1 < n_1 \mid \cdots \mid n_k$ como una abreviatura de $1 < n_1$, $n_1 \mid n_2$, $n_2 \mid n_3, \ldots, n_{k-1} \mid n_k$.

El siguiente teorema es conocido como el *Teorema Fundamental de los Grupos Abelianos Finitamente Generados*. Su demostración se puede encontrar en la mayoría de los libros de Teoría de Grupos. Por ejemplo, puede encontrarse en [AB, Teorema 7.5.13].

Teorema 1.1 *Sea G un grupo abeliano finitamente generado. Entonces existen enteros $n \geq 0$ y $1 < n_1 \mid \cdots \mid n_k$ tales que*

$$G \cong \mathbb{Z}^n \times \prod_{i=1}^{k} \mathbb{Z}_{n_i}.$$

Además, estos números determinan G salvo isomorfismos, es decir si $n, m \geq 0$, $1 < n_1 \mid \cdots \mid n_k$ y $1 < m_1 \mid \cdots \mid m_k$ entonces $\mathbb{Z}^n \times \prod_{i=1}^{k} \mathbb{Z}_{n_i} \cong \mathbb{Z}^m \times \prod_{i=1}^{l} \mathbb{Z}_{m_i}$ si y solo si $n = m$, $k = l$ y $n_i = m_i$ para todo i.

El número n del Teorema 1.1 se llama *rango* de G y los números $n_1, \ldots, n_k$ se llaman *divisores elementales* de G. Un grupo abeliano finitamente generado se dice que es *libre* si es isomorfo a $\mathbb{Z}^n$ para algún n, o lo que es lo mismo si tiene una base como $\mathbb{Z}$-modulo. Obsérvese que un subconjunto de $\mathbb{Z}^n$ es linealmente independiente sobre $\mathbb{Z}$ si y solo si lo es sobre $\mathbb{Q}$. Por tanto, todas las bases de $\mathbb{Z}^n$ sobre $\mathbb{Z}$ tienen n elementos pero no todos los conjuntos linealmente independientes de cardinal n son base de $\mathbb{Z}^n$ (aunque sí lo serían de $\mathbb{Q}^n$ sobre $\mathbb{Q}$).

Un grupo se dice de *torsión* si todo elemento tiene orden finito y se dice que es *libre de torsión* si su único elemento de torsión es el elemento neutro.

Del Teorema 1.1 se deduce el siguiente

Corolario 1.2 *Sea G un grupo abeliano finitamente generado. Entonces*

(1) G es finito si y solo si tiene rango 0 si y solo si G es de torsión.

(2) G es libre si y solo si es libre de torsión. En este caso G tiene una base y todas sus bases tienen n elementos.

La siguiente proposición se deduce también facilmente del Teorema 1.1:

Proposición 1.3 *Si F es un grupo abeliano libre de rango n y G es un subgrupo de F, entonces G es libre de rango menor o igual que n. Además, existen enteros positivos $a_1, \ldots, a_k$ y una base $x_1, \ldots, x_n$ de F tales que $a_1x_1, \ldots, a_kx_k$ es una base de G. En particular $[F : G] < \infty$ si y solo si $k = n$ y en tal caso $[F : G] = a_1 \ldots a_n$.*

El siguiente lema proporciona un sistema para calcular $[F : G]$, en caso de que sea finito, a partir de una base de G.

Lema 1.4 *Sea $x_1, \ldots, x_n$ una base de un grupo abeliano libre F, $A = (a_{ij})$ una matriz $n \times n$ de números enteros y G el subgrupo de F generado por $y_1, \ldots, y_n$, donde $y_i = \sum_{i=1}^{n} a_{ij}x_j$ $(i = 1, 2, \ldots, n)$. Entonces G tiene rango n si y solo si $\det(A) \neq 0$ y en tal caso $[F : G]$ es el valor absoluto de $\det(A)$. En particular, $y_1, \ldots, y_n$ forman una base de F si y solo si $\det(A) = \pm 1$.*

Demostración. Si identificamos F con $\mathbb{Z}^n$, el rango de G es n si y solo si $y_1, \ldots, y_n$ son linealmente independientes cuando los consideramos en $\mathbb{Q}^n$ y eso es equivalente a que el determinante de A sea distinto de 0.

Supongamos que $y_1, \ldots, y_n$ sean linealmente independientes. Por la Proposición 1.3, existen enteros positivos $a_1, \ldots, a_n$ y una base $\alpha_1, \ldots, \alpha_n$ de F de forma que $a_1\alpha_1, \ldots, a_n\alpha_n$ es una base de G y $[F : G] = a_1 \cdots a_n$. Consideremos las siguientes matrices B, C y D de cambio de base entre las bases que se indican en el siguiente esquema donde la flecha significa "cambio de base de la primera base a la segunda":

$$\begin{array}{rccc} B: & y_1, \ldots, y_n & \longrightarrow & a_1\alpha_1, \ldots, a_n\alpha_n, \\ C: & a_1\alpha_1, \ldots, a_n\alpha_n & \longrightarrow & \alpha_1, \ldots, \alpha_n, \\ D: & \alpha_1, \ldots, \alpha_n & \longrightarrow & x_1, \ldots, x_n. \end{array}$$

Entonces $A = BCD$, C es la matriz diagonal con entradas $a_1, \ldots, a_n$ en la diagonal y los determinantes de B y D son ambos ± 1 ya que tanto ambas matrices como sus inversas están formadas por números enteros. Por tanto

$$|\det(A)| = |\det(C)| = |a_1 \ldots a_n| = [F : G].$$

∎

1.2 Extensiones de cuerpos

En esta sección F/K es una extension de cuerpos, es decir F es un cuerpo y K es un subcuerpo de F. El *grado* de F sobre K es la dimensión de F sobre K y lo denotamos $[F : K]$.

Sea $\alpha \in F$. Entonces $K[\alpha]$ denota el menor subanillo de F que contiene a K y a α y $K(\alpha)$ el menor subcuerpo de F que contiene a K y a α. Más generalmente si X es un subconjunto de F entonces $K[X]$ y $K(X)$ denotarán respectivamente el menor subanillo y el menor subcuerpo de F que contiene a $K \cup X$. Si $X = \{\alpha_1, \ldots, \alpha_n\}$ entonces $K[X]$ y $K(X)$ también se denotan $K[\alpha_1, \ldots, \alpha_n]$ y $K(\alpha_1, \ldots, \alpha_n)$ respectivamente.

La aplicación

$$\begin{array}{rcl} E_\alpha : K[X] & \to & F \\ P(X) & \mapsto & P(\alpha) \end{array}$$

es un homorfismo de anillos cuya imagen es $K[\alpha]$. Si E_α es inyectivo entonces se dice que α es *transcendente* sobre K. En caso contrario α es *algebraico* sobre K. O sea α es algebraico sobre K si es la raíz de un polinomio no nulo con coeficientes en K. Obsérvese que como $K[X]$ es un dominio euclídeo, $\mathrm{Ker}(E_\alpha)$ es un ideal principal de $K[X]$ que debe ser primo pues $K[X]/\mathrm{Ker}(E_\alpha)$ es isomorfo a $K[\alpha]$, que es un dominio por ser un subanillo de un cuerpo.

Supongamos que α es algebraico sobre K. Entonces $\mathrm{Ker}(E_\alpha)$ es un ideal maximal de $K[X]$, pues todo ideal primo no nulo de un dominio euclídeo es maximal, y está generado por el polinomio mónico de grado más pequeño que tiene a α como raíz. Dicho polinomio se llama *polinomio mínimo* de α sobre K y lo denotaremos $\mathrm{Min}_K(\alpha)$. Obsérvese que $\mathrm{Min}_K(\alpha)$ es irreducible, y de hecho es el único polinomio mónico irreducible de $K[X]$ que tiene a α como raíz. Por tanto $K[\alpha]$ es un cuerpo, con lo que $K[\alpha] = K(\alpha)$ y $[K(\alpha) : K]$ es igual al grado de $\mathrm{Min}_K(\alpha)$. De hecho, si este grado es n entonces $1, X, \ldots, X^{n-1}$ es una base de $K(\alpha)$ sobre K. Obsérvese que α es algebraico sobre K si y solo si $[K(\alpha) : K] < \infty$. De aquí se deduce que el conjunto de los elementos de F que son algebraicos sobre K forma un subcuerpo de F que contiene a K pues si α y β son algebraicos sobre K entonces β es algebraico sobre $K(\alpha)$ con lo que $[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)] \cdot [K(\alpha) : K] < \infty$ y como $K(\alpha \pm \beta)$ y $K(\alpha\beta)$ están incluidos en $K[\alpha, \beta]$ se tiene que $[K(\alpha + \beta) : K]$, $[K(\alpha - \beta) : K]$ y $K[(\alpha\beta) : K]$ son finitos y por tanto $\alpha + \beta$, $\alpha - \beta$ y $\alpha\beta$ son algebraicos sobre K.

Recordemos que un polinomio $P(X_1, X_2, \ldots, X_n)$ en n variables se dice *simétrico* si es invariante por una permutaciones de las variables. Los *polinomios simétricos elementales* $S_1, \ldots, S_n$ vienen dados por la fórmula

$$S_i = \sum_{1 \le j_1 < \cdots < j_i \le n} \prod_{k=1}^{i} X_{j_i}.$$

En particular

$$S_1 = X_1 + \cdots + X_n \quad \text{y} \quad S_n = X_1 \cdots X_n.$$

Entonces los polinomios simétricos en n variables con coeficientes en K son precisamente los de la forma $P(S_1, \ldots, S_n)$ con P un polinomio en n-variables arbitrario (ver el Teorema 2.38 de [EA]).

Supongamos además que F/K es una extensión separable, es decir, todo $\alpha \in F$ es algebraico sobre K y $\mathrm{Min}_K(\alpha)$ no tiene raíces múltiples en ninguna extensión de F (ver [EA: Capítulo 9]). Sea $\alpha \in F$ con $[K(\alpha) : K] = n$ y sea L un cuerpo algebraicamente cerrado que contenga a F. Entonces para cada homomorfismo $\sigma : K \to L$ existen exactamente n homomorfismos de $K(\alpha)$ a L que extienden σ. Los homomorfismos de F en L que restringen a la identidad en K se llaman K-homomorfismos. Si $\sigma_1, \ldots, \sigma_n$ son los K-homomorfismos de $K(\alpha)$ en L entonces las raíces de $\mathrm{Min}_K(\alpha)$ son los elementos de la forma $\alpha_i = \sigma_i(\alpha)$, y son todas distintas porque F/K es una extensión separable. Estas raíces se llaman *conjugados* de α sobre K y se verifica la siguiente igualdad:

$$\mathrm{Min}_K(X) = \prod_{i=1}^{n}(X - \alpha_i) = X^n + \sum_{i=1}^{n}(-1)^i S_i(\alpha_1, \ldots, \alpha_n)X^{n-i}.$$

En particular $S_i(\alpha_1, \ldots, \alpha_n) \in K$ para todo i. Más aún, si $Q(X_1, \ldots, X_n)$ es un polinomio simétrico entonces $Q = P(S_1, \ldots, S_n)$ para algún polinomio $P \in K[X_1, \ldots, X_n]$. Eso implica que $Q(\alpha_1, \ldots, \alpha_n) = P(S_1(\alpha_1, \ldots, \alpha_n), \ldots, S_n(\alpha_1, \ldots, \alpha_n)) \in K$. O sea la evaluación de un polinomio simétrico en los conjugados de α tiene coeficientes en K.

Supongamos que $[F : K] = n$. Por el Teorema del Elemento Primitivo [EA, Corolario 9.20] existe $\theta \in F$ tal que $F = K(\theta)$. Por tanto hay exactamente n K-homomorfismos $\sigma_1, \ldots, \sigma_n$ de F a L. Si $\alpha \in F$ entonces el siguiente polinomio se llama *polinomio característico* de α en la extensión F/K:

$$\chi_{F/K}(\alpha) = \prod_{i=1}^{n}(X - \sigma_i(\alpha)).$$

La *norma* y la *traza* de α en la extensión F/K se definen respectivamente como

$$N_{F/K}(\alpha) = \prod_{i=1}^{n}\sigma_i(\alpha) \quad \text{y} \quad T_{F/K}(\alpha) = \sum_{i=1}^{n}\sigma_i(\alpha).$$

Proposición 1.5 *Supongamos que F/K es una extensión separable de grado n. Sea $\alpha \in F$ y supongamos que $m = [K(\alpha) : K]$, $n = [F : K]$ y $\sigma_1, \ldots, \sigma_n$ son los K-homomorfismos de F en L. Entonces*

(1) m divide a n.

(2) $\chi_{F/K}(\alpha) = Min_K(\alpha)^{\frac{n}{m}} \in K[X]$.

(3) La lista $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ está formada por los conjugados de α sobre K cada uno repetidos $\frac{n}{m}$ veces.

(4) $\alpha \in K$ si y solo si $\sigma_i(\alpha) = \alpha$ para todo $i = 1, \ldots, n$.

(5) $K(\alpha) = F$ precisamente si $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ para todo $i \neq j$.

(6) $N_{F/K}(\alpha), T_{F/K}(\alpha) \in K$.

(7) Si $\alpha, \beta \in F$ *y* $a \in K$ *entonces* $N_{F/K}(\alpha\beta) = N_{F/K}(\alpha)N_{F/K}(\beta)$, $N_{F/K}(a) = a^{[F:K]}$, $T_{F/K}(\alpha+\beta) = T_{F/K}(\alpha) + T_{F/K}(\beta)$ *y* $T_{F/K}(a) = [F:K]a$.

Demostración. Sean $q = \mathrm{Min}_K(\alpha)$ y $k = [F : K(\alpha)]$. Entonces $n = [F : K] = [F : K(\alpha)]\,[K(\alpha) : K] = k\,m$. Esto demuestra (1).

Si $\tau_1, \ldots, \tau_m$ son los K-homomorfismos de $K(\alpha)$ en L entonces cada τ_i tiene k extensiones distintas a un homomorfismo de F en L y la lista total de todas extensiones será $\sigma_1, \ldots, \sigma_n$. Las k extensiones que extienden τ_i al aplicarlas a α dan el mismo conjugado α_j de α y cada uno de estos aparecerá k veces distintas al aplicar a α los distintos σ_i. Esto demuestra (2)

(3), (4) y (5) son consecuencia directas de (2), mientras que (6) es consecuencia de que la norma y la traza son salvo el signo iguales a un coeficiente de $\chi_{F/K}(\alpha)$. (7) es obvio. ∎

Supongamos que F/K y $\sigma_1, \ldots, \sigma_n$ son como en la Proposición 1.5. El *discriminante* sobre K de una lista $\alpha_1, \ldots, \alpha_n$ de elementos de F es

$$\Delta_{F/K}[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2.$$

Además, para todo $\alpha \in F$ denotamos $\Delta_{F/K}(\alpha) = \Delta_{F/K}[1, \alpha, \alpha^2, \ldots, \alpha^{n-1}]$.

Cuando F y K están claros por el contexto escribiremos simplemente $N = N_{F/K}$, $N = T_{F/K}$ y $\Delta = \Delta_{F/K}$.

Proposición 1.6 *Sea* F/K *una extensión separable de grado* n *y sean* $\alpha_1, \ldots, \alpha_n \in F$. *Entonces:*

(1) $\Delta_{F/K}[\alpha_1, \ldots, \alpha_n] = \det(T_{F/K}(\alpha_i\alpha_j)) \in K$.

(2) Si para cada $i = 1, \ldots, n$ *se tiene* $\beta_i = \sum_{j=1}^n c_{i,j}\alpha_j$ *con* $c_{i,j} \in K$ *entonces* $\Delta_{F/K}[\alpha_1, \ldots, \alpha_n] = \Delta_{F/K}[\beta_1, \ldots, \beta_n]\det(c_{ij})^2$.

(3) Si $F = K(\theta)$ *y* $p = Min_K(\theta)$ *entonces* $\Delta_{F/K}(\theta) = (-1)^{\frac{n(n-1)}{2}} N_{F/K}(p'(\theta))$. *Además, si* $\theta_1, \ldots, \theta_n$ *son los conjugados de* θ *sobre* K *entonces* $\Delta_{F/K}(\theta) = \prod_{1\le i<j\le n}(\theta_i - \theta_j)^2$.

(4) $\Delta_{F/K}[\alpha_1, \ldots, \alpha_n] \neq 0$ *si y solo si* $\alpha_1, \ldots, \alpha_n$ *forman una base de* F *sobre* K. *En particular, si* $\alpha \in F$ *entonces* $\Delta_{F/K}(\alpha) \neq 0$ *si y solo si* $F = K(\alpha)$.

Demostración. (1) Mantenemos la notación previa para $\sigma_1, \ldots, \sigma_n$ y ponemos $A = (\sigma_i(\alpha_j))$ y $A^T = (\sigma_j(\alpha_i))$, la transpuesta de A. Entonces la entrada (i, j) de $A^T A$ es $\sum_{k=1}^n \sigma_k(\alpha_i)\sigma_k(\alpha_j) = T_{F/K}(\alpha_i\alpha_j)$ y por tanto

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(A)^2 = \det(A^T)\det(A) = \det(A^T A) = \det(T(\alpha_i\alpha_j)).$$

(2) Es una consecuencia inmediata de $(\sigma_i(\beta_j)) = (\sigma_i(\alpha_j))(c_{ij})$.

(3) Pongamos $\theta_i = \sigma_i(\theta)$. Entonces

$$\Delta(\theta) = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \theta_1 & \theta_2 & \ldots & \theta_n \\ \theta_1^2 & \theta_2^2 & \ldots & \theta_n^2 \\ \ldots & \ldots & \ldots & \ldots \\ \theta_1^{n-1} & \theta_2^{n-1} & \ldots & \theta_n^{n-1} \end{vmatrix}^2 = \prod_{i<j}(\theta_i - \theta_j)^2 \neq 0.$$

Además $p(X) = \prod_{i=1}^n (X - \theta_i)$, con lo que $p'(X) = \sum_{i=1}^n \prod_{j\neq i}(X - \theta_j)$ y, por tanto, $p'(\theta_i) = \prod_{j\neq i}(\theta_i - \theta_j)$. Luego

$$\begin{aligned}\Delta(\theta) &= \prod_{i<j}(\theta_i - \theta_j)^2 = (-1)^{\binom{n}{2}} \prod_{i\neq j}(\theta_i - \theta_j) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n p'(\theta_i) = (-1)^{\frac{n(n-1)}{2}} N(p'(\theta)).\end{aligned}$$

(4) En la demostración de (3) hemos visto que $\Delta(\theta) \neq 0$. Como $1, \theta, \theta^2, \ldots, \theta^{n-1}$ forman una base de F sobre K tenemos $\alpha_i = \sum_{i=1}^n c_{i,j}\theta^{i-1}$ para ciertos $c_{i,j} \in K$. Aplicando (2) deducimos que $\Delta[\alpha_1, \ldots, \alpha_n] \neq 0$ si y solo si $(c_{i,j})$ es invertible si y solo si $\alpha_1, \ldots, \alpha_n$ forman una base de F sobre K. La última afirmación proviene de que $F = K(\alpha)$ si y solo si $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ forman una base de F sobre K. ∎

Definición 1.7 *Un* cuerpo de números *es un subcuerpo del cuerpo $\mathbb{C}$ de los números complejos que tiene grado finito sobre el cuerpo $\mathbb{Q}$ de los números racionales.*

Como $\mathbb{C}$ es algebraicamente cerrado toda extensión finita de los racionales es isomorfa a un cuerpo de números. Si $\alpha \in \mathbb{C}$ es algebraico sobre $\mathbb{Q}$ entonces $\mathbb{Q}(\alpha)$ es un cuerpo de números. Además, por el Teorema del Elemento Primitivo todo cuerpo de números es de esta forma.

Como las extensiones de cuerpos de característica cero son separables [EA, Proposición 9.11], todo lo dicho en esta sección es válido para extensiones de cuerpos de números F/K tomando como $L = \mathbb{C}$ el cuerpo de los números complejos. En particular, si $n = [F : K]$ entonces F tiene n homomorfismos que se restringen a la identidad de K. Por tanto cualquier cuerpo de números F tiene $[F : \mathbb{Q}]$ homomorfismos de F a $\mathbb{C}$ a los que nos referiremos como inclusiones de F en $\mathbb{C}$. Las imagenes de un elemento α de F por estas inclusiones son los conjugados de α sobre $\mathbb{Q}$ que simplemente llamaremos *conjugados* de α.

1.3 Divisibilidad en dominios

Por defecto todos los anillos que consideremos serán conmutativos.

Sea A un anillo. Si X es un subconjunto de A entonces el ideal de A generado por X lo denotamos AX o (X), pero la segunda notación solo la usaremos si no hay ambigüedad sobre el anillo de referencia A. En el caso en que $X = \{x_i : i \in I\}$ abusaremos de la notación poniendo $(X) = (x_i : i \in I) = \sum_{i\in I} Ax_i$ y abusaremos aún más de la notación poniendo $0 = \{0\} = (0)$ y $(X, Y) = (X \cup Y) = AX + AY$ para X e Y subconjuntos de A. Claramente, $(X) = (0)$ si y solo si $X \subseteq \{0\}$.

El conjunto de las unidades de A lo denotaremos por $\mathcal{U}(A)$. Es claro que $\mathcal{U}(A)$ es un grupo multiplicativo.

Si $a, b \in A$ entonces decimos que a divide a b en A, y escribimos $a \mid b$ en A, si $b = ac$ para algún $c \in C$. Está claro que

$$a \mid b \text{ en } A \text{ si y solo si } b \in Aa \text{ si y solo si } Ab \subseteq Aa.$$

Dos elementos $a, b \in A$ se dicen *asociados* en A si $a \mid b$ y $b \mid a$ en A, o lo que es lo mismo, si $Aa = Ab$. En particular, las unidades de A son los elementos asociados a 1. Es evidente que si existe $u \in \mathcal{U}(A)$ tal que $a = bu$ entonces a y b son asociados en A.

Recordemos que un ideal de I de A es *primo* si $I \neq A$ y para todo $a, b \in A \setminus I$ se tiene que $ab \notin I$. Un elemento de A se dice que es *primo* en A si Aa es un ideal primo o lo que es lo mismo si $a \notin \mathcal{U}(A)$ y para todo $x, y \in A$ si $a \mid xy$ en A entonces $a \mid x$ o $a \mid y$ en A.

A partir de ahora D es un dominio. Es fácil demostrar que si $a, b \in D \setminus \{0\}$ entonces a y b son asociados si y solo si $b = au$ para algún $u \in \mathcal{U}(D)$.

Un elemento $a \in D$ se dice que es *irreducible* en D si satisface cualquiera de las siguientes condiciones equivalentes (dejamos como ejercicio la comprobación de que las condiciones son equivalentes):

- a no es una unidad de D y ni producto de dos no unidades de D.
- $a \notin \mathcal{U}(D)$ y todo divisor de a es o unidad o asociado con a.
- Si $a = bc$ entonces o b es unidad y c no lo es o c es unidad y b no lo es.

Está claro que en un dominio todo primo es irreducible, sin embargo el reciproco no es cierto en general como veremos en el Ejemplo 3.4.

Los conceptos de divisibilidad, asociado e irreducible se pueden expresar en términos de los ideales generados por los elementos en cuestión de la siguiente forma:

(1) a divide a b en D si y solo si $Da \supseteq Db$.

(2) a y b son asociados en D si y solo si $Da = Db$.

(3) a es irreducible en D precisamente si Da es maximal entre los ideales principales propios de D.

Definición 1.8 *Decimos que D es un* dominio de factorización *si todo elemento de D que no sea ni cero ni unidad se puede escribir como producto de irreducibles de D.*

Ejemplo 1.9 *Veamos ahora un ejemplo en que la factorización en irreducibles no puede ser más imposible. Sea α una no unidad de $\mathbb{A}$ distinta de 0. Por ejemplo, α puede ser cualquier elemento de $\mathbb{Z}\setminus\{0, 1, -1\}$ pues en tal caso $\frac{1}{\alpha} \notin \mathbb{A}$. Entonces α no es irreducible pues $\alpha = \sqrt{\alpha}\sqrt{\alpha}$ y $\sqrt{\alpha} \in \mathbb{A} \setminus \mathcal{U}(\mathbb{A})$. Luego $\mathbb{A}$ no tiene ningún irreducible.*

Definición 1.10 *Un* dominio de factorización única*, abreviado* DFU*, es un dominio de factorización D tal que siempre que*

$$p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

con todos los p_i y q_i irreducibles de D se verifica:

(1) $r = s$ y

(2) Existe una permutación π de $\{1, 2, \dots, r\}$ tal que p_i y $q_{\pi(i)}$ son asociados para todo i.

Vamos a considerar un concepto más genérico de factorización en producto de irreducibles para poder hablar de factorizaciones de unidades admitiendo que un producto sin factores representa el 1. De esta manera una *factorización en irreducible de* D es una expresión de la forma

$$up_1 \dots p_k$$

con $u \in \mathcal{U}(D)$, $k \geq 0$ y $p_1, \dots, p_k$ son irreducibles. Entonces D es un dominio de factorización si todo elemento de $D \setminus \{0\}$ admite una factorización en irreducibles en D. Dos *factorizaciones* en irreducibles $up_1 \dots p_k$ y $vq_1 \dots q_l$ son *equivalentes* si $k = l$ y existe una permutación $\sigma \in S_k$ tal que q_i y $p_{\sigma(i)}$ son asociados en D para todo $i = 1, \dots, k$. Es fácil ver que D es un dominio de factorización si todo elemento de $D \setminus 0$ tiene una factorización en irreducibles de D y que D es dominio de factorización única si además todas las factorizaciones en irreducibles de D de un mismo elemento son equivalentes.

El siguiente Teorema caracteriza los dominios de factorización única. Su demostración se puede encontrar en [GA, Proposición 2.22].

Teorema 1.11 *Las condiciones siguientes son equivalentes para un dominio D.*

(1) D es un dominio de factorización única.

(2) D es un dominio de factorización y todo elemento irreducible de D es primo en D.

(3) Todo elemento de D que no sea nulo ni unidad es producto de elementos primos de D.

Muchas de las ideas de la factorización en $\mathbb{Z}$ pueden ser generalizadas a dominios de factorización única. Por ejemplo, el método de cálculo del máximo común divisor y el mínimo común múltiplo de dos elementos en función de sus factorizaciones.

El teorema anterior sirve para dar una amplia clase de dominios en los que la factorización es única: La clase de los dominios de ideales principales (DIP), entre los que están los dominios euclídeos. Recordemos que un *dominio euclídeo* es un dominio D con una función euclídea y que una *función euclídea* es una función $\phi : D \setminus \{0\} \to \mathbb{N}$ tal que

(1) $a \mid b$ implica $\phi(a) \leq \phi(b)$.

(2) Para todo $a, b \in D \setminus \{0\}$ existen $q, r \in D$ tales que $a = bq + r$ y, o bien $r = 0$ ó $\phi(r) < \phi(b)$.

Recordamos sin demostración los dos resultados fundamentales de la teoría elemental de anillos.

Teorema 1.12 *Todo dominio de ideales principales es un dominio de factorización única.*

Teorema 1.13 *Todo dominio euclídeo es un dominio de ideales principales.*

Capítulo 2

Cuerpos de números y anillos de enteros

2.1 Elementos enteros sobre un anillo

En esta sección B/A es una extensión de anillos, es decir B es un anillo y A es un subanillo de B. Si $b \in B$ entonces $A[b]$ denota el menor subanillo de B que contiene a A y a b. Está claro que

$$A[b] = \{a_0 + a_1 b + \cdots + a_n b^n : n \geq 0, a_0, a_1, \ldots, a_n \in A\}.$$

Más generalmente, si $b_1, \ldots, b_n \in B$ entonces $A[b_1, \ldots, b_n]$ denota el menor subanillo de B que contiene a $A \cup \{b_1, \ldots, b_n\}$. Este anillo está formado por los elementos de B que se obtienen al evaluar $b_1, \ldots, b_n$ en un polinomio en n variables. Todavía más generalmente, si $X \subseteq A$ entonces $A[X]$ denota el menor subanillo de B que contiene a $A \cup X$. Los elementos de $A[X]$ son los que resultan de sustituir los elementos de X en polinomios en una cantidad arbitraria de variables.

El ejemplo que vamos a encontrar más frecuentemente será con $A = \mathbb{Z}$, el anillo de los números enteros, y B un cuerpo de números.

Consideraremos B como A-módulo de la forma natural. Recuérdese que un *A-módulo M* es *fiel* si el único elemento $a \in A$ tal que $aM = 0$ es $a = 0$. Por ejemplo, B es fiel cómo A-módulo, pues $a1 = a$ para todo $a \in A$.

Definición 2.1 *Sea $b \in B$. Decimos que b es* algebraico *sobre A si b es la raíz de un polinomio no constante con coeficientes en A. Decimos que b es* entero algebraico *(o simplemente* entero*) sobre A si es la raíz de un polinomio mónico con coeficientes en A. Decimos que B es* entero *sobre A si todo elemento de B es entero sobre A.*

Claramente si b es entero sobre A entonces también es algebraico sobre A. Si además A es cuerpo entonces el recíproco se verifica. En general el recíproco no se verifica como podemos ver aplicando la siguiente proposición por ejemplo a $R = \mathbb{Z}$ pues todo elemento de $\mathbb{Q}$ es algebraico sobre $\mathbb{Z}$.

Proposición 2.2 *Sea R un dominio de factorización única (DFU), F es su cuerpo de fracciones y $a \in F$. Entonces a es entero sobre R si y solo si $a \in R$. En particular los únicos números racionales que son enteros sobre $\mathbb{Z}$ son los números enteros.*

Demostración. Sea $\alpha = \frac{a}{b}$, con a e b elementos no nulos y coprimos de R. Entonces α es algebraico sobre R pues es raíz del polinomio $bX - a$. Supongamos que

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0,$$

con $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$. Eso implica que

$$a^n + a_{n-1}a^{n-1}b + \ldots + a_1ab^{n-1} + a_0b^n = 0$$

y, por tanto, b divide a a^n en R. Como a y b son coprimos también a^n y b son coprimos en R, lo que implica que b es invertible en R. Por tanto $\alpha \in R$. ∎

Proposición 2.3 *Sea B/A una extensión de anillos. Las siguientes condiciones son equivalentes para un elemento $b \in B$.*

(1) b es entero sobre A.

(2) $A[b]$ es finitamente generado como A-módulo.

(3) $A[b]$ está contenido en un subanillo de B que es finitamente generado como A-módulo.

(4) Existe un $A[b]$-módulo fiel que es finitamente generado como A-módulo.

Demostración. (1) implica (2). Supongamos que b es entero sobre A y sea $P = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in A[X]$ con $P(b) = 0$. Entonces, para todo $m \geq n$,

$$b^m = -(a_{n-1}b^{m-1} + \ldots + a_1b^{m-n+1} + a_0b^{m-n})$$

y razonando por inducción se obtiene que $b^m \in A + Ab + \ldots + Ab^{n-1}$, para todo m. Luego $A[b]$ está generado por $1, b, b^2, \ldots, b^{n-1}$ como A-módulo.

Para demostrar (2) implica (3) considérese el anillo $A[b]$.

(3) implica (4). Si C es un subanillo de B que contiene a $A[b]$ entonces C es un $A[b]$-módulo fiel.

(4) implica (1). Sea M un $A[b]$-módulo fiel que es finitamente generado como A-módulo y sea $\{x_1, \ldots, x_n\}$ un conjunto de generadores de ${}_AM$. Entonces para cada $i = 1, 2, \ldots, n$ tenemos

$$bx_i = \sum_{i=1}^{n} a_{ij}x_j$$

para ciertos $a_{ij} \in A$. Luego tenemos la siguiente ecuación matricial

$$(bI - (a_{ij}))(x_i) = 0$$

Multiplicando por la izquierda por la adjunta de la matriz $(bI - (a_{ij}))$ se obtiene que el determinante d de esta matriz cumple $dx_i = 0$ para todo i y como M está generado por $x_1, \ldots, x_n$ se tiene que $dM = 0$. Luego $d = 0$, pues M es fiel como A-módulo. Si P es el polinomio característico de la matriz (a_{ij}) entonces $P(b) = \det(bI - a_{ij}) = d = 0$ y P un polinomio mónico con coeficientes en A. Luego b es entero sobre A. ∎

Corolario 2.4 *Si $b_1, \ldots, b_n \in B$ son enteros sobre A, entonces $A[b_1, \ldots, b_n]$ es finitamente generado como A-módulo.*

Demostración. Por inducción respecto de n. Como b_n es entero sobre A, tambien es entero sobre $A[b_1, \ldots, b_{n-1}]$ y, por tanto, $A[b_1, \ldots, b_n]$ es finitamente generado como $A[b_1, \ldots, b_{n-1}]$-módulo. Por hipótesis de inducción, $A[b_1, \ldots, b_{n-1}]$ es finitamente generado como A-módulo y, por tanto, $A[b_1, \ldots, b_n]$ es finitamente generado como A-módulo. ∎

Corolario 2.5 *El conjunto de los elementos de B que son enteros sobre A forma un subanillo de B.*

Demostración. Si $b, c \in B$ son enteros sobre A, entonces $A[b, c]$ es finitamente generado como A-módulo. Por tanto, $A[b, c]$ es fiel y finitamente generado, como A-módulo. Como $A[b + c], A[c]$ y $A[bc]$ están contenidos en $A[b, c]$, de la Proposición 2.3 deducimos que $b + c$, $-b$ y bc son enteros sobre A. Como obviamente 1 es entero sobre A, el corolario es claro. ∎

Definición 2.6 *El conjunto de elementos de B que son enteros en A se llama* clausura entera *de A en B. Se dice que A en* integramente cerrado *en B si coincide con su clausura entera en B.*

Si A es un dominio decimos que A es integramente cerrado *si lo es en su cuerpo de cocientes.*

Por ejemplo, B es entero sobre A si y solo si B es la clausura entera de A en B. La Proposición 2.2 se puede reescribir como:

Proposición 2.7 *Todo DFU es integramente cerrado.*

Corolario 2.8 *Si B es entero sobre A y C es entero sobre A, entonces C es entero sobre A.*

Demostración. Sea $c \in C$ y $c^n + b_{n-1}c^{n-1} + \ldots + b_1c + b_0 = 0$, con $b_0, b_1, \ldots, b_{n-1} \in B$. Como estos elementos son enteros sobre A, del Corolario 2.4 se tiene que $B' = A[b_1, \ldots, b_n]$ es finitamente generado como A-módulo. Como además c es entero sobre B', tenemos que $B'[c]$ es finitamente generado como B'-módulo. Eso implica que $B'[c]$ es finitamente generado como A-módulo y, por tanto, c es entero sobre A por la Proposición 2.3. ∎

Corolario 2.9 *La clausura entera de A en B es integramente cerrada en B.*

Demostración. Sea $b \in B$ entero sobre la clausura entera C de A en B. Entonces $C[b]$ es entero sobre C y C es entero sobre A. Por el corolario anterior, b es entero sobre A y, por tanto $b \in C$. ∎

2.2 Anillos de enteros

Un *número algebraico* es un número complejo que es entero sobre $\mathbb{Q}$. Un *entero algebraico* es un número complejo que es entero sobre $\mathbb{Z}$. El conjunto de los números algebraicos es la clausura algebraica $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ en $\mathbb{C}$ y el conjunto $\mathbb{A}$ de los enteros algebraicos es la clausura entera de $\mathbb{Z}$ en $\mathbb{C}$.

Definición 2.10 *El* anillo de enteros *de un cuerpo de números K es la clausura entera de $\mathbb{Z}$ en K y lo denotaremos $\mathbb{A}_K$, o sea $\mathbb{A}_K = K \cap \mathbb{A}$.*

A partir de ahora K denota un cuerpo de números. Por defecto, *entero* significa, entero sobre $\mathbb{Z}$. O sea los elementos de $\mathbb{A}_K$ se llaman *enteros de K*. En particular, los enteros de $\mathbb{Q}$ son los elementos de $\mathbb{Z}$ y nos referimos a ellos como *enteros racionales*.

Lema 2.11 *Si $\alpha \in K$, entonces existe $c \in \mathbb{Z}^+$ tal que $c\alpha \in \mathbb{A}_K$.*

Demostración. Supongamos que $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$, con $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$. Entonces existe $c \in \mathbb{Z}^+$ tal que $ca_i \in \mathbb{Z}$, para todo i y

$$(c\alpha)^n + ca_{n-1}(c\alpha)^{n-1} + \ldots + c^{n-1}a_1(c\alpha) + c^n a_0 = 0.$$

Luego $c\alpha \in \mathbb{A}_K$. ∎

Si c es entero racional, entonces $\mathbb{Q}(c\alpha) = \mathbb{Q}(\alpha)$, por tanto, del Teorema del Elemento Primitivo y el Lema 2.11 deducimos el siguiente:

Corolario 2.12 *Si K es un cuerpo de números, entonces existe un entero θ tal que $K = \mathbb{Q}(\theta)$.*

Lema 2.13 (Gauss) *Sean $f, g \in \mathbb{Q}[X]$ tales que $fg \in \mathbb{Z}[X]$. Entonces existe $0 \neq c \in \mathbb{Q}$ tal que $cf \in \mathbb{Z}[X]$ y $c^{-1}g \in \mathbb{Z}[X]$.*

Demostración. Obviamente podemos suponer que f y g son distintos de cero. Multiplicando por los denominadores de f y g podemos encontrar $n \in \mathbb{Z}^+$ tal que $nfg = f_1 g_1$ donde $f_1 = af \in \mathbb{Z}[X]$ y $g_1 = bg \in \mathbb{Z}[X]$ para ciertos racionales a y b. Vamos a razonar por inducción sobre n. Por supuesto no hay nada que demostrar para $n = 1$. Sea p un factor primo de n. Entonces, $p \mid f_1 g_1$ y como p genera un ideal primo de $\mathbb{Z}[X]$ [EA, Lema 2.14], deducimos que p divide a f_1 ó g_1 en $\mathbb{Z}[X]$. Por simetría podemos suponer que p divide a f_1. Entonces $\frac{n}{p} fg = \frac{f_1}{p} g_1 = f_2 g_1$ con $f_2 = \frac{a}{p} f \in \mathbb{Z}[X]$. Sólo falta aplicar la hipótesis de inducción. ∎

Corolario 2.14 *Si $f = gh$ con $f \in \mathbb{Z}[X]$, $g, h \in \mathbb{Q}[X]$ y f y g son mónicos entonces $h \in \mathbb{Z}[X]$. En particular, si f y g son polinomios mónicos con coeficientes en $\mathbb{Z}$ entonces f divide a g en $\mathbb{Q}[X]$ si y solo si f divide a g en $\mathbb{Z}[x]$.*

Demostración. Como f y g son mónicos, también lo es h. Por el Lemma de Gauss (Lemma 2.13) existe $c \in \mathbb{Q} \setminus \{0\}$ tal que $cg \in \mathbb{Z}[X]$ y $c^{-1}h \in \mathbb{Z}[X]$. Como g y h son mónico $c, c^{-1} \in \mathbb{Z}$. Por tanto $c = \pm 1$ y por tanto $h \in \mathbb{Z}[X]$. ∎

Lema 2.15 *Un número algebraico es un entero algebraico precisamente si su polinomio mínimo sobre $\mathbb{Q}$ está en $\mathbb{Z}[X]$.*

Demostración. Una implicación es obvia. Supongamos que α es un entero algebraico y sea p el polinomio mínimo de α sobre $\mathbb{Q}$ y $q \in \mathbb{Z}[X]$ un polinomio mónico tal que $q(\alpha) = 0$. Entonces $q = fp$ para algún polinomio $f \in \mathbb{Q}[X]$. Aplicando el Lema de Gauss (Lema 2.13), existe $c \in \mathbb{Q}$ tal que $c^{-1}f \in \mathbb{Z}[X]$ y $cp \in \mathbb{Z}[X]$. Pero, como f y p son mónicos, $c, c^{-1} \in \mathbb{Z}$. Luego $c = \pm 1$ y, por tanto, $p \in \mathbb{Z}[X]$. ∎

Como consecuencia del Lema 2.15y la Proposición 1.5, y teniendo en cuenta que la norma y la traza son, salvo el signo, coeficientes del polinomio característico deducimos el siguiente

Corolario 2.16 *Si K es un cuerpo de números y $\alpha \in \mathbb{A}_K$ entonces $\chi_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}[X]$ y $N_{K/\mathbb{Q}}(\alpha), T_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.*

Vamos a acabar esta sección viendo cómo la norma nos ayuda a identificar las unidades, los elementos irreducibles y el que dos elementos sean asociados en el anillo de enteros de un cuerpo numérico.

Proposición 2.17 *Sea K un cuerpo de números, sea $N = N_{K/\mathbb{Q}}$ y sean $x, y \in \mathbb{A}_K$.*

(1) Si $x \mid y$ en $\mathbb{A}_K$ entonces $N(x) \mid N(y)$ en $\mathbb{Z}$.

(2) $x \in \mathcal{U}(\mathbb{A}_K)$ si y solo si $N(x) = \pm 1$.

(3) Si x e y son asociados, entonces $N(x) = \pm N(y)$.

(4) Si $N(x)$ es un primo racional, entonces x es irreducible en $\mathbb{A}_K$.

(5) Si $x \mid y$ en $\mathbb{A}_K$ entonces x e y son asociados en $\mathbb{A}_K$ si y solo si $|N(x)| = |N(y)|$.

Demostración. (1) y la condición necesaria de (2) son consecuencia inmediata de que $N(xy) = N(x)N(y)$ y $N(x) \in \mathbb{Z}$ para todo $x, y \in \mathbb{A}_K$. Además, si σ es un homomorfismo de K en $\mathbb{C}$ entonces $\sigma(x) \in \mathbb{A}$ y por tanto si $x \neq 0$ y $\sigma_1, \ldots, \sigma_n$ son los homomorfismos de K en $\mathbb{C}$ distintos de la inclusión entonces $\frac{N(x)}{x} = \prod_{i=1}^{n} \sigma_i(x) \in K \cap \mathbb{A} = \mathbb{A}_K$. Por tanto, si $N(x) = \pm 1$ entonces $x^{-1} = \pm \frac{N(x)}{x} \in \mathbb{A}_K$ y por tanto $x \in \mathcal{U}(\mathbb{A}_K)$. Esto demuestra la condición suficiente de (2). Claramente (3), (4) y (5) son consecuencia inmediata de (1) y (2). ∎

2.3 Cuerpos cuadráticos

Un número entero se dice que es *libre de cuadrados* si no es divisible por el cuadrado de ningún entero mayor que 1, o lo que es lo mismo si su valor absoluto es 1 o un producto de primos distintos.

Un *cuerpo cuadrático* es una extensión K de $\mathbb{Q}$ de grado 2. La siguiente proposición describe todos los cuerpos cuadráticos:

Proposición 2.18 *Todo cuerpo cuadrático es de la forma* $\mathbb{Q}(\sqrt{d})$ *con* d *un entero libre de cuadrados diferente de* 1.

Demostración. Sea K un cuerpo cuadrático. Por el Corolario 2.12, $K = \mathbb{Q}(\theta)$ con θ entero y del Lema 2.15 se deduce que $\mathrm{Min}_{\mathbb{Q}}(\theta) = X^2 + aX + b$ con $a, b \in \mathbb{Z}$. Pongamos que $a^2 - 4b = r^2 d$ con $r, d \in \mathbb{Z}$ y d libre de cuadrados. Entonces

$$\theta = \frac{-a + r\sqrt{d}}{2}$$

y, por tanto $K = \mathbb{Q}(\sqrt{d})$. ∎

El entero libre de cuadrados de la Proposición 2.18 es único:

Problema 2.19 *Demostrar que si* d_1 *y* d_2 *son dos enteros libres de cuadrados entonces* $\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$ *si y solo si* $d_1 = d_2$.

Claramente $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$ si y solo si $d > 1$ y en tal caso se dice que $\mathbb{Q}(\sqrt{d})$ es *real*. En caso contrario decimos que $\mathbb{Q}(\sqrt{d})$ es *imaginario*.

Veamos como podemos utilizar el Lema 2.15 para calcular el anillo de enteros de un cuerpo cuadrático.

Proposición 2.20 *Si* d *es un entero libre de cuadrados entonces*

$$A_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}, & \text{si } d \not\equiv 1 \mod 4; \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{\frac{a+b\sqrt{d}}{2} : a, b \in \mathbb{Z}, a \equiv b \mod 2\right\}, & \text{si } d \equiv 1 \mod 4. \end{cases}$$

Demostración. Ya sabemos que $\mathbb{A}_{\mathbb{Q}(\sqrt{1})} = \mathbb{A}_{\mathbb{Q}} = \mathbb{Z} = \mathbb{Z}\left[\frac{1+\sqrt{1}}{2}\right]$ y las igualdades a la derecha de la llave son sencillas de demostrar. Supongamos que $d \neq 1$ y pongamos $K = \mathbb{Q}(\sqrt{d})$. Claramente $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{A}_K$. Cada elemento de K tiene una forma unica

$$\alpha = \frac{a + b\sqrt{d}}{c}$$

con $a, b, c \in \mathbb{Z}$, $c > 0$ y $\mathrm{mcd}(a, b, c) = 1$. Los conjugados de α sobre $\mathbb{Q}$ son α y $\overline{\alpha} = \frac{a-b\sqrt{d}}{c}$. Supongamos que $\alpha \notin \mathbb{Z}$. Entonces el polinomio mínimo de α es

$$(X - \alpha)(X - \bar{\alpha}) = X^2 - \frac{2a}{c}X + \frac{a^2 - b^2 d}{c^2}.$$

Del Lema 2.15 deducimos que $\alpha \in \mathbb{A}_K$ si y solo si $\frac{2a}{c}, \frac{a^2-b^2d}{c^2} \in \mathbb{Z}$. Por ejemplo,

$$\frac{1 + \sqrt{d}}{2} \in \mathbb{A}_K \text{ si y solo si } d \equiv 1 \mod 4. \tag{2.1}$$

Afirmamos que si $\alpha \in \mathbb{A}_K$ entonces $c = 1$ ó $c = 2$ y en el segundo caso $d \equiv 1 \mod 4$ y a y b son impares. En efecto, sea p un primo que divide a c. Entonces p divide a $2a$ y p^2 divide

a $a^2 - b^2 d$. Si $p \neq 2$ entonces $p \mid a$ y por tanto p no divide a b y p^2 divide a $b^2 d$. Luego p^2 divide a d en contra de que d es libre de cuadrados. Luego $p = 2$. Esto demuestra que c es una potencia de 2 pero la misma demostración prueba que 4 no divide a c. Por tanto, $c = 1$ ó $c = 2$. Supongamos que $c = 2$. Entonces $a^2 \equiv db^2 \mod 4$. De esto se deduce que a y b son impares pues d no es múltiplo de 4 y a y b no son ambos pares. Por tanto $a^2 \equiv b^2 \equiv 1 \mod 4$ y concluimos que $d \equiv 1 \mod 4$. Esto termina la demostración de la afirmación.

Por la afirmación, todo elemento α de $\mathbb{A}_K$ que no esté en $\mathbb{Z}[\sqrt{d}]$ es de la forma $\frac{a+b\sqrt{d}}{2}$ con a y b impares. Entonces $\alpha = \frac{a-b}{2} + b\frac{1+\sqrt{d}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Esto demuestra que $\mathbb{A}_K \subseteq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Si además $d \equiv 1 \mod 4$ entonces se da la inclusión recíproca por (2.1). Luego en tal caso $\mathbb{A}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Sin embargo, de la afirmación se tiene que si $d \not\equiv 1 \mod 4$ entonces $\mathbb{A}_K \subseteq \mathbb{Z}[\sqrt{d}]$ y en consecuencia $\mathbb{A}_K = \mathbb{Z}[\sqrt{d}]$. ∎

2.4 Bases enteras

En esta sección K es un cuerpo de números de grado n.

Como el grupo aditivo de K es libre de torsión cualquier subgrupo finitamente generado del grupo aditivo de K será libre. Además un subconjunto de K es linealmente independiente sobre $\mathbb{Z}$ si y sólo si lo es sobre $\mathbb{Q}$. Por tanto todos los subgrupos aditivos finitamente generados de K tienen rango menor o igual que n y tendrán rango n si contienen una base de K.

Sea G un subgrupo aditivo finitamente generado de K. Por el párrafo anterior G está generado por n elementos $\alpha_1, \ldots, \alpha_n$. Por definición el *discriminante* de G es

$$\Delta[G] = \Delta_{K/\mathbb{Q}}[\alpha_1, \ldots, \alpha_n].$$

Esto no depende de la elección de los α_i pues si G tiene rango menor que n entonces $\alpha_1, \ldots, \alpha_n$ no son linealmente independientes y por tanto $\Delta_{K/\mathbb{Q}}[\alpha_1, \ldots, a_n] = 0$, por la Proposición 1.6.(4). En caso contrario $\alpha_1, \ldots, \alpha_n$ es una base de K sobre $\mathbb{Q}$ y lo mismo pasa para otro conjunto $\beta_1, \ldots, \beta_n$ de generadores de G. Como ambos generan el mismo grupo, las matrices de cambio de base entre estas dos bases tienen entradas enteras y como son inversas una de la otra tienen determinante ± 1. Aplicando la Proposición 1.6.(2) deducimos que $\Delta_{F/K}[\beta_1, \ldots, \beta_n] = \Delta_{F/K}[\alpha_1, \ldots, \alpha_n]$.

Definición 2.21 *Una* base entera *de K es una base de $\mathbb{A}_K$ como $\mathbb{Z}$-módulo, es decir una lista $\alpha_1, \ldots, \alpha_n$ que cumple $\mathbb{A}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$.*

Pronto veremos que K tiene una base entera con lo que podemos definir el discriminante *Δ_K de K como el discriminante de $\mathbb{A}_K$. O sea $\Delta_K = \Delta[\mathbb{A}_K]$.*

Ejemplo 2.22 Si d un entero libre de cuadrados, entonces, de la Proposición 2.20 tenemos

que una base entera de $\mathbb{Q}(\sqrt{d})$ es $1, \sqrt{d}$, si $d \not\equiv 1 \mod 4$ y $1, \frac{1+\sqrt{d}}{2}$ en caso contrario. Por tanto

$$\Delta_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d, & \text{si } d \not\equiv 1 \mod 4; \\ \\ \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = d, & \text{si } d \equiv 1 \mod 4. \end{cases}$$

Obsérvese que dos cuerpos cuadráticos son iguales si y solo si tienen el mismo discriminante.

Problema 2.23 *Demostrar que dos cuerpos cuadráticos son iguales si y solo si tienen el mismo discriminante.*

Para demostrar la existencia de bases enteras utilizaremos el siguiente lema.

Lema 2.24 *Si $\alpha_1, \ldots, \alpha_n \in \mathbb{A}_K$ entonces $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Z}$.*

Demostración. Sabemos que $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Q}$, pero además como $\alpha_1, \ldots, \alpha_n \in \mathbb{A}_K$, sus conjugados también están en $\mathbb{A}_K$ y, por tanto, utilizando las Proposiciones 1.6.(1) y (2.2) tenemos que $\Delta[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2 \in \mathbb{A}_K \cap \mathbb{Q} = \mathbb{A}_{\mathbb{Q}} = \mathbb{Z}$. ∎

Teorema 2.25 *Todo cuerpo de números K tiene una base entera y el grupo aditivo de su anillo de enteros es libre de rango $[K : \mathbb{Q}]$.*

Demostración. Del Lema 2.11 se deduce que $\mathbb{A}_K$ contiene una base de K sobre $\mathbb{Q}$ y del Lema 2.24 se deduce que entre todas las bases de K contenidas en $\mathbb{A}_K$ hay una con discriminante mínimo en valor absoluto. Sea $\omega_1, \ldots, \omega_n$ una de estas bases y vamos a ver que es de hecho una base entera de K. En caso contrario, tomamos $w \in \mathbb{A}_K \setminus (\mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n)$, con lo que existen $a_1, \ldots, a_n \in \mathbb{Q}$ tales que

$$\omega = a_1\omega_1 + \ldots + a_n\omega_n \in \mathbb{A}_K$$

y no todos los a_i están en $\mathbb{Z}$. Podemos reordenar los ω_i para que $a_1 \notin \mathbb{Z}$. Pongamos $a_1 = a + r$, con $a \in \mathbb{Z}$ y $0 < r < 1$. Poniendo $\psi_1 = \omega - a\omega_1$ y $\psi_i = \omega_i$ $(i = 2, 3, \ldots, n)$ tenemos que $\psi_1, \ldots, \psi_n$ es otra base de K sobre $\mathbb{Q}$ formada por elementos de $\mathbb{A}_K$. Además el determinante de la matriz de cambio de base es

$$\begin{vmatrix} a_1 - a & a_2 & a_3 & \ldots & a_n \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 1 \end{vmatrix} = r.$$

De la Proposición 1.6.(2) deducimos $\Delta[\psi_1, \ldots, \psi_n] = r^2\Delta[\omega_1, \ldots, \omega_n] < \Delta[\omega_1, \ldots, \omega_n]$, en contra de la elección de $\omega_1, \ldots, \omega_n$. ∎

2.5 Cálculo efectivo de bases de enteras

El Teorema 2.25 nos asegura la existencia de una base entera, pero la búsqueda efectiva de una base entera concreta es una tarea más complicada. En el resto de la sección vamos a ver un procedimiento algorítmico para calcular una base entera de nuestro cuerpo de números K. De las Proposiciones 1.6.(4) y 1.3 deducimos que si G es un subgrupo de $\mathbb{A}_K$ entonces $\Delta[G] \neq 0$ si y solo si $[\mathbb{A}_K : G] < \infty$. Más generalmente, tenemos la siguiente proposición que será útil para calcular bases enteras.

Proposición 2.26 *Si G es un subgrupo aditivo de índice finito en $\mathbb{A}_K$ entonces*

$$\Delta[G] = [\mathbb{A}_K : G]^2 \Delta_K.$$

En particular, $[\mathbb{A}_K : G]^2$ divide a $\Delta[G]$.

Demostración. Es consecuencia de las proposiciones 1.6.(2) y 1.4. ∎

Una consecuencia de la Proposición 2.26 es el siguiente corolario:

Corolario 2.27 *Sea $\alpha_1, \ldots, \alpha_n$ una $\mathbb{Q}$-base de K formada por elementos enteros. Si $\Delta[\alpha_1, \ldots, \alpha_n]$ es libre de cuadrados, entonces $\alpha_1, \ldots, \alpha_n$ es una base entera de K.*

Por ejemplo, podríamos haber utilizado esto para dar una demostración de que si $d \equiv 1 \mod 4$ entonces $1, \frac{1+\sqrt{d}}{2}$ forman una base entera de $\mathbb{Q}(\sqrt{d})$ pues se trata de una base de $\mathbb{Q}(\sqrt{d})$ formada por elementos enteros cuyo discriminante es d, un entero libre de cuadrados.

Lema 2.28 *Sea G un subgrupo aditivo de $\mathbb{A}_K$ con base $\alpha_1, \ldots, \alpha_n$. Si $G \neq \mathbb{A}_K$, entonces existe un primo p tal que p^2 divide a $\Delta[G]$ y un entero algebraico no nulo de la forma*

$$\frac{1}{p}(c_1\alpha_1 + \ldots + c_n\alpha_n)$$

con $c_1, \ldots, c_n$ enteros entre 0 y $p-1$.

Demostración. Sea p un divisor primo de $[\mathbb{A}_K : G]$. Por la Proposición 2.26, p^2 divide a $\Delta[G]$. Además, del Teorema de Cauchy de Teoría de Grupos [AB, Teorema 8.3.1], o del Teorema Fundamental de Grupos Abelianos Finitamente Generados (Teorema 1.1), deducimos que $\mathbb{A}_K/G$ tiene un elemento de orden p, es decir, existe $u \in \mathbb{A}_K \setminus G$ tal que $pu \in G$. Entonces $pu = a_1\alpha_1 + \ldots + a_n\alpha_n$ para ciertos enteros $a_1, \ldots, a_n$. Para cada i sean c_i y q_i enteros con $a_i = pq_i + c_i$ y $0 \leq c_i \leq p-1$. Entonces $v = u - \sum_{i=1}^n q_i\alpha_i = \frac{1}{p}(c_1\alpha_i + \ldots + c_n\alpha_n) \in \mathbb{A}_K$. Como $u \notin G$ se tiene que $u \neq \sum_{i=1} q_i\alpha_i$ y por tanto $v \neq 0$. ∎

Algoritmo para el cálculo efectivo de una base entera:

La entrada del algoritmo es un cuerpo de números K. Sea $n = [K : \mathbb{Q}]$.

(1) Empezamos con una base de K sobre $\mathbb{Q}$ formada por elementos enteros[1] La existencia está garantizada por la Proposición 2.25.

[1] La idea es tomar una lista que sospechamos que pueda ser una base de $\mathbb{A}_K$. Por ejemplo, si $K = \mathbb{Q}(\theta)$ con θ entero podemos tomar la base $1, \theta, \theta^2, \ldots, \theta^{n-1}$.

(2) Calculamos $\Delta = \Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$. Esto es un número entero por la Proposición 2.24. Si es libre de cuadrados concluimos del Corolario 2.27 que $\alpha_1, \ldots, \alpha_n$ es una base entera de K y el algoritmo concluye con la salida $\alpha_1, \ldots, \alpha_n$.

(3) En caso contrario elegimos un primo p tal que p^2 divida a Δ y analizamos si alguno de los elementos de la forma $\beta = \frac{1}{p}(c_1\alpha_1 + \ldots + c_n\alpha_n)$ con $0 \leq c_i < p$ y algún $c_i \neq 0$ es entero. Esto es un proceso finito pues solo hay un número finito de tales elementos. Además para decidir si un elemento es entero podemos utilizar la Proposición 2.15.

   (a) Si alguno de ellos $\beta = \frac{1}{p}(c_1\alpha_1 + \ldots + c_n\alpha_n)$ es entero y $c_i \neq 0$ entonces cambiamos α_i por β y volvemos al paso (2).

   (b) Si ningún elemento de esta forma es entero concluimos del Lemma 2.28 que $\alpha_1, \ldots, \alpha_n$ es una base entera de K y el algoritmo concluye con la salida $\alpha_1, \ldots, \alpha_n$.

Vamos a ver que este algoritmo acaba en un conjunto finito de pasos. Para ello observamos que cada vez que vamos del paso (3a) al paso (2) el valor de Δ se multiplica por $\left(\frac{c_i}{p}\right)^2 < 1$. Esto es consecuencia de la Proposición 1.6.(2). Por tanto los valores absolutos de los Δ calculados en (2) forman una sucesión decreciente de enteros positivos. Como estos números no pueden decrecer indefinidamente el algoritmo tiene que parar en algún momento en el paso (2) ó (3b) proporcionando una base entera de K.

En realidad podemos acelerar el procedimiento modificando ligeramente β para que $c_i = 1$, con lo cual cada vez que se pasa del paso (4) al paso (2) el valor de Δ se divide por p^2. Para ver esto, reordenando los α_i podemos suponer que $c_1 \neq 0$. Como $c_i < p$, tenemos que $\mathrm{mcd}(c_i, p) = 1$ y por tanto existen enteros u y v con $uc_i + vp = 1$. Para cada $j = 2, \ldots, n$ sean q_j y r_j el cociente y el resto de dividir uc_j entre p. Entonces $\beta' = u\beta + v\alpha_1 - (q_2\alpha_2 + \cdots + q_n\alpha_n)$ es entero y

$$\begin{aligned}
\beta' &= \frac{u}{p}(c_1\alpha_1 + \cdots + c_n\alpha_n) + v\alpha_1 - (q_2\alpha_2 + \cdots + q_n\alpha_n) \\
&= \frac{1}{p}((uc_1 + vp)\alpha_1 + (uc_2 - q_2p)\alpha_2 + \cdots + (uc_n - q_jp)\alpha_n) \\
&= \frac{1}{p}(\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n).
\end{aligned}$$

Ejemplo 2.29 Si $\theta = \sqrt[3]{7}$, es decir θ es la raíz cúbica real de 7 entonces $1, \theta, \theta^2$ forman una base entera de $\mathbb{Q}(\sqrt[3]{7})$.

Demostración. Sean $K = \mathbb{Q}(\theta)$ y $R = \mathbb{Z}[\theta]$. Claramente $R \subseteq \mathbb{A}_K$ y $1, \theta, \theta^2$ forman una base del grupo aditivo de R. Por tanto, basta con demostrar que $R = \mathbb{A}_K$.

Sea ω una raíz cúbica primitiva de la unidad. El polinomio mínimo de ω es $\frac{X^3-1}{X-1} = 1 + X + X^2$, con lo que $1 + \omega + \omega^2 = 0$. Las raíces de $X^3 - 7$ son θ, $\omega\theta$ y $\omega^2\theta$. Luego las inclusiones de K en $\mathbb{C}$ vienen dadas por $\sigma_1 : \theta \mapsto \theta, \sigma_2 : \theta \mapsto \omega\theta$ y $\sigma_2 : \theta \mapsto \omega^2\theta$. Por tanto,

$$\begin{aligned}
\Delta[G] &= \begin{vmatrix} 1 & \theta & \theta^2 \\ 1 & \omega\theta & \omega^2\theta^2 \\ 1 & \omega^2\theta & \omega\theta^2 \end{vmatrix}^2 = \left(\theta^3 \begin{vmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{vmatrix}\right)^2 = 7^2 3^2(\omega^2 - \omega)^2 = 7^2 3^2(-1 - 2\omega)^2 \\
&= 7^2 3^2(1 + 4\omega + 4\omega^2) = 7^2 3^2(-3) = -7^2 3^3
\end{aligned}$$

Según el algoritmo explicado anteriormente ahora tenemos que buscar un entero algebraico de una de las dos siguientes formas

$$\frac{1}{3}(c_0+c_1\theta+c_2\theta^2), 0\le c_1,c_2,c_3\le 2; \qquad \frac{1}{7}(c_0+c_1\theta+c_2\theta^2), 0\le c_1,c_2,c_3\le 6.$$

Veremos que no existe ninguno y en consecuencia concluiremos que $R=\mathbb{A}_K$. Para ello empezamos calculando una fórmula para los coeficientes del polinomio característico de un elemento genérico $\alpha=a_0+a_1\theta+a_2\theta^2\in K$ con $a_0,a_1,a_2\in\mathbb{Q}$. Salvo el signo, dos de estos coeficientes son la traza y la norma:

$$T(a_0+a_1\theta+a_2\theta^2)=3a_0$$

$$\begin{aligned} N(a_0+a_1\theta+a_2\theta^2) &= (a_0+a_1\theta+a_2\theta^2)(a_0+a_1\omega\theta+a_2\omega^2\theta^2)(a_0+a_1\omega^2\theta+a_2\omega\theta^2)\\ &= a_0^3+7a_1^3+49a_2^3-21a_0a_1a_2 \end{aligned}$$

Con estas dos expresiones conseguimos descartar los elementos del segundo tipo pues si α es del segundo tipo deducimos que $T(\alpha)=\frac{3c_0}{7}\in\mathbb{Z}$ y, como $0\le c_0<6$, deducimos que $c_0=0$. Tomando ahora normas deducimos que $N(\alpha)=\frac{c_1^3+7c_2^3}{49}\in\mathbb{Z}$. Luego $7\mid c_1$ y de nuevo $c_1=0$, con lo que $N(\alpha)=\frac{c_2^3}{7}\in\mathbb{Z}$ y concluímos que $c_2=0$. Luego $\mathbb{A}_K$ no tiene elementos de la segunda forma.

Para descartar los del primer tipo necesitaremos considerar el coeficiente del polinomio característico que nos falta por considerar que es el siguiente:

$$\begin{aligned} f(\alpha) &= (a_0+a_1\theta+a_2\theta^2)(a_0+a_1\omega\theta+a_2\omega^2\theta^2)+\\ &\quad (a_0+a_1\theta+a_2\theta^2)(a_0+a_1\omega^2\theta+a_2\omega\theta^2)+\\ &\quad (a_0+a_1\omega\theta+a_2\omega^2\theta^2)(a_0+a_1\omega^2\theta+a_2\omega\theta^2)\\ &= 3a_0^2. \end{aligned}$$

Si α es de la primera forma la traza no nos aporta ninguna información, pues $T(\alpha)=c_0\in\mathbb{Z}$. Sin embargo la norma es

$$N(\alpha)=\frac{c_0^3+7c_1^3+49c_2^3-21c_0c_1c_2}{27}.$$

y el coeficiente de X en el polinomio característico de α es

$$f(\alpha)=\frac{c_0^2}{3}.$$

Como ambos son enteros, y $0\le c_0,c_1,c_2\le 2$, deducimos que $c_0=0$ y $7c_1^3+49c_2^3$ es múltiplo de 27. Supongamos que c_1 ó c_2 no es 0. Entonces c_1 y c_2 son ambos diferentes de 0 y por tanto $c_1,c_2\in\{1,2\}$. Pero $0\equiv 7c_1^3+49c_2^3\equiv c_1+c_2 \mod 3$ y por tanto $\{c_1,c_2\}=\{1,2\}$ con lo que $\{c_1^3,c_2^3\}=\{1,8\}$. Pero $c_1^3\equiv -c_2^3\equiv\pm 1 \mod 9$ y, por tanto, $0\equiv 7c_1^3+49c_2^3\equiv\pm 42 \mod 9$, que nos proporciona una contradicción. Esto prueba que $c_1=c_2=0$. ∎

2.6 El anillo de enteros del compositum de dos cuerpos de números

Si R y S son dos subanillos de un anillo fijo A entonces RS denota el menor subanillo de A que contiene a R y a S. Esto tiene sentido por tanto para todos los subanillos de $\mathbb{C}$ y en particular para los cuerpos de números y sus anillos de enteros.

Lema 2.30 *Sean K y F dos cuerpos de números tales que $[KF:\mathbb{Q}] = [K:\mathbb{Q}]\,[F:\mathbb{Q}]$. Entonces para cada inclusión σ de K en $\mathbb{C}$ y cada inclusión τ de F en $\mathbb{C}$ existe una única inclusión de KF en $\mathbb{C}$ que extiende σ y τ.*

Demostración. Sea $n = [F:\mathbb{Q}]$. Entonces $[KF:K] = [KF:\mathbb{Q}] : [K:Q] = [F:\mathbb{Q}] = n$ y por tanto σ tiene n extensiones diferentes a una inclusión de KF en $\mathbb{C}$. Todas ellas tienen que tener restricciones distintas a F con lo cual una de ellas, y solo una, se restringe a τ. ∎

Proposición 2.31 *Sean K y F dos cuerpos de números. Si $[KF:\mathbb{Q}] = [K:\mathbb{Q}]\,[F:\mathbb{Q}]$ y $d = \operatorname{mcd}(\Delta_K, \Delta_F)$ entonces*

$$\mathbb{A}_K\mathbb{A}_F \subseteq \mathbb{A}_{KF} \subseteq \frac{1}{d}\mathbb{A}_K\mathbb{A}_F.$$

En particular, si $d = 1$ entonces $\mathbb{A}_{KF} = \mathbb{A}_K\mathbb{A}_F$.

Demostración. Sean $\alpha_1, \ldots, \alpha_m$ una base entera de K y $\beta_1, \ldots, \beta_n$ una base entera de F. Luego $m = [K:\mathbb{Q}]$ y $n = [F:\mathbb{Q}]$ y, por hipótesis, $[KF:\mathbb{Q}] = mn$. Como además $KF = \sum_{i=1}^m \sum_{j=1}^n \mathbb{Q}\alpha_i\beta_j$ deducimos que los $\alpha_i\beta_j$ forman una base de F sobre $\mathbb{Q}$. Claramente $\mathbb{A}_K\mathbb{A}_F \subseteq \mathbb{A}_{KF}$. Sea $\gamma \in \mathbb{A}_{KF}$. Entonces

$$\gamma = \sum_{i,j} \frac{a_{ij}}{r}\alpha_i\beta_j$$

con r y todos los $a_{i,j}$ enteros tales que $\operatorname{mcd}(r, \operatorname{mcd}(a_{i,j})) = 1$. Queremos demostrar que $\gamma \in \frac{1}{d}\mathbb{A}_K\mathbb{A}_F$, para lo cual basta demostrar que $r \mid d$ y para ello demostraremos que r divide a Δ_K y de forma análoga demostraríamos que r divide a Δ_F.

Sean $\sigma_1, \ldots, \sigma_m$ las inclusiones de K en $\mathbb{C}$. Por el Lema 2.30, cada σ_i tiene una única extensión a KF cuya restricción a F es la identidad. Denotaremos esta extensión también σ_i. Sea $x_i = \sum_{j=1}^n \frac{a_{i,j}}{r}\beta_j$ para cada $i = 1, \ldots, m$. Entonces

$$\sigma_k(\gamma) = \sum_{i,j} \frac{a_{i,j}}{r}\sigma_k(\alpha_i)\beta_j = \sum_{i=1}^m \sigma_k(\alpha_i)x_i.$$

Por tanto los x_i forman una solución de un sistema de ecuaciones lineales en el que la matriz de los coeficientes es $(\sigma_k(\alpha_i))$ y los términos independientes son los $\sigma_k(\gamma)$. El determinante de la matriz de los coeficientes es $\delta = \pm\sqrt{\Delta_K} \neq 0$ con lo que se trata de un sistema de Cramer. Resolviendo por Cramer obtendremos $x_i = \frac{y_i}{\delta}$ con δ y todos los y_i enteros, pues los coeficientes

y términos independientes del sistema lo son. Por tanto los siguientes números complejos son enteros algebraicos para cada i:

$$\delta y_i = \delta^2 x_i = \Delta_K x_i = \sum_{j=1}^{n} \frac{\Delta_K a_{i,j}}{r} \beta_j.$$

Por tanto se trata de elementos de $\mathbb{A}_F$ y como los β_j forman una base entera de F sobre $\mathbb{Z}$ deducimos que $\frac{\Delta_K a_{i,j}}{r} \in \mathbb{Z}$ para todo i y j. Luego r divide a $\mathrm{mcd}(\Delta_K a_{i,j} : i,j) = \Delta_K \mathrm{mcd}(a_{i,j} : i,j)$ y como r es coprimo con $\mathrm{mcd}(a_{i,j} : i,j)$ deducimos que r divide a Δ_K, como queríamos. ∎

2.7 Enteros ciclotómicos

Esta sección la vamos a dedicar a estudiar los cuerpos ciclotómicos y su anillo de enteros. Si m es un entero positivo entonces el m-ésimo *cuerpo ciclotómico* es $\mathbb{Q}_m = \mathbb{Q}(\zeta_m)$, donde $\zeta_m = e^{\frac{2\pi i}{m}}$, una raíz primitiva m-ésima compleja de la unidad.

Usamos φ para denotar la función de Euler, o sea $\varphi(n)$ es el cardinal del grupo de unidades de $\mathbb{Z}_n$.

Empezamos calculando los conjugados de ζ_m.

Proposición 2.32 *Los conjugados de ζ_m son los elementos de la forma ζ_m^k con $\mathrm{mcd}(k,m) = 1$. En consecuencia, $[\mathbb{Q}_m : \mathbb{Q}] = \varphi(m)$,*

$$Min_{\mathbb{Q}}(\zeta_m) = \prod_{\substack{1 \le k < m \\ \mathrm{mcd}(k,m)=1}} (X - \zeta_m^k)$$

y $\mathbb{Q}_m/\mathbb{Q}$ es una extensión de Galois cuyo grupo de Galois es

$$\mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q}) = \{\sigma_k : 1 \le k \le m, \mathrm{mcd}(k,m) = 1\}$$

donde σ_k está determinado por $\sigma_k(\zeta_m) = \zeta_m^k$. Además la aplicación

$$\begin{array}{ccc} \mathbb{Z}_n^* & \to & \mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q}) \\ k & \mapsto & \sigma_k \end{array}$$

es un isomorfismo de grupos.

Demostración. Los elementos de la forma ζ_m^k con $\mathrm{mcd}(k,m) = 1$ son las raíces m-ésimas primitivas de la unidad. Por tanto tenemos que demostrar que los conjugados de ζ_m son precisamente las raíces m-ésimas primitivas de la unidad. Si α es conjugado de ζ_m entonces $\alpha^m = 1$ y $\alpha^d \neq 1$ para todo $d < m$. Por tanto, α es una raíz m-ésima primitiva de la unidad.

Antes de demostrar el recíproco demostraremos que si ξ es una raíz m-ésima primitiva de la unidad y p es un primo que no divide a m entonces ξ y ξ^p son conjugados sobre $\mathbb{Q}$. En efecto, sea f el polinomio mínimo de ξ sobre $\mathbb{Q}$. Entonces $X^m - 1 = f(X)g(X)$ para algún $g \in \mathbb{Q}[X]$

mónico. Del Lema 2.15 deducimos que $f \in \mathbb{Z}[X]$ y del Lema 2.14 que $g \in \mathbb{Z}[X]$. Como ξ^p es una raíz de $X^m - 1$, también será raíz de f ó g y queremos demostrar que ξ^p es raíz de f. En caso contrario $g(\xi^p) = 0$. Luego ξ es raíz del polinomio $g(X^p)$, con lo que $f(X)$ divide a $g(X^p)$ en $\mathbb{Q}[X]$. Aplicando el Lema de Gauss de nuevo deducimos que en realidad $f(X)$ divide a $g(X^p)$ en $\mathbb{Z}[X]$. Reduciendo módulo p, que lo denotamos usando barras, deducimos que $\overline{f}(X)$ divide a $\overline{g}(X^p) = \overline{g}(X)^p$. Como $\mathbb{Z}_p[X]$ es un dominio de factorización única deducimos que $\overline{f}(X)$ y $\overline{g}(X)$ tienen un factor común irreducible $h(X)$ en $\mathbb{Z}_p[X]$. Luego $h^2(X) \mid \overline{f}(X)\overline{g}(X) = \overline{X^m - 1}$. Por tanto que $X^m - 1$ tiene una raíz múltiple en una clausura algebraica $\overline{\mathbb{Z}_p}$ de $\mathbb{Z}_p$. Pero eso implica que su derivada, que es mX^{m-1}, tiene una raíz común con $X^m - 1$ en $\mathbb{Z}_p$, lo cual no es posible pues como $p \nmid m$, la única raíz del primero es 0 que no es raíz del segundo. Concluimos que ξ^p es raíz del polinomio mínimo f de ξ sobre $\mathbb{Q}$, o lo que es lo mismo ξ^p es conjugado de ξ sobre $\mathbb{Q}$, que es lo que queríamos demostrar.

Finalmente demostramos que si k es coprimo con m entonces ζ_m^k es conjugado con ζ_m sobre $\mathbb{Q}$. Para ello razonamos en la longitud de la factorización de k. Cuando esa longitud sea 0 no hay nada que demostrar y si es 1 entonces la afirmación es consecuencia de lo demostrado en el párrafo anterior. Para el paso de inducción, si p divide a k entonces ζ_m es conjugado de ζ_m^p por el párrafo anterior y ζ_m^p es conjugado de $\zeta_m^k = (\zeta_m^p)^{\frac{k}{p}}$ por la hipótesis de inducción. Como el ser conjugado es una relación de equivalencia, ζ_m es conjugado de ζ_m^k sobre $\mathbb{Q}$. ∎

Lema 2.33 *Sean m y h dos enteros positivos con $m \mid h$. Entonces $\varphi(m) = \varphi(h)$ si y solo si $m = h$ ó m es impar y $h = 2m$.*

Demostración. Es facil ver que si m es impar entonces $\varphi(2m) = \varphi(m)$. Esto demuestra una implicación.

Supongamos que $p_1, p_2, \ldots, p_r$ son los primos impares que dividen a m y $q_1, \ldots, q_s$ son los primos impares que dividen a h pero no a m. Sean $p_0 = \text{mcd}(2, m)$ y $q_0 = \text{mcd}(2, h)$. Supongamos que $\varphi(m) = \varphi(h)$. Entonces

$$m\frac{(p_1 - 1)\ldots(p_r - 1)}{p_0 p_1 \ldots p_r} = \varphi(m) = \varphi(h) = h\frac{(p_1 - 1)\ldots(p_r - 1)(q_1 - 1)\ldots(q_s - 1)}{q_0 p_1 \ldots p_r q_1 \ldots q_s}.$$

Por tanto, $\frac{q_0}{p_0} q_1 \cdots q_s \mid \frac{h}{m} = \frac{q_0}{p_0}\frac{q_1 \ldots q_s}{(q_1 - 1)\ldots(q_s - 1)}$ y por tanto $q_1 \cdots q_s \leq \frac{q_1 \ldots q_s}{(q_1 - 1)\ldots(q_s - 1)} \leq q_1 \cdots q_s$. Como todos los q_i son impares, en realidad no puede haber ninguno, es decir todos los primos impares que dividen a m también dividen a h. De la fórmula anterior concluimos que si m es par o h es impar entonces $h = m$. En otro caso, m es impar y $h = 2m$. ∎

Corolario 2.34 *Sean m y n dos enteros positivos con $m < n$. Entonces*

(1) $\mathbb{Q}_m = \mathbb{Q}_n$ si y solo si m es impar y $n = 2m$.

(2) El conjunto de las raíces de la unidad de $\mathbb{Q}_m$ está formado por las raíces $\text{mcm}(2, m)$*-ésimas de la unidad.*

Demostración. (1) Si m es impar entonces $-\zeta_m$ es una raíz $2m$-ésima primitiva de la unidad. De la Proposición 2.32 deducimos que $-\zeta_m$ y ζ_{2m} son conjugados y por tanto $\mathbb{Q}_m = \mathbb{Q}(-\zeta_m) = \mathbb{Q}_{2m}$. Recíprocamente, supongamos que $\mathbb{Q}_m = \mathbb{Q}_n$. Por tanto $\varphi(m) = \varphi(n)$ por la Proposición 2.32. Si m divide a n entonces, por el Lema 2.33 se tiene m es impar y $n = 2m$. Supongamos que m no divide a n y sea $k = \text{mcm}(m, n)$. Entonces $\langle \zeta_m, \zeta_n \rangle$ es un subgrupo finito de $\mathbb{Q}_m^* = \mathbb{Q}_n^*$ de orden múltiplo de k. Como todo subgrupo finito del grupo de unidades de un grupo es cíclico deducimos que $\mathbb{Q}_m$ tiene una raíz k-ésima primitiva de la unidad y por tanto $\mathbb{Q}_k \subseteq \mathbb{Q}_m \subseteq \mathbb{Q}_k$. Concluímos que $\mathbb{Q}_m = \mathbb{Q}_k = \mathbb{Q}_n$, m y n son divisores de k con $\varphi(m) = \varphi(n) = \varphi(k)$. Del Lema 2.33 deducimos que m es impar y $n = k = 2m$.

(2) Como consecuencia de la condición suficiente de (1), podemos suponer sin pérdida de generalidad que m es par. En tal caso lo que hay que demostrar es que toda raíz de la unidad de $\mathbb{Q}_m$ es una raíz m-ésima de la unidad. Supongamos que ξ es una raíz de la unidad de $\mathbb{Q}_m$ de orden n y sea k el mínimo común múltiplo de n y m. Entonces $\langle \zeta_m, \xi \rangle$ es un subgrupo finito de $\mathbb{C}^*$ con un elemento de orden m y otro de orden n. Como todo subgrupo finito de un cuerpo es cíclico el orden de dicho grupo es cíclico múltiplo de k, con lo que $\zeta_k \in \langle \zeta, \xi \rangle \subseteq \mathbb{Q}_m$. Como claramente $\zeta_m \in \mathbb{Q}_k$, deducimos que $\mathbb{Q}_m = \mathbb{Q}_k$. Como m es par y $m \leq k$, de (1) deducimos que $m = k$, es decir n divide a m. Por tanto ξ es una raíz m-ésima de la unidad. ∎

Corolario 2.35 *Si m es una potencia de un primo p entonces*

$$N_{\mathbb{Q}_m/\mathbb{Q}}(1 - \zeta_m) = p \quad y \quad \frac{p}{(1-\zeta_m)^{\varphi(m)}} \in \mathbb{Z}[\zeta_m].$$

Demostración. Supongamos que $m = p^r$ y sea $f = \text{Min}_{\mathbb{Q}}(\zeta_m)$. Entonces, de la Proposición 2.32 se tiene que

$$f = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = 1 + X^{p^{r-1}} + \cdots + X^{p^{r-1}(p-1)} = \prod_{\substack{1 \leq k < m \\ p \nmid m}} (X - \zeta_m^k)$$

pues las raíces de $X^{p^r} - 1$ son las raíces p^r-ésimas de la unidad. Usando de nuevo la Proposición 2.32 se tiene que

$$N_{\mathbb{Q}_m/\mathbb{Q}}(1 - \zeta_m) = \prod_{\substack{1 \leq k < m \\ p \nmid m}} (1 - \zeta_m^k) = f(1) = p.$$

Por tanto

$$\frac{p}{(1-\zeta_m)^{\varphi(m)}} = \prod_{p \nmid m, 1 \leq k < m} \frac{1 - \zeta_m^k}{1 - \zeta_m}$$

y esto pertenece a $\mathbb{Z}[\zeta_m]$ pues $\frac{1-\zeta_m^k}{1-\zeta_m} = 1 + \zeta_m + \cdots + \zeta_m^{k-1}$ para todo k. ∎

Lema 2.36 *$\Delta_{\mathbb{Q}_m/\mathbb{Q}}(\zeta_m)$ y $\Delta_{\mathbb{Q}_m/\mathbb{Q}}(1 - \zeta_m)$ son iguales y dividen a $m^{\varphi(m)}$.*

Demostración. Pongamos $\Delta = \Delta_{\mathbb{Q}_m/\mathbb{Q}}$. Sean $\xi_1, \ldots, \xi_n$ los conjugados de ζ_m. Entonces los conjugados de $1-\zeta_m$ son $1-\xi_1, \ldots, 1-\xi_n$. De la Proposición 1.6.(3) deducimos

$$\Delta(1-\zeta_m) = \prod_{i<j}((1-\xi_i)-(1-\xi_j))^2 = \prod_{i<j}(\xi_i-\xi_j)^2 = \Delta(\zeta_m).$$

Sea f el polinomio mínimo de ζ_m sobre $\mathbb{Q}$. Del Lema 2.14 tenemos que $X^m-1 = f(X)g(X)$ para algún $g \in \mathbb{Z}[X]$. Tomando derivadas y sustituyendo X por ζ_m deducimos que $m = \zeta_m m\zeta_m^{m-1} = \zeta_m f'(\zeta_m)g(\zeta_m)$. Tomando normas, de la Proposición 1.6.(3) deducimos

$$m^{\varphi(m)} = N(f'(\zeta_m))N(\zeta_m g(\zeta_m)) = \Delta(\zeta_m)N(\zeta_m g(\zeta_m)).$$

Como $\zeta_m g(\zeta_m)$ es entero deducimos que su norma es un número entero y por tanto $\Delta(\zeta_m)$ divide a $m^{\varphi(m)}$. ∎

Teorema 2.37 *El anillo de enteros de $\mathbb{Q}_m$ es $\mathbb{Z}[\zeta_m]$.*

Demostración. Sea R el anillo de enteros de $\mathbb{Q}_m$. Tenemos que demostrar que $R = \mathbb{Z}[\zeta_m]$. Si $m = 1$ entonces $\mathbb{Q}_m = \mathbb{Q}$ y, por tanto, $R = \mathbb{Z} = \mathbb{Z}[\zeta_1]$. Suponemos pues que $m > 1$ y razonamos por inducción en el número de divisores primos de m.

Supongamos que m es divisible por un único primo p. Sean $\theta = 1-\zeta_m$ y $n = \varphi(m)$. Como $\mathbb{Z}[\zeta_m] = \mathbb{Z}[\theta]$, basta demostrar que $1, \theta, \theta^2, \ldots, \theta^{n-1}$ forman una base entera de $\mathbb{Q}_m$. Por reducción al absurdo suponemos que no lo es. Del Lema 2.36 se tiene que $\Delta(\theta)$ es una potencia de p y por tanto, del Lemma 2.28 se tiene que R contiene un elemento no nulo de la forma

$$\alpha = \frac{1}{p}(c_0 + c_1\theta + c_2\theta^2 + \ldots c_n\theta^{n-1})$$

con $0 \leq c_i < p$ para todo i. Tomando $1 \leq i \leq n$ con $c_{i-1} \neq 0$ y teniendo en cuenta que $\frac{p}{\theta^i} = \theta^{n-i}\frac{p}{\theta^n} \in \mathbb{Z}[\theta] \subseteq R$, por el Lema 2.35, deducimos que $\frac{c_{i-1}}{\theta} = \alpha\frac{p}{\theta^i} - \sum_{j=i}^{n-1} c_j\theta^{j-i} \in R$. Tomando normas deducimos que $\frac{c_{i-1}^n}{p} \in \mathbb{Z}$. Pero esto es imposible pues $1 \leq c_{i-1} < p$.

Supongamos ahora que m es divisible por más de un primo y pongamos $m = m_1m_2$ con m_1 una potencia de un primo y m_2 coprimo con m_1. Por hipótesis de inducción el anillo de enteros de $\mathbb{Q}_{m_i}$ es $\mathbb{Z}[\zeta_{m_i}]$ para $i = 1, 2$. Eso implica que $\Delta_{\mathbb{Q}_{m_i}} = \Delta(\zeta_{m_i})$ y además, este último divide una potencia de m_i por el Lema 2.36. Por tanto $\Delta_{\mathbb{Q}_{m_1}}$ y $\Delta_{\mathbb{Q}_{m_2}}$ son coprimos. Además, $[\mathbb{Q}_m : \mathbb{Q}] = \varphi(m) = \varphi(m_1)\varphi(m_2) = [\mathbb{Q}_{m_1} : \mathbb{Q}]\ [\mathbb{Q}_{m_2} : \mathbb{Q}]$ y $\mathbb{Q}_m = \mathbb{Q}_{m_1}\ \mathbb{Q}_{m_2}$. Usando la Proposición 2.31 deducimos que el anillo de enteros de $\mathbb{Q}_m$ es $\mathbb{Z}[\zeta_{m_1}]\mathbb{Z}[\zeta_{m_2}]$, es decir el menor subanillo de $\mathbb{C}$ que contiene a ζ_{m_1} y ζ_{m_2} y dicho anillo es $\mathbb{Z}[\zeta_m]$ pues $\zeta_{m_1}\zeta_{m_2}$ y ζ_m son ambos raíces m-ésimas primitivas de la unidad por ser m_1 y m_2 coprimos. ∎

Capítulo 3

Anillos de enteros con factorización única

3.1 Factorización en anillos de enteros

Recordemos que un ideal I de A se dice *finitamente generado* si es de la forma (X) para X un subconjunto finito de A.

Proposición 3.1 *Las siguientes condiciones son equivalentes para un anillo A:*

(1) Si $I_1 \subseteq I_2 \subseteq \ldots$ es una cadena de ideales de A, entonces existe $n \in \mathbb{N}$, tal que $I_n = I_{n+h}$ para todo $h \in \mathbb{N}$.

(2) Todo conjunto no vacio de ideales de A tiene un elemento maximal.

(3) Todo ideal de A es finitamente generado.

Demostración. (1) implica (2) Si X es un conjunto no vacio de ideales de A que no tiene ningún elemento maximal entonces partiendo de cualquier elemento I de X podemos construir una sucesión estrictamente creciente $I_1 = I \subset I_2 \subset \ldots$ de elementos de X.

(2) implica (3) Sea I un ideal de A que no es finitamente generado y sea X el conjunto de los ideales finitamente generados de A contenidos en I. Claramente X no es vacío. Vamos a ver que X no tiene ningún elemento maximal. En efecto, si J fuera un elemento maximal de X entonces $I \neq J$, ya que J es finitamente generado e I no lo es, y por tanto existe $x \in I \setminus J$. Entonces $K = (J, x)$ es un elemento de X que contiene propiamente a J, en contra de la elección de J.

(3) implica (1) Supongamos que todo ideal de A es finitamente generado y sea $I_1 \subseteq I_2 \subseteq \ldots$ es una sucesión de ideales de A. Entonces $I = \cup_{i \geq 1} I_i$ es un ideal de A. (Observa que esto no funcionaría si los ideales no formaran una cadena.) Por hipótesis $I = (x_1, \ldots, x_n)$ y cada x_i está en algún I_{j_i}. Si $j = \max\{j_1, \ldots, j_n\}$ tenemos que $I = (x_1, \ldots, x_n) \subseteq I_j \subseteq I_k \subseteq I$ para todo $k \geq j$ con lo que $I_k = I$ para todo $k \geq j$. ∎

Los anillos que satisfacen las condiciones equivalentes de la proposición anterior se llaman *noetherianos*. Obviamente todos los dominios de ideales principales son anillos noetherianos.

Teorema 3.2 *Todo dominio noetheriano es un dominio de factorización.*

Demostración. Sea X el conjunto de los elementos no nulos de D que ni son unidades ni se pueden escribir como producto de irreducibles. Tenemos que demostrar que X es vacio. En caso contrario, $\{Dx : x \in X\}$ tendrá un elemento maximal (x). Entonces x no es una unidad, ni es irreducible, luego $x = yz$ para ciertos $y, z \in D$, tales que ni y ni z son unidades. Luego (y) y (z) contienen propiamente a (x) y, por tanto, no están en X. Eso implica que y y z se pueden escribir como producto de irreducibles y, por tanto, x también es un producto de irreducibles, en contra de la definición de X. ∎

Teorema 3.3 *El anillo de enteros de un cuerpo de números es noetheriano y, en particular, es un dominio de factorización.*

Demostración. Por el Teorema 2.25, el grupo aditivo de un anillo de enteros D es libre de rango finito. Por tanto todo ideal de D, que es un subgrupo de D, es también libre de rango finito, y por tanto es finitamente generado como ideal. ∎

Ejemplo 3.4 2 *es irreducible pero no primo en* $\mathbb{Z}[\sqrt{-5}]$.

Demostración. La norma en $\mathbb{Z}[\sqrt{-5}]$ viene dada por

$$N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

Si $2 = xy$, con x e y no unidades de $\mathbb{Z}[\sqrt{-5}]$, entonces $4 = N(xy) = N(x)N(y)$ y, por tanto $N(x) = N(y) = \pm 2$, lo cual es imposible porque no hay ningún elemento con norma ± 2 en $\mathbb{Z}[\sqrt{-5}]$. Esto prueba que 2 es irreducible. Por otro lado $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, pero 2 no divide ni a $1 + \sqrt{-5}$ ni a $1 - \sqrt{-5}$ por que ambos tienen norma 6, que no es un multiplo de $4 = N(2)$. ∎

Obsérvese que si K es un cuerpo de números entonces la aplicación $\phi(\alpha) = |N_{K/\mathbb{Q}}(\alpha)|$ satisface el primer axioma de función euclídea. Decimos K tiene norma euclídea si la restricción de ϕ a $\mathbb{A}_K$ define una función euclídea en $\mathbb{A}_K$.

Lema 3.5 *Sea K un cuerpo de números y sea D su anillo de enteros. La norma define una función euclídea en K si y solo si para todo $\epsilon \in K$ existe $q \in D$ tal que $|N_{K/\mathbb{Q}}(\epsilon - q)| < 1$.*

Demostración. Mantenemos la notación $\phi(x) = |N_{K/\mathbb{Q}}(x)$ para $x \in K$. Supongamos que K tiene norma euclídea sea $\epsilon \in K \setminus \{0\}$. Por el Lema 2.11 existe $n \in \mathbb{Z}^+$, tal que $n\epsilon \in D$. Por hipótesis existen $q, r \in D$ tales que $n\epsilon = nq + r$ y $r = 0$ o $\phi(r) < \phi(n)$. Si $r = 0$, entonces $|N_{K/\mathbb{Q}}(\epsilon - q)| = 0 < 1$. Si $\phi(r) < \phi(n)$ entonces $|N_{K/\mathbb{Q}}(\epsilon - q)| = \phi\left(\frac{r}{n}\right) = \frac{\phi(r)}{\phi(n)} < 1$.

Recíprocamente, supongamos que se cumple la propiedad y sean $a, b \in D \setminus \{0\}$. Por hipótesis existe $q \in D$ tal que $N_{K/\mathbb{Q}}\left(\frac{a}{b} - q\right) < 1$. Sea $r = a - bq$. Entonces $r \in D$ y o bien $r = 0$ o bien $\phi(r) = \phi(b)\phi\left(\frac{a}{b} - q\right) < \phi(b)$. ∎

Teorema 3.6 *Si d es un entero negativo libre de cuadrados entonces $\mathbb{Q}(\sqrt{d})$ tiene norma euclídea si y sólo si $d = -1, -2, -3, -7, -11$.*

Demostración. Sea D el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ y sea $\epsilon = r + s\sqrt{d} \in K$ con $r, s \in \mathbb{Q}$

Supongamos primero que $d \not\equiv 1 \mod 4$. Entonces $D = \mathbb{Z}[\sqrt{d}]$. Por tanto todo elemento de D es de la forma $q = x + y\sqrt{d}$ con $x, y \in \mathbb{Z}$ y

$$\phi(\epsilon - q) = (r - x)^2 - d(r - y)^2.$$

Si elegimos $x, y \in \mathbb{Z}$ tales que $|r - x|$ y $|s - y|$ sean mínimos. Entonces $|r - x|, |s - y| \leq \frac{1}{2}$ con lo que $\phi(\epsilon - q) = (r - x)^2 - d(s - y)^2 \leq \frac{1-d}{4}$. Si $d = -1$ ó $d = -2$ entonces $1 - d \leq 3$ con lo que en ambos casos $\phi(\epsilon - q) \leq \frac{3}{4} < 1$. Por tanto, la condición del Lema 3.5 se cumple en estos casos. Sin embargo, si $d < -2$ y $d \not\equiv 1 \mod 4$ entonces $1 - d > 4$. Si tomamos $\epsilon = \frac{1}{2} + \frac{1}{2}\sqrt{d}$ entonces para todo $x, y \in \mathbb{Z}$ se tiene que $|x - \frac{1}{2}| \geq \frac{1}{2}$ e $|y - \frac{1}{2}| \geq \frac{1}{2}$ con lo que para todo $a \in \mathbb{Z}[\sqrt{d}]$ se verifica que $\phi(\epsilon - q) \geq \frac{1-d}{4} > 1$. Luego en este caso la norma no define una función euclídea por el Lema 3.5.

Supongamos ahora que $d \equiv 1 \mod 4$. Obsérvese que como $d < 0$ se tiene que $d \equiv 1 \mod 4$ y $d \geq -11$ si y solo si $d \in \{-3, -7, -11\}$. En este caso

$$D = \mathbb{Z}\left[\frac{1 + \sqrt{d}}{2}\right] = \left\{x + y\frac{1 + \sqrt{d}}{2} : x, y \in \mathbb{Z}\right\} = \left\{\frac{x + y\sqrt{d}}{2} : x, y \in \mathbb{Z}, x \equiv y \mod 2\right\}.$$

Tomemos $y \in \mathbb{Z}$ tal que $|2s - y|$ sea mínimo y para tal y tomamos $x \in \mathbb{Z}$ con $|r - \frac{y}{2} - x|$ mínimo. Por tanto $|2s - y|, |r - \frac{y}{2} - x| \leq \frac{1}{2}$. Si tomamos $q = x + y\frac{1+\sqrt{d}}{2}$ tenemos

$$\phi(\epsilon - q) = \left(r - x - \frac{y}{2}\right)^2 - d\left(\frac{2s - y}{2}\right)^2 \leq \frac{1}{4} - d\frac{1}{16} = \frac{4 - d}{16}.$$

En consecuencia si $d \geq -11$ entonces la norma define una función euclídea. Sin embargo si $d < -11$, como $d \equiv 1 \mod 4$ entonces $d \leq -15$. Tomando $\epsilon = \frac{1}{4} + \frac{1}{4}\sqrt{d}$ y $q \in D$ tenemos que $q = \frac{x+y\sqrt{d}}{2}$ con $x, y \in \mathbb{Z}$ y por tanto

$$\phi(\epsilon - q) = \frac{(1 - 2x)^2 - d(1 - 2y)^2}{16} \geq \frac{1 - d}{16} \geq 1.$$

con lo que $\mathbb{Q}(\sqrt{d})$ no tiene norma euclídea. ∎

De la Proposición 2.20 sabemos que $\mathbb{Z}[\sqrt{-5}]$ es el anillo de enteros de $\mathbb{Q}(\sqrt{-5})$, pero del Ejemplo 3.4 y el Teorema 1.11 sabemos que $\mathbb{Z}[\sqrt{-5}]$ no es un DFU y por tanto no es un dominio euclídeo.

Es más difícil aplicar el Lema 3.5 cuando es positivo pues en este caso $N(x+y\sqrt{d}) = x^2 - dy^2$ puede tomar valores negativos y positivos. Aquí dejamos un resultado sin demostración.

Teorema 3.7 *Sea d un entero positivo libre de cuadrados. Entonces la norma define una función euclídea en $\mathbb{Q}(\sqrt{d})$ si y solo si $d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 55, 73\}$.*

3.2 Aplicaciones de la factorización única en $\mathbb{Z}[i] = \mathbb{A}_{\mathbb{Q}(i)}$

En esta sección vamos a ver cómo resolver algunos problemas sobre los números enteros utilizando las propiedades del anillo de los enteros de Gauss $\mathbb{Z}[i]$. Obsérvese que $\mathbb{Z}[i]$ es el anillo de enteros de $\mathbb{Q}[i]$ (Proposición 2.20 ó Teorema 2.37), y $\mathbb{Z}[i]$ es un DFU por el Teorema 3.6. En toda la sección $N = N_{\mathbb{Q}(i)/\mathbb{Q}}$.

Ternas pitagóricas

Recordemos que una ecuación diofántica es una ecuación en la que las variables representan números enteros, o dicho de otra manera, cuando consideramos una ecuación como diofántica solo nos importan las soluciones formadas por números enteros.

Comenzamos considerando la ecuación pitagórica $x^2+y^2 = z^2$ como ecuación diofántica, es decir queremos encontrar las ternas de números enteros x, y, z para las que $x^2+y^2 = z^2$. Dichas ternas se llaman *ternas pitagóricas*. Para empezar si x, y y z son múltiplos de un número dado a entonces (x, y, z) es una terna pitagórica si y solo si lo es $\left(\frac{x}{a}, \frac{y}{a}, \frac{z}{a}\right)$. Por tanto, para calcular todas las ternas pitagóricas podemos restringirnos al caso en el que las tres componentes son coprimas. Eso es equivalente a que sean coprimas dos a dos pues un divisor de dos componentes de una terna pitagórica será divisor del tercero. En particular, una de las componentes es impar lo que implica que lo sean exactamente dos. Sin embargo x e y no pueden ser ambos impares por que en tal caso $2 \equiv x^2 + y^2 = z^2 \equiv 0 \mod 4$. Por tanto, z es impar y podemos suponer que x es impar e y es par.

Aunque solo nos interesen las soluciones enteras nos vamos a aprovechar del anillo $\mathbb{Z}[i]$ reescribiendo la ecuación como

$$(x + yi)(x - yi) = z^2.$$

Ya sabemos que x e y son enteros racionales coprimos en $\mathbb{Z}$. De hecho también lo son en $\mathbb{Z}[i]$, pues si p es un irreducible de $\mathbb{Z}[i]$ que divide a x y a y entonces $N(p)$ divide a $N(x) = x^2$ y a $N(y) = y^2$, con lo que $N(p)$ es una unidad de $\mathbb{Z}[i]$. Vamos a ver que $x + yi$ y $x - yi$ también son coprimos en $\mathbb{Z}[i]$. En caso contrario tendrían un divisor irreducible común p en $\mathbb{Z}[i]$, lo que implicaría que $p \mid 2x$ y $p \mid 2y$ en $\mathbb{Z}[i]$. Por tanto, $p \mid \text{mcd}(2x, 2y) = 2\text{mcd}(x, y) = 2 = -i(1+i)^2$. Como $N(1 + i) = 2$, de la Proposición 2.17.(4) deducimos que $1 + i$ es irreducible y como i es invertible se tiene que p es asociado de $1 + i$. Pero eso no es posible por que entonces $1 + i$ dividiría a $x + yi$ y a $x - iy$ y por tanto $2 = -i^3(1 + i)^2$ divide a z^2 en $\mathbb{Z}[i]$, lo que no es posible pues z es un entero impar. Por tanto $x + yi$ y $x - yi$ son coprimos en $\mathbb{Z}[i]$.

Usando que $\mathbb{Z}[i]$ es un DFU y la igualdad $(x + yi)(x - yi) = z^2$, deducimos que $x + yi = u(a + bi)^2 = u(a^2 - b^2 + 2abi)$ para $u \in \mathcal{U}(\mathbb{Z}[i])$ y $a, b \in \mathbb{Z}$. Como las únicas unidades de $\mathbb{Z}[i]$ son ± 1 y $\pm i$ pero y es par deducimos que necesariamente $u = \pm 1$ con lo que $\pm x = \pm(a^2 - b^2)$ e $y = \pm 2ab$. Finalmente, $z = \pm(a + bi)(a - bi) = \pm(a^2 + b^2)$. Obsérvese que como x, y y z son coprimos, necesariamente a y b son coprimos y como z es impar, de a y b tienen distinta paridad. Esto demuestra el siguiente

Teorema 3.8 *Las ternas pitagóricas son las de la forma* $(\pm(a^2 - b^2)c, \pm 2abc, \pm(a^2 + b^2)c)$ *con* a *y* b *coprimos de distinta paridad y* c *un entero, y las que se obtienen intercambiando las dos primeras coordenadas*

Teorema 3.9 *Si x e y son enteros no nulos entonces $x^4 + y^4$ no es un cuadrado.*

Demostración. Por reducción al absurdo suponemos que $x^4 + y^4 = z^2$ con x, y y z enteros positivos y z mínimo para el que existen x e y que satisfacen la igualdad. Entonces x, y y z son primos dos a dos, pues si p es un divisor primo de dos de ellos entonces también divide al tercero y de hecho p^2 divide a z. Entonces $\left(\frac{x}{p}\right)^4 + \left(\frac{y}{p}\right) = \left(\frac{z}{p^2}\right)^2$, en contra de la minimalidad de z.

El mismo argumento que utilizamos antes del Teorema 3.8 muestra que z es impar y podemos suponer que y es par y x impar. Aplicando el Teorema 3.8 obtenemos que existen r y s coprimos, uno de ellos par, tales que

$$x^2 = r^2 - s^2,\ y^2 = 2rs,\ z = r^2 + s^2.$$

Entonces

$$x^2 + s^2 = r^2$$

y x, r y s son coprimos dos a dos (pues x e y lo son). Aplicando el Teorema 3.8 deducimos que r es impar y por tanto s es par. Luego existen a y b coprimos tales que

$$x = a^2 - b^2,\ s = 2ab,\ r = a^2 + b^2.$$

Luego

$$y^2 = 2rs = 4ab(a^2 + b^2)$$

Pongamos $y = 2k$. Entonces

$$k^2 = ab(a^2 + b^2).$$

Pero como a, b y $a^2 + b^2$ son coprimos dos a dos, la ecuación anterior implica que los tres son cuadrados. Pongamos

$$a = c^2,\ b = d^2,\ a^2 + b^2 = e^2$$

Luego

$$c^4 + d^4 = e^2$$

y $e \leq a^2 + b^2 = r < z$, contradiciendo la minimalidad de z. ∎

Sumas de dos cuadrados

En esta sección vamos a ver una descripción de cuáles son los números que son suma de dos cuadrados. Obviamente son los elementos de $N(\mathbb{Z}[i])$ pero eso no proporciona un método efectivo para decidir si un número concreto es o no suma de dos cuadrados.

Comenzamos recordando el Teorema de Wilson.

Teorema 3.10 (Wilson) *Si K es un cuerpo finito entonces el producto de sus elementos no nulos es -1.*

Demostración. Está claro que el producto de los elementos no nulos de K es igual al producto de aquellos que sean su propio inverso que claramente son 1 y -1, de donde se deduce el resultado de forma obvia. ∎

Teorema 3.11 *Las siguientes condiciones son equivalentes para un número primo p.*

(1) p es suma de dos cuadrados.

(2) $p \not\equiv 3 \mod 4$.

(3) $p = 2$ ó $p \equiv 1 \mod 4$.

(4) -1 es un cuadrado en $\mathbb{Z}_p$.

(5) p no es irreducible en $\mathbb{Z}[i]$.

En tal caso solo hay una forma de escribir p como suma de dos cuadrados (salvo el orden de los sumandos).

Demostración. (1) implica (2). Los cuadrados de $\mathbb{Z}_4$ son 0 y 1, con lo que 3 no es suma de dos cuadrados de $\mathbb{Z}_4$.

(2) implica (3) es obvio.

(3) implica (4). En $\mathbb{Z}_2$ se tiene que $-1 = 1 = 1^2$. Supongamos que $p \equiv 1 \mod 4$ y pongamos $p = 4t + 1$. Entonces del Teorema de Wilson tenemos que

$$\begin{aligned} -1 &\equiv (p-1)! = (4t)! = (2t)! \left(\prod_{i=1}^{2t} (2t+i) \right) \equiv (2t)! \left(\prod_{i=1}^{2t} (i-2t-1) \right) \\ &= (2t)! \left(\prod_{i=1}^{2t} (2t+1-i) \right) = ((2t)!)^2 \mod p \end{aligned}$$

(4) implica (5). Si $-1 \equiv x^2 \mod p$ entonces $ap = x^2 + 1 = (x+i)(x-i)$ para algún entero a. Eso implica que $(x+i)(x-i) \in \mathbb{Z}[i]p$ y obviamente $x+i, x-i \notin \mathbb{Z}[i]p$. Eso implica que p no es primo en $\mathbb{Z}[i]$ y, como $\mathbb{Z}[i]$ es un DFU, p no es irreducible en $\mathbb{Z}[i]$.

(5) implica (1). Supongamos que p no es irreducible en $\mathbb{Z}[i]$ y sea $p = q_1 \dots q_n$ una factorización de p en producto de irreducibles de $\mathbb{Z}[i]$. Por hipótesis $n \geq 2$. Entonces $p^2 = N(q_1) \cdots N(q_n)$ y cada $N(q_i)$ es un entero mayor que 1, con lo $n = 2$ y $p = N(q_1) = N(q_2)$, lo que implica que p es suma de dos cuadrados.

Finalmente si $p = a_1^2 + a_2^2 = b_1^2 + b_2^2$ con a_i y b_i enteros positivos y $a = a_1 + b_1 i$ y $b = b_1 + b_2 i$ entonces a y b son irreducibles de $\mathbb{Z}[i]$, por la Proposición 2.17 y $p = a\overline{a} = b\overline{b}$. Como $\overline{a}$ y $\overline{b}$ también son irreducibles, de la factorización única de $\mathbb{Z}[i]$ se tiene que b es asociado de a ó $\overline{a} = a_1 - a_2 i$. Pero los asociados de a son $a = a_1 + a_2 i, -a = -a_1 - a_2 i, ia = -a_2 + a_1 i$ y $-ia = a_2 - a_1 i$ y los de $\overline{a}$ son $a_1 - a_2 i$, $-a_1 + a_2 i$, $a_2 + a_1 i$ y $-a_2 - a_1 i$. Como los a_i y b_i son no negativos tenemos que $b = a$ ó $b = a_2 + a_1 i$, en cualquier caso. ∎

Corolario 3.12 *Los irreducibles de $\mathbb{Z}[i]$ son los asociados de primos racionales congruentes con 3 módulo 4 y los elementos $a \in \mathbb{Z}[i]$ con $N(a)$ primo que no es congruente con 3 módulo 4.*

Demostración. De la Proposición 2.17 y del Teorema 3.11 se deduce que los elementos que se mencionan son irreducibles de $\mathbb{Z}[i]$. Vamos a ver que son todos los irreducibles. Sea $x = a + bi$ un irreducible de $\mathbb{Z}[i]$. Si x es asociado de un número entero positivo entonces dicho número entero debe de ser irreducible en $\mathbb{Z}[i]$ con lo que será un número primo congruente con 3 módulo 4, por el Teorema 3.11. Supongamos que x no es asociado de un número entero y pongamos $N(x) = nm$ con n y m enteros positivos. Entonces x divide a n ó m en $\mathbb{Z}[i]$. Supongamos que x divide a n en $\mathbb{Z}[i]$. Entonces $\overline{x} = \frac{n}{x}m$ y $\frac{n}{x}$ no es invertible en $\mathbb{Z}[i]$ por hipótesis. Como $\overline{x}$ es irreducible de $\mathbb{Z}[i]$ tenemos que m es un entero positivo que es invertible en $\mathbb{Z}[i]$, es decir $m = 1$. Esto demuestra que $N(x)$ es un número primo que es suma de dos cuadrados y por tanto no es congruente con 3 módulo 4. ∎

Teorema 3.13 *Un entero positivo n es suma de dos cuadrados si y solo si el exponente en la factorización de n de cada primo p congruente con 3 módulo 4 es par.*

Demostración. Supongamos que $n = p_1^{2\alpha_1} \cdots p_k^{2\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l}$ donde $p_1, \ldots, p_k$ son los primos que dividen a n que son congruentes con 3 módulo 4. Por el Teorema 3.11 para cada $i = 1, \ldots, l$ tenemos $q_i = N(b_i)$ para algún $a_i \in \mathbb{Z}[i]$, con lo que $n = N(p_1^{\alpha_1} \cdots p_k^{\alpha_k} b_1 \ldots b_l)$. Luego n es suma de dos cuadrados.

Recíprocamente, supongamos que n es suma de dos cuadrados, con lo que $n = N(a)$ para algún $a \in \mathbb{Z}[i]$. De la Proposición 3.12 deducimos que la factorización de a en $\mathbb{Z}[i]$ será de la forma $a = p_1^{\alpha_1} \ldots p_k^{\alpha_k} b_1^{\beta_1} \ldots b_l^{\beta_l}$ con p_i números primos congruentes con 3 módulo 4 y $q_j = N(b_j)$ un número primo no congruente con 3 módulo 4. Por tanto $n = N(a) = p_1^{\alpha_1} \ldots p_k^{2\alpha_k} q_1^{\beta_1} \cdots p_l^{\beta_l}$ es una factorización de n en $\mathbb{Z}$ que cumple las condiciones del Teorema. ∎

3.3 Una aplicación de la factorización única en $\mathbb{Z}[\zeta_3] = \mathbb{A}_{\mathbb{Q}(\zeta_3)}$

En esta sección vamos a demostrar el Teorema de Fermat para exponente 3. Para ello vamos a usar el anillo de enteros de $\mathbb{Q}(\zeta_3)$ que es $\mathbb{Z}[\zeta_3]$ por el Teorema 2.37. En realidad $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = \varphi(3) = 2$, con lo que $\mathbb{Q}(\zeta_3)$ es un cuerpo cuadrático. De hecho $\zeta_3 = e^{\frac{2\pi i}{3}} = \cos\frac{2\pi}{3} + \operatorname{sen}\frac{2\pi}{3} = \frac{-1+\sqrt{-3}}{2} = \frac{1+\sqrt{-3}}{2} - 1$ con lo que $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ y otra forma de ver que el anillo de enteros de este cuerpo es usar el Teorema 2.20. Además los elementos de $\mathbb{Z}[\zeta_3]$ son los de la forma $\frac{a+b\sqrt{-3}}{2}$ con a y b enteros de la misma paridad. Del Teorema 3.6 se tiene que $\mathbb{Z}[\zeta_3]$ es un dominio euclídeo y en particular es un DFU.

Vamos a abreviar poniendo $N = N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}$. Obsérvese que $N(a + b\sqrt{-3}) = (a + b\sqrt{-3})(a - b\sqrt{-3}) = a^2 + 3b^2$ que es siempre no negativo.

Por el Teorema 1.2, las raíces de la unidad de $\mathbb{Q}(\zeta)$ son precisamente los elementos de $\langle\zeta_6\rangle = \langle -\zeta_3\rangle$. Por supuesto todas las raíces de la unidad son enteros y elementos invertibles de $\mathbb{Z}[\zeta_3]$. Por tanto $\langle\zeta_6\rangle$ es un subgrupo de $\mathcal{U}(\mathbb{Z}[\zeta_3])$. De hecho se verifica la igualdad pues si $x \in$

$\mathcal{U}(\mathbb{Z}[\zeta_3])$ entonces $x = \frac{a+b\sqrt{-3}}{2}$ con a y b enteros de la misma paridad y, por la Proposición 2.17, se tiene $1 = N(x) = \frac{a+b\sqrt{-3}}{2} \cdot \frac{a-b\sqrt{-3}}{2} = \frac{a^2+3b^2}{4}$. Luego $a^2 + 3b^2 = 4$, con lo que o bien $b = 0$ y $a = \pm 2$, lo que implica que $x = \pm 1$ o bien $a = \pm 1$ y $b = \pm 1$. En total hay seis unidades que son los seis elementos de $\langle \zeta_6 \rangle$.

El siguiente elemento va a representar un papel muy importante:

$$\lambda = 1 - \zeta_3 = \frac{3 - \sqrt{-3}}{2}.$$

Lema 3.14 *(1) λ es irreducible en $\mathbb{Z}[\zeta_3]$.*

(2) $\mathbb{Z}[\zeta_3]/\lambda\mathbb{Z}[\zeta_3]$ tiene exactamente 3 elementos representados por $0, 1$ y 2 respectivamente.

(3) Si a y b son dos elementos de $\mathbb{Z}[\zeta_3]$ tales que $a \equiv b \mod \lambda$, entonces $a^3 \equiv b^3 \mod \lambda^3$. Si además $b = \pm 1$, entonces $a^3 \equiv b \mod \lambda^4$.

Demostración. (1) Utilizaremos varias veces la igualdad $3 = -\zeta_3^2\lambda^2$ que implica que λ^2 es asociado de 3. También implica que $9 = N(\lambda^2)$ y por tanto $N(\lambda) = 3$ lo que, por la Proposición 2.17, implica que λ es irreducible (y primo) en $\mathbb{Z}[\zeta_3]$.

(2) Pongamos $x = a + b\zeta_3$ con $a, b \in \mathbb{Z}$. Como $\lambda = 1 - \zeta_3$, tenemos que $\zeta_3 \equiv 1 \mod \lambda$ y, por tanto, $x \equiv a + b \mod \lambda$. Esto demuestra que x es congruente módulo λ con un número entero $y = a + b$. Como $\lambda \mid 3$ en $\mathbb{Z}[\zeta_3]$, cada entero es congruente módulo λ con $0, 1$ ó 2 con lo que todo elemento de $\mathbb{Z}[\zeta_3]$ es congruente con $0, 1$ ó 2 módulo λ. Como las diferencias entre dos de estos elementos no son múltiplos de $3 = N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\lambda)$, concluimos que $0, 1$ y 2 no son congruentes módulo λ.

(3) Supongamos que $a \equiv b \mod \lambda$, es decir, suponemos que λ divide a $a - b$. Entonces $a = b + c\lambda$, para un $c \in \mathbb{Z}[\zeta_3]$. Luego

$$a^3 = (b + c\lambda)^3 = b^3 + 3b^2c\lambda + 3bc^2\lambda^2 + c^3\lambda^3 \equiv b^3 \mod \lambda^3$$

pues λ^2 divide a 3.

Supongamos ahora que $b = \pm 1$. Si $c \equiv 0 \mod \lambda$, entonces λ^4 divide a $3c\lambda$, $3c^2\lambda^2$ y $c^3\lambda^3$ y por tanto

$$a^3 = b^3 + c\lambda + 3bc^2\lambda^2 + c^3\lambda^3 \equiv b^3 = b \mod \lambda^4$$

como se desea. En caso contrario $c \equiv \pm 1 \mod \lambda$ y, por tanto, $c^3 \equiv c \mod \lambda$, lo que implica

$$-\zeta_3^2 c + c^3 \equiv c(1 - \zeta_3^2) \equiv 0 \mod \lambda.$$

Es decir, λ divide a $-\zeta_3^2 c + c^3$ y, deducimos que, λ^4 divide a

$$\lambda^3(-\zeta_3^2 c - bc^2\zeta_3^2\lambda + c^3) = 3c\lambda + 3bc^2\lambda^2 + bc^3\lambda^3 = a^3 - b^3 = a^3 - b,$$

es decir, $a^3 \equiv b \mod \lambda^4$. ∎

Observación 3.15 *Si n es un entero impar entonces $x^n + y^n = \prod_{i=0}^{n-1}(x + \zeta_n^i y)$ pues de $X^n - 1 = \prod_{i=0}^{n-1}(X - \zeta_n^i)$ deducimos que*

$$x^n+y^n = (-y)^n\left(\left(-\frac{x}{y}\right)^n - 1\right) = (-y)^n\prod_{i=0}^{n-1}\left(-\frac{x}{y} - \zeta_n^i\right) = \prod_{i=0}^{n-1}(-y)\left(-\frac{x}{y} - \zeta_n^i\right) = \prod_{i=0}^{n-1}(x+\zeta_n^i y).$$

Teorema 3.16 *(**Gauss**) Si $a, b, c \in \mathbb{Z}[\zeta_3]$ satisfacen $a^3 + b^3 + c^3 = 0$, entonces $abc = 0$.*

Demostración. Razonaremos por reducción al absurdo. Pongamos pues que $a, b, c \in \mathbb{Z}[\zeta_3]$ satisfacen $a^3 + b^3 + c^3 = 0$ y $abc \neq 0$. Usaremos que $\mathbb{Z}[\zeta_3]$ es un DFU (Teorema 3.6) y las nociones de divisibilidad (divide a, es múltiplo de, es primo, es un máximo común divisor, etc) son relativas a $\mathbb{Z}[\zeta_3]$, con lo que nos ahorraremos repetir "en $\mathbb{Z}[\zeta_3]$".

Dividiendo a, b y c por su máximo común divisor podemos suponer que a, b y c son coprimos dos a dos. En particular, λ como mucho divide a uno de los tres a, b y c. Por simetría, podemos suponer que $\lambda \nmid a$ y $\lambda \nmid b$.

Vamos a distinguir dos casos.

Caso I: λ no divide a c.

Entonces a, b y c son congruentes con ± 1 módulo λ y, del Lema 3.14 tenemos que a^3, b^3 y c^3 son congruentes con ± 1 módulo λ^3. Por tanto

$$0 = a^3 + b^3 + c^3 \equiv \pm 1 \pm 1 \pm 1 \mod \lambda^3$$

y la combinación de todas las posibilidades de signos muestra que

$$0 \equiv \pm 1 \mod \lambda^3 \quad \text{ó} \quad 0 \equiv \pm 3 \mod \lambda^3.$$

La primera opción es imposible pues λ no es una unidad y la segunda implicaría que λ^3 divide a $3 = -\zeta_3^2\lambda^2$ y, por tanto, λ divide a $-\zeta_3^2$, lo que proporciona una contradicción pues λ es irreducible y ζ_3 una unidad.

Caso II: λ divide a c en $\mathbb{Z}[\zeta_3]$.

Sea X el conjunto formado por todas las 5-uplas (k, u, x, y, z) que satisfacen las siguientes propiedades:

(1) k es un entero positivo.

(2) $u \in \mathcal{U}(\mathbb{Z}[\zeta_3])$,

(3) x, y y z son elementos coprimos dos a dos de $\mathbb{Z}[\zeta_3]$,

(4) $\lambda \nmid x$, $\lambda \nmid y$ y $\lambda \nmid z$.

(5) $x^3 + y^3 + u\lambda^{3k}z^3 = 0$.

Usando que $\mathbb{Z}[\zeta_3]$ es DFU tenemos que $c = \lambda^n c_1$ para un elemento c_1 de $\mathbb{Z}[\zeta_3]$ que no es múltiplo de λ y además $n \geq 1$, pues λ divide a c, por hipótesis. Por tanto $a^3 + b^3 + \lambda^{3n}c_1^3 = 0$ y esto muestra que $(n, 1, a, b, c)$ pertenece a X. En particular, X no es el conjunto vacío.

El resto de la demostración es un argumento por el Método del Descenso Infinito en el que se prueba que para cada elemento (k, u, x, y, z) de X existe otro elemento $(k_1, u_1, x_1, y_1, z_1)$ de X con $k_1 < k$.

Sea (k, u, x, y, z) un elemento de X. Del Lema 3.14 tenemos que

$$-u\lambda^{3k}z^3 = x^3 + y^3 \equiv \pm 1 \pm 1 \mod \lambda^4.$$

Como λ no divide a 2, se tiene que $-u\lambda^{3k}z^3 \not\equiv \pm 2 \mod \lambda^4$ y, por tanto, $-u\lambda^{3k}z^3 \equiv 0 \mod \lambda^4$. Es decir λ^4 divide a $-u\lambda^{3k}z^3$ o, lo que es lo mismo, λ divide a $-u\lambda^{3(k-1)}z^3$. Como λ es primo y no divide a u, porque es unidad, ni a z, por hipótesis, necesariamente λ divide a $\lambda^{3(k-1)}$ y, concluimos que $k \geq 2$.

Por otro lado, utilizando la igualdad $1 + \zeta_3 + \zeta_3^2 = 0$ se obtiene que

$$-u\lambda^{3k}z^3 = x^3 + y^3 = (x + y)(x + \zeta_3 y)(x + \zeta_3^2 y),$$

de donde deducimos que λ divide a uno de los tres factores de la derecha. Pero eso implica que los divide a los tres ya que $x + y \equiv x + \zeta_3 y \equiv x + \zeta_3^2 y \mod \lambda$, pues $\lambda = 1 - \zeta_3$. Pongamos por tanto

$$-u\lambda^{3(k-1)}z^3 = \frac{x + y}{\lambda} \cdot \frac{x + \zeta_3 y}{\lambda} \cdot \frac{x + \zeta_3^2 y}{\lambda}.$$

Como $k \geq 2$, λ también divide a alguno de los tres factores de la derecha. Sin embargo, sólo puede dividir a uno de ellos, ya que si λ dividiera a dos de ellos, entonces λ dividiría a la diferencia de estos dos lo cual no es cierto pues, salvo el signo, estas diferencias son

$$\begin{array}{rcl} \frac{(x+y)-(x+y\zeta_3)}{\lambda} & = & y, \\ \frac{(x+\zeta_3 y)-(x+\zeta_3^2 y)}{\lambda} & = & \zeta_3 y, \\ \frac{(x+y)-(x+\zeta_3^2 y)}{\lambda} & = & (1+\zeta_3)y = (\lambda + 2\zeta_3)y. \end{array}$$

ninguna de las cuales es múltiplo de λ por ser ζ_3 unidad e y no ser múltiplo de λ.

Ahora vamos a ver que podemos suponer que λ^2 divide a $x + y$. En efecto, si ponemos $y_1 = y$, $y_2 = \zeta_3 y$ e $y_3 = \zeta_3^2 y$, entonces utilizando que $\zeta_3^3 = 1$ se ve fácilmente que (k, u, x, y_1, z), (k, u, x, y_2, z) y (k, u, x, y_3, z) pertenecen a X y hemos visto que λ divide a $x + y = x + y_1$, $x + \lambda y = x + y_2$ ó $x + \zeta_3^2 y = x + y_3$, con que podemos elegir y igual a y_1, y_2 ó y_3 para que se verifique que λ divida a $x + y$.

En resumen

$$\begin{array}{rcl} x + y & = & \lambda^{3k-2}\alpha_1 \\ x + \zeta_3 y & = & \lambda\alpha_2 \\ x + \zeta_3^2 y & = & \lambda\alpha_3 \end{array}$$

con α_1, α_2 y α_3 elementos de $\mathbb{Z}[\zeta_3]$ que no son múltiplos de λ. Además α_1, α_2 y α_3 son coprimos dos a dos. En efecto, supongamos que p es un divisor común de α_1 y α_2. Entonces p no divide a λ, pues en caso contrario p y λ son asociados, por que ambos son primos, lo que implicaría que λ divide a α_1, lo que no es cierto. Además p divide a $\lambda^{3k-2}\alpha_1 - \lambda\alpha_2 = (x + y) - (x + \zeta_3 y) = (1 - \zeta_3)y = -\lambda y$. Como p no divide a λ y es primo, deducimos que p divide a y. Por tanto p divide a $\lambda^{3k-2}\alpha_1 - y = x$, lo que contradice el hecho de que x e y son

coprimos. Esto demuestra que α_1 y α_2 son coprimos. Las demostraciones de que las otras dos parejas de α_i son coprimas son similares.

Entonces

$$-uz^3 = \frac{x+y}{\lambda^{3k-2}} \cdot \frac{x+\zeta_3 y}{\lambda} \cdot \frac{x+\zeta_3^2 y}{\lambda} = \alpha_1\alpha_2\alpha_3.$$

Utilizando que $-u$ es una unidad, que α_1, α_2 y α_3 son coprimos dos a dos, y la última igualdad (junto con que $\mathbb{Z}[\zeta_3]$ es un DFU, se deduce que α_1, α_2 y α_3 son asociados de cubos de $\mathbb{Z}[\zeta_3]$, es decir, existen elementos β_1, β_2 y β_3 de $\mathbb{Z}[\zeta_3]$ y unidades u_1, u_2 y u_3 de $\mathbb{Z}[\zeta_3]$ tales que $\alpha_i = u_i\beta_i^3$, para $i = 1, 2$ y 3. Por tanto, $\beta_1, \beta_2, \beta_3$ son coprimos dos a dos y coprimos con λ y además

$$x + y = \lambda^{3k-2}u_1\beta_1^3, \quad x + \zeta_3 y = \lambda u_2\beta_2^3 \quad \text{y} \quad x + \zeta_3^2 y = \lambda u_3\beta_3^3.$$

Pero entonces

$$0 = (x+y) + \zeta_3(x+\zeta_3 y) + \zeta_3^2(x+\zeta_3^2 y) = \lambda^{3k-2}u_1\beta_1^3 + \zeta_3\lambda u_2\beta_2^3 + \zeta_3^2\lambda u_3\beta_3^3.$$

Dividiendo por $\zeta_3\lambda u_2$ y poniendo $v_1 = \zeta_3 u_3 u_2^{-1}$ y $v_2 = \zeta_3^2 u_1 u_2^{-1}$, tenemos que

$$\beta_2^3 + v_1\beta_3^3 + \lambda^{3(k-1)}v_2\beta_1^3 = 0$$

donde v_1 y v_2 son unidades de $\mathbb{Z}[\zeta_3]$. Como λ no divide a ningún β_i, del Lema 3.14 tenemos que $\beta_i^3 \equiv \pm 1 \mod \lambda^3$. Como además $k \geq 2$,

$$0 \equiv -\lambda^{3(k-1)}v_2\beta_1^3 = \beta_2^3 + v_1\beta_3^3 \equiv \pm 1 \pm v_1 \mod \lambda^3.$$

Es decir, v_1 es una unidad de $\mathbb{Z}[\zeta_3]$ que es congruente con ± 1 módulo λ^3. Pero ninguna de las cuatro unidades $\pm\zeta_3$ y $\pm\zeta_3^2$, es congruente con ± 1 módulo λ^3 pues como λ es irreducible y λ^2 es asociado de 3 tenemos que $\lambda \nmid 2$ y por tanto

$$\begin{aligned}
\lambda^3 &\nmid \lambda = 1 - \zeta_3 = -(-1 + \zeta_3),\\
\lambda &\nmid \lambda + 2\zeta_3 = 1 + \zeta_3 = -(-1 - \zeta_3),\\
\lambda^3 &\nmid \lambda(1+\zeta_3) = \lambda + \zeta_3 - \zeta_3^2 = 1 - \zeta_3^2 = -(-1 + \zeta_3^2),\\
\lambda &\nmid \lambda + \zeta_3(1+\zeta_3) = 1 + \zeta_3^2 = -(-1 - \zeta_3^2).
\end{aligned}$$

Luego $v_1 = \pm 1$ y por tanto

$$\beta_2^3 + (\pm\beta_3)^3 + \lambda^{3(k-1)}v_2\beta_1^3 = 0,$$

con β_1, β_2 y β_3 coprimos y no múltiplos de λ. Repasando las cinco propiedades que definen el conjunto X, concluimos que

$$(k-1, v_2, \beta_2, \pm\beta_3, \beta_1) \in X,$$

lo que completa el argumento por el Método del Descenso. ∎

El siguiente caso del Último Teorema de Fermat que es consecuencia inmediata del Teorema 3.16 podría haberlo demostrado Fermat, aunque no hay pruebas de ello. Quien sí lo demostró antes de Gauss fue Euler, aunque todos sus argumentos eran dentro de los números enteros.

Corolario 3.17 *Si a, b y c son enteros no nulos entonces $a^3 + b^3 \neq c^3$.*

3.4 Ecuaciones diofánticas

En esta sección vamos a ver un resultado de Fermat que utiliza la factorización única en $\mathbb{Z}[i]$ para resolver la ecuación diofántica $y^2 + 4 = z^3$ y otro de Ramanujan-Nagen que usa la factorización única en $\mathbb{Z}[\sqrt{-7}]$ para resolver la ecuación diofántica $x^2 + 7 = 2^n$.

Teorema 3.18 (Fermat) *Las únicas soluciones de la ecuación diofántica*

$$y^2 + 4 = z^3$$

son $y = \pm 11, z = 5$ *y* $y = \pm 2, z = 2$.

Demostración. Vamos a trabajar en el anillo de enteros de Gauss $\mathbb{Z}[i]$, que como se vió en el Teorema 3.6 es un dominio euclídeo y, por tanto, es un DFU. Podemos reescribir la ecuación como

$$(2 + iy)(2 - iy) = z^3.$$

Un factor común $q = a + bi$ de $2 + iy$ y $2 - iy$ es un factor común de 4 y de $2y$. Tomando normas tenemos que $a^2 + b^2$ divide a 16 y $4y^2$.

Supongamos que y es impar. Entonces $a^2 + b^2 \mid 4$ y, por tanto $q = \pm 1, \pm i, \pm 2, \pm 2i, \pm 1 + \pm i$, como hay que eliminar los dos primeros casos, porque son unidades y los dos siguientes casos porque y es impar, resulta que solo queda el último caso, que también se elimina porque tampoco resulta ser un divisor de $2 + iy$, ya que si

$$2 + iy = (1 + i)(\alpha + \beta i) = (\alpha - \beta) + (\alpha + \beta)i$$

entonces $y - 2 = 2\beta$, en contra de que y es impar. Los otros casos se resuelven similarmente. Por tanto, $2+iy$ y $2-iy$ son coprimos. Por factorización única se obtiene que como el producto es un cubo, entonces uno de ellos es de la forma $u\alpha^3$ y el otro de la forma $u^{-1}\beta^3$, para cierta unidad u. Como las únicas unidades de $\mathbb{Z}[i]$ son ± 1 y $\pm i$ que son todas cubos, podemos suponer que $u = 1$, o sea $2 + iy$ y $2 - iy$ son cubos. Si $2 + iy = (a + bi)^3$, tomando conjugados tenemos que $2 + iy = (a - bi)^3$. Sumando estas dos ecuaciones tenemos que

$$4 = 2a^3 - 6ab^2 = 2a(a^2 - 3b^2)$$

y, por tanto,

$$2 = a(a^2 - 3b^2)$$

Luego a es un divisor de 2, o sea $a = \pm 1$ o $a = \pm 2$. Como a determina b se ve fácilmente que las soluciones son

$$\begin{aligned} a = -1, &\quad b = \pm 1; \\ a = 2, &\quad b = \pm 2. \end{aligned}$$

$z^3 = (a + bi)^3(a - bi)^3 = (a^2 + b^2)^3$, Luego $z = a^2 + b^2 = 2, 5$ y, por tanto, $y^2 + 4 = 8, 125$, luego $y = \pm 2, \pm 11$. Como estamos suponiendo que y es impar, $y = \pm 11$ y $z = 5$.

Supongamos ahora que y es par. Esto implica que z tambien es par. Pongamos $y = 2Y$ y $z = 2Z$, con lo que tenemos que resolver la ecuación

$$Y^2 + 1 = 2Z^3.$$

Eso implica que Y es impar, pongamos $Y = 2k+1$. El máximo común divisor de $Y+i$ y $Y-i$ tiene que dividir a la diferencia que es $2i = (1+i)^2$. Como $N(1+i) = 2$, $1+i$ es irreducible de $\mathbb{Z}[i]$. Como $Y+i = 2k+1+i = (1+i)((1-i)k+1)$ e $Y-i = 2k+1-i = (1+i)((1-i)k-i)$, pero $(1+i)^2 = 2i$ no divide a $Y+i$, el máximo común divisor de $Y+i$ e $Y-i$ es $1+i$. Descomponiendo la ecuación $Y^2+1 = 2Z^3$ como

$$(1+iY)(1-iY) = 2Z^3$$

y observando que $1+iY$ es asociado de $Y-i$ y $1-iY$ es asociado de $Y+i$, resulta que $1+i$ aparece al menos dos veces en la factorización de la parte derecha. Como la factorización de 2 es $-i(1+i)^2$, todos los factores irreducibles de $1+iY$ y $1-iY$ que no sean asociados de $1+i$ tienen un exponente múltiplo de 3, o sea

$$1+Yi = (1+i)(a+bi)^3$$

Observando la parte real tenemos

$$1 = a^3 - 3a^2b - 3ab^2 + b^3 = (a+b)(a^2 - 4ab + b^2)$$

Luego

$$a+b = a^2 - 4ab + b^2 = \pm 1$$

Resolviendo estas ecuaciones obtenemos solo dos soluciones $a = 1, b = 0$ y $a = 0, b = 1$. Eso implica que $Y = \pm 1$ y, por tanto $y = \pm 2$, en cuyo caso $z = 2$. ∎

Lema 3.19 *Sean n, m y p enteros con p primo y $m \geq 0$. Si $n \equiv 1 \mod p$ entonces $n^{p^m} \equiv 1 \mod p^{m+1}$.*

Demostración. Razonamos por inducción sobre m. El caso $m = 0$ es precisamente la hipótesis. Supongamos que $n^{p^m} \equiv 1 \mod p^{m+1}$ y pongamos $n^{p^m} = 1 + hp^{m+1}$. Como $m \geq 0$ $i(m+1) \geq m+2$ para todo $i \geq 2$. Luego

$$n^{p^{m+1}} = 1 + hp^{m+2} + \sum_{i=2}^{p^{m+1}} \binom{p^{m+1}}{i} h^i p^{i(m+1)} \equiv 1 \mod p^{m+2}.$$

∎

Lema 3.20 *Sean a un elemento de un anillo A y sea p un primo mayor que 4 tal que $p \in Aa^2$. Sean m un entero positivo y n un entero no negativo tal que $p^n \mid m$. Entonces $(1+a)^m \equiv 1+ma \mod Ap^{n+1}$.*

Demostración. Razonamos por inducción sobre n. Si $n = 0$ entonces $(1+a)^m = 1 + ma + \sum_{i=2}^{m} \binom{m}{i} a^i \equiv 1 + ma \mod p$ pues $p \in Aa^i$ para todo $i \geq 2$. Si $n = 1$ entonces $m \geq p > 4$ y

$$(1+a)^m = 1 + ma + \binom{m}{2} a^2 + \binom{m}{3} a^3 + \sum_{i=4}^{m} \binom{m}{i} a^i \equiv 1 + ma \mod p^2$$

pues p divide a $\binom{m}{2}$, a $\binom{m}{3}$ y a a^2.

Supongamos que $n \geq 2$ y que el lema se verifica para n menor. Como $p^{n-1} \mid \frac{m}{p}$, de la hipótesis de inducción tenemos que $(1+a)^{\frac{m}{p}} = 1 + \frac{m}{p}a + p^n b$ para algún $b \in A$ y, por tanto,

$$\begin{aligned}(1+a)^m &= \left(1 + \frac{m}{p}a + p^n b\right)^p = 1 + ma + p^{n+1}b + \sum_{i=2}^{p} \binom{p}{i} \left(\frac{m}{p}a + p^{n+1}b\right)^i \\ &= 1 + ma + p^{n+1}b + \sum_{i=2}^{p} \binom{p}{i} \sum_{j=0}^{i} \binom{i}{j} \left(\frac{m}{p}a\right)^j (p^{n+1}b)^{i-j} \equiv 1 + ma \mod p^{n+1}\end{aligned}$$

pues en caso contrario p^{n+1} no divide a $\binom{p}{i}\left(\frac{m}{p}a\right)^j (p^{n+1}b)^{i-j}$ para algún $2 \leq i \leq p$ y algún $0 \leq j \leq i$. Entonces $i = j$ y p^{n+1} no divide a $\left(\frac{m}{p}a\right)^i$. Pero como $p^n \mid m$, $i \geq 2$ y $p \mid a^2$, eso implica que $(n-1)i + 1 < n + 1$. Luego $1 \leq (n-1)(i-1) < 1$, pues $n, i \geq 2$. Esto proporciona una contradicción. ∎

Teorema 3.21 (Ramanujan-Nagen) *Las únicas soluciones de la ecuación diofántica*

$$x^2 + 7 = 2^n$$

son

x	$=$	± 1	± 3	± 5	± 11	± 181
n	$=$	3	4	5	7	15.

Demostración. Vamos a trabajar en el anillo $D = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] = \mathbb{A}_{\mathbb{Q}(\sqrt{-7})}$ que por el Teorema 3.6 es un dominio euclídeo.

Empezaremos suponiendo que n es par y sea $n = 2N$, en cuyo caso podemos reescribir la ecuación como

$$(2^N + x)(2^N - x) = 7$$

Entonces, salvo un cambio de signo en x tenemos

$$\begin{aligned}2^N + x &= 7 \\ 2^N - x &= 1\end{aligned}$$

y, por tanto $N = 2$ y $x = 3$, con lo que $n = 4$.

En el resto de la demostración n es impar y necesariamente mayor o igual que 3. Si $n = 3$ entonces $x = \pm 1$. Supongamos que $n > 3$ y sea $m = n - 2$, que es también impar y mayor o igual que 3. Tenemos que demostrar que los enteros positivos impares m para los que la siguiente ecuación tiene solución son $3, 5$ y 13:

$$\frac{x^2 + 7}{4} = 2^m. \tag{3.1}$$

Sea

$$a = \frac{1 + \sqrt{-7}}{2}.$$

La descomposición de 2 en factores irreducibles en D es

$$2 = a\overline{a} = N_{\mathbb{Q}(\sqrt{-7})/\mathbb{Q}}(a)$$

(3.1) puede reescribirse como

$$\left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right) = a^m b^m$$

La parte de la derecha es una factorización en irreducibles. Un factor común de los dos factores de la izquierda será un divisor de la diferencia $\sqrt{-7}$, luego, ni a ni b son factores comunes de los factores de la izquierda. Eso implica que uno de los factores de la izquierda es asociado de a^m y el otro de b^m. Como las únicas unidades de $\mathbb{Z}[\sqrt{-7}]$ son ± 1 tenemos

$$\frac{x+\sqrt{-7}}{2} = \pm b^m \quad \text{y} \quad \frac{x-\sqrt{-7}}{2} = \pm \overline{b}^m \quad (b = a \text{ ó } \overline{a})$$

Luego

$$a - \overline{a} = \frac{x+\sqrt{-7}}{2} - \frac{x-\sqrt{-7}}{2} = \pm(a^m - \overline{a}^m).$$

Vamos a ver que en la parte derecha de esta igualdad el signo es el negativo. En caso contrario, como $a\overline{a} = 2$, se tiene que $(1-\overline{a})^2 = 1 - 2a\overline{a} + \overline{a}^2 = 1 - a^2\overline{a}^2 + \overline{a}^2$ y $a^2 - 1 = \frac{-5+\sqrt{-7}}{2} = \overline{a}^3$. Luego

$$a^2 \equiv (1-\overline{a})^2 \equiv 1 \mod \overline{a}^2$$

y, por tanto,

$$a^m \equiv a(a^2)^{\frac{m-1}{2}} \equiv a \mod \overline{a}^2$$

De lo que deducimos que $a \equiv a^m - \overline{a}^m = a - \overline{a} \mod \overline{a}^2$ y, por tanto, $\overline{a}^2 \mid a$ en D, en contradicción con que a y $\overline{a}$ son irreducibles en D. Luego

$$-\sqrt{-7} = \overline{a} - a = a^m - \overline{a}^m.$$

Desarrollando las potencias en la diferencia anterior tenemos que

$$-2^{m-1} = \binom{m}{1}1 + \binom{m}{3}7 + \binom{m}{5}7^2 \ldots + \binom{m}{m}7^{m-1}$$

luego

$$-2^{m-1} \equiv m \mod 7.$$

Supongamos que $m \equiv r \mod 42$ con $1 \leq r \leq 41$. Luego $m - 1 \equiv r - 1 \mod 6$ y $m \equiv r \mod 7$. Como $2^3 \equiv 1 \mod 7$.

$$-2^{r-1} \equiv r \mod 7$$

Las únicas soluciones $0 \leq r < 42$ de esta ecuación de congruencias son $r = 3, 5, 13$, luego

$$m \equiv 3, 5, 13 \mod 42.$$

Solo falta demostrar que $m = r$. Para ver esto observemos que todo lo que hemos dicho para m es válido para r pues la ecuación 3.1 tiene solución para $m = 3, 5$ y 13. En particular $-\sqrt{-7} = a^m - \overline{a}^m = a^r - \overline{a}^r$. Supongamos que $m > r$ y sea 7^l la mayor potencia de 7 que divide a $m - r$. Entonces

$$2^{m-r}a^m = a^r(2a)^{m-r} = a^r(1 + \sqrt{-7})^{m-r}. \tag{3.2}$$

Ahora usamos el hecho de que $m - r$ es múltiplo de $3 \cdot 7^l$ y $2^3 \equiv 1 \mod 7$ aplicando primero el Lema 3.19 a $n = 2^3$ deducir que $2^{3\cdot 7^l} \equiv 1 \mod 7^{l+1}$ y por tanto

$$2^{m-r} \equiv 1 \mod 7^{l+1}.$$

Entonces aplicando el Lema 3.20 con $a = \sqrt{-7}$ y $p = 7$ y $n = l$ tenemos que

$$(1 + \sqrt{-7})^{m-r} \equiv 1 + (m - r)\sqrt{-7} \mod 7^{l+1}.$$

Juntando estas dos congruencias con (3.2) tenemos

$$a^m \equiv a^r(1 + (m - r)\sqrt{-7}) = a^r + a^r(m - r)\sqrt{-7} \mod 7^{l+1}.$$

Pero $2^r a^r \equiv (1 + r\sqrt{-7}) \mod 7$ con lo que como además 7^l divide a $m - r$ tenemos que 7^{l+1} divide a $2^r a^r - (1 + r\sqrt{-7})(m - r)\sqrt{-7}$. Por tanto $2^r a^r(m - r)\sqrt{-7} \equiv 2^r(1 + r\sqrt{-7})(m - r)\sqrt{-7} \equiv 2^r(m-r)\sqrt{-7} \mod 7^{l+1}$. Como 2 es coprimo con 7 esto implica que $a^r(m-r)\sqrt{-7} \equiv (m - r)\sqrt{-7} \mod 7^{l+1}$. Por tanto

$$a^m \equiv a^r + (m - r)\sqrt{-7} \mod 7^{l+1}.$$

Similarmente se obtiene

$$\overline{a}^m \equiv \overline{a}^r - (m - r)\sqrt{-7} \mod 7^{l+1}.$$

Entonces, teniendo en cuenta que $a^r - \overline{a}^r = a^m - \overline{a}^m$ tenemos que

$$2(m - r)\sqrt{-7} \equiv 0 \mod 7^{l+1}.$$

Usando de nuevo que 2 y 7 con coprimos deducimos que 7^{l+1} divide a $(m - r)\sqrt{-7}$. Tomando normas deducimos que $7^{2(l+1)}$ divide a $7(m-r)^2$. Luego 7^{2l+1} divide a $(m-r)^2$ lo que implica que 7^{l+1} divide a $m - r$, en contra de la elección de l. ∎

Capítulo 4

Dominios de Dedekind

En las secciones anteriores hemos visto que los anillos de enteros son dominios de factorización pero no necesariamente de factorización única. Lo que vamos a ver ahora es cómo podemos recuperar un tipo de unicidad sustituyendo la factorización de elementos por una teoría de factorización de ideales. Esto fue idea de Kummer y Dedekind. Vamos a desarrollar esta idea un poco más con un ejemplo.

Observemos la factorización siguiente en el anillo de enteros $D = \mathbb{Z}[\sqrt{15}]$ de $K = \mathbb{Q}(\sqrt{15})$:

$$2 \cdot 5 = (5 + \sqrt{15})(5 - \sqrt{15}).$$

$\sqrt{5}$ y $\sqrt{3}$ no son elementos de $\sqrt{15}$, pero si nos olvidamos de este hecho podemos escribir

$$\begin{aligned} 2 &= (\sqrt{5} + \sqrt{3})(\sqrt{5} - \sqrt{3}) \\ 5 &= \sqrt{5}\sqrt{5} \\ 5 + \sqrt{15} &= \sqrt{5}(\sqrt{5} + \sqrt{3}) \\ 5 - \sqrt{15} &= \sqrt{5}(\sqrt{5} - \sqrt{3}) \end{aligned}$$

O sea, si extendemos el anillo original al anillo de enteros de $\mathbb{Q}(\sqrt{5}, \sqrt{3})$ la factorización original se convierte en la siguiente factorización

$$\sqrt{5}\sqrt{5}(\sqrt{5} + \sqrt{3})(\sqrt{5} - \sqrt{3})$$

Esta fue esencialmente la idea de Kummer, es decir, considerar un cuerpo de números L que contenga en K. Entonces los anillos de enteros D_K, de K, y D_L de L no tienen porque ser DFU, pero en algunos casos los elementos de D_K pueden tener factorización única en L.

Otra aproximación fue la de Dedekind a partir del concepto de ideal. Una factorización de un elemento

$$x = ab$$

corresponde a una factorización de ideales principales

$$(x) = (a)(b)$$

de forma que una factorización en producto de irreducibles

$$x = p_1 p_2 \dots p_n$$

corresponde a una factorización de ideales

$$(x) = (p_1)(p_2)\dots(p_n).$$

Además en el caso en que el dominio es de factorización única los ideales (p_i) son primos.

Una de las ventajas de considerar factorización en ideales es que elementos asociados corresponden a los mismos ideales, luego la unicidad de la factorización solo se refiere a "unicidad salvo orden". Pero hay una ventaja mayor. Veamos esto con el ejemplo anterior de la siguiente factorización:

$$10 = 2 \cdot 5 = (5+\sqrt{15})(5-\sqrt{15}) = \sqrt{5}\sqrt{5}(\sqrt{5}+\sqrt{3})(\sqrt{5}-\sqrt{3}).$$

Sean $K = \mathbb{Q}(\sqrt{15})$, $L = \mathbb{Q}(\sqrt{5},\sqrt{3})$ y $\mathbb{A}_K$ y $\mathbb{A}_L$ sus anillos de enteros. La última factorización anterior corresponde a la siguiente factorización en producto de ideales primos de $\mathbb{A}_L$.

$$10\mathbb{A}_L = (\sqrt{5}\mathbb{A}_L)(\sqrt{5}\mathbb{A}_L)((\sqrt{5}+\sqrt{3})\mathbb{A}_L)((\sqrt{5}-\sqrt{3})\mathbb{A}_L).$$

Si ahora intersectamos con $\mathbb{A}_K$ tenemos

$$\begin{aligned} 10\mathbb{A}_K &= (10\mathbb{A}_L)\cap\mathbb{A}_K \\ &= ((\sqrt{5}\mathbb{A}_L)\cap\mathbb{A}_K)((\sqrt{5}\mathbb{A}_L)\cap\mathbb{A}_K)(((\sqrt{5}+\sqrt{3})\mathbb{A}_L)\cap\mathbb{A}_K)(((\sqrt{5}-\sqrt{3})\mathbb{A}_L)\cap\mathbb{A}_K). \end{aligned}$$

Sin embargo los nuevos factores pueden no ser ideales principales. Por ejemplo, vamos a ver que

$$I = ((\sqrt{5}+\sqrt{3})\mathbb{A}_L)\cap\mathbb{A}_K$$

no es un ideal principal de $\mathbb{A}_K$. Sea $N = N_{K/\mathbb{Q}}$ y supongamos que $I = \mathbb{A}_K k$ con $k = a+b\sqrt{15}$. Entonces $\sqrt{3}(\sqrt{5}+\sqrt{3}) = \sqrt{15}+3 \in I$ y $\sqrt{5}(\sqrt{5}+\sqrt{3}) = 5+\sqrt{15} \in I$ luego sus normas -6 y 10 son múltiplos de $N(k)$. Eso implica que $N(k) \mid 2$. Como $N(k) \neq \pm 1$, se tiene que $N(k) = a^2 - 15b^2 = \pm 2$. Tomando módulo 5 tenemos que $a^2 \equiv \pm 2 \mod 5$ lo cual es imposible. La idea es que la factorización de (x) en producto de ideales puede ser única pero los factores pueden ser ideales no principales.

4.1 Factorización de ideales

Definición 4.1 *Un* dominio de Dedekind *es un dominio noetheriano integramente cerrado tal que todos sus ideales primos no nulos son maximales.*

Como todo anillo de enteros es íntegramente cerrado, del Teorema 3.3 y el Lema 4.12 deducimos que el anillo de enteros de un cuerpo de números es un dominio de Dedekind. La propiedad que nos interesa de los dominios de Dedekind es la existencia de factorización única de ideales.

Vamos a analizar el producto de ideales en un dominio D con cuerpo de fracciones K. Por supuesto, este producto es conmutativo, asociativo y tiene un elemento neutro: el anillo total. Es decir el conjunto de los ideales no nulos de D es un monoide conmutativo en el que D es el único elemento invertible. Vamos a ver como podemos añadir inversos a este monoide inspirados por la idea de que los ideales de D son los D-submódulos de D.

Definición 4.2 *Un* ideal fraccional *de un dominio D es un D-submódulo no nulo F de su cuerpo de fracciones K tal que $cF \subseteq D$ para algún $c \in D \setminus \{0\}$.*

Obsérvese que si F es un ideal fraccional de K y $cF \subseteq D$, con $c \in D \setminus \{0\}$, entonces $I = cF$ es un ideal no nulo de D y $F = c^{-1}I$. Recíprocamente, si I es un ideal no nulo de D y $c \in D \setminus \{0\}$, entonces $c^{-1}I$ es un ideal fraccional de D. Luego los ideales fraccionales son los subconjuntos de K de la forma $c^{-1}I$, con $c \in D \setminus \{0\}$ e I un ideal no nulo de D.

Claramente un ideal es un ideal fraccional de D y un ideal fraccional de D es un ideal de D precisamente si está contenido en D.

El producto de ideales fraccionales es un ideal fraccional pues $c^{-1}Id^{-1}J = (cd)^{-1}IJ$. Además esta multiplicación es conmutativa, asociativa y tiene un neutro. Pero además veremos que todo ideal fraccional tiene un inverso, con lo cual los ideales fraccionales de un dominio de Dedekind forman un grupo abeliano multiplicativo. La demostración de este hecho va unida a la demostración del teorema de factorización única de ideales en dominios de Dedekind.

Teorema 4.3 *Sea D un dominio de Dedekind.*

(1) Los ideales fraccionales de D forman un grupo abeliano. En particular, el producto de ideales fraccionales es cancelativo.

(2) Cada ideal no nulo se puede escribir de forma única (salvo el orden de los factores) como producto de ideales primos.

Prepararemos la demostración del Teorema 4.3 con una serie de lemas. En todos ellos D es un dominio de Dedekind.

Lema 4.4 *Para todo ideal no nulo I de D existen ideales primos $P_1, P_2, \ldots, P_r$, tales que $P_1P_2 \ldots P_r \subseteq I$.*

Demostración. Supongamos que la afirmación no es cierta y sea I un elemento maximal en el conjunto de los ideales de D que no la cumplan. La existencia de tal elemento maximal es consecuencia de que D es noetheriano. Como I no cumple la propiedad del lema, en particular I no es primo. Por tanto existen $a, b \in D \setminus I$ con $ab \in I$. Entonces $I + Da$ e $I + Db$ contienen propiamente a I. De la maximalidad de I se tiene que existen ideales primos $P_1, \ldots, P_k, P_{k+1}, \ldots, P_n$ tales que $P_1 \cdots P_k \subseteq I + Da$ y $P_{k+1} \cdots P_n \subseteq I + Db$. Luego $P_1 \cdots P_n \subseteq (I + Da)(I + Db) \subseteq I + Dab = I$, en contra de la hipótesis que hemos hecho sobre I. ∎

Para cada ideal I de D sea

$$I^{-1} = \{x \in K \mid xI \subseteq D\}$$

Claramente I^{-1} es un D-submódulo de K. Además, si $I \neq 0$, entonces $cI^{-1} \subseteq D$, para todo $0 \neq c \in I$, luego, I^{-1} es un ideal fraccional de D. Además, $D \subseteq I^{-1}$, luego $I = ID \subseteq II^{-1} \subseteq D$. Por tanto, II^{-1} es un ideal de D que contiene a I.

Obsérvese que la operación $^{-1}$ invierte el orden, es decir, $I \subseteq J$ implica $J^{-1} \subseteq I^{-1}$.

Lema 4.5 *Si I es un ideal propio de D, entonces I^{-1} contiene propiamente D.*

Demostración. Sea P un ideal maximal de D que contiene a I. Entonces $D \subseteq P^{-1} \subseteq I^{-1}$, con lo cual solo hay que demostrar que $D \neq P^{-1}$. Sea $a \in P \setminus \{0\}$ y sea r el menor entero positivo tal que existen ideales primos $P_1, \ldots, P_r$ con $P_1 \ldots P_r \subseteq (a)$. Esto es posible por el Lema 4.4. Como $P_1 \ldots P_r \subseteq (a) \subseteq P$, algún P_i está contenido en P. Podemos suponer que $P_1 \subseteq P$ pero como P_1 es maximal, $P_1 = P$. Como además $P_2 \ldots P_r \not\subseteq (a)$ existe $b \in P_2 \ldots P_r \setminus (a)$. Luego $bP \subseteq (a)$ y, por tanto $ba^{-1}P \subseteq D$. Luego $ba^{-1} \in P^{-1}$. Pero, como $b \notin (a)$, $ba^{-1} \notin D$. Luego $D \neq P^{-1}$. ∎

Lema 4.6 *Si I es un ideal no nulo de D y S es un subconjunto de K tal que $IS \subseteq I$, entonces $S \subseteq D$.*

Demostración. Sea $a_1, a_2, \ldots, a_n$ un conjunto de generadores de I. (Recuérdese que D es un dominio de Dedekind y por tanto es noetheriano, con lo que todo ideal de D es finitamente generado.)

Sea $x \in S$. Entonces existen $b_{ij} \in D$ tales que

$$\begin{array}{lcccc} a_1x & = & b_{11}a_1 & +\cdots+ & b_{1n}a_n \\ a_2x & = & b_{21}a_1 & +\cdots+ & b_{2n}a_n \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_nx & = & b_{n1}a_1 & +\cdots+ & b_{nn}a_n \end{array}$$

Como algún $a_i \neq 0$, el determinante de la matriz

$$xI - (b_{ij}) = \begin{pmatrix} x - b_{11} & -b_{12} & \ldots & -b_{1n} \\ -b_{21} & x - b_{22} & \ldots & -b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ -b_{n1} & -b_{n2} & \ldots & x - b_{nn} \end{pmatrix}$$

es 0. Desarrollando dicho determinante tenemos que x es la raíz de un polinomio mónico con coeficientes en D, o sea x es entero sobre D. Como D es integramente cerrado, por ser dominio de Dedekind, concluimos que $x \in D$. ∎

Lema 4.7 *Si I es un ideal no nulo de D, entonces $II^{-1} = D$.*

Demostración. Empezaremos suponiendo que I es un ideal maximal P de D. Como $D \subseteq P^{-1}$ y $P \subseteq D$ tenemos que $P \subseteq PP^{-1} \subseteq D$. Luego $P = PP^{-1}$ ó $PP^{-1} = D$. Pero, del Lema 4.5 tenemos que P^{-1} no está contenido en D y, por tanto, del Lemma 4.6 deducimos que la primera igualdad no se da. Luego $PP^{-1} = D$.

Demostramos ahora el caso general por reducción al absurdo. Sea I un ideal maximal entre los que cumplen la condición $II^{-1} \neq D$ y sea P un ideal maximal de D que contiene a I. Para la existencia de I estamos usando de nuevo que D es noetheriano pero no lo necesitamos para

lo segundo porque todo ideal propio de un anillo está contenido en un ideal maximal. Como $D \subset P^{-1} \subset I^{-1}$, multiplicando por I tenemos

$$I \subseteq IP^{-1} \subseteq II^{-1} \subseteq D.$$

Utilizando de nuevo los lemas 4.5 y 4.6 deducimos que $IP^{-1} \not\subseteq I$. Por tanto, I está contenido propiamente en IP^{-1}. De la maximalidad de I deducimos que

$$IP^{-1}(IP^{-1})^{-1} = D$$

luego

$$P^{-1}(IP^{-1})^{-1} \subseteq I^{-1}$$

y, por tanto,

$$D = IP^{-1}(IP^{-1})^{-1} \subseteq II^{-1} \subseteq D.$$

∎

Demostración del Teorema 4.3. (1) Sólo hay que probar que todo ideal fraccional tiene un inverso. Sea I un ideal fraccional. Entonces existe $c \in D \setminus \{0\}$ y J ideal de D, tal que $I = c^{-1}J$. Aplicando el Lema 4.7 deducimos que cJ^{-1} es inverso de I.

(2) Como D es el producto de una cantidad vacía de ideales primos, basta demostrar la afirmación para ideales propios de D y por reducción al absurdo podemos suponer que I es un ideal no nulo propio, maximal entre los que no son producto de ideales primos. Sea P un ideal maximal que contiene a I. Entonces

$$I \subseteq IP^{-1} \subseteq PP^{-1} = D.$$

(De hecho la última es igualdad por el Lema 4.7 pero no lo necesitamos.) La primera inclusión es estricta pues si se diera la igualdad tendríamos $D = I^{-1}I = I^{-1}IP^{-1} = DP^{-1} = P^{-1}$, lo que contradiría el Lema 4.5. Por la maximalidad de I, tenemos que $IP^{-1} = P_2 \dots P_r$ para ciertos ideales primos y, por tanto $I = PP_2 \dots P_r$.

Sólo falta demostrar que la factorización es única. Obsérvese que de (1) se deduce que el producto de ideales es cancelativo. Supongamos que

$$P_1 \dots P_r = Q_1 \dots Q_s$$

con los factores, ideales primos de D. Argumentamos por inducción sobre r. Para $r = 1$ el resultado es trivial pues, el hecho de que P_1 sea primo implica que $Q_i \subseteq P_1$, para algún i (podemos suponer $i = 1$). Pero como en realidad Q_1 y P_1 son maximales, $Q_1 = P_1$ y de la cancelatividad del producto de ideales se obtiene que $r = 1$. Si $r \geq 1$ tenemos que $Q_1 \dots Q_s \subseteq P_1 \dots P_r \subseteq P_1$ y argumentamos como antes para demostrar que $P_1 = Q_i$ para algún i (que supondremos igual a 1). Para acabar, volvemos a aplicar la cancelatividad y la hipótesis de inducción. ∎

4.2 Consecuencias de la factorización en dominios de Dedekind

A partir de haber demostrado la unicidad de la factorización de ideales en dominios de Dedekind, el papel que representaban los elementos del anillo lo asumen los ideales. Entonces las relaciones de divisibilidad que nos interesan son entre ideales, de forma que decimos que un ideal I *divide* a otro J en D si $IK = J$ para algún ideal K. En tal caso escribimos $I \mid J$. Claramente $I \mid 0$ para todo ideal I. Sin embargo, por la propiedad cancelativa del producto de ideales fraccionales si $I \neq 0$ y $I \mid J$ entonces el único ideal K que satisface $IK = J$ es $I^{-1}J$. Por tanto, en tal caso $I \mid J$ si y solo si $I^{-1}J \subseteq D$ si y sólo si $J \subseteq I$. O sea en el conjunto de ideales de un dominio de Dedekind "divide" es lo mismo que "contiene":

Corolario 4.8 *Si I y J son ideales de D entonces $I \mid J$ si y solo si $I \supseteq J$.*

Usaremos los adjetivos "divisor" y "múltiplo" indistintamente sobre ideales y elementos de D y los mezclaremos de forma que que un elemento sea múltiplo de un ideal significa que el ideal generado por el elemento $a \in D$ es múltiplo del ideal I o lo que es lo mismo si $a \in I$.

La existencia de factorización única de los ideales no nulos de D tiene muchas consecuencias. Una de ellas es que un ideal solo tiene un número finito de divisores o lo que es lo mismo está contenida solo en un número finito de ideales. Si aplicamos esto al caso en que el ideal es principal se obtiene que cada elemento no nulo solo está en un número finito de ideales. Otra consecuencia es que los conceptos de máximo común divisor y mínimo común múltiplo de ideales I y J pueden definirse bien como el mayor divisor (menor múltiplo) común o en función de la factorización única. Como consecuencia del Corolario 4.8 tenemos que el máximo común divisor de I y J es el menor ideal que contiene a I y a J y el mínimo común múltiplo es el mayor ideal contenido en I y J. Por tanto si las factorizaciones de I y J son

$$I = \prod_{i=1}^{r} P_i^{e_i} \quad \text{y} \quad J = \prod_{i=1}^{r} P_i^{f_i}$$

entonces

$$I + J = \prod_{i=1}^{r} P_i^{\min(e_i, f_i)} \quad \text{e} \quad I \cap J = \prod_{i=1}^{r} P_i^{\max(e_i, f_i)}.$$

Lema 4.9 *Si I es un ideal de D entonces existe un ideal no nulo J de D tal que IJ es principal.*

Demostración. El resultado es claro si $I = 0$. Supongamos que $I \neq 0$ y fijemos $a \in I \setminus \{0\}$. Sea $J = \{b \in D : bI \subseteq Da\}$. Entonces J es un ideal no nulo de D tal que $IJ \subseteq Da$. Para demostrar el lema basta ver que $IJ = Da$ y demostramos esto por reducción al absurdo. Supongamos que $IJ \neq Da$ y sea $A = \frac{IJ}{a}$. Entonces A es un ideal propio de D que contiene a J pues $a \in I$. Luego A^{-1} contiene propiamente a D, por el Lema 4.5. Sea $b \in A^{-1} \setminus D$. Entonces $bA \subseteq D$. Luego $bJI = bAa \subseteq Da$ y, por tanto, $bJ \subseteq J$. Esto contradice el Lema 4.6 pues $b \notin D$. ∎

Sabemos que todo ideal de D es finitamente generado como D-módulo. De hecho vamos a demostrar que cada ideal está generado por a lo sumo dos elementos. Primero necesitamos el siguiente lema.

Lema 4.10 *Si I y J son dos ideales no nulos de D, entonces existe $a \in I$ tal que*

$$aI^{-1} + J = D.$$

Demostración. Sean $P_1, \ldots, P_r$ los distintos ideales primos que dividen a J. Si $r = 0$ entonces $J = D$ y el resultado está claro.

Para cada i sea

$$I_i = IP_1 \ldots P_{i-1}P_{i+1} \ldots P_r.$$

Por la unicidad de la factorización I_iP_i está contenido propiamente en I_i. Por tanto, para cada i existe

$$a_i \in I_i \setminus I_iP_i.$$

Pongamos

$$a = a_1 + \ldots + a_r.$$

Como $a_i \in I_i \subseteq I$, para todo i, tenemos que $a \in I$. Pero para todo $i \neq j$, $a_j \in IP_i$, luego $a - a_i \in IP_i$, mientras que $a_i \notin IP_i$ y por tanto $a \notin IP_i$. Concluimos que $a \in I \setminus IP_i$ para todo i. O sea I divide a a pero IP_i no divide a a. Lo primero implica que aI^{-1} es un ideal de D y lo segundo que P_i no divide a aI^{-1}. Como $P_1, \ldots, P_r$ son todos los ideales maximales de D que contienen a J deducimos que aI^{-1} y J son coprimos, es decir $aI^{-1} + J = D$. ∎

Teorema 4.11 *Si I un ideal no nulo de D y $0 \neq b \in I$, entonces existe $a \in I$ tal que $I = Da + Db$.*

Demostración. Sea $a \in I$ tal que $aI^{-1} + bI^{-1} = D$. Por tanto, existen $u, v \in I^{-1}$ tales que $1 = ua + vb$. Por la definición de I^{-1} si $x \in I$ entonces $xu, xv \in D$. Luego $x = (xu)a + (xv)b \in Da + Db$. Esto demuestra que $I \subseteq Da + Db$. La otra inclusión es consecuencia de que $a, b \in I$.
∎

4.3 La norma de un ideal

En esta sección K es un cuerpo de números y $R = \mathbb{A}_K$.

Sabemos que un ideal I de un anillo A es primo si y solo si A/I es un dominio. Además I es maximal en A si y solo si A/I es un cuerpo. Por tanto todo ideal maximal es primo. El recíproco de la última propiedad no es cierto en general, pero veremos que sí que lo es para ideales primos no nulos de R.

Obsérvese que todo dominio finito es cuerpo pues un anillo conmutativo R es dominio si las aplicaciones $R \to R$ dadas por $x \mapsto rx$ para $r \in R \setminus \{0\}$ son todas inyectivas y es cuerpo si todas esas aplicaciones son suprayectivas.

Lema 4.12 *Sea D el anillo de enteros de un cuerpo de números.*

(1) Si I es un ideal no nulo de D, entonces D/I es finito.

(2) Los ideales primos no nulos de D son maximales.

Demostración. Sea $0 \neq a \in I$. Entonces $n = N_{K/\mathbb{Q}}(a)$ es un entero no nulo. Como a es un divisor de n en D tenemos que $n \in I$ y, por tanto D/I es un cociente de D/nD. Si consideramos la estructura aditiva de D/nD y $m = [K : \mathbb{Q}]$ tenemos que $|D/I| \leq |D/nD| = |\mathbb{Z}^m/n\mathbb{Z}^m| = n^m$, luego $|D/I|$ es finito. Si además I es primo entonces D/I es un dominio finito y, por tanto, un cuerpo. Luego I es ideal maximal de D. ∎

Del Lema 2.11 se deduce que K es el cuerpo de fracciones de R. Por tanto R es integramente cerrado. Como además R es notheriano por el Teorema 3.3, del Lema 4.12 deducimos el siguiente:

Teorema 4.13 *Todo anillo de enteros de un cuerpo de números es un dominio de Dedekind.*

Definición 4.14 *Un* primo *de K es por definición un ideal maximal de R, o sea un ideal primo no nulo de R.*

Por tanto todo ideal de R tiene una expresión única como producto de primos de K.
Por el Lema 4.12, para todo ideal I de R, R/I es finito.

Definición 4.15 *Se define la* norma de un ideal I *como $N(I) = [R : I] = |R/I|$.*

Por ejemplo, si m es un entero positivo, $n = [F : \mathbb{Q}]$ entonces $N(Rm) = [R : Rm] = [\mathbb{Z}^n, m\mathbb{Z}^n] = m^n$. O sea,

$$N(mR) = m^n \text{ para todo } m \in \mathbb{Z}^+. \tag{4.1}$$

Más adelante veremos que la norma de un elemento de R coincide con la el valor absoluto de norma del ideal generado por él. La siguiente proposición es una consecuencia directa de la Proposición 2.26

Proposición 4.16 *Sea n el grado de K, Δ el discriminante de K e I un ideal de R. Entonces*

$$N(I) = \left|\frac{\Delta[I]}{\Delta}\right|^{1/2}.$$

La norma de ideales tiene propiedades similares a la norma de elementos:

Proposición 4.17 *Sean I y J dos ideales de R. Entonces*

$$N(IJ) = N(I)N(J).$$

Demostración. Por unicidad de la factorización, e inducción en el número de factores primos podemos suponer que $J = P$ es primo. Para demostrar el resultado, en este caso, basta probar las dos siguientes fórmulas:

$$[R : IP] = [R : I] \mid [I : IP] \quad \text{e} \quad [I : IP] = [R : P],$$

pues de estas igualdades se deduce que $N(IP) = [R : IP] = [R : I][R : P] = N(I)N(P)$.

La primera de las igualdades es consecuencia del Tercer Teorema de Isomorfía:

$$R/I \simeq \frac{R/IP}{I/IP}.$$

Para demostrar la segunda primero observemos que el Teorema 4.3 implica que $IP \subset I$, o sea IP está propiamente contenido en I. Vamos a ver que no hay ideales entre IP e I. Supongamos que existe un ideal B de R con $IP \subseteq B \subseteq I$. Entonces

$$P = I^{-1}IP \subseteq I^{-1}B \subseteq I^{-1}I = R$$

y, como P es un ideal maximal,

$$P = I^{-1}B \quad \text{ó} \quad I^{-1}b = R,$$

o sea, $B = IP$ ó $B = I$.

Sea $a \in I \setminus IP$. Por lo visto arriba $I = IP + (a)$. La aplicación $\psi : R \to I/aP$ dada por $\psi(x) = ax + IP$ es un homomorfismo suprayectivo de R-módulos cuyo núcleo contiene a P pero no es R. De la maximalidad de P, se tiene que el núcleo es precisamente P. Del Primer Teorema de Isomorfía deducimos que $R/P \cong I/IP$ y por tanto $[R : P] = [I : IP]$. ∎

Proposición 4.18 *Sea I un ideal no nulo de R.*

(1) $I = R$ si y sólo si $N(I) = 1$.

(2) Si $N(I)$ es primo racional, entonces I es primo de K.

(3) $N(I) \in I$, o equivalentemente $I \mid N(I)$.

(4) Si I es primo, entonces I solo divide a un primo racional p y, en tal caso $N(I) = p^f$ para algún entero $1 \leq f \leq [K : \mathbb{Q}]$ y p es el único primo racional que pertenece a I.

(5) Sólo un número finito de ideales tienen una norma predeterminada.

Demostración. (1) es obvio y (2) es una consecuencia de la Proposición 4.17 y de la unicidad de la factorización.

(3) Obsérvese que $N(I) = [R : I]$. Luego, por el Teorema de Lagrange, para todo $x \in R$, $N(I)x \in I$. Particularizando al caso $x = 1$ se sigue el resultado.

(4) Como I es primo, $I \cap \mathbb{Z}$ es un ideal primo de $\mathbb{Z}$. Además, $N(I) \in I \cap \mathbb{Z} \setminus \{0\}$, con lo que $I \cap \mathbb{Z} = p\mathbb{Z}$ para algún primo racional p y p es el único primo racional de I. Como $p \in I$, tenemos que $I \mid Dp$ y de la Proposición 4.17 deducimos que $N(I) \mid N(Rp) = p^{[K:\mathbb{Q}]}$. Luego $N(I) = p^f$ con $1 \leq f \leq [K : \mathbb{Q}]$.

(5) Es una consecuencia de $I \mid N(I)R$ y de que cada ideal no nulo de R solo tiene un número finito de divisores. ∎

Acabamos esta sección demostrando que R tiene factorización única precisamente si es un DIP.

Teorema 4.19 *Un anillo de enteros de un cuerpo de números es un DFU precisamente si es un DIP.*

Demostración. Una implicación es bien conocida. Supongamos que R es un DFU. Como todo ideal es producto de ideales primos, basta con demostrar que todo ideal primo no nulo es principal. Sea P un ideal primo no nulo y sea $N = N(P) = p_1 \dots p_n$ una factorización de N como producto de irreducibles de R. Como N es un múltiplo de P y éste es primo, $P \mid Rp_i$ para algún i, o sea $Rp_i \subseteq P$. Como p_i es irreducible y R es un DFU, Rp_i es un ideal maximal de R. Luego $P = Rp_i$. ∎

Obsérvese que no es cierto que todo DFU sea un DIP, por ejemplo, $K[X, Y]$ es un DFU, pero no es un DIP.

4.4 Índice de ramificación y grado residual

En esta sección E/F es una extensión de cuerpos de números y R y S son los anillos de enteros de F y E respectivamente.

Sea Q un primo de E and sea $P = Q \cap F = Q \cap R$ (la última igualdad es consecuencia de que los elementos de Q son enteros y por tanto $Q \cap F \subseteq R$). Entonces P es un ideal primo de R que no es nulo pues $N(Q) \in P \cap R$, es decir P es un primo de F. Además $SP \subseteq Q$, o lo que es lo mismo $Q \mid SP$. Por otro lado, la composición de la inclusión $R \to S$ con la composición $S \to S/Q$ induce un homomorfismo inyectivo $R/P \to S/Q$ que utilizamos para ver S/Q como espacio vectorial sobre R/P.

El *índice de ramificación* de Q sobre F, que denotaremos $e(Q/F)$ es por definición el exponente de Q en la factorización de SP. El *grado residual* o *grado de inercia* de Q sobre R es

$$f(Q/F) = [S/Q : R/P] = \dim_{R/P}(S/Q)$$

Obsérvese que $f(Q/F)$ también se puede definir con la siguiente igualdad

$$N(Q) = |S/Q| = |(R/P)|^{f(Q/F)} = N(P)^{f(Q/F)} = N(Q \cap F)^{f(Q/F)}. \tag{4.2}$$

Recíprocamente, si P es un primo de F entonces los primos de E que contienen a P (o sea, los que aparecen en la factorización de SP) se llaman *primos* de E *sobre* P. Estos son precisamente los ideales maximales Q de S que satisfacen $Q \cap F = P$ (equivalentemente, $Q \cap R = P$). Por tanto, si los primos de E sobre P son $Q_1, \dots, Q_k$ entonces

$$SP = Q_1^{e(Q_1/F)} \dots Q_k^{e(Q_k/F)}.$$

Decimos que:

- Q es *ramificado sobre* F if $e(Q/F) > 1$.
- P es *ramificado en* E, o que P *ramifica* en E si algún primo de E sobre P es ramificado sobre F.
- P es *inerte* en E si PS es un ideal primo del anillo de S.

- P es *totalmente ramificado* en E si $PS = Q^{[E:F]}$ para un ideal maximal Q de S.
- P *escinde completamente* en E si PS es un producto de $[E:F]$ primos distintos.

Lema 4.20 *Si L es un cuerpo intermedio entre F y E y Q es un primo de E entonces*

(1) $e(Q/F) = e(Q/L)\, e(Q \cap L/F)$.

(2) $f(Q/F) = f(Q/L)\, f(Q \cap L/F)$.

Demostración. (1) Sean T el anillo de enteros de L, $P_1 = Q \cap L$ y $P = Q \cap F = P_1 \cap F$. Sean $PT = P_1^{e_1} \dots P_k^{e_k}$ y $P_1 S = Q_1^{e'_1} \dots Q_t^{e'_t}$ las factorizaciones de PT y $P_1 S$ en T y S respectivamente, con $Q = Q_1$. Entonces $e_1 = e(P_1/F)$ y $e'_1 = e(Q/E)$. Tenemos que demostrar $e(Q/F) = e_1 e'_1$. Si Q' es un ideal maximal de S que contiene a P_i entonces $Q' \cap T = P_i$. Como cada Q_i contiene a P_1 deducimos que $P_j \not\subseteq Q_i$ para todo $i = 1, \dots, t$ y $j \geq 2$. Esto implica que la factorización de PS en S es de la forma $PS = (P_1 S)^{e_1} \dots (P_k S)^{e_k} = (Q_1^{e_1 e'_1} \dots Q_t^{e_1 e'_t}) Q_{t+1}^{e'_{t+1}} \dots Q_m^{e'_m}$, para algunos ideales maximales $Q_{t+1}, \dots, Q_m$ distintos de $Q_1, \dots, Q_t$ y enteros no negativos $e'_{t+1}, \dots, e'_m$. Luego $e(Q/F) = e_1 e'_1$.

(2) $f(Q/F) = [S/Q : R/P] = [S/Q : T/P_1][T/P_1 : R/P] = f(Q/T) f(L \cap Q/F)$. ∎

Lema 4.21 *Si I es un ideal no nulo de R entonces $N(SI) = N(I)^{[E:F]}$.*

Demostración. Usando el Teorema 4.3, la Proposición 4.17 y que $S(IJ) = (SI)(SJ)$, es suficiente demostrar el lema para el caso en que I es un ideal primo que vamos a denotar por P para ayudar a recordar que es primo. Entonces S/PS es un espacio vectorial sobre R/P y será suficiente con demostrar

$$\dim_{R/P}(S/PS) = [E:F]. \tag{4.3}$$

pues en tal caso tendremos que $N(PS) = |S/PS| = |R/P|^{[E:F]} = N(P)^{[E:F]}$ que es lo que queremos demostrar.

Demostrar (4.3) es fácil si $F = \mathbb{Q}$ pues entonces $R = \mathbb{Z}$ y $P = p\mathbb{Z}$ para algún primo p con lo que $PS = pS$ y $S/pS \cong (\mathbb{Z}/p\mathbb{Z})^{[E:\mathbb{Q}]}$, de donde deducimos que $\dim_{\mathbb{Z}/p\mathbb{Z}}(S/pS) = [E:\mathbb{Q}]$.

Para demostrar (4.3) en general ponemos $n = [E:F]$ y primero demostramos que $n \geq \dim_{R/P}(S/PS)$. En caso contrario S tiene $n+1$ elementos $s_0, s_1, \dots, s_n$ cuyas imágenes $\overline{s_i}$ en S/PS son linealmente independientes sobre R/P. Como $s_0, s_1, \dots, s_n$ son linealmente dependientes sobre K también lo son sobre R con lo que existen $r_0, r_1, \dots, r_n \in R$ tales que $\sum_{i=0}^n r_i s_i = 0$ y algún $r_i \neq 0$. Sea $I = \sum_{i=0}^n R r_i$. Por el Lema 4.9 existe un ideal J de R tal que $IJ = Ra$ para algún $a \in R \setminus \{0\}$. Como P es un ideal maximal de R, de la unicidad de la factorización tenemos que $Ra \neq Pa$. Luego existe $b \in J$ tal que $Ib \not\subseteq Pa$, con lo que $\frac{b}{a} I \subseteq R$ pero $I\frac{b}{a} \not\subseteq P$. Eso implica que cada $r'_i = \frac{b}{a} r_i \in R$ y algún $r'_j \notin P$. Como $\sum_{i=0}^n r'_i s_i = 0$ deducimos que $\sum_{i=0}^n \overline{r'_i}\,\overline{s_i} = 0$ pero $\overline{r'_j} \neq 0$. Luego $\overline{s_0}, \overline{s_1}, \dots, \overline{s_n}$ son linealmente dependientes sobre R/P en contra de la hipótesis.

Sea $m = [F:\mathbb{Q}]$, $P \cap \mathbb{Z} = p\mathbb{Z}$, con p un primo racional positivo, y $P_1, \dots, P_r$ los primos de F sobre p. Uno de ellos será P, con lo que podemos suponer que $P_1 = P$. Pongamos

$e'_i = e(P_i/\mathbb{Q})$, $f'_i = f(P_i/\mathbb{Q})$, $n_i = \dim_{R/P_i}(S/P_iS)$. Aplicando (4.1) y la Proposición 4.17 tenemos que

$$p^m = N(pR) = N(P_1^{e_1} \cdots P_r^{e_r}) = N(P_1)^{e_1} \cdots N(P_r)^{e_r} = p^{e_1 f_1 + \cdots + e_r f_r}$$

Por tanto $m = \sum_{i=1}^r e'_i f'_i$. Además, en el párrafo anterior hemos demostrado que cada $n_i \leq n$. Como $pS = \prod_{i=1}^r (P_iS)^{e'_i}$, usando de nuevo (4.1) y la Proposición 4.17 tenemos que

$$p^{nm} = N(pS) = \prod_{i=1}^r N(P_iS)^{e'_i} = \prod_{i=1}^r N(P_i)^{n_i e'_i} = \prod_{i=1}^r p^{n_i e'_i f'_i} = p^{\sum_{i=1}^r n_i e'_i f'_i}.$$

Luego $nm = \sum_{i=1}^r n_i e'_i f'_i \leq n \sum_{i=1}^r e'_i f'_i = nm$. Pero como $n_i \leq n$ para todo i deducimos que $n_i = n$ para todo i y aplicando esto para $i = 1$ tenemos (4.3). ∎

Corolario 4.22 *Si R es el anillo de enteros de un cuerpo de números F y $a \in R\backslash\{0\}$ entonces $N(Ra) = |N_{F/\mathbb{Q}}(a)|$.*

Demostración. Sean $\sigma_1, \ldots, \sigma_n$ las inclusiones de F en $\mathbb{C}$ y sea E la clausura normal de K en $\mathbb{C}$, es decir E es el menor subcuerpo de $\mathbb{C}$ que contiene a $\sigma_i(F)$ para todo i. Sea S el anillo de enteros de E y supongamos que $m = [E : F]$ y $k = N_{F/\mathbb{Q}}(a)$. Cada σ_i extiende a un automorfismo de E, que también denotaremos σ_i. Además $S = \sigma_i(S)$ y por tanto $\sigma_i(Sa) = S\sigma_i(a)$, con lo que σ_i induce un isomorfismo $S/Sa \to S/S\sigma_i(a)$. Por tanto

$$N(S\sigma_i(a)) = N(Sa).$$

Usando (4.1), la Proposición 4.17 y el Lema 4.21 deducimos que

$$|k|^{mn} = N(Sk) = N\left(S\prod_{i=1}^n \sigma_i(a)\right) = N\left(\prod_{i=1}^n S\sigma_i(a)\right) = \prod_{i=1}^n N(S\sigma_i(a)) = N(Sa)^n = N(Ra)^{nm}$$

y por tanto $N(Ra) = |k|$, como queríamos. ∎

Teorema 4.23 *Sea R el anillo de enteros de un cuerpo de números F y sean P un ideal maximal de R y E una extensión finita de F. Si $e_1, \ldots, e_k$ y $f_1, \ldots, f_k$ son los índices de ramificación y los grados residuales de los primos de E sobre P, entonces*

$$\sum_{i=1}^k e_i f_i = [E : F].$$

Demostración. Sea $PS = Q_1^{e_1} \ldots Q_k^{e_k}$ la factorización de PS y para cada i sea $f_i = \dim_{R/P}(S/Q_i)$ para todo i. Aplicando primero el Lema 4.21 y después la Proposición 4.17 tenemos que

$$N(P)^{[E:F]} = N(PS) = N(Q_1)^{e_1} \cdots N(Q_f)^{e_k} = N(P)^{\sum_{i=1}^k e_i f_i}$$

y por tanto $[E : F] = \sum_{i=1}^k e_i f_i$. ∎

Corolario 4.24 *Sean E/F una extensión de cuerpos de números y P un primo de F.*

(1) P es inerte en E si y solo si E contiene un primo sobre P tal que $f(Q/F) = [E : F]$. En tal caso P no es ramificado en E.

(2) P es totalmente ramificado en E si y solo si E contiene un primo Q sobre P con $e(Q/E) = [E : F]$.

(3) P escinde completamente en E si $e(Q/F) = f(Q/F) = 1$ para todo primo Q de E sobre F. En particular, en tal caso, P no es ramificado en E.

Sea P un primo de F. Si σ es un F-automorfismo de E entonces $\sigma(R) = R$, $\sigma(P) = P$ y $\sigma(S) = S$. Por tanto, si $PS = Q_1^{e_1} \cdots Q_g^{e_g}$ es la factorización PS en producto de maximales de S entonces cada $\sigma(Q_i)$ es un ideal maximal de S sobre P y $PS = \sigma(Q_1)^{e_1} \cdots \sigma(Q_g)^{e_g}$. De la unicidad de la factorización deducimos que σ permuta los Q_i's y $e(\sigma(Q_i)/F) = e(Q_i/F)$ para todo i, es decir:

Proposición 4.25 *Sea E/F una extensión de cuerpos de números y sea P un primo de F. El grupo de Galois $\mathrm{Gal}(E/F)$ permuta los primos de E sobre P y todos los primos de E sobre P en la misma órbita de la acción de $\mathrm{Gal}(E/F)$ tienen el mismo índice de ramificación.*

4.5 Factorización de un primo racional

Sea p un primo racional. Denotamos la imagen de un entero a en $\mathbb{Z}_p$ como $\overline{a}$ y para un polinomio $f = a_0 + a_1X + \ldots \in \mathbb{Z}[X]$, denotaremos por $\overline{f}$ al polinomio de $\overline{a_0} + \overline{a_1}X + \ldots \in \mathbb{Z}_p[X]$.

El siguiente teorema nos proporciona un método para calcular los primos de un cuerpo de número K sobre $p\mathbb{Z}$ y sus indices de ramificación y grados residuales, en el caso en el que el anillo de enteros de K sea se la forma $\mathbb{Z}[\theta]$ para algún θ.

Teorema 4.26 (Dedekind) *Sea K un cuerpo de números de grado n tal que su anillo de enteros sea de la forma $R = \mathbb{Z}[\theta]$ para algún $\theta \in R$. Sea $f = Min_{\mathbb{Q}}(\theta)$, el polinomio mínimo de θ sobre $\mathbb{Q}$. Sea p un primo de $\mathbb{Z}$ y sea*

$$\overline{f} = \overline{f_1}^{e_1} \ldots \overline{f_r}^{e_r}$$

la factorización de $\overline{f}$ en $\mathbb{Z}_p[X]$ con $f_1, \ldots, f_r \in \mathbb{Z}[X]$ y $\mathrm{gr}(f_i) = \mathrm{gr}(\overline{f_i})$ para todo i. Entonces los ideales

$$P_i = Rp + Rf_i(\theta)$$

son maximales en R y distintos dos a dos. Además $f(P_i/\mathbb{Q}) = \mathrm{gr}(f_i)$ y $e(P_i/\mathbb{Q}) = e_i$ para todo i, y por tanto

$$pR = P_1^{e_1} \cdots P_k^{e_k}.$$

Demostración. Sea θ_i una raíz de $\overline{f_i}$ en una extensión de $\mathbb{Z}_p$. Entonces $\mathbb{Z}_p[\theta_i] \simeq \mathbb{Z}_p[X]/(\overline{f_i})$. Sea $\nu_i : \mathbb{Z}[\theta] \to \mathbb{Z}_p[\theta_i]$ el homomorfismo dado por

$$\nu_i(g(\theta)) = \overline{g}(\theta_i).$$

Esta aplicación está bien definida pues si $g(\theta) = 0$ con $g \in \mathbb{Z}[X]$, entonces $f \mid g$ en $\mathbb{Q}[X]$. Si $g = fh$ con $h \in \mathbb{Q}[X]$ entonces, del Lema de Gauss (2.13) existe $c \in \mathbb{Q} \setminus \{0\}$ tal que $cf, c^{-1}h \in \mathbb{Z}[X]$. Como f es mónico $c \in \mathbb{Z}$ y $\overline{f_i} \mid \overline{g}$ en $\mathbb{Z}_p$, lo que implica que $\overline{g}(\theta_i) = 0$. La imagen de ν_i es $\mathbb{Z}_p[\theta_i]$ que es un cuerpo por ser θ_i algebraico sobre $\mathbb{Z}_p$. Luego $P_i = \ker \nu_i$ es un ideal maximal de $R = \mathbb{Z}[\theta]$. Si $g(\theta) \in \ker \nu_i$, entonces $\overline{g} = \overline{f_i}\,\overline{h}$ para algún $h \in \mathbb{Z}[X]$, luego los coeficientes de $g - f_i h$ son múltiplos de p. Por tanto

$$g(\theta) = (g - f_i h_i)(\theta) + f_i(\theta)h(\theta) \in Rp + Rf_i(\theta) = P_i.$$

Esto prueba que $\ker \nu_i \subseteq P_i$. Como la otra inclusión es obvia tenemos que

$$P_i = \ker \nu_i.$$

En particular P_i divide a Rp. Luego

$$\begin{aligned} P_1^{e_1} \dots P_r^{e_r} &= (Rp + Rf_1(\theta))^{e_1} \cdots (Rp + Rf_r(\theta))^{e_r} \\ &\subseteq Rp + Rf_1(\theta)^{e_1} \cdots f_1(\theta)^{e_n} \subseteq Rp + Rf(\theta) = Rp. \end{aligned}$$

Es decir, $Rp \mid P_1^{e_1} \cdots P_r^{e_r}$ y los únicos divisores primos de Rp (o sea los primos de K sobre p) son $P_1, \dots, P_r$ y $e(P_i/\mathbb{Q}) \leq e_i$ para todo i. Para probar la igualdad obsérvese que

$$R/P_i = \mathbb{Z}[\theta]/P_i \simeq \mathbb{Z}_p[\theta_i],$$

que tiene dimensión $\mathrm{gr}(\overline{f_i})$, es decir $f_i(P_i/\mathbb{Q}) = \mathrm{gr}(f_i)$. Aplicando el Teorema 4.23 tenemos que

$$n = \sum_{i=1}^{r} e_i(P_i/\mathbb{Q}) f_i(P_i/\mathbb{Q}) \leq \sum_{i=1}^{r} \mathrm{gr}(\overline{f_i}) e_i = \mathrm{gr}(f) = n$$

y como $e(P_i/\mathbb{Q}) \leq e_i$ para todo i necesariamente se tiene que dar la igualdad. ∎

Hay que tener cuidado con el teorema que acabamos de probar porque no todos los anillos de enteros son de la forma $\mathbb{Z}[\theta]$. Al menos sí lo son los anillos de enteros de los cuerpos cuadráticos y ciclotómicos.

Problema 4.27 *Sean p un primo racional, d un entero racional libre de cuadrados. Calcular los primos de $\mathbb{Q}(\sqrt{d})$ sobre p y sus índices de ramificación y grados residuales sobre $\mathbb{Q}$.*

Capítulo 5

Métodos Geométricos

5.1 Retículos

En esta sección V es un un espacio vectorial sobre $\mathbb{R}$ de dimensión n. Consideramos V como espacio topológico con la topología euclídea. Más precisamente si fijamos un isomorfismo de espacios vectoriales $f : V \to \mathbb{R}^n$ y consideramos en $\mathbb{R}^n$ la topología dada por una norma, entonces la topología de f es tal que f es un homeomorfismo. Por la unicidad de todas las topologías de las normas en $\mathbb{R}^n$, la topología de V no depende del isomorfismo f.

Obsérvese que la elección de f equivale a la elección de una base $B = \{v_1, \ldots, v_n\}$ de V dada por $f(v_i) = e_i$, donde $e_1, \ldots, e_n$ es la base canónica de $\mathbb{R}^n$. Nos referimos a B como la *base de referencia*. Consideramos $\mathbb{R}^n$ como espacio métrico con respecto a la norma estándar: o sea

$$\|(x_1, \ldots, x_n)\| = \sqrt{x_1^2 + \cdots + x_n^2}.$$

Usamos f para transferir los conceptos métricos de $\mathbb{R}^n$ a V, pero esta noción sí que depende de la elección de f. En otras palabras la métrica depende de la base de referencia pero la topología no. Por ejemplo, si $x, y \in V$, entonces se definen la distancia $d(x, y)$ entre x e y y la norma $\|x\|$ de x en la base de referencia, como la distancia euclídea $d(f(x), f(y))$ y la norma euclídea $\|f(x)\|$ respectivamente. Sin embargo, algunos conceptos no dependen de la base de referencia. Por ejemplo, el que un conjunto sea acotado no depende de la referencia.

Si X es un subconjunto de V entonces decimos que X es *medible* si la integral de Riemann $\int_{f(X)} dx$ existe y en tal caso el *volumen* of X con respecto a la base de referencia es

$$\mathrm{vol}(X) = \int_{f(X)} dx.$$

La medibilidad de X es independente de la base de referencía pero el valor del volumen sí que depende de esa base. Si $T : V \to V$ es una aplicación lineal entonces para cada subconjunto X de V se verifica

$$\mathrm{vol}(T(X)) = |\det(T)|\ \mathrm{vol}(X), \quad (X \subseteq V). \tag{5.1}$$

(Esta igualdad implícitamente asegura que X es medible si y sólo si lo es $T(X)$.) Además (5.1) implica que si B si B' y son dos bases de referencia entonces $\mathrm{vol}_{B'} = |\det(A)|\mathrm{vol}_B$, donde A es

la matriz de cambio de base de B a B'. De (5.1) se deduce que si $a \in \mathbb{R}$ entonces

$$\mathrm{vol}(aX) = |a|^n \,\mathrm{vol}(X). \tag{5.2}$$

Esta fórmula es independiente de la base de referencia.

Un subconjunto X de V se dice que es *discreto* si para todo subconjunto compacto K de V se verifica que $X \cap K$ es finito. Es bien conocido que un subconjunto de V es compacto si y sólo si es cerrado y acotado. Por tanto un subconjunto X de V es discreto si y sólo si todo subconjunto acotado de V tiene un número finito de elementos de X.

Un *retículo* L de *rango* k en V es un subgrupo aditivo de V generado por k elementos linealmente independientes sobre $\mathbb{R}$. En tal caso decimos que esos k elementos son una base de L. Un retículo de V se dice que es *pleno* si su rango coincide con la dimensión de V.

Lema 5.1 *Sea L un retículo en un espacio vectorial real V de dimensión n. Entonces L es pleno en V si y solo si existe un subconjunto acotado B de V tal que*

$$V = \bigcup_{x \in L} (x + B).$$

Demostración. La condición necesaria se obtiene cogiendo $B = \{a_1 v_1 + \cdots + a_n v_n : 0 \le a_i \le 1\}$ con $v_1, \ldots, v_n$ una base de L.

Sean W el subespacio vectorial generado por L, W' el complemento ortonormal de W en V y $p : V \to W'$ la proyección ortonormal a lo largo de W. Obsérvese que p transforma conjuntos acotados en conjuntos acotados. Supongamos que existe B acotado tal que $V = \cup_{x \in L}(x + B)$. Entonces $V = W + B$ y, por tanto $W' = p(B)$. Como B es acotado, W' también es acotado y, por tanto $W' = 0$. Luego $V = W$, o sea L es pleno en V. ∎

Proposición 5.2 *Sea V un espacio vectorial sobre $\mathbb{R}$ de dimensión finita. Un subgrupo aditivo de V es un retículo si y sólo si es discreto.*

Demostración. Supongamos primero que L es un retículo de V. Ampliando L si fuera necesario podemos suponer que L es un retículo pleno. Luego $L = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$, con $v_1, \ldots, v_n$ una $\mathbb{R}$-base de V. Sea K un subconjunto acotado de V. Entonces existe un número real positivo ϵ, tal que K está contenido en $\{\sum_{i=1}^n a_i v_i \ : \ a_i \in \mathbb{R},\ |a_i| \le \epsilon\}$. Si $x \in L \cap K$ entonces $x = \sum_{i=1}^k a_i v_i$, con $a_i \in \mathbb{Z} \cap [-\epsilon, \epsilon]$. Luego $L \cap K$ es finito.

Recíprocamente, supongamos que L es un subgrupo discreto de V. Demostramos que L es un retículo por inducción sobre la dimensión n de V. El caso $n = 0$ es obvio. Supongamos que $n \ge 1$ y que el resultado se verifica para subespacios vectoriales de dimensión menor que n. Esto implica que podemos suponer que L no está contenido en ningún subespacio propio de V. En consecuencia L contiene una base $v_1, \ldots, v_n$ de V sobre $\mathbb{R}$. Sean $W = \mathbb{R}v_1 + \cdots + \mathbb{R}v_{n-1}$ y $L_0 = L \cap W$. Como L es discreto, también lo es L_0 y como L_0 es un subgrupo aditivo de W, por la hipótesis de inducción L_0 es un retículo en W. Además $v_1, \ldots, v_{n-1} \in L_0$ y por tanto L_0 es un retículo pleno de W. Luego $L_0 = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_{n-1}$ para alguna base $w_1, \ldots, w_{n-1}$ de W. Claramente $w_1, \ldots, w_{n-1}, v_n$ es una base de V. Sea

$$K = \{a_1 w_1 + \cdots + a_{n-1} w_{n-1} + a_n v_n : 0 \le a_1, \ldots, a_{n-1} < 1 \text{ y } 0 \le a_n \le 1\}.$$

Entonces K es un subconjunto acotado de V y $v_n \in (K \cap L) \setminus W$. Por hipótesis $(K \cap L) \setminus W$ es finito y por tanto existe un menor real no negativo ϵ con $x_0 = a_1 w_1 + \cdots + a_{n-1} w_{n-1} + \epsilon v_n \in (K \cap L) \setminus W$ para algunos $0 \leq a_1, \ldots, a_{n-1} < 1$. Como $x_0 \notin W$ necesariamente $0 < \epsilon$ y como $v_n \in (K \cap L) \setminus W$ tenemos que $\epsilon \leq 1$. Sea $L_1 = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_{n-1} + \mathbb{Z}x_0$. Está claro que $L_1 \subseteq L$ y demostraremos que en realidad se da la igualdad. En efecto, sea $x = b_1 w_1 + \cdots + b_{n-1} w_{n-1} + b_n v_n$ un elemento arbitrario de L, con cada $b_i \in \mathbb{R}$. Pongamos $b_n = m_n \epsilon + c_n$ con $m_n \in \mathbb{Z}$ y $0 \leq c_n < \epsilon$ para cada $i = 1, \ldots, n-1$ sea $b_i - m_n a_i = m_i + c_i$ con $m_i \in \mathbb{Z}$ y $0 \leq c_i < 1$. Consideremos el siguiente elemento de L_1:

$$\begin{aligned} y &= m_1 w_1 + \cdots + m_{n-1} w_{n-1} + m_n x_0 \\ &= (m_1 + m_n a_1) w_1 + \cdots + (m_{n-1} + m_n a_{n-1}) w_{n-1} + m_n \epsilon v_n \\ &= x - (c_1 w_1 + \cdots + c_{n-1} w_{n-1} + c_n v_n) . \end{aligned}$$

O sea $x - y = c_1 w_1 + \cdots + c_{n-1} w_{n-1} + c_n v_n \in L \cap K$. La elección de ϵ implica que $c_n = 0$. Luego $x - y \in L \cap W = L_0 \subseteq L_1$ y por tanto $x \in L_1$. Esto demuestra que $L = L_1 = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_{n-1} + \mathbb{Z}x_0$. Luego L es un retículo en V. ∎

Sea L un retículo pleno en V y sea $B = \{v_1, \ldots, v_n\}$ una base de L. Entonces B también es una $\mathbb{R}$-base de V. El *poliedro fundamental* o *dominio fundamental* de B es

$$P_B = \left\{ \sum_{i=1}^{n} x_i v_i : 0 \leq x_i < 1 \right\}. \tag{5.3}$$

Está claro que los conjuntos $a + P_B = \{v + x : x \in P_B\}$ con a recorriendo los elementos de L forman una partición de V con lo que para cada $x \in V$ existe un único $f(x) \in P_B$ tal que $x - f(x) \in L$. Aunque el poliedro fundamental P_B depende de la base, su volumen sólo depende del retículo.

Lema 5.3 *Todos los poliedros fundamentales de un retículo pleno tienen el mismo volumen.*

Demostración. Sean $B = \{v_1, \ldots, v_n\}$ y $B_1 = \{w_1, \ldots, w_n\}$ bases de un mismo retículo L en V. Sea f el isomorfismo $V \to V$ que asocia cada v_i con w_i. Como $\mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n$ la matriz A asociada a f en la base B tiene entradas enteras y su inversa también. Eso implica que $\det(f) = \det(A) = \pm 1$. Además, $f(P_B) = P_{B_1}$. Aplicando (5.1), deducimos que $\mathrm{vol}(F_{B_1}) = |\det(f)| \mathrm{vol}(F_B) = \mathrm{vol}(F_B)$. ∎

Para cada retículo L en V definimos

$$\mathrm{vol}(V/L) = \begin{cases} \mathrm{vol}(P_B), & \text{si } L \text{ es pleno en } V \text{ y } B \text{ es una base de } L; \\ \infty, & \text{si } L \text{ no es pleno en } V. \end{cases}.$$

Esto a veces se llama *covolumen* de L en V.

Lema 5.4 *Sea L un retículo pleno en V con base $B = \{v_1, \ldots, v_n\}$. Sea $w_1, \ldots, w_n \in L$ y pongamos $w_i = \sum_{i=1}^{n} a_{ij} v_j$, con $a_{ij} \in \mathbb{Z}$ para $1 \leq i, j \leq n$. Sea $M = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n$.*

Entonces M es un retículo en V. Además, M es pleno en V si y sólo si $\det((a_{ij})) \neq 0$, *o equivalentemente si M tiene índice finito en L. En este caso*

$$[L : M] = |\det((a_{ij}))| = \frac{\mathrm{vol}(V/M)}{\mathrm{vol}(V/L)}.$$

Demostración. Por la Proposition 5.2, L es discreto en V. Luego también lo es M. Aplicando la misma proposición deducimos que M es un retículo en V. Claramente, M es pleno en V si y sólo si $\det((a_{ij})) \neq 0$ y, por el Lema 1.4, esto pasa si y sólo si L/M is finito, y en tal caso $[L : M] = |\det((a_{ij}))|$. Sea f el automorfismo de V que asocia v_i con w_i. Entonces $f(P_B) = P_{B_1}$ con $B_1 = \{w_1, \ldots, w_n\}$ y la matriz asociada a este isomorfismo en la base B es (a_{ij}). Luego $\mathrm{vol}(V/M) = \mathrm{vol}(F_{B_1}) = |\det((a_{ij}))|\mathrm{vol}(F) = |\det((a_{ij}))|\mathrm{vol}(V/L)$, por (5.1). ∎

Obsérvese que la fórmula del Lemma 5.4 es independiente de la base de referencia que se usa para calcular el volumen. De la misma manera las hipótesis del siguiente Teorema son independiente de la base de referencia.

Teorema 5.5 (Minkowski) *Sea V un espacio vectorial sobre $\mathbb{R}$ de dimensión n y sea L un retículo pleno en V. Sea X un subconjunto acotado medible de V que cumple las siguientes condiciones:*

(1) $\mathrm{vol}(X) > 2^n \mathrm{vol}(V/L)$.

(2) si $x, y \in X$ entonces $\frac{x-y}{2} \in X$.

Entonces, $X \cap L$ tiene un elemento distinto de 0.

En caso de que X sea compacto se puede sustituir la desigualdad estricta de (1) por una desigualdad no estricta.

Demostración. Fijamos una base de $B = \{v_1, \ldots, v_n\}$ de L. Entonces $2B = \{2v_1, \ldots, 2v_n\}$ es una base de $2L$. Sea F un poliedro fundamental de $2B$. Por la primera hipótesis y por el Lema 5.4 tenemos $\mathrm{vol}(F) = \mathrm{vol}(V/2L) = 2^n \mathrm{vol}(V/L) < \mathrm{vol}(X)$. Cada elemento de V tiene una única expresión como $x + y$ con $x \in 2L$ e $y \in F$. Consideremos la aplicación $f : V \to F$ que asocia $x \in V$ con el único $f(x) \in F$ para el que $x - f(x) \in 2L$. Para cada $a \in 2L$ y cada $x \in a + F$ tenemos $f(x) = x - a$. Como las traslaciones conservan el volumen tenemos que $\mathrm{vol}(f(Y)) = \mathrm{vol}(Y)$ para cada subconjunto medible Y de $a + F$.

Como X está acotado existen elementos distintos $a_1, \ldots, a_k$ de $2L$ de forma que $X \subseteq \cup_{i=1}^k (a_i + F)$. Luego $X = \cup_{i=1}^k (X \cap (a_i + F))$ y esta es una unión disjunta. Luego $\mathrm{vol}(F) < \mathrm{vol}(X) = \sum_{i=1}^k \mathrm{vol}(X \cap (a_i + F)) = \sum_{i=1}^k \mathrm{vol}(f(X \cap (a_i + F)))$. Como cada $f(X \cap (a_i + F)) \subseteq F$, la anterior desigualdad implica que los conjuntos $f(X \cap (a_1 + F)), \ldots, f(X \cap (a_k + F))$ no pueden ser disjuntos dos a dos. Luego la restricción de f a X no es inyectiva. Por tanto existen elementos distintos x e y de X con $f(x) = f(y)$. Luego $x - y = (x - f(x)) + (f(y) - y) \in 2L$. Aplicando la segunda hipótesis tenemos que $\frac{x-y}{2}$ es un elemento no nulo de $X \cap L$.

Vemos ahora que en el caso en que X sea compacto basta con suponer que $\mathrm{vol}(X) \geq 2^n \mathrm{vol}(V/L)$. En efecto, para cada $\epsilon > 1$ se cumple que $\mathrm{vol}(\epsilon X) > \mathrm{vol}(X)$, con lo que aplicando el teorema a ϵX se verificará que existe $x_\epsilon \in (\epsilon X) \cap L \setminus \{0\}$. Sea $B(0, \alpha)$ una bola que contiene

a X. Como L es discreto $B(0,2\alpha) \cap L$ es finito, digamos que formado por 0 y $a_1, \ldots, a_k$. Supongamos que $X \cap L$ no contiene ningún elemento no nulo. Como $a_i \notin X$ y X es compacto para cada $i = 1, \ldots, k$ existe un $\epsilon_i > 1$ tal que $a_i \notin \epsilon_i X$. Entonces $\epsilon = \min(\epsilon_i : i = 1, \ldots, k) > 1$ y $X \cap \epsilon L \setminus \{0\} = \emptyset$, en contra de lo que hemos visto antes. ∎

Observación 5.6 En la mayoría de referencias la hipótesis (2) es reemplazada por la siguiente hipótesis más fuerte: X es convexo y 0-simétrico, es decir para todo $x, y \in X$ el segmento que une x e y está contenido en X y $-x \in X$.

5.2 Teoremas de los dos y cuatro cuadrados

En esta sección vamos a ver dos aplicaciones del Teorema de Minkowski. En realidad la primera ya la vimos en la Proposición 3.11 pero ahora vemos una demostración diferente.

Teorema 5.7 *(Teorema de los Dos Cuadrados. Fermat-Euler) Si p es un primo tal que $p \equiv 1 \mod 4$, entonces p es suma de dos cuadrados.*

Demostración. El grupo multiplicativo del cuerpo $\mathbb{Z}_p$ es cíclico de orden $p-1$. Luego dicho grupo contiene un elemento u de orden 4. Eso implica que $\overline{u^2}$ es el único elemento de orden 2 (recuérdese que un grupo cíclico tiene exactamente un subgrupo de orden un divisor dado del orden del grupo), o sea $u^2 \equiv -1 \mod p$. Sea

$$L = \{(a,b) \in \mathbb{Z}^2 : b \equiv ua \mod p\}.$$

Este es un subgrupo de $\mathbb{Z}^2$ de indice p pues si $(n,m) \in \mathbb{Z}^2$ y $n - um \equiv t \mod p$ $(0 \leq t \leq p-1)$, entonces $(n,m) - (t,0) \in L$. Por el Lema 5.4, el volumen del poliedro fundamental del retículo L es p. Por el Teorema de Minkowski cada bola $B(0;r)$ con área $\pi r^2 > 4p$ contiene un punto de L distinto del origen. Sea $r = \sqrt{\frac{3p}{2}}$. Entonces $\pi r^2 = \frac{3\pi p}{2} > 4p$. Sea (a,b) un punto de $L \cap B(0,r)$ distinto del origen. Entonces

$$0 \neq a^2 + b^2 \leq r^2 = \frac{3p}{2} < 2p$$

y

$$a^2 + b^2 \equiv a^2 + u^2 a^2 \equiv 0 \mod p.$$

Luego $a^2 + b^2$ es un múltiplo de p contenido estrictamente entre 0 y $2p$ y, por tanto es p. ∎

Refinando el argumento del Teorema de los Dos Cuadrados podemos obtener el Teorema de las Cuatro Cuadrados. Primero recordemos el siguiente hecho básico sobre cuerpos finitos de orden impar.

Lema 5.8 *Si F es un cuerpo finito de orden impar y F^2 denota el conjunto de los cuadrados de F, entonces $|F^2| = \frac{|F|+1}{2}$.*

Demostración. Si $x^2 = y^2$, entonces $(x+y)(x-y) = 0$, luego, $x = y$ ó $x = -y$. Esto prueba que si $f : F \to F^2$ viene dada por $f(x) = x^2$ entonces para cada $x \in F^2$ se tiene que

$$|f^{-1}(x)| = \begin{cases} 1, & \text{si } x = 0; \\ 2, & \text{si } x \neq 0. \end{cases}$$

Luego $|F^2| = 1 + \frac{|F|-1}{2} = \frac{|F|+1}{2}$. ∎

Teorema 5.9 *(Teorema de los Cuatro Cuadrados. Fermat-Lagrange) Todo entero positivo es suma de cuatro cuadrados.*

Demostración. Primero probamos el resultado para los primos y después lo extendemos a todos los enteros positivos. Para 2 el resultado es trivial. Sea p un primo impar y $F = \mathbb{Z}_p$. Como $|F^2| = |-1 - F^2| = \frac{p+1}{2}$, necesariamente $F^2 \cap (-1 - F^2) \neq \emptyset$, luego existen u, v enteros tales que

$$u^2 + v^2 + 1 \equiv 0 \mod p.$$

Consideramos el siguiente retículo

$$L = \{(a,b,c,d) \in \mathbb{Z}^4 | c \equiv ua + vb \mod p \text{ y } d \equiv ub - va \mod p\}.$$

Se demuestra fácilmente que L tiene índice p^2 en $\mathbb{Z}^4$, con lo que del Lema 5.4 se tiene que $\text{vol}(\mathbb{R}^n/L) = p^2$. Consideramos la esfera de dimensión cuatro $B(0;r)$ (que tiene volumen $\frac{\pi^2 r^4}{2}$). Eligiendo $r = \sqrt{2p}$ tenemos una esfera de volumen $> 16p^2$. Aplicando el Teorema de Minkowski elegimos un elemento no nulo (a,b,c,d) de esta esfera que pertenezca a L. Luego

$$0 \neq a^2 + b^2 + c^2 + d^2 < 2p.$$

y

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &\equiv a^2 + b^2 + (ua + vb)^2 + (ub - va)^2 \\ &\equiv (1 + u^2 + v^2)a^2 + (1 + u^2 + v^2)b^2 \\ &\equiv 0 \mod p. \end{aligned}$$

Por tanto $a^2 + b^2 + c^2 + d^2 = p$.

Ahora consideramos el caso general de un entero positivo n y razonamos por inducción en el número de factores en su descomposición en irreducibles. Para el paso de inducción basta aplicar la fórmula

$$\begin{aligned} (a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) =& (aA - bB - cC - dD)^2 + (aB + bA + cD - dC)^2 + \\ & (aC + bD + cA + dB)^2 + (aD + bC - cB + dA)^2. \end{aligned}$$

∎

Una forma alternativa de ver la última fórmula de la demostración anterior es la siguiente: Consideremos el álgebra de cuaterniones $\mathbb{H}(\mathbb{R}) = \{a + bi + cj + dk : a,b,c,d \in \mathbb{R}\}$ donde $i^2 = j^2 = -1$ y $k = ij = -ji$. Este álgebra tiene una "conjugación" dada por

$$\overline{a + bi + cj + dk} = a - bi - cj - dk, \quad a,b,c,d \in \mathbb{R}$$

que verifica

$$\overline{\alpha+\beta}=\overline{\alpha}+\overline{\beta} \quad \text{y} \quad \overline{\alpha\beta}=\overline{\beta}\overline{\alpha} \quad (\alpha,\beta\in\mathbb{H}(\mathbb{R})).$$

Usando esto podemos definir la norma

$$N(\alpha)=\alpha\,\overline{\alpha}.$$

Una cuentas sencillas muestran que

$$N(a+bi+cj+dk)=a^2+b^2+c^2+d^2 \quad (a,b,c,d\in\mathbb{R}). \tag{5.4}$$

En particular $N(\alpha)\in\mathbb{R}$ para todo $\alpha\in\mathbb{H}(\mathbb{R})$ y $N(\alpha)=0$ si y solo si $\alpha=0$. Además

$$N(\alpha\beta)=\alpha\,\beta\,\overline{\alpha\,\beta}=\alpha\,\beta\,\overline{\beta}\,\overline{\alpha}=N(\alpha)\,N(\beta).$$

Usando (5.4) se tiene que la última fórmula es equivalente a la que aparece al final de la demostración del Teorema (5.9). Por otro lado, es fácil ver que todo elemento no nulo α de $\mathbb{H}(\mathbb{R})$ es invertible y

$$\alpha^{-1}=\frac{\overline{\alpha}}{N(\alpha)}.$$

5.3 Representación geométrica de números algebraicos

Sea K un cuerpo de números de grado n sobre $\mathbb{Q}$. Sea $\sigma : K\to\mathbb{C}$ un homomorfismo. Diremos que σ es *real* si $\sigma(K)\subseteq\mathbb{R}$. En caso contrario se dice que σ es *complejo*. El conjugado de σ es el homomorfismo $\overline{\sigma} : K\to\mathbb{C}$ definido por

$$\overline{\sigma}(x)=\overline{\sigma(x)}.$$

Si σ es complejo entonces $\overline{\sigma}$ es otro homomorfismo, los homomorfismos complejos $K\to\mathbb{C}$ van pareados luego

$$n=r+2s$$

donde r es el número de homomorfismos reales y $2s$ el de monomorfismos complejos.

Sean

$$\sigma_1,\ldots,\sigma_r,\sigma_{r+1},\overline{\sigma_{r+1}},\ldots,\sigma_{r+s},\overline{\sigma_{r+s}}$$

los homomorfismos de K en $\mathbb{C}$ de forma que los r primeros son los reales y los otros los complejos. Sea

$$L^{r,s}=\mathbb{R}^s\times\mathbb{C}^t$$

que es una álgebra real de dimensión $r+2s$. Además $L^{r,s}$ tiene una norma dada por

$$N(x_1,\ldots,x_n)=x_1\ldots x_2|x_{s+1}|^2\ldots|x_{r+s}|^2.$$

Claramente esta norma es real y multiplicativa.

Vamos a usar como base de referencia en $L^{r,s}$ la formada por todos los elementos que tengan un 1 en una coordenada y 0 en las demás y a todos los que tengan i en una de las últimas s coordenadas y 0 en las demás.

Juntamos todos los monomorfismos (sin repetir los conjugados) en una aplicación:

$$\sigma : K \to L^{r,s}.$$

Es decir,

$$\sigma(x) = (\sigma_1(x), \dots, \sigma_{r+s}(x))$$

que es un homomorfismo de $\mathbb{Q}$-álgebras. Además, σ conserva la norma, es decir:

$$N(\sigma(x)) = N_{K/\mathbb{Q}}(x)$$

donde la primera norma es la norma en $L^{r,s}$ y la segunda es la norma de K.

Como σ es un monomorfismo de $\mathbb{Q}$-espacios vectoriales, conserva la independencia lineal como $\mathbb{Q}$-espacios vectoriales. Es decir, si $\alpha_1, \dots, \alpha_n$ es una base de K sobre $\mathbb{Q}$ entonces $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ son linealmente independientes sobre $\mathbb{Q}$ y por tanto la matriz formada por las coordenadas de estos vectores en la base de referencia tiene determinante diferente de 0. Pero eso implica que también $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ son linealmente independientes sobre $\mathbb{R}$. Esto demuestra que $\sigma(R)$ es un retículo pleno de $L^{r,s}$. De hecho esto también demuestra que $\sigma(I)$ es un retículo pleno de $L^{r,s}$ para todo ideal no nulo I de R. En la siguiente proposición recopilamos esto y demos una fórmula para el covolumen de $\sigma(I)$ en $L^{r,s}$ que vamos a denotar $\mathrm{vol}(L^{r,s}/I)$ para simplificar la notación.

Proposición 5.10 *Si I es un ideal no nulo de R entonces $\sigma(I)$ es un retículo pleno de $L^{r,s}$ y* $\mathrm{vol}(L^{r,s}/I) = \frac{\sqrt{|\Delta(F)|}N(I)}{2^s}$.

Demostración. Aplicando el Lema 5.4 tenemos que $\mathrm{vol}(L^{r,s}/I) = N(I)\mathrm{vol}(L^{r,s}/R)$, con lo que basta demostrar el resultado para $I = R$. Sea $\alpha_1, \dots, \alpha_n$ una base entera de R. Pongamos

$$\sigma(\alpha_l) = (x_1^{(l)}, \dots, x_s^{(l)}, y_1^{(l)} + iz_1^{(l)}, \dots, y_s^{(l)} + iz_s^{(l)})$$

con $x_k^{(l)}, y_k^{(l)}, z_k^{(l)}$ reales. Consideremos los siguientes vectores columna para $k = 1, \dots, r$ y $j = 1, \dots, s$:

$$x_k = \begin{pmatrix} x_i^{(1)} \\ \vdots \\ x_i^{(n)} \end{pmatrix}, \quad y_j = \begin{pmatrix} y_i^{(1)} \\ \vdots \\ y_i^{(n)} \end{pmatrix}, \quad z_j = \begin{pmatrix} z_i^{(1)} \\ \vdots \\ z_i^{(n)} \end{pmatrix}, \quad v_j = y_j + iz_j, \quad \overline{v_j} = y_j - iz_j.$$

Por el Lema 5.4 sabemos que $\mathrm{vol}(L^{r,s}/R)$ es el valor absoluto del siguiente determinante:

$$D = \det(x_1, \dots, x_r, y_1, z_1, \dots, y_s, z_s).$$

Por otro lado

$$\begin{aligned} \Delta[\alpha_1, \dots, \alpha_n] &= \det(x_1, \dots, x_r, v_1, \overline{v_1}, \dots, v_s, \overline{v_s})^2 \\ &= \det(x_1, \dots, x_r, v_1, 2y_i, \dots, v_s, 2y_s)^2 \\ &= 2^s \det(x_1, \dots, x_r, z_1 i, y_1, \dots, z_s i, y_s)^2 = \pm 2^{2s} D^2 \end{aligned}$$

Tomando valores absolutos y raíces cuadradas concluimos que $2^s\mathrm{vol}(L^{r,s}/I) = 2^s|D| = \sqrt{|\Delta(F)|}$.

∎

5.4 Espacio logarítmico

Sea K un cuerpo de números de grado $n = r + 2s$, con r y s como en la sección anterior. Vamos a denotar por $U^{r,s}$ al grupo de unidades del anillo $L^{r,s}$, es decir

$$U^{r,s} = \{x = (x_1, \ldots, x_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s : x_i \neq 0 \text{ para todo } i = 1, \ldots, r+s\}.$$

Definimos la aplicación

$$l : U^{r,s} \to \mathbb{R}^{r+s}$$

poniendo

$$l(x) = (l_1(x), \ldots, l_{r+s}(x)) \quad \text{con} \quad l_k(x) = \begin{cases} \log|x_k|, & \text{si } k \leq s; \\ \log|x_k|^2, & \text{si } k > s. \end{cases}$$

Por las propiedades del logaritmo se tiene que

$$l(xy) = l(x) + l(y),$$

para todo $x, y \in U^{r,s}$, es decir l es un homomorfismo de $U^{r,s}$ al grupo aditivo de $\mathbb{R}^{r+s}$. De la definición de la norma en $L^{r,s}$ tenemos que

$$\log|N(x)| = \sum_{i=1}^{r+s} l_k(x) \quad (x \in U^{r,s}).$$

Recordemos que hemos definido la aplicación $\sigma : K \to L^{r,s}$ que es un monomorfismo de $\mathbb{Q}$-álgebras y que por tanto se restringe a un homomorfismo injectivo $\sigma : K^* \to U^{r,s}$ que compuesto con l proporciona un homomorfismo $K^* \to \mathbb{R}^{r+s}$ que también denotaremos con l, es decir

$$l(\alpha) = l(\sigma(\alpha)) \quad \text{y} \quad l_k(\alpha) = l_k(\sigma(\alpha)) \quad (\alpha \in K^*).$$

O sea

$$l(\alpha) = (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_r(\alpha)|, \log|\sigma_{r+1}(\alpha)|^2, \ldots, \log|\sigma_{r+s}(\alpha)|^2).$$

Nos referiremos a $\mathbb{R}^{r+s}$ como el **espacio logarítmico** y a $l : K^* \to \mathbb{R}^{r+s}$ como la **representación logarítmica** de K.

Por lo visto arriba, l es un homomorfismo de grupos $l : (K^*, \cdot) \to (\mathbb{R}^{r+s}, +)$ y, como la norma en $L^{r,s}$ es compatible con la norma en K también tenemos

$$\log|N_{K/\mathbb{Q}}(x)| = \log|N(\sigma(x))| = \sum_{i=1}^{r+s} l_k(\sigma(x)) \quad (x \in K^*).$$

Sean R el anillo de enteros de K y U el grupo de las unidades de R. Nuestro objetivo es describir la estructura de U. Para ello usamos la restricción de l a U que proporciona un homomorfismo de grupos $U \to \mathbb{R}^{r+s}$.

Lema 5.11 *$l(U)$ es un retículo dentro del hiperplano*

$$\pi = \{(x_1, \ldots, x_{r+s}) \in \mathbb{R}^{r+s} : x_1 + \cdots + x_{r+s} = 0\}.$$

Demostración. Sea $u \in U$. Entonces $N(u) = \pm 1$ y, por tanto,

$$\sum_{i=1}^{r+s} l_k(u) = \log |N(u)| = \log 1 = 0.$$

Luego los elementos de $l(U)$ pertenecen a π. Para probar que $l(U)$ es un retículo vemos que es discreto. Sea $r > 0$ y supongamos que $u \in U$ y $l(u) \in B(0;r)$. Entonces $|l_k(u)| \leq \|l(u)\| < r$, luego

$$\begin{array}{rl} |\sigma_i(u)| & < e^r \quad \text{si } k \leq s \\ |\sigma_i(u)|^2 & < e^r \quad \text{si } k > s. \end{array}$$

Luego $\|\sigma(u)\| < e^r\sqrt{r+s}$. O sea $\sigma^{-1}(l(U) \cap B(0;r))$ es un subconjunto acotado de $\sigma(R)$. Como $\sigma(R)$ es un retículo de $L^{r,s}$, deducimos que $\sigma^{-1}(l(U) \cap B(0;r))$ es finito. Como σ es inyectivo, $l(U) \cap B(0;r)$ también es finito. ∎

Para describir el núcleo de la restricción de l a U necesitamos el siguiente lema.

Lema 5.12 *Sea $P \in \mathbb{Z}[X]$ un polinomio mónico cuyas raíces tienen módulo ≤ 1. Entonces cada raíz de P es una raíz de la unidad.*

Demostración. Pongamos $P = \prod_{i=1}^{k}(X - \alpha_i)$, es decir las raíces de P son $\alpha_1, \ldots, \alpha_k$, repetidas tantas veces como su multiplicidad como raíz de P. Sea $F = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$, el cuerpo de descomposición de P sobre $\mathbb{Q}$ y sea R el anillo de enteros de F. Entonces $F/\mathbb{Q}$ es una extensión de Galois. Sean $S_1 = X_1 + \cdots + X_k, S_2 = \prod_{1 \leq i < j \leq k} X_i X_j, \ldots, \ldots, S_n = X_1 \ldots X_k$ los polinomios simétricos elementales en k variables. Sea m un entero positivo y para cada $i = 1, \ldots, n$ sea $a_i = S_i(\alpha_1^m, \ldots, \alpha_k^m)$ y sea

$$P_m = \prod_{i=1}^{k}(X - \alpha_i^m) = X^k + \sum_{i=1}^{k}(-1)^i a_i X^i.$$

Entonces $\sigma(a_i) = a_i$ para todo $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ y por tanto $a_i \in \mathbb{Q}$. Como cada α_i es entero, deducimos que $a_i \in \mathbb{Z}$ para todo i. Además

$$|a_i| \leq \binom{k}{i}$$

pues a_i es una suma de $\binom{k}{i}$ productos de α_j's y por hipótesis cada $|\alpha_j| \leq 1$. Como $(-1)^i a_i$ es el coeficiente de X^{k-i} en P_m, deducimos que $\{P_m : m \geq 1\}$ es un conjunto finito. Por tanto existen enteros positivos $m_1 \neq m_2$ tales que $P_{m_1} = P_{m_2}$. Como estos dos polinomios son iguales tienen las mismas raíces. Pero las raíces de P_m son $\alpha_1^m, \ldots, \alpha_k^m$. Por tanto existe un permutación π tal que

$$\alpha_i^{m_1} = \alpha_{\pi(i)}^{m_2}.$$

Por inducción sobre r podemos demostrar

$$\alpha_i^{m_1^r} = \alpha_{\pi^r(i)}^{m_2^r}$$

para todo i y, como $\pi^r = 1$, para algún r resulta que

$$\alpha_i^{m_1^r} = \alpha_i^{m_2^r},$$

o sea

$$\alpha_i^{m_1^r - m_2^r} = 1$$

y, por tanto, α_i es una raíz de la unidad. ∎

Ahora podemos describir el núcleo de l.

Lema 5.13 *El núcleo W de $l : U \to \mathbb{R}^{r+s}$ es el conjunto de las raíces de la unidad de F. Además W es un grupo cíclico finito de orden par.*

Demostración. Si α es una raíz de la unidad de F entonces $\alpha \in U$ y $l(u) = 0$ pues $|\sigma(u)| = 1$ para toda inclusión de F en $\mathbb{C}$. Luego $\alpha \in W$. Recíprocamente, sea $\alpha \in W$. Entonces $|\sigma_i(\alpha)| = 1$, para todo i. Luego las raíces del polinomio característico P de α tienen módulo 1. Por el Lema 5.12 esas raíces son raíces de la unidad y en particular α es una raíz de la unidad.

Por otro lado de (5.10) se deduce que $\sigma(R)$ es un retículo de $L^{r,s}$ y, por tanto, es discreto. Como $\sigma(W)$ está acotado y contenido en $\sigma(R)$ deducimos que $\sigma(W)$ es finito y como σ es inyectivo deducimos que W es finito. Pero todo subgrupo finito del subgrupo multiplicativo de un cuerpo es cíclico. Además, $-1 \in W$ y por tanto el orden de W es par. ∎

5.5 Teorema de las Unidades de Dirichlet

Como W es finito y U/W es isomorfo a $l(U)$ que es un retículo (en particular finitamente generado) en π, se tiene que U también es finitamente generado. Luego U es el producto directo de un grupo finito y un grupo abeliano libre de rango $\leq r + s - 1 = \dim_{\mathbb{R}}(\pi)$. El Teorema de Dirichlet asegura que el grupo abeliano libre tiene rango precisamente $r + s - 1$, para lo cual es suficiente probar que $l(U)$ tiene dicho rango, es decir que $l(U)$ es un retículo pleno del hiperplano π.

Para cada $y \in L^{r,s}$ sea $\lambda_y : L^{r,s} \to L^{r,s}$ la aplicación dada por $\lambda_y(x) = yx$. λ_y es una aplicación lineal. El siguiente lema calcula su determinante.

Lema 5.14 $\det \lambda_y = N(y)$.

Demostración. Supongamos que $y = (x_1, \ldots, x_r, y_1 + z_1 i, \ldots, y_s + z_s i)$. Entonces la matriz asociada a λ_y en la base de referencia es

$$\begin{pmatrix}
x_1 & 0 & \ldots & 0 & & & & \\
0 & x_2 & \ldots & 0 & & & & \\
\ldots & \ldots & \ldots & \ldots & \multicolumn{2}{c}{\mathbf{0}} & \ldots & 0 \\
0 & 0 & \ldots & x_s & & & & \\
\multicolumn{4}{c}{\multirow{2}{*}{$\mathbf{0}$}} & y_1 & -z_1 & \ldots & \mathbf{0} \\
\multicolumn{4}{c}{} & z_1 & y_1 & & \\
\multicolumn{4}{c}{\ldots} & \multicolumn{2}{c}{\ldots} & \ldots & \ldots \\
\multicolumn{4}{c}{\mathbf{0}} & \multicolumn{2}{c}{\mathbf{0}} & \ldots & \begin{matrix} y_s & -z_s \\ z_s & y_s \end{matrix}
\end{pmatrix}$$

cuyo determinante es

$$x_1 x_2 \dots x_s (y_1^2 + z_1^2) \dots (y_s^2 + z_s^2) = N_{K/\mathbb{Q}}(y)$$

∎

Necesitamos un lema más:

Lema 5.15 *Sea M un retículo pleno de $L^{r,s}$ de dimensión $r+2s$ y sean $c_1, \dots, c_{r+s} > 0$ tales que*

$$c_1 \dots c_{r+s} > \left(\frac{4}{\pi}\right)^s \mathrm{vol}(L^{r,s}/M)$$

entonces existe $0 \neq x = (x_1, \dots, x_{r+s}) \in M$ tal que

$$\begin{array}{rl} |x_i| & < c_i \quad si\ i \leq s \\ |x_i|^2 & < c_i \quad si\ i > s \end{array} \tag{5.5}$$

Demostración. Sea X el conjunto de los puntos de $L^{r,s}$ que satisfacen (5.5). Entonces X satisface las hipótesis del Teorema de Minkowski (Teorema 5.5). En efecto, la segunda condición es obvia y la primera se comprueba así:

$$\begin{aligned} v(X) &= \int_{-c_1}^{c_1} dx_1 \dots \int_{-c_r}^{c_r} dx_r \int\int_{y_1^2+z_1^2<c_1} dy_1 dz_1 \dots \int\int_{y_s^2+z_s^2<c_s} dy_s dz_s \\ &= 2c_1 \dots 2c_r \pi c_{r+1} \dots \pi c_{r+s} = 2^r \pi^s c_1 \dots c_{r+s} > 2^{r+2s} \mathrm{vol}(L^{r+s}/M). \end{aligned}$$

∎

Proposición 5.16 *La imagen $l(U)$ de U por la aplicación logarítmica l es un retículo de dimensión $r+s-1$.*

Demostración. Ya hemos visto que $l(U)$ es un retículo en el hiperplano π. Falta ver que es un retículo pleno y por el Lema 5.1 eso equivale a demostrar que existe un subconjunto acotado B de π tal que

$$\pi = \bigcup_{x \in l(U)} (x + B).$$

Obsérvese que $S = l^{-1}(\pi) = \{x \in L^{r,s} : |N(x)| = 1\}$.

Usando la aplicación logarítmica, la igualdad (aditiva) anterior se puede convertir en una igualdad (multiplicativa).

$$S = \bigcup_{u \in U} \sigma(u) C \tag{5.6}$$

donde C es un subconjunto acotado de $L^{r,s}$ (pues l transforma conjuntos acotados en conjuntos acotados). Vamos a buscar C acotado satisfaciendo (5.6).

Sean $M = \sigma(R)$ y sean $c_1, \ldots, c_{r+s}$ números reales positivos tales que

$$Q = c_1 \ldots c_{r+s} > \left(\frac{4}{\pi}\right)^s \mathrm{vol}(L^{r,s}/M).$$

Sea

$$X = \left\{ (x_1, \ldots, x_{r+s}) \in L^{r,s} : \begin{array}{ll} |x_i| & < c_i, \quad \text{si } i \leq r; \\ |x_i|^2 & < c_i, \quad \text{si } i > r \end{array} \right\}.$$

Por la Proposición 4.18 sólo un número finito de ideales tienen norma menor que Q. Como el valor absoluto de la norma de un elemento coincide con la norma del ideal que genera en R (Corolario 4.22), se tiene que existen $\alpha_1, \ldots, \alpha_k \in R$ tales que todo elemento de R que tenga norma en valor absoluto menor o igual que Q es asociado de algún α_i en R. Pongamos

$$C = S \cap \left(\bigcup_{i=1}^{k} \sigma(\alpha_i^{-1}) X \right).$$

Como X es acotado, también lo es C. Además, como $\sigma(u) \in S$, para todo $u \in U$, y S es un subgrupo multiplicativo de $U^{r,s}$ tenemos que

$$S \supseteq \bigcup_{u \in U} \sigma(u) C$$

Vamos a ver la otra inclusión. Sea $y \in S$. Por (5.1) y el Lema 5.14, $\mathrm{vol}(L^{r,s}/yM) = \mathrm{vol}(L^{r,s}/M)$. Luego, por el Lema 5.15 existe $0 \neq x \in X \cap yM$. Pongamos $x = y\sigma(\alpha)$ con $0 \neq \alpha \in R$. Entonces $Q > |N(x)| = |N_{K/\mathbb{Q}}(\alpha)|$. Luego $\alpha u = \alpha_i$ para algún i y algún $u \in U$. Entonces

$$y = x\sigma(\alpha_i^{-1})\sigma(u).$$

Pero, como $y\sigma(u)^{-1} \in S$, tenemos que $x\sigma(\alpha_i^{-1}) \in S$, luego $x\sigma(\alpha_i^{-1}) \in C$, por tanto $y \in \sigma(u)C$. ∎

Refinando un poco la proposición anterior obtenemos el Teorema de las Unidades de Dirichlet.

Teorema 5.17 *(Teorema de la Unidades de Dirichlet) El grupo de las unidades del anillo de enteros de un cuerpo de números K con r inclusiones reales y $2s$ inclusiones complejas es isomorfo a*

$$W \times \mathbb{Z}^{r+s-1}$$

donde W es el conjunto de las raíces de la unidad de K, que es un grupo cíclico finito de orden par.

Demostración. Por el Lema 5.13 y la Proposición 5.16, $U/W \simeq \mathbb{Z}^{r+s-1}$. Luego U es un grupo abeliano finitamente generado lo que implica que $U = T(U) \times (U/T(U))$ donde $T(U)$ es el subgrupo de torsión de U. Como W es finito y U/W es libre de torsión, deducimos que $W = T(U)$. ∎

Capítulo 6

El grupo de clase

6.1 El grupo de clase

En este capítulo K es un cuerpo de números y $R = \mathbb{A}_K$, el anillo de enteros de K.

Hemos visto en el Capítulo 3 que R es un DFU precisamente si es un DIP. El objetivo de este capítulo es medir como está de lejos R de ser un DIP. Para esto usamos el grupo $\mathcal{F}$ de los ideales fraccionales de R. Recordemos que los ideales fraccionales son los subconjuntos de K de la forma $c^{-1}I$ con $c \in R \setminus \{0\}$ e I un ideal no nulo de R y que forman un grupo abeliano con respecto al producto

$$M\ N = \left\{ \sum_{i=1}^{k} m_i n_i : m_i \in M, n_i \in N \right\}.$$

Diremos que un *ideal fraccional* es *principal* si es de la forma $c^{-1}I$ con $c \in R \setminus \{0\}$ e I un ideal principal no nulo de R, o equivalentemente de la forma αR con $\alpha \in K \setminus \{0\}$. Claramente el conjunto $\mathcal{P}$ de los ideales fraccionales principales es un subgrupo de F.

Definición 6.1 *El* grupo de clase *de R es el grupo cociente*

$$\mathcal{C}_K = \mathcal{F}/\mathcal{P}$$

del grupo $\mathcal{F}$ de los ideales fraccionales de K por el subgrupo $\mathcal{P}$ de los ideales fraccionales principales de K. El número de clase *de K es el orden $h = h(K)$ de $\mathcal{C}_K$.*

Claramente R es un DIP precisamente si $\mathcal{F} = \mathcal{P}$ o equivalentemente si $\mathcal{K} = 1$.

Diremos que dos *ideales fraccionales* I y J son *equivalentes* (y escribiremos $I \sim J$) si están en la misma clase módulo P, o sea si $I = J\alpha$ para algún $\alpha \in K \setminus \{0\}$. La clase de equivalencia de I por esta relación de equivalencia será denotada por $[I]$.

Si I es un ideal fraccional, entonces $I = c^{-1}J$ para algún $c \in R \setminus \{0\}$ y algún ideal no nulo J de R. Luego $J = cI$ y, por tanto $[I] = [J]$. O sea, toda clase contiene un ideal de R. Supongamos que I y J son dos ideales no nulos de R que son equivalentes. Eso implica que $I = \alpha J$ para algún $\alpha \in K \setminus \{0\}$. Como $\alpha = \frac{a}{b}$ con $a, b \in R \setminus \{0\}$, tenemos que $bI = aJ$.

Reciprocamente, si $bI = aJ$ con $a, b \in R\setminus\{0\}$ entonces $I \sim J$. Luego la relación de equivalencia anterior restringe a la siguiente relación de equivalencia en el conjunto de los ideales no nulos de R:

$$I \sim J \quad \Leftrightarrow \quad aI = bJ \text{ con } a, b \in R \setminus \{0\}.$$

6.2 Finitud del grupo de clase

En esta sección vamos a demostrar que el grupo de clase es finito y por tanto el número de clase es un número natural. Para ello primero vamos a ver que toda clase contiene un ideal cuya norma está acotada por cierto número

Teorema 6.2 *Sea K un cuerpo de números con grado n, discriminante Δ y s parejas de inclusiones complejas. Si I es un ideal no nulo de $\mathbb{A}_K$ entonces existe $\alpha \in I \setminus \{0\}$ tal que*

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} N(I)\sqrt{\Delta}.$$

Demostración. Sean $\sigma_1, \ldots, \sigma_r$ las inclusiones reales de K y $\sigma_{r+1}, \ldots, \sigma_{r+s}$ y sus conjugadas las inclusiones complejas de K. Empezamos demostrando que para cada número real positivo d que satisfaga

$$d^n > \left(\frac{4}{\pi}\right)^s n! N(I)\sqrt{\Delta} \tag{6.1}$$

existe $\alpha \in I \setminus \{0\}$ tal que $|\sigma_1(\alpha)| + \ldots + |\sigma_r(\alpha)| + 2|\sigma_{r+1}(\alpha)| + \ldots + 2|\sigma_{r+s}(\alpha)| < d$.

Para ello consideramos el conjunto

$$X_d = \{x = (x_1, \ldots, x_{r+s}) \in L^{r,s} : |x_1| + \ldots + |x_r| + 2|x_{r+1}| + \ldots + 2|x_{r+s}| < d\}.$$

Claramente X_d cumple la segunda hipótesis del Teorema de Minkowski (Teorema 5.5). Cambiando a coordenadas polares las parejas (y_i, z_i) y razonando por inducción se demuestra que el volumen de X_d es

$$\text{vol}(X_d) = 2^r \left(\frac{\pi}{2}\right)^s \frac{1}{n!} d^n.$$

Por el Teorema de Minkowski, X_d interseca a $\sigma(I)$ en un elemento no nulo si

$$\text{vol}(X_d) > 2^{r+2s}\text{vol}(L^{r,s}/\sigma(I)) \tag{6.2}$$

Por la Proposición 5.10, $\text{vol}(L^{r,s}/\sigma(I)) = \frac{N(I)\sqrt{\Delta}}{2^t}$. Luego la condición (6.2) es equivalente a

$$\left(\frac{\pi}{2}\right)^s \frac{1}{n!} d^n > 2^s N(I)\sqrt{\Delta}$$

que a su vez es equivalente a la hipótesis (6.1). Por tanto, del Teorema de Minkowski deducimos que I contiene un elemento α tal que $\sigma(\alpha) \in X_d$, o sea

$$|\sigma_1(\alpha)| + \ldots + |\sigma_s(\alpha)| + 2|\sigma_{s+1}(\alpha)| + \ldots + 2|\sigma_{r+s}(\alpha)| \leq d.$$

Esto es precisamente lo que queríamos demostrar.

Ahora fijamos $c \in \mathbb{R}^+$ tal que

$$c^n = \left(\frac{4}{\pi}\right)^s n! N(I)\sqrt{\Delta}.$$

Entonces los números de la forma $d = c + \epsilon$ con $\epsilon > 0$ satisfacen (6.1). Por tanto Entonces, para cada $\epsilon > 0$ existe $\alpha \in I \setminus \{0\}$ tal que $\sigma(\alpha) \in X_{c+\epsilon}$. Como $X_{c+\epsilon}$ es un conjunto acotado y $\sigma(I)$ es un retículo en $L^{r,s}$ el conjunto A_ϵ finito de elementos de esta forma. Además si $\epsilon' < \epsilon$ entonces $A_{\epsilon'} \subseteq A_\epsilon$ y por tanto $A = \cap_{\epsilon>0} A_\epsilon$ no es vacío. Eso implica que I tiene un elemento no nulo α tal que

$$|\sigma_1(\alpha)| + \ldots + |\sigma_s(\alpha)| + 2|\sigma_{s+1}(\alpha)| + \ldots + 2|\sigma_{r+s}(\alpha)| \leq c.$$

Recordando la desigualdad

$$(a_1 \ldots a_n)^{1/n} \leq \frac{a_1 + \ldots + a_n}{n},$$

obtenemos que

$$\begin{aligned} |N_{K/\mathbb{Q}}(\alpha)| &= |\sigma_1(\alpha)\ldots\sigma_s(\alpha)\sigma_{s+1}(\alpha)^2\ldots\sigma_{r+s}(\alpha)^2| \\ &\leq \left(\frac{|\sigma_1(\alpha)| + \ldots + |\sigma_s(\alpha)| + 2|\sigma_{s+1}(\alpha)| + \ldots + 2|\sigma_{r+s}(\alpha)|}{n}\right)^n \\ &\leq \left(\frac{c}{n}\right)^n = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} N(I)\sqrt{\Delta}, \end{aligned}$$

como deseábamos. ∎

El Teorema 6.2 sugiere introducir las conocidas como *constantes de Minkowski*:

$$M_{rs} = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}, \quad \text{con } n = r + 2s.$$

Teorema 6.3 *Sea K un cuerpo de números con discriminante Δ, r inclusiones reales y s parejas de inclusiones complejas. Entonces todo ideal no nulo de $\mathbb{A}_K$ es equivalente a un ideal con norma menor o igual que $M_{r,s}\sqrt{\Delta}$.*

Demostración. Sea I un ideal no nulo de R. Sabemos que I^{-1} es equivalente a un ideal no nulo J de R. Luego $IJ \sim R$. Por el Teorema 6.2 existe $\alpha \in J \setminus \{0\}$ tal que

$$|N_{K/\mathbb{Q}}(\alpha)| \leq M_{r,s} N(J)\sqrt{\Delta}.$$

Como $I|R\alpha$, existe un ideal M de R tal que

$$R\alpha = JM.$$

Luego $N(J)N(M) = N(JM) = N(R\alpha) = |N_{K/\mathbb{Q}}(\alpha)|$ y, por tanto

$$N(M) = \frac{|N_{K/\mathbb{Q}}(\alpha)|}{N(J)} \leq M_{r,s}\sqrt{\Delta}.$$

Finalmente, $J \sim I^{-1}$ y $M \sim J^{-1}$, luego $I \sim M$. ∎

Como cada clase contiene un ideal no nulo de norma $M_{r,s}\sqrt{\Delta}$ y sólo hay un número finito de ideales no nulos con norma menor o igual que un cierto número, se deduce el siguiente.

Corolario 6.4 *El grupo de clase de un cuerpo de números es finito.*

Acabamos esta sección con algunas consecuencias inmediatas de la finitud del grupo de clase.

Corolario 6.5 *Sea I un ideal del anillo de enteros de un cuerpo numérico y sea h el número de clase de dicho cuerpo. Entonces*

(1) I^h es principal.

(2) Si k es coprimo con h e I^k es principal, entonces a es principal.

Ahora podemos dar un criterio de cuando un cuerpo numerico tiene número de clase 1 y, por tanto su anillo de enteros es un DFU.

Corolario 6.6 *Sean K, Δ, r y s como en el Teorema 6.3. Supongamos que todo ideal maximal de $\mathbb{A}_K$ que contenga un primo racional $p \leq M_{rs}\sqrt{\Delta}$ es principal, entonces el número de clase de K es 1, o sea $\mathbb{A}_K$ es un DIP.*

Demostración. Cada clase de ideales fraccionales contiene un ideal no nulo I con $N(I) \leq M_{rs}\sqrt{\Delta}$. Entonces cada ideal maximal Q de $\mathbb{A}_K$ que divida a I divide a $N(I)$ y por tanto contiene un primo racional p que divide a $N(I)$. Por la hipótesis Q es principal. Como esto pasa para todos los ideales que dividan a I, tenemos que I es producto de ideales principales y por tanto es principal, o sea $I \in \mathcal{P}$. Por tanto $\mathcal{F} = \mathcal{P}$, o sea el número de clases de K es 1. ∎

6.3 Cálculo de números de clase

Vamos a dedicar la última sección de este capítulo a calcular algunos números de clase. En particular vamos a demostrar el siguiente Teorema

Teorema 6.7 *El número de clase de $\mathbb{Q}(\sqrt{d})$ es 1 para $d = -1$, -2, -3, -7, -11, -19, -43, -67 y -163.*

Demostración. Por el Teorema 3.6 sólo tenemos que considerar los cuatro últimos casos. El anillo de enteros de $K = \mathbb{Q}(\sqrt{-19})$ es $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. El polinomio mínimo de $\theta = \frac{1+\sqrt{-19}}{2}$ es $f = X^2 - X + 5$. Por otro lado el discriminante de K es 19. Luego $M_{rs}\sqrt{\Delta} \leq 0.637\sqrt{19} < 3$. Luego basta con comprobar que se verifican las condiciones del Corolario 6.6 para $p = 2$, es decir tenemos que calcular la descomposición de 2 en R. Para eso utilizamos el Teorema 4.26. Tenemos que factorizar f en $\mathbb{Z}_2$. Pero este polinomio es irreducible en $\mathbb{Z}_2$. Del Teorema 4.26

se deduce que el único ideal maximal de R que divide a 2 es (2) y se puede aplicar el corolario 6.6.

Para $d = -43$ el polinomio mínimo es $f = X^2 - X + 11$ y $M_{rs} \leq 0.637\sqrt{43} < 4$, luego hay que considerar $p = 2, 3$. Como en el caso anterior se ve que (2) y (3) son primos pues $f_2 = X^2 + X + 1$ y $f_3 = X^2 - X - 1$ son irreducibles en $\mathbb{Z}_2[X]$ y $\mathbb{Z}_3[X]$ respectivamente.

Consideremos ahora $d = -67$. Entonces $f = X^2 - X + 17$ y $M_{rs} \leq 0.637\sqrt{67} < 6$. Ahora hay que considerar $p = 2, 3, 5$. En todos los cases f es irreducible módulo p y, por tanto, (2), (3) y (5) son irreducibles.

Finalmente para $d = -163$, $f = X^2 - X + 41$ y $M_{rs}\sqrt{\Delta}) \leq 0.637\sqrt{163} < 9$. Ahora hay que considerar $p = 2, 3, 5, 7$ y sale lo mismo. ∎

Recuérdese que si Q es un primo de K entonces $N(Q)$ es una potencia de p donde p es el único primo racional en Q. Como cada clase contiene un ideal con $N(I) \leq M_{rs}\sqrt{\Delta}$ si $I = Q_1^{e_1} \cdots Q_g^{e_g}$ es la factorización de I entonces $N(Q_1)^{e_1} \cdots N(Q_g)^{e_g} = N(I) \leq M_{rs}\sqrt{\Delta}$. Por tanto las normas de los Q_i son menores o iguales que M_{rs} y en particular los Q_i son primos que aparecen en las factorizaciones de $p\mathbb{A}_K$ para primos racionales a lo sumo $M_{rs}\sqrt{\Delta}$. Por tanto para calcular el grupo de clases podemos empezar calculando dichas factorizaciones. O sea si $p_1, \ldots, p_k$ son los primos menores que $M_{rs}\sqrt{\Delta}$ y $p_i\mathbb{A}_K = Q_{i,1}^{e_{1,1}} \ldots Q_{i,g_i}^{e_{i,g_i}}$ es la correspondiente factorización solo tenemos que considerar ideales de la forma $I = \prod_{i=1}^{k} \prod_{j=1}^{g_i} Q_{i,j}^{k_{i,j}}$. Pero además si $N(Q_{i,j}) = p_i^{\alpha_{i,j}}$ entonces $N(I) = \prod_{i=1}^{k} p_i^{\sum_{j=1}^{g_i} k_i \alpha_{i,j}}$ con que los k_i hay que elegirlos para que este número sea menor que $M_{r,s}\sqrt{\Delta}$.

Vamos a aplicar estas ideas para calcular número de clase de los primeros cuerpos ciclotómicos.

Teorema 6.8 *El número de clase del cuerpo ciclotómico $\mathbb{Q}(\zeta_p)$ es 1 para $p = 3, 5, 7$.*

Demostración. $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ que ya sabemos que es euclídeo.

El grado de $\mathbb{Q}(\zeta_5)$ es 4, el número de inclusiones reales es $r = 0$ y el de inclusiones complejas es $2s = 4$. Por último el discriminante es $\Delta = 5^3 = 125$. Luego $M_{rs} \leq 0.152\sqrt{125} < 2$. No hay que hacer ninguna comprobación.

Pongamos $\zeta = \zeta_7$. En este caso, tenemos $n = 6$, $r = 0$, $s = 3$ y $\Delta = -7^5$. Luego $M_{rs}\sqrt{\Delta} \leq 0.032\sqrt{16807} < 5$. Luego tenemos que considerar los primos $p = 2, 3$. El polinomio mínimo es $X^6 + \ldots + 1$. En $\mathbb{Z}_2$ podemos factorizarlo como $(X^3 + X^2 + 1)(X^3 + X + 1)$, luego $(2) = P_1P_2$, donde P_1 y P_2 son dos ideales maximales distintos. Por otro lado

$$2 = \zeta^4(\zeta^3 + \zeta^2 + 1)(\zeta^3 + \zeta + 1)$$

Luego

$$R(\zeta^3 + \zeta^2 + 1)\ R(\zeta^3 + \zeta + 1) = 2R$$

y, por tanto, $P_1 = R(\zeta^3 + \zeta^2 + 1)$ y $P_2 = R(\zeta^3 + \zeta + 1)$, o viceversa, que son principales. ∎

Acabamos con un ejemplo con número de clase 2.

Ejemplo 6.9 *El número de clases de $\mathbb{Q}(\sqrt{10})$ es 2.*

Demostración. Sea $K = \mathbb{Q}(\sqrt{10})$. Con la notación habitual tenemos $\Delta = 40$, $n = 2$, $r = 2$, $s = 0$. Entonces cada clase de ideales fraccionales contiene un ideal no nulo con norma

$$\leq M_{2,0}\sqrt{|\Delta|} \leq 0.5\sqrt{40} < 4.$$

Luego sólo hay que considerar factorizaciones de 2 y 3 y de hecho todo ideal que no esté en $\mathcal{P}$ ha de ser equivalente a uno de los primos que aparezcan en dichas factorizaciones. El anillo de enteros es $R = \mathbb{Z}[\theta]$, siendo $\theta = \sqrt{10}$. El polinomio mínimo es $f = X^2 - 10$. Entonces $f \equiv (X-1)(X+1) \mod 3$. De forma que (3) es producto de dos ideales maximales distintos $P_1 = (3, 1+\sqrt{10})$ y $P_2 = (3, 1-\sqrt{10})$. Por tanto todo ideal es equivalente a uno de los siguientes cuatro: R, P, P_1 ó P_2.

Por otro lado $f \equiv X^2 \mod 2$, luego $2R = P^2$ para un ideal maximal P. Si $P = (a+b\sqrt{10})$ fuera principal, entonces $N(P)^2 = |N_{K/\mathbb{Q}}(2)| = 4$, luego $N(P) = 2$, o sea $a^2 - 10b^2 = \pm 2$. Luego $a^2 \equiv \pm 2 \mod 5$ lo cual es imposible. Luego P no es principal, o sea R y P no son equivalentes.

Por otro lado, como $RN(-2+\sqrt{10}) = -6R = P^2P_1P_2$, P, P_1 y P_2 son los únicos posibles divisores de $(-2+\sqrt{10})$. Pero ni $P^2 = 2R$ ni P_2 dividen a $R(-2+\sqrt{10})$, luego $R(-2+\sqrt{10}) = PP_1$, lo que implica que $P = P_1^{-1} = P_2$ y $P_1 = P_2^{-1} = P^{-1} = P$. Entonces cada ideal no nulo está en la clase de R o de P. Como P no es principal estas dos clases son distintas, luego el número de clase de R es 2. ∎

Capítulo 7

El Último Teorema de Fermat

7.1 Consideraciones elementales

Como es bien conocido el Último Teorema de Fermat afirma que la ecuación diofántica

$$x^n + y^n = z^n \tag{7.1}$$

no tiene soluciones no triviales, si $n \geq 3$. O sea si x, y y z son enteros diferentes de cero y n es un entero mayor que 2 entonces la igualdad (7.1) no se verifica. Vamos a hablar un poco de la historia de este famoso teorema.

Alrededor del año 250 antes de Cristo, Diofantus de Alejandría escribió un tratado sobre ecuaciones polinómicas titulado *Aritmética*. Durante la Edad Media los conocimientos de matemáticas permanecieron ignorados salvo en pequeños guetos como la Escuela de Constantinopla. Cuando las tropas turcas conquistaron Constantinopla en 1453 esta escuela también desapareció. En 1462 apareció una copia del libro de Diofantus en la Biblioteca del Vaticano, probablemente superviviente del incendio de la Biblioteca de Alejandría. En 1621 se publicó una versión griega del libro con una tradución al latín. Esto hizo muy popular el libro a partir de ese momento. Fermat (1601-1665), que era un jurista aficionado a las matemáticas estudió la Aritmética de Diofantus profundamente. En el margen de su copía apareció la siguiente anotación:

> Resolver un cubo en suma de dos cubos, una potencia cuarta en suma de potencias cuartas, o en general cualquier potencia superior a la segunda en dos del mismo tipo, es imposible; de este hecho he encontrado una demostración fascinante. El margen de este libro es demasiado pequeño para contenerla.

La demostración que Fermat aseguraba haber encontrado, nunca apareció salvo para $n = 4$, con lo cual el Último Teorema de Fermat paso a ser una conjetura, posiblemente la más famosa de la historia de las matemáticas. Años mas tarde Euler demostró independientemente los casos $n = 3$ y $n = 4$. En 1828 (doscientos años después de la afirmación de Fermat), Dirichlet consiguió demostrar la afirmación para $n = 5$ en 1828 (e independientemente Legendre dos años mas tarde) y para $n = 14$ en 1832. Mientras tanto, el caso $n = 7$ se atragantó durante

algunos años. Gauss proporcionó algunas ideas pero no consiguió resolverlo. Lamé ofreció una demostración en 1838 para $n = 7$, pero Lebesgue descubrió un error en ella y consiguió dar una demostración correcta. Hasta ese momento todos los intentos de dar una demostración general habían fallado. Por un momento pareció que Lamé había conseguido dar una demostración general. Sin embargo, la demostración de Lamé suponía factorización única en $\mathbb{Z}[\zeta_n]$, lo cual fué puntualizado por Liuoville y Kummer. Cauchy pareció resolver la pega de la demostración de Lamé cuando en 1897 demostró (hecho que sabemos que es falso) factorización única en $\mathbb{Z}[\zeta_n]$. Finalmente Cauchy admitió que su demostración fallaba para el caso $n = 23$. Kummer acabó con el espejismo de la demostración de Lamé cuando probó que $\mathbb{Z}[\zeta_{23}]$ no tiene factorización única. En 1850 Kummer consiguió dar un tremendo empujón a la resolución del problema cuando consiguió demostrar el Último Teorema de Fermat para los primos regulares, que serán introducidos en este capítulo. Eso incluye todos los primos menores que 100, excepto 37, 59 y 67. Kummer también presento demostraciones para estos tres casos pero contenían errores que permanecieron ocultos hasta que Vandiver los desveló en 1920. Al menos el caso $n = 37$ había sido resuelto por Mirimanoff en 1893 quien además consiguió en 1905 dar una demostración para todos los valores de $n \leq 257$. Con los métodos de Vandiver y el uso de computadoras se consiguió demostrar el Teorema de Fermat para todos los exponentes $n \leq 120.000$.

Por otro lado hubo quién se concentró en casos particulares. Entre estos hay que citar a Legendre, Wiefrich, Mirimanoff, Frobenius, Vandiver, Pollackzed, Morishima, Rosser y más recientemente Lehmers, Brillhart, Tonascia y Weinberger. En 1979 se sabía que si existía un contraejemplo, x debía tener al menos 18×10^5 dígitos.

Un avance importante fué debido a Gerd Faltings en 1983 que demostró que si el Último Teorema de Fermat fallaba para n, al menos sólo había un número finito de soluciones para x, y y z. En realidad el resultado de Faltings es un caso particular de un teorema más general para ecuaciones homogéneas.

En 1994, durante la celebración de un congreso y al final de tres charlas Wiles anunció una demostración definitiva. Por unos meses pareció resuelto el problema, pero pronto se descubrió que Wiles había supuesto que cierto resultado, que alguién le había comentado, había sido demostrado, cuando solo era el tema de trabajo de otro matemático. Por tanto la demostración de Wiles quedó en suspenso. Finalmente, Taylor y Wiles consiguieron superar los obstáculos que quedaban y en 1975 se publicó una demostración que es aceptada como correcta. Los métodos de esta demostración superan con creces el ámbito de este curso. Nosotros nos limitaremos a ver la demostración de Kummer para primos regulares. Las posteriores están fuera de nuestras posibilidades.

Vamos ahora a hacer algunas consideraciones elementales. Obsérvese que si hay una solución de la ecuación (7.1) entonces hay alguna solución en la que x, y y z son primos entre si dos a dos. En efecto, si $x = qx_1$, $y = qy_1$ con q primo, entonces

$$q^n(x_1^n + y_1^n) = z^n.$$

Luego q divide a z. Si $z = qz_1$, entonces

$$q^n(x_1^n + y_1^n) = q^n z_1^n$$

lo que implica que x_1, y_1, z_1 es una solución y, ahora podemos razonar por inducción en el número de factores que aparece en la descomposición del máximo común múltiplo de x e y.

Por otro lado, si hay una solución para un cierto n, también hay una solución para cada divisor de n pues si $n = kl$, entonces la ecuación original es equivalente a

$$(x^k)^l + (y^k)^l = (z^k)^l.$$

Como todo número ≥ 3 es o múltiplo de 4 o múltiplo de un primo impar, teniendo en cuenta el párrafo anterior, para probar el Teorema podemos suponer que n es primo o 4. Que la Ecuación de Fermat no tenía solución no trivial para $n = 4$ es consecuencia inmediata del Teorema 3.9. Por tanto, para demostrar el Último Teorema de Fermat basta considerar el caso en el que el exponente es primo impar. El caso $n = 3$ ya lo vimos en el Corolario 3.17.

7.2 Teorema de Kummer

Ahora nos vamos a concentrar en revisar las aportaciones de Kummer al Último Teorema de Fermat.

En esta sección $K = \mathbb{Q}(\zeta)$ y $R = \mathbb{Z}[\zeta]$ donde $\zeta = \zeta_p$ con p primo impar. Pondremos

$$\lambda = 1 - \zeta \quad \text{e} \quad P = (\lambda)$$

el ideal generado por λ en R. Los conjugados de ζ son los elementos de la forma ζ^k con $1 \leq k < p$ y por tanto los conjugados de λ son los de la forma $1 - \zeta^k$ con $1 \leq k < p$. Todos son asociados en R pues como k es coprimo con p existe un entero l tal que $kl \equiv 1 \mod p$ y por tanto

$$u_k = \frac{1-\zeta^k}{\lambda} = 1+\zeta+\cdots+\zeta^{k-1} \in R \quad \text{y} \quad u_k^{-1} = \frac{\lambda}{1-\zeta^k} = \frac{1-\zeta^{kl}}{1-\zeta^k} = 1+\zeta^k+\cdots+\zeta^{k(l-1)} \in R,$$

es decir $1 - \zeta^k = u_k\lambda$ con u_k unidad de R. Además del Corolario 2.35 tenemos

$$N(P) = p = \prod_{k=1}^{p-1}(1-\zeta^k) = N_{K/\mathbb{Q}}(\lambda) \quad \text{y} \quad P^{p-1} = \prod_{k=1}^{p-1}(1-\zeta^k) = (p). \tag{7.2}$$

Obsérvese que de (7.2) se deduce que R/P tiene p elementos y, como $j \notin P$, para todo $1 \leq j \leq p-1$, resulta que todo elemento de R es congruente con un $0 \leq j \leq p-1$. En particular dos enteros racionales son congruentes módulo P precisamente si son congruentes módulo p. Además se verifica lo siguiente:

Lema 7.1 *Para cada $\alpha \in R$, existe $a \in \mathbb{Z}$ tal que $\alpha^p - a^p \in P^p$.*

Demostración. Sabemos que existe $a \in \mathbb{Z}$ tal que $\alpha - a \in P$. Sea $1 \leq i \leq p-1$. Entonces $1 - \zeta^i \in P$ y por tanto $\alpha \equiv a \equiv \zeta^i a \mod P$. Usando la factorización $X^p - 1 = \prod_{i=0}^{p-1}(X - \zeta^i)$ deducimos que

$$\alpha^p - a^p = a^p\left(\left(\frac{\alpha}{a}\right)^p - 1\right) = a^p\prod_{i=0}^{p-1}\left(\frac{\alpha}{a} - \zeta^i\right) = \prod_{j=0}^{p-1}(\alpha - \zeta^j a) \in P^p.$$

∎

Por el Corolario 2.34.(2) se tiene

Lema 7.2 *Las raíces de la unidad de K son los elementos de la forma $\pm\zeta^s$ para $0 \leq k < p$.*

El siguiente resultado es conocido como Lema de Kummer.

Lema 7.3 *Si ζ es una raíz p-ésima primitiva de la unidad con p un primo racional impar entonces toda unidad de $R = \mathbb{Z}[\zeta]$ es de la forma $r\zeta^u$ con $r \in \mathbb{R}$ y $0 \leq u < p$.*

Demostración. Sea ϵ una unidad de $\mathbb{Z}[\zeta]$ y sea $f \in \mathbb{Z}[X]$ tal que $\epsilon = f(\zeta)$. Los conjugados de ϵ son los siguientes números complejos:

$$\epsilon_s = f(\zeta^s) \quad \text{con} \quad 1 \leq s < p.$$

Luego $1 = \pm N(\epsilon) = \pm\epsilon_1 \dots \epsilon_{p-1}$ y, por tanto, cada ϵ es también una unidad de R. Además

$$\epsilon_{p-s} = f(\epsilon^{p-s}) = f(\zeta^{-s}) = f(\overline{\zeta^s}) = \overline{f(\zeta^s)} = \overline{\epsilon_s}.$$

Luego $\epsilon_s\epsilon_{p-s} = |\epsilon_s|^2 > 0$, y por tanto

$$\pm 1 = N(\epsilon) = (\epsilon_1\epsilon_{p-1})(\epsilon_2\epsilon_{p-2}) \dots (\epsilon_{\frac{p-1}{2}}\epsilon_{\frac{p-1}{2}}) > 0.$$

Luego $N(\epsilon) = 1$.

Vamos a ver que los coeficientes del polinomio

$$Q(X) = \prod_{s=1}^{p-1} \left(X - \frac{\epsilon_s}{\epsilon_{p-s}} \right)$$

son enteros. Estos coeficientes son de la forma

$$S\left(\frac{\epsilon_1}{\epsilon_{p-1}}, \dots, \frac{\epsilon_{p-1}}{\epsilon_1} \right)$$

donde S es un polinomio simétrico. Si σ es un automorfismo de K entonces $\sigma(\zeta) = \zeta^i$ para algún $1 \leq i < p$ y $\sigma(\epsilon_j) = \epsilon_k$ con k el resto de dividir ij entre p. Eso implica que $\sigma\left(\frac{\epsilon_j}{\epsilon_{p-j}}\right) = \frac{\epsilon_k}{\epsilon_{p-k}}$. Por tanto σ permuta los $\frac{\epsilon_s}{\epsilon_{p-s}}$. Esto demuestra que todos los automorfismos de K dejan fijo cada uno de los coeficientes de $Q(X)$ y, como $K/\mathbb{Q}$ es una extensión de Galois, dichos coeficientes pertenecen a $\mathbb{Q} \cap R = \mathbb{Z}$.

Por otro lado, $\epsilon_s/\epsilon_{p-s}$ es una unidad de módulo 1. Del Lema 5.12 deducimos que $\epsilon_s/\epsilon_{p-s}$ es una raíz de la unidad, para cada s. Aplicando el Lema 7.2 tenemos que $\epsilon = \pm\epsilon_{p-1}\zeta^k$ para algún entero k. Como p es impar, bien k ó $k + p$ es par, luego podemos suponer que k es par. Pongamos $k = 2u$. Sea $v \in \mathbb{Z}$ tal que

$$\zeta^{-u}\epsilon \equiv v \mod P.$$

Tomando conjugados tenemos $\zeta^u\epsilon_{p-1} \equiv v \mod (\bar{\lambda})$. Pero como $\bar{\lambda} = 1 - \lambda^{p-1}$ es asociado de λ en R, tenemos

$$\zeta^u\epsilon_{p-1} \equiv v \mod P.$$

Luego $\zeta^{-u}\epsilon \equiv \zeta^u \epsilon_{p-1} \mod P$. Multiplicando por ζ^u tenemos

$$\pm\zeta^{2u}\epsilon_{p-1} = \epsilon \equiv \zeta^{2u}\epsilon_{p-1} \mod P.$$

Como P es un ideal primo y $\zeta^{2u}\epsilon_{p-1}$ es una unidad en R deducimos que si el signo es negativo entonces $2 \in P \cap \mathbb{Z} = p\mathbb{Z}$, en contra de que p es primo impar. Luego el signo es positivo con lo que $r = \zeta^{-u}\epsilon = \zeta^u\epsilon_{p-1} = \bar{r}$. Luego $r \in \mathbb{R}$. ∎

Definición 7.4 *Un entero racional primo p se dice que es* regular *si no divide al número de clases de $\mathbb{Q}(\zeta_p)$.*

Por el Teorema 6.8, el 3, 5 y 7 son regulares y de hecho una gran cantidad de primos son regulares, como veremos en la siguiente sección. El resultado fundamental de Kummer dice que el Teorema de Fermat se verifica para exponentes primos regulares. Para su demostración necesitaremos el siguiente lema de Kummer. Por desgracia la demostración de este lema requiere técnicas de Teoría Analítica de Números que supera los contenidos de estas notas. Se puede ver en [Borevich-Shafarevich, Number Theory, página 377].

Lema 7.5 *(Kummer) Sea p un primo regular impar y u una unidad de $R = \mathbb{Z}[\zeta_p]$. Si u es congruente a un entero racional módulo p, entonces $u = u_0^p$ para alguna unidad u_0 de R.*

Obsérvese que el lema anterior no se verifica para $p = 2$ pues 2 es un primo regular ya que el número de clases de $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ es 1 y -1 es una unidad de orden 2 que no es un cuadrado en $\mathbb{Z} = \mathbb{A}_{\mathbb{Q}}$.

Teorema 7.6 *(Kummer) Si p es un primo regular impar entonces la ecuación difofántica*

$$x^p + y^p = z^p$$

no tiene soluciones no triviales.

Demostración. La ecuación se puede reescribir como

$$\prod_{i=1}^{p-1}(x - \zeta^i y) = z^p \tag{7.3}$$

que implica la siguiente ecuación de ideales

$$\prod_{i=1}^{p-1}(x - \zeta^i y) = (z)^p \tag{7.4}$$

Supondremos que (x, y, z) es una solución. Sin perdida de generalidad podemos suponer que x, y y z son coprimos dos a dos.

Caso 1: Primero vamos a suponer que $p \nmid xyz$.
Entonces los ideales $(x - \zeta^i y)$ son coprimos dos a dos. En efecto, sea Q un ideal primo que divide a $(x - \zeta^i y)$ y $(x - \zeta^j y)$, con $0 \leq i < j \leq p - 1$. Entonces

$$(x - \zeta^i) - (x - \zeta^j y) = -y\zeta^i(1 - \zeta^{j-i}) \in Q.$$

Como $(1 - \zeta^{j-i})$ es asociado de $\lambda = 1 - \zeta$ y ζ^i es unidad, resulta que $y\lambda \in Q$. Luego, $y \in Q$ ó $\lambda \in Q$. Vamos a ver que el primer caso no se puede dar. De la ecuación 7.3 se tiene que Q divide a (z), o sea $z \in Q$. Como y y z son coprimos, $1 \in (y) + (z) \subseteq Q$, contradiciendo que Q es primo. Luego $\lambda \in Q$. O sea Q divide a $P = (\lambda)$ pero como P es primo necesariamente $Q = P$. Luego $p = N(P) \mid N(z) = z^{p-1}$ y, por tanto p divide a z, en contra de la hipótesis.

Ahora aplicamos la unicidad en la factorización de ideales para deducir que $(x - \zeta^i y)$ es una potencia n-ésima de un ideal, para todo i. En particular

$$(x - \zeta y) = I^p$$

para algún ideal I de $\mathbb{Z}[\zeta]$. Como p es regular, p no divide al número de clases y, por tanto no divide al orden de la clase que contiene a I. Como I^p es principal, entonces I es principal. Pongamos $I = (\delta)$. Entonces $x - \zeta y = u\delta^p$, donde u es una unidad de $\mathbb{Z}[\zeta]$. Del Lema 7.3 $u = r\zeta^i$ para algún real r y algún entero i. Del Lema 7.1 sabemos que existe un entero $k \in \mathbb{Z}$ tal

$$\delta^p \equiv k \mod P^p.$$

Luego

$$x - \zeta y \equiv rk\zeta^i \mod P^p.$$

Pero, de (7.2) tenemos que $(p) = P^{p-1} \mid P^p$ y, por tanto

$$x - \zeta y \equiv rk\zeta^i \mod (p)$$

lo que implica

$$\zeta^{-i}(x - \zeta y) \equiv rk \mod (p).$$

Tomando conjugados tenemos

$$\zeta^i(x - \zeta^{-1} y) \equiv rk \mod (p).$$

Restando las dos ecuaciones anteriores tenemos

$$x\zeta^{-i} - y\zeta^{1-i} - x\zeta^i + y\zeta^{i-1} \equiv 0 \mod (p). \tag{7.5}$$

Pongamos

$$x\zeta^{-i} - y\zeta^{1-i} - x\zeta^i + y\zeta^{i-1} = \alpha p$$

con $\alpha \in \mathbb{Z}[\zeta]$. Entonces

$$\alpha = \frac{x}{p}\zeta^{-i} - \frac{y}{p}\zeta^{1-i} - \frac{x}{p}\zeta^i + \frac{y}{p}\zeta^{i-1}.$$

Como $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ son linealmente independientes, si no hay dos de los exponentes (o sea $i, 1 - i, i - 1, -i$) que sean congruentes módulo p, entonces los coeficientes de α en está base

son los que aparecen, o sea, dos de los coeficientes son $\frac{x}{p}$ y $\frac{y}{p}$ que no son enteros. Eso nos llevaría a una contradicción. O sea, al menos dos de los siguientes números $i, 1-i, i-1, -i$ son congruentes módulo p. Como $p \neq 2$, eso implica que se verifica una de las tres siguientes condiciones: $p \mid i$, $p \mid 1-i$ ó $2i \equiv 1 \mod p$.

Vamos a derivar una contradicción de una de estas tres posibilidades. Obsérvese que $1+\zeta$ es una unidad de $\mathbb{Z}[\zeta]$ pues

$$(X-\zeta)(X-\zeta^2)\dots(X-\zeta^{p-1}) = \frac{X^p-1}{X-1}.$$

Luego evaluando en $X=-1$ tenemos

$$-(1+\zeta)(-1-\zeta^2)\dots(-1-\zeta^{p-1}) = 1.$$

Consideremos el primer caso $p \mid i$. Entonces los términos con x en (7.5) se anulan y queda la ecuación

$$y(\zeta-\zeta^{-1}) \equiv 0 \mod (p).$$

Multiplicando por ζ, que es una unidad, resulta

$$y(1+\zeta)(1-\zeta) \equiv 0 \mod (p)$$

y, como $1+\zeta$ es una unidad

$$y\lambda \in (p) = P^{p-1}.$$

Como $p \geq 2$, resulta que $\lambda \mid y$. Tomando normas resulta que $p \mid y$ en contra de la hipótesis. Luego $i \not\equiv 0 \mod p$.

El mismo argumento demuestra que p no divide a $1-i$ y sólo nos queda el caso $2i \equiv 1 \mod p$, lo que implica que $\zeta^{2i} = \zeta$. Multiplicando por ζ^i tenemos

$$\alpha p\zeta^i = x + y\zeta - x\zeta^{2i} - y\zeta^{2i-1} = (x-y)\lambda.$$

Tomando normas se obtiene que $p \mid (x-y)$, luego

$$x \equiv y \mod (p).$$

Aplicando lo demostrado con la igualdad $y^p + (-z)^p = (-x)^p$ tendríamos también

$$y \equiv -z \mod (p)$$

y, por tanto

$$0 = x^p + y^p - z^p \equiv 3x^p \mod (p).$$

Como p no divide a x se deduce que $p=3$. Pero, como todos los cubos no múltiplos de 3 son congruentes con ± 1 módulo 9 tendríamos

$$\pm 1 \pm 1 \pm 1 \equiv 0 \mod 9$$

lo que es imposible.

Caso 2: Supongamos ahora que $p \mid xyz$.

Como x, y y z son coprimos dos a dos, p divide a uno y sólo uno de x, y y z. Como podemos cambiar (x, y, z) por $(x, -z, -y)$ o $(y, -z, -x)$ podemos suponer que divide a z. Sea $z = p^k z_0$ con $(p, z_0) = 1$. Del Lema 7.2, tenemos que $p = v\lambda^{p-1}$ para alguna unidad v de $\mathbb{Z}[\zeta]$. Luego

$$x^p + y^p = v^{kp}\lambda^{p(p-1)k} z_0^p.$$

Ponemos $\epsilon = v^{kp}$ y $m = (p-1)k > 0$ y nos quedamos con la ecuación

$$x^p + y^p = \epsilon\lambda^{pm} z_0^p \tag{7.6}$$

con $m > 0$ y ϵ una unidad $\mathbb{Z}[\zeta]$, que vamos a ver que no tiene soluciones enteras racionales x, y y z_0, de forma que p no divide ni a z_0, ni a x, ni a y. De hecho vamos a demostrar un poco más: La ecuación (7.6) no tiene soluciones en $\mathbb{Z}[\zeta]$ relativamente primas con λ. Por reducción al absurdo supongamos que tenemos una solución con m mínimo.

Factorizando la parte de la izquierda y tomando ideales tenemos

$$\prod_{i=0}^{p-1}(x - \zeta^i y) = P^{pm}(z_0)^p \tag{7.7}$$

Como $pm > 0$, al menos uno de los ideales de la izquierda es divisible por P. Pero para todo $i > j$

$$x - \zeta^i y = x - \zeta^j y + \zeta^j(1 - \zeta^{i-j})y \equiv x + \zeta^j y \mod P$$

luego todos los ideales de la izquierda dividen a P.

Como $(p, y) = 1$, los ideales (y) e P son primos relativos en $\mathbb{Z}[\zeta]$. Por otro lado $1 - \zeta^k$ es asociado de λ para todo $0 < k < p$. Luego P^2 no puede dividir a $(y(1 - \zeta^i))$ y por tanto, si $0 \le i < j \le p - 1$

$$(x - \zeta^i y) - (x - \zeta^j y) = \zeta^i y(1 - \zeta^{j-i}) \notin P^2.$$

Luego

$$\frac{x - \zeta^i y}{\lambda} \not\equiv \frac{x - \zeta^j y}{\lambda} \mod P.$$

Como $N(P) = p$,

$$\left\{ \frac{x - \zeta^i y}{\lambda} \mid 0 \le i \le p - 1 \right\}$$

forma un conjunto completo de representantes de $\mathbb{Z}[i]$ módulo P. Por tanto

$$\frac{x - \zeta^i y}{\lambda} \in P$$

para exactamente un $0 \le i \le p - 1$, o sea

$$x - \zeta^i y \in P^2$$

para exactamente un $0 \le i \le p-1$. Reemplazando y por $y\zeta^i$ podemos suponer que $x - y \in P^2$ y $x - y\zeta^i \in P \setminus P^2$ para todo $i = 1, \ldots, p-1$. Como todos los factores de la izquierda dividen a

P y exactamente uno divide a P^2, la multiplicidad de P en la descomposición de la izquierda es al menos $p+1$, lo que implica que $m > 1$. Además la multiplicidad de P en la descomposición de $(x-y)$ tiene que ser $p(m-1)-1$.

Sea D el máximo común divisor de (x) e (y). Como P no divide a (x) ni a (y), tampoco divide a D y, por tanto $x-\zeta^i y$ es divisible por PD y $x-y$ es divisible por $P^{p(m-1)-1}D$. Pongamos

$$\begin{aligned}(x-y) &= P^{p(m-1)-1}DC_0 \\ (x-\zeta^i y) &= PDC_i \qquad\qquad (1 \le i \le p-1)\end{aligned}$$

Vamos a demostrar que los C_i son coprimos dos a dos. Sea Q un divisor común primo de C_i y C_j con $i < j$. Entonces PDQ divide a $(x-\zeta^i y)$ y a $(x-\zeta^j y)$, lo que implica que $(\zeta^i y(1-\zeta^{j-i})) = (y(1-\zeta^{j-i})) = (y)P$ y $(x(1-\zeta^{j-i})) = (x)P$ son divisibles por PDQ, de donde se deduce que (x) e (y) son divisibles por DQ en contra de la elección de D. Concluimos que en efecto los C_i son coprimos dos a dos.

Entonces reescribimos la ecuación (7.7) en la forma

$$D^p P^{pm} C_0 C_1 \dots C_{p-1} = P^{pm}(z_0)^p.$$

De aquí se deduce, teniendo en cuenta que los C_i son coprimos dos a dos, que todos ellos C_i son potencias p-ésimas de otros ideales. Pongamos $C_k = A_k^p$ de donde tenemos.

$$\begin{aligned}(x-y) &= P^{p(m-1)-1}DA_0^p \\ (x-\zeta^i y) &= PDA_i^p \qquad\qquad (1 \le i \le p-1)\end{aligned}$$

Despejamos D en la primera y sustituimos en la segunda:

$$(x-\zeta^i y)P^{p(m-1)} = (x-y)(A_i A_0^{-1})^p.$$

Eso implica que el ideal fraccional $(A_i A_0)^{-1})^p$ es principal. Como p es regular, el ideal fraccional $A_i A_0^{-1}$ también es principal. Pongamos $A_i A_0^{-1}\beta_i = (\alpha_i)$, con $\alpha_i, \beta_i \in \mathbb{Z}[\zeta] \setminus \{0\}$, o lo que es lo mismo $A_i\beta_i = A_0\alpha_i$, o equivalentemente $A_i A_0^{-1} = (\alpha_i)(\beta_i)^{-1}$. Como A_i y A_0 no son divisibles por P, podemos suponer que (α_i) y (β_i) tampoco son divisibles por P. Sustituyendo $A_i A_0^{-1}$ por $(\alpha_i)(\beta_i)^{-1}$ en la fórmula anterior tenemos que

$$(x-\zeta^i y)(\lambda)^{p(m-1)}(\beta_i)^p = (x-y)(\alpha_i)^p$$

lo que implica

$$(x-\zeta^i y)\lambda^{p(m-1)}\beta_i^p = (x-y)(\alpha_i)^p\epsilon_i \tag{7.8}$$

para alguna unidad ϵ_i de $\mathbb{Z}[\zeta]$.

Consideramos la siguiente igualdad:

$$(x-\zeta y)(1+\zeta) - (x+\zeta^2 y) = \zeta(x-y)$$

y multiplicando por $\lambda^{p(m-1)}$ tenemos

$$(x-\zeta y)\lambda^{p(m-1)}(1+\zeta) - (x+\zeta^2 y)\lambda^{p(m-1)} = \zeta(x-y)\lambda^{p(m-1)}$$

Aplicando la ecuación (7.8), la última igualdad toma la forma

$$(x-y)\left(\frac{\alpha_1}{\beta_1}\right)^p \epsilon_1(1+\zeta) - (x-y)\left(\frac{\alpha_2}{\beta_2}\right)^p \epsilon_2 = \zeta(x-y)\lambda^{p(m-1)}$$

Luego

$$(\alpha_1\beta_2)^p - \frac{\epsilon_2}{\epsilon_1(1+\zeta)}(\alpha_2\beta_1)^p = \frac{\zeta}{\epsilon_1(1+\zeta)}\lambda^{p(m-1)}(\beta_1\beta_2)^p.$$

Poniendo $\alpha = \alpha_1\beta_2$, $\beta = \alpha_2\beta_1$, $\gamma = \beta_1\beta_2$, $u = \frac{\epsilon_2}{\epsilon_1(1+\zeta)}$ y $v = \frac{\zeta}{\epsilon_1(1+\zeta)}$ tenemos

$$\alpha^p - u\beta^p = v\lambda^{p(m-1)}\gamma^p \tag{7.9}$$

donde u y v son unidades de $\mathbb{Z}[\zeta]$ y α, β y γ elementos de $\mathbb{Z}[\zeta]$ que no son divisibles por P.

Como $m > 1$, $p(m-1) \geq p$. Luego

$$\alpha^p - u\beta^p \equiv 0 \mod P^p.$$

Por otro lado, como β es relativamente primo con P, existe β' tal que $\beta\beta' \equiv 1 \mod P^p$. Multiplicando por β'^p más arriba tenemos que

$$u \equiv -(\alpha\beta')^p \mod P^p.$$

Por el Lema 7.1 existe un entero racional a tal que $(-\alpha\beta')^p \equiv a \mod P^p$. Luego $u \equiv a \mod P^p$. Recordemos del Lema 7.2 que $P^{p-1} = (p)$, luego u es congruente a un entero racional módulo p. Aplicando el Lema 7.5, deducimos que $u = u_0^p$ para algún $u_0 \in \mathbb{Z}[\zeta]$. Sustituyendo en la ecuación (7.9) tenemos

$$\alpha^p + (-u_0\beta)^p = \alpha^p - (u_0\beta)^p = v\lambda^{p(m-1)}\gamma^p$$

contradiciendo la minimalidad de m. ∎

Obsérvese que solo hemos utilizado el Lema 7.5 al final de la demostración en el Caso 2.

7.3 Primos regulares

El Teorema de Kummer no sirve para nada si no tenemos ninguna forma de comprobar cuando un primo es regular. Esto resulta bastante difícil y requiere métodos de análisis funcional y complejo. Vamos a ver un criterio de regularidad pero sin demostración.

Dado un cuerpo numérico K, se define la *función zeta de Dedekind* de K como la aplicación $\zeta_K : \mathbb{R}^+ \to \mathbb{R}$ dada por

$$\zeta_K(x) = \sum_{I \in \mathcal{I}} N(I)^{-x}$$

donde $\mathcal{I}$ es el conjunto de los ideales del anillo de enteros R de K.

Sean

$$\begin{array}{lcl} r & = & \text{número de inclusiones reales de } K, \\ 2s & = & \text{número de inclusiones complejas de } K, \\ m & & \text{número de raíces de la unidad de } K, \\ \Delta & = & \text{discriminante de } K, \\ h & = & \text{número de clases de } K, \\ v & = & \text{volumen de un conjunto fundamental del retículo } R, \\ R & = & \frac{v}{\sqrt{r+s}} \end{array}$$

Entonces se verifica la siguiente fórmula conocida como *Fórmula Analítica del Número de Clases*

$$\lim_{x\to 1}(x-1)\zeta_K(x) = \frac{2^{r+s}\pi^s R}{m\sqrt{|\Delta|}}h.$$

La idea es que todo lo que hay a la derecha de la fórmula, excepto h es relativamente fácil de calcular. Si podemos calcular el límite de la derecha, podremos calcular h. Para calcular este límite ampliamos la definición de ζ_K para admitir valores complejos de x y, entonces se utilizan técnicas de variable compleja.

En el caso en que $K = \mathbb{Q}(\zeta)$, para ζ una raíz p-ésima primitiva de la unidad, el número de clases h se puede descomponer como producto de dos enteros

$$h = h_1 h_2$$

donde

$$h_1 = \text{numero de clases de } \mathbb{Q}(\zeta + \zeta^{-1})$$

y se demuestra que p es regular precisamente si p no divide a h_1.

Estudiando h_1 se demuestra el siguiente [Borevich-Shafarevich, Number Theory, página 366]

Teorema 7.7 *Si p es un número impar entonces p es regular si y solo si ninguno de los siguientes números es divisible por p^2:*

$$S_k = \sum_{n=1}^{p-1} n^{2k} \quad \left(k = 1, \ldots, \frac{p-3}{2}\right).$$

Por ejemplo utilizando la esto se pueden calcular los primeros 10 primos no regulares que son $37, 59, 67, 101, 103, 131, 149, 157, 233$ y 257.

También se pueden introducir los números de Bernouilli por la expansión de la función $\frac{t}{e^t-1}$ en series de potencias, o sea

$$\frac{t}{e^t-1} = 1 + \sum_{i=1}^{\infty} \frac{B_m}{m!}t^m.$$

Se verifica:

Teorema 7.8 *Un primo racional p es regular precisamente si no divide a los numeradores de los números de Bernouilli $B_2, \ldots, B_{p-3}$.*

Capítulo 8

Extensiones de Galois de cuerpos de números

8.1 Grupos de descomposición e inercia

En esta sección E/F es una extensión de Galois de cuerpos de números con grupo de Galois G y R y S denotan los anillos de enteros de F y E respectivamente.

El grupo de Galois G actúa en los primos de E y para cada primo de P de F esta acción permuta los primos de E que están sobre P. El *subgrupo de decomposición* de un primo Q de S es el estabilizador de Q por esta acción, es decir, el grupo

$$D(Q/F) = \{\sigma \in G : \sigma(Q) = Q\}.$$

Definimos

$$g(Q/F) = [G : D(Q/F)].$$

Claramente $g(Q/F)$ es el cardinal de la órbita de Q bajo la acción de G.

Usamos la barra para reducción módulo Q (en S) y modulo P (en R). Cada $\sigma \in D(Q/F)$ induce un elemento $\overline{\sigma} : \overline{s} \mapsto \overline{\sigma(s)}$ de $\mathrm{Gal}(\overline{S}/\overline{R})$. Esto define un homomorfismo de grupos

$$\alpha_Q : D(Q/F) \to \mathrm{Gal}(\overline{S}/\overline{R}).$$

El núcleo de α_Q se llama *grupo de inercia* of Q sobre R y se denota $I(Q/F)$.

Teorema 8.1 *Sea E/F una extensión de Galois de cuerpos de números con grupo de Galois G y sea P un primo F. Entonces*

(1) G permuta transitivamente los primos de E sobre P.

(2) Existen enteros e, f y g tales que

$$e = e(Q/F), \quad f = f(Q/F) \quad y \quad g = g(Q/F)$$

para todo ideal maximal Q de S sobre P.

(3) $[E:F] = efg$ *y* E *tiene* g *primos sobre* P.

(4) Los grupos de descomposición de los primos de E *sobre* P *forman una clase de conjugación de subgrupos de* G *y sus grupos de inercia son conjugados en* G. *En particular si* Q *y* Q' *son dos primos de* E *sobre* P *entonces existe un* $\sigma \in G$ *tal que* $Q' = \sigma(Q)$ *y en tal caso* $D(Q'/F) = \sigma D(Q/F)\sigma^{-1}$ *e* $I(Q'/F) = \sigma I(Q/F)\sigma^{-1}$.

Demostración. Sea S el anillo de enteros de E y sea $D = D(Q/F)$.

(1) Suponemos por contradicción que Q y Q' son dos primos de E sobre P que no están en la misma G-órbita. Sea I el producto de los primos en la G-órbita de Q' y sean $Q = Q_1, \ldots, Q_g$ los elementos de la G-órbita de Q. Entonces $I_i = I\prod_{j,\, j\neq i} Q_j \not\subseteq Q_i$ para cada $i = 1, \ldots, n$ y por tanto para cada i existe $a_i \in I_i \setminus Q_i$. Luego $a = \sum_{i=1}^{n} a_i \in I \setminus Q_i$ para cada i. Si $\sigma \in G$ entonces σ permuta los elementos de la órbita de Q' y por tanto $\sigma(a) \in I$. Luego $N_{E/F}(a) = \prod_{\sigma\in G} \sigma(a) \in F \cap I = F \cap Q' = P \subseteq Q$. Como Q es un ideal primo de $\mathbb{A}_E$, tenemos que $\sigma(a) \in Q$ para algún $\sigma \in G$. Luego $a \in \sigma^{-1}(Q) = Q_i$, para algún i. Esto contradice la elección de a y acaba la demostración de (1).

(2) y (3) son consecuencia inmediata de (1) y el Teorema 4.23.

(4) Sean Q y Q' dos primos de E sobre P. Por (1), existe $\sigma \in G$ tal que $Q' = \sigma(Q)$. Entonces $D(Q'/F) = \sigma D(Q/F)\sigma^{-1}$. Además $\sigma I(Q/F)\sigma^{-1} = I(Q_i/F)$. En efecto, si $\rho \in D(Q/F)$ entonces $\rho = \sigma\tau\sigma^{-1}$ para algún $\tau \in D(Q/F)$ y $\alpha_{Q_i}(\rho)(\overline{s}) = \overline{\rho(s)} = \overline{\sigma\tau\sigma^{-1}(s)}$. Usando que σ es la identidad en los elementos de F y $\sigma(S) = S$ deducimos que $\sigma \in I(Q'/F)$ si y solo si $\sigma\tau\sigma^{-1}(s) - s \in Q$ para todo $s \in S$ si y solo si $\tau(s) - s \in Q$ para todo $s \in S$ si y solo si $\tau \in I(Q/F)$ si y solo si $\rho \in \sigma I(Q/F)\sigma^{-1}$. Por tanto $I(Q'/F) = \sigma I(Q/F)\sigma^{-1}$ como queríamos demostrar. Esto demuestra que los grupos de descomposición de los primos sobre Q son conjugados entre si y que sus grupos de inercia también son conjugados. Para demostrar que los primeros forman una clase de conjugación de subgrupos de G, tomamos un subgrupo H de G conjugado de $D(Q/F)$. Entonces existe $\sigma \in G$ tal que $H = \sigma D(Q/F)\sigma^{-1}$. Entonces $\sigma(Q)$ es un primo de E sobre F y $H = D(\sigma(Q)/F)$. ∎

Recuérdese que una extensión de cuerpos se dice que es abeliana si es de Galois y su grupo de Galois es abeliano. Como consecuencia del Teorema 8.1.(4) tenemos que

Corolario 8.2 *Si* E/F *es una extensión abeliana de cuerpos de números y* P *es un primo de* F *entonces todos los primos de* E *sobre* E *tienen el mismo grupo de descomposición sobre* F *y el mismo grupo de inercia.*

Sean R y S los anillos de enteros de F y E respectivamente. Sean P un ideal maximal de R y Q primo de E sobre P Entonces usamos la notación

$$e(E/P) = e(Q/F), \quad f(E/P) = f(Q/F) \quad \text{y} \quad g(E/P) = g(Q/F).$$

Por el Teorema 8.1, estos números solo dependen de P y E, o sea no dependen de Q.

Proposición 8.3 *Sea* E/F *una extensión de Galois y sea* P *un primo de* F. *Entonces*

(1) P *es inerte en* E *si y solo si* $[E:F] = f(E/P)$.

(2) P es totalmente ramificado si y solo si $[E:F] = e(E/P)$.

(3) P escinde completamente en E si y solo si $e(E/P) = f(E/P) = 1$.

Recordemos que si K es un cuerpo finito entonces su característica es un número primo p y $|K|$ es una potencia de p. Más generalmente, si L/K es una extensión de cuerpos finitos de grado n y $|K| = q$ entonces $|L| = q^n$, L/K es una extensión de Galois y $\mathrm{Gal}(L/K)$ está generado por el automorfismo de L dado por $\sigma(x) = x^q$. Este automorfismo se llama *automorfismo de Frobenius*.

Teorema 8.4 *Sea E/F una extensión de Galois de cuerpos de números y sea P un primo de F. Entonces para todo primo Q de E sobre P la aplicación α_Q es suprayectiva, $D(Q/F)/I(Q/F)$ es cíclico y*

$$|D(Q/F)| = e(E/P)f(E/P), \quad |I(Q/f)| = e(E/P), \quad [D(Q/F) : I(Q/F)] = f(E/P).$$

Demostración. Sean $R = \mathbb{A}_F$, $S = \mathbb{A}_E$, $P = F \cap P$, $\overline{R} = R/P$ y $\overline{S} = S/Q$. Además usamos la notación $\overline{a}$ para la imagen de a por las proyecciones $R \to \overline{R}$ y $S \to \overline{S}$. Como $\overline{S}/\overline{R}$ es una extensión de cuerpos finitos existe $a \in S$ tal que $\overline{S} = \overline{R}(\overline{a})$. Sean $P = Q \cap R$, $G = \mathrm{Gal}(E/F)$, $D = D(Q/F)$ e $I = I(Q/F)$. Aplicando el Teorema Chino de los Restos a los primos de E sobre P podemos suponer que a pertenece a todos ellos excepto a Q, para ello sustituimos a por otro elemento de S que sea congruente con a módulo Q y con cero módulo todos los demás primos de E sobre P. Por el Teorema 8.1, los primos de E sobre P diferentes de Q son los de la forma $\sigma(Q)$ con $\sigma \in G \setminus D$. Por tanto la suposición sobre a implica que $\sigma(a) \in Q$ para todo $\sigma \in G \setminus D$. Al calcular la imagen del polinomio característico $P = \prod_{\sigma\in G}(X - \sigma(a)) \in R[X]$ módulo Q obtenemos un polinomio $\overline{P} = \prod_{\sigma\in G}\left(X - \overline{\sigma(a)}\right) \in \overline{R}[X]$ cuyas raíces no nulas son los elementos $\overline{\sigma(a)}$ con $\sigma \in D$. Luego, si $\tau \in \mathrm{Gal}(\overline{S}/\overline{R})$ entonces $\tau(\overline{a}) = \overline{\sigma(a)}$ para algún $\sigma \in D$. Luego $\tau = \alpha_Q(\sigma)$. Esto demuestra que α_Q es suprayectiva.

Pongamos $e = e(E/P)$, $f = f(E/P)$ y $g = g(E/P)$. Por el Teorema 8.1, $efg = [E : F] = |G|$ y por definición $g(E/P) = [G : D(Q/F)]$. Por tanto $|D(Q/F)| = ef$. Como α_Q es suprayectiva, aplicando el Primer Teorema de Isomorfía tenemos que $D(Q/F)/I(Q/F) \cong \mathrm{Gal}(\overline{S}/\overline{R})$, que es un grupo cíclico de orden f, porque $\overline{S}/\overline{R}$ es una extensión de cuerpos finitos de grado f. Por tanto $|I(Q/F)| = \frac{|D(Q/F)|}{[D(Q/F):I(Q/F)]} = e$. ∎

8.2 Extensiones de Galois: Cuerpos de descomposición e inercia

En esta sección E/F sigue siendo una extensión de Galois de cuerpos de números y $G = \mathrm{Gal}(E/F)$.

Si H es un subgrupo de G entonces el subcuerpo de E fijo por H es

$$E^H = \{x \in E : \sigma(x) = x \text{ para todo } h \in H\}.$$

El Teorema Principal de la Teoría de Galois, asegura que las aplicaciones

$$H \mapsto E^H, \quad K \mapsto \mathrm{Gal}(E/K)$$

definen biyecciones (inversa, una de la otra) que invierten el orden entre el conjunto de los subgrupos de G y el de los cuerpos intermedios $F \subseteq K \subseteq E$ de forma que $[E : E^H] = |H|$, o equivalentemente $[E^H : F] = [G : H]$. Además, F/F^H es una extensión de Galois y

$$D(Q/F^H) = D(Q/F) \cap H \quad \text{e} \quad I(Q/F^H) = I(Q/F) \cap H. \tag{8.1}$$

Por otro lado, H es normal en G si y solo si F^H/F es una extensión de Galois. Más generalmente, si $\sigma \in G$ entonces para todo subgrupo H de G tenemos

$$E^{\sigma H \sigma^{-1}} = \sigma(E^H).$$

Esto es equivalente a la siguiente igualdad para K un cuerpo entre E y F.

$$\mathrm{Gal}(E/\sigma(K)) = \sigma \mathrm{Gal}(E/K)\sigma^{-1}.$$

Para cada subconjunto X de E y cada subgrupo H de G ponemos

$$X^H = X \cap E^H = \{x \in X : \sigma(x) = x \text{ para todo } h \in H\}.$$

Claramente $\mathbb{A}_E^H = \mathbb{A}_{E^H}$ y si Q es un primo de E sobre P entonces $Q^H = Q \cap E^H$ es un primo de E^H sobre P.

Los cuerpos fijos $F^{D(Q/F)}$ y $F^{I(D/F)}$ de $D(Q/F)$ y $I(Q/F)$ se llaman respectivamente *cuerpo de descomposición* y *cuerpo de inercia* de Q sobre F. Como consecuencia del Teorema 8.1.(4) se tiene

Corolario 8.5 *Sea E/F una extensión de Galois de cuerpos de números con grupo de Galois G y sea P un primo de F y sean L el cuerpo de descomposición de un primo de E sobre P y M el cuerpo de inercia de un primo de E sobre P y K otro cuerpo entre F y E. Entonces*

(1) K es el cuerpo de descomposición de un primo de E sobre P si y solo si existe un $\sigma \in G$ tal que $K = \sigma(L)$.

(2) Si K es el cuerpo de inercia de un primo de E sobre P si y solo si existe un $\sigma \in G$ tal que $K = \sigma(M)$.

Teorema 8.6 *Sea E/F una extensión de Galois de cuerpos de números y sea Q un primo de E. Sean $G = \mathrm{Gal}(E/F)$, $I = I(Q/F)$ y $D = D(Q/F)$. Entonces*

(1) E^I/E^D es una extensión de Galois con grupo de Galois isomorfo a D/I.

(2) Se verifican las siguientes igualdades

$$\begin{aligned} e(Q/F) &= [E : E^I] = e(Q/E^I) = |I|, \\ f(Q/F) &= [E^I : E^D] = f(Q^I/E^D) = f(E/Q^D) = [D : I] \\ g(Q/F) &= [E^D : F] = [G : D], \\ e(Q^I/F) &= e(Q^D/F) = f(Q/E^I) = f(Q^D/F) = g(E/Q^D) = 1. \end{aligned}$$

Representamos esto en la siguiente tabla:

Grado	*Cuerpos*	*Primos*	*Índice de ramificación*	*Grado residual*	*Primos sobre P*
	E	Q			$Q_1, \ldots, Q_g$
e	|	|	e	*1*	*1*
	E^I	Q^I			$Q_1^{I_1}, \ldots, Q_g^{I_g}$
f	|	|	1	f	*1*
	E^D	Q^D			$Q_1^{D_1}, \ldots, Q_g^{D_g}$
g	|	|	1	1	g
	F	P			P

Además si tenemos un cuerpo intermedio $F \subseteq K \subseteq E$ entonces

(3) $E^D \subseteq K$ si y solo si Q es el único primo de E que contiene a $Q \cap K$.

(4) $K \subseteq E^D$ si y solo si $e(Q \cap K/F) = f(Q \cap K/F) = 1$.

(5) $K \subseteq E^I$ si y solo si $e(Q \cap K/F) = 1$.

(6) $E^I \subseteq K$ si y solo si $Q \cap K$ es totalmente ramificado en E.

Demostración. Pongamos $P = Q \cap F$, $e = e(Q/F) = e(E/P)$, $f = f(Q/F) = f(E/P)$ y $g = g(Q/F) = g(E/P)$.

(1) Por Teoría de Galois E/E^D y E/E^I son extensiones de Galois con grupos de Galois D e I respectivamente. Además, como I es normal en D la extensión F^I/F^D es de Galois con grupo de Galois isomorfo a D/I que es un grupo cíclico por el Teorema 8.4.

(2) Usando (8.1) tenemos

$$D(Q/E^D) = D(Q/F) \cap D = D, \quad I(Q/E^D) = I(Q/F) \cap D = I$$

y

$$D(Q/E^I) = D(Q/E) \cap I = I(Q/E^I) \cap I = I.$$

Aplicando los Teoremas 8.1 y (8.4) a las extensiones de Galois E/E^D y E/E^I tenemos que

$$e(Q/E^D)f(Q/E^D)g(Q/E^D) = [E : E^D] = |D| = ef = e(Q/E^D)f(Q/E^D)$$

y

$$e(Q/E^I)f(Q/E^I)g(Q/E^I) = [E : E^I] = |I| = e = e(Q/E^I) = e(Q/E^D).$$

Por tanto $g(Q/E^D) = f(Q/E^I) = g(Q/E^I) = 1$ y $f(Q/E^D) = f$. Aplicando el Lema 4.20 tenemos $e(Q^I/F) = e(Q^D/F) = e(Q^I/Q^D) = f(Q^D/F) = 1$.

(3)-(6) E/K es una extensión de Galois con grupo de Galois $H = \mathrm{Gal}(E/K)$, y la correspondencia de Galois de E/F asocia K con H. Los grupos de descomposición e inercia de la extensión E/K son $D' = D \cap H$ e $I' = I \cap H$. Por tanto los cuerpos de descomposición e inercia de esta extensión son los correspondientes de Galois de D' e I', o sea los compositum $E^{D'} = E^D K$ y $E^{I'} = E^I K$. Aplicando (2) a la extensión E/K deducimos que $e' = e(Q/K) = [E : E^{I'}]$, $f' = f(Q/K) = [E^{I'} : E^{D'}]$ y $g' = g(Q/K) = [E^{D'} : K]$. Representamos esto en el diagrama de la Figura 8.1. Con la ayuda de este diagrama observamos

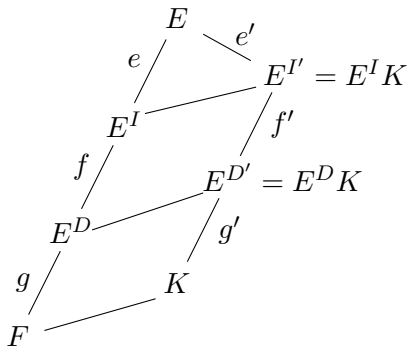

Figure 8.1:

que

(3) Q es el único primo de E que contiene a $Q \cap K$ si y solo si $g' = 1$ si y solo si $E^D K = K$ si y solo si $E^D \subseteq K$.

(4) $e(Q \cap K/F) = f(Q \cap K/F) = 1$ si y solo si $e = e'$ y $f = f'$ si y solo si $[E : E^D] = [E : E^D K]$ si y solo si $K \subseteq E^D$.

(5) $e(Q \cap K/F) = 1$ si y solo $e = e'$ si y solo si $E^I = E^I K$ si y solo si $K \subseteq E^I$.

(6) $Q \cap K$ es totalmente ramificado en E si y solo si $e' = [E : K]$ si y solo si $K = E^I K$ si y solo si $E^I \subseteq K$. ∎

Corolario 8.7 *Sea E/F una extensión de Galois de cuerpos de números, P un primo de F y S el anillo de enteros de E. Supongamos que el grupo de descomposición D de un primo de E sobre P es normal en* $\mathrm{Gal}(E/F)$. *Entonces*

(1) PS^D es el producto de $g(E/P)$ primos distintos de E^D.

(2) Si además el grupo de inercia de un primos de E sobre P también es normal en E entonces para cada primo Q de E^D sobre P se tiene que QS^I es primo en S^I y QS es una potencia de un primo de E.

(3) P escinde completamente en K si y solo si $K \subseteq E^D$.

Demostración. Sean $G = \mathrm{Gal}(E/F)$ y D e I los grupos de descomposición de un primo de Q de E sobre P. Obsérvese que por el Teorema 8.6.(4), la hipótesis significa que D sea normal en G y por tanto E^D/F es una extensión de Galois y, se verifica la hipótesis de (2) precisamente si I es normal en G.

(1) Del Teorema 8.6.(2) se tiene que $e(E^D/P) = f(E^D/P) = 1$. Por tanto PS^D es un producto de $[E^D : F] = g(Q/F)$ primos distintos.

(2) En este caso I es normal en G y aplicando el mismo argumento a F^I deducimos que para cada primo Q de E^D sobre P se verifica $e(Q/F) = e(E^I/P) = e(Q^I/F) = 1$ y, por tanto, $[E : E^I] = e(E/P) = e(Q/F) = e(Q/E^I)$ para todo primo Q' de E sobre F, es decir QS^I es primo y QS es una potencia $e(E/P)$-ésima de un primo de E.

(3) Por el apartado (4) $K \subseteq E^D$ si y solo si $e(Q \cap K/F) = f(Q \cap K/F) = 1$, y como K/F es una extensión de Galois esto pasa si y solo si $e(K/P) = f(K/P) = 1$ si y solo si P escinde completamente en K. ∎

Veamos algunas aplicaciones a extensiones de cuerpos de números que no son necesariamente de Galois.

Corolario 8.8 *Sea F un cuerpo de números de F y sean E_1 y E_2 dos extensiones finitas de F. Sea P un primo de F.*

(1) P no ramifica en E_1 ni en E_2 si y solo si no ramifica en E_1E_2.

(2) P escinde completamente en E_1 y E_2 si y solo si escinde completamente en E_1E_2.

Demostración. Las dos demostraciones son iguales, la primera usando el apartado (5) del Teorema 8.6 y la segunda usando el apartado (3) del mismo Teorema. Sólo hacemos la primera.

Usando el Lema 4.20 se obtiene fácilmente que si P no ramifica en E_1E_2 entonces no ramifica ni en E_1 ni en E_2. Recíprocamente supongamos que P no ramifica ni en E_1 ni en E_2. Sea Q un primo de E_1E_2 sobre P. Tenemos que demostrar que $e(Q/F) = 1$. Sea E la clausura normal de E_1E_2 sobre F y sea Q' un primo de K sobre Q. Sea $I = I(Q'/F)$, el correspondiente grupo de inercia y E^I el cuerpo de inercia de Q' sobre F. Como P no ramifica en E_i se tiene que $e(Q' \cap E_i/F) = 1$. Luego $E_i \subseteq E^I$, por el Teorema 8.6.(5). Como esto pasa para $i = 1$ e $i = 2$ tenemos que $E_1E_2 \subseteq E^I$ y en consecuencia, aplicando otra vez el Teorema 8.6.(5) tenemos que $e(Q/F) = e(Q' \cap E_1E_2/F) = 1$. ∎

Corolario 8.9 *Sea E/F una extensión de cuerpos de números, sea L la clausura normal de E sobre F y sea P un primo de F. Entonces*

(1) P ramifica en E si y solo si ramifica en L.

(2) P es completamente ramificado en E si y solo si es completamente ramificado en L.

Demostración. Como L es el compositum de los cuerpos $\sigma(E)$ con σ recorriendo los F-homomorfismos de E en $\mathbb{C}$, el resultado es consecuencia del Corolario 8.8. ∎

8.3 El automorfismo de Frobenius

En esta sección sigue siendo E/F una extensión de Galois con grupo de Galois G y fijamos un primo Q de E y $P = Q \cap F$ y mantenemos la notación $R = \mathbb{A}_F$, $S = \mathbb{A}_E$, $\overline{R} = R/P$ y $\overline{S} = S/Q$.

Hemos visto que el homomorfismo $\alpha_Q : D = D(Q/F) \to \mathrm{Gal}(\overline{S}/\overline{R})$ es suprayectivo con núcleo $I = I(Q/F)$. Además, si $q = N(P) = |\overline{R}|$ entonces $\mathrm{Gal}(\overline{S}/\overline{R})$ está generado por el automorfismo dado F_q dado por $F_q(x) = x^q$. Este automorfismo se suele llamar *automorfismo de Frobenius* de las extensión $\overline{S}/\overline{R}$. Por tanto D contiene un elemento σ_Q que cumple lo siguiente

$$\sigma_Q(a) \equiv a^q \mod Q, \text{ para todo } a \in E.$$

Si P no ramifica en E entonces $I = 1$ con lo que solo hay un único automorfismo que cumple esta propiedad que llamaremos el *automorfismo de Frobenius* de Q sobre F y que denotaremos $\phi(Q/F)$. El orden de $\phi(Q/F)$ es $f(E/P)$ y si $\sigma \in G$ entonces

$$\phi(\sigma(Q)/F) = \sigma\phi(Q/F)\sigma^{-1} \tag{8.2}$$

En resumen

Proposición 8.10 *Si E/F es una extensión de Galois y P es un primo de F que no ramifica en E entonces los automorfismos de Frobenius de los primos de E sobre P tienen orden $f(E/P)$ y forman una clase de conjugación de* $\mathrm{Gal}(E/F)$.

En particular, si E/F es una extensión abeliana entonces los automorfismos de los primos de E sobre P son iguales al único automorfismo $\phi(E/P)$ de E que verifica

$$\phi(E/P)(a) \equiv a^{N(P)} \mod PS \quad (a \in E).$$

Vamos a ver ahora cómo se puede usar el automorfismo de Frobenius para ver cómo factoriza un primo que no ramifica en una extensión no necesariamente de Galois.

Teorema 8.11 *Sea E/F una extensión de cuerpos de números y sea P un primo de F que no ramifica en E. Sean:*

L la clausura normal de E sobre F,

$G = \mathrm{Gal}(L/F)$,

$H = \mathrm{Gal}(L/E)$,

U un primo de L sobre P,

$\phi = \phi(U/F)$, el automorfismo de Frobenius de U sobre F.

Consideremos $\langle\phi\rangle$ actuando por la derecha en las clases laterales por la derecha de H en G (o sea $H\sigma \cdot \phi^i = H\sigma\phi^i$), sean $O_1, \ldots, O_g$ las órbitas de esta acción, para cada $i = 1, \ldots, g$ fijemos un representante $H\sigma_i \in O_i$ y sea $Q_i = \sigma_i(U) \cap \mathbb{A}_E$. Entonces la factorización de $P\mathbb{A}_E$ es

$$P\mathbb{A}_E = Q_1 \ldots Q_g \quad y \quad f(Q_i/F) = |O_i| \text{ para todo } i = 1, \ldots, g.$$

Demostración. Recordemos que como P no ramifica en E tampoco ramifica en L por el Corolario 8.9. Eso justifica la existencia del automorfismo de Frobenius ϕ.

Primero demostramos que los Q_i son diferentes dos a dos. En efecto, si $Q_i = Q_j$ entonces $\sigma_i(U)$ y $\sigma_j(U)$ son dos primos de L que están sobre Q_i. Como L/K es una extensión de Galois, del Teorema 8.1.(1) se tiene que $\sigma_i(U) = \tau\sigma_j(U)$ para algún $\tau \in H$. Luego $\sigma_i^{-1}\tau\sigma_j \in D(U/F) = \langle\phi\rangle$, es decir $\tau\sigma_j = \sigma_i\phi^k$ para algún k. Por tanto, $H\sigma_i\phi^k = H\tau\sigma_j = H\sigma_j$. Luego $H\sigma_j \in O_i$ y por tanto $i = j$ ya que los $H\sigma_j$ son los representantes de las órbitas.

Sea $f_i = f(Q_i/F)$. Obsérvese que f_i es el índice de $\mathrm{Gal}(\overline{T}/\overline{S})$ en $\mathrm{Gal}(\overline{T}/\overline{R})$ donde R, S y T denotan los anillos de enteros de F, E y L y $\overline{R} = R/P$, $\overline{S} = S/Q_i$ y $\overline{T} = T/\sigma_i(U)$. Por tanto, si ϕ es el automorfismo de Frobenius de la extensión de cuerpos finitos $\overline{T}/\overline{R}$ entonces ϕ^{f_i} es el automorfismo de Frobenius de $\overline{T}/\overline{S}$. Eso implica que $\phi(\sigma_i(U)/F)^{f_i} = \phi(\sigma_i(U)/K)$. Usando esto junto con (8.2) tenemos que

$$\sigma_i\phi^{f_i}\sigma_i^{-1} = \phi(\sigma_i(U)/F)^{f_i} = \phi(\sigma_i(U)/E) \in H,$$

y por tanto

$$H\sigma_i\phi^{f_i} \in H\sigma_i.$$

Eso demuestra que $|O_i| \leq f_i$ para todo i.

Por el Teorema 4.23, tenemos $\sum_{i=1}^{g} f_i \leq [E:F] = [G:H]$. Como además $O_1, \ldots, O_g$ es una partición de las clases laterales por la derecha de H en G, tenemos $\sum_{i=1}^{g} |O_i| = [G:H]$. Combinando esto con la conclusión del párrafo anterior deducimos que $f(Q_i/F) = f_i = |O_i|$ para todo i y necesariamente $P\mathbb{A}_E = Q_1 \ldots Q_g$. ∎

8.4 Ramificación y discriminante

Teorema 8.12 *Sean F un cuerpo de números y p un entero racional. Entonces p ramifica en F si y solo si p divide al discriminante de F.*

Demostración. Sea R el anillo de enteros de F y sea $\alpha_1, \ldots, \alpha_n$ una base entera de R con lo que el discriminante de F es $\Delta = \Delta[\alpha_1, \ldots, \alpha_n]$. Sean $\sigma_1, \ldots, \sigma_n$ las inclusiones de F en $\mathbb{C}$, E la clausura normal de F en $\mathbb{C}$ y S su anillo de enteros. Cada σ_i tiene una extensión a un automorfismo de E que también denotaremos σ_i.

Supongamos que p ramifica en F, o sea p pertenece a un ideal maximal P de R con $e(P/F) > 0$. Eso es equivalente a que $pR = PI$ para un ideal I de R que contenido en todos los primos de F sobre p. Eso implica que I contiene propiamente a pR y usamos esto para fijar un elemento $\alpha \in I \setminus pR$. Entonces $\alpha = \sum_{i=1}^{n} m_i\alpha_i$ con $m_i \in \mathbb{Z}$, pero como p no divide a α en R, algún m_i no es múltiplo de p. Podemos suponer sin pérdida de generalidad que $p \nmid m_1$. Eso en particular implica que $\alpha, \alpha_2, \ldots, \alpha_n$ es otra base de F sobre $\mathbb{Q}$ (no necesariamente una base entera) y de la Proposición 1.6.(2) se deduce que $\Delta(\alpha, \alpha_2, \ldots, \alpha_n) = m_1^2\Delta(\alpha_1, \ldots, \alpha_n) = m_1^2\Delta_F$.

Sea Q un primo de E sobre p y sea $i = 1, \ldots, n$. Entonces $\sigma_i^{-1}(Q)$ es otro primo de E sobre p y por tanto contiene a algún primo P de F sobre p. Luego $\alpha \in I \subseteq P \subseteq \sigma_i^{-1}(Q)$ y por tanto $\sigma_i(\alpha) \in Q$. Utilizando la definición del discriminante deducimos que $m_1^2\Delta_F = \Delta(\alpha, \alpha_2, \ldots \alpha_n) \in Q \cap \mathbb{Z} = pR$. Concluimos, como queríamos, que $p \mid \Delta_F$, pues $p \nmid m_1$.

Demostramos el recíproco por reducción al absurdo. Suponemos pues que p no ramifica en F y que p divide al discriminante de F, es decir $p \mid \det(T_{F/\mathbb{Q}}(\alpha_i\alpha_j))$. Lo primero implica que p no ramifica en E por el Corolario 8.9, es decir pS es un producto de primos distintos y lo segundo que las columnas de la matriz $(T_{F/\mathbb{Q}}(\alpha_i\alpha_j))$ son linealmente dependientes cuando se consideran en $\mathbb{Z}/p\mathbb{Z}$. Es decir, existen enteros $m_1, \ldots, m_n$ que no son todos múltiplos de p pero que cumplen

$$T_{F/\mathbb{Q}}\left(\sum_{i=1}^{n} m_i\alpha_i\alpha_j\right) = \sum_{i=1}^{n} m_i T_{F/\mathbb{Q}}(\alpha_i\alpha_j) \equiv 0 \mod p$$

para todo j. Es decir, si $\alpha = \sum_{i=1}^{n} m_i\alpha_i$ entonces $\alpha \notin pR$ y $p \mid T_{F/\mathbb{Q}}(\alpha\alpha_j)$ para todo $j = 1, \ldots, n$. Como $R = \sum_{j=1}^{n} \mathbb{Z}\alpha_j$ deducimos que $T_{F/\mathbb{Q}}(\alpha R) \subseteq p\mathbb{Z}$

Como $\alpha \in R \setminus pR$ y $pR = R \cap Q$ para todo primo Q de F sobre p, te tiene que α no pertenece a ninguno de los primos de E sobre p. Fijemos uno de ellos Q. Como Q no contiene

al producto de los demás primos de E sobre p existe un elemento β que está en dicho producto pero no está en Q. O sea β está en todos los primos de E sobre p menos en Q. Pero,

$$T_{E/Q}(\alpha S) = T_{F/\mathbb{Q}}T_{E/F}(\alpha S) = T_{F/\mathbb{Q}}(\alpha T_{E/F}(S)) \subset T_{F/\mathbb{Q}}(\alpha R) \subseteq p\mathbb{Z}.$$

En particular, $T_{E/Q}(\alpha\beta S) \subseteq p\mathbb{Z} \subseteq Q$. Por otro lado si D es el grupo de descomposición de Q sobre $\mathbb{Q}$ y $\sigma \in G \setminus D$ entonces $\sigma^{-1}(Q)$ es un primo de E sobre p distinto de Q y por la elección de β tenemos que $\alpha\beta S \subseteq \sigma^{-1}(Q)$. Es decir $\sigma(\alpha\beta S) \subseteq Q$ para todo $\sigma \in G \setminus D$. En consecuencia, si $s \in S$ entonces

$$\sum_{\sigma\in D} \sigma(\alpha\beta s) = T_{E/\mathbb{Q}}(\alpha\beta s) - \sum_{\sigma\in G\setminus D} \sigma(\alpha\beta s) \in Q.$$

Luego

$$\sum_{\sigma\in D} \alpha_Q(\sigma)(\overline{\alpha}\overline{\beta}\overline{s}) = 0.$$

Pero $\overline{S}$ es un cuerpo y $\overline{\alpha\beta} \neq 0$ pues $\alpha\beta \notin Q$. Luego $\sum_{\sigma\in D} \alpha_Q(\sigma) = 0$. Como p no ramifica en E tenemos que $|I(Q/\mathbb{Q})| = e(Q/\mathbb{Q}) = 1$ (Teorema 8.6), es decir α_Q es injectiva y eso implica que los $\alpha_Q(\sigma)$, con $\sigma \in D$ son distintos dos a dos. Pero eso contradice el Teorema de Artin que dice que los automorfismos de un cuerpo son linealmente independientes. ∎

Corolario 8.13 *Supongamos que $F = \mathbb{Q}(\alpha)$ y $f \in \mathbb{Z}[X]$ con $f(\alpha) = 0$. Si $p \nmid N_{F/\mathbb{Q}}(f'(\alpha))$ entonces p no ramifica en F.*

Demostración. Sea $g = \mathrm{Irr}_{\mathbb{Q}}(\alpha)$. Entonces g divide a f en $\mathbb{Q}[X]$. Pongamos $f = gh$. Además $g \in \mathbb{Z}[X]$ por el Lema 2.15 y, usando el Lema de Gauss (Lema 2.13) se deduce que $h \in \mathbb{Z}[X]$. Además $f'(\alpha) = g'(\alpha)h(\alpha) = \pm\Delta_K h(\alpha)$ por la Proposición 1.6.(3) con lo que $N_{F/\mathbb{Q}}(f'(\alpha)) = \pm N_{F/\mathbb{Q}}(\Delta_F)N_{F/K}(h(\alpha)) = \pm\Delta_K^{[F:\mathbb{Q}]}N_{F/K}(h(\alpha))$. En consecuencia, si p no divide a $N_{F/\mathbb{Q}}(f'(\alpha))$, entonces tampoco divide a Δ_F y por tanto p no ramifica en F, por el Teorema 8.12. ∎

Corolario 8.14 *Si E/F es una extensión de cuerpos de números entonces solo un número finito de primos de F ramifica en E.*

Demostración. Si P es un primo de F y P ramifica en E entonces $P \cap \mathbb{Z}$ ramifica en E también. Por tanto basta demostrar el resultado cuando $K = \mathbb{Q}$ y en este caso el resultado es consecuencia del Teorema 8.12. ∎

8.5 Factorización en cuerpos cuadráticos y ciclotómicos

En esta sección vamos a ver cómo calcular la factorización de pR para p un primo racional y R el anillo de entero de un cuerpo cuadrático o un cuerpo ciclotómico.

En primer lugar si n y m son enteros decimos que m es un cuadrado módulo n si existe otro entero a tal que $m \equiv a^2 \mod m$. Más generalmente, si k es un entero positivo decimos que m es una potencia k-ésima de módulo n si $m \equiv a^k \mod n$ para algún entero a.

Obsérvese que si F es un cuerpo con q elementos entonces el grupo F^* de unidades de F es cíclico con $q-1$ elementos. Por tanto, si m es un entero positivo entonces las potencias m-ésimas de F^* forman el único subgrupo de F^* de orden $\frac{q-1}{\mathrm{mcd}(m,q-1)}$. Por ejemplo, si q es par todos los elementos de F^* son cuadrados pero si q es impar entonces la mitad de los elementos de F^* son cuadrados (los que están en el único subgrupo de índice 2) y la otra mitad no los son. En particular, si p es un primo impar, la mitad de las unidades de $\mathbb{Z}/(p)$ son cuadrados (o sea están representadas por cuadrados módulo p) y la otra mitad no. Más generalmente, si q es otro primo entonces si q no divide a $p-1$ entonces todos los enteros son potencias q-ésimas módulo p pero si q divide a $p-1$ entonces el grupo de las unidades de $\mathbb{Z}/(p)$ tiene $\frac{p-1}{q}$ potencias q ésimas, las que forman el único subgrupo con $\frac{p-1}{q}$ elementos.

Supongamos que F es un cuerpo cuadrático. Entonces $F/\mathbb{Q}$ es una extensión de Galois y hay tres posibilidades: pR es primo, pR es el cuadrado de primo de F, o el producto de dos primos de F. En el primer caso $f(F/p) = 2$ y $e(F/p) = 1$, en el segundo caso $e(F/p) = 2$ y $f(F/p) = 1$ y en el tercer caso $e(E/p) = f(F/p) = 1$. La siguiente proposición dice cuándo se da cada caso y cuáles son los primos de F sobre p:

Proposición 8.15 *Sea R el anillo de enteros de $F = \mathbb{Q}(\sqrt{d})$ con d un entero libre de cuadrados distinto de 1 y sea p un primo racional. Entonces se tiene la siguiente factorización en producto de primos de F:*

$$pR = \begin{cases} (pR + \sqrt{d}R)^2, & \text{si } p \mid d; \\ (2R + (1+\sqrt{d})R)^2 & \text{si } p = 2 \text{ y } d \equiv 3 \mod 4; \\ \left(2R + \frac{1+\sqrt{d}}{2}R\right)\left(2R + \frac{1-\sqrt{d}}{2}R\right) & \text{si } p = 2 \text{ y } d \equiv 1 \mod 8; \\ (pR + (n+\sqrt{d})R)(pR + (n-\sqrt{d})R) & \text{si } p \nmid 2d \text{ y } d \equiv n^2 \mod p; \\ pR, & \text{si } \begin{cases} p = 2 \text{ y } d \equiv 5 \mod 8 \\ \text{ó} \\ p \neq 2 \text{ y } d \text{ no es cuadrado módulo } p. \end{cases} \end{cases}$$

Es decir, en los dos primeros casos pR es el cuadrado de un primo (totalmente ramificado), en los dos siguientes es un producto de dos primos distintos (escisión completa) y en el último caso pR es primo (inerte).

Demostración. La extensión $F/\mathbb{Q}$ es de Galois de grado 2. Por tanto, del Teorema 8.1 deducimos que si $f(F/p) = 2$ entonces pR es primo y en los demás casos o bien pR es el cuadrado de un primo de F o el producto de dos primos. En particular, de la factorización única en producto de primos de F se deduce que si I y J son dos ideales de R que contienen

propiamente a pR y $IJ \subseteq pR$ entonces $pR = IJ$ e I y J son primos. En efecto, de $IJ \subseteq pR \subset I$ se deduce que $J \neq R$ y de la misma forma tendríamos que $I \neq R$. Como pR no puede ser el producto de más de dos primos e I y J son divisores propios de pR, necesariamente I y J son primos. Si pR es primo entonces como pR divide a IJ entonces $pR = I$ ó $pR = J$, una contradicción. Por tanto, $pR = IQ$ para otros primo Q y como $IJ \subseteq pR$, se tiene que IQ divide a IJ, con lo que $Q = J$.

Si p divide a d entonces $(pR+\sqrt{d}R)^2 = p^2R+p\sqrt{d}R+dR \subseteq pR \subseteq pR+\sqrt{d}R$, pues $\sqrt{d} \mid p$. Luego $pR = (pR+\sqrt{d}R)^2$, es la factorización de pR.

Similarmente, si $d \equiv 3 \mod 4$ entonces $(2R+(1+\sqrt{d})R)^2 = 4R+2(1+\sqrt{d})R+2\sqrt{d} \subseteq 2R \subseteq 2R+(1+\sqrt{d})R$ pues $1+\sqrt{d} \notin pR$. Por tanto $2R = (2R+(1+\sqrt{d})R)^2$ es la factorización de $2R$.

Obsérvese que en los dos casos anteriores p divide al discriminante de F que recuérdese que es d si $d \equiv 1 \mod 4$ y $4d$ en caso contrario (Ejemplo 2.22). En los demás casos p no divide al discriminante de F, con lo que p no ramifica en F por el Teorema 8.12.

Supongamos que $d = 1 + 4t$ con $t \in \mathbb{Z}$. Entonces $\frac{1+\sqrt{d}}{2}$ y $\frac{1-\sqrt{d}}{2}$ pertenecen a R. Sean $P = 2R+\frac{1+\sqrt{d}}{2}R$ y $Q = 2R+\frac{1-\sqrt{d}}{2}R$. Entonces $2 = (1+\sqrt{d})+(1-\sqrt{d}) \in PQ$ y $t = \frac{\sqrt{d}+1}{2}\,\frac{\sqrt{d}-1}{2} \in PQ$. Por tanto, si t es impar (o sea si $d \not\equiv 1 \mod 8$) entonces $PQ = R$. Sin embargo, si t es par, (es decir si $d \equiv 1 \mod 8$), entonces $PQ = 4R + (1+\sqrt{d})R + (1-\sqrt{d})R + tR \subseteq 2R$. Como claramente ni P ni Q están contenidos en $2R$ deducimos que P y Q son ideales propios de R y por tanto $PQ = 2R$ es la factorización de $2R$.

Supongamos que $p \nmid 2d$. Si $d = n^2 + tp$ con n y t enteros entonces ponemos $P = pR + (n+\sqrt{d})R$ y $Q = pR + (n-\sqrt{d})R$. De nuevo ni P ni Q están contenidos en pR y $PQ = p^2R + p(n+\sqrt{d})R + p(n-\sqrt{d})R + tpR \subseteq pR$. Luego $pR = PQ$ es la factorización de pR.

En los casos que faltan o bien $p = 2$ y $d \equiv 5 \mod 8$ ó $p \nmid 2d$ y d no es cuadrado módulo p. Falta demostrar que en ambos casos pR es primo lo cual es equivalente a demostrar que $f(F/p) = 2$ y para ello vamos a ver que R tiene un elemento α cuyo polinomio mínimo f sobre $\mathbb{Q}$ es irreducible módulo p. Eso implica que si Q es un primo de R sobre p entonces la imagen $\overline{\alpha}$ en R/Q, que será raíz del polinomio f módulo p no pertenece a $\mathbb{Z}/p\mathbb{Z}$. Por tanto $f(F/p) = 2$ lo que implica que pR es primo. En efecto, $p \neq 2$ y d no es cuadrado módulo p entonces el polinomio $X^2 - d$ es el polinomio mínimo de $\sqrt{d}$ y es irreducible sobre $\mathbb{Z}/p\mathbb{Z}$. Si $d \equiv 5 \mod 8$ entonces $\alpha = \frac{1+\sqrt{d}}{2}$ es un elemento de R cuyo polinomio mínimo sobre $\mathbb{Q}$ es $X^2 - X + \frac{1-d}{4}$. Como $d-1$ no es múltiplo de 8 al reducir este polinomio módulo 2 se convierte en X^2+X+1 que es irreducible sobre $\mathbb{Z}/2\mathbb{Z}$. ∎

Consideramos ahora extensiones ciclotómicas. Si n y m son enteros coprimos, denotamos por $o_n(m)$ a orden multiplicativo de m módulo n, o sea el menor entero positivo k tal que $m^k \equiv 1 \mod n$.

Teorema 8.16 *Sea m un entero positivo y sean $F = \mathbb{Q}(\zeta_m)$ y p es un primo racional. Sean $m = p^k n$ con $p \nmid n$, $e = \varphi(p^k)$ y f el orden multiplicativo de p módulo n (es decir $p^f \equiv 1 \not\equiv p^{f-1} \mod n$). Entonces $e(F/p) = \varphi(p^k)$, $f = o_n(p)$ con lo que*

$$pR = (Q_1 \dots Q_g)^{\varphi(p^k)}$$

con $g = \frac{\varphi(m)}{\varphi(p^k)o_n(p)} = \frac{\varphi(n)}{o_n(p)}$ y $Q_1, \dots, Q_g$ primos distintos de F.

Demostración. Vamos a poner $E = \mathbb{Q}(\zeta_n)$ y $L = \mathbb{Q}(\zeta_{p^k})$ e ilustrar la demostración con la Figura 8.2.

Por el Teorema 2.37 y el Lema 2.36 se tiene que $\Delta_F = \Delta_{F/\mathbb{Q}}(\zeta_m)$ y este es un divisor de una potencia de m. Aplicando entonces el Teorema 8.12 se deduce que si p ramifica en F entonces $p \mid m$. Por tanto $e(L/p) = 1$. Sea Q un primo de $\mathbb{Q}(\zeta_n)$ sobre p y sea $\pi : \mathbb{Z}[\zeta_n] \to K = \mathbb{Z}[\zeta_n]/Q$ la proyección canónica. Como $p \nmid n$, se tiene que $n \notin p\mathbb{Z} = Q \cap \mathbb{Z}$ y por tanto $\pi(n) \neq 0$. Si $\xi \in \langle \zeta_n \rangle \setminus \{1\}$ con $\pi(\xi) = 1$ entonces $\sum_{i=0}^{n} \xi^i = 0$, luego $\pi(n) = \sum_{i=0}^{n} \pi(\xi)^i = \pi\left(\sum_{i=0}^{n} \xi^i\right) = \pi(0) = 0$, una contradicción. Esto demuestra que la restricción de π a $\langle \zeta_n \rangle$ es inyectiva, o sea $\pi(\zeta_n)$ es una raíz n-ésima primitiva de la unidad en K. Pero K está generado sobre $\mathbb{Z}/p\mathbb{Z}$ por $\pi(\zeta_n)$ y por tanto K es minimal entre los cuerpo de característica p que contienen una raíz n-ésima primitiva de la unidad, con lo que su cardinal es la menor potencia de p que es 1 módulo n, o sea $|K| = p^{o_n(p)}$. Concluimos que $f(\mathbb{Q}(\zeta_n)/p)? = o_n(p)$. Esto demuestra el resultado para el caso en que $k = 0$.

Supongamos que $k > 0$. Entonces, del apartado anterior, el Lema 4.20 y el Teorema 4.23 deducimos que $e(F/p) = e(F/Q) \leq [F : \mathbb{Q}(\zeta_n)] = \varphi(p^k)$ y $f(F/p) \geq f(\mathbb{Q}(\zeta_n)/p) = o_n(p)$. Sean $S = \mathbb{Z}[\zeta_{p^k}]$ y $P = S(1 - \zeta_{p^k})$. Por el Corolario 2.35, $N_{K/\mathbb{Q}}(P) = p$ y $pS = P^{\varphi(p^k)}$. Por tanto P es primo de L y $e(L/p) = \varphi(p^k) = [L : \mathbb{Q}]$. Por tanto $f(L/p) = 1$, $e(F/p) \geq e(L/p) = \varphi(p^k)$. Luego $e(F/p) = \varphi(p^k)$. Además si Q es un primo de F sobre p entonces $e(Q/E) = e(F/p) = \varphi(p^k) = [F : \mathbb{Q}(\zeta_n)]$ y por tanto $f(Q/E) = 1$. Luego $f(F/p) = f(E/p) = o_n(p)$. ∎

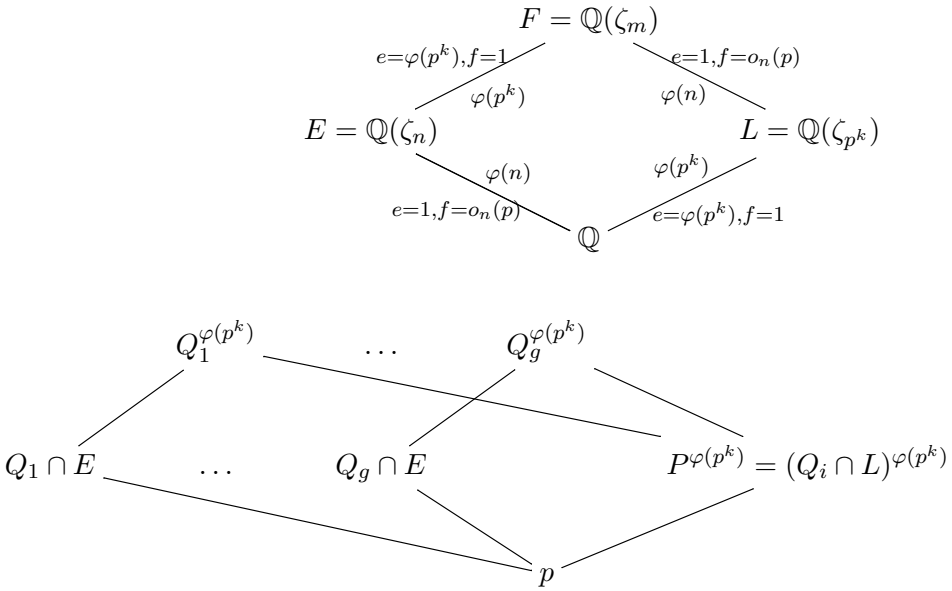

Figure 8.2:

Combinando los Teoremas 8.12 y 8.16 deducimos:

Corolario 8.17 *Sea m un entero positivo y p un primo racional. Entonces las siguientes condiciones son equivalentes:*

(1) p ramifica en $\mathbb{Q}(\zeta_m)$.

(2) p divide a $\Delta(\mathbb{Q}(\zeta_m)/\mathbb{Q})$.

(3) p es impar y divide a m ó $p = 2$ y $4 \mid m$.

8.6 Ley de Reciprocidad Cuadrática y otras aplicaciones

En esta sección vamos ver algunas aplicaciones de las propiedades aritméticas del anillo de enteros ciclotómicos.

Sea p un primo impar y sean $F = \mathbb{Q}(\zeta_p)$ y $G = \mathrm{Gal}(F/\mathbb{Q})$. Entonces G es isomorfo al grupo de unidades de $\mathbb{Z}_p$ que cíclico de orden $p-1$ y, por tanto, G tiene un único subgrupo de orden d para cada d que divide a $p-1$. Además, $G^d = \{g^d : g \in G\}$ es el único subgrupo de G de orden $\frac{p-1}{d}$ y su cuerpo fijo que denotaremos por F_d es el único subcuerpo de F con $[F : \mathbb{Q}] = d$. Se tiene por tanto que si d' es otro divisor de $p-1$ entonces $F_d \subseteq F_{d'}$ si y solo si d divide a d'.

En particular, si p es impar entonces F_2 es el único cuerpo cuadrático contenido en F. Supongamos que $F_2 = \mathbb{Q}(\sqrt{d})$ con d libre de cuadrados. Si q es un primo que divide a d entonces q ramifica en F_2 y por tanto también ramifica en F. Pero eso implica que $q = p$. Eso implica que o bien $d = -1$ o $d = \pm p$. Pero el primer caso no es posible pues $i \notin F$. Luego $d = \pm p$. Además, por el Corolario 8.17, 2 no ramifica en F y por tanto tampoco ramifica en F_2 con lo que no divide al discriminante de F_2. Eso implica que $d \equiv 1 \mod 4$. Esto demuestra lo siguiente:

Teorema 8.18 *Si p es un primo impar entonces el único subcuerpo cuadrático de $\mathbb{Q}(\zeta_p)$ es $\mathbb{Q}(\sqrt{\varepsilon_p p})$, with $\varepsilon_p = (-1)^{\frac{p-1}{2}}$.*

Ejemplo 8.19 *$\mathbb{Z}[\zeta_{23}]$ no es DFU.*

Demostración. Pongamos $F = \mathbb{Q}(\zeta_{23})$, $D = \mathbb{Z}[\zeta_{23}]$ que es el anillo de enteros de F y $N = N_{F/\mathbb{Q}}$. Sea $F_2 = \mathbb{Q}(\sqrt{-23})$, que es el único subcuerpo cuadrático de F por el Corolario 8.18. Sea

$$\mu = 1 - \zeta_{23} + \zeta_{23}^{-2}.$$

Después de muchos cálculos se obtiene que

$$N(\mu) = 6533 = 47 \cdot 139.$$

Esto se puede conseguir utilizando el programa GAP:

```
gap> F:=CF(23);
CF(23)
gap> z:=E(23);
E(23)
gap> a:=1-z+z^-2;
-2*E(23)-E(23)^2-E(23)^3-E(23)^4-E(23)^5-E(23)^6-E(23)^7-E(23)^8-E(23)^9
-E(23)^10-E(23)^11-E(23)^12-E(23)^13-E(23)^14-E(23)^15-E(23)^16-E(23)^17
```

```
-E(23)^18-E(23)^19-E(23)^20-E(23)^22
gap> Norm(F,a);
6533
```

Como $N(\mu)$ no es una potencia de un primo, el ideal $I = (\mu)$ no es primo (Proposición 4.18.(4)). De hecho I debe ser el producto de dos primos (ya que la norma de I es producto de dos primos) $I = PQ$, cuyas normas son $N(P) = 47$ y $N(Q) = 139$. Si D es DFU entonces $P = (\nu)$ para algún $\nu \in D$ (Teorema 4.19). Entonces $N_{F/F_2}(\nu)$ pertenece al anillo de enteros de F_2 que es $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$ (Proposición 2.20). O sea $N_{F/F_2}(\nu) = \frac{a+b\sqrt{-3}}{2}$ para dos enteros a, b y aplicando el Corolario 4.22 obtenemos

$$\pm 47 = N(\nu) = N_{F_2/\mathbb{Q}}(N_{F/F_2}(\nu)) = N_{F_2/\mathbb{Q}}\left(\frac{a+b\sqrt{-23}}{2}\right) = \frac{a^2+23b^2}{4}.$$

Por tanto

$$a^2 + 23\, b^2 = 4 \cdot 47 = 188$$

Pero un cálculo sencillo muestra que 188 no se puede escribir como $a^2 + 23b^2$ con $a, b \in \mathbb{Z}$. ∎

Teorema 8.20 *Sean p y q son primos distintos. Sea d es un divisor de $p-1$ y sea F_d el único subcuerpo de $\mathbb{Q}(\zeta_p)$ de grado d sobre $\mathbb{Q}$. Entonces q es una potencia d-ésima módulo p si y solo si q escinde completamente en F_d.*

Demostración. Sea $F = \mathbb{Q}(\zeta_p)$. Si $p = 2$ entonces $d = 1$ con lo que seguro que q es potencia d-ésima y q escinde completamente en $F_d = \mathbb{Q}$. Por tanto, a partir de ahora suponemos que p es impar. Por el Teorema 8.17, sabemos que $e(F/q) = 1$ y que $f = f(F/q)$ es el orden multiplicativo de q módulo p. Por tanto el grupo de descomposición de un primo de F sobre p es el grupo que tiene orden f y ese es precisamente el orden del grupo generado por q en $\mathbb{Z}_p^*$, es decir $\langle q \rangle$ es el grupo de descomposición de cada uno de los primos de F sobre q, que es un subgrupo de índice $g = g(F/q) = \frac{p-1}{f}$ en $(\mathbb{Z}/p\mathbb{Z})^*$ y por tanto el cuerpo de descomposición es $F^{\langle q \rangle} = F_g$. Luego $F^{\langle q \rangle} = F_g$. Del Corolario 8.7.(3) tenemos que q escinde completamente en F_d si y solo si $F_d \subseteq F_g$ si y solo si $d \mid g$ si y solo si $f \mid \frac{p-1}{d}$ si y solo si el subgrupo del grupo de unidades de $\mathbb{Z}/(p)$ de orden f está contenido en el de orden $\frac{p-1}{d}$. Como el primero de estos grupos es el generado por q y el segundo es el de potencias d-ésimas concluímos que q escinde completamente en F_d si y solo si q es una potencia d-ésima módulo p. ∎

Recordemos que si m es un entero positivo y p es un primo el símbolo de Legendre se define como

$$\left(\frac{m}{p}\right) = \begin{cases} 0, & \text{si } p \mid m; \\ 1, & \text{si } p \nmid m \text{ y } m \text{ es cuadrado módulo } p; \\ -1, & \text{si } p \nmid m \text{ y } m \text{ no es cuadrado módulo } p. \end{cases}$$

Está claro que

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{q}\right)\left(\frac{n}{q}\right)$$

y que

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{si } p \equiv 1 \mod 4; \\ -1, & \text{si } p \equiv -1 \mod 4. \end{cases}$$

Por tanto

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

Concluimos con un famoso Teorema debido a Legendre.

Corolario 8.21 (Ley de Reciprocidad Cuadrática) *Si p y q son primos impares distintos entonces*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Demostración. Sean $K_p = \mathbb{Q}(\sqrt{\varepsilon_p p})$ y y $K_q = \mathbb{Q}(\sqrt{\varepsilon_q q})$ los subcuerpos cuadrático de $\mathbb{Q}(\zeta_p)$ y $\mathbb{Q}(\zeta_p)$ respectivamente. Usando el Teorema 8.20 y la Proposición 8.15 tenemos que $\left(\frac{q}{p}\right) = 1$ si y solo si q es un cuadrado módulo p si y solo si q escinde completamente en $K_p = \mathbb{Q}(\sqrt{\varepsilon_p p})$ si y solo si $\varepsilon_p p$ es un cuadrado módulo q. Esto demuestra que $\left(\frac{q}{p}\right) = \left(\frac{\varepsilon_p p}{q}\right) = \left(\frac{\varepsilon_p}{q}\right)\left(\frac{p}{q}\right)$, o lo que es lo mismo

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = \left(\frac{\varepsilon_p}{q}\right).$$

Esto es 1 si y solo si o bien $(-1)^{\frac{p-1}{2}} = \varepsilon_p = 1$ o bien $(-1)^{\frac{q-1}{2}} = \left(\frac{-1}{q}\right) = 1$. En tal caso $(-1)^{\frac{(p-1)(q-1)}{4}} = 1$. En caso contrario, $\frac{p-1}{2}$ y $\frac{q-1}{2}$ son impares y por tanto $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1 = (-1)^{\frac{(p-1)(q-1)}{4}}$. ∎

Index