Facultad
de
Ciencias

Descomposición de primos racionales en los cuerpos cuadráticos y ciclotómicos

(Decomposition of rational primes in the quadratic and cyclotomic fields)

Trabajo de Fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autor: Daniel Sebastián San Martín

Director: María Pilar Fernández-Ferreirós Erviti

Junio - 2017

Índice general

Resumen:

El objetivo de este trabajo es enunciar y demostrar un Teorema que fue inicialmente probado por Richard Dedekind. Este Teorema determina la descomposición de cualquier primo racional en un cuerpo de números cuyo anillo de enteros sea una extensión simple de $\mathbb{Z}$. Para la elaboración y comprensión de su demostración ha sido necesario realizar un amplio estudio de la estructura y de las propiedades de los anillos de enteros algebraicos y de sus ideales.

Palabras clave: Dedekind, Entero, Algebraico, Factorización

Abstract:

In this work, we proof a theorem that was initially proven by Richard Dedekind. This theorem shows the decomposition of any rational prime in a number field whose ring of integers is a simple extension of $\mathbb{Z}$. To proof and understand this Dedekind's Theorem, it has been necessary to study the structure and properties of the rings of algebraic integers as well as those of their ideals.

Key words: Dedekind, Integer, Algebraic, Factorization

Introducción

El objetivo de este trabajo es demostrar el Teorema 4.1.1. Se trata de un resultado probado por Richard Dedekind que determina la descomposición de cualquier primo racional en un cuerpo de números cuyo anillo de enteros sea una extensión simple de $\mathbb{Z}$.

Precediendo a la demostración del teorema anterior, se incluyen todos los conceptos y resultados que son necesarios para su comprensión. Estos conceptos y resultados han sido obtenidos de distintas fuentes, siendo las principales: Stewart [1] y Marcus [3]. Además, se han incluido referencias a los "Vorlesungen über Zahlentheorie" originales de Dedekind y Dirichlet, en los cuales se desarrolló la teoría de ideales por primera vez [5] [6] [7].

En el Capítulo 1 se realiza una introducción histórica a la Teoría de Ideales, indicando su motivación y sus autores.

En el Capítulo 2 se introduce el concepto de anillo de enteros y otros conceptos relacionados con éste como la norma, la traza o el discriminante. Además, se estudia la estructura aditiva de estos anillos y se da un algoritmo que permitirá el cálculo de las bases enteras. Al final de este capítulo, se calculan y obtienen las bases enteras de los cuerpos cuadráticos y ciclotómicos para probar que sus anillos de enteros son extensiones simples de $\mathbb{Z}$, por lo que podremos aplicarles el Teorema 4.1.1.

En el Capítulo 3 se realiza un estudio sobre la factorización en los anillos de enteros. En primer lugar, se comprueba que la unicidad de la factorización en irreducibles de los elementos del anillo no se da siempre. Sin embargo, veremos en el Teorema 3.2.4 que los ideales de los anillos de enteros factorizan de forma única como producto de ideales primos. Además, probaremos en el Teorema 3.3.4 que cada ideal puede ser generado a lo sumo por dos elementos. En el Teorema 3.3.5, obtendremos que las condiciones de DIP y DFU son equivalentes en los anillos de enteros.

Por último, en el Capítulo 4 se probará el Teorema 4.1.1 acompañado de algunos ejemplos.

Capítulo 1

Historia

1.1. La teoría de ideales

Se llama ideal $\mathfrak{a}$ de un anillo conmutativo R a un subconjunto de R tal que $(\mathfrak{a}, +)$ es subgrupo de $(R, +)$ y $ra \in \mathfrak{a}$, $\forall a \in \mathfrak{a}$, $\forall r \in R$.

Este concepto fue introducido por el matemático alemán Ernst Kummer en 1844 mientras intentaba demostrar el último Teorema de Fermat. Observó que para los elementos de los anillos de enteros falla la propiedad de factorización única en irreducibles. En concreto, Kummer comprobó que la propiedad anterior fallaba en el anillo de enteros $\mathbb{Z}[\omega]$ del vigésimo tercer cuerpo ciclotómico $\mathbb{Q}(\omega)$. Para solucionar el problema de la factorización única en irreducibles, Kummer introdujo lo que llamó números ideales, que eran factores que se introducían en un anillo R cuando un elemento $r \in R$ no cumplía la propiedad de la factorización única. De esta forma, se obtenía un anillo $R' \supseteq R$ de modo que el elemento r podía factorizarse de forma única en irreducibles en el anillo R'. Su trabajo fue fundamental para el desarrollo de las matemáticas durante muchos años y su concepto de ideal fue la base para toda la teoría de anillos e ideales tal y como se conoce hoy.

Usando las ideas de Kummer y lo aprendido de Dirichlet, Dedekind elaboró la teoría de ideales. Richard Dedekind era estudiante de Carl Friedrich Gauss en la Universidad de Gotinga; cuando este último murió a principios de 1855, su puesto fue ocupado por Peter Gustav Lejeune Dirichlet que venía de la Universidad de Berlín, el cual impartió una serie de cursos de Teoría de Números a los que asistió Dedekind.

Dedekind editó las lecciones de Dirichlet sobre Teoría de Números y las publicó en 1863 con el título "Vorlesungen über Zahlentheorie"[5]. Dedekind elaboró 3 entregas más de "Vorlesungen über Zahlentheorie", las cuales fueron publicadas en los años 1871 (2^a edición con los suplementos del I al X, [6], [10]), 1879 (3^a edición con el suplemento XI) y 1894 (4^a edición [7]) respectivamente.

En las dos últimas fue donde aparece la Teoría de Ideales prácticamente como hoy la conocemos; sin embargo, en estos textos no aparecía el término de anillo, ya que éste fue introducido posteriormente por el matemático David Hilbert como generalización tanto de los dominios de Dedekind como de los anillos de polinomios.

Capítulo 2

Anillos de Enteros Algebraicos

Se llama cuerpo de números a cualquier cuerpo K que sea extensión finita de $\mathbb{Q}$. El bien conocido Teorema del Elemento Primitivo afirma que cualquier cuerpo de números es una extensión simple de $\mathbb{Q}$.

2.1. Enteros Algebraicos

Definición 2.1.1 *Un número complejo α es entero algebraico si y sólo si existe un polinomio mónico $f(x)$ con coeficientes enteros tal que $f(\alpha) = 0$.*

Por ejemplo, tenemos que $\alpha = \sqrt[3]{5}$ es un entero algebraico, ya que $\alpha^3 - 5 = 0$; y que $\theta = \frac{1}{2}(1 + \sqrt{5})$ es también un entero algebraico, ya que $\theta^2 - \theta - 1 = 0$.

Cabe destacar, que en la definición de entero algebraico, no se requiere que el polinomio $f(x)$ sea irreducible en $\mathbb{Q}[x]$. Sin embargo, es cierto que cada entero algebraico es raíz de algún polinomio mónico con coeficientes enteros e irreducible en $\mathbb{Q}[x]$.

Normalmente, para distinguir a los enteros algebraicos de los elementos de $\mathbb{Z}$, estos últimos se suelen llamar enteros racionales.

Corolario 2.1.1 *Los enteros algebraicos de $\mathbb{Q}$ son los números enteros.*

Dem: Sea $\alpha \in \mathbb{Q}$ un entero algebraico. Podemos escribir $\alpha = \frac{m}{n}$ donde m, n son enteros racionales coprimos, con $n > 0$. Entonces existe un polinomio mónico

$$f(x) = x^k + a_{k-1} \cdot x^{k-1} + \ldots + a_0$$

con $a_0, \ldots, a_{k-1} \in \mathbb{Z}$ tal que

$$f(\alpha) = (\frac{m}{n})^k + a_{k-1} \cdot (\frac{m}{n})^{k-1} + \ldots + a_0 = 0$$

Multiplicando la ecuación anterior por n^k, tenemos

$$m^k = -a_{k-1} \cdot m^{k-1} \cdot n - \ldots - a_0 \cdot n^k$$

lo que implica que $n|m^k$. Pero, como m y n son coprimos, se tiene que $n = 1$, y por lo tanto $\alpha = m \in \mathbb{Z}$.

Teorema 2.1.1 *Sea α un entero algebraico y $f(x)$ un polinomio mónico en $\mathbb{Z}[x]$ de grado mínimo teniendo a α como raíz. Entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$ y es, por tanto, el polinomio mínimo de α sobre $\mathbb{Q}$.*

Dem: Supongamos que $f(x)$ no es irreducible en $\mathbb{Q}[x]$, esto es, $\exists g(x), h(x) \in \mathbb{Q}[x]$ con grado$(g(x))$, grado$(h(x)) > 0$, tal que $f(x) = g(x)h(x)$. Sea n el menor entero positivo tal que $n \cdot g(x) \in \mathbb{Z}[x]$ y m el menor entero positivo tal que $m \cdot h(x) \in \mathbb{Z}[x]$. La minimalidad de n y m nos aseguran que $n \cdot g(x)$ y $m \cdot h(x)$ son primitivos.

Si $nm > 1$ y p es cualquier primo divisor de nm, al reducir coeficientes módulo p en la ecuación $nm \cdot f(x) = (n \cdot g(x))(m \cdot h(x))$, tenemos que $0 \equiv \overline{(n \cdot g(x))}\ \overline{(m \cdot h(x))}$ en $\mathbb{Z}_p[x]$. Como $\mathbb{Z}_p[x]$ es un dominio de integridad, debe ser $\overline{n \cdot g(x)} = 0$ o $\overline{m \cdot h(x)} = 0$. Por ello, p divide a todos los coeficientes de $n \cdot g(x)$ o a todos los coeficientes de $m \cdot h(x)$, pero esto es imposible ya que $n \cdot g(x)$ y $m \cdot h(x)$ son primitivos.

Por lo tanto, ha de ser $n = m = 1$ y $g(x), h(x) \in \mathbb{Z}[x]$. Como α es raíz de alguno de los dos polinomios anteriores y ambos tienen grado menor que $f(x)$, se llega a una contradicción.

Teorema 2.1.2 *Sea K un cuerpo de números.*

1. *Para cada $\alpha \in K$ existe $b \in \mathbb{Z}$ tal que $b\alpha$ es un entero algebraico. En particular, $K = \mathbb{Q}(\alpha)$ para algún entero algebraico $\alpha \in K$.*

2. *Para cada base $\{\alpha_1, \ldots, \alpha_n\}$ de $K/\mathbb{Q}$ existen enteros $c_1, \ldots, c_n$ de forma que $\{c_1\alpha_1, \ldots, c_n\alpha_n\}$ es una base de $K/\mathbb{Q}$ formada por enteros algebraicos.*

Dem:

1. Sea $\alpha \in K$ y $f(x) = x^k + a_{k-1} \cdot x^{k-1} + \ldots + a_1 \cdot x + a_0$ el polinomio mínimo de α sobre $\mathbb{Q}$. Escribimos cada uno de los coeficientes $a_i \in \mathbb{Q}$ de la forma $a_i = \frac{b_i}{b}$ con $b_i, b \in \mathbb{Z}$ y obtenemos

$$\alpha^k + \frac{b_{k-1}}{b} \cdot \alpha^{k-1} + \ldots + \frac{b_1}{b} \cdot \alpha + \frac{b_0}{b} = 0$$

Multiplicando por b, llegamos a que

$$b \cdot \alpha^k + b_{k-1} \cdot \alpha^{k-1} + \ldots + b_1 \cdot \alpha + b_0 = 0$$

Tenemos que $f_1(x) = b \cdot x^k + b_{k-1} \cdot x^{k-1} + \ldots + b_1 \cdot x + b_0 \in \mathbb{Z}[x]$ se anula en α, por lo que

$$g(x) = b^{k-1} \cdot f_1(x) = b^k \cdot x^k + b^{k-1} \cdot b_{k-1} \cdot x^{k-1} + \ldots + b^{k-1} \cdot b_1 \cdot x + b^{k-1} \cdot b_0 \in \mathbb{Z}[x]$$

y $g(\alpha) = 0$. Por lo tanto, $b\alpha$ es raíz del polinomio mónico

$$g(x) = x^k + b_{k-1} \cdot x^{k-1} + \ldots + b^{k-2} \cdot b_1 \cdot x + b^{k-1} \cdot b_0$$

y $b\alpha$ es un entero algebraico.

Para probar la segunda afirmación, basta aplicar este resultado a un elemento primitivo α de la extensión $K/\mathbb{Q}$.

2. Si $\{\alpha_1, \ldots, \alpha_n\}$ es base de $K/\mathbb{Q}$, es obvio que $\{c_1\alpha_1, \ldots, c_n\alpha_n\}$ es también base para cualquier colección de enteros no nulos $c_1, \ldots, c_n$. Por el apartado previo, tenemos que los enteros $c_1, \ldots, c_n$ pueden elegirse de forma que $\{c_1\alpha_1, \ldots, c_n\alpha_n\}$ sean enteros algebraicos.

El conjunto de enteros algebraicos de cualquier cuerpo de números tiene estructura de anillo. Para probarlo, serán necesarias nuevas caracterizaciones de los enteros algebraicos.

Teorema 2.1.3 *Si $\alpha \in \mathbb{C}$, son equivalentes*

1. *α es entero algebraico.*
2. *El grupo aditivo $\mathbb{Z}[\alpha] = \langle \alpha^i / i = 0, 1, 2, \ldots \rangle$ es finitamente generado.*
3. *α pertenece a algún subanillo de $\mathbb{C}$ cuyo grupo aditivo es finitamente generado.*
4. *$\alpha A \subseteq A$ para algún subgrupo aditivo finitamente generado y no nulo de $\mathbb{C}$.*

Dem: (1) $\Rightarrow$ (2) : Si α es un entero algebraico, entonces para algún n tenemos que

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

con $a_i \in \mathbb{Z}$. Por lo tanto,

$$\alpha^n = -a_{n-1} \cdot \alpha^{n-1} - \ldots - a_0 \in G = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle$$

Si $m \geq n$ y $\alpha^m \in G$, con $\alpha^m = b_{n-1} \cdot \alpha^{n-1} + \ldots + b_1 \cdot \alpha + b_0$, entonces

$$\alpha^{m+1} = b_{n-1} \cdot \alpha^n + \ldots + b_1 \cdot \alpha^2 + b_0 \cdot \alpha =$$

$$= b_{n-1} \cdot (-a_{n-1} \cdot \alpha^{n-1} - \ldots - a_0) + \ldots + b_1 \cdot \alpha^2 + b_0 \cdot \alpha \in G$$

Por lo tanto, $\alpha^m \in \langle 1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \rangle, \forall m > 0$ y $\mathbb{Z}[\alpha] = \langle 1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \rangle$.

(2) $\Rightarrow$ (3) $\Rightarrow$ (4) : Trivial.

(4) $\Rightarrow$ (1) : Sea A un subgrupo aditivo no nulo de $\mathbb{C}$ generado por $v_1, \ldots, v_n$ tal que $\alpha A \subseteq A$. Si expresamos cada $\alpha \cdot v_i (i = 1, \ldots, n)$ como combinación lineal de $v_1, \ldots, v_n$ con coeficientes en $\mathbb{Z}$, se tiene

$$\alpha \cdot v_i = \sum_{j=1}^{n} b_{ij} \cdot v_j \ \text{ con } \ b_{ij} \in \mathbb{Z}$$

La expresión anterior, nos lleva a un sistema homogéneo de ecuaciones con incógnitas v_i de la forma:

$$\begin{gathered}
(b_{11} - \alpha) \cdot v_1 + b_{12} \cdot v_2 + \ldots + b_{1n} \cdot v_n = 0 \\
b_{21} \cdot v_1 + (b_{22} - \alpha) \cdot v_2 + \ldots + b_{1n} \cdot v_n = 0 \\
\ldots\ldots \\
b_{n1} \cdot v_1 + b_{n2} \cdot v_2 + \ldots + (b_{nn} - \alpha) \cdot v_n = 0
\end{gathered}$$

Como existe una solución no trivial $v_1, \ldots, v_n \in \mathbb{C}$, se tiene que el determinante

$$\begin{vmatrix}
b_{11} - \alpha & b_{12} & \ldots & b_{1n} \\
b_{21} & b_{22} - \alpha & \ldots & b_{2n} \\
\ldots & \ldots & \ldots & \ldots \\
b_{n1} & b_{n2} & \ldots & b_{nn} - \alpha
\end{vmatrix}$$

es cero. Al expandir el determinante, podemos ver que α es raíz de un polinomio mónico de grado n con coeficientes en $\mathbb{Z}$.

Teorema 2.1.4 *El conjunto de enteros algebraicos de cualquier cuerpo de números es un anillo.*

Dem: Supongamos que α y β son dos enteros algebraicos, tenemos que probar que $-\alpha$, $\alpha + \beta$ y $\alpha \cdot \beta$ son también enteros algebraicos.

Como α y β son enteros algebraicos, por el segundo apartado del Teorema 2.1.3, tenemos que los grupos aditivos $\mathbb{Z}[\alpha]$, $\mathbb{Z}[\beta]$ son finitamente generados. Si $u_1, \ldots, u_m$ generan $\mathbb{Z}[\alpha]$ y $v_1, \ldots, v_n$ generan $\mathbb{Z}[\beta]$, entonces $\mathbb{Z}[\alpha, \beta] = \langle \alpha^k \cdot \beta^l / \, k, l = 0, 1, \ldots \rangle$ está generado por $\{u_i \cdot v_j / i = 1, \ldots, m; \ j = 1, \ldots n\}$. Por lo tanto, como todas las potencias de $\alpha + \beta$, $\alpha \cdot \beta$ están en un subgrupo finitamente

generado de $\mathbb{C}$, usando el Teorema 2.1.3, podemos concluir que $\alpha+\beta$ y $\alpha\cdot\beta$ son enteros algebraicos.

Como -1 es entero algebraico, usando lo anterior, es obvio que $-\alpha$ será un entero algebraico.

Denotaremos por $\mathfrak{B} = \{\alpha \in \mathbb{C}/\alpha$ es entero algebraico$\}$ al anillo formado por todos los enteros algebraicos.

Teorema 2.1.5 *Sea α un número complejo que es raíz de un polinomio mónico cuyos coeficientes son enteros algebraicos. Entonces, α es un entero algebraico.*

Dem: Supongamos que

$$\alpha^n + \psi_{n-1}\cdot\alpha^{n-1} + \ldots + \psi_0 = 0$$

con $\psi_0, \ldots, \psi_{n-1} \in \mathfrak{B}$.

Vamos a probar que el subanillo Ψ de $\mathfrak{B}$ generado por $\alpha, \psi_0, \ldots, \psi_{n-1}$, $\Psi = \mathbb{Z}[\alpha, \psi_0, \ldots, \psi_{n-1}]$, es un subgrupo aditivo finitamente generado. Sabemos que Ψ está generado como grupo por todos los elementos de la forma

$$\alpha^k \psi_0^{k_0} \psi_1^{k_1} \ldots \psi_{n-1}^{k_{n-1}}$$

donde $k, k_0, \ldots, k_{n-1}$ son enteros no negativos.

Para cada $i = 1, \ldots, n-1$, se tiene que $\psi_i \in \mathfrak{B}$ y entonces por el segundo apartado del Teorema 2.1.3, existe un entero $n_i \geq 0$ tal que $\psi_i^t \in \langle 1, \psi_i, \ldots, \psi_i^{n_i}\rangle$, $\forall t \in \mathbb{N}$.

Por ser $\alpha^n = -\psi_{n-1}\cdot\alpha^{n-1} - \ldots - \psi_1\cdot\alpha - \psi_0$, se cumple que para cada entero $t \geq 0$, α^t es combinación lineal de elementos de la forma $\alpha^r \psi_0^{k_0} \psi_1^{k_1} \ldots \psi_{n-1}^{k_{n-1}}$ con $r < n$. Por lo tanto, todo elemento de la forma $\alpha^k \psi_0^{k_0} \psi_1^{k_1} \ldots \psi_{n-1}^{k_{n-1}}$ con $k, k_0, \ldots, k_{n-1}$ enteros no negativos, es combinación lineal de elementos

$$\alpha^r \psi_0^{r_0} \ldots \psi_{n-1}^{r_n - 1}$$

con $r_i \leq n_i$ para $i = 0, \ldots, n$ y $r < n$.

En conclusión, Ψ está generado por

$$\{\alpha^r \psi_0^{r_0} \ldots \psi_{n-1}^{r_{n-1}} / \; r_i \leq n_i, r < n\}$$

Ahora, aplicando el tercer apartado del Teorema 2.1.3 obtenemos que α es entero algebraico.

2.2. Inclusiones en $\mathbb{C}$

Sea K un cuerpo de números de grado n sobre $\mathbb{Q}$. Es bien conocido que hay exactamente n inclusiones de K en $\mathbb{C}$, las cuales pueden ser descritas fácilmente teniendo en cuenta que $K = \mathbb{Q}(\alpha)$ para algún elemento primitivo α de la extensión $K/\mathbb{Q}$ y observando que cada una de éstas aplica α en alguno de sus n conjugados sobre $\mathbb{Q}$.

Teorema 2.2.1 *Sean K, L dos cuerpos de números tales que $K \subseteq L$. Entonces, cada inclusión de K en $\mathbb{C}$ se extiende a exactamente $[L : K]$ inclusiones de L en $\mathbb{C}$.*

Dem: Como K y L son cuerpos de números, usando el Teorema del Elemento Primitivo podemos escribir $K = \mathbb{Q}(\alpha)$ y $L = K(\beta)$, con $\beta \notin K$.

Para cada uno de los conjugados α_i de α sobre $\mathbb{Q}$ existe un isomorfismo $\sigma_i : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha_i)$ tal que $\sigma_i(\alpha) = \alpha_i$. De igual forma, para cada conjugado β_j de β sobre K, existe un isomorfismo $\tau_j : K(\beta) \to K(\beta_j)$ tal que $\tau_j(\beta) = \beta_j$ y existen, por tanto, $[L : K]$ inclusiones de L en $\mathbb{C}$ que dejan fijo cada elemento de K.

Normalmente, se trabaja con los automorfismos de un cuerpo en lugar de hacerlo con inclusiones en $\mathbb{C}$, ya que los primeros se pueden componer. Un truco habitual para reemplazar inclusiones de un cuerpo de números K en $\mathbb{C}$ por automorfismos es extender estas inclusiones a automorfismos de la clausura normal L de $K/\mathbb{Q}$; así, cada inclusión de K en $\mathbb{C}$ se extiende a $[L : K]$ inclusiones de L, y como $L/\mathbb{Q}$ es normal, todas ellas serán automorfismos de L.

2.3. Traza y Norma

Sea K un cuerpo de números. Vamos a definir dos funciones, a las que llamaremos T (traza) y N (norma) en K de la siguiente forma:

Sean $\sigma_1, \ldots, \sigma_n$ las inclusiones de K en $\mathbb{C}$, donde $[K : \mathbb{Q}] = n$. Para cada $\alpha \in K$, se tiene

$$\begin{aligned} T(\alpha) &= \sigma_1(\alpha) + \ldots + \sigma_n(\alpha) \\ N(\alpha) &= \sigma_1(\alpha) \ldots \sigma_n(\alpha) \end{aligned}$$

Es claro que $T(\alpha)$ y $N(\alpha)$ dependen tanto de α como de K. Por ejemplo, si $K = \mathbb{Q}(\sqrt{3})$, $L = \mathbb{Q}(\sqrt[4]{3})$ y $\alpha = \sqrt{3}$ se cumple que $N_K(\alpha) = -3$ y $N_L(\alpha) = 9$. Por ello, cuando trabajemos con más de un cuerpo, escribiremos $T_K(\alpha)$, $N_K(\alpha)$ para evitar confusiones.

A partir de la definición, es claro que $T(\alpha+\beta) = T(\alpha)+T(\beta)$ y que $N(\alpha\cdot\beta) = N(\alpha)\cdot N(\beta)$ para cada par de elementos $\alpha,\ \beta \in K$. Además, se tiene que para cada $r \in \mathbb{Q}$, $T(r) = n\cdot r,\ N(r) = r^n$. Por lo tanto, también se cumplirá:

$$T(r\cdot\alpha) = r\cdot T(\alpha) \qquad N(r\cdot\alpha) = r^n\cdot N(\alpha) \quad \forall r \in \mathbb{Q},\ \forall \alpha \in K$$

A continuación, vamos a definir otras fórmulas para la traza y la norma que nos ayudarán a demostrar que estas funciones toman siempre valores racionales.

Teorema 2.3.1 *Sea $\alpha \in K$ con $[K:\mathbb{Q}] = n$, $[\mathbb{Q}(\alpha):\mathbb{Q}] = d$ y $t(\alpha), n(\alpha)$, respectivamente, la suma y el producto de los d conjugados de α sobre $\mathbb{Q}$. Entonces,*

$$\begin{aligned} T(\alpha) &= [K:\mathbb{Q}(\alpha)]\cdot t(\alpha) \\ N(\alpha) &= (n(\alpha))^{[K:\mathbb{Q}(\alpha)]} \end{aligned}$$

Dem: Tenemos que $t(\alpha) = T_{\mathbb{Q}(\alpha)}(\alpha)$ y $n(\alpha) = N_{\mathbb{Q}(\alpha)}(\alpha)$.

Teniendo en cuenta que cada inclusión de $\mathbb{Q}(\alpha)$ en $\mathbb{C}$ se extiende exactamente a $\frac{n}{d} = [K:\mathbb{Q}(\alpha)]$ inclusiones de K en $\mathbb{C}$ resultan las fórmulas del enunciado.

Corolario 2.3.1 *$T(\alpha), N(\alpha) \in \mathbb{Q}$.*

Dem: Por el teorema anterior, basta ver que $t(\alpha)$ y $n(\alpha)$ son racionales. Esto es claro ya que $-t(\alpha)$ es el coeficiente que acompaña a x^{d-1} en el polinomio mínimo de α sobre $\mathbb{Q}$ y $\pm n(\alpha)$ su término independiente.

Si α es entero algebraico, su polinomio mínimo sobre $\mathbb{Q}$ tiene coeficientes enteros, de lo que resulta que

Corolario 2.3.2 *Si α es entero algebraico, $T(\alpha)$ y $N(\alpha)$ son números enteros.*

2.4. El discriminante de una n-tupla

Sea K un cuerpo de números tal que $[K:\mathbb{Q}] = n$ y sean $\sigma_1,\ldots,\sigma_n$ las inclusiones de K en $\mathbb{C}$. Para cada n-tupla de elementos $\alpha_1,\ldots,\alpha_n$ se define su discriminante por

$$disc(\alpha_1,\ldots,\alpha_n) = |(\sigma_i(\alpha_j))|^2$$

donde $(\sigma_i(\alpha_j))$ representa la matriz cuyo elemento (i,j) es $\sigma_i(\alpha_j)$

$$(\sigma_i(\alpha_j)) = \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_n) \end{pmatrix}$$

Cabe descatar, que al estar el determinante elevado al cuadrado, es independiente de la ordenación elegida para los σ_i y α_j.

En la sección anterior, hemos probado que si $\alpha \in \mathfrak{B}$, su traza y su norma son números enteros. El siguiente resultado prueba que sucede lo mismo con el discriminante.

Teorema 2.4.1 *$disc(\alpha_1, \ldots, \alpha_n) = |T(\alpha_i\alpha_j)|$*

Dem: Sea $M = (\sigma_i(\alpha_j))$.

$$M^tM = \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_n(\alpha_1) \\ \vdots & & \vdots \\ \sigma_1(\alpha_n) & \ldots & \sigma_n(\alpha_n) \end{pmatrix} \cdot \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_n) \end{pmatrix} =$$

$$= (\sigma_1(\alpha_i\alpha_j) + \ldots + \sigma_n(\alpha_i\alpha_j)) = (T(\alpha_i\alpha_j))$$

Como el determinante de una matriz y su traspuesta es el mismo, se tiene que $|M|^2 = |T(\alpha_i\alpha_j)| = disc(\alpha_1, \ldots, \alpha_n)$.

Corolario 2.4.1 *$disc(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$. Si para cada $i = 1, \ldots, n$, α_i es entero algebraico, $disc(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.*

Ejemplo 2.4.1 *Calcular $disc(1, \sqrt{2}, \sqrt{7}, \sqrt{14})$ en $\mathbb{Q}(\sqrt{2}, \sqrt{7})$.*

$$disc(1, \sqrt{2}, \sqrt{7}, \sqrt{14}) = \begin{vmatrix} 1 & \sqrt{2} & \sqrt{7} & \sqrt{14} \\ 1 & -\sqrt{2} & \sqrt{7} & -\sqrt{14} \\ 1 & \sqrt{2} & -\sqrt{7} & -\sqrt{14} \\ 1 & -\sqrt{2} & -\sqrt{7} & \sqrt{14} \end{vmatrix}^2 = 224^2 = 50176$$

También, podríamos hacer

$$\begin{vmatrix} T(1) & T(\sqrt{2}) & T(\sqrt{7}) & T(\sqrt{14}) \\ T(\sqrt{2}) & T(2) & T(\sqrt{14}) & T(2\cdot\sqrt{7}) \\ T(\sqrt{7}) & T(\sqrt{14}) & T(7) & T(7\cdot\sqrt{2}) \\ T(\sqrt{14}) & T(2\cdot\sqrt{7}) & T(7\cdot\sqrt{2}) & T(14) \end{vmatrix} = \begin{vmatrix} 4 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 \\ 0 & 0 & 28 & 0 \\ 0 & 0 & 0 & 56 \end{vmatrix} = 50176$$

El discriminante nos ayuda a determinar si $\alpha_1, \ldots, \alpha_n$ son linealmente independientes sobre $\mathbb{Q}$.

Teorema 2.4.2 *$disc(\alpha_1, \ldots, \alpha_n) = 0 \Leftrightarrow \alpha_1, \ldots, \alpha_n$ son linealmente dependientes sobre $\mathbb{Q}$.*

Dem: Los $\alpha_1, \ldots, \alpha_n$ son linealmente dependientes sobre $\mathbb{Q}$ si y sólo si lo son las columnas de la matriz $M = (\sigma_i(\alpha_j))$ ya que

$$q_1 \cdot \alpha_1 + \ldots + q_n \cdot \alpha_n = 0 \Leftrightarrow q_1 \cdot \begin{pmatrix} \sigma_1(\alpha_1) \\ \vdots \\ \sigma_n(\alpha_1) \end{pmatrix} + \ldots + q_n \cdot \begin{pmatrix} \sigma_1(\alpha_n) \\ \vdots \\ \sigma_n(\alpha_n) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Nótese que las aplicaciones $\sigma_1, \ldots, \sigma_n$ no modifican a los elementos del cuerpo base $\mathbb{Q}$.

A continuación, daremos un resultado que relaciona los discriminantes de dos bases distintas de un cuerpo de números K.

Teorema 2.4.3 *Sea K un cuerpo de números, y sean $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_n\}$ dos bases distintas de $K/\mathbb{Q}$, se cumple que*

$$disc(\beta_1, \ldots, \beta_n) = |A|^2 disc(\alpha_1, \ldots, \alpha_n)$$

siendo $A = (r_{jk})$ la matriz de cambio de base $\beta_j = \sum_{k=1}^{n} r_{jk} \cdot \alpha_k$.

Dem: Para cada $i, j = 1, \ldots, n$, se tiene

$$\sigma_i(\beta_j) = \sum_{k=1}^{n} r_{jk} \cdot \sigma_i(\alpha_k) = (r_{j1}, \ldots, r_{jn}) \cdot \begin{pmatrix} \sigma_i(\alpha_1) \\ \vdots \\ \sigma_i(\alpha_n) \end{pmatrix}$$

Por lo tanto, para cada $j \in \{1, \ldots, n\}$ se tiene

$$(\sigma_1(\beta_j), \ldots, \sigma_n(\beta_j)) = (r_{j1}, \ldots, r_{jn}) \cdot \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_n(\alpha_1) \\ \vdots & & \vdots \\ \sigma_1(\alpha_n) & \ldots & \sigma_n(\alpha_n) \end{pmatrix}$$

y entonces

$$\begin{pmatrix} \sigma_1(\beta_1) & \ldots & \sigma_n(\beta_1) \\ \vdots & & \vdots \\ \sigma_1(\beta_n) & \ldots & \sigma_n(\beta_n) \end{pmatrix} = \begin{pmatrix} r_{11} & \ldots & r_{1n} \\ \vdots & & \vdots \\ r_{n1} & \ldots & r_{nn} \end{pmatrix} \cdot \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_n(\alpha_1) \\ \vdots & & \vdots \\ \sigma_1(\alpha_n) & \ldots & \sigma_n(\alpha_n) \end{pmatrix}$$

Tomando determinantes y elevando al cuadrado se obtiene la expresión buscada.

Cuando la base está formada por potencias de un único elemento, podemos obtener una expresión para el discriminante relativamente sencilla.

Teorema 2.4.4 *Si $K = \mathbb{Q}(\alpha)$ con $[K : \mathbb{Q}] = n$ y $\alpha_1, \ldots, \alpha_n$ son los conjugados de α sobre $\mathbb{Q}$*

$$disc(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \le r \le s \le n} (\alpha_s - \alpha_r)^2 = \pm N_k(f'(\alpha))$$

siendo $f(x)$ el polinomio mínimo de α sobre $\mathbb{Q}$.

Dem:

- Primera igualdad. Si $\alpha = \alpha_1, \ldots, \alpha_n$ son los conjugados de α, se ordenan los $\sigma_1, \ldots, \sigma_n$ de forma que $\sigma_i(\alpha) = \alpha_i$ para $i = 1, \ldots, n$. Entonces, para la base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ se tiene

$$M = \begin{pmatrix} \sigma_1(1) & \sigma_1(\alpha) & \ldots & \sigma_1(\alpha^{n-1}) \\ \vdots & \vdots & & \vdots \\ \sigma_n(1) & \sigma_n(\alpha) & \ldots & \sigma_n(\alpha^{n-1}) \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \ldots & \alpha_n^{n-1} \end{pmatrix}$$

  que es una matriz de Vandermonde, cuyo determinante está dado por

$$|M| = \prod_{1 \le r \le s \le n} (\alpha_s - \alpha_r)$$

  Por lo tanto, $disc(1, \alpha, \ldots, \alpha^{n-1}) = |M|^2 = \prod_{1 \le r \le s \le n} (\alpha_s - \alpha_r)^2$.

- Segunda igualdad. En primer lugar, observar que

$$\prod_{r<s} (\alpha_s - \alpha_r)^2 = \pm \prod_{r \ne s} (\alpha_s - \alpha_r)$$

  donde el segundo producto se toma sobre los $n \cdot (n-1)$ pares (r, s) con $r \ne s$.

  Por otra parte, $f(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$ y $f'(x) = \Sigma_{i=1}^n \prod_{r \ne i} (x - \alpha_r)$. Entonces, para cada $s = 1, \ldots, n$ es $f'(\alpha_s) = \prod_{r \ne s} (\alpha_s - \alpha_r)$.

  Como $N_K(f'(\alpha)) = \prod_{s=1}^n \sigma_s(f'(\alpha)) = \prod_{s=1}^n f'(\sigma_s(\alpha)) = \prod_{s=1}^n (f'(\alpha_s))$ resulta que

$$N_K(f'(\alpha)) = \prod_{s=1}^n (f'(\alpha_s)) = \prod_{s=1}^n \prod_{r \ne s} (\alpha_s - \alpha_r) = \prod_{r \ne s} (\alpha_s - \alpha_r)$$

  Por lo tanto, $\prod_{r<s} (\alpha_s - \alpha_r)^2 = \pm N_K(f'(\alpha))$.

2.5. Estructura aditiva de un anillo de enteros

Sea K un cuerpo de números con $[K:\mathbb{Q}]=n$. Denotaremos por $\mathfrak{D}=\mathfrak{B}\cap K$ al anillo de enteros algebraicos de K. Usaremos el discriminante para determinar la estructura de $\mathfrak{D}$ como grupo aditivo. En concreto, probaremos que $\mathfrak{D}$ es un grupo abeliano libre de rango n, esto es, existen elementos $\alpha_1,\ldots,\alpha_n\in\mathfrak{D}$ de forma que cada elemento $\alpha\in\mathfrak{D}$ se puede expresar de forma única en la forma $\alpha=a_1\cdot\alpha_1+\ldots+a_n\cdot\alpha_n$ con $a_1,\ldots,a_n\in\mathbb{Z}$, lo que se resume diciendo que $\alpha_1,\ldots,\alpha_n$ forman una $\mathbb{Z}$-base de $\mathfrak{D}$.

Definición 2.5.1 *Se llama base entera de K a cualquier $\mathbb{Z}$-base de $\mathfrak{D}=\mathfrak{B}\cap K$.*

Proposición 2.5.1 *Toda base entera de K es una base de $K/\mathbb{Q}$, y tiene por tanto $n=[K:\mathbb{Q}]$ elementos.*

Dem: Sea $\alpha_1,\ldots,\alpha_n$ una base entera de K y $\alpha\in K$. Por el Teorema 2.1.2, para cada $\alpha\in K$ existe $c\in\mathbb{Z}$ tal que $c\cdot\alpha\in\mathfrak{D}$. Por tanto, $c\cdot\alpha=a_1\cdot\alpha_1+\ldots+a_n\cdot\alpha_n$ con $a_1,\ldots,a_n\in\mathbb{Z}$ y $\alpha=\frac{a_1}{c}\cdot\alpha_1+\ldots+\frac{a_n}{c}\cdot\alpha_n$ con $\frac{a_1}{c},\ldots,\frac{a_n}{c}\in\mathbb{Q}$. Por lo tanto, $\alpha_1,\ldots,\alpha_n$ generan K como $\mathbb{Q}$-espacio vectorial.

Conviene destacar, que es imposible que exista una combinación lineal $q_1\cdot\alpha_1+\ldots+q_n\cdot\alpha_n=0$ con los $q_i\in\mathbb{Q}$ no todos nulos, ya que al quitar los denominadores obtendríamos una combinación lineal nula de los $\alpha_1,\ldots,\alpha_n$ con coeficientes enteros, lo que va en contra de las propiedades de una $\mathbb{Z}$-base.

Sin embargo, no cualquier base de $K/\mathbb{Q}$ formada por enteros algebraicos es una base entera. Por ejemplo, $K=\mathbb{Q}(\sqrt{13})$, $\{1,\sqrt{13}\}$ es una base de $K/\mathbb{Q}$ formada por enteros algebraicos, pero no es una base entera ya que $\frac{1+\sqrt{13}}{2}\in\mathfrak{D}=\mathfrak{B}\cap K$ (es raíz de x^2-x-3) y $\frac{1+\sqrt{13}}{2}\notin\mathbb{Z}[\sqrt{13}]=\{a+b\cdot\sqrt{13}/a,b\in\mathbb{Z}\}$.

Lo anterior muestra la necesidad de demostrar la existencia de bases enteras en cada cuerpo de números.

Teorema 2.5.1 *Todo cuerpo de números posee una base entera. Por lo tanto, el anillo de enteros $\mathfrak{D}$ de K es un grupo abeliano libre de rango $n=[K:\mathbb{Q}]$ y cualquier subgrupo G de $\mathfrak{D}$ es abeliano libre con rango $\leq n$.*

Dem: Sabemos que K puede expresarse como $K=\mathbb{Q}(\alpha)$ con α entero algebraico. Si $n=[K:\mathbb{Q}]$, $\{1,\alpha,\ldots,\alpha^n\}$ es una base de $K/\mathbb{Q}$ formada por enteros algebraicos y cuyo discriminante es un número entero por el Corolario 2.4.1. Escogemos ahora entre todas las bases de $K/\mathbb{Q}$ formadas por enteros algebraicos una $\{\beta_1,\ldots,\beta_n\}$ tal que $|disc(\beta_1,\ldots,\beta_n)|$ sea minimal.

$\{\beta_1,\ldots,\beta_n\}$ es base de $K/\mathbb{Q}$ y, si no es base entera, existe $\beta\in\mathfrak{D}=\mathfrak{B}\cap K$ de forma que $\beta=a_1\cdot\beta_1+\ldots+a_n\cdot\beta_n$ con $a_i\in\mathbb{Q}$ y no todos los $a_i\in\mathbb{Z}$.

Reordenando los $\beta_1, \ldots, \beta_n$ se puede suponer que $a_1 \notin \mathbb{Z}$ y escribir $a_1 = a + r$ con $a \in \mathbb{Z}$ y $0 < r < 1$.

Sean ahora $\gamma_1 = \beta - a \cdot \beta_1$ y $\gamma_i = \beta_i$ para $i = 2, \ldots, n$. Entonces $\{\gamma_1, \ldots, \gamma_n\}$ es una base de $K/\mathbb{Q}$ formada por enteros algebraicos. El determinante de la matriz de cambio de base es

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

y por el Teorema 2.4.3, sabemos que $disc(\gamma_1, \ldots, \gamma_n) = r^2 disc(\beta_1, \ldots, \beta_n) < disc(\beta_1, \ldots, \beta_n)$, lo que contradice la elección de $\beta_1, \ldots, \beta_n$.

Por tanto $\{\beta_1, \ldots, \beta_n\}$ es una base entera y $\mathfrak{D}$ es un grupo abeliano libre de rango n.

Corolario 2.5.1 *Dos bases enteras de K tienen el mismo discriminante.*

Dem: Basta tener en cuenta que la matriz de cambio de base en un grupo abeliano libre de rango r es una matriz de $M_r(\mathbb{Z})$ que tiene inversa en $M_r(\mathbb{Z})$. Por lo tanto, su determinante ha de ser ± 1. Teniendo en cuenta lo anterior, el resultado se deduce directamente del Teorema 2.4.3.

Definición 2.5.2 *Se define el discriminante de K como el de cualquiera de sus bases enteras.*

Teorema 2.5.2 *Si $\{\alpha_1, \ldots, \alpha_n\}$ es una base de $K/\mathbb{Q}$ contenida en $\mathfrak{D}$ y $d = disc(\alpha_1, \ldots, \alpha_n)$, cada $\alpha \in \mathfrak{D}$ se puede expresar en la forma $\frac{m_1 \cdot \alpha_1 + \ldots + m_n \cdot \alpha_n}{d}$ con $m_1, \ldots, m_n \in \mathbb{Z}$ y d divisor de m_j^2 para cada $j = 1, \ldots, n$.*

Dem: Si $\alpha \in \mathfrak{D}$, podemos expresarlo en función de la base de K, esto es, $\alpha = q_1 \cdot \alpha_1 + \ldots + q_n \cdot \alpha_n$ con $q_1, \ldots, q_n \in \mathbb{Q}$. Si $\sigma_1, \ldots, \sigma_n$ son las inclusiones de K en $\mathbb{C}$, aplicando cada uno de los σ_i a la ecuación anterior obtenemos el siguiente sistema

$$\begin{array}{rcl} \sigma_1(\alpha) & = & q_1 \cdot \sigma_1(\alpha_1) + \ldots + q_n \cdot \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha) & = & q_1 \cdot \sigma_n(\alpha_1) + \ldots + q_n \sigma_n \cdot (\alpha_n) \end{array}$$

Usando la Regla Cramer para resolver el sistema, resulta que $q_j = \frac{\gamma_j}{\delta}$ donde $\delta = |(\sigma_i(\alpha_j))|$ y γ_j se obtiene de δ reemplazando la columna j por los $\sigma_i(\alpha)$. Es obvio que γ_j y δ son enteros algebraicos y que además $\delta^2 = d$.

De $\delta q_j = \gamma_j$ resulta que $dq_j = \delta\gamma_j$. Por lo tanto, $dq_j \in \mathbb{Q}$ y es entero algebraico, entonces $dq_j \in \mathbb{Z}$ por el Corolario 2.1.1. Por consiguiente, para cada j, es $q_j = \frac{m_j}{d}$ con $m_j \in \mathbb{Z}$.

Entonces, $\alpha = \frac{m_1 \cdot \alpha_1 + \ldots + m_n \cdot \alpha_n}{d}$ con $m_j \in \mathbb{Z}$.

Queda por demostrar que $d|m_j^2$. Dado que $\frac{m_j^2}{d} \in \mathbb{Q}$, para probar que es entero, basta ver que es entero algebraico. Sustituyendo, llegamos al resultado buscado

$$\frac{m_j^2}{d} = \frac{d^2 q_j^2}{d} = dq_j^2 = (\delta q_j)^2 = \gamma_j^2$$

2.6. Cálculo de bases enteras

Los resultados que se presentan en esta sección, nos permitirán calcular bases enteras de un cuerpo de números.

Teorema 2.6.1 *Sea K un cuerpo de números de grado n, $\{\alpha_1, \ldots, \alpha_n\}$ una base de $K/\mathbb{Q}$ formada por enteros algebraicos y $G = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ el subgrupo de $\mathfrak{D} = \mathfrak{B} \cap K$ generado por $\alpha_1, \ldots, \alpha_n$. Entonces, el grupo $\mathfrak{D}/G$ es finito y*

$$disc(\alpha_1, \ldots, \alpha_n) = |\mathfrak{D}/G|^2 disc\ \mathfrak{D}$$

Dem: Denotamos $\mathbb{Z}\alpha_i = \{n \cdot \alpha_i / n \in \mathbb{Z}\}$.

Teniendo en cuenta que tanto G como $\mathfrak{D}$ tienen rango n, el Teorema de las Bases para subgrupos de un grupo abeliano libre (ver [9]), asegura que existe una base $\{\beta_1, \ldots, \beta_n\}$ de $\mathfrak{D}$ y enteros positivos $d_1, \ldots, d_n$ tales $d_1|d_2| \ldots |d_n$ y $\{d_1\beta_1, \ldots, d_n\beta_n\}$ es base de G.

Puesto que $\{\alpha_1, \ldots, \alpha_n\}$ y $\{d_1\beta_1, \ldots, d_n\beta_n\}$ son dos bases de G, la matriz de cambio de base tiene determinante ± 1 y entonces, por el Teorema 2.4.3, se cumple que

$$disc(\alpha_1, \ldots, \alpha_n) = disc(d_1\beta_1, \ldots, d_n\beta_n)$$

Por otro lado,

$$disc(d_1\beta_1, \ldots, d_n\beta_n) = (d_1 \ldots d_n)^2 disc(\beta_1, \ldots, \beta_n)$$

y como $|\mathfrak{D}/G| = d_1 \ldots d_n$ tenemos que

$$disc(\alpha_1, \ldots, \alpha_n) = |\mathfrak{D}/G|^2 disc(\beta_1, \ldots, \beta_n)$$

Corolario 2.6.1 *Sea K un cuerpo de números de grado n y sea $\{\alpha_1, \ldots, \alpha_n\}$ una base de $K/\mathbb{Q}$ formada por enteros algebraicos y G el subgrupo de $\mathfrak{D} = \mathfrak{B} \cap K$ generado por $\alpha_1, \ldots, \alpha_n$. Si $disc(\alpha_1, \ldots, \alpha_n)$ es libre de cuadrados, es $G = \mathfrak{D}$.*

Teorema 2.6.2 *Sea K un cuerpo de números de grado n, G un subgrupo aditivo de $\mathfrak{D}$ de rango n y $\{\alpha_1, \ldots, \alpha_n\}$ una base de G. Si $G \neq \mathfrak{D}$, existe un primo racional p y un entero algebraico de la forma $\frac{1}{p}(r_1 \cdot \alpha_1 + \ldots + r_n \cdot \alpha_n)$ con $r_i \in \mathbb{Z}$, $0 \leq r_i \leq p-1$ tal que p^2 divide a $disc(\alpha_1, \ldots, \alpha_n)$.*

Dem: Si $G \neq \mathfrak{D}$, es $|\mathfrak{D}/G| > 1$ y existe un primo racional p tal que $p \,|\, |\mathfrak{D}/G|$ y un elemento $u + G \in \mathfrak{D}/G$ de orden p. Entonces, $u \in \mathfrak{D} \setminus G$ y $g = pu \in G$. Por el Teorema 2.6.1, p^2 divide a $disc(\alpha_1, \ldots, \alpha_n)$. Además, existen enteros $a_1, \ldots, a_n$ de forma que $pu = a_1 \cdot \alpha_1 + \ldots + a_n \cdot \alpha_n$ de donde $u = \frac{1}{p}(a_1 \cdot \alpha_1 + \ldots + a_n \cdot \alpha_n)$.

Si se representan por $r_1, \ldots, r_n$ los respectivos restos de la división de $a_1, \ldots, a_n$ por p y por $q_1, \ldots, q_n$ los respectivos cocientes, resulta que

$$u = q_1 \cdot \alpha_1 + \ldots + q_n \cdot \alpha_n + \frac{1}{p}(r_1 \cdot \alpha_1 + \ldots r_n \cdot \alpha_n)$$

de donde $u - (q_1 \cdot \alpha_1 + \ldots + q_n \cdot \alpha_n) = \frac{1}{p}(r_1 \cdot \alpha_1 + \ldots + r_n \cdot \alpha_n)$ es entero algebraico y $0 \leq r_i \leq p-1$ para cada $i = 1, \ldots, n$.

Proposición 2.6.1 *Si G es un subgrupo de $\mathfrak{D}$ con base $\{\alpha_1, \ldots, \alpha_n\}$, p un primo, $a_1, \ldots, a_n \in \mathbb{Z}$, $\beta = \frac{1}{p}(a_1\alpha_1 + \ldots + a_n\alpha_n) \in \mathfrak{D} \setminus G$ y $G' = \langle \alpha_1, \ldots, \alpha_n, \beta \rangle$ se cumple que $G < G' \leq \mathfrak{D}, p^2 \,|\, disc\ G$ y $disc\ G' = \frac{disc\ G}{p^2}$.*

Dem: Como $\beta \in G' \setminus G$ y $p\beta \in G$, es claro que $\beta + G \in G'/G$ tiene orden p. Por lo tanto, p divide a $|G'/G|$ y a $|\mathfrak{D}/G|$. Entonces, como $disc\ G = |\mathfrak{D}/G|^2 disc\ \mathfrak{D}$, tenemos que $p^2 \,|\, disc\ G$. Por otro lado, es obvio por definición de G y G' que $G'/G = \langle \beta + G \rangle$ es un grupo de orden p. Entonces por el Teorema 2.6.2, resulta que

$$disc\ G' = |\mathfrak{D}/G'|^2 disc\ \mathfrak{D} = \frac{|\mathfrak{D}/G|^2}{|G'/G|^2}\ disc\ \mathfrak{D} = \frac{disc\ G}{p^2}$$

La Proposición anterior puede usarse para determinar elementos en $\mathfrak{D} \setminus G$ por el método ensayo-error a partir de un subgrupo G conocido hasta obtener una base entera de K. Destacar que el resultado asegura que sólo hay que ensayar un número finito de posibilidades para $\frac{1}{p}(r_1 \cdot \alpha_1 + \ldots + r_n \cdot \alpha_n)$. El método será el siguiente:

1. Elegir una base de $K/\mathbb{Q}$ formada por enteros algebraicos $\{\alpha_1, \ldots, \alpha_n\}$ que será base de un cierto subgrupo G de $\mathfrak{D}$.

2. Calcular $disc(\alpha_1, \ldots, \alpha_n) = disc\ G$.

3. Si *disc* G es libre de cuadrados, se ha encontrado una base entera por el Corolario 2.6.1. En otro caso, para cada primo p cuyo cuadrado divide a *disc* G, hay que buscar algún entero algebraico entre todos los números de la forma $\frac{1}{p}(r_1 \cdot \alpha_1 + \ldots + r_n \cdot \alpha_n)$ con $0 \leq r_i \leq p-1$.

4. Si se obtienen nuevos enteros algebraicos, ampliar G con ellos hasta obtener un nuevo subgrupo G' y considerar *disc* G'.

5. Se repite el proceso hasta que no se obtengan nuevos enteros algebraicos.

Ejemplo 2.6.1 *Determinar el anillo de enteros del cuerpo de números* $K = \mathbb{Q}(\sqrt[3]{5})$.

Si $\alpha = \sqrt[3]{5}$, $\{1, \alpha, \alpha^2\}$ es una base de $K/\mathbb{Q}$, $\alpha \in \mathfrak{D}$ y $\mathbb{Z}[\alpha] \subseteq \mathfrak{D}$. Consideramos $G = \langle 1, \alpha, \alpha^2 \rangle$ y calculamos $disc\ G = disc(1, \alpha, \alpha^2)$.

Si denotamos $\epsilon = e^{2\pi i/3}$, se tiene

$$\begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha\epsilon & \alpha^2\epsilon^2 \\ 1 & \alpha\epsilon^2 & \alpha^2\epsilon \end{vmatrix}^2 = \alpha^6 \begin{vmatrix} 1 & 1 & 1 \\ 1 & \epsilon & \epsilon^2 \\ 1 & \epsilon^2 & \epsilon \end{vmatrix}^2 = 5^2(3\epsilon^2 - 3\epsilon)^2 = 5^2 3^2(\epsilon^2 - \epsilon)^2$$

Como $\epsilon^2 = -\epsilon - 1$ (raíz del polinomio ciclotómico $x^2 + x + 1 = 0$), $(\epsilon^2 - \epsilon)^2 = (-2\epsilon - 1)^2 = 4(\epsilon^2 + \epsilon) + 1 = -3$ y entonces $disc(1, \alpha, \alpha^2) = -3^3 5^2$.

Por el Teorema 2.6.2, solo hay dos posibles valores $p = 3, 5$.

1. $p = 3$: Se trata de averiguar si existe $\beta \in \mathfrak{D}$ tal que $\beta = \frac{1}{3}(\lambda_1 + \lambda_2\alpha + \lambda_3\alpha^2)$ con $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}$ y $0 \leq \lambda_1, \lambda_2, \lambda_3 \leq 2$.

   En este caso, $\beta = \frac{1}{3}(\lambda_1 + \lambda_2\alpha + \lambda_3\alpha^2) \in \mathfrak{D}$ implica que $T(\beta) \in \mathbb{Z}$ y $N(\beta) \in \mathbb{Z}$. Como $T(\beta) = \lambda_1 \in \mathbb{Z}$, la información debe obtenerse de $N(\beta)$.

   $N(\beta) = \frac{1}{27}(\lambda_1 + \lambda_2\alpha + \lambda_3\alpha^2)(\lambda_1 + \lambda_2\alpha\epsilon + \lambda_3\alpha^2\epsilon^2)(\lambda_1 + \lambda_2\alpha\epsilon + \lambda_3\alpha^2\epsilon) =$
   $= \frac{1}{27}(\lambda_1^3 - 15\lambda_1\lambda_2\lambda_3 + 5\lambda_3^2 + 25\lambda_3^3)$

   Por lo tanto, debe ser $\frac{1}{27}(\lambda_1^3 - 15\lambda_1\lambda_2\lambda_3 + 5\lambda_3^2 + 25\lambda_3^3) \in \mathbb{Z}$ y

   $$\lambda_1^3 - 15\lambda_1\lambda_2\lambda_3 + 5\lambda_3^2 + 25\lambda_3^3 \equiv 0\ (mod\ 27)$$

   - $\lambda_1 = 0 \Rightarrow 5\lambda_2^3 + 25\lambda_3^3 \equiv 0\ (mod\ 27)$. Entonces
     $\lambda_2 = 0 \Rightarrow \lambda_3^3 \equiv 0\ (mod\ 27) \Rightarrow \lambda_3 \equiv 0\ (mod\ 3) \Rightarrow \lambda_3 = 0$.
     $\lambda_2 = 1 \Rightarrow 5 + 25\lambda_3^3 \equiv 0\ (mod\ 27)$ y no existe $\lambda_3 \in \{0, 1, 2\}$.
     $\lambda_2 = 2 \Rightarrow -14 + 25\lambda_3^3 \equiv 0\ (mod\ 27)$ y no existe $\lambda_3 \in \{0, 1, 2\}$.
   - $\lambda_1 = 1 \Rightarrow 1 - 15\lambda_2\lambda_3 + 5\lambda_2^3 + 25\lambda_3^3 \equiv 0$. Entonces
     $\lambda_2 = 0 \Rightarrow 1 + 25\lambda_3^3 \equiv 0\ (mod\ 27)$ y no existe $\lambda_3 \in \{0, 1, 2\}$.
     $\lambda_2 = 1 \Rightarrow 6 - 15\lambda_3 + 25\lambda_3^3 \equiv 0\ (mod\ 27)$ y no existe $\lambda_3 \in \{0, 1, 2\}$.
     $\lambda_2 = 2 \Rightarrow 14 - 3\lambda_3 + 25\lambda_3^3 \equiv 0\ (mod\ 27)$ y no existe $\lambda_3 \in \{0, 1, 2\}$.

- $\lambda_1 = 2 \Rightarrow 8 - 3\lambda_2\lambda_3 + 5\lambda_2^3 + 25\lambda_3^3 \equiv 0\,(mod\,27)$. Entonces
  $\lambda_2 = 0 \Rightarrow 8 + 25\lambda_3^3 \equiv 0\,(mod\,27)$ y no existe $\lambda_3 \in \{0,1,2\}$.
  $\lambda_2 = 1 \Rightarrow 13 - 3\lambda_3 + 25\lambda_3^3 \equiv 0\,(mod\,27)$ y no existe $\lambda_3 \in \{0,1,2\}$.
  $\lambda_2 = 2 \Rightarrow -6 - 6\lambda_3 + 25\lambda_3^3 \equiv 0\,(mod\,27)$ y no existe $\lambda_3 \in \{0,1,2\}$.

2. $p = 5$: Se busca ahora un $\beta \in \mathfrak{D}$ tal que $\beta = \frac{1}{5}(\lambda_1 + \lambda_2\alpha + \lambda_3\alpha^2)$ con $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}$ y $0 \leq \lambda_1, \lambda_2, \lambda_3 \leq 4$.

   Si $\beta = \frac{1}{5}(\lambda_1 + \lambda_2\alpha + \lambda_3\alpha^2) \in \mathfrak{D}, T(\beta) = \frac{3\lambda_1}{5} \in \mathbb{Z}$; entonces $\lambda_1 \equiv 0\,(mod\,5)$ y $\lambda_1 = 0$. Por tanto, $\beta = \frac{1}{5}(\lambda_2\alpha + \lambda_3\alpha^2)$. Como $N(\beta) \in \mathbb{Z}$, se tiene que

$$N(\beta) = \frac{1}{125}(5\lambda_2^3 + 25\lambda_3^3) = \frac{1}{25}(\lambda_2^3 + 5\lambda_3^3) \Rightarrow \lambda_2^3 + 5\lambda_3^3 \equiv 0\,(mod\,25)$$

   Entonces $\lambda_2^3 \equiv 0\,(mod\,5)$ y $\lambda_2 = 0$, de donde $5\lambda_3^3 \equiv 0\,(mod\,25)$, $\lambda_3 \equiv 0\,(mod\,5)$ y $\lambda_3 = 0$.

   Como no han aparecido nuevos enteros algebraicos, se concluye que $G = \mathfrak{D}$ y que $\{1, \alpha, \alpha^2\}$ es una base entera de K.

2.7. Casos Particulares

En esta sección se estudiarán los discriminantes y las bases enteras de dos clases bien conocidas de cuerpos de números, cuyos anillos de enteros son extensiones simples de $\mathbb{Z}$ y por tanto proporcionan dos colecciones infinitas de ejemplos de cuerpos de números en los que se puede aplicar el teorema objeto de este trabajo: la clase formada por los cuerpos ciclotómicos $\mathbb{Q}(\omega)$ donde ω es cualquier raíz primitiva m-ésima de la unidad y la de los cuerpos cuadráticos, es decir, los de la forma $\mathbb{Q}(\sqrt{m})$ con $m \in \mathbb{Z}$ libre de cuadrados. Los cuerpos cuadráticos correspondientes a los $m > 0$ se llaman cuerpos cuadráticos reales y los correspondientes a los $m < 0$, se llaman cuerpos cuadráticos imaginarios.

2.7.1. Cuerpos cuadráticos

Definición 2.7.1 *Un cuerpo cuadrático es un cuerpo de números K tal que $[K : \mathbb{Q}] = 2$.*

Por lo tanto, será $K = \mathbb{Q}(\theta)$ donde θ es un entero algebraico que satisface una ecuación de la forma

$$x^2 + ax + b = 0\,(a, b \in \mathbb{Z})$$

Resolviendo la ecuación anterior, obtenemos

$$\theta = \frac{-a \pm \sqrt{(a^2 - 4b)}}{2}$$

Sea $a^2 - 4b = r^2 m$ con $r, m \in \mathbb{Z}$ y siendo m libre de cuadrados. Entonces

$$\theta = \frac{-a \pm r\sqrt{m}}{2}$$

y se tiene que $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{m})$. Con lo anterior, podemos caracterizar los cuerpos cuadráticos de la siguiente forma:

Proposición 2.7.1 *Los cuerpos cuadráticos son aquellos de la forma $\mathbb{Q}(\sqrt{m})$ con $m \in \mathbb{Z}$ libre de cuadrados.*

A continuación, se determinará el anillo de enteros de cualquier cuerpo cuadrático.

Teorema 2.7.1 *Sea $m \in \mathbb{Z}$ libre de cuadrados. Entonces, el anillo de enteros algebraicos de $\mathbb{Q}(\sqrt{m})$ es:*

1. $\mathbb{Z}[\sqrt{m}]$ *si* $m \not\equiv 1 (mod\, 4)$
2. $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ *si* $m \equiv 1 (mod\, 4)$

Dem: Sea $\alpha = r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$, con $r, s \in \mathbb{Q}$. Si $s \neq 0$, $\alpha^2 - 2r\alpha = ms^2 - r^2$ y el polinomio mínimo de α sobre $\mathbb{Q}$ es $x^2 - 2rx + r^2 - ms^2$. Por lo tanto, α es un entero algebraico si y sólo si $2r$ y $r^2 - ms^2$ son números enteros.

Si $\alpha \in \mathbb{Q}(\sqrt{m})$ es un entero algebraico, se deduce de lo anterior que $2r \in \mathbb{Z}$ y $r^2 - ms^2 \in \mathbb{Z}$. Entonces, $4r^2 \in \mathbb{Z}$ y $4s^2 m = (2s)^2 m \in \mathbb{Z}$. Como m es libre de cuadrados, resulta ahora que $2s \in \mathbb{Z}$.

A continuación, sustituyendo $a = 2r$, $b = 2s$, se tiene que $r^2 - ms^2 \in \mathbb{Z} \Rightarrow 4|(a^2 - mb^2)$. Ahora, si $m \equiv 2, 3\ (mod\, 4)$, entonces

$$a^2 - mb^2 \equiv a^2 + 2b^2,\ a^2 + b^2\ (mod\, 4)$$

Para que la expresión anterior sea divisible por 4, es necesario que a, b sean números pares, lo que implica que $r, s \in \mathbb{Z}$. Por lo tanto, tenemos que el anillo de enteros algebraicos para el caso $m \equiv 2, 3\ (mod\, 4)$ es $\mathbb{Z}[\sqrt{m}]$.

Si $m \equiv 1\ (mod\, 4)$, entonces $a^2 - mb^2 \equiv a^2 - b^2\ (mod\, 4)$, pero $4|(a^2 - b^2)$ si y sólo si $a \equiv b\ (mod\, 2)$, por lo que se obtiene el anillo de enteros algebraicos

$$\mathcal{D} = \left\{ \frac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z} \text{ y } a \equiv b\ (mod\, 2) \right\}$$

Podemos escribir cada elemento de $\mathcal{D}$ de la siguiente forma

$$\frac{1}{2}(a + b\sqrt{m}) = \frac{a - b}{2} + b(\frac{1 + \sqrt{m}}{2})$$

Como a y b tienen la misma paridad, se tiene que $\frac{a-b}{2} \in \mathbb{Z}$ y entonces $\mathcal{D} \subseteq \mathbb{Z} + \frac{1+\sqrt{m}}{2}\mathbb{Z}$. Para ver el otro contenido, basta tener en cuenta que $\frac{1+\sqrt{m}}{2} \in \mathcal{D}$. Por lo tanto, $\mathcal{D} = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$.

Si $K = \mathbb{Q}(\sqrt{m})$, los monomorfismos de $K \to \mathbb{C}$ son:

$$\sigma_1(r + s\sqrt{m}) = r + s\sqrt{m}$$

$$\sigma_2(r + s\sqrt{m}) = r - s\sqrt{m}$$

A continuación, calcularemos el valor del discriminante de K.

Teorema 2.7.2 *Sea $K = \mathbb{Q}(\sqrt{m})$. Si $m \not\equiv 1\,(mod\,4)$, $\{1, \sqrt{m}\}$ es base entera de K y su discriminante es $4m$. Si $m \equiv 1\,(mod\,4)$, $\{1, \frac{1+\sqrt{m}}{2}\}$ es base entera de K y su discriminante es m.*

Dem: Las bases se deducen directamente del Teorema 2.7.1. Para los discriminantes, calculamos directamente su valor

$$\begin{vmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{vmatrix}^2 = (-2\sqrt{m})^2 = 4m,$$

$$\begin{vmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{vmatrix}^2 = (-\sqrt{m})^2 = m.$$

También, es bastante sencillo el cálculo de la traza y la norma en los cuerpos cuadráticos:

$$N(r + s\sqrt{m}) = r^2 - ms^2$$

$$T(r + s\sqrt{m}) = 2r$$

2.7.2. Cuerpos ciclotómicos

Definición 2.7.2 *Si m es un entero positivo y ω una raíz primitiva m-ésima de la unidad, se llama m-ésimo cuerpo ciclotómico al cuerpo $\mathbb{Q}(\omega)$.*

A continuación, probaremos dos Lemas y una Proposición que nos servirán para calcular el anillo de enteros algebraicos de $\mathbb{Q}(\omega)$.

Lema 2.7.1 *Si $m \geq 3$, $\mathbb{Z}[1-\omega] = \mathbb{Z}[\omega]$ y $disc(1-w) = disc(w)$.*

Dem: En primer lugar, es obvio que $\mathbb{Z}[1-\omega] = \mathbb{Z}[\omega]$ ya que $\omega = 1-(1-\omega)$. Para probar la igualdad de los discriminantes, basta observar que cuando α_i recorre todos los conjugados de ω, $1-\alpha_i$ recorre todos los conjugados de $1-\omega$. Por lo tanto, usando la primera igualdad del Teorema 2.4.4, tenemos que

$$disc(\omega) = \prod_{1\leq r<s\leq n} (\alpha_r - \alpha_s)^2 = \prod_{1\leq r<s\leq n} ((1-\alpha_r) - (1-\alpha_s))^2 = disc(1-\omega)$$

Como se puede comprobar en el Ejercicio 23 del Capítulo 2 de [3], cuando m es un entero positivo cualquiera existe una expresión bastante complicada para obtener el valor de $disc(w)$. Sin embargo, es sencillo probar que $disc(w)$ divide a $m^{\varphi(m)}$.

Proposición 2.7.2 *Si ω es una raíz primitiva m-ésima de la unidad, entonces $disc(\omega)$ divide a $m^{\varphi(m)}$.*

Dem: Si $f(x)$ es el polinomio mínimo de ω sobre $\mathbb{Q}$, existe $g(x) \in \mathbb{Q}[x]$ tal que $x^m - 1 = f(x)\cdot g(x)$. Haciendo la derivada y sustituyendo x por ω, se obtiene

$$mx^{m-1} = f'(x)g(x) + f(x)g'(x) \qquad m\omega^{m-1} = f'(\omega)g(\omega) \qquad m = \omega f'(\omega)g(\omega)$$

Tomando normas y aplicando la segunda igualdad del Teorema 2.4.4 resulta que

$$m^{\varphi(m)} = N(f'(\omega))N(\omega g(\omega)) = \pm disc(\omega)N(\omega g(\omega))$$

con $disc(\omega) \in \mathbb{Z}$ y $N(\omega g(\omega)) \in \mathbb{Z}$ ya que $g(x) \in \mathbb{Z}[x]$. Por lo tanto, $disc(\omega)$ divide a $m^{\varphi(m)}$.

En lo que sigue se calcula el discriminante para el caso particular en el que m es potencia de un primo p.

Lema 2.7.2 *Si $m = p^r$ con p primo racional y $K = \mathbb{Q}(\omega)$, $N_K(1-w) = p$.*

Dem: El polinomio mínimo de ω sobre $\mathbb{Q}$ es

$$\phi_{p^r} = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \ldots + x^{(p-1)p^{r-1}}$$

y sus raíces en $\mathbb{C}$ son los w^k donde $k \in \{1,\ldots,m-1\}$ y $m.c.d.(k,m) = 1$.

Por lo tanto, $N_k(1-\omega) = \prod_k (1-\omega^k) = \phi_{p^r}(1) = p$.

Utilizando la Proposición y los Lemas anteriores, podemos probar que cuando m es potencia de primo, el anillo de enteros de $\mathbb{Q}(\omega)$ es $\mathbb{Z}[\omega]$.

Teorema 2.7.3 *Si $m = p^r$, p primo y ω una raíz primitiva m-ésima de la unidad, $\mathfrak{B} \cap \mathbb{Q}(\omega) = \mathbb{Z}[w]$.*

Dem: Los elementos $1-\omega, \ldots, (1-\omega)^n$ con $n = \varphi(p^r)$ son enteros algebraicos y forman una base de $\mathbb{Q}(\omega)$. Por lo tanto, por el Teorema 2.5.2, cada $\alpha \in \mathfrak{D} = \mathfrak{B} \cap \mathbb{Q}(\omega)$ puede expresarse de la forma $\alpha = \frac{m_1+m_2\cdot(1-\omega)+\ldots+m_n\cdot(1-\omega)^{n-1}}{d}$ con $n = \varphi(p^r)$, $m_1, \ldots, m_n \in \mathbb{Z}$ y $d = disc(1-\omega) = disc(\omega)$ por el Lema 2.7.1. En la Proposición 2.7.2, hemos visto que $disc(\omega)$ divide a $m^{\varphi(m)}$, por lo que, en este caso d es potencia de p.

Probando que $\mathfrak{D} = \mathbb{Z}[1-\omega]$, se deducirá el resultado aplicando el Lema 2.7.1. Si $\mathfrak{D} \neq \mathbb{Z}[1-\omega]$, existirá algún $\alpha \in \mathfrak{D}$ de forma que no todos los correspondientes m_i sean divisibles por d y por lo tanto, no estén en $\mathbb{Z}[1-\omega]$. Entonces, existe $\beta \in \mathfrak{D}$ de la forma

$$\beta = \frac{m_i \cdot (1-\omega)^{i-1} + m_{i+1} \cdot (1-\omega)^i + \ldots + m_n \cdot (1-\omega)^{n-1}}{p}$$

para algún $i \leq n$ y enteros $m_i, m_{i+1}, \ldots, m_n$ tales que p no divide a m_i.

Dado que, para todo k, $1-\omega^k$ es divisible por $(1-\omega)$, del Lema 2.7.2 se deduce que $(1-\omega)^n$ es divisor de p en $\mathbb{Z}[\omega]$. Por lo tanto, $\frac{p}{(1-\omega)^i} \in \mathbb{Z}[\omega]$ y

$$\beta\frac{p}{(1-\omega)^i} = \frac{m_i}{1-\omega} + m_{i+1} + \ldots + m_n \cdot (1-\omega)^{n-1-i} \in \mathfrak{D}$$

Suprimiendo ahora los sumandos que obviamente están en $\mathfrak{D}$, resulta que $\frac{m_i}{1-\omega} \in \mathfrak{D}$. Entonces $N_{\mathbb{Q}(\omega)}(1-\omega)$ divide a $N_{\mathbb{Q}(\omega)}(m_i) = m_i^n$ en $\mathbb{Z}$. Sin embargo, esto imposible ya que por el Lema 2.7.2 sabemos que $N_{\mathbb{Q}(\omega)}(1-\omega) = p$.

El resultado anterior, es válido para cualquier valor de m. Sin embargo, la demostración del resultado general, queda fuera del alcance de este trabajo. Puede encontrarse la demostración completa en [3] (Corolario 2 del Capítulo 2).

Capítulo 3

Factorización de Enteros Algebraicos

3.1. El problema de factorizar en irreducibles

En esta sección demostraremos que el anillo de enteros $\mathfrak{D}$ de un cuerpo de números K es noetheriano, lo que asegura que cada elemento no unidad de $\mathfrak{D}^*$ se puede expresar como producto de un número finito de elementos irreducibles. Probaremos también, que esta expresión no es única en general.

Definición 3.1.1 *Se dice que un dominio de integridad D es noetheriano si todos los ideales de D son finitamente generados.*

Proposición 3.1.1 *Las siguientes condiciones son equivalentes para cualquier dominio de integridad D:*

1. *D es noetheriano.*
2. *D satisface la condición de cadena ascendente, es decir, dada una cadena ascendente de ideales*

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_n \subseteq \ldots$$

   existe algún N tal que $\mathfrak{a}_n = \mathfrak{a}_N$ para todo $n \geq N$.

3. *Todo conjunto no vacío de ideales de D tiene un elemento maximal.*

Dem: Supongamos que D es noetheriano. Consideramos la siguiente cadena ascendente de ideales

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_n \subseteq \ldots$$

Sea $\mathfrak{a} = \cup_{n=1}^{\infty} \mathfrak{a}_n$. Tenemos que $\mathfrak{a}$ es un ideal y es finitamente generado, esto es, $\mathfrak{a} = (x_1, \ldots, x_m)$. Cada uno de los x_i pertenece a algún $\mathfrak{a}_{n(i)}$. Si denotamos

por $N = max_i\, n(i)$, entonces tenemos que $\mathfrak{a} = \mathfrak{a}_N$, de lo que se deduce que $\mathfrak{a}_n = \mathfrak{a}_N$ para todo $n \geq N$ y queda probado que (1) implica (2).

Ahora, supongamos que se satisface la condición de cadena ascendente, y sea S un conjunto no vacío de ideales que no tiene elemento maximal. Sea $\mathfrak{a}_0 \in S$, como $\mathfrak{a}_0$ no es maximal, podemos escoger $\mathfrak{a}_1 \in S$ con $\mathfrak{a}_0 \subsetneq \mathfrak{a}_1$. Repitiendo el proceso, obtendremos, para cada entero positivo $n \geq 1$ un ideal $\mathfrak{a}_{n+1} \in S$ con $\mathfrak{a}_n \subsetneq \mathfrak{a}_{n+1}$ lo que da lugar a una cadena ascendente no estacionaria que nos lleva a una contradicción. Por lo tanto, se tiene que (2) implica (3).

Por último, supongamos que cada conjunto no vacío de ideales de D posee un elemento maximal. Sea $\mathfrak{a}$ cualquier ideal de D y sea S el conjunto de todos los ideales finitamente generados contenidos en $\mathfrak{a}$. Puesto que $\{0\} \in S$, S no es vacío y tendrá un elemento maximal $\mathfrak{b}$. Si $\mathfrak{b} \neq \mathfrak{a}$, basta escoger $x \in \mathfrak{a}\backslash\mathfrak{b}$ para obtener un ideal finitamente generado $(\mathfrak{b}, x) \subseteq \mathfrak{a}$ estrictamente mayor que $\mathfrak{b}$, lo que nos lleva a una contradicción. Por lo tanto, $\mathfrak{a} = \mathfrak{b}$ y es finitamente generado, con lo que hemos probado que (3) implica (1).

Teorema 3.1.1 *Si un dominio de integridad D es noetheriano, cada elemento no unidad de D^* se puede expresar como producto de un número finito de irreducibles de D.*

Dem: Supongamos que D es noetheriano, y que existe un elemento x no unidad en D^* que no puede ser expresado como producto de un número finito de elementos irreducibles.

Gracias a la condición de maximalidad, podemos escoger x de forma que (x) sea maximal bajo las condiciones anteriores. Por cómo se ha definido x, éste no puede ser irreducible, por lo tanto, $x = yz$ donde y y z no son unidades. Entonces, tendremos que $(y) \supseteq (x)$. Si $(x) = (y)$, entonces x e y serían elementos asociados, lo que implicaría que z sería una unidad. Por lo tanto, $(y) \supsetneq (x)$, y usando un razonamiento análogo se deduce que $(z) \supsetneq (x)$. Por la maximalidad de (x), ha de ser

$$\begin{aligned} y &= p_1 \dots p_r \\ z &= q_1 \dots q_s \end{aligned}$$

donde cada uno de los p_i, q_j son elementos irreducibles. Multiplicando los elementos irreducibles anteriores, podemos expresar x como producto de un número finito de elementos irreducibles, lo que nos lleva a una contradicción. Por lo tanto, la factorización en irreducibles es posible en D.

Teorema 3.1.2 *El anillo de enteros algebraicos $\mathfrak{D}$ de un cuerpo de números K es noetheriano.*

Dem: Vamos a probar que cada ideal $\mathfrak{a}$ de $\mathfrak{D}$ es finitamente generado. Sabemos por el Teorema 2.5.1 que $(\mathfrak{D}, +)$ es un grupo abeliano libre de rango $n = [K : \mathbb{Q}]$. Por lo tanto, $(\mathfrak{a}, +)$ es abeliano libre de rango $r \leq n$. Basta observar ahora que cualquier $\mathbb{Z}$-base del grupo $(\mathfrak{a}, +)$ genera $\mathfrak{a}$ como ideal.

De los Teoremas 3.1.1 y 3.1.2, se deduce el siguiente Corolario:

Corolario 3.1.1 *Todo anillo de enteros posee la propiedad de factorización en irreducibles.*

La siguiente Proposición nos ayudará a detectar unidades y elementos irreducibles en $\mathfrak{D}$ más fácilmente.

Proposición 3.1.2 *Sea $\mathfrak{D}$ el anillo de enteros algebraicos de un cuerpo de números K, y sean $x, y \in \mathfrak{D}$. Entonces:*

1. *x es una unidad si y sólo si $N(x) = \pm 1$.*
2. *Si x e y son asociados, entonces $N(x) = \pm N(y)$.*
3. *Si $N(x) = p$ con p primo racional, entonces x es irreducible en $\mathfrak{D}$.*

Dem:

1. Si $xu = 1$, entonces $N(x)N(u) = 1$. Por ser x, u enteros algebraicos, sabemos por el Corolario 2.3.2 que $N(x), N(u) \in \mathbb{Z}$. Por lo tanto, ha de ser $N(x) = \pm 1$.

   Para la otra implicación, tenemos que si $N(x) = \pm 1$, entonces

   $$\sigma_1(x)\sigma_2(x)\dots\sigma_n(x) = \pm 1$$

   donde σ_i son los monomorfismos de K en $\mathbb{C}$. Sabemos que uno de los monomorfismos deja invariante a x. Sin pérdida de generalidad, podemos suponer que $\sigma_1(x) = x$. Además, el resto de los $\sigma_i(x)$ son enteros algebraicos. Si escribimos

   $$u = \pm\sigma_2(x)\dots\sigma_n(x)$$

   tenemos que $xu = 1$, por lo que $u = x^{-1} \in K$. Como $u \in K \cap \mathfrak{B} = \mathfrak{D}$, se deduce que x es una unidad.

2. Si x, y son asociados, entonces $x = uy$ para alguna unidad u. Por lo tanto, por el apartado (1), tenemos que $N(x) = N(yu) = N(y)N(u) = \pm N(y)$.

3. Sea $N(x) = p$, con p primo racional. Si escribimos $x = yz$, tenemos que $N(y)N(z) = N(yz) = N(x) = p$, por lo tanto, alguno de los $N(y)$ y $N(z)$ es $\pm p$ y el otro es ± 1. Por el apartado (1), tenemos que y o z es una unidad, y por lo tanto, x es irreducible.

Observar que el recíproco no es cierto, por ejemplo, 2 es irreducible en $\mathbb{Z}[\sqrt{3}]$ y tiene norma 4.

Es importante destacar que, aunque en los anillos de enteros la factorización en irreducibles es posible, no tiene por qué ser única, como muestra el siguiente ejemplo.

Ejemplo 3.1.1 *La factorización en irreducibles no es única en el anillo de enteros algebraicos de* $\mathbb{Q}(\sqrt{-13})$.

Se consideran las siguientes factorizaciones:

$$14 = 2 \cdot 7 = (1 + \sqrt{-13}) \cdot (1 - \sqrt{-13})$$

Vamos a demostrar que $2, 7, 1 + \sqrt{-13}$ *y* $1 - \sqrt{-13}$ *son irreducibles en el anillo de enteros algebraicos* $\mathfrak{D}$ *de* $\mathbb{Q}(\sqrt{-13})$. *Por el Teorema 2.7.1, sabemos que* $\mathfrak{D} = \mathbb{Z}[\sqrt{-13}]$.

Como $N(a + b\sqrt{-17}) = a^2 + 13b^2$, *las normas de los factores* $2, 7, 1 \pm \sqrt{-13}$ *son* $4, 49, 14$ *respectivamente. Si* $2 = xy$ *donde* $x, y \in \mathfrak{D}$ *no son unidades, entonces como* $N(2) = 4$, *ha de ser* $N(x) = \pm 2$, $N(y) = \pm 2$. *De forma análoga, si existen divisores no triviales de* 7 *han de tener norma* ± 7. *Los divisores no triviales de* $1 \pm \sqrt{-13}$ *han de tener norma* ± 2 *o* ± 7. *Teniendo en cuenta todo lo anterior, tenemos las ecuaciones*

$$N(a + b\sqrt{-13}) = a^2 + 13b^2 = \pm 2, \pm 7 \text{ con } a, b \in \mathbb{Z}$$

Ahora bien, si $|b| \geq 1$, $|a^2 + 13b^2| \geq 13$, *por lo tanto, la única opción es que* $|b| = 0$, *por lo que nos queda que* $a^2 = \pm 2, \pm 7$, *lo cual es imposible. Por consiguiente, al no existir divisores propios, los cuatro factores son irreducibles. Como* $N(2) = 4$, $N(7) = 49$ *y* $N(1 \pm \sqrt{-13}) = 14$, *por la Proposición 3.1.2, tenemos que* 2 *y* 7 *no son asociados a* $1 \pm \sqrt{-13}$, *por lo que la factorización en irreducibles no es única.*

En este contexto, mencionamos el siguiente resultado cuya demostración requiere técnicas no contempladas en este trabajo:

Proposición 3.1.3 *El anillo de enteros del cuerpo* $\mathbb{Q}(\sqrt{m})$ *con* $m < 0$ *tiene la propiedad de factorización única en irreducibles si y sólo si*

$$m = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

Cuando $m > 0$ la factorización única se da en muchos más casos, incluso es posible que se cumpla para infinitos valores de m (ver [11], [12] Cap. I sección 6)

3.2. Propiedades de los ideales de $\mathfrak{D}$

En esta sección estudiaremos las propiedades de los ideales del anillo de enteros $\mathfrak{D}$ de un cuerpo de números K. A pesar de que la unicidad de la factorización de un elemento en irreducibles no se da en todos los anillos de enteros, la factorización de ideales en ideales primos es única en todos los anillos de enteros.

Teorema 3.2.1 *El anillo de enteros $\mathfrak{D}$ de un cuerpo de números K tiene las siguientes propiedades:*

1. *Es un dominio de integridad, cuyo cuerpo de cocientes es K.*
2. *Es noetheriano.*
3. *$\mathfrak{D}$ es íntegramente cerrado, es decir, si $\alpha \in K$ satisface una ecuación polinómica con coeficientes en $\mathfrak{D}$, entonces $\alpha \in \mathfrak{D}$.*
4. *Todo ideal primo no nulo de $\mathfrak{D}$ es maximal.*

Dem:

1. Ser dominio de integridad se deduce del hecho de que todo subanillo de un cuerpo es dominio de integridad. Para ver que su cuerpo de cocientes es K, basta aplicar el Teorema 2.1.2 que asegura que para cada $\alpha \in K$ existe algún entero b tal que $b\alpha \in \mathfrak{D}$ y reescribir $\alpha \in K$ como $\alpha = \frac{\alpha b}{b}$.

2,3. Probadas en los Teoremas 3.1.2 y 2.1.5 respectivamente.

4. Sea $\mathfrak{p}$ un ideal primo de $\mathfrak{D}$. Sea $0 \neq \alpha \in \mathfrak{p}$. Entonces

$$N = N(\alpha) = \alpha_1 \dots \alpha_n \in \mathfrak{p}$$

donde los α_i son los conjugados de $\alpha = \alpha_1$. Por lo tanto, $N\mathfrak{D} \subseteq \mathfrak{p}$ y, como $\mathfrak{D}/N\mathfrak{D}$ es finito, también lo es $\mathfrak{D}/\mathfrak{p}$ ya que es un anillo cociente de $\mathfrak{D}/N\mathfrak{D}$.

Resulta así que $\mathfrak{D}/\mathfrak{p}$ es un dominio de integridad finito y entonces es cuerpo. Por lo tanto, $\mathfrak{p}$ es un ideal maximal.

Todas estas propiedades de $\mathfrak{D}$ fueron probadas por Dedekind, por ello, en la actualidad, se llama dominio de Dedekind a cualquier dominio noetheriano e íntegramente cerrado en el que cada ideal primo no nulo es maximal.

Para probar la existencia y la unicidad de la factorización de un ideal en ideales primos, es necesario profundizar en el estudio de los ideales de $\mathfrak{D}$. Para ello, ampliaremos el concepto de ideal introduciendo el concepto de ideal fraccionario y probaremos que el conjunto de los ideales fraccionarios de un cuerpo de números forma un grupo multiplicativo.

Definición 3.2.1 *Sea $\mathfrak{D}$ un anillo de enteros con cuerpo de cocientes K. Un ideal fraccionario de $\mathfrak{D}$ es un $\mathfrak{D}$-submódulo no nulo $\mathfrak{a}$ de K tal que existe $\alpha \in \mathfrak{D}$ no nulo de forma que $\alpha\mathfrak{a} \subseteq \mathfrak{D}$.*

Se deduce de la definición que, si $\mathfrak{a}$ es un ideal fraccionario de $\mathfrak{D}$, existe un entero algebraico $0 \neq \alpha \in \mathfrak{D}$ tal que $\mathfrak{b} = \alpha\mathfrak{a} \subseteq \mathfrak{D}$ es un ideal de $\mathfrak{D}$ y $\mathfrak{a} = \alpha^{-1}\mathfrak{b}$. Por otro lado, es claro que para cualquier $\alpha \in K^*$ y para cualquier ideal no nulo $\mathfrak{b}$ de $\mathfrak{D}$, $\alpha^{-1}\mathfrak{b}$ es un ideal fraccionario. Esto permite definir un ideal fraccionario como cualquier subconjunto de K de la forma $\alpha^{-1}\mathfrak{b}$ con $\alpha \in K^*$ y $\mathfrak{b}$ ideal no nulo de $\mathfrak{D}$.

Es consecuencia inmediata de la definición que todo ideal de $\mathfrak{D}$ es un ideal fraccionario y que un ideal fraccionario $\mathfrak{a}$ es un ideal si y sólo si $\mathfrak{a} \subseteq \mathfrak{D}$.

Ejemplo 3.2.1 *Los ideales fraccionarios de $\mathbb{Z}$ son de la forma $r\mathbb{Z}$ con $r \in \mathbb{Q}$.*

Definiendo ahora el producto de ideales fraccionarios a partir del producto ordinario de ideales, se obtiene el siguiente resultado.

Proposición 3.2.1 *El producto de ideales fraccionarios es un ideal fraccionario. Además, esta operación es asociativa y conmutativa con $\mathfrak{D}$ actuándo como elemento neutro.*

Dem: Sean $\mathfrak{a}_1, \mathfrak{a}_2$ ideales fraccionarios. Si $\mathfrak{a}_1 = \alpha_1^{-1}\mathfrak{b}_1, \mathfrak{a}_2 = \alpha_2^{-1}\mathfrak{b}_2$ donde $\mathfrak{b}_1, \mathfrak{b}_2$ son ideales y α_1, α_2 elementos no nulos de $\mathfrak{D}$, se define el producto $\mathfrak{a}_1\mathfrak{a}_2 = (\alpha_1\alpha_2)^{-1}\mathfrak{b}_1\mathfrak{b}_2$ que, obviamente, es un ideal fraccionario. Las propiedades de la operación se deducen de las correspondientes para el producto de ideales.

Definición 3.2.2 *Si $\mathfrak{a}$ es un ideal no nulo de $\mathfrak{D}$, llamaremos*

$$\mathfrak{a}^{-1} = \{x \in K |\, x\mathfrak{a} \subseteq \mathfrak{D}\}$$

En primer lugar, es obvio que $\mathfrak{a}^{-1}$ es un $\mathfrak{D}$-submódulo de K. Si $\mathfrak{a} \neq 0$, para cualquier $c \in \mathfrak{a}$, $c \neq 0$, tenemos que $c\mathfrak{a}^{-1} \subseteq \mathfrak{D}$, por lo que $\mathfrak{a}^{-1}$ es un ideal fraccionario de $\mathfrak{D}$. Obviamente $\mathfrak{D} \subseteq \mathfrak{a}^{-1}$, luego $\mathfrak{a} = \mathfrak{a}\mathfrak{D} \subseteq \mathfrak{a}\mathfrak{a}^{-1}$. Ahora, usando la definición de $\mathfrak{a}^{-1}$ se tiene que

$$\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathfrak{D}$$

De lo anterior, se deduce que $\mathfrak{a}\mathfrak{a}^{-1}$ es un $\mathfrak{D}$-submódulo contenido en $\mathfrak{D}$, o lo que es lo mismo, un ideal de $\mathfrak{D}$. En el Teorema 3.2.3 se probará que, en realidad, el ideal $\mathfrak{a}\mathfrak{a}^{-1}$ coincide con $\mathfrak{D}$.

A continuación, probaremos que cualquier ideal contiene un producto de ideales primos.

Lema 3.2.1 *Sea $\mathfrak{a} \neq 0$ un ideal de $\mathfrak{D}$. Entonces, existen ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ tales que $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq \mathfrak{a}$.*

Dem: Supongamos que no es cierto. Entonces, como $\mathfrak{D}$ es noetheriano, podemos tomar un ideal $\mathfrak{a}$ para el cual no existen primos en las condiciones pedidas y que es maximal entre aquellos para los que esto ocurre.

En particular, $\mathfrak{a}$ no es primo, por lo tanto, existen elementos $b, c \in \mathfrak{D}$ tales que $b \cdot c \in \mathfrak{a}, b \notin \mathfrak{a}, c \notin \mathfrak{a}$. Sean

$$\mathfrak{a}_1 = \mathfrak{a} + (b)$$

$$\mathfrak{a}_2 = \mathfrak{a} + (c)$$

Entonces, $\mathfrak{a}_1 \supsetneq \mathfrak{a}$, $\mathfrak{a}_2 \supsetneq \mathfrak{a}$ y $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$. Por la maximalidad de $\mathfrak{a}$ existen ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \mathfrak{p}_{s+1}, \ldots, \mathfrak{p}_r$ tales que

$$\mathfrak{p}_1 \ldots \mathfrak{p}_s \subseteq \mathfrak{a}_1,$$

$$\mathfrak{p}_{s+1} \ldots \mathfrak{p}_r \subseteq \mathfrak{a}_2$$

Por lo tanto,

$$\mathfrak{p}_1 \ldots \mathfrak{p}_s\mathfrak{p}_{s+1} \ldots \mathfrak{p}_r \subseteq \mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$$

lo que contradice la elección del ideal $\mathfrak{a}$ que habíamos realizado.

Usando el Lema anterior, podemos probar que dado un ideal $\mathfrak{a}$ de $\mathfrak{D}$, el ideal fraccionario $\mathfrak{a}^{-1}$ es estrictamente mayor que $\mathfrak{D}$.

Corolario 3.2.1 *Si $\mathfrak{a}$ es un ideal propio, entonces $\mathfrak{a}^{-1} \supsetneq \mathfrak{D}$.*

Dem: Si $\mathfrak{a}$ es un ideal propio de $\mathfrak{D}$ y $\mathfrak{p}$ un ideal maximal de $\mathfrak{D}$ tal que $\mathfrak{a} \subseteq \mathfrak{p}$, tendremos que $\mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$. Por lo tanto, solamente será necesario probar que $\mathfrak{p}^{-1} \supsetneq \mathfrak{D}$ para $\mathfrak{p}$ maximal. Para ello, tenemos que encontrar un número que no sea entero algebraico en $\mathfrak{p}^{-1}$. Comenzaremos tomando cualquier $a \in \mathfrak{p}, a \neq 0$. Usando el Lema 3.2.1, escogeremos el menor r tal que

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq (a)$$

con $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ ideales primos. Como $(a) \subseteq \mathfrak{p}$ y $\mathfrak{p}$ es primo, alguno de los $\mathfrak{p}_i \subseteq \mathfrak{p}$. Sin pérdida de generalidad, podemos suponer que $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Por lo tanto, tendremos $\mathfrak{p}_1 = \mathfrak{p}$ ya que los ideales primos en $\mathfrak{D}$ son maximales y entonces

$$\mathfrak{p}_2 \ldots \mathfrak{p}_r \nsubseteq (a)$$

por minimalidad de r. Por consiguiente, existe $b \in \mathfrak{p}_2, \ldots, \mathfrak{p}_r \backslash (a)$. Pero, al ser $b\mathfrak{p} \subseteq (a)$, $ba^{-1}\mathfrak{p} \subseteq \mathfrak{D}$ y $ba^{-1} \in \mathfrak{p}^{-1}$. Sin embargo, $b \notin a\mathfrak{D}$ y $ba^{-1} \notin \mathfrak{D}$, por lo que $ba^{-1} \in \mathfrak{p}^{-1} \backslash \mathfrak{D}$ y $\mathfrak{p}^{-1} \supsetneq \mathfrak{D}$.

La siguiente Proposición nos permitirá demostrar que los ideales fraccionarios tienen estructura de grupo respecto al producto.

Proposición 3.2.2 *Si $\mathfrak{a}$ es un ideal no nulo de $\mathfrak{D}$ y S es un subconjunto de K tal que $\mathfrak{a}S \subseteq \mathfrak{a}$, entonces $S \subseteq \mathfrak{D}$.*

Dem: Sea $s \in S$. Tenemos que probar que si $\mathfrak{a}s \subseteq \mathfrak{a}$, entonces $s \in \mathfrak{D}$. Como $\mathfrak{D}$ es noetherianio, podemos escribir $\mathfrak{a} = (a_1, \ldots, a_m)$ con $a_1, \ldots, a_m \in \mathfrak{D}$ no todos nulos. Entonces, si $\mathfrak{a}s \subseteq \mathfrak{a}$, tenemos que

$$\begin{array}{rcl} a_1 \cdot s & = & b_{11} \cdot a_1 + \ldots + b_{1m} \cdot a_m \\ \vdots & & \vdots \\ a_m \cdot s & = & b_{m1} \cdot a_1 + \ldots + b_{mm} \cdot a_m \end{array}$$

con $b_{ij} \in \mathfrak{D}$.

Al igual que en el Lema 2.1.3, se deduce que el sistema de ecuaciones

$$\begin{array}{rcl} (b_{11} - s) \cdot x_1 + \ldots + b_{1m} \cdot x_m = & & 0 \\ \vdots & & \vdots \\ b_{m1} \cdot x_1 + \ldots + (b_{mm} - s) \cdot x_m = & & 0 \end{array}$$

tiene solución no nula $x_1 = a_1, \ldots, x_m = a_m$. Por lo tanto, el determinante es nulo y se obtiene un polinomio mónico con coeficientes en $\mathfrak{D}$ que se anula en s, de lo que se deduce que $s \in \mathfrak{D}$ por el Teorema 2.1.5.

Lema 3.2.2 *Si $\mathfrak{p}$ es un ideal maximal de $\mathfrak{D}$, entonces $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{D}$.*

Dem: Sabemos que $\mathfrak{p}\mathfrak{p}^{-1}$ es un ideal tal que $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{D}$. Al ser $\mathfrak{p}$ maximal, tenemos que $\mathfrak{p}\mathfrak{p}^{-1}$ es igual a $\mathfrak{p}$ o a $\mathfrak{D}$. Pero si $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, entonces la Proposición 3.2.2 implicaría que $\mathfrak{p}^{-1} \subseteq \mathfrak{D}$, contradiciendo al Corolario 3.2.1. Por lo tanto, ha de ser $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{D}$.

En el siguiente Teorema, veremos que lo obtenido en el Lema 3.2.2 es válido para cualquier ideal.

Teorema 3.2.2 *Si $\mathfrak{a} \neq 0$ es un ideal, entonces $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{D}$.*

Dem: Supongamos que no es cierto. Como $\mathfrak{D}$ es noetheriano, existe un ideal $\mathfrak{a}$ maximal entre los que cumplen que $\mathfrak{a}\mathfrak{a}^{-1} \neq \mathfrak{D}$. Sabemos que, si $\mathfrak{p}$ es un ideal maximal que contiene a $\mathfrak{a}$, $\mathfrak{D} \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$, por lo tanto

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{D}$$

De lo anterior, se deduce que el ideal fraccionario $\mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{D}$ es un ideal. Por otra parte, no puede ser que $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, ya que la Proposición 3.2.2 implicaría que $\mathfrak{p}^{-1} \subseteq \mathfrak{D}$, contradiciendo al Corolario 3.2.1. Por lo tanto, $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1}$ y la condición de maximalidad de $\mathfrak{a}$ implica que el ideal $\mathfrak{a}\mathfrak{p}^{-1}$ cumple

$$\mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} = \mathfrak{D}$$

Por la definición de $\mathfrak{a}^{-1}$, lo anterior significa que

$$\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}^{-1}$$

Por lo tanto,

$$\mathfrak{D} = \mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{D}$$

en contra de lo que habíamos supuesto.

Ahora, estamos en condiciones de probar que el conjunto de los ideales fraccionarios no nulos de $\mathfrak{D}$ forman un grupo abeliano multiplicativo.

Teorema 3.2.3 *Los ideales fraccionarios no nulos de $\mathfrak{D}$ forman un grupo abeliano multiplicativo.*

Dem: En la Proposición 3.2.1 se ha probado que el conjunto de ideales fraccionarios tiene estructura de monoide abeliano respecto al producto. Por lo tanto, únicamente nos falta probar, que dado un ideal fraccionario $\mathfrak{a}$, existe otro ideal fraccionario $\mathfrak{a}'$ tal que $\mathfrak{a}\mathfrak{a}' = \mathfrak{D}$, donde $\mathfrak{a}'$ será el inverso buscado. Sabemos que existe un ideal $\mathfrak{b}$ de $\mathfrak{D}$ y un elemento $\alpha \in \mathfrak{D}$ de modo que $\mathfrak{a} = \alpha^{-1}\mathfrak{b}$. Por lo tanto, podemos poner $\mathfrak{a}' = \alpha\mathfrak{b}^{-1}$ y se obtiene $\mathfrak{a}\mathfrak{a}' = \mathfrak{D}$.

A continuación, probaremos que todo ideal propio de $\mathfrak{D}$ se expresa de forma única, salvo el orden, como producto de ideales primos. Este resultado fue probado en 1871 por Richard Dedekind en un suplemento que añadió al texto "Vorlesungen über Zahlentheorie"[6], redactado antes por él, en el que recogía las notas del curso impartido por Peter Gustav Lejeune Dirichlet en Gotinga y que había sido publicado en 1863 [5].

Teorema 3.2.4 *Todo ideal propio de $\mathfrak{D}$ es producto de ideales primos, de forma única salvo por el orden de los factores.*

Dem: Supongamos que no es cierto. Como $\mathfrak{D}$ es noetheriano, existe un ideal $\mathfrak{a}$ maximal entre aquellos que no pueden expresarse como producto de ideales primos. En particular, $\mathfrak{a}$ no es un ideal primo. Sea $\mathfrak{p}$ un ideal maximal, y por tanto primo, tal que $\mathfrak{a} \subseteq \mathfrak{p}$. Al igual que en el Teorema 3.2.2 obtenemos

$$\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{D}$$

Por la condición de maximalidad de $\mathfrak{a}$, tenemos que

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_2 \dots \mathfrak{p}_r$$

para ideales primos $\mathfrak{p}_2, \dots, \mathfrak{p}_r$. Por lo tanto,

$$\mathfrak{a} = \mathfrak{p}\mathfrak{p}_2 \dots \mathfrak{p}_r$$

que entra en contradicción con la elección que hemos hecho de $\mathfrak{a}$.

Si existen ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$ que verifican

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r = \mathfrak{q}_1 \ldots \mathfrak{q}_s,$$

se cumple que $\mathfrak{p}_1 \supseteq \mathfrak{q}_1 \ldots \mathfrak{q}_s$ y como $\mathfrak{p}_1$ es primo, debe existir $j \in \{1, \ldots, s\}$ tal que $\mathfrak{p}_1 \supseteq \mathfrak{q}_j$. Reordenando los $\mathfrak{q}_\mathfrak{j}$ se puede suponer que $\mathfrak{p}_1 \supseteq \mathfrak{q}_1$ y entonces, como ambos ideales son maximales, es $\mathfrak{p}_1 = \mathfrak{q}_1$.

Multiplicando ahora ambos miembros por $\mathfrak{p}_1^{-1}$ y usando inducción se obtiene la unicidad de la factorización en ideales primos, salvo por el orden de los factores.

El resultado anterior se puede extender a los ideales fraccionarios si admitimos potencias negativas de ideales primos. Es decir, si $\mathfrak{a}$ es un ideal fraccionario, existirá $\alpha \in \mathfrak{D}$, $\alpha \neq 0$ de modo que $\alpha\mathfrak{a}$ es un ideal, y por ello

$$(\alpha) = \mathfrak{p}_1 \ldots \mathfrak{p}_r$$

$$\alpha\mathfrak{a} = \mathfrak{q}_1 \ldots \mathfrak{q}_s$$

Por lo tanto,

$$\mathfrak{a} = \mathfrak{p}_1^{-1} \ldots \mathfrak{p}_r^{-1}\mathfrak{q}_1 \ldots \mathfrak{q}_s$$

Teniendo en cuenta el resultado probado en Teorema 3.2.4, para cualquier par de ideales no nulos $\mathfrak{a}$ y $\mathfrak{b}$ de $\mathfrak{D}$, se pueden definir su máximo común divisor, $m.c.d.(\mathfrak{a}, \mathfrak{b})$, y su mínimo común múltiplo, $m.c.m.(\mathfrak{a}, \mathfrak{b})$, de la manera obvia a partir de sus factorizaciones en primos.

Definición 3.2.3 *Si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales no nulos tales que $\mathfrak{a} = \prod_{i=1}^{r} p_i^{e_i}$ y $\mathfrak{b} = \prod_{i=1}^{r} p_i^{f_i}$, con $\mathfrak{p}_1, \ldots \mathfrak{p}_r$ ideales primos distintos y $e_i, f_i \geq 0$ $\forall i$, se define*

$$m.c.d.(\mathfrak{a}, \mathfrak{b}) = \prod_{i=1}^{r} p_i^{min(e_i, f_i)}$$

$$m.c.m.(\mathfrak{a}, \mathfrak{b}) = \prod_{i=1}^{r} p_i^{max(e_i, f_i)}$$

Corolario 3.2.2 *Todo par de ideales no nulos, posee m.c.d. y m.c.m.*

Diremos que el ideal $\mathfrak{a}$ divide al ideal $\mathfrak{b}$ (escrito $\mathfrak{a}|\mathfrak{b}$) si existe un ideal $\mathfrak{c}$ tal que $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, obviamente, esto implica que $\mathfrak{a} \supseteq \mathfrak{b}$. Por otra parte,

Proposición 3.2.3 *Si $\mathfrak{a}, \mathfrak{b}$ son dos ideales de $\mathfrak{D}$, entonces,*

$$\mathfrak{a} \supseteq \mathfrak{b} \Rightarrow \mathfrak{a} \textit{ divide a } \mathfrak{b}$$

Dem: Sabemos que $\mathfrak{D} \supseteq \mathfrak{a}^{-1}\mathfrak{b}$ y por lo tanto existirá un ideal $\mathfrak{c}$ de $\mathfrak{D}$ de modo que $\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b}$, y entonces $\mathfrak{a}$ divide a $\mathfrak{b}$.

La Proposición 3.2.3 nos permite obtener expresiones alternativas para el máximo común divisor y el mínimo común múltiplo.

Corolario 3.2.3 *Si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales de $\mathfrak{D}$, $\mathfrak{g}, \mathfrak{l}$ son el máximo común divisor y el mínimo común múltiplo, respectivamente, de $\mathfrak{a}$ y $\mathfrak{b}$ y*

$$\mathfrak{a} = \prod_{i=1}^{r} p_i^{e_i} \qquad \mathfrak{b} = \prod_{i=1}^{r} p_i^{f_i}$$

son las respectivas factorizaciones en ideales primos de $\mathfrak{a}$ y $\mathfrak{b}$, entonces

$$\mathfrak{g} = \mathfrak{a} + \mathfrak{b} = \prod p_i^{min(e_i,f_i)} \qquad \mathfrak{l} = \mathfrak{a} \cap \mathfrak{b} = \prod p_i^{max(e_i,f_i)}$$

Dem: Sabemos que $\mathfrak{c}|\mathfrak{a}$ si y sólo si $\mathfrak{c} \supseteq \mathfrak{a}$. Por lo tanto, $\mathfrak{g}$ debe ser el ideal más pequeño que contiene a $\mathfrak{a}$ y a $\mathfrak{b}$, y $\mathfrak{l}$ el ideal más grande que está contenido en $\mathfrak{a}$ y en $\mathfrak{b}$. Por ello y por la Definición 3.2.3, debe ser

$$\mathfrak{g} = \mathfrak{a} + \mathfrak{b} = \prod p_i^{min(e_i,f_i)} \quad \text{y} \quad \mathfrak{l} = \mathfrak{a} \cap \mathfrak{b} = \prod p_i^{max(e_i,f_i)}$$

Al igual que en el caso de los enteros, se cumplen las siguientes propiedades:

Corolario 3.2.4 *Si $\mathfrak{a}, \mathfrak{b}$ son ideales no nulos de $\mathfrak{D}$, $\mathfrak{g} = m.c.d.(\mathfrak{a}, \mathfrak{b})$ y $\mathfrak{l} = m.c.m.((\mathfrak{a}, \mathfrak{b}))$, se cumple:*

a) $\mathfrak{g}|\mathfrak{a}$, $\mathfrak{g}|\mathfrak{b}$.

b) *Si $\mathfrak{g}'$ es un ideal tal que $\mathfrak{g}'|\mathfrak{a}$ y $\mathfrak{g}'|\mathfrak{b}$, se cumple que $\mathfrak{g}'|\mathfrak{g}$.*

c) $\mathfrak{a}|\mathfrak{l}$ *y* $\mathfrak{b}|\mathfrak{l}$.

d) *Si $\mathfrak{l}'$ es un ideal tal que $\mathfrak{a}|\mathfrak{l}'$ y $\mathfrak{b}|\mathfrak{l}'$, se cumple que $\mathfrak{l}|\mathfrak{l}'$.*

3.3. La norma de un ideal

Lema 3.3.1 *Cada ideal no nulo $\mathfrak{a}$ de $\mathfrak{D}$ es un grupo abeliano libre de rango $n = [K : \mathbb{Q}]$.*

Dem: En primer lugar, sabemos por el Teorema 2.5.1 que $(\mathfrak{D}, +)$ es un grupo abeliano libre de rango n, por lo que cada ideal de $\mathfrak{D}$ es abeliano libre de rango $\leq n$.

Para ver que cada ideal no nulo $\mathfrak{a}$ tiene también rango n, vamos a considerar un elemento no nulo $\alpha \in \mathfrak{a}$ y $m = N(\alpha)$. Por el Corolario 2.3.2 tenemos que $m \in \mathbb{Z}$ y de la definición de norma se obtiene que $m \neq 0$. Además, $m = \alpha_1 \dots \alpha_n$ donde $\alpha_1, \alpha_2 \dots, \alpha_n$ son los conjugados de $\alpha = \alpha_1$. Si escribimos $\beta = \alpha_2 \dots \alpha_n$ se obtiene que $\beta = \frac{m}{\alpha} \in K \cap \mathfrak{B} = \mathfrak{D}$. Por lo tanto, $m = \beta\alpha \in (\alpha) \subseteq \mathfrak{a}$.

Como $\mathfrak{D}/(m)$ es finito y $(m) \subseteq \mathfrak{a}$, se tiene $|\mathfrak{D}/\mathfrak{a}|$ es finito y por lo tanto $\mathfrak{a}$ es un grupo abeliano libre de rango n.

Una vez probado que $\mathfrak{D}/\mathfrak{a}$ es finito para cada ideal no nulo $\mathfrak{a}$ de $\mathfrak{D}$, tiene sentido la siguiente definición.

Definición 3.3.1 *Sea $\mathfrak{a}$ un ideal no nulo de $\mathfrak{D}$. Llamamos norma del ideal $\mathfrak{a}$ a $N(\mathfrak{a}) = |\mathfrak{D}/\mathfrak{a}|$.*

Lema 3.3.2 *Sea K un cuerpo de números con anillo de enteros $\mathfrak{D}$. Sea $\{\alpha_1, \dots, \alpha_n\}$ una $\mathbb{Z}$-base del ideal $\mathfrak{a}$ de $\mathfrak{D}$. Se cumple que*

$$N(\mathfrak{a}) = \left| \frac{disc(\alpha_1, \dots, \alpha_n)}{disc(K)} \right|^{1/2}$$

Dem: Sea $\{\omega_1, \dots, \omega_n\}$ una base entera de K.

Supongamos que $\alpha_i = \sum_{j=1}^{n} c_{ij}\omega_j$, entonces

$$N(\mathfrak{a}) = |\mathfrak{D}/\mathfrak{a}| = |det\, c_{ij}|$$

Usando la fórmula del Teorema 2.6.1, tenemos que

$$disc(\alpha_1, \dots, \alpha_n) = (det\, c_{ij})^2\, disc(\omega_1, \dots, \omega_n) =$$

$$= (N(\mathfrak{a}))^2\, disc(K)$$

Basta tomar la raíz cuadrada y tener en cuenta que $N(\mathfrak{a})$ es siempre un valor positivo para obtener el resultado buscado.

El siguiente Corolario muestra la relación que existe entre la norma de un elemento y la norma del ideal principal que genera.

Corolario 3.3.1 *Si $\mathfrak{a} = (a)$ es un ideal principal, entonces $N(\mathfrak{a}) = |N(a)|$.*

Dem: Si $\{\omega_1, \ldots, \omega_n\}$ una base entera de K, $\{a\omega_1, \ldots, a\omega_n\}$ es una $\mathbb{Z}$-base para $\mathfrak{a}$. Para obtener el resultado buscado, basta tener en cuenta la relación entre los determinantes que definen, respectivamente, los discriminantes de $\{\omega_1, \ldots, \omega_n\}$ y $\{a\omega_1, \ldots, a\omega_n\}$. Ésta conduce a $disc(\ a\omega_1, \ldots, a\omega_n) = N(a)^2\, disc(\omega_1, \ldots, \omega_n)$. Ahora, aplicando la fórmula obtenida en el Lema 3.3.2 se obtiene el resultado buscado.

A continuación, estudiaremos las propiedades de la norma de un ideal. La primera propiedad que probaremos es la multiplicativa, la cual se daba también en la norma de un número.

Teorema 3.3.1 *Si $\mathfrak{a}$ y $\mathfrak{b}$ son dos ideales no nulos de $\mathfrak{D}$, entonces*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$$

Dem: Debido a que la factorización es única, y aplicando inducción en el número de factores, es suficiente con demostrar que

$$N(\mathfrak{ap}) = N(\mathfrak{a})N(\mathfrak{p})$$

donde $\mathfrak{p}$ es un ideal primo.

Para probar la igualdad anterior, vamos a probar que son ciertas las siguientes expresiones

$$|\mathfrak{D}/\mathfrak{ap}| = |\mathfrak{D}/\mathfrak{a}||\mathfrak{a}/\mathfrak{ap}|$$

$$|\mathfrak{a}/\mathfrak{ap}| = |\mathfrak{D}/\mathfrak{p}|$$

Es obvio, que la igualdad que queremos probar se deduce inmediatamente de las dos anteriores y de la definición de la norma de un ideal.

Comenzaremos probando

$$|\mathfrak{D}/\mathfrak{ap}| = |\mathfrak{D}/\mathfrak{a}||\mathfrak{a}/\mathfrak{ap}|$$

La expresión previa es consecuencia del tercer teorema de isomorfía. Basta considerar el homomorfismo de anillos $\phi : \mathfrak{D}/\mathfrak{ap} \to \mathfrak{D}/\mathfrak{a}$ dado por $\phi(x + \mathfrak{ap}) = x + \mathfrak{a}$, el cual es suprayectivo y su núcleo es $\mathfrak{a}/\mathfrak{ap}$.

Ahora, probaremos

$$|\mathfrak{a}/\mathfrak{ap}| = |\mathfrak{D}/\mathfrak{p}|$$

Nótese que la factorización única implica que $\mathfrak{a} \neq \mathfrak{ap}$, y en consecuencia $\mathfrak{a} \supsetneq \mathfrak{p}$. A continuación, demostraremos que no existe ningún ideal $\mathfrak{b}$ que se encuentra entre $\mathfrak{a}$ y $\mathfrak{ap}$. Tenemos

$$\mathfrak{a} \supseteq \mathfrak{b} \supseteq \mathfrak{ap}$$

Si operamos con ellos como ideales fraccionarios, obtenemos

$$\mathfrak{a}^{-1}\mathfrak{a} \supseteq \mathfrak{a}^{-1}\mathfrak{b} \supseteq \mathfrak{a}^{-1}\mathfrak{a}\mathfrak{p}$$

Entonces,

$$\mathfrak{D} \supseteq \mathfrak{a}^{-1}\mathfrak{b} \supseteq \mathfrak{p}$$

Al estar $\mathfrak{a}^{-1}\mathfrak{b}$ contenido en $\mathfrak{D}$, sabemos que es un ideal, y como $\mathfrak{p}$ es un ideal maximal, tenemos que

$$\mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{D} \text{ o } \mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{p}$$

o de forma equivalente

$$\mathfrak{b} = \mathfrak{a} \text{ o } \mathfrak{b} = \mathfrak{a}\mathfrak{p}$$

Por consiguiente, no hay ningún ideal $\mathfrak{b}$ contenido entre $\mathfrak{a}$ y $\mathfrak{a}\mathfrak{p}$.

De lo anterior, se deduce que para cualquier elemento $a \in \mathfrak{a}\backslash\mathfrak{a}\mathfrak{p}$ tenemos que

$$\mathfrak{a}\mathfrak{p} + (a) = \mathfrak{a}$$

Ahora, fijando a, podemos definir el homomorfismo $\theta : \mathfrak{D} \to \mathfrak{a}/\mathfrak{a}\mathfrak{p}$ dado por

$$\theta(x) = \mathfrak{a}\mathfrak{p} + ax$$

Por lo tanto, θ es un homomorfismo de $\mathfrak{D}$-módulos y suprayectivo, cuyo núcleo es un ideal que satisface

$$\mathfrak{p} \subseteq ker(\theta)$$

Como $ker(\theta) \neq \mathfrak{D}$ (en caso contrario, sería $\mathfrak{a}/\mathfrak{a}\mathfrak{p} \approx \mathfrak{D}/ker(\theta) = 0$, lo que contradice que $\mathfrak{a} \neq \mathfrak{a}\mathfrak{p}$), y como $\mathfrak{p}$ es maximal, entonces

$$ker(\theta) = \mathfrak{p}$$

Por lo tanto, $\mathfrak{D}/\mathfrak{p} \approx \mathfrak{a}/\mathfrak{a}\mathfrak{p}$ como $\mathfrak{D}$-módulos, lo que demuestra la expresión y completa la demostración.

Vamos a introducir otro uso de la palabra "divide". Si $\mathfrak{a}$ es un ideal de $\mathfrak{D}$ y b es un elemento de $\mathfrak{D}$ tal que $\mathfrak{a}|(b)$, escribiremos que $\mathfrak{a}|b$ y diremos que $\mathfrak{a}$ divide a b. Es obvio, que $\mathfrak{a}|b$ si y sólo si $b \in \mathfrak{a}$. Esta nueva notación, tiene una serie de ventajas, por ejemplo, si $\mathfrak{p}$ es un ideal primo y $\mathfrak{p}|(a)(b)$, entonces tenemos que $\mathfrak{p}|(a)$ o $\mathfrak{p}|(b)$.

Teorema 3.3.2 *Sea $\mathfrak{a}$ un ideal no nulo de $\mathfrak{D}$:*

1. *Si $N(\mathfrak{a})$ es un número primo, entonces $\mathfrak{a}$ es un ideal primo.*
2. *$N(\mathfrak{a})$ es un elemento de $\mathfrak{a}$, o equivalentemente $\mathfrak{a}|N(\mathfrak{a})$.*
3. *Si $\mathfrak{a}$ es un ideal primo no nulo, entonces $\mathfrak{a}$ divide exactamente a un único primo racional p y se cumple que $N(\mathfrak{a}) = p^m$ para cierto $m \in \mathbb{N}$ menor o igual que $n = [K : \mathbb{Q}]$.*

Dem:

1. Basta con escribir $\mathfrak{a}$ como producto de ideales primos e igualar las normas.

2. Por definición, tenemos que $N(\mathfrak{a}) = |\mathfrak{D}/\mathfrak{a}|$. El anillo cociente $\mathfrak{D}/\mathfrak{a}$ es en particular, un grupo finito respecto a la operación suma, y el orden de cualquier elemento divide a $N(\mathfrak{a})$. Por lo tanto, tenemos que para cualquier $x \in \mathfrak{D}$, se cumple que $xN(\mathfrak{a}) + \mathfrak{a} = \mathfrak{a}$ en el anillo cociente $\mathfrak{D}/\mathfrak{a}$, lo que implica que $xN(\mathfrak{a}) \in \mathfrak{D}$. Para obtener el resultado buscado, basta poner $x = 1 \in \mathfrak{D}$.

3. Como $\mathfrak{a}|N(\mathfrak{a}) = p_1^{m_1} \dots p_r^{m_r}$ y $\mathfrak{a}$ es primo, debe dividir a alguno de los ideales principales generados por los primos racionales p_i en $\mathfrak{D}$. Si p y q son números primos distintos, ambos divisibles por $\mathfrak{a}$, podemos encontrar coeficientes $u, v \in \mathbb{Z}$ tales que $up + vq = 1$, de lo que se deduce que $\mathfrak{a}|1$, y por lo tanto $\mathfrak{a} = \mathfrak{D}$, lo que nos lleva a una contradicción. Por lo tanto,

$$N(\mathfrak{a})|N((p)) = p^n$$

y entonces $N(\mathfrak{a}) = p^m$, con $m \leq n$.

Teorema 3.3.3

1. *Cada ideal no nulo de $\mathfrak{D}$ tiene un número finito de divisores.*

2. *Un número entero solo pertenece a un número finito de ideales de $\mathfrak{D}$.*

3. *Solo un número finito de ideales pueden tener la misma norma.*

Dem:

1. Se deduce directamente de la factorización en ideales primos.

2. Sea $r \in \mathbb{Z}$ y $\mathfrak{a}$ un ideal de $\mathfrak{D}$. Sabemos que $r \in \mathfrak{a}$ si y sólo si $\mathfrak{a}$ divide a (r), y por la factorización única, (r) tiene un número finito de divisores.

3. Sea $\mathfrak{a}$ un ideal de $\mathfrak{D}$. Si $N(\mathfrak{a}) = r$, entonces por el Teorema 3.3.2, $r \in \mathfrak{a}$, y usando (2) obtenemos el resultado.

Sabemos que por ser $\mathfrak{D}$ noetheriano, cada ideal es finitamente generado. Se probará ahora mediante el Lema 3.3.3 y el Teorema 3.3.4 que todo ideal de $\mathfrak{D}$ puede ser generado por dos elementos y uno de ellos puede ser elegido arbitrariamente entre los elementos no nulos del ideal.

Lema 3.3.3 *Si $\mathfrak{a}, \mathfrak{b}$ son ideales no nulos de $\mathfrak{D}$, entonces existe $\alpha \in \mathfrak{a}$ tal que*

$$\alpha\mathfrak{a}^{-1} + \mathfrak{b} = \mathfrak{D}$$

Dem: Si $\alpha \in \mathfrak{a}$, tenemos que $\alpha\mathfrak{a}^{-1}$ es un ideal y no solamente un ideal fraccionario. Sabemos por el Lema 3.2.3 que $\alpha\mathfrak{a}^{-1} + \mathfrak{b}$ es el máximo común divisor de $\alpha\mathfrak{a}^{-1}$ y $\mathfrak{b}$. Por lo tanto, será suficiente escoger α de forma que

$$\alpha\mathfrak{a}^{-1} + \mathfrak{p}_i = \mathfrak{D}, (i = 1, \ldots, r)$$

donde $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ son los distintos ideales primos que dividen a $\mathfrak{b}$. Obtendremos lo anterior si escogemos α de forma que $\mathfrak{p}_i$ no contenga a $\alpha\mathfrak{a}^{-1}$, lo que equivale a que

$$p_i \nmid \alpha\mathfrak{a}^{-1}$$

Por lo tanto, será suficiente tomar $\alpha \in \mathfrak{a}\backslash\mathfrak{a}\mathfrak{p}_i$ para todo $i = 1, \ldots, r$.

El caso $r = 1$ es sencillo ya que la unicidad de la factorización en ideales primos implica que $\mathfrak{a} \neq \mathfrak{a}\mathfrak{p}_i$, por lo que tomaremos $\alpha \in \mathfrak{a} \setminus \mathfrak{a}\mathfrak{p}_1$.

Cuando $r > 1$, definimos para cada $i \in \{1, \ldots, r\}$

$$\mathfrak{a}_i = \mathfrak{a}\mathfrak{p}_1 \ldots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \ldots \mathfrak{p}_r$$

y elegimos, como en el caso $r = 1$,

$$\alpha_i \in \mathfrak{a}_i\backslash\mathfrak{a}_i\mathfrak{p}_i$$

Tomamos ahora α como

$$\alpha = \alpha_1 + \ldots + \alpha_r$$

Puesto que cada $\alpha_i \in \mathfrak{a}_i \subseteq \mathfrak{a}$, resulta que $\alpha \in \mathfrak{a}$.

Supongamos que $\alpha \in \mathfrak{a}\mathfrak{p}_i$. Si $j \neq i$, entonces $\alpha_j \in \mathfrak{a}_j \subseteq \mathfrak{a}\mathfrak{p}_i$, de lo que se deduce que

$$\alpha_i = \alpha - \alpha_1 - \ldots - \alpha_{i-1} - \alpha_{i+1} - \ldots - \alpha_r \in \mathfrak{a}\mathfrak{p}_i.$$

Por lo tanto, $\mathfrak{a}\mathfrak{p}_i|(\alpha_i)$. Por otra parte, se tiene que $\mathfrak{a}_i|(\alpha_i)$. Entonces, $\mathfrak{a}_i\mathfrak{p}_i|(\alpha_i)$, lo que contradice la elección que hemos hecho para α_i. Luego $\alpha \in \mathfrak{a}\backslash\mathfrak{a}\mathfrak{p}_i$.

Teorema 3.3.4 *Sea $\mathfrak{a}$ un ideal no nulo de $\mathfrak{D}$ y β cualquier elemento no nulo de $\mathfrak{a}$. Entonces, existe $\alpha \in \mathfrak{a}$ tal que $\mathfrak{a} = (\alpha, \beta)$.*

Dem: Sea $\mathfrak{b} = \beta\mathfrak{a}^{-1}$. Por el Lema 3.3.3, existe $\alpha \in \mathfrak{a}$ tal que

$$\alpha\mathfrak{a}^{-1} + \mathfrak{b} = \alpha\mathfrak{a}^{-1} + \beta\mathfrak{a}^{-1} = \mathfrak{D}$$

Por lo tanto,

$$((\alpha) + (\beta))\,\mathfrak{a}^{-1} = \mathfrak{D}$$

de lo que se deduce que

$$\mathfrak{a} = (\alpha) + (\beta) = (\alpha, \beta)$$

Para finalizar el capítulo, probaremos que las condiciones de DFU y DIP son equivalentes en los anillos de enteros.

Teorema 3.3.5 *La factorización de elementos de $\mathfrak{D}$ en irreducibles es única si y sólo si cada ideal de $\mathfrak{D}$ es principal.*

Dem: La primera implicación es obvia, ya que para cualquier dominio de integridad, se tiene, que ser DIP implica ser DFU.

Para probar la otra implicación, basta demostrar que si la factorización de elementos es única, entonces cada ideal primo es principal, ya que el resto de ideales es producto de ideales primos, y por lo tanto serán principales. Sea $\mathfrak{p} \neq 0$ un ideal primo de $\mathfrak{D}$. Por el Teorema 3.3.2 existe un entero $N = N(\mathfrak{p})$ tal que $\mathfrak{p}|N$. Podemos factorizar N como producto de elementos irreducibles en $\mathfrak{D}$:

$$N = \pi_1 \dots \pi_s$$

Como $\mathfrak{p}|N$ y $\mathfrak{p}$ es un ideal primo, se tiene que $\mathfrak{p}|(\pi_i)$. Sin embargo, como la factorización es única en $\mathfrak{D}$, el irreducible π_i es en realidad primo, y por lo tanto el ideal principal (π_i) es primo.

Entonces, por la unicidad de la factorización, tenemos que

$$\mathfrak{p} = (\pi_i)$$

Por lo tanto, $\mathfrak{p}$ es principal.

Capítulo 4

Factorización de primos racionales

Finalmente, probaremos el Teorema 4.1.1 usando los resultados y los conceptos vistos en los capítulos anteriores. Además, aplicaremos el Teorema a algunos ejemplos.

En general, si p es un primo racional, no es cierto que (p) sea un ideal primo en un anillo de enteros $\mathfrak{D}$ de un cuerpo de números K. El Teorema 4.1.1, probado por primera vez por Richard Dedekind, nos permitirá calcular los factores de (p) en aquellos cuerpos de números cuyo anillo de enteros sea una extensión simple de $\mathbb{Z}$.

Teorema 4.1.1 *Sea K un cuerpo de números de grado n tal que su anillo de enteros $\mathfrak{D}$ es de la forma $\mathbb{Z}[\theta]$ para algún $\theta \in \mathfrak{D}$. Sea p un primo racional y δ el homomorfismo $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$ que extiende a la proyección canónica $\mathbb{Z} \to \mathbb{Z}_p$ y aplica x en x.*

Si $f(x)$ es el polinomio mínimo de θ sobre $\mathbb{Q}$ y

$$\delta(f(x)) = \overline{f_1}(x)^{e_1} \dots \overline{f_r}(x)^{e_r}$$

es la factorización de $\delta(f(x))$ en irreducibles de $\mathbb{Z}_p[x]$, se cumple:

Para cada $i = 1, \dots, r$ y cada $f_i(x) \in \mathbb{Z}[x]$ cuya imagen por δ es $\overline{f_i}(x)$, el ideal $\mathfrak{p}_i = (p) + (f_i(\theta))$ es primo y la factorización de (p) en ideales primos de $\mathfrak{D}$ es

$$(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$$

Dem: Por ser $f(x)$ el polinomio mínimo de θ sobre $\mathbb{Q}$, se cumple que $\mathbb{Z}[x]/(f(x)) \approx \mathbb{Z}[\theta]$. Por otra parte, si θ_i una raíz de $\overline{f_i}(x)$, entonces tenemos que $\mathbb{Z}_p[x]/(\overline{f_i}(x)) \approx \mathbb{Z}_p[\theta_i]$. Ahora, consideramos la proyección canónica

$$\begin{array}{rcl} \delta' : \mathbb{Z}_p[x] & \rightarrow & \mathbb{Z}_p[x]/(\overline{f_i}(x)) \\ p(x) & \rightarrow & p(x) + (\overline{f_i}(x)) \end{array}$$

y la composición

$$\begin{array}{rcl} \delta'' = \delta' \circ \delta : \mathbb{Z}[x] & \rightarrow & \mathbb{Z}_p[x]/(\overline{f_i}(x)) \\ p(x) & \rightarrow & \delta(p(x)) + (\overline{f_i}(x)) \end{array}$$

Como el ideal generado por $f(x)$ en $\mathbb{Z}[x]$ está en $ker(\delta'')$, δ'' induce el homomorfismo

$$\begin{array}{rcl} \delta''' : \mathbb{Z}[x]/(f(x)) & \rightarrow & \mathbb{Z}_p[x]/(\overline{f_i}(x)) \\ p(x) + (f(x)) & \rightarrow & \delta(p(x)) + (\overline{f_i}(x)) \end{array}$$

y, teniendo ahora en cuenta los isomorfismos anteriores, se obtiene el epimorfismo

$$\begin{array}{rcl} \nu_i : \mathbb{Z}[\theta] & \rightarrow & \mathbb{Z}_p[\theta_i] \\ p(\theta) & \rightarrow & \bar{p}(\theta_i) \end{array}$$

La imagen de la aplicación ν_i es $\mathbb{Z}_p[\theta_i]$, que es un cuerpo. Por ello, $ker(\nu_i)$ ha de ser un ideal primo de $\mathbb{Z}[\theta] = \mathfrak{D}$. Por otra parte, es obvio que

$$(p) + (f_i(\theta)) \subseteq ker\ (\nu_i)$$

Si $g(\theta) \in ker(\nu_i)$, tenemos que $\overline{g}(\theta_i) = 0$, y por lo tanto $\overline{g}(x) = \overline{f_i}(x)\overline{h}(x)$ para algún $\overline{h}(x) \in \mathbb{Z}_p[x]$, lo que significa que $g(x) - f_i(x)h(x) \in \mathbb{Z}[x]$ tiene coeficientes divisibles por p. Por lo tanto,

$$g(\theta) = (g(\theta) - f_i(\theta)h(\theta)) + f_i(\theta)h(\theta) \in (p) + (f_i(\theta))$$

de lo que se obtiene la igualdad

$$ker(\nu_i) = (p) + (f_i(\theta))$$

Sea

$$\mathfrak{p}_i = (p) + (f_i(\theta))$$

Entonces para cada $\overline{f_i}$, el ideal $\mathfrak{p}_i$ es un ideal primo que satisface $(p) \subseteq \mathfrak{p}_i$, o dicho de otra forma, $\mathfrak{p}_i|(p)$.

Teniendo en cuenta que, para cualquier terna de ideales $\mathfrak{a}$, $\mathfrak{b}_1$, $\mathfrak{b}_2$, se tiene

$$(\mathfrak{a}+\mathfrak{b}_1)(\mathfrak{a}+\mathfrak{b}_2) \subseteq \mathfrak{a}+\mathfrak{b}_1\mathfrak{b}_2$$

se comprueba por inducción que

$$\mathfrak{p}_1^{e_1}\dots\mathfrak{p}_r^{e_r} \subseteq (p)+(f_1(\theta)^{e_1}\dots f_r(\theta)^{e_r}) \subseteq (p)+(f(\theta)) = (p)$$

Por lo tanto,

$$(p) \mid \mathfrak{p}_1^{e_1}\dots\mathfrak{p}_r^{e_r}$$

y por ello, (p) tiene que ser de la forma

$$(p) = \mathfrak{p}_1^{k_1}\dots\mathfrak{p}_r^{k_r} \qquad \text{con} \qquad 0 \leq k_i \leq e_i \ (1 \leq i \leq r)$$

Por otra parte, la norma del ideal $\mathfrak{p}_i$, es por definición $|\mathfrak{D}/\mathfrak{p}_i|$, y usando el tercer teorema de isomorfía llegamos a que

$$\mathfrak{D}/\mathfrak{p}_i = \mathbb{Z}[\theta]/\mathfrak{p}_i \approx \mathbb{Z}_p[\theta_i]$$

Por lo tanto, la norma de $\mathfrak{p}_i$ es

$$N(\mathfrak{p}_i) = |\mathbb{Z}_p[\theta_i]| = p^{d_i}$$

donde d_i es el grado del polinomio $f_i(x)$, o equivalentemente, el grado del polinomio $\overline{f_i}(x)$. También, tenemos que

$$N((p)) = |\mathbb{Z}[\theta]/(p)| = p^n$$

Entonces, tomando normas en la igualdad $(p) = \mathfrak{p}_1^{k_1}\dots\mathfrak{p}_r^{k_r}$, tenemos que

$$p^n = N((p)) = N(\mathfrak{p}_1)^{k_1}\dots N(\mathfrak{p}_r)^{k_r} = p^{d_1k_1+\dots+d_rk_e},$$

lo que implica que

$$d_1k_1+\dots+d_rk_r = n = d_1e_1+\dots+d_re_r$$

Por lo tanto, tenemos que $k_i = e_i$ $(1 \leq i \leq r)$ con lo que se termina la demostración.

Existe una generalización del resultado anterior para anillos de enteros que no sean extensiones simples de $\mathbb{Z}$ con alguna restricción sobre los primos a los que se puede aplicar el resultado. Una demostración de este resultado puede encontrarse en el Teorema 27 del Capítulo 3 de [3]. No se ha incluido en el trabajo porque las técnicas utilizadas en su demostración quedan fuera del alcance del mismo.

A continuación, se muestran algunos ejemplos de factorizaciones de primos en anillos de enteros.

Por el Teorema 2.7.1, sabemos que los anillos de enteros de los cuerpos cuadráticos están generados por un elemento, por lo que se cumple la condición para aplicar el Teorema 4.1.1.

Ejemplo 4.1.1 *Calcular la factorización de* (19) *en el anillo de enteros* $\mathfrak{D}$ *de* $\mathbb{Q}(\sqrt{5})$.

Como $5 \equiv 1 \,(mod\, 4)$*, por el Teorema 2.7.1 sabemos que* $\mathfrak{D} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. *En primer lugar, el polinomio mínimo de* $\frac{1+\sqrt{5}}{2}$ *es* $x^2 - x - 1$. *Su imagen en* $\mathbb{Z}_{19}[x]$ *es* $x^2 - x - 1 = (x + 4)(x + 14)$. *Luego,* (19) *factoriza como* $(19) = (19, \frac{1+\sqrt{5}}{2} + 4)(19, \frac{1+\sqrt{5}}{2} + 14)$ *en* $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

Ejemplo 4.1.2 *Calcular la factorización de* (13) *en el anillo de enteros* $\mathfrak{D}$ *de* $\mathbb{Q}(\sqrt{-17})$.

Como $-17 \not\equiv 1 \,(mod\, 4)$*, por el Teorema 2.7.1 sabemos que* $\mathfrak{D} = \mathbb{Z}[\sqrt{-17}]$. *En primer lugar, el polinomio mínimo de* $\sqrt{-17}$ *es* x^2+17. *Su imagen en* $\mathbb{Z}_{13}[x]$ *es* $x^2 + 4 = (x + 3)(x + 10)$. *Luego,* (13) *factoriza como* $(13) = (13, \sqrt{-17} + 3)(13, \sqrt{-17} + 10)$ *en* $\mathbb{Z}[\sqrt{-17}]$.

Por el Teorema 2.7.3, sabemos que los anillos de enteros de los cuerpos ciclotómicos están generados por un elemento, por lo que se cumple la condición para aplicar el Teorema 4.1.1.

Ejemplo 4.1.3 *Calcular la factorización de* (11) *en el anillo de enteros* $\mathfrak{D}$ *de* $\mathbb{Q}(\omega)$*, donde* ω *es cualquier raíz compleja de* $x^7 - 1$.

Por el Teorema 2.7.3, sabemos que el anillo de enteros es $\mathbb{Z}[\omega]$. *En primer lugar, el polinomio mínimo de* ω *sobre* $\mathbb{Q}$ *es* $f(x) = x^6+x^5+x^4+x^3+x^2+x+1$.

Su factorización en irreducibles en $\mathbb{Z}_{11}[x]$ *es* [1]

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + 5x^2 + 4x + 10)(x^3 + 7x^2 + 6x + 10)$$

Luego el ideal (11) *factoriza en* $\mathbb{Z}[\omega]$ *como*

$$(11) = (11, \omega^3 + 5\omega^2 + 4\omega + 10)(11, \omega^3 + 7\omega^2 + 6\omega + 3)$$

Ahora, aplicaremos el Teorema 4.1.1 a un cuerpo cúbico. En el Ejemplo 2.6.1, vimos que el anillo de enteros de $\mathbb{Q}(\sqrt[3]{5})$ es $\mathbb{Z}[\sqrt[3]{5}]$, el cual está generado solo por un elemento.

Ejemplo 4.1.4 *Calcular la factorización de* (3) *en el anillo de enteros* $\mathfrak{D}$ *de* $\mathbb{Q}(\sqrt[3]{5})$.

Como ya hemos dicho previamente, $\mathfrak{D} = \mathbb{Z}[\sqrt[3]{5}]$. *En primer lugar, el polinomio mínimo de* $\sqrt[3]{5}$ *es* x^3-5. *Su imagen en* $\mathbb{Z}_3[x]$ *es* $x^3-5 = x^3+1 = (x+1)^3$. *Luego,* (3) *factoriza como* $(3) = (3, \sqrt[3]{5} + 1)^3$ *en* $\mathbb{Z}[\sqrt[3]{5}]$.

[1] Cálculos realizados con el Software SageMath [13].

Por último, queremos destacar que como consecuencia del Teorema 4.1.1 conocemos la factorización de cualquier ideal de la forma (a) con $a \in \mathbb{Z}$ en un anillo de enteros que sea extensión simple de $\mathbb{Z}$. Basta factorizar a en primos racionales y aplicar el Teorema 4.1.1 a cada uno de sus factores.

Ejemplo 4.1.5 *Calcular la factorización de* (281048) *en el anillo de enteros* $\mathfrak{D}$ *de* $\mathbb{Q}(\sqrt{23})$.

Como $23 \not\equiv 1 \,(mod\, 4)$*, por el Teorema 2.7.1 sabemos que* $\mathfrak{D} = \mathbb{Z}[\sqrt{23}]$*. Sabemos que* $281048 = 2^3 \cdot 19 \cdot 43^2$*, por lo tanto, será* $(281048) = (2)^3(19)(43)^2$*. Por ello, para calcular la factorización en ideales primos de* (281048)*, calcularemos las factorizaciones de* (2)*,* (19) *y* (43).

En primer lugar, el polinomio mínimo de $\sqrt{23}$ *es* $x^2 - 23$*. A continuación, calculamos la factorización de cada uno de los primos racionales que componen la factorización de* 281048*:* [2]

- *La imagen del polinomio* $x^2 - 23$ *en* $\mathbb{Z}_2[x]$ *es* $(x+1)^2$*. Luego,* (2) *factoriza como* $(2) = (2, \sqrt{23} + 1)^2$ *en* $\mathbb{Z}[\sqrt{23}]$.
- *La imagen del polinomio* $x^2 - 23$ *en* $\mathbb{Z}_{19}[x]$ *es* $(x+2)(x+17)$*. Luego,* (19) *factoriza como* $(19) = (19, \sqrt{23} + 2)(19, \sqrt{23} + 17)$ *en* $\mathbb{Z}[\sqrt{23}]$.
- *La imagen del polinomio* $x^2 - 23$ *en* $\mathbb{Z}_{43}[x]$ *es* $(x+18)(x+25)$*. Luego,* (43) *factoriza como* $(43) = (43, \sqrt{23} + 18)(43, \sqrt{23} + 25)$ *en* $\mathbb{Z}[\sqrt{23}]$.

Por lo tanto, (281048) *factoriza en* $\mathbb{Z}[\sqrt{23}]$ *como*

$$(281048) = (2, \sqrt{23}+1)^6(19, \sqrt{23}+2)(19, \sqrt{23}+17)(43, \sqrt{23}+18)^2(43, \sqrt{23}+25)^2$$

[2] Cálculos realizados con el Software SageMath [13].

Bibliografía

[1] I. Stewart, "Algebraic number theory and Fermat's last theorem", 3 ed., D Tall. A. K. Peters, 2002.

[2] I. Stewart, "Galois Theory", 2 ed., Chapman and Hall, 1989.

[3] Daniel A. Marcus, "Number Fields", Springer-Verlag New York, 1977.

[4] José F. Fernando; J. Manuel Gamboa. "Ecuaciones Algebraicas: Extensiones de Cuerpos y Teoría de Galois". Ed. Sanz y Torres, 2015.

[5] Peter Gustav Lejeune Dirichlet, Richard Dedekind, "Vorlesungen über Zahlentheorie", F. Vieweg und Sohn, 1863, `https://archive.org/details/vorlesungenberz03dedegoog`

[6] Peter Gustav Lejeune Dirichlet, Richard Dedekind, "Vorlesungen über Zahlentheorie", F. Vieweg und Sohn, 1871, `https://archive.org/details/vorlesungenberz04dedegoog`

[7] Peter Gustav Lejeune Dirichlet, Richard Dedekind, "Vorlesungen über Zahlentheorie", 1894, `https://archive.org/details/vorlesungenber00lejeuoft`

[8] Harold M. Edwards, "Dedekind's Invention of Ideals", Bulletin of the London Mathematical Society

[9] Thomas W. Hungerford , "Algebra", Springer, 1974

[10] Jeremy Avigad, "Dedekind's 1871 version of the theory of ideals", 2004 `https://www.andrew.cmu.edu/user/avigad/Papers/ideals71.pdf`

[11] Wikipedia, List of number fields with class number one, 6 de Abril de 2017, `https://en.wikipedia.org/wiki/List_of_number_fields_with_class_number_one`

[12] Neukirch, Jürgen (1999). Algebraic Number Theory. Grundlehren der mathematischen Wissenschaften. 322. Berlin: Springer-Verlag. ISBN 978-3-540-65399-8.

[13] The Sage Developers, "SageMath, the Sage Mathematics Software System", version 7.6, 2017, `http://www.sagemath.org`