Sección de Matemáticas
Universidad de La Laguna

Lara Niebla Cañete

Estructura de los anillos de enteros algebraicos

Ring of algebraic integers and its structure

Trabajo Fin de Grado
Grado en Matemáticas
La Laguna, Septiembre de 2022

Dirigido por
Luis José Santana Sánchez

Luis José Santana Sánchez
Departamento Matemáticas,
Estadística e Investigaciíon
Operativa
Universidad de La Laguna
38200 La Laguna, Tenerife

Agradecimientos

A Luis, por contagiarme de su entusiasmo y por confiar desde el primer momento en mí y en este proyecto. Por su inestimable comprensión y su cercanía.

A mi familia, por estar siempre ahí. A mi abuela, que desde pequeña me inculcó el gusto por las Matemáticas.

A mis amigos, en especial a los que me ha brindado mi paso por la carrera, que han sido mi punto de apoyo día tras día, incluso en las tardes más frías de biblioteca. Gracias por hacer de estos últimos años una etapa maravillosa.

A Alba, que decía que algo raro tenía que pasarme en la cabeza para querer estudiar Matemáticas. Seguramente tuviera razón.

A los discos que han servido de banda sonora durante las horas dedicadas a esta memoria.

A quienes me quieren. Yo también les quiero a ustedes.

Lara Niebla Cañete
La Laguna, 9 de septiembre de 2022

Resumen · Abstract

Resumen

El objetivo de esta memoria es servir de introducción a la teoría algebraica de números moderna.
Introducimos el concepto de cuerpo numérico, así como algunas herramientas básicas. Posteriormente, definimos el anillo de enteros algebraicos y analizamos su estructura. Probamos que todo anillo de enteros algebraicos es dominio de Dedekind. Por último, estudiamos cómo factorizar extensiones de ideales primos en anillos de enteros algebraicos. Finalizamos comentando brevemente una reducción del Teorema de Kronecker-Weber.

Palabras clave: *Cuerpos numéricos – Anillos de enteros algebraicos – Dominios de Dedekind.*

Abstract

This essay aims to set the framework for modern algebraic number theory.
We introduce the concept of number fields, as well as some basic tools. Next, we define the ring of algebraic integers and analyze its structure. Moreover, we prove that every ring of algebraic integers is a Dedekind domain. Lastly, we study how extensions of prime ideals in rings of algebraic integers are factored. Finally, we make a brief comment about a reduction of Kronecker-Weber's Theorem.

Keywords: *Number fields – Rings of algebraic integers – Dedekind domains.*

Contenido

Introducción

A raíz de la publicación de las Disquistiones Aritmeticae de Gauss en 1801, la comunidad matemática del siglo XIX se encontraba envuelta en un bullicioso auge de nuevos descubrimientos e investigaciones. En particular, existía especial interés por la resolución de ecuaciones, objeto de estudio de Abel y Galois. En ellas subyace la noción de una nueva estructura algebraica, hasta el momento no determinada, a través de la cual poder trabajar con raíces de polinomios. Fue Dedekind quien, varias décadas más tarde, formaliza este nuevo tipo de estructuras, dándoles el nombre de cuerpo (*Körper* en alemán).

En la misma época, Kronecker, considerado uno de los precursores de la matemática moderna, enuncia el resultado conocido a día de hoy como Teorema de Kronecker-Weber, en el que se caracterizan ciertas extensiones de cuerpos de $\mathbb{Q}$. Este afirma que toda *extensión abeliana* finita de $\mathbb{Q}$ está contenida en una *extensión ciclotómica*. Kronecker únicamente pudo plantear la demostración para extensiones de grado par. Posteriormente, tanto Weber en 1886 como Hilbert en 1896 conseguirían completar los detalles de la prueba. De hecho, el Teorema de Kronecker-Weber asienta las bases que motivan el planteamiento del duodécimo problema de Hilbert, también conocido como *Jugendtraum* de Kronecker, pues Kronecker lo describía habitualmente como su "sueño de juventud". Este problema de Hilbert, que a día de hoy continúa abierto, plantea una generalización del Teorema de Kronecker-Weber para extensiones abelianas de *cuerpos numéricos*.

Naturalmente, comienzan a surgir ideas sobre cómo implementar las ya conocidas técnicas aritméticas en estructuras más abstractas. Concretamente, dentro de los elementos de los cuerpos numéricos, se observó que las raíces de polinomios mónicos con coeficientes enteros constituían un conjunto con estructura de anillo. De esta manera surgen los *anillos de enteros algebraicos*, que fueron objeto de estudio de cabezas visibles del panorama matemático de la época: Gauss, Dirichlet, Kummer, Eisenstein, Hermite, Kronecker, Dedekind,... Resulta crucial destacar que, particularmente, los anillos de enteros algebraicos son *dominios de Dedekind*, por lo que existe factorización única de ideales. Por

tanto, en estos anillos, las técnicas de la aritmética clásica se aplican en ideales de la misma forma que en enteros.

Estas son las estructuras y elementos de estudio de la teoría algebraica de números moderna. El objetivo de esta memoria es el de introducir al lector a estos conceptos y aportar el marco teórico necesario para adentrarse en este campo. Además, veremos cómo aplicar esta teoría a la resolución de problemas tanto teóricos, como podría ser la simplificación de la demostración del Teorema de Kronecker-Weber, como prácticos, por ejemplo, la ampliación del sistema criptográfico RSA para ideales en anillos de enteros algebraicos.

Para ello, procederemos siguiendo el siguiente esquema:

En el Capítulo 1 introduciremos el concepto de cuerpo numérico y trabajaremos con traza, norma y discriminante, que son herramientas básicas para entender este tipo de cuerpos. Por último, comentaremos brevemente un problema clásico que busca determinar cuántos tipos de cuerpos numéricos hay (salvo isomorfismos). Recientemente, en 2020, Jean-Marc Couveignes publica en la revista Annals of Mathematics el artículo [2] en el que se mejoran las cotas ya conocidas.

En el Capítulo 2 definiremos los anillos de enteros algebraicos y estudiaremos la estructura que presentan. En particular, demostraremos que son dominios de Dedekind y que, por tanto, existe factorización única de ideales. Para acabar, abordaremos brevemente la ampliación del sistema criptográfico RSA a ideales de anillos de enteros algebraicos.

El Capítulo 3 se centrará en observar qué sucede con los ideales primos en anillos de enteros algebraicos al extenderse a otros anillos. En general, al extenderse pueden perder su condición de primalidad, luego analizaremos cómo se descomponen estos ideales extendidos. Es más, estableceremos una correspondencia entre factorizaciones de ideales primos extendidos y factorizaciones de polinomios con coeficientes en un determinado cuerpo finito. Finalmente, veremos cómo esto permite reducir los casos a estudiar en la demostración del Teorema de Kronecker-Weber.

La bibliografía principal que se sigue en esta memoria es el libro de Marcus [4], que iremos complementando a la hora de tratar temas más concretos.

1

Cuerpos numéricos

En este capítulo presentaremos formalmente uno de los pilares básicos de la memoria: los cuerpos numéricos, que no son más que extensiones de cuerpos finitas de $\mathbb{Q}$. A su vez introduciremos la traza, la norma y el discriminante como herramientas clave para trabajar en este tipo de estructuras.

1.1. Extensiones de cuerpos

Las extensiones de cuerpos constituyen un elemento central dentro de la Teoría de Galois. En esta primera sección recordaremos algunos aspectos referentes a esta materia. Para más detalles, se recomienda consultar el libro de Cox [1].

Definición 1.1. *Sean K y L cuerpos. Decimos que L es una extensión de K si se tiene la inclusión $K \subset L$. Habitualmente lo denotamos por $K \hookrightarrow L$.*

Definición 1.2. *Sea $K \hookrightarrow L$ una extensión de cuerpos, y sea $\alpha \in L$. Diremos que α es algebraico sobre K si existe un polinomio $f(x)$ no constante en $K[x]$ tal que $f(\alpha) = 0$.*

Recordamos que el cuerpo de los números complejos nace del afán de extender $\mathbb{R}$ incluyendo las raíces del polinomio $x^2 + 1$. De la misma forma, dado un elemento α algebraico sobre un cuerpo K, se extiende K al menor cuerpo que conteiene a α y a K. En general tenemos lo siguiente.

Definición 1.3. *Sea A un dominio de integridad y $b \in B$ con $A \subset B$ subanillo. Se define el anillo $A[b]$ como*

$$A[b] := \{f(b) \mid f(x) \in A[x]\},$$

que es el menor dominio de integridad que contiene a A y b.
Así, tenemos que

$$A(b) := \left\{ \frac{f(b)}{g(b)} \mid f(b), g(b) \in A[b],\ g(b) \neq 0 \right\}$$

es su cuerpo de fracciones.
Particularmente, cuando $A = K$ cuerpo y b es algebraico sobre K, se cumple que $K[b]$ es cuerpo y, por tanto, $K[b] = K(b)$.

Sabemos que un mismo elemento algebraico α puede anular a distintos polinomios en $K[x]$. Sin embargo, nos interesará particularmente aquel que sea de menor grado y, además, mónico. De forma equivalente, tenemos la siguiente definición.

Definición 1.4. *Sea K cuerpo y α un elemento algebraico sobre K. Se denomina polinomio mínimo de α sobre K al único polinomio mónico e irreducible en $K[x]$ que tiene a α como raíz. Se denota por $m_{\alpha,K}(x)$.*

Dada una extensión de cuerpos $K \hookrightarrow L$ no es difícil ver que $(L, +)$ es K-espacio vectorial teniendo como producto escalar el producto del cuerpo.

Definición 1.5. *Se denomina grado de la extensión $K \hookrightarrow L$ a la dimensión de L como K-espacio vectorial y lo denotamos por $[L : K]$.*

En el caso particular en el que $L = K(\alpha)$ con α algebraico sobre K, se tiene que

$$[K(\alpha) : K] = deg(m_{\alpha,K}(x));$$

de hecho se puede comprobar que $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base de $K(\alpha)$ como K-espacio vectorial.

Finalmente, llega el momento de introducir uno de los conceptos clave de la memoria, con el que trabajaremos a lo largo de los próximos capítulos.

Definición 1.6. *Diremos que K es un cuerpo numérico si $K \subset \mathbb{C}$ y el grado de su extensión sobre $\mathbb{Q}$ es finito; es decir, $[K : \mathbb{Q}] = n$ para cierto $n \in \mathbb{N}$.*

A lo largo de la memoria analizaremos el comportamiento de las extensiones finitas de cuerpos, para las que conocer y trabajar con su grado es fundamental. Es por ello que el siguiente teorema resulta especialmente relevante.

Teorema 1.7. *Sean K, L, M cuerpos, con $K \hookrightarrow L \hookrightarrow M$ extensiones finitas. Entonces*

$$[M : K] = [L : K] \cdot [M : L].$$

Su demostración puede encontrarse en [1, Teorema 4.3.8].

Si bien hemos dicho que las extensiones de cuerpos son un elemento central de la Teoría de Galois, es bien sabido que el interés de Galois era el de entender el comportamiento de las raíces de polinomios. Sin embargo, hay una relación intrínseca entre ambas, que viene dada por las *inmersiones*.

Definición 1.8. *Sea $K \hookrightarrow L$ una extensión de cuerpos y $\overline{K}$ la clausura algebraica de K. Decimos que un homomorfismo de cuerpos $\sigma : L \to \overline{K}$ es una K-inmersión de L si $\sigma_{|K} = i$, donde i denota la inclusión de K en L.*

Observación 1.9. Una de las aportaciones más relevantes de Galois fue plantear la correspondencia biunívoca entre las raíces de polinomios en $K[x]$ con las K-inmersiones de extensiones de K que contienen a esas raíces. En efecto, dado α algebraico sobre K, tenemos la biyección

$$\begin{aligned} \{\beta \mid \beta \text{ raíz de } m_{\alpha,K}(x)\} &\longrightarrow \{\sigma : K(\alpha) \to \overline{K} \mid \sigma \ K\text{-inmersión}\} \\ \beta \qquad &\longmapsto \quad \sigma_\beta : \quad K(\alpha) \longrightarrow \overline{K} \\ & \qquad\qquad\quad f(\alpha) \longmapsto f(\beta) \end{aligned}$$

donde $f(x) \in K[x]$. Esto se demuestra fácilmente teniendo en cuenta que si $\sigma : L \to \overline{K}$ es una K-inmersión y $\alpha \in L$, entonces $\sigma(\alpha)$ deberá ser raíz de $m_{\alpha,K}(x)$. Diremos entonces que $\sigma(\alpha)$ es un *conjugado* de α. Podemos además reescribir $m_{\alpha,K}(x)$ en función de las inmersiones o conjugados de α de la siguiente forma:

$$m_{\alpha,K}(x) = \prod_{i=1}^{[K(\alpha):K]} (x - \sigma_i(\alpha)). \tag{1.1}$$

Esto es suficiente para entender las K-inmersiones de los cuerpos numéricos al ser estas siempre extensiones simples; es decir, sabemos que para cualquier extensión de cuerpos numéricos $K \hookrightarrow L$, existe $\alpha \in L$ tal que $L = K(\alpha)$. Por tanto, según lo visto anteriormente, habrá tantas K-inmersiones de L como grado tenga la extensión, pues

$$[L : K] = [K(\alpha) : K] = deg(m_{\alpha,K}(x)) = |\{\sigma : K(\alpha) \to \overline{K} \mid \sigma \ K\text{-inmersión}\}|.$$

De esta manera, somos capaces de saber cómo se construyen las K-inmersiones y cómo se extienden a otros cuerpos numéricos.

1.2. Traza y norma

En primer lugar trataremos la traza y la norma, que introduciremos de manera conjunta al definirse de maneras muy similares.

Definición 1.10. *Sea K un cuerpo numérico y sean $\sigma_1, \ldots, \sigma_n$ las n $\mathbb{Q}$-inmersiones de K en $\mathbb{C}$, con $n = [K : \mathbb{Q}]$. Dado $\alpha \in K$,*

(a) definimos la traza de α en K como

$$T(\alpha) := T^K(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha),$$

(b) y se define la norma de α en K como

$$N(\alpha) := N^K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Observación 1.11. Esta nueva definición de norma generaliza la ya conocida para el anillo de enteros de Gauss. Veámoslo.
Tomamos $\alpha = a + bi \in \mathbb{Z}[i]$. Calculando la norma de la manera usual, llegamos a que

$$N(\alpha) = a^2 + b^2.$$

Por otra parte, sabemos que $\mathbb{Z}[i] \subset \mathbb{Q}[i]$ y

$$[\mathbb{Q}[i] : \mathbb{Q}] = deg(m_{i,\mathbb{Q}}(x)) = deg(x^2 + 1) = 2.$$

De hecho, las dos $\mathbb{Q}$-inmersiones de $\mathbb{Q}[i]$ serán

$$\sigma_1(a + bi) = a + bi,$$

$$\sigma_2(a + bi) = a + b(-i),$$

tal y como se explica en la Observación 1.9. Luego, observamos que efectivamente el resultado coincide con el obtenido por el anterior método, pues

$$N(\alpha) = N^{\mathbb{Q}[i]}(\alpha) = \prod_{j=1}^{2} \sigma_j(\alpha) = \sigma_1(\alpha) \cdot \sigma_2(\alpha) = (a + bi) \cdot (a - bi) = a^2 + b^2.$$

Sea K un cuerpo numérico con $[K : \mathbb{Q}] = n$, y $\alpha \in K$ tal que $deg(m_{\alpha,\mathbb{Q}}) = d$. Notamos que si $d = n$ entonces la traza y la norma de α en K, por definición, no son más que la suma y el producto, respectivamente, de sus n conjugados. Para el caso general $d \leq n$ tenemos el siguiente teorema:

Teorema 1.12. *Sea K un cuerpo numérico con $[K : \mathbb{Q}] = n$ y $\alpha \in K$ tal que $deg(m_{\alpha,\mathbb{Q}}(x)) = d$. Entonces*

$$T(\alpha) = \frac{n}{d} \cdot T^{\mathbb{Q}(\alpha)}(\alpha),$$

$$N(\alpha) = (N^{\mathbb{Q}(\alpha)}(\alpha))^{\frac{n}{d}}.$$

La prueba de este resultado no es muy complicada. La idea es tomar la torre de cuerpos

$$\mathbb{Q} \hookrightarrow \mathbb{Q}(\alpha) \hookrightarrow K.$$

Siguiendo el hilo de la Observación 1.9, sabemos que existen $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ $\mathbb{Q}$-inmersiones de $\mathbb{Q}(\alpha)$. La Teoría de Galois nos dice que cada una de ellas se extiende a $[K : \mathbb{Q}(\alpha)]$ de las n $\mathbb{Q}$-inmersiones de K. Además, tenemos que $\frac{n}{d} = [K : \mathbb{Q}(\alpha)]$ por el Teorema 1.7. Esto es suficiente para concluir, pues basta con reagrupar los factores comunes. Veámoslo en un ejemplo.

Ejemplo 1.13. Tomamos la torre de cuerpos

$$\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt[3]{2}) \hookrightarrow K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{5}).$$

En este caso se puede comprobar fácilmente que $[K : \mathbb{Q}] = 6$ y sus seis $\mathbb{Q}$-inmersiones vienen determinadas por las imágenes de $\sqrt[3]{2}$ y $\sqrt{5}$, tal y como se recoge en la siguiente tabla:

$\mapsto$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$
$\sqrt{5}$	$\sqrt{5}$	$\sqrt{5}$	$\sqrt{5}$	$-\sqrt{5}$	$-\sqrt{5}$	$-\sqrt{5}$

donde ω denota una raíz cúbica primitiva de la unidad. Calculamos entonces la traza y norma de $\alpha = \sqrt[3]{2}$ mediante la definición:

$$T^K(\sqrt[3]{2}) = \sum_{i=1}^{6} \sigma_i(\sqrt[3]{2}) = \sqrt[3]{2}+\sqrt[3]{2}\omega+\sqrt[3]{2}\omega^2+\sqrt[3]{2}+\sqrt[3]{2}\omega+\sqrt[3]{2}\omega^2 = 2\cdot(\sqrt[3]{2}+\sqrt[3]{2}\omega+\sqrt[3]{2}\omega^2),$$

$$N^K(\sqrt[3]{2}) = \prod_{i=1}^{6} \sigma_i(\sqrt[3]{2}) = \sqrt[3]{2}\cdot\sqrt[3]{2}\omega\cdot\sqrt[3]{2}\omega^2\cdot\sqrt[3]{2}\cdot\sqrt[3]{2}\omega\cdot\sqrt[3]{2}\omega^2 = (\sqrt[3]{2}\cdot\sqrt[3]{2}\omega\cdot\sqrt[3]{2}\omega^2)^2.$$

Por otro lado, si decidimos aplicar el Teorema 1.12, debemos considerar únicamente las tres $\mathbb{Q}$-inmersiones de $\mathbb{Q}(\sqrt[3]{2})$, que serán

$$\begin{aligned}\tau_1(\sqrt[3]{2}) &= \sqrt[3]{2},\\ \tau_2(\sqrt[3]{2}) &= \sqrt[3]{2}\omega,\\ \tau_3(\sqrt[3]{2}) &= \sqrt[3]{2}\omega^2.\end{aligned}$$

Observamos que $\tau_1(\alpha)$ coincide con $\sigma_1(\alpha)$ y $\sigma_4(\alpha)$, $\tau_2(\alpha)$ con $\sigma_2(\alpha)$ y $\sigma_5(\alpha)$, y $\tau_3(\alpha)$ coincide con $\sigma_3(\alpha)$ y $\sigma_6(\alpha)$. Con esto, se observa que

$$T^K(\sqrt[3]{2}) = 2T^{\mathbb{Q}(\sqrt[3]{2})}(\sqrt[3]{2}),$$

$$N^K(\sqrt[3]{2}) = (N^{\mathbb{Q}(\sqrt[3]{2})}(\sqrt[3]{2}))^2,$$

tal y como nos asegura el teorema.

Como consecuencia se tiene que la traza y la norma son siempre racionales.

Corolario 1.14. *Sean K un cuerpo numérico y un elemento $\alpha \in K$. Se tiene que $T(\alpha), N(\alpha) \in \mathbb{Q}$.*

Demostración. Bastaría probar que $T^{\mathbb{Q}(\alpha)}, N^{\mathbb{Q}(\alpha)} \in \mathbb{Q}$ de acuerdo con el Teorema 1.12. Para ello consideramos

$$m_{\alpha,\mathbb{Q}}(x) = \prod_{i=1}^{d}(x - \sigma_i(\alpha)),$$

con $d = deg(m_{\alpha,\mathbb{Q}}(x))$ y los σ_i las $\mathbb{Q}$-inmersiones de $\mathbb{Q}(\alpha)$ en $\mathbb{C}$.
Si lo expresáramos matricialmente nos quedaría

$$\begin{vmatrix} x - \sigma_1(\alpha) & 0 & \dots & 0 \\ 0 & x - \sigma_2(\alpha) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & x - \sigma_d(\alpha) \end{vmatrix} = 0.$$

Desarrollando este determinante obtenemos

$$m_{\alpha,\mathbb{Q}}(x) = x^d + tr(A)x^{d-1} + \cdots + det(A),$$

con

$$A = \begin{pmatrix} \sigma_1(\alpha) & 0 & \dots & 0 \\ 0 & \sigma_2(\alpha) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma_d(\alpha) \end{pmatrix}. \tag{1.2}$$

Observamos que $tr(A) = T^{\mathbb{Q}(\alpha)}$ y $det(A) = N^{\mathbb{Q}(\alpha)}$, por tanto, como $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Q}[x]$, $T^{\mathbb{Q}(\alpha)}$ y $N^{\mathbb{Q}(\alpha)}$ deben ser racionales. □

1.3. Discriminante

Conociendo cómo funcionan la traza y la norma, en esta sección trataremos el concepto de discriminante. De igual forma que, dado un polinomio, el discriminante es una herramienta clave para entender la naturaleza de sus raíces, para cuerpos numéricos podemos asociar un discriminante que nos dé información relevante sobre estos.

Definición 1.15. *Sean K un cuerpo numérico, $[K : \mathbb{Q}] = n$, y $\sigma_1, \dots, \sigma_n$ las n $\mathbb{Q}$-inmersiones de K sobre $\mathbb{Q}$. Se define el discriminante de la n-upla $(\alpha_1, \dots, \alpha_n) \in K^n$ como*

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

siendo

$$(\sigma_i(\alpha_j)) = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n) \end{pmatrix}. \tag{1.3}$$

Notamos que el discriminante se caracteriza con la traza de la siguiente manera.

Teorema 1.16. *En las condiciones de la definición anterior,* $disc(\alpha_1, \ldots, \alpha_n) = |(T(\alpha_i\alpha_j))|$ *con*

$$(T(\alpha_i\alpha_j)) = \begin{pmatrix} T(\alpha_1\alpha_1) & T(\alpha_1\alpha_2) & \ldots & T(\alpha_1\alpha_n) \\ T(\alpha_2\alpha_1) & T(\alpha_2\alpha_2) & \ldots & T(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ T(\alpha_n\alpha_1) & T(\alpha_n\alpha_2) & \ldots & T(\alpha_n\alpha_n) \end{pmatrix},$$

que llamaremos matriz traza.

Demostración. Tomando la matriz descrita en la ecuación (1.3):

$$|(\sigma_i(\alpha_j))|^2 = |(\sigma_i(\alpha_j))| \cdot |(\sigma_i(\alpha_j))| = |(\sigma_i(\alpha_j))^t| \cdot |(\sigma_i(\alpha_j))| = |(\sigma_i(\alpha_j))^t \cdot (\sigma_i(\alpha_j))|$$

Operamos este producto matricial, teniendo en cuenta que $\sigma_1, \sigma_2, \ldots, \sigma_n$ son homomorfismos de anillos. Así, se tiene que

$$\begin{aligned} (\sigma_i(\alpha_j))^t \cdot (\sigma_i(\alpha_j)) &= \begin{pmatrix} \sum_{i=1}^n \sigma_i(\alpha_1\alpha_1) & \sum_{i=1}^n \sigma_i(\alpha_1\alpha_2) & \ldots & \sum_{i=1}^n \sigma_i(\alpha_1\alpha_n) \\ \sum_{i=1}^n \sigma_i(\alpha_2\alpha_1) & \sum_{i=1}^n \sigma_i(\alpha_2\alpha_2) & \ldots & \sum_{i=1}^n \sigma_i(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n \sigma_i(\alpha_n\alpha_1) & \sum_{i=1}^n \sigma_i(\alpha_n\alpha_2) & \ldots & \sum_{i=1}^n \sigma_i(\alpha_n\alpha_n) \end{pmatrix} \\ &= \begin{pmatrix} T(\alpha_1\alpha_1) & T(\alpha_1\alpha_2) & \ldots & T(\alpha_1\alpha_n) \\ T(\alpha_2\alpha_1) & T(\alpha_2\alpha_2) & \ldots & T(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ T(\alpha_n\alpha_1) & T(\alpha_n\alpha_2) & \ldots & T(\alpha_n\alpha_n) \end{pmatrix} = (T(\alpha_i\alpha_j)), \end{aligned}$$

de tal forma que queda probada la igualdad. □

Corolario 1.17. *Sea* K *un cuerpo numérico y sean los elementos* $\alpha_1, \ldots, \alpha_n \in K$*. Se tiene que* $disc(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$*.*

Demostración. Este resultado se sigue del teorema anterior y de que, para todo $i, j \in \{1, \ldots, n\}$, $T(\alpha_i\alpha_j) \in \mathbb{Q}$, por el Corolario 1.14. □

Un motivo de la relevancia del discriminante es el siguiente.

Teorema 1.18. *Sea K un cuerpo numérico con $[K:\mathbb{Q}] = n$ y sean $\alpha_1, \ldots, \alpha_n \in K$. Se tiene que $disc(\alpha_1, ..., \alpha_n) = 0$ si, y solo si, $\alpha_1, \ldots, \alpha_n$ son linealmente dependientes sobre $\mathbb{Q}$.*

Demostración. Probamos la doble implicación.

$\Leftarrow$ Consideramos que $\{\alpha_1, \ldots, \alpha_n\}$ es un conjunto linealmente dependiente sobre $\mathbb{Q}$, entonces existen $a_1, \ldots, a_n \in \mathbb{Q}$ no todos nulos tales que $a_1\alpha_1 + \cdots + a_n\alpha_n = 0$. Como para todo $i = 1, \ldots, n$ σ_i es homomorfismo de anillos que deja fijo a $\mathbb{Q}$, se tiene que

$$a_1\sigma_i(\alpha_1) + \cdots + a_n\sigma_i(\alpha_n) = \sigma_i(a_1\alpha_1 + \cdots + a_n\alpha_n) = \sigma_i(0) = 0.$$

Esto muestra que las columnas de la matriz (1.3) son linealmente dependientes y en consecuencia $disc(\alpha_1, \ldots, \alpha_n) = 0$.

$\Rightarrow$ Como $disc(\alpha_1, \ldots, \alpha_n) = 0$, por definición se tiene que el determinante de la matriz (1.3) debe ser nulo. Podemos decir entonces que las columnas de la matriz (1.3) son linealmente dependientes sobre $\mathbb{Q}$. Es decir, si $C_1, \ldots, C_n$ son las columnas de dicha matriz, existen $a_1, \ldots, a_n \in \mathbb{Q}$ no todos nulos tales que

$$a_1C_1 + \cdots + a_nC_n = \vec{0}.$$

Observando la primera componente de este vector columna, tenemos que

$$a_1\sigma_1(\alpha_1) + \cdots + a_n\sigma_1(\alpha_n) = \sigma_1(a_1\alpha_1 + \cdots + a_n\alpha_n) = 0, \tag{1.4}$$

pues σ_1 es $\mathbb{Q}$-inmersión. Como σ_1 es de hecho homomorfismo de cuerpos, necesariamente es inyectivo, con lo cual concluimos de la ecuación (1.4) que

$$a_1\alpha_1 + \cdots + a_n\alpha_n = 0,$$

esto es, $\alpha_1, \ldots, \alpha_n$ son linealmente dependientes sobre $\mathbb{Q}$.

□

Por último, concluimos este capítulo mencionando un problema clásico cuyo origen se remonta a finales del siglo XIX, pero que sigue siendo relevante en la actualidad. Como comentamos en la introducción, en esa época la comunidad matemática estaba muy interesada en el estudio de los cuerpos numéricos. Uno de los aspectos que tanto Hermite como Minkowski se plantearon fue el de saber cuántos cuerpos numéricos hay, salvo isomorfismos.

Notar que dos cuerpos numéricos con distinta dimensión como $\mathbb{Q}$-espacio vectorial no pueden ser isomorfos. Por tanto, por ejemplo, $\{\mathbb{Q}(\sqrt[n]{2}) \mid n \in \mathbb{N}\}$ es

una familia de cuerpos numéricos no isomorfos entre ellos, pues $\left[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}\right] = n$.

Llegados a este punto, podríamos plantearnos qué ocurre al fijar el grado de la extensión sobre $\mathbb{Q}$. En este caso, por ejemplo, dados n y m dos enteros libres de cuadrados distintos, se tiene que $[\mathbb{Q}(\sqrt{n}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 2$; sin embargo estos no pueden ser isomorfos. Esto es así pues, si suponemos por reducción al absurdo que existe un isomorfismo $\phi : \mathbb{Q}(\sqrt{n}) \longrightarrow \mathbb{Q}(\sqrt{m})$, entonces $\phi(1) = 1$, por ser homomorfismo de anillos. Luego, tenemos que ϕ debe dejar fijos a los elementos de $\mathbb{Q}$, en otras palabras, ϕ es una $\mathbb{Q}$-inmersión. Entonces $\phi(\sqrt{n})$ debe ser una raíz de $m_{\sqrt{n},\mathbb{Q}}(x) = x^2 - n$, es decir, $\phi(\sqrt{n}) = \pm\sqrt{n}$. Pero $\pm\sqrt{n} \notin \mathbb{Q}(\sqrt{m})$, por lo que llegamos al absurdo.

De lo que Hermite y Minkowski se dan cuenta es de que al hablar de cuerpos numéricos con un grado y también un discriminante restringidos, encontramos únicamente un número finito de ellos. De hecho, demuestran la existencia de una cota para el número de cuerpos numéricos con grado y discriminante acotados.

En las últimas décadas esta cota se ha ido refinando. La mejor cota que se conoce actualmente fue probada en 2020 por el matemático francés Jean-Marc Couveignes en su artículo [2]. La relevancia de este problema es notoria en el hecho de que este artículo fue publicado en la revista de renombre Annals of Mathematics. Es más, la anterior cota, encontrada por Jordan S. Ellenberg y Akshay Venkatesh en 2006, fue también publicada en esta revista.

2

Anillos de enteros algebraicos

Una vez familiarizados con los cuerpos numéricos podemos dar paso a un nuevo tipo de estructura clave en el desarrollo de la memoria. El objetivo principal de este segundo capítulo es introducir los anillos de enteros algebraicos y analizar qué estructura poseen. Como resultado final, demostraremos que todo anillo de enteros algebraicos es dominio de Dedekind.

2.1. Enteros algebraicos

Definición 2.1. *Decimos que $\alpha \in \mathbb{C}$ es entero algebraico si existe un polinomio mónico $p(x) \in \mathbb{Z}[x]$ tal que $p(\alpha) = 0$.*
Dado K cuerpo numérico llamamos anillo de enteros algebraicos de K al conjunto

$$\mathcal{O}_K := \{\alpha \in K \mid \alpha \text{ entero algebraico}\},$$

formado por todos los enteros algebraicos de K.

Veremos que, en efecto, $\mathcal{O}_K$ tiene estructura de anillo con las operaciones usuales de K.

Observación 2.2. Si $\alpha \in \mathbb{C}$ es entero algebraico, entonces no es difícil ver que $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$ y si además $d = deg(m_{\alpha,\mathbb{Q}}(x))$ se tiene que los conjugados de α, esto es, $\sigma_1(\alpha), \ldots, \sigma_d(\alpha)$, son también enteros algebraicos al ser raíces de $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$, como vimos en (1.1).

Es importante notar que dado K cuerpo numérico y $\alpha \in \mathcal{O}_K$, aunque los conjugados de α sean enteros algebraicos, estos no pertenecen necesariamente a $\mathcal{O}_K$. En efecto, retomando el Ejemplo 1.13, se observa que $\sqrt[3]{2}$ es entero algebraico pues anula al polinomio $x^3 - 2$, al igual que $\sigma_2(\sqrt[3]{2})$ y $\sigma_3(\sqrt[3]{2})$. Sin embargo, $\sqrt[3]{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})}$, mientras que $\sigma_2(\sqrt[3]{2}), \sigma_3(\sqrt[3]{2}) \notin \mathbb{Q}(\sqrt[3]{2})$, luego no pueden pertenecer a $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2}))}$.

El siguiente teorema da varias caracterizaciones de los enteros algebraicos, con las que nos será sencillo demostrar la estructura de anillo de $\mathcal{O}_K$ para cualquier cuerpo numérico K.

Teorema 2.3. *Sea $\alpha \in \mathbb{C}$, entonces son equivalentes:*

(1) α es un entero algebraico.
(2) $(\mathbb{Z}[\alpha], +)$ es un grupo finitamente generado.
(3) α pertenece a algún subanillo de $\mathbb{C}$ finitamente generado como grupo aditivo.
(4) $\alpha A \subset A$, siendo $A \subset \mathbb{C}$ un subgrupo aditivo finitamente generado.

Demostración. Demostramos una cadena de implicaciones:
(1) $\Longrightarrow$ (2) : sea α un entero algebraico con $n = deg(m_{\alpha,\mathbb{Q}}(x))$. Veamos que $\mathbb{Z}[\alpha]$ está generado por $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Sea $f(\alpha) \in \mathbb{Z}[\alpha]$ un elemento cualquiera con $f(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$. Como $\mathbb{Q}[x]$ es dominio euclídeo, de forma única existen $q(x), r(x) \in \mathbb{Q}[x]$ tales que

$$f(x) = q(x) \cdot m_{\alpha,\mathbb{Q}}(x) + r(x),$$

con $deg(r(x)) < deg(m_{\alpha,\mathbb{Q}}(x)) = n$.
Evaluando en α, tenemos

$$f(\alpha) = q(\alpha) \cdot m_{\alpha,\mathbb{Q}}(\alpha) + r(\alpha) = q(\alpha) \cdot 0 + r(\alpha) = r(\alpha).$$

Tanto $f(x)$ como $m_{\alpha,\mathbb{Q}}(x)$ tienen coeficientes enteros y, además, $m_{\alpha,\mathbb{Q}}(x)$ es mónico, por tanto $r(x) \in \mathbb{Z}[x]$. Se sigue que

$$\mathbb{Z}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Z}\}.$$

(2) $\Longrightarrow$ (3) : Es claro ya que $\alpha \in \mathbb{Z}[\alpha]$, que es subanillo de $\mathbb{C}$.
(3) $\Longrightarrow$ (4) : Basta con tomar A como el subanillo de $\mathbb{C}$ con $\alpha \in A$ y finitamente generado como grupo aditivo. Claramente, al ser anillo y $\alpha \in A$, se tiene que $\alpha A \subset A$.
(4) $\Longrightarrow$ (1) : Sean $a_1, a_2, \ldots, a_n$ los generadores de A como grupo aditivo. Podemos expresar todo elemento αa_i de $\alpha A \subset A$ como combinación lineal de $a_1, \ldots, a_n$. Esto se puede expresar matricialmente como:

$$\begin{pmatrix} \alpha a_1 \\ \alpha a_2 \\ \vdots \\ \alpha a_n \end{pmatrix} = M \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix},$$

donde $M = (m_{ij}) \in \mathcal{M}_n(\mathbb{Z})$ es una matriz de dimensión $n \times n$ de elementos enteros. En otras palabras, α es autovalor de M.
Por tanto, α anula al polinomio característico

$$p(x) = \mid M - xI \mid = \begin{vmatrix} m_{1,1} - x & m_{1,2} & \ldots & m_{1,n} \\ m_{2,1} & m_{2,2} - x & \ldots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n,1} & m_{n,2} & \ldots & m_{n,n} - x \end{vmatrix} =$$

$$= (m_{1,1} - x) \cdot (m_{2,2} - x) \cdot \ \ldots \ \cdot (m_{n,n} - x) + \text{ términos de menor grado.}$$

Operando, llegamos a

$$p(x) = (-1)^n x^n + \text{ términos de grado menor} \in \mathbb{Z}[x].$$

Tenemos que $p(x)$ o $-p(x)$ es un polinomio mónico, con coeficientes enteros y que anula a α. Concluimos que α es entero algebraico. □

Corolario 2.4. *Si α, β son enteros algebraicos, $\alpha + \beta$ y $\alpha \cdot \beta$ también.*

Demostración. Sean α, β enteros algebraicos tales que $deg(m_{\alpha,\mathbb{Q}}(x)) = n$ y $deg(m_{\beta,\mathbb{Q}}(x)) = m$. En la demostración del teorema anterior vimos que $(\mathbb{Z}[\alpha], +)$ está finitamente generado por $\{1, \alpha, \ldots, \alpha^{n-1}\}$; por su parte, $\{1, \beta, \ldots, \beta^{m-1}\}$ genera $(\mathbb{Z}[\beta], +)$.
No es difícil ver que

$$\{\alpha^i \beta^j \mid i \in \{0, \ldots, n-1\},\ j \in \{0, \ldots, m-1\}\}$$

es un conjunto de generadores de $\mathbb{Z}[\alpha, \beta]$. Como $\alpha+\beta$ y $\alpha\cdot\beta$ pertenecen a $\mathbb{Z}[\alpha, \beta]$, y este es un subanillo de $\mathbb{C}$ finitamente generado como grupo aditivo, concluimos por el punto (3) del Teorema 2.3 que $\alpha + \beta$ y $\alpha \cdot \beta$ son enteros algebraicos. □

Observación 2.5. Este corolario demuestra que $\mathcal{O}_K$ es un subanillo de K.

Otra consecuencia del teorema anterior es que si α es raíz de un polinomio mónico, cuyos coeficientes son enteros algebraicos, entonces α es también entero algebraico, como se ve a continuación.

Corolario 2.6. *Sean K cuerpo numérico, $a_0, \ldots, a_{n-1} \in \mathcal{O}_K$ y $\alpha \in \mathbb{C}$ tales que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Entonces el anillo $\mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$ es un grupo aditivo finitamente generado y, por tanto, $\alpha \in \mathcal{O}_K$.*

Demostración. Sean $d_0, d_1, \ldots, d_{n-1}$ los grados de los polinomios mínimos de $a_0, a_1, \ldots, a_{n-1}$, respectivamente. Siguiendo el mismo argumento que el corolario anterior, vemos que el conjunto

$$\{a_0^{e_0} \cdot a_1^{e_1} \cdot \ \ldots \ \cdot a_{n-1}^{e_{n-1}} \cdot \alpha^e \mid 0 \leq e_i < d_i,\ 0 \leq e < n\}$$

es un sistema generador del grupo $(\mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha], +)$.
Como $\alpha \in \mathbb{Z}[a_0, \ldots, a_{n-1}]$, por el punto (3) del Teorema 2.3 tenemos que α es entero algebraico. □

Llegados a este punto, es interesante observar cómo se comportan la traza, la norma y el discriminante para enteros algebraicos.

Proposición 2.7. *Sea K cuerpo numérico y sea $\alpha \in \mathcal{O}_K$. Entonces $T(\alpha), N(\alpha) \in \mathbb{Z}$.*

Demostración. Tomemos $n = [K : \mathbb{Q}]$ y sea $d = deg(m_{\alpha,\mathbb{Q}}(x))$. La torre de cuerpos $\mathbb{Q} \hookrightarrow \mathbb{Q}(\alpha) \hookrightarrow K$ nos indica que d es un divisor de n. Luego, por el Teorema 1.12, es suficiente ver que $T^{\mathbb{Q}(\alpha)}(\alpha)$ y $N^{\mathbb{Q}(\alpha)}(\alpha)$ son enteros. Esto último se sigue claramente de la definición de traza y norma y de la Observación 2.2. □

Corolario 2.8. *Si $\alpha_1, \ldots, \alpha_n$ son enteros algebraicos, entonces $disc(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.*

Demostración. Se sigue del Teorema 1.16 y de la proposición anterior. □

En las próximas secciones veremos que $\mathcal{O}_K$ no es únicamente un anillo sino que posee una mayor estructura.

2.2. $(\mathcal{O}_K, +)$ es un grupo libre de rango n

Probaremos que $(\mathcal{O}_K, +)$ es un grupo libre de rango n. Para ello, seguiremos la siguiente estrategia: veremos que existen $(A, +)$ y $(B, +)$ grupos abelianos libres de rango n tales que $A \subset \mathcal{O}_K \subset B$. Esto necesariamente implica que $(\mathcal{O}_K, +)$ también debe serlo.

Hallamos A.

Proposición 2.9. *Sea K un cuerpo numérico con $[K : \mathbb{Q}] = n$. Para todo $\alpha \in K$ existe $m \in \mathbb{Z}$ tal que $m\alpha$ es entero algebraico.*

Demostración. Sea $\alpha \in K$ y sea

$$m_{\alpha,\mathbb{Q}}(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{Q}[x]$$

su polinomio mínimo en $\mathbb{Q}[x]$. Asumiendo que $a_i = \dfrac{b_i}{c_i}$ con $b_i, c_i \in \mathbb{Z}$, para todo $i \in \{0, 1, \ldots, n-1\}$, podemos tomar

$$m = mcm(c_o, c_1, \ldots, c_{n-1}),$$

de forma que

$$f(x) := m \cdot m_{\alpha,\mathbb{Q}}(x) = ma_0 + ma_1 x + \cdots + ma_{n-1}x^{n-1} + mx^n \in \mathbb{Z}[x].$$

Multiplicando por m^{n-1} y evaluando en α,

$$m^n a_0 + m^n a_1 \alpha + m^n a_2 \alpha^2 + \cdots + m^n a_{n-1}\alpha^{n-1} + m^n \alpha^n =$$

$$= m^n a_0 + a_1 m^{n-1}(m\alpha) + a_2 m^{n-2}(m\alpha)^2 + \cdots + ma_{n-1}(m\alpha)^{n-1} + (m\alpha)^n = 0,$$

por tanto,

$$g(x) = m^n a_0 + a_1 m^{n-1} x + a_2 m^{n-2} x^2 + \cdots + ma_{n-1}x^{n-1} + x^n$$

es un polinomio mónico con coeficientes enteros que se anula en $m\alpha$; es decir, $m\alpha$ es entero algebraico. □

Observación 2.10. Cabe destacar que, de lo anterior, se tiene que, dada una base $\{\alpha_1, \ldots, \alpha_n\}$ de K como $\mathbb{Q}$-espacio vectorial, siempre podemos asumir que está formada por enteros algebraicos. Basta multiplicar aquellos α_i que no pertenezcan al anillo de enteros algebraicos por el $m_i \in \mathbb{Z}$ correspondiente para que $m_i\alpha_i \in \mathcal{O}_K$ y seguirá siendo base de K.

De esta forma, observamos que si $\{\alpha_1, \ldots, \alpha_n\} \subset \mathcal{O}_K$ es base de K, podemos tomar el grupo abeliano libre de rango n

$$A := \{m_1\alpha_1 + \cdots + m_n\alpha_n \mid m_i \in \mathbb{Z}\} = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n \subset \mathcal{O}_K.$$

Hallamos B.

Teorema 2.11. *Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base de K sobre $\mathbb{Q}$, con α_i enteros algebraicos, y $d = disc(\alpha_1, \ldots, \alpha_n)$. Entonces todo $\alpha \in \mathcal{O}_K$ puede expresarse de la forma*

$$\frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}$$

donde, para todo $j \in \{1, \ldots, n\}$, $m_j \in \mathbb{Z}$ y m_j^2 es divisible por d.

Demostración. Tomamos $\alpha \in \mathcal{O}_K$ de la forma

$$\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n, \text{ con } x_1, \ldots, x_n \in \mathbb{Q}.$$

Sean $\sigma_1, \ldots, \sigma_n$ las n $\mathbb{Q}$-inmersiones de K en $\mathbb{C}$, entonces para todo $i \in \{1, \ldots, n\}$,

$$\sigma_i(\alpha) = \sigma_i\left(\sum_{i=1}^{n} x_j\alpha_j\right) = \sum_{i=1}^{n} \sigma_i(x_j)\sigma_i(\alpha_j) = \sum_{i=1}^{n} x_j\sigma_i(\alpha_j).$$

De esta forma, viendo a $x_1, \ldots, x_n$ como incógnitas, llegamos al siguiente sistema de n ecuaciones con n incógnitas:

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \cdots + \sigma_1(\alpha_n)x_n = \sigma_1(\alpha) \\ \sigma_2(\alpha_1)x_1 + \sigma_2(\alpha_2)x_2 + \cdots + \sigma_2(\alpha_n)x_n = \sigma_2(\alpha) \\ \vdots \\ \sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \cdots + \sigma_n(\alpha_n)x_n = \sigma_n(\alpha). \end{cases} \tag{2.1}$$

Como $\{\alpha_1, \ldots, \alpha_n\}$ es una base, es un conjunto linealmente independiente en $\mathbb{Q}$. Aplicando el Teorema 1.18 tenemos que $d = disc(\alpha_1, \ldots, \alpha_n) \neq 0$, entonces

$$\delta = \sqrt{d} = \mid (\sigma_i(\alpha_j)) \mid = \begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n) \end{vmatrix} \neq 0.$$

Esto indica que el sistema (2.1) es compatible determinado. Por el método de Cramer tenemos que, para todo $r \in \{1, \ldots, n\}$,

$$x_r = \frac{\begin{vmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_{r-1}) & \sigma_1(\alpha) & \sigma_1(\alpha_{r+1}) & \ldots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_{r-1}) & \sigma_n(\alpha) & \sigma_n(\alpha_{r+1}) & \ldots & \sigma_n(\alpha_n) \end{vmatrix}}{\begin{vmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_{r-1}) & \sigma_1(\alpha_r) & \sigma_1(\alpha_{r+1}) & \ldots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_{r-1}) & \sigma_n(\alpha_r) & \sigma_n(\alpha_{r+1}) & \ldots & \sigma_n(\alpha_n) \end{vmatrix}} = \frac{y_r}{\delta}. \tag{2.2}$$

Tanto y_r como δ son enteros algebraicos: δ anula al polinomio $x^2 - d \in \mathbb{Z}[x]$; por su parte, y_r es igual a una expresión algebraica de los $\sigma_i(\alpha_j)$ (también de los $\sigma_i(\alpha)$), que son enteros algebraicos, por la Observación 2.2.
Partiendo de la expresión (2.2), para todo $j \in \{1, \ldots, n\}$,

$$dx_j = \frac{d}{\delta} y_j = \delta y_j.$$

Luego, $dx_j \in \mathbb{Q}$ y además es entero algebraico al ser igual a un producto de enteros algebraicos, por tanto

$$m_j := dx_j \in \mathcal{O}_{\mathbb{Q}} = \mathbb{Z}.$$

En consecuencia,

$$y_j^2 = d\frac{y_j^2}{d} = d\frac{y_j^2}{\delta^2} = dx_j^2 = \frac{d^2 x_j^2}{d} = \frac{m_j^2}{d} \in \mathbb{Q}.$$

Como y_j^2 es entero algebraico en $\mathbb{Q}$, es entero y, por tanto, d divide a m_j^2. Esto demuestra el enunciado del teorema. □

En consecuencia, se tiene que $\mathcal{O}_K$ está contenido en el grupo

$$B := \frac{1}{d} A = \mathbb{Z}\frac{\alpha_1}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha_n}{d},$$

esto es, $\mathcal{O}_K \subset B$, que claramente es grupo abeliano libre de rango n.

Atendiendo a lo discutido al principio de esta sección, concluimos lo siguiente.

Proposición 2.12. *Para K cuerpo numérico, con $[K : \mathbb{Q}] = n$, $(\mathcal{O}_K, +)$ es un grupo abeliano libre finitamente generado de rango n.*

Esto implica que para todo elemento $\alpha \in \mathcal{O}_K$ existen $\beta_1, \ldots, \beta_n \in \mathcal{O}_K$ tales que α puede representarse de forma única como

$$\alpha = m_1\beta_1 + \cdots + m_n\beta_n,$$

con $m_1, \ldots, m_n \in \mathbb{Z}$. Diremos entonces que $\{\beta_1, \ldots, \beta_n\}$ es una *base entera* de $\mathcal{O}_K$; es decir, una base de $\mathcal{O}_K$ vista como $\mathbb{Z}$-módulo.

Conviene señalar que una base entera de K no tiene por qué ser una base de $\mathcal{O}_K$, tal y como se plasma en el siguiente ejemplo:

Ejemplo 2.13. Sea $K = \mathbb{Q}(\sqrt{5})$. Sabemos que $\{1, \sqrt{5}\}$ es una base de K sobre $\mathbb{Q}$. Sin embargo, no es sistema generador de $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ pues $\frac{1+\sqrt{5}}{2} \notin \mathbb{Z} \oplus \mathbb{Z}\sqrt{5}$, pero sí es entero algebraico pues anula al polinomio $x^2 - x - 1$.
De hecho, en este caso es fácilmente comprobable que $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ y tiene a $\{1, \frac{1+\sqrt{5}}{2}\}$ como base entera.

En el capítulo anterior demostramos en el Teorema 1.18 que el discriminante juega un papel crucial a la hora de encontrar bases de cuerpos numéricos, teniendo que $\{\alpha_1, \ldots, \alpha_n\} \subset K$ es una base de K si, y solo si, $disc(\alpha_1, \ldots, \alpha_n) \neq 0$. El siguiente resultado muestra que, en el caso de anillos de enteros algebraicos, el discriminante es un invariante de las bases.

Teorema 2.14. *Sea K un cuerpo numérico. Dados $\{\beta_1, \ldots, \beta_n\}$ y $\{\gamma_1, \ldots, \gamma_n\}$ dos bases enteras de $\mathcal{O}_K$, se tiene que*

$$disc(\beta_1, \ldots, \beta_n) = disc(\gamma_1, \ldots, \gamma_n).$$

Demostración. Para esta demostración, comenzaremos viendo que $disc(\gamma_1, \ldots, \gamma_n)$ divide a $disc(\beta_1, \ldots, \beta_n)$.
Expresando cada elemento $\beta_1, \ldots, \beta_n$ en función de la base $\{\gamma_1, \ldots, \gamma_n\}$ obtenemos

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = M \cdot \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix},$$

siendo $M = (m_{ij}) \in \mathcal{M}_n(\mathbb{Z})$ una matriz de coeficientes enteros de dimensión $n \times n$.
De manera equivalente, se tiene el siguiente sistema de ecuaciones:

$$\begin{cases} \beta_1 = m_{1,1}\gamma_1 +_{1,2} \gamma_2 + \cdots + m_{1,n}\gamma_n \\ \beta_2 = m_{2,1}\gamma_1 +_{2,2} \gamma_2 + \cdots + m_{2,n}\gamma_n \\ \vdots \\ \beta_n = m_{n,1}\gamma_1 +_{n,2} \gamma_2 + \cdots + m_{n,n}\gamma_n. \end{cases}$$

Aplicando las $\mathbb{Q}$-inmersiones $\sigma_1, \ldots, \sigma_n$ a cada ecuación del sistema y expresándolo en forma matricial tenemos

$$(\sigma_j(\beta_i)) = \begin{pmatrix} \sigma_1(\beta_1) & \sigma_2(\beta_1) & \ldots & \sigma_n(\beta_1) \\ \sigma_1(\beta_2) & \sigma_2(\beta_2) & \ldots & \sigma_n(\beta_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\beta_n) & \sigma_2(\beta_n) & \ldots & \sigma_n(\beta_n) \end{pmatrix}$$
$$= M \cdot \begin{pmatrix} \sigma_1(\gamma_1) & \sigma_2(\gamma_1) & \ldots & \sigma_n(\gamma_1) \\ \sigma_1(\gamma_2) & \sigma_2(\gamma_2) & \ldots & \sigma_n(\gamma_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\gamma_n) & \sigma_2(\gamma_n) & \ldots & \sigma_n(\gamma_n) \end{pmatrix} = M \cdot (\sigma_j(\gamma_i)).$$

Considerando los determinantes, se sigue que

$$|(\sigma_j(\beta_i))| = |M \cdot (\sigma_j(\gamma_i))| = |M| \cdot |(\sigma_j(\gamma_i))|.$$

Elevando al cuadrado,

$$|(\sigma_j(\beta_i))|^2 = |M|^2 \cdot |(\sigma_j(\gamma_i))|^2,$$

luego

$$disc(\beta_1, \ldots, \beta_n) = |M|^2 \cdot disc(\gamma_1, \ldots, \gamma_n).$$

Ya que los elementos de M son enteros, el determinante $|M|$ también lo es. Además, $disc(\beta_1, \ldots, \beta_n)$ y $disc(\gamma_1, \ldots, \gamma_n)$ son enteros por el Corolario 2.8. De esto concluimos que $disc(\gamma_1, \ldots, \gamma_n)$ divide a $disc(\beta_1, \ldots, \beta_n)$. Notamos que de manera análoga se deduce que $disc(\beta_1, \ldots, \beta_n)$ divide a $disc(\gamma_1, \ldots, \gamma_n)$ y, al ser ambos positivos, se tiene la igualdad. □

De esta forma, dado $\mathcal{O}_K$ podemos definir el discriminante de $\mathcal{O}_K$ como el discriminante de cualquier base entera de $\mathcal{O}_K$ y lo denotamos $disc(\mathcal{O}_K)$. Más aún, podemos demostrar que si el discriminante de un conjunto $\{\alpha_1, \ldots, \alpha_n\} \subset \mathcal{O}_K$ coincide con $disc(\mathcal{O}_K)$ entonces es una base entera de $\mathcal{O}_K$.

Proposición 2.15. *Sea K un cuerpo numérico y sean $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$. Si $disc(\alpha_1, \ldots, \alpha_n) = disc(\mathcal{O}_K)$, entonces $\{\alpha_1, \ldots, \alpha_n\}$ es una base entera de $\mathcal{O}_K$.*

Demostración. Siguiendo todos los pasos de la demostración anterior, para todo $j \in \{1, \ldots, n\}$ podemos expresar cada α_j en función de una base entera conocida $\{\gamma_1, \ldots, \gamma_n\}$. Llegamos a concluir que existe una matriz $M \in \mathcal{M}_n(\mathbb{Z})$ tal que

$$disc(\alpha_1, \ldots, \alpha_n) = |M|^2 \cdot disc(\gamma_1, \ldots, \gamma_n) = |M|^2 \cdot disc(\mathcal{O}_K).$$

Por hipótesis, $disc(\alpha_1, \ldots, \alpha_n) = disc(\mathcal{O}_K)$, que solo es posible si $|M| = \pm 1$. Esto implica que existe $M^{-1} \in \mathcal{M}_n(\mathbb{Z})$ de forma que

$$\begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} = M^{-1} \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

En otras palabras, para todo $i \in \{1, \ldots, n\}$ podemos expresar γ_i en función de $\{\alpha_1, \ldots, \alpha_n\}$, y por tanto, $\{\alpha_1, \ldots, \alpha_n\}$ es necesariamente una base entera de $\mathcal{O}_K$. □

2.3. $(\mathcal{O}_K, +, \cdot)$ es un dominio de Dedekind

En esta última sección vamos a probar que $(\mathcal{O}_K, +, \cdot)$ es un dominio de Dedekind.

Definición 2.16. *Un dominio de Dedekind es un dominio de integridad que verifica las siguientes tres condiciones:*

(a) Todo ideal está finitamente generado.
(b) Todo ideal primo distinto del trivial es maximal.
(c) El dominio es íntegramente cerrado en su cuerpo de fracciones.

Recordar que, dado un dominio D y su cuerpo de fracciones $c.f.(D)$, decimos que D es íntegramente cerrado si todo elemento de $c.f.(D)$ que sea raíz de un polinomio mónico en $D[x]$ debe pertenecer a D, es decir,

$$D = \{\alpha \in c.f.(D) \mid \exists f(x) \in D[x] \text{ mónico tal que } f(\alpha) = 0\}.$$

Teorema 2.17. *Todo anillo de enteros algebraicos es dominio de Dedekind.*

Demostración. Sea K un cuerpo numérico con $n = [K : \mathbb{Q}]$ y $\mathcal{O}_K$ su anillo de enteros algebraicos. Necesitamos probar las tres condiciones de dominio de Dedekind:

(a) Por la Proposición 2.12, $\mathcal{O}_K$ es un grupo abeliano libre de rango n; es decir, $\mathcal{O}_K \cong \mathbb{Z}^n$. Sabemos que todo ideal I de $\mathcal{O}_K$ es un subgrupo aditivo del mismo, luego I será también un grupo abeliano libre de rango, en este caso, menor o igual a n. Queda probado entonces que todo ideal de $\mathcal{O}_K$ está finitamente generado.

(b) Sea $\mathfrak{p}$ un ideal primo no nulo de $\mathcal{O}_K$. Ver que necesariamente es maximal es equivalente a comprobar que $\mathcal{O}_K/\mathfrak{p}$ es cuerpo. Como $\mathfrak{p}$ es primo, $\mathcal{O}_K/\mathfrak{p}$ es dominio de integridad y probar que es finito será suficiente para concluir que es cuerpo.
Para $\alpha \in \mathfrak{p}$ no nulo sabemos que

$$m := N(\alpha) = N^K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \in \mathbb{Z}$$

por el Corolario 2.7. Además, fácilmente podemos comprobar que $m \in \mathfrak{p}$: consideramos $m = \alpha \cdot \beta$, con $\beta = \prod_{i=2}^{n} \sigma_i(\alpha)$ y asumiendo sin pérdida de generalidad que $\sigma_1(\alpha) = \alpha$. A priori solamente sabemos que β es entero algebraico por ser producto de enteros algebraicos pero no tiene por qué pertenecer a K, tal y como vimos en la Observación 2.2. Sin embargo, en este caso sí podemos afirmar que $\beta \in K$ ya que $m \in \mathbb{Z} \subset K$ y $\alpha \in \mathfrak{p} \subset K$ implican que $\beta = \dfrac{m}{\alpha} \in K$. Por tanto, como $\alpha \in \mathfrak{p}$ y $\beta \in \mathcal{O}_K$, $m \in \mathfrak{p}$.
En consecuencia,

$$I = (m) = \{m \cdot (a_1\gamma_1 + \cdots + a_n\gamma_n) \mid a_i \in \mathbb{Z}\} \subset \mathfrak{p},$$

siendo $\{\gamma_1, \ldots, \gamma_n\}$ una base entera de $\mathcal{O}_K$ e I ideal en $\mathcal{O}_K$. Por ello, la aplicación

$$\mathcal{O}_K/I \longrightarrow \mathcal{O}_K/\mathfrak{p}$$
$$x + I \longrightarrow x + \mathfrak{p}$$

es un epimorfismo. Entonces, es suficiente ver que $\mathcal{O}_K/I$ es finito para verificar que $\mathcal{O}_K/\mathfrak{p}$ también lo es. Definimos el siguiente epimorfismo ϕ como sigue:

$$\phi : \mathcal{O}_K \longrightarrow \mathbb{Z}_m^n$$
$$a_1\gamma_1 + \cdots + a_n\gamma_n \longrightarrow ([a_1]_m, \ldots, [a_n]_m)$$

Se tiene que $ker\phi = I$, por tanto, aplicando el Primer Teorema de Isomorfía, $\mathcal{O}_K/I \cong \mathbb{Z}_m^n$. En otras palabras, $\mathcal{O}_K/I$ es finito y concluimos que $\mathfrak{p}$ es maximal siguiendo lo razonado previamente.

(c) Sea $\zeta \in K$ raíz de un polinomio mónico en $\mathcal{O}_K$. Aplicando el Corolario 2.6, se llega a que $\zeta \in \mathcal{O}_K$, luego $\mathcal{O}_K$ es íntegramente cerrado.

□

Observación 2.18. En la demostración del apartado (b) del teorema anterior hemos probado una pieza fundamental para el Capítulo 3. Esto es, para K cuerpo numérico, si $m \in \mathbb{Z}$, el cociente $\mathcal{O}_K/m\mathcal{O}_K$ tiene cardinal m^n donde $n = [K : \mathbb{Q}]$.

Resulta esencial resaltar que en los dominios de Dedekind existe factorización única de ideales, de hecho, es una de sus características más llamativas. Por esto entendemos lo siguiente: para I ideal de $\mathcal{O}_K$, I se descompone de forma única como

$$I = \mathfrak{p}_1^{e_1} \cdot \ \ldots \ \cdot \mathfrak{p}_r^{e_r},$$

donde $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ son ideales primos de $\mathcal{O}_K$ y $e_1, \ldots, e_r \in \mathbb{Z}^+$. Por ello, es natural extender la aritmética ya conocida para elementos al estudio de ideales. De esta forma, aspectos como el máximo común divisor y el mínimo común múltiplo entre dos ideales pueden calcularse fácilmente siguiendo las reglas habituales.

Definición 2.19. *Sean I, J dos ideales.*

- *Se define el máximo común divisor de ambos como el ideal más pequeño que contiene a ambos; es decir, $I + J$. Se denota por mcd(I,J).*
- *A su vez, se define el mínimo común múltiplo como el ideal más grande contenido en I y en J; es decir, $I \cap J$. Se denota por mcm(I,J).*

Observación 2.20. En general esta es la definición de máximo común divisor y mínimo común múltiplo para ideales. Sin embargo, en el caso de dominios de Dedekind, para hallar el máximo común divisor de dos ideales podemos tomar los factores comunes de su descomposición elevados al menor exponente; por otro lado, para el mínimo común múltiplo tomamos los factores comunes y no comunes elevados al mayor exponente.

Por último introducimos algunos resultados técnicos necesarios para el desarrollo del próximo capítulo.

Teorema 2.21. *Si I es un ideal en un dominio de Dedekind, entonces existe un ideal J tal que IJ es un ideal principal.*

Demostración. Consultar la referencia [4, Teorema 15, Capítulo 3]. □

Corolario 2.22. *Sean I y J ideales propios de un dominio de Dedekind $\mathcal{O}_K$, con $J \subset I$. Entonces existe $\gamma \in K$ tal que $\gamma J \subset \mathcal{O}_K$ y $\gamma J \not\subset I$.*

Demostración. Por el teorema previo, se tiene que existe un ideal H de $\mathcal{O}_K$ tal que $JH = (\alpha)$, con $\alpha \in \mathcal{O}_K$. Como I es un ideal propio, $1 \notin I$, luego $(\alpha) \not\subset \alpha I$. Así, podemos fijar $\beta \in H$ tal que $\beta J \not\subset \alpha I$. Entonces, se tiene que $\gamma = \dfrac{\beta}{\alpha}$ cumple las condiciones del enunciado. En efecto, por un lado,

$$\gamma J = \frac{\beta}{\alpha} J \subset \frac{1}{\alpha} JH = \frac{1}{\alpha}(\alpha) = \mathcal{O}_K,$$

mientras que, por otra parte, al tenerse que $\beta J \not\subset \alpha I$, claramente $\gamma J \not\subset I$.

Corolario 2.23. *Sean I, J ideales en el dominio de Dedekind $\mathcal{O}_K$. Entonces*

$$I \mid J \text{ si, y solo si, } J \subset I;$$

es decir, I divide a J si y solo si lo contiene. Con dividir nos referimos a que existe un ideal C de $\mathcal{O}_K$ tal que $J = IC$.

Demostración. Demostramos la doble implicación:

$\Rightarrow$ Sea C ideal de $\mathcal{O}_K$ tal que $J = IC$, entonces

$$J = IC \subset I \cap C \subset I.$$

$\Leftarrow$ Aplicando el Teorema 2.21 tenemos que existe un ideal H de $\mathcal{O}_K$ tal que $IH = (\alpha)$, con $\alpha \in \mathcal{O}_K$. Vamos a probar que $C := \frac{1}{\alpha}JH$ es un ideal de $\mathcal{O}_K$ e $IC = J$. De esta manera se concluye que $I \mid J$.
Por hipótesis, $J \subset I$, luego

$$C = \frac{1}{\alpha}JH \subset \frac{1}{\alpha}IH = \frac{1}{\alpha}(\alpha) = \mathcal{O}_K,$$

luego $C \subset \mathcal{O}_K$. Además, C es ideal, pues JH es ideal.
Probamos ahora que $IC = J$:

$$IC = I \cdot \frac{1}{\alpha}JH = \frac{1}{\alpha}IHJ = \frac{1}{\alpha}(\alpha)J = \mathcal{O}_K J = J.$$

□

En las últimas décadas, esta aritmética ha encontrado un hueco dentro de las investigaciones en materia de criptografía, concretamente, en el desarrollo de una extensión del conocido sistema criptográfico RSA en anillos de enteros algebraicos. Muy recientemente, a principios de este mismo año, Zhiyong Zheng y Fengxia Liu publican el *preprint* [6], en el que generalizan las técnicas aritméticas clave del RSA a anillos de enteros algebraicos.

Brevemente, la idea de este artículo es la siguiente: sea K un cuerpo numérico y sea I un ideal de su anillo de enteros algebraicos $\mathcal{O}_K$. Se define la función φ de Euler de I como

$$\varphi(I) := |(\mathcal{O}_K/I)^*|,$$

es decir, el número de unidades que hay en el anillo cociente $\mathcal{O}_K/I$. Lo que Zheng y Liu demuestran es que dados dos ideales primos $\mathfrak{p}_1, \mathfrak{p}_2$ de $\mathcal{O}_K$ distintos, y considerando $I = \mathfrak{p}_1 \cdot \mathfrak{p}_2$, se tiene que, para todo $\alpha \in \mathcal{O}_K$ y para todo entero $k \geq 0$,

$$\alpha^{k\varphi(I)+1} \equiv \alpha \ (\text{mód } I).$$

Esto recuerda al resultado clave en el que se basa el RSA clásico y con él, consiguen extenderlo a anillos de enteros algebraicos.

Cabe destacar que el RSA deja de ser seguro con la introducción de ordenadores cuánticos. Lo curioso es que en su artículo Zheng y Liu prueban que esta ampliación corresponde con un sistema de criptografía basada en retículos, y que a día de hoy, es el único sistema post-cuántico avalado por el NIST (National Institute of Standards and Technology), motivando así la investigación en anillos de enteros algebraicos.

3

Factorización de ideales primos extendidos

En el Capítulo 2 comprobamos que $\mathcal{O}_K$ posee estructura de dominio de Dedekind, y por tanto, que existe factorización única de ideales en los anillos de enteros algebraicos. Este es el tema central que abordaremos en este capítulo. Concretamente, estudiaremos qué sucede al extender un ideal primo $\mathfrak{p}$ en $\mathcal{O}_K$ a un anillo de enteros algebraicos que lo contenga.

Definición 3.1. *Sean K y L dos cuerpos numéricos, $K \subset L$, con $\mathcal{O}_K$ y $\mathcal{O}_L$ sus respectivos anillos de enteros algebraicos. Tomando un ideal primo $\mathfrak{p}$ en $\mathcal{O}_K$ denotamos por $\mathfrak{p}\mathcal{O}_L$ a la extensión del ideal $\mathfrak{p}$ a través de la inclusión $i : \mathcal{O}_K \hookrightarrow \mathcal{O}_L$, esto es,*

$$\mathfrak{p}\mathcal{O}_L = \{\alpha_1\beta_1 + \cdots + \alpha_r\beta_r \mid \alpha_i \in \mathfrak{p},\ \beta_i \in \mathcal{O}_L,\ r \in \mathbb{Z}^+\}.$$

Es importante remarcar que $\mathfrak{p}\mathcal{O}_L$ no tiene por qué ser también primo y, precisamente, esto motiva el estudio de la descomposición de $\mathfrak{p}\mathcal{O}_L$ en ideales primos de $\mathcal{O}_L$. En este capítulo profundizaremos en cómo determinar quiénes son estos ideales y qué relación guardan con $\mathfrak{p}$, con qué potencia exacta aparecen en la descomposición, entre otros aspectos.

A lo largo de las siguientes páginas, dado un cuerpo numérico K, hablaremos de ideales primos de $\mathcal{O}_K$ asumiendo en todo momento que son no nulos pues el ideal cero no tendrá especial relevancia.

Teorema 3.2. *Sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$ y $\mathfrak{q}$ un ideal primo de $\mathcal{O}_L$. Se tiene que las siguientes afirmaciones son equivalentes:*

(a) $\mathfrak{q} \mid \mathfrak{p}\mathcal{O}_L$
(b) $\mathfrak{q} \supset \mathfrak{p}\mathcal{O}_L$
(c) $\mathfrak{q} \supset \mathfrak{p}$
(d) $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$
(e) $\mathfrak{q} \cap K = \mathfrak{p}$

Demostración. Demostramos cada doble implicación:
$\boxed{(a) \iff (b)}$: $\mathfrak{q}$ y $\mathfrak{p}\mathcal{O}_L$ son ideales de $\mathcal{O}_L$, que es un dominio de Dedekind.

Aplicando el Corolario 2.23 se demuestra la doble implicación.

$\boxed{(b) \iff (c)}$: sabiendo que $\mathfrak{q}$ es ideal de $\mathcal{O}_L$, desarrollamos cada implicación:
$(b) \Rightarrow (c)$: $\mathfrak{p} \subset \mathfrak{p}\mathcal{O}_L$ entonces, aplicando la hipótesis, $\mathfrak{p} \subset \mathfrak{q}$.
$(c) \Rightarrow (b)$: $\mathfrak{p} \subset \mathfrak{q}$, luego $\mathfrak{p}\mathcal{O}_L \subset \mathfrak{q}\mathcal{O}_L \subset \mathfrak{q}$, por la condición de ideal de $\mathfrak{q}$.

$\boxed{(c) \iff (d)}$
$(d) \Rightarrow (c)$: se deduce trivialmente.
$(c) \Rightarrow (d)$: tenemos por hipótesis que $\mathfrak{p} \subset \mathfrak{q}$, y sabemos que $\mathfrak{p}$ es ideal de $\mathcal{O}_K$, por tanto $\mathfrak{p} \subset \mathfrak{q} \cap \mathcal{O}_K$. $\mathcal{O}_K$ es dominio de Dedekind, luego $\mathfrak{p}$ será un ideal maximal. Entonces $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$ o $\mathfrak{q} \cap \mathcal{O}_K = \mathcal{O}_K$. Si $\mathfrak{q} \cap \mathcal{O}_K = \mathcal{O}_K$, entonces $1 \in \mathfrak{q}$, lo cual es absurdo dado que es primo. Por tanto, $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$.

$\boxed{(d) \iff (e)}$
$(d) \Rightarrow (e)$: sabemos de antemano que $\mathfrak{q} \cap \mathcal{O}_K \subset \mathfrak{q} \cap K$, luego $\mathfrak{p} \subset \mathfrak{q} \cap K$. Seguidamente, para probar el otro contenido, tomaremos un elemento $x \in \mathfrak{q} \cap K$, entonces $x \in \mathfrak{q}$ y $x \in K$. Que x sea elemento de $\mathfrak{q}$ implica que es necesariamente un entero algebraico y, al pertenecer a K también, tenemos que $x \in \mathcal{O}_K$, luego $x \in \mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$.
$(e) \Rightarrow (d)$: como $\mathfrak{q} \cap \mathcal{O}_K \subset \mathfrak{q} \cap K$, es claro que $\mathfrak{q} \cap \mathcal{O}_K \subset \mathfrak{p}$. Ahora, tomamos $x \in \mathfrak{p}$, entonces $x \in \mathfrak{q} \cap K$, esto es, $x \in \mathfrak{q}$ y $x \in K$. Utilizamos el mismo razonamiento de la implicación anterior para deducir que $x \in \mathcal{O}_K$ y que $x \in \mathfrak{q} \cap \mathcal{O}_K$. □

De verificarse estas condiciones, diremos que $\mathfrak{q}$ *yace sobre* $\mathfrak{p}$ o, de manera equivalente, que $\mathfrak{p}$ *yace bajo* $\mathfrak{q}$. Observamos que, en la descomposición

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1 \cdot \ \ldots \ \cdot \mathfrak{q}_r,$$

$\mathfrak{q}_i$ yace sobre $\mathfrak{p}$ para todo $i \in \{1, \ldots, n\}$ y a su vez $\mathfrak{p}$ yace bajo cada uno de los $\mathfrak{q}_i$.

Teorema 3.3. *Dada $K \subset L$ una extensión de cuerpos numéricos y $\mathcal{O}_K$, $\mathcal{O}_L$ sus anillos de enteros algebraicos, respectivamente, se tiene:*

(1) Todo ideal primo $\mathfrak{q}$ de $\mathcal{O}_L$ yace sobre un único ideal primo no nulo $\mathfrak{p}$ de $\mathcal{O}_K$.
(2) Todo ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ yace bajo al menos un ideal primo no nulo $\mathfrak{q}$ de $\mathcal{O}_L$.

Demostración. (1) Debemos probar una de las cinco condiciones del Teorema 3.2. Tomamos (d), esto es, se debe demostrar que $\mathfrak{q} \cap \mathcal{O}_K$ es un ideal primo en $\mathcal{O}_K$.
Veámoslo. Es claro que $\mathfrak{q} \cap \mathcal{O}_K \neq \mathcal{O}_K$ dado que, como $1 \notin \mathfrak{q}$, entonces $1 \notin \mathfrak{q} \cap \mathcal{O}_K$. Sin embargo, sí pertenece a $\mathcal{O}_K$. Debemos comprobar ahora que, para cualesquiera $x, y \in \mathcal{O}_K$ tales que $xy \in \mathfrak{q} \cap \mathcal{O}_K$, al menos uno de ellos es

elemento de $\mathfrak{q} \cap \mathcal{O}_K$.
Tomamos dos elementos $x, y \in \mathcal{O}_K$ que cumplan la hipótesis, se sigue que $xy \in \mathfrak{q}$, siendo $\mathfrak{q}$ un ideal primo, por lo que se concluye que $x \in \mathfrak{q}$ o $y \in \mathfrak{q}$. Como ambos pertenecen a $\mathcal{O}_K$ llegamos a las dos opciones que buscábamos: $x \in \mathfrak{q} \cap \mathcal{O}_K$ o $y \in \mathfrak{q} \cap \mathcal{O}_K$.
A su vez tenemos que asegurarnos de que $\mathfrak{q} \cap \mathcal{O}_K \neq \{0\}$. Tomamos $\alpha \in \mathfrak{q}$ no nulo y consideramos su norma en L. Suponiendo $[L : \mathbb{Q}] = m$, tendremos

$$N_{\mathbb{Q}}^{L}(\alpha) = \prod_{i=1}^{m} \sigma_i(\alpha) = \sigma_1(\alpha) \cdot \sigma_2(\alpha) \cdot \ \ldots \ \cdot \sigma_m(\alpha).$$

Suponemos, sin pérdida de generalidad, que σ_1 es la identidad y sea $\beta := \sigma_2(\alpha) \cdot \ \ldots \ \cdot \sigma_m(\alpha)$. Recordemos que en la prueba del Teorema 2.17(b) ya vimos que

$$a := N_{\mathbb{Q}}^{L}(\alpha) = \alpha \cdot \beta \in \mathbb{Z},$$

y como $\alpha \neq 0$, tenemos que $a \neq 0$. Además, también vimos que $\beta \in \mathcal{O}_L$. Por tanto, al ser $\mathfrak{q}$ un ideal de $\mathcal{O}_L$, se sigue que $a = \alpha \cdot \beta \in \mathfrak{q}$. Por otra parte, $a \in \mathbb{Z} \subset \mathcal{O}_K$, lo que significa que hemos encontrado un elemento a no nulo en $\mathfrak{q} \cap \mathcal{O}_K$.
Por último, notemos que el ideal sobre el que yace $\mathfrak{q}$ es único. Suponiendo que existan dos ideales primos en $\mathcal{O}_K$, $\mathfrak{p}_1$ y $\mathfrak{p}_2$, tales que $\mathfrak{q}$ yazca sobre ambos entonces ambos serían iguales a $\mathfrak{q} \cap \mathcal{O}_K$.

(2) Notemos que los ideales primos de $\mathcal{O}_L$ que yacen sobre $\mathfrak{p}$ son los divisores primos de $\mathfrak{p}\mathcal{O}_L$. Para probar este punto es suficiente con garantizar que al menos existe un primo en dicha descomposición y para ello basta ver que $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$.
Como $\mathfrak{p}$ es primo, $1 \notin \mathfrak{p}$. Por el Corolario 2.22 (tomando $I = J = \mathfrak{p} \subset \mathcal{O}_K$), sabemos que existe $\gamma \in K - \mathcal{O}_K$ tal que $\gamma\mathfrak{p} \subset \mathcal{O}_K$. Entonces $\gamma\mathfrak{p}\mathcal{O}_L \subset \mathcal{O}_K\mathcal{O}_L$, y como $\mathcal{O}_K \subset \mathcal{O}_L$, $\mathcal{O}_K\mathcal{O}_L = \mathcal{O}_L$, así que $\gamma\mathfrak{p}\mathcal{O}_L \subset \mathcal{O}_L$.
Ahora suponemos por reducción al absurdo que $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$, entonces $1 \in \mathfrak{p}\mathcal{O}_L$. Esto implica que $\gamma = \gamma \cdot 1 \in \gamma\mathfrak{p}\mathcal{O}_L \subset \mathcal{O}_L$. Sin embargo, $\gamma \in K - \mathcal{O}_K \subset L - \mathcal{O}_L$, por lo que se llega a una contradicción.

□

Dado un ideal primo $\mathfrak{p} \in \mathcal{O}_K$ y un ideal primo $\mathfrak{q} \in \mathcal{O}_L$ que yace sobre $\mathfrak{p}$, existen dos parámetros asociados a $\mathfrak{q}$ esenciales para entender la naturaleza de estas extensiones: el índice de ramificación y el grado residual.

Definición 3.4. *Sea $\mathfrak{q}$ un ideal de $\mathcal{O}_L$ que yace sobre $\mathfrak{p}$ tal que $\mathfrak{q}^e$ es la potencia exacta con la que divide a $\mathfrak{p}\mathcal{O}_L$ en su descomposición prima. Diremos que $e = e(\mathfrak{q}|\mathfrak{p})$ es el índice de ramificación de $\mathfrak{q}$ sobre $\mathfrak{p}$.*

Definición 3.5. *Sean $\mathfrak{p}$ y $\mathfrak{q}$ ideales de $\mathcal{O}_K$ y $\mathcal{O}_L$, respectivamente, tales que $\mathfrak{q}$ yace sobre $\mathfrak{p}$. Consideramos $\mathcal{O}_K/\mathfrak{p}$ y $\mathcal{O}_L/\mathfrak{q}$ los cuerpos residuales asociados a $\mathfrak{p}$ y $\mathfrak{q}$. Llamamos grado residual de $\mathfrak{q}$ sobre $\mathfrak{p}$ al grado $f = f(\mathfrak{q} \mid \mathfrak{p})$ de la extensión de $\mathcal{O}_L/\mathfrak{q}$ sobre $\mathcal{O}_K/\mathfrak{p}$.*

Recordemos que un cuerpo residual es el cuerpo $A/\mathfrak{m}$ formado por las clases de A módulo $\mathfrak{m}$, siendo $\mathfrak{m}$ un ideal maximal de A. Tal y como demostramos en el Teorema 2.17, todo ideal primo no nulo de $\mathcal{O}_K$ es maximal, por tanto $\mathcal{O}_K/\mathfrak{p}$ y $\mathcal{O}_L/\mathfrak{q}$ son cuerpos. De hecho, en la demostración del teorema también probamos que son cuerpos finitos, luego tiene sentido hablar del grado residual pues $f(\mathfrak{q} \mid \mathfrak{p})$ es un valor finito.

Ejemplo 3.6. Consideramos la extensión $\mathbb{Q} \hookrightarrow \mathbb{Q}[i]$ con sus respectivos anillos de enteros algebraicos $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ y $\mathcal{O}_{\mathbb{Q}[i]} = \mathbb{Z}[i]$. Tomamos el ideal $2\mathbb{Z} = (2)$ en $\mathbb{Z}$. Al extenderlo a $\mathbb{Z}[i]$ no es difícil observar que

$$(2)\mathbb{Z}[i] = \{2(a + b\ i) \mid a, b \in \mathbb{Z}\}\,.$$

Sea $\langle 1 - i\rangle$ el ideal generado por $1 - i$ en $\mathbb{Z}[i]$. Recordar que, en el anillo de los enteros de Gauss, si la norma del generador de un ideal principal es un número primo, entonces el ideal es primo. En nuestro caso,

$$N^{\mathbb{Q}[i]}(1 - i) = (1 - i) \cdot (1 + i) = 2,$$

luego $\langle 1 - i\rangle$ es un ideal primo. Además, el cálculo de la norma nos dice que $2 \in \langle 1 - i\rangle$, así que $(2)\mathbb{Z}[i] \subset \langle 1 - i\rangle$. En otras palabras, $\langle 1 - i\rangle$ divide a $(2)\mathbb{Z}[i]$, siendo por tanto uno de sus factores primos.

Ahora notamos que, al ser $(1 - i)^2 = -2i$, es fácil comprobar que

$$\langle 1 - i\rangle^2 = \{2(a + b\ i) \mid a, b \in \mathbb{Z}\} = (2)\mathbb{Z}[i].$$

Por tanto, en este caso particular, la descomposición en primos de $(2)\mathbb{Z}[i]$ es de la forma $(2)\mathbb{Z}[i] = \langle 1 - i\rangle^2$. Esto implica que $e(\langle 1 - i\rangle \mid (2)) = 2$.

Calculamos el grado residual. En este caso,

$$\mathbb{Z}/(2) = \{0 + (2), 1 + (2)\} \text{ y}$$

$$\mathbb{Z}[i]/\langle 1 - i\rangle = \{0 + \langle 1 - i\rangle, 1 + \langle 1 - i\rangle\}.$$

En consecuencia,

$$|\mathbb{Z}/(2)| = |\mathbb{Z}[i]/\langle 1 - i\rangle| = 2,$$

por lo tanto, $f(\langle 1 - i\rangle \mid (2)) = 1$.

Claramente tanto el índice de ramificación como el grado residual son números enteros positivos. Veamos que guardan especial relación con el grado de la extensión.

Teorema 3.7. *Sea $K \subset L$ una extensión de cuerpos numéricos con n=[L:K], y sean $\mathcal{O}_K$, $\mathcal{O}_L$ sus anillos de enteros algebraicos, respectivamente. Consideramos $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ los ideales primos de $\mathcal{O}_L$ que yacen sobre un primo $\mathfrak{p}$ de $\mathcal{O}_K$, y $e_1, \ldots, e_r$ y $f_1, \ldots, f_r$ sus índices de ramificación y grados residuales, respectivamente. Entonces*

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

Aunque en apariencia sencilla, la demostración de este teorema no es para nada evidente. Para desarrollarla necesitaremos emplear el siguiente teorema, cuya demostración tampoco es sencilla. Iremos intercalando ambas pruebas para facilitar la compresión de las mismas.

Previamente, es necesario introducir una nueva notación: siendo I ideal de un anillo de enteros algebraicos $\mathcal{O}_K$ cualquiera. Denotamos por

$$||I|| := |\mathcal{O}_K / I|$$

al índice de I como subgrupo aditivo de $\mathcal{O}_K$.

Teorema 3.8. *Sea $K \subset L$ una extensión de cuerpos numéricos, con n=[L:K], y $\mathcal{O}_K$, $\mathcal{O}_L$ sus respectivos anillos de enteros algebraicos.*

(a) Para I, J ideales en $\mathcal{O}_K$

$$||IJ|| = ||I|| \cdot ||J||.$$

(b) Sea I ideal en $\mathcal{O}_K$ e $I\mathcal{O}_L$ el ideal extendido en $\mathcal{O}_L$. Se tiene que

$$||I\mathcal{O}_L|| = ||I||^n.$$

Demostración (Teorema 3.8(a)). Sean I, J ideales en $\mathcal{O}_K$, y sean

$$I = \mathfrak{p}_1^{a_1} \cdot \ \ldots \ \cdot \mathfrak{p}_r^{a_r} \cdot \mathfrak{p}_{r+1}^{a_{r+1}} \cdot \ \ldots \ \cdot \mathfrak{p}_s^{a_s},$$

$$J = \mathfrak{p}_1^{b_1} \cdot \ \ldots \ \cdot \mathfrak{p}_r^{b_r} \cdot \mathfrak{q}_1^{c_1} \cdot \ \ldots \ \cdot \mathfrak{q}_t^{c_t}$$

sus descomposiciones en ideales primos de $\mathcal{O}_K$. La estrategia que seguiremos consiste en lo siguiente: en primer lugar, veremos que el resultado es cierto para ideales coprimos. De esta forma, se llegaría a que

$$||IJ|| = ||\mathfrak{p}_1^{a_1+b_1}|| \cdot \ \ldots \ \cdot ||\mathfrak{p}_r^{a_r+b_r}|| \cdot ||\mathfrak{p}_{r+1}^{a_{r+1}}|| \cdot \ \ldots \ \cdot ||\mathfrak{p}_s^{a_s}|| \cdot ||\mathfrak{q}_1^{c_1}|| \cdot \ \ldots \ \cdot ||\mathfrak{q}_t^{c_t}||. \quad (3.1)$$

En segundo lugar, pasaremos a demostrar que para todo ideal primo $\mathfrak{p} \in \mathcal{O}_K$ se tiene que $||\mathfrak{p}^m|| = ||\mathfrak{p}||^m$ para todo $m \in \mathbb{Z}^+$. Así, retomando la expresión (3.1), podemos extraer los exponentes y reagrupar, concluyendo lo que se quiere demostrar.

Demostramos en primer lugar que el resultado es cierto para ideales coprimos. Basta aplicar del Teorema Chino del resto para ideales (ver [3, Proposición

12.3.1 en Capítulo 12]), que nos asegura que si I, J son coprimos, entonces existe un isomorfismo de anillos

$$\mathcal{O}_K/IJ \longrightarrow \mathcal{O}_K/I \times \mathcal{O}_K/J.$$

Es claro que, en consecuencia, $|\mathcal{O}_K/IJ| = |\mathcal{O}_K/I| \cdot |\mathcal{O}_K/J|$ y por tanto,

$$||IJ|| = ||I|| \cdot ||J||.$$

Pasamos ahora a demostrar que para todo ideal primo $\mathfrak{p} \subset \mathcal{O}_K$ y $m \in \mathbb{Z}^+$, $||\mathfrak{p}^m|| = p^m$. Para ello consideramos la cadena de ideales

$$\mathcal{O}_K \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \cdots \supset \mathfrak{p}^m.$$

Por el Tercer Teorema de Isomorfía para grupos tenemos $(\mathcal{O}_K/\mathfrak{p}^2)/(\mathfrak{p}/\mathfrak{p}^2) \cong \mathcal{O}_K/\mathfrak{p}$, esto es, $|\mathcal{O}_K/\mathfrak{p}^2| = |\mathcal{O}_K/\mathfrak{p}| \cdot |\mathfrak{p}/\mathfrak{p}^2|$, considerando los ideales como grupos aditivos. De manera recursiva, podemos seguir aplicando este resultado hasta obtener

$$|\mathcal{O}_K/\mathfrak{p}^m| = |\mathcal{O}_K/\mathfrak{p}| \cdot |\mathfrak{p}/\mathfrak{p}^2| \cdot \cdots \cdot |\mathfrak{p}^{m-1}/\mathfrak{p}^m|. \tag{3.2}$$

Así, demostrando $||\mathfrak{p}|| = |\mathfrak{p}^k/\mathfrak{p}^{k+1}|$ para todo $k \in \{1, \ldots, m-1\}$, llegaríamos al resultado que buscamos.

Al estar en un dominio de Dedekind sabemos que $\mathfrak{p}^k \neq \mathfrak{p}^{k+1}$, pues son descomposiciones de ideales primos distintas. De esta forma, siempre podemos tomar un $\alpha \in \mathfrak{p}^k - \mathfrak{p}^{k+1}$. Así, fijando un α de estas características, es posible definir el isomorfismo

$$\begin{aligned} \varphi : \mathcal{O}_K/\mathfrak{p} &\xrightarrow{\cong} \alpha\mathcal{O}_K/\alpha\mathfrak{p} \\ a + \mathfrak{p} &\longmapsto \alpha a + \alpha\mathfrak{p}. \end{aligned}$$

Por otra parte, como $\alpha \in \mathfrak{p}^k$, $\alpha\mathcal{O}_K \subset \mathfrak{p}^k$ y podemos definir un segundo homomorfismo

$$\begin{aligned} \phi : \alpha\mathcal{O}_K &\longrightarrow \mathfrak{p}^k/\mathfrak{p}^{k+1} \\ \alpha a &\longmapsto \alpha a + \mathfrak{p}^{k+1}, \end{aligned}$$

cuyo núcleo e imagen son, respectivamente,

$$ker\phi = (\alpha\mathcal{O}_K) \cap (\mathfrak{p}^{k+1}) \quad \text{e} \quad Im\phi = ((\alpha\mathcal{O}_K) + \mathfrak{p}^{k+1})/\mathfrak{p}^{k+1}.$$

Ahora probaremos que

$$(\alpha\mathcal{O}_K) \cap (\mathfrak{p}^{k+1}) = \alpha\mathfrak{p} \quad \text{y} \quad (\alpha\mathcal{O}_K) + \mathfrak{p}^{k+1} = \mathfrak{p}^k. \tag{3.3}$$

De esta forma, aplicando el Primer Teorema de Isomorfía y el isomorfismo φ, tendremos que

$$\mathfrak{p}^k/\mathfrak{p}^{k+1} \cong \alpha\mathcal{O}_K/\alpha\mathfrak{p} \cong \mathcal{O}_K/\mathfrak{p},$$

concluyendo que $||\mathfrak{p}|| = |\mathfrak{p}^k/\mathfrak{p}^{k+1}|$.

Demostramos las igualdades (3.3) utilizando el máximo común divisor y mínimo común múltiplo. Sabemos que α pertenece a $\mathfrak{p}^k$ pero no a $\mathfrak{p}^{k+1}$, entonces en la descomposición de $\alpha\mathcal{O}_K$ en ideales primos aparece $\mathfrak{p}$ precisamente con exponente k; es decir,

$$\alpha\mathcal{O}_K = \mathfrak{p}^k \cdot \mathfrak{p}_2^{a_2} \cdot \cdots \cdot \mathfrak{p}_s^{a_s},$$

siendo $\mathfrak{p}_2, \ldots, \mathfrak{p}_s$ ideales primos distintos de $\mathfrak{p}$ y $a_2, \ldots, a_s \in \mathbb{Z}^+$. Por su parte, la descomposición en primos de $\mathfrak{p}^{k+1}$ es exactamente $\mathfrak{p}^{k+1}$. Recordando la Definición 2.19 y atendiendo a la Observación 2.20, llegamos a que

$$\alpha\mathcal{O}_K + \mathfrak{p}^{k+1} = mcd(\alpha\mathcal{O}_K, \mathfrak{p}^{k+1}) = \mathfrak{p}^k,$$

mientras que

$$\alpha\mathcal{O}_K \cap \mathfrak{p}^{k+1} = mcm(\alpha\mathcal{O}_K, \mathfrak{p}^{k+1}) = \alpha\mathcal{O}_K\mathfrak{p} = \alpha\mathfrak{p},$$

tal y como queríamos probar. Por tanto, por la relación (3.2), se concluye que

$$||\mathfrak{p}^m|| = |\mathcal{O}_K/\mathfrak{p}^m| = ||\mathfrak{p}|| \cdot ||\mathfrak{p}|| \cdot \ \ldots \ \cdot ||\mathfrak{p}|| = ||\mathfrak{p}||^m.$$

Demostración (Teorema 3.7 caso particular $K = \mathbb{Q}$). Demostramos el Teorema 3.7 en el caso particular en que K=$\mathbb{Q}$. Tomamos un ideal primo $\mathfrak{p}$ en $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, que será de la forma $p\mathbb{Z}$, con p un número primo entero. Descomponemos $\mathfrak{p}\mathcal{O}_L$ en factores primos de $\mathcal{O}_L$:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}.$$

Del Teorema 3.8(a) se sigue que

$$||\mathfrak{p}\mathcal{O}_L|| = ||\prod_{i=1}^{r} \mathfrak{q}_i^{e_i}|| = \prod_{i=1}^{r} ||\mathfrak{q}_i^{e_i}|| = \prod_{i=1}^{r} ||\mathfrak{q}_i||^{e_i}.$$

Por otra parte, sabemos que para todo $i \in \{1, \ldots, n\}$ el grado de la extensión

$$\mathcal{O}_K/\mathfrak{p} \longrightarrow \mathcal{O}_L/\mathfrak{q}_i$$

es f_i por la definición de grado residual. Como en este caso $\mathcal{O}_K/\mathfrak{p} = \mathbb{Z}/\mathfrak{p} = \mathbb{Z}/p\mathbb{Z}$, tenemos que $\mathcal{O}_L/\mathfrak{q}_i$ es un $\mathbb{Z}_p$-espacio vectorial de dimensión f_i, luego

$$|\mathcal{O}_L/\mathfrak{q}_i| = ||\mathfrak{q}_i|| = p^{f_i}.$$

De esta forma, volviendo a lo anterior

$$||\mathfrak{p}\mathcal{O}_L|| = \prod_{i=1}^{r} (p^{f_i})^{e_i} = \prod_{i=1}^{r} p^{e_i f_i} = p^{\sum_{i=1}^{r} e_i f_i}.$$

Por su parte, en el capítulo anterior demostramos, tal y como indica la Observación 2.18, que al tomar el ideal (p) de $\mathbb{Z}$ y extenderlo a $\mathcal{O}_L$ se tiene que $|\mathcal{O}_L/(p)\mathcal{O}_L|| = p^n$, con $n = [L : \mathbb{Q}]$. Concluimos que

$$p^n = ||\mathfrak{p}\mathcal{O}_L|| = p^{\sum_{i=1}^{r} e_i f_i},$$

esto es,

$$n = \sum_{i=1}^{r} e_i f_i,$$

como queríamos demostrar.

Demostración (Teorema 3.8(b)). Basta probar esta igualdad para ideales primos en $\mathcal{O}_K$ ya que siempre es posible descomponer cualquier ideal en sus factores primos y aplicar el apartado (a) del Teorema 3.8.
Sea entonces $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$. Como $\mathcal{O}_K \subset \mathcal{O}_L$, tenemos la inclusión natural $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$, luego podemos considerar $(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L, +)$ como un $(\mathcal{O}_K/\mathfrak{p})$-espacio vectorial donde el producto escalar es el producto en $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ como anillo.
Se pide demostrar que $dim(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = n$ como espacio vectorial sobre $\mathcal{O}_K/\mathfrak{p}$, de tal forma que

$$||\mathfrak{p}\mathcal{O}_L|| = |\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L| = |\mathcal{O}_K/\mathfrak{p}|^n = ||\mathfrak{p}||^n.$$

Comenzaremos probando que $dim(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) \leq n$. Para ello, tomamos $\alpha_1, \ldots, \alpha_{n+1} \in \mathcal{O}_L$ y veremos que $\alpha_1 + \mathfrak{p}\mathcal{O}_L, \ldots, \alpha_{n+1} + \mathfrak{p}\mathcal{O}_L$ son linealmente dependientes sobre $\mathcal{O}_K/\mathfrak{p}$.

Como $[L : K] = n < n + 1$, $\{\alpha_1, \ldots, \alpha_{n+1}\}$ es necesariamente un conjunto linealmente dependiente sobre K; es decir, existirán $a_1, \ldots, a_{n+1} \in K$ no todos nulos tales que

$$a_1\alpha_1 + \cdots + a_{n+1}\alpha_{n+1} = 0.$$

Nuestro objetivo ahora es ver que a partir de esta dependencia siemre se puede encontrar una dependencia lineal de $\alpha_1 + \mathfrak{p}\mathcal{O}_L, \ldots, \alpha_n + \mathfrak{p}\mathcal{O}_L \in \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ sobre $\mathcal{O}_K/\mathfrak{p}$. Considerando la Proposición 2.9, podemos asegurar la existencia de un $m \in \mathbb{Z}$ de manera que $ma_1, \ldots, ma_{n+1} \in \mathcal{O}_K$. Llamamos $b_i = ma_i$ para todo $i = 1, \ldots, n + 1$. Tenemos entonces dependencia lineal sobre $\mathcal{O}_K$, esto es,

$$b_1\alpha_1 + \cdots + b_{n+1}\alpha_{n+1} = 0,$$

con al menos un b_i no nulo.

Para hallar la dependencia sobre $\mathcal{O}_K/\mathfrak{p}$ basta con poder asegurar que no todos los coeficientes $b_1, \ldots, b_{n+1}$ pertenecen a $\mathfrak{p}$. En caso contrario, tendríamos $\beta_i + \mathfrak{p} = 0 + \mathfrak{p}$ para todo $i \in \{1, \ldots, n+1\}$. Esto se consigue aplicando el Corolario

2.22 para $I = \mathfrak{p}$ y $J = (b_1, \ldots, b_{n+1})$. El corolario asegura la existencia de un $\gamma \in K$ tal que

$$\gamma(\beta_1, \ldots, \beta_{n+1}) \subset \mathcal{O}_K \text{ y } \gamma(\beta_1, \ldots, \beta_{n+1}) \not\subset \mathfrak{p},$$

lo que implica que

$$(\gamma b_1 + \mathfrak{p})(\alpha_1 + \mathfrak{p}\mathcal{O}_L) + \cdots + (\gamma b_{n+1} + \mathfrak{p})(\alpha_{n+1} + \mathfrak{p}\mathcal{O}_L) = 0$$

es una dependencia lineal sobre $\mathcal{O}_K/\mathfrak{p}$, pues existe algún $\gamma b_i + \mathfrak{p} \neq 0 + \mathfrak{p}$. Tomaríamos entonces este conjunto de coeficientes para establecer la dependencia lineal.

Hemos visto que $dim(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) \leq n$. Vamos a comprobar que es exactamente n. Para ello haremos uso del caso particular del Teorema 3.7 que hemos demostrado anteriormente. A su vez, consideramos la extensión $\mathbb{Q} \hookrightarrow K$ y el ideal $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z} = (p)$ en $\mathbb{Z}$ para algún primo $p \in \mathbb{Z}$. Sea

$$(p)\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \cdot \ \ldots \ \cdot \mathfrak{p}_r^{e_r} \tag{3.4}$$

la descomposición en ideales primos de $\mathcal{O}_K$, donde $\mathfrak{p}$ es uno de los factores. Sin pérdida de generalidad podemos asumir que $\mathfrak{p}_1 = \mathfrak{p}$. Basándonos en lo que acabamos de probar, tenemos que $dim_{\mathcal{O}_K/\mathfrak{p}_i}(\mathcal{O}_L/\mathfrak{p}_i\mathcal{O}_L) = n_i \leq n$. Probemos que, de hecho, $n_i = n$ para todo $i \in \{1, 2, \ldots, r\}$.

Extendiendo la descomposición de la expresión (3.4) a $\mathcal{O}_L$, tenemos que

$$(p)\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}\mathcal{O}_L.$$

Tomando índices y aplicando el Teorema 3.8(a), llegamos a que

$$||(p)\mathcal{O}_L|| = \prod_{i=1}^{r} ||\mathfrak{p}_i\mathcal{O}_L||^{e_i}.$$

Sabiendo que n_i es la dimensión de $\mathcal{O}_L/\mathfrak{p}_i\mathcal{O}_L$ como $\mathcal{O}_K/\mathfrak{p}_i$-espacio vectorial, se tiene que

$$||\mathfrak{p}_i\mathcal{O}_L|| = |\mathcal{O}_L/\mathfrak{p}_i\mathcal{O}_L| = |\mathcal{O}_K/\mathfrak{p}_i|^{n_i} = ||\mathfrak{p}_i||^{n_i},$$

luego

$$||(p)\mathcal{O}_L|| = \prod_{i=1}^{r} (||\mathfrak{p}_i||^{n_i})^{e_i}.$$

Como $||\mathfrak{p}_i|| = |\mathcal{O}_K/\mathfrak{p}_i| = |\mathbb{Z}/p\mathbb{Z}|^{f_i} = p^{f_i}$, con f_i el grado residual $f(\mathfrak{p}_i \mid (p))$, entonces

$$||(p)\mathcal{O}_L|| = \prod_{i=1}^{r} ((p^{f_i})^{n_i})^{e_i} = p^{\sum_{i=1}^{r} f_i n_i e_i}.$$

Por otro lado, si $m = [K : \mathbb{Q}]$ entonces $[L : \mathbb{Q}] = n \cdot m$, y sabemos por la Observación 2.18 que $||(p)\mathcal{O}_L|| = p^{m \cdot n}$, luego

$$m \cdot n = \sum_{i=1}^{r} f_i e_i n_i.$$

Por el caso particular del Teorema 3.7 tenemos que $m = \sum_{i=1}^{r} f_i e_i$. Como $n_i \leq n$ para todo $i \in \{1, \ldots, r\}$, para darse la igualdad necesariamente se debe cumplir que $n_i = n$, concluyendo así que el resultado es cierto para $\mathfrak{p}$ ideal primo de $\mathcal{O}_K$, tal y como buscábamos.

Demostración (Teorema 3.7 caso general). Una vez demostrados los anteriores apartados, estamos en disposición de demostrar el Teorema 3.7 para el caso general. En las condiciones del teorema tenemos que, por el Teorema 3.8(a),

$$||\mathfrak{p}\mathcal{O}_L|| = \left|\left|\prod_{i=1}^{r} \mathfrak{q}_i^{e_i}\right|\right| = \prod_{i=1}^{r} ||\mathfrak{q}_i||^{e_i}.$$

Aplicando la misma idea que para el caso particular tenemos que

$$||\mathfrak{q}_i|| = |\mathcal{O}_L/\mathfrak{q}_i| = |\mathcal{O}_K/\mathfrak{p}|^{f_i} = ||\mathfrak{p}||^{f_i}$$

Luego,

$$||\mathfrak{p}\mathcal{O}_L|| = \prod_{i=1}^{r} ||\mathfrak{q}_i||^{e_i} = \prod_{i=1}^{r} (||\mathfrak{p}||^{f_i})^{e_i} = ||\mathfrak{p}||^{\sum_{i=1}^{r} e_i f_i}$$

Además, por Teorema 3.8(b), sabemos que $||\mathfrak{p}\mathcal{O}_L|| = ||\mathfrak{p}||^n$, lo que directamente implica que $\sum_{i=1}^{r} e_i f_i = n$. □

El siguiente y último teorema de esta sección evidencia que existe una correspondencia entre la factorización de ideales primos $\mathfrak{p}$ de $\mathcal{O}_K$ extendidos en un anillo de enteros algebraicos mayor y la factorización de polinomios con coeficientes en el cuerpo finito $\mathcal{O}_K/\mathfrak{p}$. Este resultado nos valdrá para todo ideal $\mathfrak{p}$ salvo un número finito.

Previamente, debemos tener en cuenta ciertas consideraciones. Sea $K \subset L$ una extensión de cuerpos numéricos, con $n = [L : K]$. Recordemos que la extensión es simple, luego $L = K(\alpha)$ para $\alpha \in L$ fijado, y además, por la Proposición 2.9, podemos tomar $\alpha \in \mathcal{O}_L$.

Primero, observamos que como $n = [K(\alpha) : K]$, no es difícil ver que $\mathcal{O}_K[\alpha]$ es un $\mathcal{O}_K$-módulo de rango n. A su vez, si $[K : \mathbb{Q}] = m$, ya hemos visto en la Sección 2.2 que $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo de rango m. Con esto, llegamos a que $\mathcal{O}_K[\alpha]$ es un $\mathbb{Z}$-módulo de rango $n \cdot m$. Por otra parte, tenemos que $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}] = n \cdot m$, por lo que $\mathcal{O}_L$ es también un $\mathbb{Z}$-módulo de rango $n \cdot m$.

Por lo tanto, $\mathcal{O}_K[\alpha] \trianglelefteq \mathcal{O}_L$ son grupos abelianos libres del mismo rango y, por ello, $|\mathcal{O}_L/\mathcal{O}_K[\alpha]|$ es finito.

Ahora, fijemos un ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$. Sabemos que $\mathfrak{p} \cap \mathbb{Z} = (p)$, con $p \in \mathbb{Z}$ primo. Escogeremos $\mathfrak{p}$ de tal manera que $p \nmid |\mathcal{O}_L/\mathcal{O}_K[\alpha]|$.

Para todo polinomio $h(x) \in \mathcal{O}_K[x]$ denotamos por $\overline{h}(x) \in (\mathcal{O}_K/\mathfrak{p})[x]$ al polinomio obtenido al reducir los coeficientes de $h(x)$ a su clase módulo $\mathfrak{p}$. Particularmente, si denotamos $g(x) := m_{\alpha,K}(x) \in \mathcal{O}_K[x]$ se sigue que $\overline{g}(x) \in (\mathcal{O}_K/\mathfrak{p})[x]$. Ya sabemos que $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo, luego $(\mathcal{O}_K/\mathfrak{p})[x]$ es dominio de factorización única. Así, $\overline{g}(x)$ se factoriza de forma única en $(\mathcal{O}_K/\mathfrak{p})[x]$ como

$$\overline{g}(x) = \overline{g_1}(x)^{e_1} \cdot \overline{g_2}(x)^{e_2} \cdot \cdots \cdot \overline{g_r}(x)^{e_r}, \tag{3.5}$$

con $\overline{g_i}(x) \in (\mathcal{O}_K/\mathfrak{p})[x]$ mónicos e irreducibles y tomando $g_i \in \mathcal{O}_K[x]$ mónicos.

Teorema 3.9. *En las consideraciones anteriores, se tiene que*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdot \ \ldots \ \cdot \mathfrak{q}_r^{e_r},$$

siendo $\mathfrak{q}_i = \mathfrak{p}\mathcal{O}_L + (g_i(\alpha))$ *para todo* $i \in \{1, \ldots, r\}$*, y con* $e_i = e(\mathfrak{q}_i/\mathfrak{p}_i)$ *y* $f_i = f(\mathfrak{q}_i/\mathfrak{p}_i) = deg(g_i)$ *los índices de ramificación y grados residuales correspondientes.*

Demostración. Procedemos a desarrollar la demostración probando los siguientes tres apartados:

(1) Para todo $i \in \{1, \ldots, r\}$, o bien $\mathfrak{q}_i = \mathcal{O}_L$, o bien $\mathcal{O}_L/\mathfrak{q}_i$ es un cuerpo cuyo cardinal es $|\mathcal{O}_K/\mathfrak{p}|^{f_i}$.
(2) Para $i, j \in \{1, \ldots, r\}$, si $i \neq j$ entonces

$$\mathfrak{q}_i + \mathfrak{q}_j = \mathcal{O}_L.$$

(3) $\mathfrak{p}\mathcal{O}_L \mid \mathfrak{q}_1^{e_1} \cdot \ \ldots \ \cdot \mathfrak{q}_r^{e_r}$.

Veamos por qué es suficiente probar (1), (2) y (3) para demostrar este teorema.

Suponemos sin pérdida de generalidad que

$$\mathfrak{q}_1, \ldots, \mathfrak{q}_s \neq \mathcal{O}_L \quad \text{y} \quad \mathfrak{q}_{s+1}, \ldots, \mathfrak{q}_r = \mathcal{O}_L,$$

siendo $s \leq r$. En (1) demostramos que los ideales distintos del total, $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$, son ideales primos de $\mathcal{O}_L$ que yacen sobre $\mathfrak{p}$ (pues lo contienen) y, además, que $f(\mathfrak{q}_i \mid \mathfrak{p}) = f_i$ para todo $i \leq s$. El punto (2) muestra que estos $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ son distintos y en (3) vemos que $\mathfrak{p}\mathcal{O}_L$ divide a $\mathfrak{q}_1^{e_1} \cdot \ \ldots \ \cdot \mathfrak{q}_r^{e_r}$. Por tanto, al factorizar $\mathfrak{p}\mathcal{O}_L$ en ideales primos en $\mathcal{O}_L$ tenemos

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{d_1} \cdot \ \ldots \ \cdot \mathfrak{q}_s^{d_s},$$

con $d_i \leq e_i$, para todo $i = 1, \ldots, s$. Se sigue del Teorema 3.7 que

$$n = d_1 f_1 + \cdots + d_s f_s,$$

mientras que, como $n = deg(g(x)) = deg(m_{\alpha,K}(x))$, de la ecuación (3.5) se sigue

$$n = e_1 f_1 + \cdots + e_r f_r.$$

Por tanto, como $s \leq r$ y $d_i \leq e_i$, debe ser

$$r = s \text{ y } e_i = d_i \text{ para todo } i = 1, \ldots, r.$$

Pasamos a demostrar (1), (2) y (3).

(1) Sea $F_i := ((\mathcal{O}_K/\mathfrak{p})[x])/(\overline{g_i}(x))$, para todo $i \in \{1, \ldots, r\}$. Como $\overline{g_i}(x)$ es por hipótesis irreducible en $\mathcal{O}_K/\mathfrak{p}[x]$, se tiene que $(\overline{g_i}(x))$ es un ideal maximal. Por tanto, F_i es un cuerpo con $||F_i|| = |\mathcal{O}_K/\mathfrak{p}|^{f_i}$, siendo $f_i = deg(\overline{g_i}(x)) = deg(g_i(x))$.
Planteamos el homomorfismo

$$\begin{aligned} \phi : \mathcal{O}_K[x] &\longrightarrow F_i \\ h(x) &\longmapsto \overline{h}(x) + (\overline{g_i}(x)). \end{aligned}$$

Se tiene que $ker\phi = (\mathfrak{p}, g_i(x))$ ya que

$$\overline{h} + (\overline{g_i}(x)) = 0 \Longleftrightarrow \overline{h} \in (\overline{g_i}(x)) \text{ ó } h(x) \in \mathfrak{p}(x) \Longleftrightarrow h \in \mathfrak{p}[x] \text{ ó } h \in (g_i(x)).$$

Además, claramente ϕ es sobreyectiva al ser una proyección sobre el cociente. Por tanto, se sigue el isomorfismo

$$\mathcal{O}_K[x]/(\mathfrak{p}, g_i(x)) \cong F_i, \tag{3.6}$$

y al ser F_i cuerpo, se deduce que $ker\phi$ es maximal.
A continuación consideramos el homomorfismo evaluación en α, $\mathcal{O}_K[x] \longrightarrow \mathcal{O}_L$, y componiéndolo con el homomorfismo cociente, se tiene de manera natural el homomorfismo siguiente:

$$\begin{aligned} \Phi : \mathcal{O}_K[x] &\longrightarrow \mathcal{O}_L/\mathfrak{q}_i \\ h(x) &\longmapsto h(\alpha) + \mathfrak{q}_i. \end{aligned}$$

Como $\mathfrak{q}_i = \mathfrak{p}\mathcal{O}_L + (g_i(\alpha))$, observamos que

$$ker\phi = (\mathfrak{p}, g_i(x)) \subset ker\Phi.$$

Efectivamente, tomando $h_1(x) + h_2(x) \in ker\phi$, con $h_1(x) \in \mathfrak{p}[x], h_2(x) \in (g_i)$, se sigue que

$$\Phi(h_1(x) + h_2(x)) = h_1(\alpha) + h_2(\alpha),$$

donde $h_1(\alpha) \in \mathfrak{p}\mathcal{O}_L \subset \mathfrak{q}_i$ y $h_2(\alpha) \in (g_i(\alpha)) \subset \mathfrak{q}_i$.
Por tanto, $\Phi(h_1(x) + h_2(x)) \in \mathfrak{q}_i$. De la expresión (3.6) tenemos que $(\mathfrak{p}, g_i)$ es maximal, luego únicamente existen dos posibilidades: $ker\Phi = (\mathfrak{p}, gi)$ o $ker\Phi = \mathcal{O}_K[x]$.
La estrategia para demostrar (1) se basará en probar que

$$\mathcal{O}_K/ker\Phi \cong \mathcal{O}_L/\mathfrak{q}_i. \tag{3.7}$$

De esta forma, si $ker\Phi = (\mathfrak{p}, g_i)$, entonces

$$F_i \cong \mathcal{O}_K/(\mathfrak{p}, g_i) \cong \mathcal{O}_L/\mathfrak{q}_i$$

es un cuerpo y, además,

$$||\mathcal{O}_L/\mathfrak{q}_i|| = ||F_i|| = ||\mathcal{O}_K/\mathfrak{p}||^{f_i}.$$

Por otra parte, si $ker\Phi = \mathcal{O}_K[x]$, entonces

$$(\mathcal{O}_K[x])/(\mathcal{O}_K[x]) \cong (0) \cong \mathcal{O}_L/\mathfrak{q}_i,$$

lo que implica que $\mathfrak{q}_i = \mathcal{O}_L$. Para probar la expresión (3.7), debemos asegurar que Φ es sobreyectiva, esto es, $Im\Phi = \mathcal{O}_L/\mathfrak{q}_i$. Sabemos, por construcción de Φ, que $Im\Phi = (\mathcal{O}_K[\alpha] + \mathfrak{q}_i)/\mathfrak{q}_i$, luego es suficiente con ver que

$$\mathcal{O}_L = \mathcal{O}_K[\alpha] + \mathfrak{q}_i.$$

Sea $p \in \mathbb{Z}$ el primo tal que $(p) = \mathfrak{p} \cap \mathbb{Z}$ que consideramos en los preliminares del teorema. Tenemos entonces que

$$(p)\mathcal{O}_L \subset (p)\mathcal{O}_L + (g_i(x)) = \mathfrak{q}_i,$$

en consecuencia, $(p)\mathcal{O}_L \subset \mathfrak{q}_i$. Entonces, se sigue que

$$\mathcal{O}_K[\alpha] + (p)\mathcal{O}_L \subset \mathcal{O}_K[\alpha] + \mathfrak{q}_i \subset \mathcal{O}_L,$$

luego bastaría probar que $\mathcal{O}_L \subset \mathcal{O}_K[\alpha] + (p)\mathcal{O}_L$. De hecho, veremos que se da la igualdad.
Para facilitar la lectura denotaremos $H := \mathcal{O}_K[\alpha] + (p)\mathcal{O}_L$. Debemos probar entonces que $\mathcal{O}_L = H$.
Es claro que $H \subset \mathcal{O}_L$ al ser un subgrupo aditivo del mismo. Como ya vimos en las consideraciones previas, $|\mathcal{O}_L/\mathcal{O}_K[\alpha]|$ es finito y, por otro lado, debido a la Observación 2.18, $|\mathcal{O}_L/(p)\mathcal{O}_L| = p^{[L:\mathbb{Q}]}$. Además, tenemos que $\mathcal{O}_K[\alpha] \trianglelefteq H$, y $p\mathcal{O}_L \trianglelefteq H$, y esto implica que

$$|\mathcal{O}_L/H| \text{ divide a } |\mathcal{O}_L/\mathcal{O}_K[\alpha]| \text{ y}$$

$$|\mathcal{O}_L/H| \text{ divide a } |\mathcal{O}_L/(p)\mathcal{O}_L|.$$

En otras palabras, $|\mathcal{O}_L/H|$ es divisor común de una potencia de p y, a su vez, del índice $|\mathcal{O}_L/\mathcal{O}_K[\alpha]|$, y por las hipótesis iniciales sabemos que $|\mathcal{O}_L/\mathcal{O}_K[\alpha]|$ no es divisible por p.
Necesariamente esto implica que $|\mathcal{O}_L/H| = 1$, y por tanto $H = \mathcal{O}_L$.
En conclusión, Φ es sobreyectiva y $\mathcal{O}_K/ker\Phi \cong \mathcal{O}_L/\mathfrak{q}_i$, de manera que, o bien $\mathfrak{q}_i = \mathcal{O}_L$, o bien $\mathcal{O}_L/\mathfrak{q}_i$ es un cuerpo de orden $|\mathcal{O}_K/\mathfrak{p}|^{f_i}$, como queríamos demostrar.

(2) Tenemos que $\overline{g_1}(x), \ldots, \overline{g_r}(x)$ son distintos e irreducibles en $\mathcal{O}_K/\mathfrak{p}[x]$. La identidad de Bézout nos dice que para todo par de polinomios $\overline{g_i}(x), \overline{g_j}(x)$ existen $\overline{h_1}, \overline{h_2} \in (\mathcal{O}_K/\mathfrak{p})[x]$ que verifican

$$\overline{g_i}(x)\overline{h_1}(x) + \overline{g_j}(x)\overline{h_2}(x) = \overline{1},$$

es decir,

$$g_i(x)h_1(x) + g_j(x)h_2(x) \equiv 1 \text{ (mód } \mathfrak{p}). \tag{3.8}$$

Esto significa que los coeficientes de los términos no independientes del polinomio $g_i(x)h_1(x) + g_j(x)h_2(x)$ pertenecen a $\mathfrak{p}$ mientras que el término independiente es congruente con 1 módulo $\mathfrak{p}$.
Al evaluar en α, tendremos que

$$g_i(\alpha)h_1(\alpha) + g_j(\alpha)h_2(\alpha) \equiv 1 \text{ (mód } \mathfrak{p}\mathcal{O}_L),$$

Esto implica que $1 \in (\mathfrak{p}, g_i(\alpha), g_j(\alpha))$, que por definición es igual a $\mathfrak{q}_i + \mathfrak{q}_j$. Se deduce que $\mathfrak{q}_i + \mathfrak{q}_j = \mathcal{O}_L$.

(3) Por el Corolario 2.23 sabemos que es equivalente demostrar $\prod_{i=1}^{r} \mathfrak{q}_i^{e_i} \subset \mathfrak{p}\mathcal{O}_L$. De ahora en adelante denotaremos $\gamma_i := g_i(\alpha)$, luego $\mathfrak{q}_i = (\mathfrak{p}, \gamma_i)$. Se sigue que

$$\mathfrak{q}_i^{e_i} = (\mathfrak{p}, \gamma_i)^{e_i} = (\mathfrak{p}, \gamma_i^{e_i}),$$

entonces,

$$\prod_{i=1}^{r} \mathfrak{q}_i^{e_i} = (\mathfrak{p}, \gamma_1^{e_1}) \cdot (\mathfrak{p}, \gamma_2^{e_2}) \cdot \cdots \cdot (\mathfrak{p}, \gamma_r^{e_r}) = (\mathfrak{p}, \prod_{i=1}^{r} \gamma_i^{e_i}).$$

Tenemos que ver que $(\mathfrak{p}, \prod_{i=1}^{r} \gamma_i^{e_i}) = \mathfrak{p}\mathcal{O}_L$. Para ello, será suficiente con comprobar que $\prod_{i=1}^{r} \gamma_i^{e_i} \in \mathfrak{p}\mathcal{O}_L$.
Sabiendo que $\overline{g}(x) = \overline{g_1}(x)^{e_1} \cdot \overline{g_2}(x)^{e_2} \cdot \cdots \cdot \overline{g_r}(x)^{e_r}$, tenemos:

$$g(x) \equiv g_1(x)^{e_1} \cdot g_2(x)^{e_2} \cdot \ \ldots \ \cdot g_r(x)^{e_r} \text{ (mód } \mathfrak{p}).$$

Evaluando en α, tenemos que

$$g_1(\alpha)^{e_1} \cdot g_2(\alpha)^{e_2} \cdot \ \ldots \ \cdot g_r(\alpha)^{e_r} = \gamma_1^{e_1} \cdot \gamma_2^{e_2} \cdot \ \ldots \ \cdot \gamma_r^{e_r} \equiv g(\alpha) = 0 \ (\text{mód } \mathfrak{p}\mathcal{O}_L).$$

Por tanto, concluimos que

$$\prod_{i=1}^{r} \mathfrak{q}_i^{e_i} = (\mathfrak{p}, \prod_{i=1}^{r} \gamma_i^{e_i}) \subset \mathfrak{p}\mathcal{O}_L.$$

□

Finalizamos este capítulo y la memoria con el problema que originalmente motivó este trabajo y el estudio de las extensiones de cuerpos numéricos y sus anillos de enteros algebraicos: el Teorema de Kronecker-Weber. Tal y como explicamos en la introducción, este teorema dice que toda *extensión abeliana* de $\mathbb{Q}$ está contenida en una *extensión ciclotómica*.

Definición 3.10. *Sea K un cuerpo. Decimos que $\mathbb{Q} \hookrightarrow K$ es una extensión abeliana si es una extensión de Galois cuyo grupo de Galois es abeliano.*

Definición 3.11. *Sea L un cuerpo. Decimos que $\mathbb{Q} \hookrightarrow L$ es una extensión ciclotómica si existe $\zeta \in \mathbb{C}$ raíz de la unidad tal que $L = \mathbb{Q}(\zeta)$.*

La Teoría de Galois nos permite hacer una primera reducción del problema, demostrando que basta con tomar extensiones abelianas cuyo grupo de Galois tenga orden p^r, siendo $p \in \mathbb{Z}$ un número primo y con $r \in \mathbb{Z}^+$. Esto se deduce de lo siguiente:

Sea $\mathbb{Q} \hookrightarrow K$ una extensión abeliana con grupo de Galois $G := Gal(K/\mathbb{Q})$, y sea $n = [K : \mathbb{Q}]$. Entonces, se tiene que G es un grupo abeliano finito de orden n y, por tanto,

$$G = G_1 \times \cdots \times G_s,$$

con G_i grupo de orden $p_i^{a_i}$ para todo $i \in \{1, \ldots, s\}$, donde

$$n = p_1^{a_1} \cdot \ \ldots \ \cdot p_s^{a_s}$$

es la descomposición en números primos de n. De esta forma, para cada $i \in \{1, \ldots, s\}$, podemos tomar

$$H_i := \prod_{j \neq i} G_j \trianglelefteq G.$$

Por la Teoría de Galois, sabemos que existe una correspondencia entre H_i y un cuerpo M_i, que estará formado por aquellos elementos de K invariantes al aplicar los elementos de H_i. Es más, también nos asegura que $\mathbb{Q} \hookrightarrow M_i \hookrightarrow K$ y que, como H_i es normal, M_i es una extensión de Galois de $\mathbb{Q}$ cuyo grupo de Galois es abeliano y de orden $p_i^{a_i}$.

Atendiendo a estas consideraciones, se tiene que si el teorema de Kronecker-Weber se cumple para extensiones abelianas con grupo de Galois de orden potencia de un número primo entonces, para todo $i \in \{1, \dots, s\}$, existe ζ_i raíz n_i-ésima de la unidad tal que

$$M_i \hookrightarrow \mathbb{Q}(\zeta_i).$$

Finalmente, se puede comprobar que en estas condiciones, podemos tomar $m = mcm(n_1, \dots, n_s)$ y se tiene que

$$K \hookrightarrow \mathbb{Q}(\zeta_m),$$

siendo ζ_m una raíz m-ésima de la unidad.

Gracias a esto somos capaces de hacer esta primera reducción del Teorema de Kronecker-Weber. El aspecto crucial que queremos recalcar es que, haciendo uso de la teoría introducida en esta memoria, se pueden simplicar aún más los casos a considerar en la demostración del teorema. En efecto, si $\mathbb{Q} \hookrightarrow K$ es una extensión abeliana de grado p^r, con $p \in \mathbb{Z}$ primo y $r \in \mathbb{Z}^+$, entonces podemos también asumir que el ideal (p) es el único ideal primo que se *ramifica* al extenderlo a $\mathcal{O}_K$.

Definición 3.12. *Sea $K \subset L$ una extensión de cuerpos numéricos y sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$. Decimos que $\mathfrak{p}$ ramifica en $\mathcal{O}_L$ si existe un ideal primo $\mathfrak{q} \subset \mathcal{O}_L$ que yace sobre $\mathfrak{p}$ y con índice de ramificación $e(\mathfrak{q}|\mathfrak{p}) \geq 2$.*

Entender cómo se reduce el Teorema de Kronecker-Weber al caso en el que (p) sea el único ideal que ramifica en $\mathcal{O}_K$ conlleva una mayor profundización en los conceptos introducidos en este último capítulo. Se recomienda consultar las notas del seminario [5]. Esto puede ser un buen punto de partida para una posible continuación de este trabajo.

Bibliografía

[1] Cox, D. A. *Galois Theory.* (2nd edition). John Wiley & Sons Incorporated. (2012).

[2] Couveignes, J. *Enumerating number fields.* Annals of Mathematics, 192(2) 487-497, (2020). Disponible en: https://doi.org/10.4007/annals.2020.192.2.4.

[3] Ireland, K. and Rosen M. *A Classical Introduction to Modern Number Theory.* Springer New York. (1998).

[4] Marcus, D. A. *Number Fields.* (2nd edition). Universitext, Springer. (2018).

[5] Travesa, A. *El teorema de Kronecker-Weber.* Seminari de Teoria de Nombres (UB-UAB-UPC) CSIC, Madrid. (2008)

[6] Zheng, Z. and Liu, F. *On the High Dimensional RSA Algorithm – A Public Key Cryptosystem Based on Lattice and Algebraic Number Theory.* (2022) Preprint. Disponible en: https://doi.org/10.48550/arXiv.2202.02675.

Ring of algebraic integers and its structure

Lara Niebla Cañete

Facultad de Ciencias • Sección de Matemáticas
Universidad de La Laguna
alu0101224596@ull.edu.es

Abstract

We aim to set the framework for modern algebraic number theory. We introduce the concept of number fields, as well as some basic tools. Next, we define the ring of algebraic integers and analyze its structure. Moreover, we prove that every ring of algebraic integers is a Dedekind domain. Lastly, we study how extensions of prime ideals in rings of algebraic integers are factored. Finally, we make a brief comment about a reduction of Kronecker-Weber's Theorem.

1. Introduction

Let K be a subfield of $\mathbb{C}$. K is a **number field** if it has finite dimension as a $\mathbb{Q}$-vector space, that is, if K is a finite field extension over $\mathbb{Q}$.

2. Rings of algebraic integers

An element $\alpha \in C$ is an **algebraic integer** if there exists a monic polynomial $p(x) \in \mathbb{Z}[x]$ that has α as a root.

Given K a number field, we define the **ring of algebraics integer** $\mathcal{O}_K$ as

$$\mathcal{O}_K := \{\alpha \in K \mid \alpha \text{ is an algebraic integer}\}.$$

$\mathcal{O}_K$ has a ring structure, moreover:

Theorem. *$(\mathcal{O}_K, +, \cdot)$ is a Dedekind domain.*

A Dedekind domain is an integral domain such that

(1) every ideal is finitely generated,
(2) every nonzero prime ideal is a maximal ideal and
(3) it is integrally closed in its field of fractions.

It is known that ideals in Dedekind domains are factored uniquely. Consequently, the previous result implies that, in a ring of algebraic integers, ideals have a unique factorization in prime ideals.

In other words, given any ideal I in a ring of algebraic integers $\mathcal{O}_K$, I is uniquely split as

$$I = \mathfrak{p}_1^{e_1} \cdot \ \dots \ \cdot \mathfrak{p}_r^{e_r},$$

where $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are different prime ideals in $\mathcal{O}_K$, and $e_i \in \mathbb{Z}^+$.

3. Splitting of primes in extensions

Let $K \subset L$ be a number fields extension, and $\mathfrak{p}$ a prime ideal in $\mathcal{O}_K$. We are able to extend $\mathfrak{p}$ in $\mathcal{O}_L$ through the natural inclusion $i : \mathcal{O}_K \hookrightarrow \mathcal{O}_L$, resulting in

$$\mathfrak{p}\mathcal{O}_L = \{\alpha_1\beta_1 + \cdots + \alpha_r\beta_r \mid \alpha_i \in \mathfrak{p},\ \beta_i \in \mathcal{O}_L,\ r \in \mathbb{Z}^+\}.$$

It is significant to note that the primality of $\mathfrak{p}\mathcal{O}_L$ cannot be concluded.

Example: Consider the number fields extension $\mathbb{Q} \subset \mathbb{Q}[i]$, with $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$ and $\mathcal{O}_{\mathbb{Q}[i]} = \mathbb{Z}[i]$ their ring of algebraic integers, respectively.

Choosing the ideal $2\mathbb{Z} = (2)$ in $\mathbb{Z}$, its extended ideal $(2)\mathbb{Z}[i]$ is not prime in $\mathbb{Z}[i]$, indeed, it splits as

$$(2)\mathbb{Z}[i] = \langle 1 - i \rangle^2.$$

Consequently, we aim to give a **factorization of the extended of a prime ideal in $\mathcal{O}_K$ in prime ideals of $\mathcal{O}_L$**.

This follows due to the correspondence established, for all but finitely many primes $\mathfrak{p}$ of $\mathcal{O}_K$, between the splitting of extended prime ideals and the factoring of polynomials with coefficients in the field $\mathcal{O}_K/\mathfrak{p}$. By doing so, we can determine the splitting of $\mathfrak{p}\mathcal{O}_L$ by factoring a certain polynomial mod $\mathfrak{p}$. The following theorem shows explicitly how this is done.

Let's consider $K \subset L$ a number fields extension of degree n, with $L = K(\alpha)$ for some $\alpha \in \mathcal{O}_L$.

We must fix a prime ideal $\mathfrak{p} \in \mathcal{O}_K$ such that p does not divide $|\mathcal{O}_L/\mathcal{O}_K[\alpha]|$, where $p \in \mathbb{Z}$ is the only prime number that verifies $\mathfrak{p} \cap \mathbb{Z} = (p)$.

Given a polynomial $h(x) \in \mathcal{O}_K[x]$, we let $\overline{h}(x) \in (\mathcal{O}_K/\mathfrak{p})[x]$ denote the polynomial obtained by reducing the coefficients of $h(x)$ mod $\mathfrak{p}$. We particularly do so for $g(x) := m_{\alpha,K}(x) \in \mathcal{O}_K[x]$.

$(\mathcal{O}_K/\mathfrak{p})[x]$ is a unique factorization domain since $\mathcal{O}_K/\mathfrak{p}$ is a field. Therefore, $\overline{g}(x)$ is uniquely factored in $(\mathcal{O}_K/\mathfrak{p})[x]$ as

$$\overline{g}(x) = \overline{g_1}(x)^{e_1} \cdot \overline{g_2}(x)^{e_2} \cdot \ \dots \ \cdot \overline{g_r}(x)^{e_r},$$

with $\overline{g_i}(x) \in (\mathcal{O}_K/\mathfrak{p})[x]$ monic and irreducibles polynomials, and $g_i \in \mathcal{O}_K[x]$ monic polynomials, for $i \in \{1, \dots, r\}$.

Theorem. *Following the previous discussion, it holds:*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdot \mathfrak{q}_2^{e_2} \cdot \ \dots \ \cdot \mathfrak{q}_r^{e_r},$$

where, for $i \in \{1, \dots, r\}$, $\mathfrak{q}_i = \mathfrak{p}\mathcal{O}_L + (g_i(\alpha))$ and $e_1, e_2, \dots, e_r$ correspond with the powers of each $\overline{g_i}(x)$ mentioned above.

References

[1] Marcus, D. A. *Number Fields*. (2nd edition). Universitext, Springer. (2018).