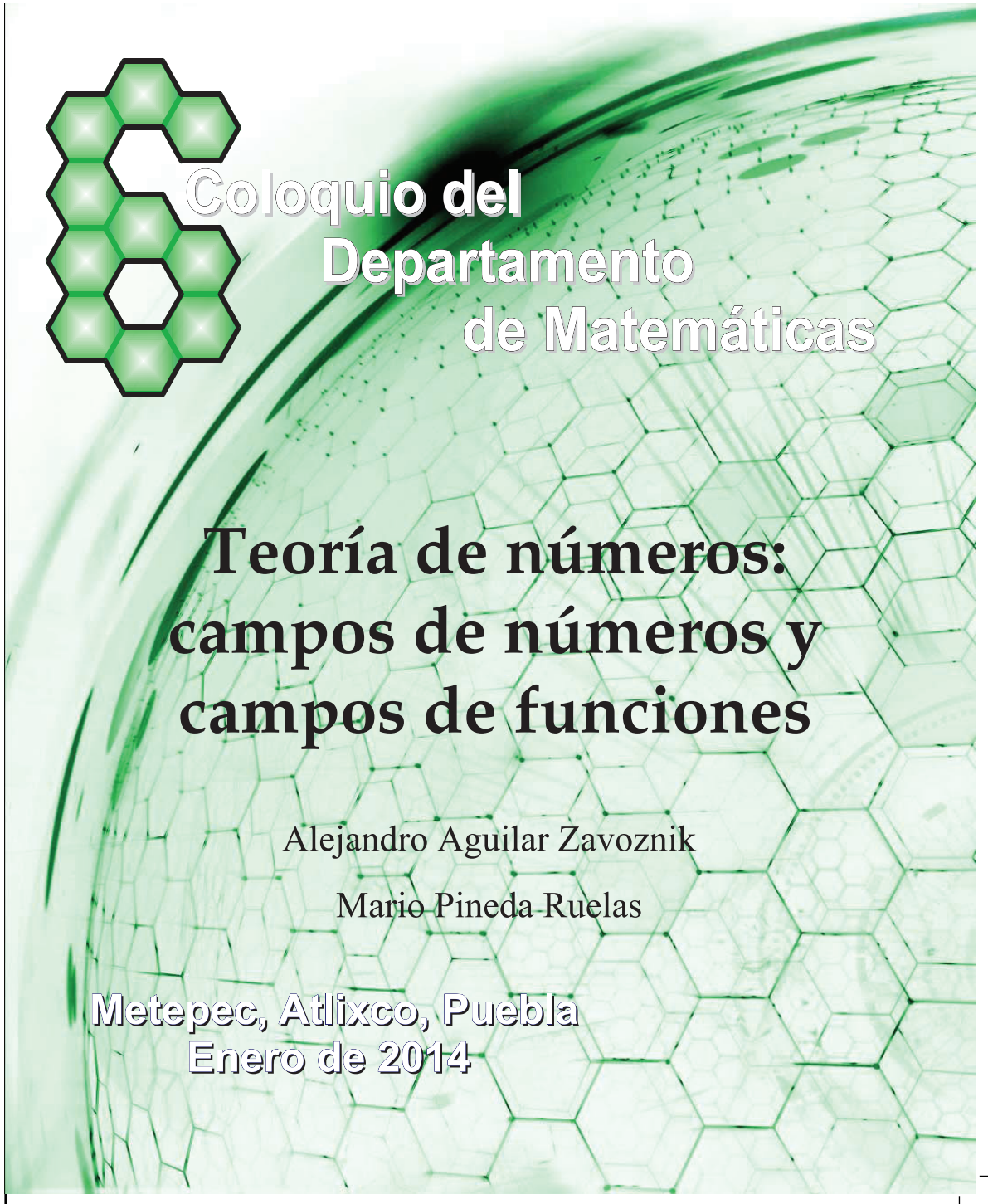
Teoría de números: campos de números y campos de funciones

Alejandro Aguilar Zavoznik
Mario Pineda Ruelas

Una propiedad importante tanto en el anillo de los enteros $\mathbb{Z}$ como en el anillo de polinomios sobre un campo es la factorización única. En Teoría de Números es común considerar anillos que contienen a alguno de los anteriores, en ocaciones estos nuevos anillos son dominios de factorización única, pero es frecuente encontrar casos en los que esta propiedad no se tiene. Una herramienta importante para librar el problema de no ser DFU son los ideales, ya que, ellos sí se factorizan de forma única como producto de ideales primos. En este taller estudiaremos las dos familias de ejemplos más importantes donde se utiliza esta herramienta: los anillos de enteros de campos de números y de campos de funciones, concentrándonos en los campos cuadráticos. Mostraremos algunos ejemplos en los que veremos cómo se utiliza la factorización de ideales para resolver problemas aritméticos.

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA
Unidad Iztapalapa



6to Coloquio del Departamento de Matemáticas

Introducción a los Campos de Números y Campos de Funciones

Alejandro Aguilar Zavoznik
Mario Pineda Ruelas

Publicación del Departamento de Matemáticas de la Universidad Autonóma Metropolitana-Iztapalapa con el apoyo de la División de Ciencias Básicas e Ingeniería y Consejo Nacional de Ciencia y Tecnología (CONACYT).

Introducción a los Campos de Números y Campos de Funciones

Alejandro Aguilar Zavoznik
Mario Pineda Ruelas

Departamento de Matemáticas, UAM-I

Casa abierta al tiempo
Universidad Autónoma Metropolitana

Contenido

Introducción

Un curso introductorio a la teoría de números algebraicos es un reto si presuponemos una audiencia que no conocemos; sólo por el posible interés en el tema. De cualquier forma, aceptamos el reto y con nuestra propuesta haremos lo que esté a nuestro alcance para inducir a nuestro joven público para que se interese en esta maravillosa disciplina de las matemáticas: la teoría de números.

Estas notas están divididas en tres capítulos. El primero contiene parte de los antecedentes que consideramos necesarios para poder iniciar el estudio del tema. El Segundo capítulo es la puerta de entrada a la teoría de números algebraicos y presentamos los resultados fundamentales, la mayoría con su respectiva demostración, acompañados de ejemplos ilustrativos que hacen más comprensible la teoría. El capítulo 3 sigue la misma lógica del capítulo anterior y es aquí donde através de ejemplos ilustramos esa otra parte de la teoría de números; los campos de funciones. Todo lo anterior está gobernado por una idea: la factorización.

Esperamos que nuestra audiencia disfrute los temas de estudio que proponemos.

La revisión que el comité editorial hizo a nuestras notas mejoró su contenido y presentación, gracias; de los posibles errores que quedaron nosotros somos los responsables.

Alejandro Aguilar Zavoznik
Mario Pineda Ruelas
Universidad Autónoma Metropolitana
México 2013.

Capítulo 1

El anillo de los enteros

1.1. $\mathbb{Z}$

Una de las estructuras aritméticas más importantes en toda la matemática es el anillo de los enteros $\mathbb{Z}$. Podemos partir de la propiedad más bella (tal vez por su simplicidad) que gozan los enteros:

TEOREMA 1.1. [Algoritmo de la división] *Sean $a, b, \in \mathbb{Z}$ con $a \neq 0$. Existen enteros q y r únicos tal que $b = aq + r$ donde $0 \leq r < |a|$.*

DEMOSTRACIÓN. Prueba rápida: el conjunto

$$S = \{b - am \geq 0 \quad \text{para ciertos valores } m \in \mathbb{Z}\}$$

es no vacío. Por el principio del buen orden (PBO), S contiene un elemento r que satisface $r \leq n$ para todo $n \in S$. Por tanto, $0 \leq r = b - aq$ para algún $q \in \mathbb{Z}$. Puesto que $a \neq 0$, tenemos $a \geq 1$ ó $a \leq -1$. Si $a \geq 1$ entonces

$$b - a(q+1) = b - aq - a < b - aq = r,$$

así que

$$r - a = b - a(q+1) < 0,$$

y $r < a$. El caso $a \leq -1$ se sigue al considerar que $b - a(q-1) < 0$. Por lo tanto, $r < |a|$. La unicidad de q y r se deja como ejercicio para el lector. □

Notemos que si en el enunciado del algoritmo de la división no pedimos que el residuo r sea positivo, entonces r y q no necesariamente son únicos:

$$2 = 11 \cdot 0 + 2 = 11 \cdot 1 + (-9).$$

Problema: Redactar y demostrar una versión general del algoritmo de la división en $\mathbb{Z}$.

COROLARIO 1.2. *$\mathbb{Z}$ es un anillo de ideales principales (DIP).*

DEMOSTRACIÓN. Sea I un ideal en $\mathbb{Z}$ y supongamos que $I \neq \{0\}$. Denotamos por n al menor entero positivo contenido en I. Es claro que $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\} \subseteq I$. Si $i \in I$, entonces por el algoritmo de la división

$$i = nq + r, \qquad 0 \leq r \leq n.$$

Observamos que $i - nq = r \in I$. Si $r \neq 0$, entonces n no es el menor entero positivo en I. Así que $r = 0$ y $I \subseteq n\mathbb{Z}$. □

Sean $a, b \in \mathbb{Z}$ con $a \neq 0$. Denotamos por $\text{mcd}(a, b)$ al mayor divisor en común de a, b. Observamos que $\text{mcd}(a, b) \geq 1$. Algunas de las propiedades más importantes del mcd son:

i) $\text{mcd}(a, b)$ es la mínima $\mathbb{Z}$-combinación lineal positiva de a y b.
ii) Si $\text{mcd}(a, b) = g$, entonces $\text{mcd}\left(\frac{a}{g}, \frac{b}{g}\right) = 1$. Lo anterior significa que g contiene en su factorización a todos los divisores que comparten a y b.
iii) Si $a \mid bc$ y $\text{mcd}(a, b) = 1$, entonces $a \mid c$.
iv) Si $a \in \mathbb{Z}$ y p es un primo (ver definición 1.3, entonces $\text{mcd}(a, p) = 1$ ó $|p|$.

Cualquier entero $a \neq 0, \pm 1$ tiene al menos cuatro divisores: $\pm 1, \pm a$. Si un entero a tiene al menos un divisor $b \neq \pm a, \pm 1$, entonces $a = bd$ y $d \neq \pm a \pm 1$.

DEFINICIÓN 1.3. Sea $p \in \mathbb{Z}$ con $|p| > 1$. Diremos que p es un número primo si $p = bd$, entonces $b = \pm 1$ ó $d = \pm 1$.

Los primeros números primos positivos son: $2, 3, 5, 7, 11, ...$, pero también los inversos aditivos de éstos $-2, -3, -5, -11, \ldots$ son números primos. Así que es claro que p es primo si y sólo si $-p$ es primo. Observemos que si $a \in \mathbb{Z}$ y p es cualquier primo, entonces $\text{mcd}(a, p) = 1$ ó $|p|$. También es fácil notar que si p, q son primos y $p \mid q$, entonces $|p| = |q|$.

TEOREMA 1.4. [Euclides] *p es primo si y sólo si siempre que $p \mid ab$, entonces $p \mid a$ ó $p \mid b$.*

DEMOSTRACIÓN. Supongamos que p es primo y $p \mid ab$. Si $p \nmid a$, entonces $\text{mcd}(a, p) = 1$ y por tanto $p \mid b$. Inversamente, sea $p = ab$ una factorización de p. En particular $p \mid ab$ y por lo tanto $p \mid a$ ó $p \mid b$. Si $p \mid a$ se tiene que $a = pt$, para algún $t \in \mathbb{N}$. Así que $p = ab = ptb$. De lo anterior se sigue que $b = 1$ y $a = p$ y por lo tanto p es primo. □

El teorema anterior nos autoriza a cambiar la definición de número primo.

DEFINICIÓN 1.5. Diremos que $p \in \mathbb{Z}$ es primo si $|p| > 1$ y siempre que $p \mid ab$, entonces $p \mid a$ ó $p \mid b$. Diremos que un entero π con $|\pi| > 1$ es irreducible si $\pi = ab$, entonces $|a| = 1$ ó $|b| = 1$.

En el Teorema 1.4 la definición de primo es equivalente a la definición de irreducible. Sin embargo, existen anillos que contienen a $\mathbb{Z}$ en donde éstos dos conceptos no son equivalentes. Veremos un ejemplo inmediatamente después de la definición 1.27.

TEOREMA 1.6. *Cualquier entero $m > 1$ admite al menos un divisor primo.*

DEMOSTRACIÓN. Fácil ejercicio para el lector. Se sugiere usar inducción sobre m. □

Seguramente la propiedad más importante de $\mathbb{Z}$ se refiere a la factorización única de sus elementos.

COROLARIO 1.7. [Teorema Fundamental de la Aritmética] *Todo entero $\neq 0, \pm 1$ se puede expresar en forma única (salvo el orden) como un producto finito de números primos.*

DEMOSTRACIÓN. Es consecuencia directa del Teorema 1.6 y del Teorema1.4, es ese orden. □

COROLARIO 1.8. *Si $n > 2$, entonces existe un primo p tal que $n < p < n!$.*

DEMOSTRACIÓN. El número $z = n! - 1 > 1$ tiene un divisor primo $p \leq z$. Si $p \leq n$, entonces $p \mid n!$ y por lo tanto $p \mid 1$ lo cual es absurdo. Así que $n < p \leq n! - 1 < n!$. □

COROLARIO 1.9. [Teorema de Euclides] *Existen suficientes primos para factorizar cualquier entero $\neq 0, \pm 1$, es decir, existe una infinidad de números primos.*

DEMOSTRACIÓN. Consideremos n suficientemente grande en el corolario anterior. □

Nota: Si $ab = c^n$ y $\text{mcd}(a, b) = 1$, entonces para ciertos enteros c_1, c_2 se tiene que $a = c_1^n$ y $b = c_2^n$. Esto es consecuencia de la factorización única. Veamos una aplicación de esta inofensiva propiedad.

TEOREMA 1.10. *La ecuación $x^2 - y^3 = 1$ tiene una única solución en los enteros positivos: $x = 3$, $y = 2$.*

DEMOSTRACIÓN. Si x es par, entonces $mcd(x-1, x+1) = 1$ y además:

$$(x-1)(x+1) = y^3.$$

Por tanto

$$x - 1 = a^3 \quad \text{y} \quad x + 1 = b^3.$$

De lo anterior se sigue que $b^3 - a^3 = (b-a)(b^2 + ab + a^2) = 2$ y así $b^2 + ab + a^2 \mid 2$, lo cual es imposible. Por lo tanto, si existiera solución, necesariamente $x = 2t + 1$ y $y = 2q$ con $t, q \geq 1$. Es claro que $t = 1$ implica $x = 3$ y $y = 2$. Si $t > 1$, tendríamos $t(t+1) = 2q^3$, lo cual es imposible porque ningún número triangular es un cubo. □

En una carta fechada en 1844 y dirigida a la revista Journal Crelle, el matemático belga E. Charles Catalan conjeturó que si

$$x^n - y^m = 1,$$

entonces $n = 2$, $m = 3$, $x = 3$, $y = 2$. Esta conjetura un poco olvidada, tal vez por el atractivo que tenía la conjetura de Fermat, ha sido resuelta por el matemático rumano Preda Mihailescu (2002). El Teorema 1.10 es una versión elemental de la conjetura de Catalan.

Regresando a nuestra discusión, el Corolario 1.2 nos asegura que el anillo $\mathbb{Z}$ es de ideales principales. Podemos desarrollar teoría general al respecto, adoptando la definición de primo e irreducible que dimos en $\mathbb{Z}$.

1.1.1. Un poco de teoría general. El objetivo de esta breve sección es ubicar parte de nuestro trabajo en un contexto general, que algunas veces es difícil aterrizarlo en anillos específicos. Esto se debe a dificultades ariméticas que no se pueden hacer explícitas. Por ejemplo, si A es un anillo ¿quiénes son las unidades de A?

En cualquier anillo conmutativo con unidad A, los elementos que tienen inverso multiplicativo forman un grupo multiplicativo el cual denotamos por $U(A)$ y llamaremos *grupo de unidades de* A. El lector puede verificar fácilmente que: $a = bu$ para algún $u \in U(A)$ si y sólo si $a \mid b$ y $b \mid a$. Cuando esto sucede diremos que a y b son asociados y escribiremos $a \sim b$. Observemos que $\langle a \rangle = \langle b \rangle$ si y sólo si $a \sim b$. El conjunto de asociados al elemento a queda descrito por $\{au : u \in U(A)\}$. Tenemos las siguientes definiciones en cualquier dominio entero con 1. Sea $\pi \in A$, con $\pi \neq o$ y $\pi \notin U(A)$. Diremos que π es *primo* si $\pi \mid \alpha\beta$, entonces $\pi \mid \alpha$ ó $\pi \mid \beta$. Diremos que π es *irreducible* si $\pi = \alpha\beta$, entonces α ó β es unidad. Es claro que en el anillo $\mathbb{Z}$ el concepto de primo e irreducible coinciden, en general no es así: ¿en qué anillos significan lo mismo primo e irreducible? más aún,

si los conceptos no coinciden ¿quiénes son los elementos irreducibles? Estas preguntas serán la guía de nuestras exposiciones.

TEOREMA 1.11. *Si π es primo, entonces π es irreducible.*

DEMOSTRACIÓN. Vea la demostración del Teorema 1.4. □

TEOREMA 1.12. *En cualquier anillo conmutativo unitario, los ideales primos principales están generados por elementos primos.*

DEMOSTRACIÓN. Sea $P = \langle \pi \rangle$ un ideal primo principal y supongamos que $\pi \mid ab$. Entonces $ab \in P$ y, por lo tanto, $a \in P$ ó $b \in P$. Así que $a = \pi q$ ó $b = \pi t$. Esto significa que $\pi \mid a$ ó $\pi \mid b$. Por lo tanto, π es primo. □

TEOREMA 1.13. *En cualquier dominio entero unitario A, los ideales máximos principales están generados por elementos irreducibles.*

DEMOSTRACIÓN. Sea $M = \langle \pi \rangle$ y $\pi = ab$. Debemos mostrar que $a \in U(A)$ ó $b \in U(A)$. Claramente $\langle \pi \rangle \subseteq \langle a \rangle \subseteq A$. Como $\langle \pi \rangle$ es máximo se tiene $\langle \pi \rangle = \langle a \rangle$ o bien $\langle a \rangle = A$. Si $\langle \pi \rangle = \langle a \rangle$ se tiene que $a = \pi t$, para algún $t \in A$ y de la igualdad $\pi = ab = \pi tb$ se sigue que $1 = tb$, de donde $b \in U(A)$. Si $\langle a \rangle = A = \langle 1 \rangle$, entonces claramente $a \in U(A)$. □

TEOREMA 1.14. *Si A es un DIP, entonces cualquier sucesión ascendente de ideales es finita.*

DEMOSTRACIÓN. Sea $I_1 \subset I_2 \subset \cdots \subset I_n \subset I_{n+1} \cdots$ cualquier sucesión ascendente de ideales de A y $I = \bigcup_{j=1}^{\infty} I_j$. Claramente I es un ideal de A. Por otro lado $I = \langle a \rangle$ para algún $a \in A$. Puesto que para algún m se tiene $a \in I_m$, se sigue que $I \subseteq I_m \subseteq I$. Lo anterior significa que $I \in \{I_j\}_{j=1}^{\infty}$. Ahora sea $n \geq m$. Entonces $I = I_m \subseteq I_n \subseteq I$, así $I_n = I_m$ y la sucesión es finita. □

Cualquier anillo que satisface el teorema anterior (no necesariamente DIP) lo llamaremos anillo noetheriano. En nuestro caso, cualquier DIP es noetheriano.

TEOREMA 1.15. *Sea $\langle a \rangle$ ideal de un anillo A que es un DIP. Entonces existe $\langle m \rangle$ ideal máximo tal que $\langle a \rangle \subseteq \langle m \rangle$.*

DEMOSTRACIÓN. Sea $X_a = \{I \subset A : I \text{ es un ideal de } A \text{ tal que } \langle a \rangle \subseteq I\}$. Definimos en X_a la siguiente relación: $I \sim J$ si y sólo si $I \subseteq J$. Es claro que X_a es un conjunto parcialmente ordenado con $\sim$. Sea $\mathscr{C}$ cualquier cadena en X_a. Vamos a demostrar que $\mathscr{C}$ tiene un elemento máximo. Sea $M = \bigcup_{I \in \mathscr{C}} I$. Es claro que:

i) M es un ideal de A.
ii) $M \neq A$, pues de lo contrario $1 \in I_j$ para algún j. Por lo tanto $M \in X_a$.
iii) $I_j \subseteq M$.

Lo anterior demuestra que cualquier cadena $\mathscr{C}$ tiene una cota superior en X_a. Entonces por el Lema de Zorn tenemos que X_a tiene al menos un elemento (un ideal que contiene a $\langle a \rangle$) máximo M. Falta ver que M es un ideal máximo de A. Supongamos que $M \subset I \subset A$. Si $I \subsetneq A$, entonces $I \in X_a$ y $M \subset I$. Por tanto M no es un elemento máximo de X_a, así tenemos $I = A$. □

Nota: ¿En dónde usamos que A es un DIP?

COROLARIO 1.16. *Sea A un DIP. Entonces los ideales primos $\neq 0$ son máximos.*

DEMOSTRACIÓN. Sea $\langle q \rangle$ un ideal primo con $q \neq 0$ y $\langle \pi \rangle$ algún ideal máximo tal que $\langle q \rangle \subseteq \langle \pi \rangle$. Vamos a mostrar que $\langle q \rangle = \langle \pi \rangle$. Sabemos que q es primo y π es irreducible. Puesto que $q \in \langle q \rangle \subseteq \langle \pi \rangle$, tenemos $q = \pi t$ para algún $t \in A$. En particular $q \mid \pi t$ y $q \mid \pi$ ó $q \mid t$. Si $q \mid t$, entonces $t = qr$ y de la igualdad $q = \pi t = \pi q r$ tenemos que $\pi \in U(A)$, lo cual no es posible. Así $q \mid \pi$ y $\pi = qu$ para algún $u \in U(A)$. Por lo tanto $\langle \pi \rangle = \langle q \rangle$. □

COROLARIO 1.17. *En un DIP primo e irreducible son lo mismo.*

DEMOSTRACIÓN. Fácil ejercicio para el lector. □

Nota: ¿Qué podemos decir si un elemento irreducible es asociado a un elemento primo?

Antes de continuar precisemos el concepto de factorización única: Diremos que el anillo A tiene la propiedad de la factorización única si cualquier elemento $a \in A \setminus U(A)$, con $a \neq 0$ se puede expresar en forma *única* como producto finito de irreducibles. Aquí la unicidad significa lo siguiente: Si

$$a = \pi_1 \pi_2 \cdots \pi_r = q_1 q_2 \cdots q_k,$$

con π_j, q_s irreducibles, entonces $r = k$ y cada π_j es asociado de algún q_l. Por ejemplo, en $\mathbb{Z}$ tenemos que $2 \cdot 3 = (-2) \cdot (-3)$ son la misma factorización, ya que 2 y -2 son asociados y 3 y -3 también lo son.

En seguida tenemos la versión de la factorización única en cualquier DIP.

TEOREMA 1.18. [Teorema Fundamental de la Aritmética en un DIP] *Sea A un DIP. Cualquier elemento $a \in A \setminus \{0\}$ es una unidad o se puede escribir como producto finito de irreducibles y unidades.*

DEMOSTRACIÓN. Sea $a \in A \setminus \{0\}$ y supongamos que $a \notin U(A)$. Así que $\langle a \rangle \subset A$. Si a es irreducible la afirmación se cumple pues $a = a \cdot 1$. Así que podemos suponer que a no es irreducible. Sea $M = \langle \pi_1 \rangle$ algún ideal máximo de A tal que $\langle a \rangle \subseteq \langle \pi_1 \rangle$. Puesto que $a \in \langle a \rangle \subseteq \langle \pi_1 \rangle$ se tiene que $a = \pi_1 t_1$, para algún $t_1 \in A$. Claramente $t_1 \notin U(A)$ pues de lo contrario $a \sim \pi$ y a sería irreducible. Sea $\langle \pi_2 \rangle$ algún ideal máximo de A tal que $\langle t_1 \rangle \subseteq \langle \pi_2 \rangle$. Entonces $t_1 = \pi_2 t_2$ para algún $t_2 \in A$. De la anterior igualdad se sigue que $\langle t_1 \rangle \subseteq \langle t_2 \rangle$. Así $a = \pi_1 \pi_2 t_2$. Continuando con este proceso obtenemos una cadena de ideales

$$\langle t_1 \rangle \subseteq \langle t_2 \rangle \subseteq \langle t_3 \rangle \subseteq \dots.$$

la cual debe terminar porque A es noetheriano. Así que el proceso es finito y se sigue el resultado. □

COROLARIO 1.19. *Sea A un DIP. La factorización que asegura el teorema anterior es única salvo orden y unidades.*

DEMOSTRACIÓN. Ejercicio para el lector □

Para verificar que cierto anillo tiene la propiedad de ser de factorización única existen varios caminos. Por ejemplo se puede intentar mostrar que es euclidiano, o que es un DIP, etc. El siguiente resultado nos proporciona una alternativa.

TEOREMA 1.20. *Sea A un anillo en donde es posible la factorización finita en irreducibles. Entonces en A la factorización es única si y sólo si primo e irreducible coinciden.*

DEMOSTRACIÓN. Supongamos que la factorización es única. Sea $\pi \in A$ un elemento irreducible y $\alpha, \beta \in A$ tal que $\pi \mid \alpha\beta$ con $\alpha \neq 0 \neq \beta$. Entonces $\alpha\beta = \pi\gamma$ para algún $\gamma \in A$. Factorizamos α, β y γ para obtener

$$\pi(p_1 \cdots p_r) = u(q_1 \cdots q_s)(r_1 \cdots r_t),$$

donde $\alpha = uq_1 \cdots q_s$, $\beta = r_1 \cdots r_t$, $\gamma = p_1 \cdots p_r$, los p_i, q_j, r_k son irreducibles y u es alguna unidad. Puesto que la factorización es única, entonces π es asociado de algún q_i ó r_j. Cualquiera que sea el caso, $\pi \mid \alpha$ ó $\pi \mid \beta$ y por tanto π es primo. Supongamos que cualquier irreducible es primo y sea

$$\alpha = u_1 \pi_1 \cdots \pi_k = u_2 q_1 \cdots q_s,$$

con π_i, q_j irreducibles en A y u_1, u_2 son unidades. Si $k = 0$, entonces $s = 0$ y α es unidad. Si $k = 1$, entonces tenemos $u_1 \pi_1 = u_2 q_1 \cdots q_s$. Supongamos que $s > 1$. Entonces $\pi_1 \mid u_2$ o $\pi_1 \mid q_j$ para algún j.

La primera afirmación no es posible, así que $q_j = u_1'\pi_1$, para algún $u_1' \in U(A)$. No perdemos generalidad si suponemos que $j = 1$ y así tenemos

$$u_1\pi_1 = u_2u_1'\pi_1q_2\cdots q_s.$$

Por lo tanto $u_1 = u_2u_1'q_2\cdots q_s$ y $q_2, ..., q_s \in U(A)$ lo cual es absurdo pues los q_j son irreducibles. Así que $s = 1$ y π_1 es asociado de q_1. Supongamos que si

$$\alpha = u_1\pi_1\cdots\pi_k = u_2q_1\cdots q_s,$$

entonces $k = s$ y cada π_i es asociado de algún q_j. Consideremos

$$u_1\pi_1\cdots\pi_k\pi_{k+1} = u_2q_1\cdots q_s,$$

con $u_1, u_2 \in U(A)$. Entonces π_{k+1} es asociado de algún q_j el cual podemos suponer que es q_1. Así $q_1 = u_1'\pi_{k+1}$. Por lo tanto

$$u_1\pi_1\cdots\pi_k\pi_{k+1} = u_2u_1'\pi_{k+1}'\cdots q_s.$$

Cancelando π_{k+1} en ambos lados obtenemos

$$u_1\pi_1\cdots\pi_k\pi_k = u_2u_1'q_2'\cdots q_s.$$

Por lo tanto $k = s - 1$ y así $k + 1 = s$. □

1.1.2. El anillo de los enteros gaussianos. Consideremos la extensión de campos $\mathbb{Q}(i)/\mathbb{Q}$. Definimos en anillo de los enteros gaussianos como:

$$\mathbb{Z}[i] = \{\alpha \in \mathbb{Q}(i) : f(\alpha) = 0 \text{ para algún } f(x) \in \mathbb{Z}[x] \text{ mónico}\}.$$

Aunque esta definición no describe explícitamente a los elementos de $\mathbb{Z}[i]$, se puede probar relativamente fácil que

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} = \mathbb{Z} + i\mathbb{Z}.$$

Más adelante veremos con detalle cómo describir estos anillos que provienen de manera natural de extensiones cuadráticas del campo $\mathbb{Q}$.

La función norma $N : \mathbb{Z}[i] \to \mathbb{N}_0$ definida como $N(a + bi) = a^2 + b^2$ tiene las siguientes propiedades:

i) $N(a + bi) \geq 0$ y $N(a + bi) = 0$ si y sólo si $a = b = 0$.
ii) $N((a + bi)(c + di)) = N(a + bi)N(c + di)$.
iii) $a + bi$ tienen inverso multiplicativo en $\mathbb{Z}[i]$ si y sólo si $N(a + bi) = 1$. Concretamente $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.
iv) Si $a + bi \mid c + di$, entonces $N(a + bi) \mid N(c + di)$.

La riqueza del anillo $\mathbb{Z}[i]$ proviene de la posibilidad de dividir, tal como sucede en $\mathbb{Z}$.

TEOREMA 1.21. [Algoritmo de la división en $\mathbb{Z}[i]$] *Si $z_1, z_2 \in \mathbb{Z}[i]$ con $z_2 \neq 0$, entonces existen $k,\ \delta \in \mathbb{Z}[i]$ tales que*

$$z_1 = z_2 k + \delta \quad y \quad 0 \leq N(\delta) < N(z_2).$$

DEMOSTRACIÓN. Prueba rápida: Escribimos $\dfrac{z_1}{z_2} = A + Bi$ con $A, B \in \mathbb{Q}$ y elegimos los enteros x, y con la siguiente propiedad:

$$|A - x| \leq \frac{1}{2} \qquad \text{y} \qquad |B - y| \leq \frac{1}{2}.$$

Los enteros gaussianos $k = x + yi$ y $\delta = z_1 - z_2(x + yi)$ satisfacen la afirmación del teorema. □

Puesto que $\mathbb{Z}[i]$ es un anillo euclidiano, entonces $\mathbb{Z}[i]$ es un dominio de ideales principales y por tanto es un dominio de factorización única. En cualquier dominio de factorización única A se cumple la siguiente afirmación: Sean $a, b \in A$ tal que $\text{mcd}(a, b) = u$, para algún $u \in U(A)$ con $ab = z^n$. Entonces $a = x^n$ y $b = y^n$. La definición de primo o irreducible es la de siempre.

TEOREMA 1.22. *Si $N(a + bi) = p$, donde p es un primo racional, entonces $a + bi$ es un primo en $\mathbb{Z}[i]$.*

DEMOSTRACIÓN. Supongamos que $a + bi = (c + di)(e + fi)$. Entonces

$$N(a + bi) = N(c + di)N(e + fi) = p.$$

Por lo anterior $N(c+di) = 1$ ó $N(e+fi) = 1$ y en consecuencia $c+di \in U(A)$ ó $e + fi \in U(A)$. Por lo tanto $a + bi$ es un primo en $\mathbb{Z}[i]$. □

Como ejemplo al teorema anterior, $1 + i$ es un primo en $\mathbb{Z}[i]$ porque $N(1 + i) = 2$ y por la misma razón $u(1 + i)$ es un primo para toda $u \in U(\mathbb{Z}[i])$.

TEOREMA 1.23 (Teorema de Fermat). *Si p es un número primo en $\mathbb{Z}$ y $p \equiv 1 \pmod 4$, entonces existen $a, b \in \mathbb{Z}$ tal que $p = a^2 + b^2$.*

DEMOSTRACIÓN. El lector interesado en una demostración, le sugerimos ver el Teorema 4.3.2 en [**25**]. □

Observe que si $a, b \in \mathbb{Z}$, entonces $a^2 + b^2 = (a + bi)(a - bi)$. Por lo anterior, un primo de $\mathbb{Z}$ de la forma $4n + 1$ lo podemos escribir como suma de dos cuadrados y por tanto es factorizable en el anillo $\mathbb{Z}[i]$. Este hecho abonará a la clasificación de los irreducibles (o primos) en el anillo $\mathbb{Z}[i]$.

TEOREMA 1.24. *Los primos en $\mathbb{Z}[i]$ son :*

i) $1 + i$ *y sus asociados.*

ii) *Los factores* $a + bi$ *de primos racionales de la forma* $4n + 1$ *y sus asociados.*
iii) *Los primos racionales de la forma* $4n + 3$ *y sus asociados.*

DEMOSTRACIÓN. Para la afirmación i) tenemos que $\mathbf{N}(1 + i) = 2$, entonces $1 + i$ y sus asociados son primos. Ahora consideremos un primo racional p de la forma $4n + 1$. Sabemos que

$$p = a^2 + b^2 = (a + bi)(a - bi),$$

así $p = \mathbf{N}(a + bi) = \mathbf{N}(a - bi)$ y por lo tanto $a + bi$ y $a - bi$ son primos. Para la afirmación iii) consideremos un primo racional $p = 4n + 3$ y supongamos que

$$p = (a + bi)(c + di)$$

con $\mathbf{N}(a + bi) > 1$ y $\mathbf{N}(c + di) > 1$. Entonces

$$\mathbf{N}(p) = p^2 = (a^2 + b^2)(c^2 + d^2)$$

implica que $p = a^2 + b^2$ ó $p = c^2 + d^2$ lo cual es imposible para un primo racional de esta forma. Por lo tanto p es primo. Ahora mostraremos que éstos son todos los primos en el anillo $\mathbb{Z}[i]$. Sea π cualquier primo. Entonces

$$\mathbf{N}(\pi) = \pi\bar{\pi} = 2^{\lambda} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} q_1^{\beta_1} q_2^{\beta_2} \cdots q_r^{\beta_r}$$

donde los p_i y q_j son primos racionales de la forma $4n + 1$ y $4n + 3$ respectivamente. Por lo tanto

$$\pi\bar{\pi} = (1 + i)^{\lambda}(1 - i)^{\lambda} \pi_1^{\alpha_1} \bar{\pi}_1{}^{\alpha_1} \pi_2^{\alpha_2} \bar{\pi}_2{}^{\alpha_2} \cdots \pi_s^{\alpha_s} \bar{\pi}_s{}^{\alpha_s} q_1^{\beta_1} \cdots q_r^{\beta_r}.$$

En virtud de la unicidad de la factorización tenemos que π es asociado de algún primo de la lista

$$1 + i,\ 1 - i,\ \pi_1,\ \bar{\pi}_1, \ldots, \pi_s,\ \bar{\pi}_s,\ q_1, \ldots, q_r.$$

Por lo tanto, cualquier primo de $\mathbb{Z}[i]$ es alguno de los considerados en este teorema. □

Problema: Completa los detalles de la demostración del Algoritmo de la división en $\mathbb{Z}[i]$.

Veamos un ejemplo de cómo usar a los enteros gaussianos para resolver una ecuación diofantina.

TEOREMA 1.25. *La ecuación* $x^2 - y^3 = -1$ *tiene como única solución entera* $y = 1$ *y* $x = 0$.

DEMOSTRACIÓN. Tenemos la factorización:

$$y^3 = (x + i)(x - i)$$

Así que esto sugiere usar el anillo de los enteros gaussianos $\mathbb{Z}[i]$. El lector interesado puede seguir los siguientes pasos para concluir la demostración:

i) Se demuestra que $\text{mcd}(x+i, x-i) = 1$.
ii) Se concluye que $x+i = (a+bi)^3$ y $x-i = (a-bi)^3$!salvo unidades.

y el resto debe ser rutina. □

Problema: Considerar el anillo $\mathbb{Z}[2i] = \{a+2bi : a, b \in \mathbb{Z}\}$. Encuentra $U(\mathbb{Z}[2i])$. Demuestra que 2 y $2i$ son irreducibles. ¿Son primos en $\mathbb{Z}[2i]$? ¿Es $\mathbb{Z}[2i]$ un anillo de factorización única aún cuando $\mathbb{Z}[2i] \subset \mathbb{Z}[i]$?

1.1.3. La ecuación de Bachet (1624) $x^2 - y^3 = -19$. En este ejemplo veremos cómo un anillo que no tiene la propiedad de ser de factorización única, está sumergido en un anillo que si es un DFU. Consideremos la ecuación diofantina $x^2 - y^3 = -19$. Primero veremos un *critero* que nos indique si nuestra ecuación es o no soluble en los enteros x, y. La igualdad

$$x^2 + 19 = (x + \sqrt{-19})(x - \sqrt{-19}) = y^3,$$

nos sugiere trabajar en el anillo $\mathbb{Z}[\sqrt{-19}] = \{a + b\sqrt{-19} : a, b \in \mathbb{Z}\}$.

En este caso, la función norma está definida como $N(a+b\sqrt{-19}) = a^2 + 19b^2$. Es fácil mostrar que el elemento $a+b\sqrt{-19}$ tiene inverso multiplicativo en el anillo $\mathbb{Z}[\sqrt{-19}]$ si y sólo si $a^2 + 19b^2 = 1$. Primeras consideraciones:

i) Si $19 \mid y$, entonces $19 \mid y^3$ y por tanto $19 \mid x$. Así $x^2 - y^3 = 19^2 q = -19$ lo cual es imposible en $\mathbb{Z}$. Similarmente $2 \nmid y$. En conclusión $19 \nmid y$ y $2 \nmid y$. Así $1 = ry^3 + s(2 \cdot 19)$ en $\mathbb{Z}$.

ii) $U(\mathbb{Z}[\sqrt{-19}]) = \{1, -1\}$.

iii) Sea $\mu \in \mathbb{Z}[\sqrt{-19}]$ tal que $\mu \mid x + \sqrt{-19}$ y $\mu \mid x - \sqrt{-19}$). Entonces $\mu \mid 2\sqrt{-19}$ y por tanto $\mu \mid 2 \cdot 19$. Pero $\mu \mid y^3$, así que $\mu \mid ry^3 + s2 \cdot 19 = 1$. Así $\mu = \pm 1$ y por lo tanto $\text{mcd}(x+\sqrt{-19}, x-\sqrt{-19}) = 1$. Notemos que cualquier unidad en $\mathbb{Z}[\sqrt{-19}]$ es un cubo.

iv) $x+\sqrt{-19} = (a+b\sqrt{-19})^3 = (a^3 - 3\cdot 19ab^2) + (3a^2b - 19b^3)\sqrt{-19}$.

v) El sistema:

$$x = a^3 - 3 \cdot 19ab^2$$
$$1 = 3a^2b - 19b^3,$$

no es soluble en $\mathbb{Z}$.

vi) De lo anterior concluimos que la ecuación $x^2 - y^3 = -19$ no es soluble en $\mathbb{Z}$.

A primera vista todas las operaciones que efectuamos son correctas. Pero

$$18^2 - 7^3 = -19$$

¿qué hicimos mal? Observemos la siguiente factorización

$$35 = 5 \cdot 7 = (4 + \sqrt{-19})(4 - \sqrt{-19})$$

¿Por qué son diferentes? ¿o son la misma? Por comodidad recordemos nuestras definiciones:

DEFINICIÓN 1.26. π es primo si $\pi \mid \alpha\beta$, entonces $\pi \mid \alpha$ ó $\pi \mid \beta$.

DEFINICIÓN 1.27. π es irreducible si $\pi = \alpha\beta$, entonces α ó β es unidad.

Como ya habiamos observado en el Teorema 1.11, cualquier elemento primo es irreducible, pero no necesariamente un elemento irreducible es primo. En nuestro caso $5, 7, 4 + \sqrt{-19}, 4 - \sqrt{-19}$ son irreducibles en $\mathbb{Z}[\sqrt{-19}]$ no asociados dos a dos. ! Y no son primos. Por ejemplo, 5 es irreducible: Si $5 = \alpha\beta$, entonces

$$25 = N(\alpha)N(\beta)$$

y por tanto

$$N(\alpha) = 5 = N(\beta) \quad \text{ó}$$
$$N(\alpha) = 25 \quad \text{y} \quad N(\beta) = 1.$$

El primer caso no es posible y así β es unidad. ¿Por qué 5 no es primo en $\mathbb{Z}[\sqrt{-19}]$? Primero notemos que

$$5 \mid (4 + \sqrt{-19})(4 - \sqrt{-19}).$$

Si $5 \mid 4 + \sqrt{-19}$, entonces $4 + \sqrt{-19} = 5(a + b\sqrt{-19}) = 5a + 5b\sqrt{-19}$. En particular $5 \mid 4$ en $\mathbb{Z}$, lo cual es imposible. Similarmente $5 \nmid 4 - \sqrt{-19}$ y por tanto 5 no es primo.

Más adelante veremos que el anillo $\mathbb{Z}[\sqrt{-19}]$ está contenido en otro anillo que es de factorización única, aún cuando $\mathbb{Z}[\sqrt{-19}]$ no lo es. ¿Cómo explicamos este fenómeno?

TEOREMA 1.28. *Las soluciones enteras de la ecuación de Bachet* $x^2 - y^3 = -19$ *son:* $x = \pm 18$ *y* $y = 7$.

DEMOSTRACIÓN. Asuma que el anillo $\mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{-19}}{2})$ es de factorización única, $U(\mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{-19}}{2})) = \{1, -1\}$. Después siga las mismas ideas desarrollando la igualdad

$$x + \sqrt{-19} = \Big(\frac{a + b\sqrt{-19}}{2}\Big)^3. \qquad \square$$

1.1.4. El problema de las unidades y la factorización. En esencia, las ideas que hemos utilizado son las mismas. Ahora consideremos la ecuación $x^2 - 18 = y^3$. En este caso tenemos

$$x^2 - 18 = (x - \sqrt{18})(x + \sqrt{18}) = (x - 3\sqrt{2})(x + 3\sqrt{2}) = y^3,$$

y por lo tanto, parece conveniente trabajar en el anillo

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : \ a, b \in \mathbb{Z}\}.$$

Se sabe que $\mathbb{Z}[\sqrt{2}]$ es euclidiano y en consecuencia, es un anillo de factorización única en donde elemento primo e irreducible coinciden. Un ejercicio fácil para el lector consiste en mostrar que $\sqrt{2}$ y 3 son elementos primos en $\mathbb{Z}[\sqrt{2}]$. Ahora notemos que si $x = 2t$ y $y = 2q$, entonces $x^2 \equiv 0 \pmod 4$ y

$$x^2 \equiv 4t^2 \equiv 8q^3 + 18 \equiv 2 \equiv 0 \pmod 4,$$

lo cual no es posible. Obviamente, no puede suceder que x, y tengan paridad diferente. Por lo tanto, si x, y es cualquier solución, necesariamente x, y deben ser impares. Supongamos que el lector ya ha verificado que 3 es primo en $\mathbb{Z}[\sqrt{2}]$.

Ahora mostraremos que la ecuación $x^2 - 18 = y^3$ no es soluble. Primero veremos que los factores $x - 3\sqrt{2}$ y $x + 3\sqrt{2}$ son primos relativos en el anillo $\mathbb{Z}[\sqrt{2}]$.

Sea $\alpha = \text{mcd}(x - 3\sqrt{2}, x + 3\sqrt{2})$ y π algún divisor primo de α. Entonces $\pi \mid 6\sqrt{2}$ y puesto que $2 = (\sqrt{2})^2$ tenemos $\pi \mid 3 \cdot (\sqrt{2})^3$. Si $\pi \mid \sqrt{2}$, tenemos que $\pi = u\sqrt{2}$ para alguna unidad $u \in \mathbb{Z}[\sqrt{2}]$. Como $\pi \mid x + 3\sqrt{2}$, entonces $\sqrt{2} \mid x + 3\sqrt{2}$. Por lo tanto $2 \mid x$ y x es par, lo cual no es posible.

Por otro lado, si $\pi \mid 3$, entonces $\pi = 3u$ para alguna unidad $u \in \mathbb{Z}[\sqrt{2}]$. Por lo anterior tenemos que $3 \mid x + 3\sqrt{2}$ y así $3 \mid y$ y $3 \mid x$. Sea $y = 3a$ y $x = 3b$. Entonces de la igualdad $x^2 - 18 = y^3$ obtenemos $b^2 \equiv 3a^3 + 2 \equiv 2 \pmod 3$. Puesto que x es impar, necesariamente b debe ser impar. Si $b = 3k + r$ y k es par, entonces $b = 3k + 1$ y por lo tanto $b^2 \equiv 1 \pmod 3$, lo cual no es posible. Análogamente si k es impar obtenemos un absurdo. Por lo anterior, $\pi \nmid 3$. En

conclusión, α no tiene divisores primos y así α debe ser una unidad. Hemos mostrado que $\text{mcd}(x+3\sqrt{2}, x-3\sqrt{2}) = 1$. Por lo tanto cada factor de $y^3 = (x+3\sqrt{2})(x-3\sqrt{2})$ debe ser un cubo. Supongamos que $x+3\sqrt{2} = (a+b\sqrt{2})^3$. Entonces

$$x+3\sqrt{2} = a^3+3a^2b\sqrt{2}+6ab^2+2b^3\sqrt{2} = (a^3+6ab^2)+(3a^2b+2b^3)\sqrt{2}.$$

De la igualdad anterior surge el sistema

$$a^3+6ab^2 = x$$
$$3a^2b+2b^3 = 3.$$

La segunda ecuación la podemos escribir como

$$b(3a^2+2b^2) = 3,$$

la cual evidentemente no tiene solución en los enteros a, b. Si trabajamos con la igualdad $x-3\sqrt{2} = (a+b\sqrt{2})^3$, llegamos a la misma conclusión. Por lo anterior $x^2-18 = y^3$ no tiene soluciones enteras x, y. Algo hicimos mal: $19^2-18 = 7^3$.

Uno de los errores que cometimos fue suponer incorrectamente que cada factor de

$$y^3 = (x+3\sqrt{2})(x-3\sqrt{2})$$

es un cubo y por otro lado, desconocemos a los elementos invertibles en $\mathbb{Z}[\sqrt{2}]$. Para esto, debemos resolver la ecuación $x^2-dy^2 = \pm 1$ y el método indicado para encontrar unidades en ésta clase de anillos es la teoría de las fracciones continuas. Una buena exposición de este tema es [**13**]. Por lo pronto nos adelantamos afirmando sin demostración que los elementos invertibles en $\mathbb{Z}[\sqrt{2}]$ son:

$$\{(\pm(1+\sqrt{2})^n : n \in \mathbb{Z}\}.$$

Por ejemplo $(1+\sqrt{2})^2 = 3+2\sqrt{2}$ satisface

$$y+3\sqrt{2} = 19+3\sqrt{2} = (3-\sqrt{2})^3(1+\sqrt{2})^2.$$

Regresando a nuestro error, no debimos explorar la igualdad $y+3\sqrt{2} = (a+b\sqrt{2})^3$, aquí lo que debimos estudiar es $y+3\sqrt{2} = (a+b\sqrt{2})^3 u$, donde u es alguna unidad del anillo $\mathbb{Z}[\sqrt{2}]$.

1.1.5. El anillo $\mathbb{Z}[\sqrt{-5}]$ y factorización de ideales. Ahora estudiemos otro ejemplo que nos ilustrará un método para factorizar ideales. Supongamos que $y^3 = x^2+5 = (x+\sqrt{-5})(x-\sqrt{-5})$. Vamos a trabajar en el anillo $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} : a, b \in \mathbb{Z}\}$, en el cual no se cumple la factorización única pues por ejemplo $21 = 3\cdot 7 = (4+\sqrt{-5})(4-\sqrt{-5})$. A nivel de ideales tenemos que

$$\langle y^3\rangle = \langle x+\sqrt{-5}\rangle\langle x-\sqrt{-5}\rangle$$

en donde $\langle x+\sqrt{-5}\rangle$ y $\langle x-\sqrt{-5}\rangle$ son ideales primos relativos. En particular

$$\langle x+\sqrt{-5}\rangle = I^3$$

para algún ideal I. El número de clase de $\mathbb{Z}[\sqrt{-5}]$ (¿?) es 2 y I^3 es principal, entonces I es principal. Digamos que $I=\langle a+b\sqrt{-5}\rangle$. Así

$$I^3 = \langle (a+b\sqrt{-5})^3\rangle = \langle x+\sqrt{-5}\rangle.$$

Por tanto

$$\begin{aligned} x+\sqrt{-5} = (a+b\sqrt{-5})^3 &= a^3+3a^2b\sqrt{-5}+3ab^2(-5)+b^3(-5)\sqrt{-5} \\ &= (a^3-15ab^2)+(3a^2b-5b^3)\sqrt{-5}. \end{aligned}$$

En particular $3a^2b-5b^3 = b(3a^2-5b^2) = 1$ y $b=\pm 1$. Cualquiera que sea el valor de b nos lleva a que $a\notin\mathbb{Z}$. Por lo tanto la ecuación $y^3=x^2+5$ no tiene soluciones enteras. ¡No tener factorización única no es grave!

1.1.6. El anillo $\mathbb{Z}[\sqrt{10}]$. En esta sección estudiaremos con detalle la aritmética del anillo

$$\mathbb{Z}[\sqrt{10}] = \{a+b\sqrt{10} : a,b\in\mathbb{Z}\}.$$

Veremos, entre otras cosas, que no es un anillo de factorización única, encontraremos el grupo de unidades y daremos ejemplos de cómo se comportan distintas factorizaciones de un mismo número. Comenzaremos definiendo la norma de un elemento. Consideremos la función

$$N : \mathbb{Z}[\sqrt{10}] \to \mathbb{Z}$$

definida como $N(a+b\sqrt{10}) = a^2-10b^2$. Observemos que

$$N(a+b\sqrt{10}) = (a+b\sqrt{10})(a-b\sqrt{10}).$$

TEOREMA 1.29. *La función N es multiplicativa.*

DEMOSTRACIÓN.

$$\begin{aligned} N(a+b\sqrt{10})N(c+d\sqrt{10}) &= (a^2-10b^2)(c^2-10b^2) \\ &= a^2c^2-10a^2d^2-10b^2c^2+100b^2d^2 \\ &= (ac+10bd)^2-10(ad+bc)^2 \\ &= N((a+b\sqrt{10})(c+d\sqrt{10})), \end{aligned}$$

□

LEMA 1.30. *$a+b\sqrt{10}\in U(\mathbb{Z}[\sqrt{10}])$ si y sólo si $|N(a+b\sqrt{10})| = 1$.*

DEMOSTRACIÓN. Si α es una unidad, entonces α^{-1} es un elemento del anillo. Como la norma es multiplicativa, entonces:

$$N(\alpha)N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1,$$

y debido a que el codominio de la norma es $\mathbb{Z}$, entonces las únicas posibilidades son

$$N(\alpha) = N(\alpha^{-1}) = 1 \qquad \text{ó} \qquad N(\alpha) = N(\alpha^{-1}) = -1,$$

en cualquier caso, se cumple la afirmación. Recíprocamente, si $N(a + b\sqrt{10}) = 1$, entonces

$$(a + b\sqrt{10})(a - b\sqrt{10}) = 1,$$

y por lo tanto, $a + b\sqrt{10}$ es una unidad, pues $a - b\sqrt{10}$ es su inverso multiplicativo. Si $N(a+b\sqrt{10}) = -1$, entonces $(a+b\sqrt{10})(a-b\sqrt{10}) = -1$ y $-a + b\sqrt{10}$ es el inverso multiplicativo de $a + b\sqrt{10}$. □

Como caso particular del célebre Teorema de las Unidades de Dirichlet sabemos que el anillo $\mathbb{Z}[\sqrt{10}]$ contiene una unidad especial $\epsilon > 1$ que satisface: si $\mu \in U(\mathbb{Z}[\sqrt{10}])$, entonces existe $n \in \mathbb{Z}$ tal que $\mu = \pm\epsilon^n$. Esta unidad se conoce como la *unidad fundamental* del anillo. Vamos a demostrar que $\epsilon = 3 + \sqrt{10}$.

PROPOSICIÓN 1.31. *Si $\mu \in U(\mathbb{Z}[\sqrt{10}])$, entonces $\mu = \pm(3+\sqrt{10})^m$, para algún $m \in \mathbb{Z}$.*

DEMOSTRACIÓN. Primero vamos a mostrar que no existen unidades μ tal que $1 < \mu < 3 + \sqrt{10}$. Supongamos que efectivamente, existe al menos una unidad μ tal que

$$1 < \mu < 3 + \sqrt{10}.$$

Si escribimos $\mu = a + b\sqrt{10}$, entonces podemos suponer sin pérdida de generalidad que $a, b \in \mathbb{N}$ (¿por qué?). Observemos que $1 = |(a + b\sqrt{10})(a - b\sqrt{10})|$. Si escribimos $\bar{\mu} = a - b\sqrt{10}$, entonces es claro que:

i) $\bar{\mu} \in \mathbb{Z}[\sqrt{10}]$.
ii) $|\mu\mu^{-1}| = |\mu\bar{\mu}| = 1$.
iii) $\mu + \bar{\mu} = 2a \in 2\mathbb{Z}$.

Puesto que $1 < \mu < 3 + \sqrt{10}$, invirtiendo se tiene

$$\sqrt{10} - 3 = \frac{1}{3 + \sqrt{10}} < \bar{\mu} < 1,$$

y por lo tanto

$$\sqrt{10} - 2 < \mu + \bar{\mu} < 4 + \sqrt{10},$$

o equivalentemente

$$\frac{\sqrt{10}}{2} - 1 < \frac{\mu + \bar{\mu}}{2} < 2 + \frac{\sqrt{10}}{2}.$$

Con ayuda de una calculadora obervamos que

$$\frac{\sqrt{10}}{2} - 1 > .5811 \qquad \text{y} \qquad \frac{\sqrt{10}}{2} + 2 < 4.$$

Por lo tanto, necesariamente $a = 1, 2$ ó 3. En cada caso producimos las ecuaciones

$$1 - 10b^2 = \pm 1, \quad 4 - 10b^2 = \pm 1, \quad 9 - 10b^2 = \pm 1,$$

las cuales no son solubles en el entero b. Lo anterior significa que la unidad $3 + \sqrt{10}$ es la menor unidad positiva en el anillo $\mathbb{Z}[\sqrt{10}]$.

Ahora fijemos una unidad positiva de $\mathbb{Z}[\sqrt{10}]$, digamos u'. Como

$$\lim_{n \to -\infty} (3 + \sqrt{10})^n = 0 \quad \text{y} \quad \lim_{n \to +\infty} (3 + \sqrt{10})^n = \infty,$$

y para todo $n \in \mathbb{Z}$ se tiene que $(3+\sqrt{10})^n < (3+\sqrt{10})^{n+1}$ entonces existe un único $m \in \mathbb{Z}$ tal que

$$(3 + \sqrt{10})^m \leq u' < (3 + \sqrt{10})^{m+1}.$$

Multiplicando por $(3 + \sqrt{10})^{-m}$ obtenemos

$$1 \leq u'(3 + \sqrt{10})^{-m} < 3 + \sqrt{10},$$

pero no hay ninguna unidad entre 1 y $3+\sqrt{10}$ así que $1 = u'(3+\sqrt{10})^{-m}$, y por lo tanto $u' = (3 + \sqrt{10})^m$.

Ahora, si u' es negativo, multipliquemos por -1, y debe cumplirse que $-u' = (3 + \sqrt{10})^m$ para algún $m \in \mathbb{Z}$; por lo tanto, $u' = -(3 + \sqrt{10})^m$. □

Problema: Encuentre un isomorfismo entre los grupos $U(\mathbb{Z}[\sqrt{10}])$ y $\mathbb{Z}_2 \times \mathbb{Z}$.

Problema: Sea $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Demuestre que la unidad fundamental en éste anillo es $1 + \sqrt{2}$.

PROPOSICIÓN 1.32. *Si $\alpha, \beta \in \mathbb{Z}[\sqrt{10}]$ son asociados, entonces $|N(\alpha)| = |N(\beta)|$.*

DEMOSTRACIÓN. Fácil ejercicio para el lector. □

Problema: Encuentre dos números en $\mathbb{Z}[i]$ con la misma norma y no asociados.

Problema: Encuentre dos números en $\mathbb{Z}[\sqrt{10}]$ con la misma norma y no asociados.

Problema: Demuestre que 2 y $\sqrt{10}$ no son asociados en el anillo $\mathbb{Z}[\sqrt{10}]$.

En conclusión, para que un dominio entero no sea de factorización única basta con encontrar un número irreducible que no sea primo. En $\mathbb{Z}[\sqrt{10}]$ el número 2 es irreducible, sin embargo $2 \cdot 5 = 10 = \sqrt{10}\sqrt{10}$, así que $2 \mid 10$, pero $2 \nmid \sqrt{10}$. Esto último lo podemos demostrar usando el siguiente lema.

LEMA 1.33. *Si $\alpha, \beta \in \mathbb{Z}[\sqrt{10}]$ y $\alpha \mid \beta$, entonces $N(\alpha) \mid N(\beta)$.*

DEMOSTRACIÓN. Fácil ejercicio para el lector. □

Regresemos a nuestra discusión de primo e irreducible. Por ejemplo, en el anillo $\mathbb{Z}[\sqrt{10}]$ tenemos que 7 es un elemento primo, y dos distintas factorizaciones de 70 son:

$$\begin{aligned} 70 &= 2 \cdot 5 \cdot 7 \\ &= \sqrt{10} \cdot \sqrt{10} \cdot 7 \end{aligned}$$

en donde $2, 5, \sqrt{10}$ son irreducibles, pero no son primos, por lo que en algunas factorizaciones sí aparecen y en otras no; sin embargo 7 sí es un elemento primo, y como tal, aparece en las dos factorizaciones de 70. ¿Será posible factorizar (aunque sea teóricamente) cualquier elemento de $\mathbb{Z}[\sqrt{10}]$?

TEOREMA 1.34. *Si $\alpha \in \mathbb{Z}[\sqrt{10}]$, con $\alpha \neq 0$ y no unidad, entonces α se puede escribir como producto finito de irreducibles.*

DEMOSTRACIÓN. Prueba rápida: Consideremos el conjunto

$$A = \{x \in \mathbb{Z}[\sqrt{10}] \setminus \{0\} : x \text{ no es unidad y } x \text{ no es producto de irreducibles}\}$$

y suponga que $B = \{|N(x)| : x \in A\} \neq \emptyset$. La conclusión es casi inmediata. □

Problema: Escriba los detalles de la demostración del Teorema 1.34.

Problema: Con respecto a las dos factorizaciones *diferentes* del número 70 piense usted ¿por qué siempre aparece el 7? Intente formular una conjetura al respecto.

Aparentemente tenemos algo muy bueno (aunque hasta el momento es teórico): la certeza de poder factorizar como producto finito de irreducibles. Ahora surgen otras dudas: ¿sabemos identificar a un elemento irreducible? ¿sabemos distinguir un irreducible de un primo? En general y afortunadamente, la respuesta no es muy alentadora y para muestra basta un botón: El caso del anillo $\mathbb{Z}$, en donde existen muchos misterios por resolver. Por ejemplo, hasta la fecha, absolutamente

nadie tiene un algoritmo eficaz para factorizar enteros y más aún, no se tiene un método o prueba (test) que identifique a los primos de $\mathbb{Z}$.

En $\mathbb{Z}[\sqrt{10}]$ el problema de la no factorización única no se hereda al semigrupo de los ideales $\neq 0$ del anillo.

TEOREMA 1.35. *En $\mathbb{Z}[\sqrt{10}]$ todo ideal distinto de $\langle 0\rangle$ y de $\langle 1\rangle$ se factoriza de forma única como producto de ideales primos.*

DEMOSTRACIÓN. Usualmente se demuestra que el número de clase es finito (!!). Luego la conclusión es fácil. Posponemos la demostración para más adelante porque aún no sabemos qué es el número de clase. □

Diremos que un ideal I divide al ideal J si existe un tercer ideal K tal que $J = IK$ (es la misma definición de divisibilidad en un anillo). Tenemos la siguiente equivalencia importante: I divide a J si y sólo si I contiene a J, esto es:

$$I \mid J \qquad \text{si y sólo si} \qquad I \supseteq J.$$

En $\mathbb{Z}$, todos los ideales son principales y gracias a esto se cumple

$$\langle a\rangle\langle b\rangle = \langle ab\rangle,$$

así que $a \mid b$ si y sólo si $\langle a\rangle \mid \langle b\rangle$ o equivalentemente

$$a \mid b \qquad \text{si y sólo si} \qquad \langle a\rangle \supseteq \langle b\rangle.$$

Por ejemplo $6 \mid 18$ pues $\langle 6\rangle \supseteq \langle 18\rangle$ y $\langle 6\rangle\langle 3\rangle = \langle 18\rangle$. Ahora daremos algunos ejemplos para ver cómo podemos utilizar la factorización única en ideales para factorizar los elementos del anillo. Regresemos al número 70 en el anillo $\mathbb{Z}[\sqrt{10}]$. Sabemos que 70 tiene dos factorizaciones como elemento, pero el ideal principal $\langle 70\rangle$ solamente tiene una factorización en ideales primos:

$$\langle 70\rangle = \langle 2, \sqrt{10}\rangle^2\langle 5, \sqrt{10}\rangle^2\langle 7\rangle.$$

Es importante observar que $\langle 2, \sqrt{10}\rangle$ y $\langle 5, \sqrt{10}\rangle$ se describen usando dos generadores; de hecho, esto es necesario pues estos dos ideales no son principales. Sin embargo

$$\langle 2, \sqrt{10}\rangle^2 = \langle 2\rangle, \quad \langle 5, \sqrt{10}\rangle^2 = \langle 5\rangle, \quad \langle 2, \sqrt{10}\rangle\langle 5, \sqrt{10}\rangle = \langle \sqrt{10}\rangle,$$

así, de aquí se obtienen las dos posibles factorizaciones de 70, la primera

$$\langle 70\rangle = \langle 2, \sqrt{10}\rangle^2\langle 5, \sqrt{10}\rangle^2\langle 7\rangle = \langle 2\rangle\langle 5\rangle\langle 7\rangle$$

y la segunda factorización se obtiene agrupando los ideales no principales de otra forma:

$$\langle 70\rangle = \langle 2, \sqrt{10}\rangle\langle 5, \sqrt{10}\rangle\langle 2, \sqrt{10}\rangle\langle 5, \sqrt{10}\rangle\langle 7\rangle = \langle \sqrt{10}\rangle\langle \sqrt{10}\rangle\langle 7\rangle.$$

El anillo $\mathbb{Z}[\sqrt{10}]$ tiene algunas propiedades que serán muy útiles a la hora de agrupar ideales como en el ejemplo anterior.

PROPOSICIÓN 1.36. *Sea $\pi \in \mathbb{Z}[\sqrt{10}]$*

i) *π es primo si y sólo si el ideal principal $\langle \pi \rangle$ es primo.*
ii) *π es irreducible, pero no primo, si y sólo si $\langle \pi \rangle = P_1 P_2$ donde P_1, P_2 son dos ideales primos tales que ninguno de los dos es principal.*

El inciso i) es válido en cualquier dominio entero, sin embargo, el inciso ii) depende del anillo en el que estamos factorizando. Como consecuencia de lo anterior, para poder clasificar los elementos primos e irreducibles de $\mathbb{Z}[\sqrt{10}]$ basta con encontrar todos los ideales de $\mathbb{Z}[\sqrt{10}]$ y decidir si son o no principales. Por ejemplo

$$I_1 = \langle 2, \sqrt{10} \rangle,\ I_2 = \langle 3, 1+\sqrt{10} \rangle\ , I_3 = \langle 13, 1+2\sqrt{10} \rangle,\ I_4 = \langle 37, 18+5\sqrt{10} \rangle$$

son cuatro ideales primos que no son principales (¿por qué?) y observamos que el producto

$$I_1 I_2 I_3 I_4 = \langle 2 + 17\sqrt{10} \rangle$$

es principal. Así que, para encontrar todas las factorizaciones de $2+17\sqrt{10}$ tendremos que encontrar todas las posibles agrupaciones de parejas de estos ideales. En total son:

$$\begin{aligned}
I_1 I_2 &= \langle 4 + \sqrt{10} \rangle \\
I_1 I_3 &= \langle 8 + 3\sqrt{10} \rangle \\
I_1 I_4 &= \langle 42 - 13\sqrt{10} \rangle \\
I_2 I_3 &= \langle 7 + \sqrt{10} \rangle \\
I_2 I_4 &= \langle 19 - 5\sqrt{10} \rangle \\
I_3 I_4 &= \langle 29 + 6\sqrt{10} \rangle \\
I_1 I_2 I_3 I_4 &= \langle 4 + \sqrt{10} \rangle \langle 29 + 6\sqrt{10} \rangle \\
I_1 I_2 I_3 I_4 &= \langle 8 + 3\sqrt{10} \rangle \langle 19 - 5\sqrt{10} \rangle \\
I_1 I_2 I_3 I_4 &= \langle 42 - 13\sqrt{10} \rangle \langle 7 + \sqrt{10} \rangle
\end{aligned}$$

Ahora observemos los siguientes productos:

$$\begin{aligned}
\langle 4 + \sqrt{10} \rangle \langle 29 + 6\sqrt{10} \rangle &= \langle 176 + 53\sqrt{10} \rangle \\
\langle 8 + 3\sqrt{10} \rangle \langle 19 - 5\sqrt{10} \rangle &= \langle 2 + 17\sqrt{10} \rangle \\
\langle 42 - 13\sqrt{10} \rangle \langle 7 + \sqrt{10} \rangle &= \langle 164 - 49\sqrt{10} \rangle,
\end{aligned}$$

y notemos que

$$(164 - 49\sqrt{10})(3 + \sqrt{10})^2 = (2 + 17\sqrt{10})(3 + \sqrt{10}) = 176 + 53\sqrt{10}.$$

Por lo tanto $164 - 49\sqrt{10} \sim 176 + 53\sqrt{10}$. Así que, para encontrar todas las factorizaciones en irreducibles de $2+17\sqrt{10}$ tomamos las tres factorizaciones de ideales anteriores y multiplicamos por la unidad correspondiente. Esto no es un ajuste artificial pues en cualquier anillo conmutativo si u es una unidad y $\langle\alpha\rangle$ es un ideal principal, entonces $\langle\alpha\rangle = \langle u\alpha\rangle$; así que lo que pasa es que tenemos los ideales que necesitamos, pero no están representados con los generadores adecuados. Si al ideal $\langle 29 + 6\sqrt{10}\rangle$ lo hubiéramos expresado como

$$\langle 29 + 6\sqrt{10}\rangle = \left\langle \frac{1}{3+\sqrt{10}}(29 + 6\sqrt{10}) \right\rangle = \langle -27 + 11\sqrt{10}\rangle,$$

tendríamos

$$\langle 2 + 17\sqrt{10}\rangle = \langle 4 + \sqrt{10}\rangle\langle -27 + 11\sqrt{10}\rangle,$$

donde ahora sí, $2 + 17\sqrt{10} = (4 + \sqrt{10})(-27 + 11\sqrt{10})$. De la misma forma, si en lugar de $\langle 7 + \sqrt{10}\rangle$ tomamos

$$\langle 7 + \sqrt{10}\rangle = \langle (7 + \sqrt{10})(3 + \sqrt{10})\rangle = \langle 31 + 10\sqrt{10}\rangle$$

encontramos que

$$\langle 2 + 17\sqrt{10}\rangle = \langle 42 - 13\sqrt{10}\rangle\langle 31 + 10\sqrt{10}\rangle.$$

Así que, como éstas son las únicas tres posibles agrupaciones de dos en dos de los ideales I_1, I_2, I_3, I_4, entonces las únicas tres factorizaciones de $2 + 17\sqrt{10}$ son:

$$\begin{aligned} 2 + 17\sqrt{10} &= (4 + \sqrt{10})(-27 + 11\sqrt{10}) \\ &= (8 + 3\sqrt{10})(19 - 5\sqrt{10}) \\ &= (42 - 13\sqrt{10})(31 + 10\sqrt{10}). \end{aligned}$$

Cualquier otra factorización que encontremos será equivalente a alguna de estas tres. Por ejemplo, si tomamos la unidad $u = 721 - 228\sqrt{10}$, la primera factorización también la podríamos escribir como:

$$\begin{aligned} 2 + 17\sqrt{10} &= (4 + \sqrt{10})(-27 + 11\sqrt{10}) \\ &= (4 + \sqrt{10})u\frac{1}{u}(-27 + 11\sqrt{10}) \\ &= (4 + \sqrt{10})(721 - 228\sqrt{10})\frac{-27 + 11\sqrt{10}}{721 - 228\sqrt{10}} \\ &= (604 - 191\sqrt{10})(5613 + 1775\sqrt{10}). \end{aligned}$$

De esta forma hemos obtenido otra factorización de $2 + \sqrt{17}$, pero esencialmente $(4+\sqrt{10})(-27+11\sqrt{10})$ y $(604-191\sqrt{10})(5613+1775\sqrt{10})$

son la misma factorización pues $4+\sqrt{10}$ y $604-191\sqrt{10}$ son asociados y $-27+11\sqrt{10}$ y $5613+1775\sqrt{10}$ también lo son.

Finalizamos el estudio del anillo $\mathbb{Z}[\sqrt{10}]$ enunciando algunos resultados (sin demostración) que más adelante nos permitirán saber cuáles son los ideales primos del anillo y distinguir si son o no principales.

PROPOSICIÓN 1.37. *Dado un ideal primo P de $\mathbb{Z}[\sqrt{10}]$, existe $p \in \mathbb{Z}$ primo tal que $P \mid \langle p \rangle$.*

El resultado anterior nos dice que basta con estudiar cómo se factorizan los ideales de la forma $\langle p \rangle$ para todos los primos p de $\mathbb{Z}$ con el objeto de encontrar todos los ideales primos de $\mathbb{Z}[\sqrt{10}]$; que es lo que tenemos gracias a la siguiente proposición.

PROPOSICIÓN 1.38. *El ideal $\langle p \rangle$ se factoriza como producto de ideales primos de acuerdo a las siguientes condiciones:*

i) *Si $p = 2$ ó $p = 5$, $\langle p \rangle = \langle p, \sqrt{10} \rangle^2$.*
ii) *Si $p \equiv 1, 3, 9, 13, 27, 31, 37, 39 \pmod{40}$ la ecuación $a^2 \equiv 10 \pmod{p}$ tiene solución, y dado un valor de a, $\langle p \rangle = \langle p, a + \sqrt{10} \rangle \langle p, a - \sqrt{10} \rangle$.*
iii) *Si $p \equiv 7, 11, 17, 19, 21, 23, 29, 33 \pmod{40}$, entonces $\langle p \rangle$ es un ideal primo.*

Notemos que cualquier otra posibilidad módulo 40 nos da un múltiplo de 2 o un múltiplo de 5, que no pueden ser números primos, por lo que estos dieciocho casos cubren todos los primos de $\mathbb{Z}$ módulo 40. Por ejemplo, 53 es un primo congruente con 13 módulo 40, así que cumple la condición del caso ii). Una solución de $a^2 \equiv 10 \pmod{53}$ es 13. Por lo tanto

$$\langle 53 \rangle = \langle 53, 13 + \sqrt{10} \rangle \langle 53, 13 - \sqrt{10} \rangle.$$

Por otro lado, $97 \equiv 17 \pmod{40}$, así que el ideal $\langle 97 \rangle$ es un ideal primo de $\mathbb{Z}[\sqrt{10}]$. Finalmente, para poder clasificar los primos y los irreducibles de $\mathbb{Z}[\sqrt{10}]$ tenemos que saber cuándo un ideal primo es principal y cuándo no lo es. En el caso del inciso iii) es claro que los ideales primos $\langle p \rangle$ son principales, y en el inciso i) el proceso es finito, por lo que podemos verificar que ninguno de los dos ideales es principal. Así que el principal problema son los ideales del inciso ii).

PROPOSICIÓN 1.39. *Sea P un ideal primo. P es principal si y sólo si se cumple alguna de las siguientes condiciones:*

i) *$P = \langle p \rangle$ con $p \equiv 7, 11, 17, 19, 21, 23, 29, 33 \pmod{40}$.*
ii) *$P = \langle p, a \pm \sqrt{10} \rangle$ con $p \equiv 1, 9, 31, 39 \pmod{40}$.*

P no es principal si y sólo si se cumple alguna de las siguientes condiciones:

iii) $P = \langle 2, \sqrt{10}\rangle$.
iv) $P = \langle 5, \sqrt{10}\rangle$.
v) $P = \langle p, a \pm \sqrt{10}\rangle$ *con* $p \equiv 3, 13, 27, 37 \pmod{40}$

Con esto ya sabemos cuándo un ideal es principal y cuándo no lo es, lo que nos ayuda a encontrar todos los primos y los irreducibles de $\mathbb{Z}[\sqrt{10}]$, pues sabemos que si P es un ideal primo principal, entonces cualquier generador de P es un elemento primo, y si P_1, P_2 son dos ideales primos no principales, el producto de ellos va a ser un ideal principal generado por un irreducible que no es primo. Por ejemplo $\langle 53, 13 + \sqrt{10}\rangle$ y $\langle 53, 13 - \sqrt{10}\rangle$ son ideales primos que no son principales, pues $53 \equiv 13 \pmod{40}$, por lo que $\langle 53\rangle$, que es el producto de éstos, es un ideal principal que es producto de dos ideales primos no principales, lo que nos indica que en $\mathbb{Z}[\sqrt{10}]$ el número 53 es irreducible, pero no es un número primo. De hecho, esto mismo sucede con cualquier primo p de $\mathbb{Z}$ congruente con 3, 13, 27 ó 37 módulo 40.

Concluimos con el siguiente criterio, que es consecuencia de todo lo anterior:

TEOREMA 1.40. *Sean $\pi = a + b\sqrt{10} \in \mathbb{Z}[\sqrt{10}]$ y $N(\pi) = a^2 - 10b^2$. Entonces π es un elemento primo si y sólo si se cumple una de las dos condiciones siguientes:*

i) $|N(\pi)| = p$, *con p un primo de $\mathbb{Z}$,* $p \equiv 1, 9, 31, 39 \pmod{40}$.
ii) $|N(\pi)| = p^2$ *con p un primo de $\mathbb{Z}$,* $p \equiv 7, 11, 17, 19, 21, 23, 29, 33 \pmod{40}$.

y π es un irreducible si y sólo si π cumple alguna de las siguientes condiciones:

i) *π es primo.*
ii) $|N(\pi)| = pq$ *con p y q dos primo de $\mathbb{Z}$ (que pueden ser iguales o distintos),* $p \equiv 2, 3, 5, 13, 27, 37 \pmod{40}$.

Capítulo 2

Números algebraicos

En este capítulo desarrollaremos formalmente la teoría que sustenta el capítulo anterior.

DEFINICIÓN 2.1. Un número complejo z es un entero algebraico si z es raíz de algún polinomio mónico con coeficientes enteros $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$.

Si denotamos por $\Omega = \{z \in \mathbb{C} : z \text{ es un entero algebraico}\}$, entonces Ω es un anillo. Antes de ver una prueba rápida de la afirmación anterior necesitamos recordar algunos conceptos. Un $\mathbb{Z}$-módulo es un conjunto $W \subseteq \mathbb{C}$ tal que:

i) Si $\gamma_1, \gamma_2 \in W$ entonces $\gamma_1 + \gamma_2 \in W$.
ii) Existen $\gamma_1, \gamma_2, \ldots, \gamma_n \in W$ tales que $W = \gamma_1\mathbb{Z} + \gamma_2\mathbb{Z} + \cdots + \gamma_n\mathbb{Z}$.

PROPOSICIÓN 2.2. *Sean W un $\mathbb{Z}$-módulo y $\omega \in \mathbb{C}$ tal que $\omega\gamma \in W$ para todo $\gamma \in W$. Entonces $\omega \in \Omega$.*

DEMOSTRACIÓN. Por hipótesis $\omega\gamma_i \in W$ para $1 \leqslant i \leqslant n$. Entonces,

$$\omega\gamma_i = \sum_{j=1}^{n} a_{ij}\gamma_j \tag{1}$$

con $a_{ij} \in \mathbb{Q}$. Sea

$$\delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases},$$

entonces,

$$\omega\gamma_i = \delta_{ii}\omega\gamma_i = \sum_{j=1}^{n} \delta_{ij}\omega\gamma_j \tag{2}$$

Igualando (1) y (2) obtenemos que

$$\sum_{j=1}^{n} a_{ij}\gamma_j = \sum_{j=1}^{n} \delta_{ij}\omega\gamma_j,$$

y por lo tanto

$$0 = \sum_{j=1}^{n} a_{ij}\gamma_j - \sum_{j=1}^{n} \delta_{ij}\omega\gamma_j = \sum_{j=1}^{n} (a_{ij} - \delta_{ij}\omega)\gamma_j.$$

Si $A = (a_{ij} - \delta Đijw)$, observamos entonces que $\det(A) = 0$ y $\det(a_{ij} - \delta_{ij}x)$ es un polinomio de grado n con coeficientes enteros del cual ω es raíz. Por lo tanto, $\omega \in \Omega$. □

Observe que si $W = \{0\}$, entonces la proposición anterior no se cumple. Por ejemplo, $\frac{2}{3} \cdot 0 \in W$ y $\frac{2}{3} \notin \Omega$.

TEOREMA 2.3. *Ω es un anillo.*

DEMOSTRACIÓN. Sean $\omega_1, \omega_2 \in \Omega$. Existen $r_0, \ldots, r_{n-1} \in \mathbb{Z}$ y $s_0, \ldots, r_{m-1} \in \mathbb{Z}$ tales que

$$\omega_1^n + r_{n-1}\omega_1^{n-1} + r_{n-2}\omega_1^{n-2} + \cdots + r_1\omega_1 + r_0 = 0,$$
$$\omega_2^m + s_{m-1}\omega_2^{m-1} + s_{m-2}\omega_2^{m-2} + \cdots + s_1\omega_2 + s_0 = 0.$$

Sea V el $\mathbb{Z}$-módulo obtenido al formar todas las $\mathbb{Z}$-combinaciones lineales de elementos $\omega_1^i\omega_2^j$ con $0 \leqslant i < n$ y $0 \leqslant j < m$. Para $\gamma \in V$, tenemos que $\omega_1\gamma \in V$ ya que si

$$\gamma = \sum_{i=0}^{n-1}\sum_{j=0}^{m-1} a_{ij}\omega_1^i\omega_2^j,$$

entonces

$$\begin{aligned}
\omega_1\gamma = \omega_1 \sum_{i=0}^{n-1}\sum_{j=0}^{m-1} a_{ij}\omega_1^i\omega_2^j &= \sum_{i=0}^{n-1}\sum_{j=0}^{m-1} a_{ij}\omega_1^{i+1}\omega_2^j \\
&= \sum_{i=0}^{n-2}\sum_{j=0}^{m-1} a_{ij}\omega_1^{i+1}\omega_2^j + \sum_{j=0}^{m-1} a_{(n-1)j}\omega_1^n\omega_2^j \\
&= \sum_{i=0}^{n-2}\sum_{j=0}^{m-1} a_{ij}\omega_1^{i+1}\omega_2^j + \omega_1^n\sum_{j=0}^{m-1} a_{(n-1)j}\omega_2^j \\
&= \sum_{i=0}^{n-2}\sum_{j=0}^{m-1} a_{ij}\omega_1^{i+1}\omega_2^j + (-r_{n-1}\omega_1^{n-1} - \cdots - r_1\omega_1 - r_0)\sum_{j=0}^{m-1} a_{(n-1)j}\omega_2^j.
\end{aligned} \tag{1.1}$$

Esto es una $\mathbb{Z}$-combinación lineal de elementos $\omega_1^i\omega_2^j$ con $1 \leqslant i < n$ y $1 \leqslant j < m$, por lo que $\gamma\omega_1 \in V$. Análogamente $\gamma\omega_2 \in V$.

Por lo anterior $\gamma\omega_1 + \gamma\omega_2 \in V$, lo que implica que $\gamma(\omega_1 + \omega_2)$ se encuentra en V para todo γ en V, por lo tanto, aplicando la proposición anterior, $\omega_1 + \omega_2$ es un entero algebraico.

Multiplicando (1.1) por ω_2 obtenemos

$$\begin{aligned}
(\omega_1\gamma)(\omega_2) = &\Bigg[\sum_{i=0}^{n-2}\sum_{j=0}^{m-1} a_{ij}\omega_1^{i+1}\omega_2^j \\
&\quad + (-r_{n-1}\omega_1^{n-1} - \cdots - r_1\omega_1 - r_0)\sum_{j=0}^{m-1} a_{(n-1)j}\omega_2^j\Bigg]\cdot\omega_2 \\
= &\sum_{i=0}^{n-2}\sum_{j=0}^{m-2} a_{ij}\omega_1^{i+1}\omega_2^{j+1} + \sum_{i=0}^{n-2} a_{i(m-1)}\omega_1^{i+1}\omega_2^m \\
&\quad + (-r_{n-1}\omega_1^{n-1} - \cdots - r_1\omega_1 - r_0)\sum_{j=0}^{m-2} a_{(n-1)j}\omega_2^{j+1} \\
&\quad + (-r_{n-1}\omega_1^{n-1} - \cdots - r_1\omega_1 - r_0)a_{(n-1)j}\omega_2^m \\
= &\sum_{i=0}^{n-2}\sum_{j=0}^{m-2} a_{ij}\omega_1^{i+1}\omega_2^{j+1} + \omega_2^m\sum_{i=1}^{n-2} a_{i(m-1)}\omega_1^{i+1} \\
&\quad + (-r_{n-1}\omega_1^{n-1} - \cdots - r_1\omega_1 - r_0)\sum_{j=1}^{m-2} a_{(n-1)j}\omega_2^{j+1} \\
&\quad + a_{(n-1)(m-1)}(-r_{n-1}\omega_1^{n-1} - \cdots - r_1\omega_1 - r_0) \\
&\qquad (-s_{n-1}\omega_2^{m-1} - \cdots - s_1\omega_1 - s_o)\sum_{i=0}^{n-2}\sum_{j=0}^{m-2} a_{ij}\omega_1^{i+1}\omega_2^{j+1} \\
&\quad + (-s_{m-1}\omega_2^{m-1} - \cdots - s_1\omega_2 - s_0)\sum_{i=1}^{n-2} a_{i(m-1)}\omega_1^{i+1} \\
&\quad + (-r_{n-1}\omega_1^{n-1} - \cdots - r_1\omega_1 - r_0)\sum_{j=1}^{m-2} a_{(n-1)j}\omega_2^{j+1} \\
&\quad + a_{(n-1)(m-1)}(-r_{n-1}\omega_1^{n-1} - \cdots - r_1\omega_1 - r_0) \\
&\qquad (-s_{n-1}\omega_2^{m-1} - \cdots - s_1\omega_1 - s_o).
\end{aligned}$$

Este número es una combinación lineal con coeficientes enteros de elementos de la forma $\omega_1^i\omega_2^j$ con $1 \leqslant i < n$ y $2 \leqslant j < m$. Por lo tanto $\gamma\omega_1\omega_2$ es un elemento de V, y por la proposición anterior $\omega_1\omega_2$ es un entero algebraico.

Ahora, si ω es un elemento de $V \setminus 0$, tenemos

$$\omega^t + e_{t-1}\omega^{t-1} + \cdots + e_1\omega + e_0 = 0$$

con $e_i \in \mathbb{Z}$. El elemento $-\omega$, satisface entonces la ecuación

$$(-1)^t(-\omega)^t + (-1)^{t-1}e_{t-1}(-\omega)^{t-1} + \cdots - e_1(-\omega) + e_0 = 0.$$

Si t es par, entonces es un polinomio mónico con coeficientes en los enteros. Si t es impar, al multiplicar por -1 queda un polinomio mónico con coeficientes en $\mathbb{Z}$. Esto implica que $(-\omega)$ es un entero algebraico.

Debido a todo lo anterior, Ω es un anillo. □

EJEMPLO 2.4. Los números $z = \dfrac{-1 \pm i\sqrt{3}}{2}$ son enteros algebraicos, pues si $f(x) = x^2 + x + 1$, entonces $f(z) = 0$.

EJEMPLO 2.5. Las raíces del polinomio $f(x) = x^4 + 1$ son

$$\frac{-1+i}{\sqrt{2}},\ \frac{1-i}{\sqrt{2}},\ \frac{1+i}{\sqrt{2}},\ \frac{-1-i}{\sqrt{2}}.$$

EJEMPLO 2.6. Si $z \in \mathbb{Z}$, entonces el polinomio $f(x) = x - z$ tiene como raíz a z. No cualquier número racional $\dfrac{a}{b}$ es un entero algebraico.

EJEMPLO 2.7. Demuestra que $\dfrac{a}{b} \in \mathbb{Q}$ es un entero algebraico si y sólo si $b = \pm 1$. Asume desde un principio que $\text{mcd}(a, b) = 1$.

DEFINICIÓN 2.8. Diremos que K es un campo de números si $[K : \mathbb{Q}] < \infty$. El anillo de enteros de un campo de números K es el conjunto

$$\mathbb{O}_K = \{x \in K : x \text{ es un entero algebraico}\}.$$

El conjunto $\mathbb{O}_K$tiene estructura de anillo pues claramente $\mathbb{O}_K = K \cap \Omega$. Si tenemos un campo de números K, la primera tarea que quisieramos resolver es saber explícitamente quién es su anillo de enteros. Necesitamos más herramientas para responder parcialmente a nuestra pregunta.

Supongamos que L/K es una extensión finita y sea $\alpha \in L \setminus \{0\}$. Si $\alpha_1, \ldots, \alpha_n$ es una base de L sobre K, entonces $\alpha\alpha_1, \ldots \alpha\alpha_n$ es también una base. Escribimos

$$\alpha\alpha_i = \sum_{i=1}^{n} a_{ij}\alpha_j.$$

Entonces la matriz $(a_{ij}) \in M_{n\times n}(K)$ determina en forma única la transformación lineal

$$T_\alpha : L \to L,$$

definida como $T(x) = \alpha x$. Una observación sumamente importante es que la matriz (a_{ij}) tiene entradas en el campo K y por tanto $det((a_{ij})) \in K$ y $traza((a_{ij})) \in K$. En particular, si $K = \mathbb{Q}$, entonces $det((a_{ij}))$ y $traza((a_{ij}))$ son números racionales.

DEFINICIÓN 2.9. Para $\alpha \in L \setminus \{0\}$ de la discusión anterior, definimos la norma y la traza de α como $N(\alpha) = det((a_{ij}))$ y $tr(\alpha) = traza((a_{ij}))$ respectivamente.

Es claro que para calcular $N(\alpha)$ y $tr(\alpha)$ es necesario tener una base, pero si calculamos $N(\alpha)$ y $tr(\alpha)$ con otra base ¿obtenemos el mismo resultado?

EJEMPLO 2.10. Sea $\alpha = a + b\sqrt{d}$ un elemento típico del campo $L = \mathbb{Q}(\sqrt{d})$ y $\{1, \sqrt{d}\}$ una base de L sobre $\mathbb{Q}$. Entonces la matriz (a_{ij}) es

$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix}.$$

Por lo tanto $N(\alpha) = a^2 - b^2 d$ y $tr(\alpha) = 2a$. Apliquemos la misma definición con otra base. Supongamos ahora que la base es $\frac{1}{2}, 1 - \sqrt{d}$. Entonces la matriz (a_{ij}) es:

$$\begin{pmatrix} a+b & 2b(1-d) \\ \frac{-b}{2} & a-b \end{pmatrix}.$$

El lector puede verificar fácilmente que el determinante y la traza de la matriz anterior coincide con el determinante y la traza de la matriz que obtuvimos en un principio.

A continuación vamos a ver que efectivamente, la norma y traza no dependen de la elección de la base.

TEOREMA 2.11. *Sea L/K una extensión finita de campos. La norma y la traza no dependen de la base.*

DEMOSTRACIÓN. Sean $A_1 = (a_{ij})$ la matriz que se obtiene con la base $B_1 = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, y $A_2 = (b_{ij})$ la matriz que se obtiene a partir de la base $B_2 = \{\beta_1, \beta_2, \ldots, \beta_n\}$. Si N es la matriz cambio de base de B_2 a B_1, se tiene que

$$A_1 = N^{-1} A_2 N$$

y aplicando el determinante a cada uno de los lados de la igualdad

$$\det(A_1) = \det(N^{-1} A_2 N) = \det(N^{-1}) \det(A_1) \det(N) = \det(A_1).$$

Por lo anterior, tenemos que $N(\alpha) = \det(A_1) = \det(A_2)$.

Finalmente, la traza de matrices cuadradas satisface la propiedad general

$$traza(CD) = traza(DC).$$

Por lo tanto

$$traza(A_1) = traza(N^{-1} A_2 N) = traza(NN^{-1} A_2) = traza(A_2). \qquad \square$$

Si L/K es separable y $[L : K] = n$, entonces la norma y traza se pueden calcular con la ayuda de los K-automorfismos de L.

TEOREMA 2.12. *Supongamos que L/K es una extensión de Galois de grado n y denotemos por $Gal(L/K) = \{\sigma_1, \ldots, \sigma_n\}$ al grupo de K-automorfismos de L. Entonces para $\alpha \in L$ tenemos que:*

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

ii) $tr(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$.

DEMOSTRACIÓN. Esta demostración la haremos en dos partes. La primera consiste en demostrar el teorema suponiendo que α es un elemento primitivo y luego demostraremos el caso general.

Si α es un elemento primitivo, entonces $L = K(\alpha)$ y $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es una base de la extensión. Supongamos que

$$Irr(\alpha, K) = \prod_{i=1}^{n}(x - \alpha^{(i)}) = x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0.$$

Se conocen las siguientes relaciones entre las raíces de un polinomio y sus coeficientes:

$$a_{n-1} = \sum_{i=1}^{n}(-1)^i\beta_i$$

$$a_0 = (-1)^n \prod_{i=1}^{n} \beta_i$$

donde β_i $(1 \leqslant i \leqslant n)$ son las distintas raíces del polinomio. Por lo anterior

$$a_{n-1} = \sum_{i=1}^{n}(-1)\sigma_i(\alpha)$$

$$a_0 = (-1)^n \prod_{i=1}^{n} \sigma_i(\alpha).$$

Ahora, como

$$\begin{aligned}
\alpha \cdot 1 &= 0 \cdot 1 + 1 \cdot \alpha + 0 \cdot \alpha^2 + \cdots + 0 \cdot \alpha^{n-1} \\
\alpha \cdot \alpha &= 0 \cdot 1 + 0 \cdot \alpha + 1 \cdot \alpha^2 + \cdots + 0 \cdot \alpha^{n-1} \\
&\vdots \quad \vdots \quad \vdots \quad \vdots \qquad \vdots \\
\alpha \cdot \alpha^{n-2} &= 0 \cdot 1 + 0 \cdot \alpha + 0 \cdot \alpha^2 + \cdots + 1 \cdot \alpha^{n-1},
\end{aligned}$$

y

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

entonces

$$(a_{ij}) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

El determinante y la traza de esta matriz son

$$\det((a_{ij})) = (-1)^n a_0 \quad \text{y} \quad traza((a_{ij})) = -a_{n-1}.$$

De esto se sigue que

$$N(\alpha) = (-1)^n a_0 = (-1)^{2n} \prod_{i=1}^{n} \sigma_i(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

$$tr(\alpha) = -a_{n-1} = -\sum_{i=1}^{n} (-1)^i \sigma_i(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha),$$

lo que demuestra el resultado cuando α es un elemento primitivo.

Ahora sea $\alpha \in L$, no necesariamente primitivo. La extensión L/K se puede dividir en dos partes: la primera $K(\alpha)/K$, y la segunda $L/K(\alpha)$. Se observa que si $[K(\alpha) : K] = d$ y $[L : K] = n$, entonces, $[L : K(\alpha)] = \dfrac{n}{d} = r$.

Ahora, si $\{1, \alpha, \ldots, \alpha^{d-1}\}$ es una base de $K(\alpha)/K$ y $\{\beta_1, \beta_2, \ldots, \beta_r\}$ es una base de la extensión $L/K(\alpha)$, entonces

$$\{\beta_k \alpha^j : 1 \leq k \leq r, 0 \leq j \leq d-1\}$$

es una base de L/K, la cual se puede escribir como una unión de subconjuntos de la siguiente manera

$$\{\beta_k \alpha^j\} = \{\beta_1 \alpha^j : 0 \leq j \leq d-1\} \cup \{\beta_2 \alpha^j : 0 \leq j \leq d-1\} \cup \cdots \cup \{\beta_r \alpha^j : 0 \leq j \leq d-1\}.$$

Observemos que $\alpha(\beta_k \alpha^j) = \beta_k(\alpha \alpha^j)$. Además, las entradas de la matriz (a_{ij}) con respecto a $K(\alpha)/K$ se encuentran tomando en cuenta que

$$\alpha \alpha^j = \sum_{i=0}^{d-1} a_{(i+1)(j+1)} \alpha^j.$$

Así,

$$\alpha(\beta_k \alpha^j) = \beta_k \sum_{i=0}^{d-1} a_{(i+1)(j+1)} \alpha^j = \sum_{i=0}^{d-1} a_{(i+1)(j+1)} \beta_k \alpha^j.$$

Sea $\gamma_l = \beta_k \alpha^j$. Entonces $\alpha\gamma_l = \sum_{i=0}^{d-1} a_{(i+1)(j+1)}\beta_k\alpha^j$ y $\beta_k\alpha^j = \gamma_{dk+j}$. Sea $c_{lm} = a_{ij}$ con $l \equiv i \pmod{d}$ y $m \equiv j \pmod{d}$ con $kd \leq l, m < (k+1)d$.

Se puede observar que

$$(c_{ij}) = \begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A \end{pmatrix}$$

es la matriz asociada a la transformación T_α con respecto a la base $\{\beta_k\alpha^j\}$, donde A es la matriz de T_α con la base $\{1, \alpha, \ldots, \alpha^{d-1}\}$ con respecto a la extensión de campos $K(\alpha)/K$. Así que

$$tr_{L/K}(\alpha) = r \cdot traza(A) \quad \text{y} \quad N_{L/K}(\alpha) = (\det(A))^r$$

Cada automorfismo de $K(\alpha)/K$ se pueden extender a L/K r-veces. Así que si tomamos un automorfismo de $K(\alpha)/K$, digamos $\sigma_i(x)$, existen r automorfismos de L/K, los cuales escribimos como $\sigma_{ij}(x)$ con $1 \leq j \leq r$, tales que al restringirlos a $K(\alpha)$

$$\sigma_{ij}(x)|_{K(\alpha)} = \sigma_i(x).$$

Utilizando ésta cualidad de los automorfismos se puede calcular la traza y la norma de α de la siguiente manera

$$tr_{L/K}(\alpha) = r \cdot tr(A) = r \cdot tr_{K(\alpha)/K}(\alpha) = r \cdot \sum_{i=1}^{d} \sigma_i(\alpha) = \sum_{\substack{1\leq i\leq d \\ 1\leq j\leq r}} \sigma_{ij}(\alpha)$$

$$N_{L/K}(\alpha) = (\det(A))^r = (N_{K(\alpha)/K}(\alpha))^r = (\prod_{i=1}^{d} \sigma_i(\alpha))^r = \prod_{\substack{1\leq i\leq d \\ 1\leq j\leq r}} \sigma_{ij}(\alpha)$$

que es el resultado que se buscaba. □

Para extensiones finitas separables el teorema anterior también se cumple. El lector interesado puede consultar los teoremas 26 y 27 en [**19**]

Una observación importante es que en extensiones separables la traza no es la función idénticamente 0. En efecto pues si $[L : K] = n$, entonces

$$tr(1) = traza \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = n = [L : K].$$

Si $car(K) = 0$, entonces $tr(1) = n \neq 0$. Si L tiene $q = p^n$ elementos, la traza de un elemento α del campo L es la suma de sus conjugados, esto es $\alpha + \alpha^{p^1} + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}}$, ya que el automorfismo de Frobenius x^p es el generador del grupo de Galois de una extensión finita de campos finitos. El polinomio

$$f(x) = x + x^{p^1} + x^{p^2} + \cdots + x^{p^{n-1}}$$

satisface que $f(\alpha) = tr(\alpha)$ y $f(x)$ es de grado p^{n-1}, así que tiene a lo más p^{n-1} raíces en L, esto quiere decir que no hay más de p^{n-1} elementos del campo L que tengan traza igual a cero, y como L tiene p^n elementos, existe alguno tal que su traza es diferente de cero.

EJEMPLO 2.13. En el campo $K = \mathbb{Q}(\sqrt{10})$ los dos monomorfismos de K a $\mathbb{C}$ son la identidad σ_1 y la conjugación $\sigma_2(a + b\sqrt{10}) = a - b\sqrt{10}$. Así que si $\alpha = a + b\sqrt{10}$ entonces

$$tr(a+b\sqrt{10}) = \sigma_1(a+b\sqrt{10})+\sigma_2(a+b\sqrt{10}) = (a+b\sqrt{10})+(a-b\sqrt{10}) = 2a,$$

y

$$\begin{aligned} N(a + b\sqrt{10}) &= \sigma_1(a + b\sqrt{10})\sigma_2(a + b\sqrt{10}) \\ &= (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2. \end{aligned}$$

PROPOSICIÓN 2.14. *Sea K un campo de números tal que $[K : \mathbb{Q}] = n$. Si $\alpha, \beta \in K$ y $c \in \mathbb{Q}$, entonces:*

i) $tr(\alpha + \beta) = tr(\alpha) + tr(\beta)$.
ii) $N(a\beta) = a^n N(\beta)$.
iii) $tr(a\alpha) = a\, tr(\alpha)$.
iv) $N(\alpha\beta) = N(\alpha)N(\beta)$.
v) $N(1) = 1$.
vi) $N(\alpha^{-1}) = N(\alpha)^{-1}$, *si* $\alpha \neq 0$.

DEMOSTRACIÓN.

i) $tr(\alpha)$ es la traza de la matriz (a_{ij}). Por lo tanto, la propiedad se sigue a partir de que la traza de matrices es lineal.

ii) $N(a\alpha) = \det(a \cdot a_{ij}) = a^n \det(a_{ij}) = a^n N(\alpha)$.

iii) Se sigue debido a que la traza de matrices es lineal.

iv) Si $\alpha\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, $\beta\alpha_i = \sum_{j=1}^{n} b_{ij}\alpha_j$, $\alpha\beta\alpha_i = \sum_{j=1}^{n} c_{ij}\alpha_j$, entonces

$$\begin{aligned} \sum_{j=1}^{n} c_{ij}\alpha_j = \alpha(\beta\alpha_i) &= \alpha \sum_{j=1}^{n} b_{ij}\alpha_j = \sum_{j=1}^{n} b_{ij}\alpha\alpha_j \\ &= \sum_{j=1}^{n}(b_{ij} \sum_{k=1}^{n} a_{jk}\alpha_k) = \sum_{j=1}^{n}\sum_{k=1}^{n} b_{ij}a_{jk}\alpha_k. \end{aligned}$$

Se puede cambiar el orden de las sumas ya que

$$\begin{aligned}\sum_{j=1}^{n}\sum_{k=1}^{n} b_{ij}a_{jk}\alpha_k &= \sum_{j=1}^{n} b_{ij}a_{j1}\alpha_1 + \cdots + b_{ij}a_{jn}\alpha_n \\ &= (b_{i1}a_{11}\alpha_1 + \cdots + b_{i1}a_{1n}\alpha_n) + \cdots \\ &\qquad + (b_{in}a_{n1}\alpha_1 + \cdots + b_{in}a_{nn}\alpha_n) \\ &= \sum_{k=1}^{n} b_{i1}a_{1k}\alpha_k + \cdots + b_{in}a_{nk}\alpha_k = \sum_{k=1}^{n}\sum_{j=1}^{n} b_{ij}a_{jk}\alpha_k.\end{aligned}$$

Entonces $\sum_{j=1}^{n} c_{ij}\alpha_j = \sum_{k=1}^{n}\sum_{j=1}^{n} b_{ij}a_{jk}\alpha_k$, y por lo tanto

$$(c_{ik}) = \left(\sum_{j=1}^{n} b_{ij}a_{jk}\right) = (b_{ik})(a_{ik}).$$

Así tenemos

$$\begin{aligned}N(\alpha\beta) &= \det(c_{ik}) = \det((b_{ik})(a_{ik})) = \det(b_{ik})\det(a_{ik}) \\ &= N(\beta)N(\alpha) = N(\alpha)N(\beta).\end{aligned}$$

v) La matriz (a_{ij}) asociada a 1 es la identidad, y por lo tanto $N(1) = 1$.

vi) Por el inciso anterior tenemos $1 = N(1) = N(a \cdot a^{-1}) = N(a) \cdot N(a^{-1})$, y por lo tanto $N(a^{-1}) = N(a)^{-1}$. □

Una propiedad importante de los enteros algebraicos es la siguiente:

PROPOSICIÓN 2.15. *Si $\alpha \in K$ es un entero algebraico, entonces $tr(\alpha)$ y $N(\alpha) \in \mathbb{Z}$.*

DEMOSTRACIÓN. Sea $f(x) = a_0 + a_1x + \cdots + x^r \in \mathbb{Z}[x]$ tal que $f(\alpha) = 0$ y σ un $\mathbb{Q}$-automorfismo de K. Entonces $f(\alpha) = 0$ y

$$0 = \sigma(f(\alpha)) = a_0 + a_1\sigma(\alpha) + a_2\sigma(\alpha)^2 + \cdots + \sigma(\alpha)^r.$$

Por lo tanto, $\sigma(\alpha)$ es un entero algebraico y así, $tr(\alpha)$ es suma de enteros algebraicos y $N(\alpha)$ es producto de enteros algebraicos. Por lo anterior, $tr(\alpha)$ y $N(\alpha)$ son enteros algebraicos. Por otro lado, $tr(\alpha), N(\alpha) \in \mathbb{Q}$, entonces por el ejercicio 2.7 tenemos que $tr(\alpha), N(\alpha) \in \mathbb{Z}$. □

2.1. Discriminante

Sea L/K una extensión finita de campos. Ahora definiremos el concepto de discriminante de una n-áda de elementos de L, que además está intimamente relacionado con la norma y la traza.

DEFINICIÓN 2.16. Definimos el discriminante del subconjunto $\{\alpha_1, \ldots, \alpha_n\} \subseteq L$ como $\Delta(\alpha_1, \ldots, \alpha_n) = det(tr(\alpha_i\alpha_j))$.

PROPOSICIÓN 2.17. *Sea L/K una extensión de grado n. Si $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$, entonces $\{\alpha_1, \ldots, \alpha_n\}$ es una base de L/K. Si L/K es separable y $\{\alpha_1, \ldots, \alpha_n\}$ es una base de la extensión, entonces $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$.*

DEMOSTRACIÓN. Supongamos que $\alpha_1, \ldots, \alpha_n$ son linealmente dependientes. Entonces existen $a_1, \ldots, a_n \in K$ tales que $\sum_{i=1}^n a_i\alpha_i = 0$ y algún $a_i \neq 0$. Multiplicando por α_j obtenemos que

$$\sum_{i=1}^{n} a_i tr(\alpha_i\alpha_j) = 0, \quad j = 1, 2, \ldots, n.$$

Observamos que la n-ádа $a_1, a_2, \ldots, a_n$ es una solución no trivial del sistema homogéneo

$$\sum_{i=1}^{n} x_i tr(\alpha_i\alpha_j) = 0, \quad j = 1, 2, \ldots, n.$$

Esto muestra que la matriz $(tr(\alpha_i\alpha_j))$ es singular, por lo que su determinante es cero, y consecuentemente $\Delta(\alpha_1, \ldots, \alpha_n) = 0$. Por lo tanto $\{\alpha_1, \ldots, \alpha_n\}$ son linealmente independientes.

Para la segunda afirmación supongamos que $\Delta(\alpha_1, \ldots, \alpha_n) = 0$. Entonces el sistema

$$\sum_{i=1}^{n} x_i tr(\alpha_i\alpha_j) = 0, \quad j = 1, \ldots, n.$$

tiene al menos una solución no trivial en K, $x_i = a_i$. Elegimos $\alpha = \sum_{i=1}^n a_i\alpha_i \neq 0$. Multiplicando α por cada uno de los α_j y aplicando la traza se observa que

$$tr(\alpha\alpha_j) = \sum_{i=1}^{n} a_i tr(\alpha_i\alpha_j) = 0, \quad j = 1, \ldots, n$$

ya que los a_i son solución del sistema. Si $\beta \in L$ y $\beta = \sum_i b_i\alpha_i$, entonces $\alpha\beta = \sum_i b_i\alpha\alpha_i$ y por lo tanto

$$tr(\alpha\beta) = \sum_i b_i tr(\alpha\alpha_i) = 0.$$

La identidad anterior es válida para cualquier $\beta \in L$, en particular si $\beta = \alpha^{-1}$. Así tenemos que

$$tr(\alpha\alpha^{-1}) = tr(1) = n = [L : K] = 0,$$

lo cual no puede ser porque la extensión es separable. □

Podemos relacionar el discriminante de dos bases de la extensión L/K por medio de la matriz cambio de base.

PROPOSICIÓN 2.18. *Si* $\{\alpha_1, \ldots, \alpha_n\}$ *y* $\{\beta_1, \cdots, \beta_n\}$ *son bases de* L/K *y* $\alpha_j = \sum_{i=1}^{n} a_{ij}\beta_i$, *entonces* $\Delta(\alpha_1, \ldots, \alpha_n) = \det(a_{ij})^2 \Delta(\beta_1, \ldots, \beta_n)$.

DEMOSTRACIÓN. Escribimos $\alpha_i = \sum_{j=1}^{n} a_{ij}\beta_j$ y $\alpha_k = \sum_{l=1}^{n} a_{kl}\beta_l$. Multiplicando se obtiene

$$\begin{aligned}\alpha_i\alpha_k &= \left(\sum_{j=1}^{n} a_{ij}\beta_j\right)\left(\sum_{l=1}^{n} a_{kl}\beta_l\right)\\ &= \sum_{j=1}^{n}\left(\sum_{l=1}^{n} a_{kl}\beta_l\right)a_{ij}\beta_j = \sum_{j=1}^{n}\sum_{l=1}^{n} a_{ij}a_{kl}\beta_j\beta_l.\end{aligned}$$

Tomando la traza en ambos lados se observa que

$$tr(\alpha_i\alpha_k) = tr\left(\sum_{j=1}^{n}\sum_{l=1}^{n} a_{ij}a_{kl}\beta_j\beta_l\right).$$

Sean $A = (tr(\alpha_i\alpha_j))$, $B = (tr(\beta_i\beta_j))$ y $C = (a_{ij})$. Entonces $A = CBC^T$ ya que

$$\begin{aligned}ent_{ij}CB &= \sum_{k=1}^{n} a_{ik}tr(\beta_k\beta_j),\\ ent_{ij}(CB)C^T &= \sum_{l=1}^{n}(ent_{il}CB)\left(ent_{lj}C^T\right) = \sum_{l=1}^{n}\sum_{k=1}^{n} a_{ik}a_{jl}tr(\beta_k\beta_l)\\ &= tr\left(\sum_{l=1}^{n}\sum_{k=1}^{n} a_{ik}a_{jl}(\beta_k\beta_l)\right)\\ &= tr\left[\left(\sum_{k=1}^{n} a_{ik}\beta_k\right)\left(\sum_{l=1}^{n} a_{jl}\beta_l\right)\right] = tr(\alpha_i\alpha_j) = ent_{ij}A.\end{aligned}$$

Por lo tanto

$$\begin{aligned}\Delta(\alpha_1, \ldots, \alpha_n) &= \det(A) = \det\left(CBC^T\right) = \det(C)\det(B)\det\left(C^T\right)\\ &= (\det(a_{ij}))^2\Delta(\beta_1, \ldots, \beta_n).\end{aligned}$$

□

PROPOSICIÓN 2.19. *Sean* L/K *Galois, finita de grado* n *y* $\{\alpha_1, \ldots, \alpha_n\} \subseteq L$. *Entonces* $\Delta(\alpha_1, \ldots, \alpha_n) = \left(det\left(\sigma_j(\alpha_i)\right)\right)^2$, *donde* $\sigma_j \in Gal(L/K)$.

DEMOSTRACIÓN. De acuerdo al Teorema 2.12

$$tr(\alpha_i\alpha_j) = \sigma_1(\alpha_i)\sigma_1(\alpha_j) + \cdots + \sigma_n(\alpha_i)\sigma_n(\alpha_j).$$

Si $B = \left(\sigma_j(\alpha_i)\right)$, entonces

$$\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} =$$

$$\begin{pmatrix} tr(\alpha_1\alpha_1) & tr(\alpha_1\alpha_2) & \cdots & tr(\alpha_1\alpha_n) \\ tr(\alpha_2\alpha_1) & tr(\alpha_2\alpha_2) & \cdots & tr(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ tr(\alpha_n\alpha_1) & tr(\alpha_n\alpha_2) & \cdots & tr(\alpha_n\alpha_n) \end{pmatrix} = BB^T$$

El discriminante de $\{\alpha_1, \ldots, \alpha_n\}$ es el determinante de esta última matriz. Por lo tanto

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det\left(BB^T\right) = (\det(B))^2 = \det\left(\sigma_j(\alpha_i)\right)^2. \qquad \square$$

Si se conoce un elemento primitivo de una extensión separable L/K se puede conocer el discriminante de la base generada por éste.

PROPOSICIÓN 2.20. *Sean $1, \beta, \beta^2, \ldots, \beta^{n-1} \in L$ linealmente independientes sobre K y $f(x) = Irr(\beta, K)$. Si L/K es separable, entonces*

$$\Delta(1, \beta, \ldots, \beta^{n-1}) = (-1)^{\frac{(n)(n-1)}{2}} N(f'(\beta))$$

donde $f'(x)$ es la derivada formal de $f(x)$.

DEMOSTRACIÓN. Definamos la matriz A como

$$A = \begin{pmatrix} (\sigma_1(\beta))^0 & (\sigma_2(\beta))^0 & \cdots & (\sigma_n(\beta))^0 \\ (\sigma_1(\beta))^1 & (\sigma_2(\beta))^1 & \cdots & (\sigma_n(\beta))^1 \\ \vdots & \vdots & \ddots & \vdots \\ (\sigma_1(\beta))^{n-1} & (\sigma_2(\beta))^{n-1} & \cdots & (\sigma_n(\beta))^{n-1} \end{pmatrix},$$

y la matriz B como

$$B = \begin{pmatrix} (\sigma_1(\beta))^0 & \cdots & (\sigma_n(\beta))^0 \\ (\sigma_1(\beta))^1 & \cdots & (\sigma_n(\beta))^1 \\ \vdots & \ddots & \vdots \\ (\sigma_1(\beta))^{n-1} & \cdots & (\sigma_n(\beta))^{n-1} \end{pmatrix} \begin{pmatrix} (\sigma_1(\beta))^0 & \cdots & (\sigma_1(\beta))^{n-1} \\ (\sigma_2(\beta))^0 & \cdots & (\sigma_2(\beta))^{n-1} \\ \vdots & \ddots & \vdots \\ (\sigma_n(\beta))^0 & \cdots & (\sigma_n(\beta))^{n-1} \end{pmatrix}$$

$$= \begin{pmatrix} tr(\beta^0\beta^0) & tr(\beta^0\beta^1) & \cdots & tr(\beta^0\beta^{n-1}) \\ tr(\beta^1\beta^0) & tr(\beta^1\beta^1) & \cdots & tr(\beta^1\beta^{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ tr(\beta^{n-1}\beta^0) & tr(\beta^{n-1}\beta^1) & \cdots & tr(\beta^{n-1}\beta^{n-1}) \end{pmatrix} = AA^T.$$

Entonces $\det(B) = \Delta(1, \beta, \ldots, \beta^{n-1}) = (\det(A))^2$. La matriz A es una matriz tipo Vandermonde, por lo que

$$\det(A) = \prod_{i<j} \left(\sigma_j(\beta) - \sigma_i(\beta)\right).$$

Existen $\sum_{i=1}^{n}(i-1) = \sum_{i=1}^{n-1} i = \dfrac{(n-1)(n-2)}{2}$ pares de enteros (i, j) con $1 \leq i, j \leq n$ tales que $i < j$. Sea $a = (-1)^{\frac{(n-1)(n-2)}{2}}$. Entonces podemos escribir

$$\prod_{i<j} \left(\sigma_j(\beta) - \sigma_i(\beta)\right) = a \prod_{i<j} \left(\sigma_i(\beta) - \sigma_j(\beta)\right) = a \prod_{i>j} \left(\sigma_j(\beta) - \sigma_i(\beta)\right).$$

La última igualdad se obtiene intercambiando j por i. Así

$$\begin{aligned}
(\det A)^2 &= \left(\prod_{i<j} \left(\sigma_j(\beta) - \sigma_i(\beta)\right)\right)^2 \\
&= (-1)^{\frac{(n-1)(n-2)}{2}} \left(\prod_{i<j} \left(\sigma_j(\beta) - \sigma_i(\beta)\right)\right) \left(\prod_{i>j} \left(\sigma_j(\beta) - \sigma_i(\beta)\right)\right) \\
&= (-1)^{\frac{(n-1)(n-2)}{2}} \prod_{i \neq j} \left(\sigma_j(\beta) - \sigma_i(\beta)\right).
\end{aligned}$$

Por lo tanto

$$\Delta(1, \beta, \beta^2, \ldots, \beta^n) = (-1)^{\frac{(n-1)(n-2)}{2}} \prod_{i \neq j} \left(\sigma_j(\beta) - \sigma_i(\beta)\right). \qquad \square$$

En lo que sigue, vamos a justificar la existencia de ciertas bases de la extensión $K/\mathbb{Q}$ con propiedades importantes.

LEMA 2.21. *Sea β en K. Entonces, existe $b \in \mathbb{Z} \setminus \{0\}$ tal que $b\beta \in \mathbb{O}_K$.*

DEMOSTRACIÓN. β satisface algún polinomio $b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0$ con $b_i \in \mathbb{Z}$ y $b_n \neq 0$. Multiplicamos este último polinomio por b_n^{n-1}. Se observa que

$$(b_n\beta)^n + b_{n-1}(b_n\beta)^{n-1} + (b_{n-2} \cdot b_n)(b_n\beta)^{n-2} + \cdots + b_0 \cdot b_n^{n-1} = 0.$$

Por lo tanto $b_n\beta$ es un entero algebraico. $\square$

COROLARIO 2.22. *Sean $\beta_1, \ldots, \beta_n \in K$. Existe $b \in \mathbb{Z}$ tal que $b\beta_1, \ldots, b\beta_n \in \mathbb{O}_K$.*

DEMOSTRACIÓN. Por el Lema 2.21, existen $b_1, \ldots, b_n \in \mathbb{Z}$ tales que $b_i\beta_i \in \mathbb{O}_K$. Si $b = \operatorname{mcm}(b_1, \ldots, b_n)$, entonces es claro que $b\beta_1, \ldots, b\beta_n \in \mathbb{O}_K$. $\square$

COROLARIO 2.23. *Cada ideal $I \neq \{0\}$ de $\mathbb{O}_K$ contiene una base de K sobre $\mathbb{Q}$.*

DEMOSTRACIÓN. Sea $\{\beta_1, \beta_2, \ldots, \beta_n\}$ una base de K sobre $\mathbb{Q}$. Por el Corolario 2.22 existe $b \in \mathbb{Z}$, $b \neq 0$ tal que $b\beta_1, b\beta_2, \ldots, b\beta_n \in \mathbb{O}_K$. Si $\alpha \in I$, $\alpha \neq 0$, entonces $\{b\beta_1\alpha, \ldots, b\beta_n\alpha\} \subseteq I$ es una base de K sobre $\mathbb{Q}$. □

Resaltamos algunos hechos sobresalientes acerca del discriminante de una base particular de un campo de números $K/\mathbb{Q}$:

1. Un número racional es un entero algebraico si y sólo si es un entero.
2. Si $\alpha \in \mathbb{O}_K$, entonces $N(\alpha), tr(\alpha) \in \mathbb{Z}$.
3. Si $\alpha_1, \ldots, \alpha_n \in \mathbb{O}_K$, entonces $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.

La siguiente proposición muestra que cada ideal I contiene una base de generadores como $\mathbb{Z}$-módulo.

PROPOSICIÓN 2.24. *Sea I un ideal en $\mathbb{O}_K$ y $\{\alpha_1, \ldots, \alpha_n\} \subseteq I$ una base de $K/\mathbb{Q}$, tal que $|\Delta(\alpha_1, \ldots, \alpha_n)|$ es mínimo. Entonces, $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$.*

DEMOSTRACIÓN. Sea $\alpha \in I$, tal que $\alpha = \gamma_1\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_n\alpha_n$, con $\gamma_i \in \mathbb{Q}$. Mostraremos que $\gamma_i \in \mathbb{Z}$. Supongamos que algún $\gamma_i \notin \mathbb{Z}$. Sin pérdida de generalidad supongamos que $\gamma_1 \notin \mathbb{Z}$. Podemos escribir $\gamma_1 = m + \theta$ con $m \in \mathbb{Z}$ y $0 < \theta < 1$.

Sea $\beta_1 = \alpha - m\alpha_1$, $\beta_2 = \alpha_2, \ldots, \beta_n = \alpha_n$. Se puede ver que $\{\beta_1, \ldots, \beta_n\}$ es una base de $K/\mathbb{Q}$. En particular $\beta_1 \in \mathbb{O}_K$ ya que α y $-m\alpha_i$ son elementos de $\mathbb{O}_K$. Así $\{\beta_1, \ldots, \beta_n\} \subset \mathbb{O}_K$. La matriz cambio de base entre estas dos base es

$$\begin{pmatrix} \theta & \gamma_2 & \gamma_3 & \cdots & \gamma_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix},$$

y su determinante es θ. Usando la Proposición 2.18 tenemos

$$|\Delta(\beta_1, \ldots, \beta_n)| = \theta^2 |\Delta(\alpha_1, \ldots, \alpha_n)| < |\Delta(\alpha_1, \ldots, \alpha_n)|,$$

lo cual no es posible ya $|\Delta(\alpha_1, \ldots, \alpha_n)|$ es mínimo. Lo anterior significa que $\gamma_i \in \mathbb{Z}$ para $1 \leq i \leq n$ y por lo tanto $I \subset \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$. La otra contención es evidente. Por lo tanto

$$I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n. \qquad \square$$

DEFINICIÓN 2.25. Si $\{\alpha_1, \ldots, \alpha_n\} \subset I$ es una base de $K/\mathbb{Q}$ tal que $I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$, entonces diremos que $\{\alpha_1, \ldots, \alpha_n\}$ es una base entera de I.

COROLARIO 2.26. *Si I es un ideal de $\mathbb{O}_K$ y $\mathcal{A}$ y $\mathcal{B}$ son bases enteras arbitrarias de I, entonces el discriminante de $\mathcal{A}$ es igual al de $\mathcal{B}$.*

DEMOSTRACIÓN. Sean $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\}$ y $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$ dos bases enteras del ideal I. Por la Proposición 2.24 el valor absoluto de los discriminantes de $\mathcal{A}$ y $\mathcal{B}$ son mínimos, y además se sabe que son enteros positivos. Por consiguiente son iguales. □

DEFINICIÓN 2.27. El discriminante de un ideal I denotado por $\Delta(I)$ es el discriminante de una base entera de I. Al discriminante de $\mathbb{O}_K$ se le llama el discriminante de K y se denota por δ_K.

DEFINICIÓN 2.28. Sea $\alpha_1, \ldots, \alpha_n$ una base entera del campo K. Sea M la matriz (a_{ij}) donde $a_{ij} = tr(\alpha_i\alpha_j)$. El discriminante del campo K se define como $\delta_K = det(M)$.

El discriminante de un campo es un concepto muy importante pues nos ayuda a identificar cuándo un conjunto de elementos de $\mathbb{O}_K$ es una base entera y además nos da información sobre la factorización de algunos ideales de $\mathbb{O}_K$.

Existen algoritmos para encontrar una base entera y el discriminante de cualquier campo de números, sin embargo, un problema interesante es encontrar una base entera explícita para alguna familia de campos. A continuación daremos algunos ejemplos.

2.2. Campos cuadráticos

Un campo cuadrático es un campo de números K tal que $[K : \mathbb{Q}] = 2$. Se puede ver que cualquier campo cuadrático es de la forma $K = \mathbb{Q}(\sqrt{d})$ con d un entero libre de cuadrados y los elementos de K son de la forma $a + b\sqrt{d}$ con $a, b \in \mathbb{Q}$. Si d es positivo, diremos que K es un campo cuadrático real ya que $K \subseteq \mathbb{R}$, y en el caso $d < 0$ lo llamaremos campo cuadrático imaginario, debido a que una parte del campo no cae en $\mathbb{R}$. Los dos monomorfismos que van de K a los números complejos son la identidad σ_1 y la conjugación $\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}$, así que

$$tr(a + b\sqrt{d}) = 2a, \quad N(a + b\sqrt{d}) = a^2 - db^2.$$

LEMA 2.29. *Sea $K = \mathbb{Q}(\sqrt{d})$ y $\alpha = a + b\sqrt{d} \in K$ con $a, b \in \mathbb{Q}$. Entonces, $\alpha \in \mathbb{O}_K$ si y sólo si $2a, 2b \in \mathbb{Z}$ y $(2a)^2 - (2b)^2 d \equiv 0 \pmod 4$.*

DEMOSTRACIÓN. Supongamos que $\alpha \in \mathbb{O}_K$. Sabemos que $tr(\alpha)$, $N(\alpha) \in \mathbb{Z}$, esto es $2a \in \mathbb{Z}$ y $a^2 - b^2 d \in \mathbb{Z}$. Así, $4(a^2 - b^2 d) \in \mathbb{Z}$,

es decir, $(2a)^2 - (2b)^2 d \equiv 0 \pmod 4$. Falta ver que $2b \in \mathbb{Z}$. Como $(2a)^2 - (2b)^2 d \in \mathbb{Z}$ y $(2a)^2 \in \mathbb{Z}$, entonces $(2b)^2 d \in \mathbb{Z}$. Escribimos $(2b)^2 d = t$ y $2b = \dfrac{x}{y}$ con $\operatorname{mcd}(x, y) = 1$. Por lo anterior, $\dfrac{x^2}{y^2} d = t$ si y sólo si $x^2 d = y^2 t$, si y sólo si $y^2 \mid 1$ y $y = \pm 1$. Por tanto $2b \in \mathbb{Z}$.

Recíprocamente, si $2a, 2b \in \mathbb{Z}$ y $(2a)^2 - (2b)^2 d \equiv 0 \pmod 4$, entonces $a^2 - b^2 d \in \mathbb{Z}$. Por lo tanto $p(x) = x^2 - 2ax + (a^2 - b^2 d) \in \mathbb{Z}[x]$ es un polinomio mónico con coeficientes enteros tal que $p(a + b\sqrt{d}) = 0$ y $\alpha \in \mathbb{O}_K$. □

COROLARIO 2.30. *Consideremos el campo $K = \mathbb{Q}(\sqrt{d})$ con d libre de cuadrados. Si $d \equiv 2, 3 \pmod 4$, entonces una base entera de $\mathbb{O}_K$ es $\{1, \sqrt{d}\}$. Si $d \equiv 1 \pmod 4$ entonces $\left\{1, \dfrac{1 + \sqrt{d}}{2}\right\}$ es una base entera de $\mathbb{O}_K$.*

DEMOSTRACIÓN. Sea $\alpha = a + b\sqrt{d} \in \mathbb{O}_K$. Si $d \equiv 2 \equiv -2 \pmod 4$, entonces

$$0 \equiv (2a)^2 - (2b)^2 d \equiv (2a)^2 + 2(2b)^2 \pmod 4,$$

y si $d \equiv 3 \equiv -1 \pmod 4$, entonces

$$0 \equiv (2a)^2 - (2b)^2 d \equiv (2a)^2 + (2b)^2 \pmod 4.$$

En cualquiera de los dos casos, $2a$ y $2b$ tienen que ser enteros pares, y por lo tanto $a, b \in \mathbb{Z}$, esto quiere decir que a y b son enteros. Por lo tanto, usando el lema anterior, tenemos que α es un entero algebraico si y sólo si $a, b \in \mathbb{Z}$, y una base entera es $\{1, \sqrt{d}\}$.

Ahora supongamos que $d \equiv 1 \pmod 4$. Tenemos que $(2a)^2 - (2b)^2 d \equiv (2a)^2 - (2b)^2 \equiv 0 \pmod 4$. Entonces $(2a)^2 \equiv (2b)^2 \pmod 4$ y $2a \equiv 2b \pmod 2$.

Podemos escribir

$$\begin{aligned} \alpha = a + b\sqrt{d} &= \frac{2(a + b\sqrt{d})}{2} = \frac{2a - 2b}{2} + \frac{2b + 2b\sqrt{d}}{2} \\ &= \frac{2a - 2b}{2} + 2b\frac{1 + \sqrt{d}}{2}, \end{aligned}$$

y ya que $\dfrac{2a - 2b}{2}, 2b \in \mathbb{Z}$, entonces se cumple que $\mathbb{O}_K \subseteq \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$. Para la otra contención es suficiente mostrar que $\dfrac{1 + \sqrt{d}}{2} \in \mathbb{O}_K$. Puesto que $\dfrac{1 - d}{4} \in \mathbb{Z}$, se tiene $f(x) = x^2 + x + \dfrac{1 - d}{4} \in \mathbb{Z}[x]$ es irreducible por el criterio de Eisenstein. Además $f\left(\frac{1+\sqrt{d}}{2}\right) = 0$ y por lo tanto

$\frac{1+\sqrt{d}}{2} \in \mathbb{O}_K$. Esto quiere decir que una base entera de $\mathbb{O}_K$ es $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$. □

Usando el resultado del corolario anterior, calcularemos el discriminante de $K = \mathbb{Q}(\sqrt{d})$.

COROLARIO 2.31. *Sea δ_K el discriminante de $K = \mathbb{Q}(\sqrt{d})$ con d un entero libre de cuadrados. Si $d \equiv 2, 3 \pmod 4$, entonces $\delta_K = 4d$. Si $d \equiv 1 \pmod 4$, entonces $\delta_K = d$.*

DEMOSTRACIÓN. Si $d \equiv 2, 3 \pmod 4$ sabemos que $\mathbb{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Sean $\alpha_1 = 1$ y $\alpha_2 = \sqrt{d}$. Entonces, como $\{\alpha_1, \alpha_2\}$ es una base entera de $\mathbb{O}_K$, se tiene que

$$\delta_K = \det(t(\alpha_i\alpha_j)) = \det \begin{pmatrix} t(1) & t(\sqrt{d}) \\ t(\sqrt{d}) & t(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

Si $d \equiv 1 \pmod 4$ entonces $\mathbb{O}_K = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$. Sean $\alpha = 1$ y $\alpha_2 = \frac{1+\sqrt{d}}{2}$. Entonces

$$\delta_K = \det(t(\alpha_i\alpha_j)) = \det \begin{pmatrix} t(1) & t\left(\frac{1+\sqrt{d}}{2}\right) \\ t\left(\frac{1+\sqrt{d}}{2}\right) & t\left(\left(\frac{1+\sqrt{d}}{2}\right)^2\right) \end{pmatrix}$$

$$\det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = d.$$

□

2.3. Otros ejemplos de bases enteras

Existen otros ejemplos en los que se tiene explícitamente una base entera de una familia de campos de números.

PROPOSICIÓN 2.32. *Sean $\xi = e^{(2\pi i/n)}$ una raíz n-ésima primitiva de la unidad y $K = \mathbb{Q}(\xi)$. Entonces $[K : \mathbb{Q}] = \phi(n)$ donde ϕ es la función ϕ de Euler y*

$$\{1, \xi, \xi^2, \ldots, \xi^{\phi(n)-2}, \xi^{\phi(n)-1}\}$$

es una base entera de K.

Por ejemplo, $\xi = e^{(2\pi i/5)}$ es una raíz quinta primitiva de la unidad, y $K(\xi)$ es una extensión de $\mathbb{Q}$ de grado 4, por lo que es un campo de números. Una base entera de K es

$$\{1, \xi, \xi^2, \xi^3\} = \{1, e^{(2\pi i/5)}, e^{(4\pi i/5)}, e^{(6\pi i/5)}\}.$$

El elemento ξ^4 también es un elemento de K, pero no está en la base entera. De hecho, no es necesario agregarlo pues $1 + \xi + \xi^2 + \xi^3 + \xi^4 = 0$, y por lo tanto

$$\xi^4 = -1 - \xi - \xi^2 - \xi^3,$$

así que se puede escribir como combinación lineal de los elementos de la base entera usando coeficientes enteros.

Si ξ es una raíz n-ésima primitiva de la unidad, la intersección de $\mathbb{Q}(\xi)$ con $\mathbb{R}$ es una extensión de grado $\phi(n)/2$, tomando en cuenta que $\phi(n)$ es par si $n \geq 3$. Sea $\varepsilon = \xi + \dfrac{1}{\xi}$. Una base entera de $\mathbb{Q}(\xi) \cap \mathbb{R}$ es

$$\{1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{(\phi(n)-1)/2}\}.$$

Cuando existe α tal que la base entera de un campo de números es de la forma $\{1, \alpha, \ldots, \alpha^k\}$ se dice que ésta es una base entera de potencias, y el anillo de enteros es igual a $\mathbb{Z}[\alpha]$, es decir, los polinomios con coeficientes enteros evaluados en α. Todos los ejemplos que hemos dado son campos de números que tienen una base entera de potencias, sin embargo, éstas no son tan frecuentes, de hecho, se sabe que hay una infinidad de campos que no tienen una base entera de potencias. Algunos de éstos se dan en los campos cúbicos.

PROPOSICIÓN 2.33. *Sean $d = ab^2$ un entero libre de cubos, con a, b libres de cuadrados, y $K = \mathbb{Q}(\sqrt[3]{d})$. Una base entera de K es:*

i) *Si $d \equiv 1 \pmod 9$,*

$$\left\{\sqrt[3]{ab^2}, \sqrt[3]{a^2b}, \frac{1 + \sqrt[3]{ab^2} + \sqrt[3]{a^2b^4}}{3}\right\}$$

es una base entera de K.

ii) *Si $d \equiv 8 \pmod 9$, entonces*

$$\left\{\sqrt[3]{ab^2}, \sqrt[3]{a^2b}, \frac{1 - \sqrt[3]{ab^2} + \sqrt[3]{a^2b^4}}{3}\right\}$$

es una base entera de K.

iii) *Si $d \not\equiv 1, 8 \pmod 9$, entonces*

$$\left\{1, \sqrt[3]{ab^2}, \sqrt[3]{a^2b}\right\}$$

es una base entera de K.

Aunque en este caso si hay bases enteras de potencias, como por ejemplo $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$, es muy fácil encontrar algunos que no tienen bases de este tipo. El lector interesado puede consultar el Theorem 2.10 y la nota 8 al final del Capítulo 2 en [**22**].

2.4. El número de clase

Como siempre, K es un campo de números y $\mathbb{O}_K$ el anillo de enteros de K.

LEMA 2.34. *Si $I \subseteq \mathbb{O}_K$ es un ideal $\neq 0$, entonces, $I \cap \mathbb{Z} \neq (0)$.*

DEMOSTRACIÓN. Sea $\alpha \in I \setminus \{0\}$ y sea $p(x) = x^r + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ tal que $p(\alpha) = 0$, con r mínimo. Entonces $a_0 \neq 0$ y $a_0 = -\alpha^r - \cdots - a_1\alpha \in \mathbb{O}_K$. □

PROPOSICIÓN 2.35. *Para cada ideal $I \neq \{0\}$ de $\mathbb{O}_K$, el cociente $\mathbb{O}_K/I$ es finito.*

DEMOSTRACIÓN. Por el Lema 2.34 existe un entero $a > 0$ en I. Sea $\langle a \rangle$ el ideal principal generado por a en $\mathbb{O}_K$ y φ la función

$$\varphi : \mathbb{O}_K/\langle a \rangle \to \mathbb{O}_K/I$$

$$\varphi(x + \langle a \rangle) = x + I.$$

Si $x + \langle a \rangle = y + \langle a \rangle$, entonces $\varphi(x + \langle a \rangle) = x + I$, $\varphi(y + \langle a \rangle) = y + I$. Como $x - y \in \langle a \rangle \subseteq I$, entonces $(x - y) + I = I$ y por lo tanto $x + I = y + I$. Así $\varphi(x + \langle a \rangle) = \varphi(y + \langle a \rangle)$ y por lo tanto φ es función y además es suprayectiva.

Por lo anterior $|\mathbb{O}_K/\langle a \rangle| \geq |\mathbb{O}_K/I|$. Para probar que $\mathbb{O}_K/I$ es finito, basta mostrar que $\mathbb{O}_K/\langle a \rangle$ lo es. Sea $\{\omega_1, \ldots, \omega_n\}$ una base entera en $\mathbb{O}_K$. Consideremos el conjunto

$$S = \left\{ \sum_{i=1}^{n} y_i \omega_i : 0 \leq y_i < a \right\}.$$

Observa que $|S| = a^n$ porque los ω_i están fijos y los únicos que varían son los y_i. Mostraremos que S es un conjunto de representantes de $\mathbb{O}_K/\langle a \rangle$, es decir

$$\mathbb{O}_K/\langle a \rangle = \{x + \langle a \rangle : x \in S\}.$$

Sea $\omega \in \mathbb{O}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$. Entonces, existen únicos $m_1, \ldots, m_n \in \mathbb{Z}$ tales que

$$\omega = \sum_{i=1}^{n} m_i \omega_i.$$

Por el algoritmo de la división, $m_i = q_i a + \gamma_i$ con $0 \leq \gamma_i < a$. Vamos a mostrar que $\omega + \langle a \rangle = \sum_{i=1}^{n} \gamma_i \omega_i + \langle a \rangle \in \mathbb{O}_K / \langle a \rangle$. Tenemos que

$$\omega - \sum_{i=1}^{n} \gamma_i \omega_i = \sum_{i=1}^{n} m_i \omega_i - \sum_{i=1}^{n} \gamma_i \omega_i = \sum_{i=1}^{n} (m_i - \gamma_i)\omega_i = \sum_{i=1}^{n} a q_i \omega_i \in \langle a \rangle.$$

Por lo tanto $\omega + \langle a \rangle = \sum_{i=1}^{n} \gamma_i \omega_i + \langle a \rangle$ y así cualquier elemento de $\mathbb{O}_K / \langle a \rangle$ contiene un representante en S. Ahora vamos a ver que los elementos del conjunto S son distintos. Supongamos que

$$\sum_{i=1}^{n} \gamma_i \omega_i + \langle a \rangle = \sum_{i=1}^{n} \gamma_i' \omega_i + \langle a \rangle.$$

Entonces $\sum_{i=1}^{n} (\gamma_i - \gamma_i')\omega_i \in \langle a \rangle$ y por lo tanto $\sum_{i=1}^{n} (\gamma_i - \gamma_i')\omega_i = a\beta$ para algún $\beta \in \mathbb{O}_K$. Ahora escribimos

$$\beta = \sum_{i=1}^{n} b_i \omega_i,$$

así que $\sum_{i=1}^{n} (\gamma_i - \gamma_i')\omega_i = a \sum_{i=1}^{n} b_i \omega_i = \sum_{i=1}^{n} a b_i \omega_i$. Entonces $\gamma_i - \gamma_i' = a b_i$. Como $0 \leq \gamma_i < a$ y $0 \leq \gamma_i' < a$, entonces

$$-a < \gamma_i - \gamma_i' < a,$$

y así $b_i = 0$ para $i = 1, \ldots, n$. Entonces $\gamma_i = \gamma_i'$ y por lo tanto, cualesquiera dos elementos de S son diferentes. Así

$$|S| = \left| \left\{ \sum \gamma_i \omega_i | 0 \leq \gamma_i < a \right\} \right| = a^n,$$

lo que significa que $\mathbb{O}_K / \langle a \rangle$ es finito, y $\mathbb{O}_K / I$ es finito para todo ideal $\neq 0$ de $\mathbb{O}_K$. □

DEFINICIÓN 2.36. Sea K un campo de números y $\mathbb{O}_K$ el anillo de enteros de K, $I \neq \{0\}$ ideal de $\mathbb{O}_K$. Definimos la norma del ideal I como $|\mathbb{O}_K / I|$.

COROLARIO 2.37. *$\mathbb{O}_K$ es un anillo Noetheriano.*

DEMOSTRACIÓN. Sea $I_1 \subseteq I_2 \subseteq \ldots$ una cadena ascendente de ideales en $\mathbb{O}_K$. Ya que $\mathbb{O}_K / I_1$ es finito, se sigue que $\mathbb{O}_K / I_1$ sólo contiene un número finito de ideales. Por lo tanto, sólo existe un número finito de ideales de $\mathbb{O}_K$ que contienen a I_1. Así que la cadena $I_1 \subseteq I_2 \subseteq \cdots$ se estaciona y por lo tanto $\mathbb{O}_K$ es Noetheriano. □

COROLARIO 2.38. *Cada ideal primo diferente de* (0) *de* $\mathbb{O}_K$ *es máximo.*

DEMOSTRACIÓN. Sea P un ideal primo. Entonces $\mathbb{O}_K/P$ es un dominio entero finito y por lo tanto $\mathbb{O}_K/P$ es un campo. □

Los anillos de enteros son anillos íntegramente cerrados (si $\alpha \in K$ satisface un polinomio mónico en $\mathbb{O}_K[x]$, entonces $\alpha \in \mathbb{O}_K$), son noetherianos y en ellos cualquier ideal primo es máximo. Estos anillos se llaman dominios de Dedekind.

LEMA 2.39. *Sea* $I \subseteq \mathbb{O}_K$ *un ideal. Si* $\beta \in K \setminus \{0\}$ *es tal que* $\beta I \subseteq I$, *entonces* $\beta \in \mathbb{O}_K$.

DEMOSTRACIÓN. Sea $\{\alpha_1, \ldots, \alpha_2\}$ una base entera de I. Entonces $I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. Como $\beta\gamma \in I$ para todo $\gamma \in I$, entonces, por la Proposición 2.2, β es un entero algebraico. □

LEMA 2.40. *Si* I, J *son ideales de* $\mathbb{O}_K$ *tales que* $IJ = I$, *entonces* $J = \mathbb{O}_K$.

DEMOSTRACIÓN. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base entera de I. Como $I = IJ$, se pueden encontrar elementos $b_{ij} \in J$ tales que cada elemento de la base se pueda escribir como $\alpha_i = \sum_{j=1}^{n} b_{ij}\alpha_j$. Entonces se cumple que

$$\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix},$$

$$\begin{pmatrix} b_{11}-1 & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22}-1 & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn}-1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = 0$$

y de esto se sigue que $\det(b_{ij} - \delta_{ij}) = 0$.

Si calculamos el determinate con el primer renglón de la matriz, es decir, con $\{b_{11}-1, b_{12}, \ldots, b_{1n}\}$, observamos que el menor de cada uno de estos, excepto posiblemente del primero es un elemento de J:

$$\det(b_{ij} - \delta_{ij}) = (b_{11}-1)|\ \ | + b_{12}|\ \ | + \ldots b_{1n}|\ \ |.$$

Excepto tal vez el primer sumando, los demás pertenecen a J porque las entradas de cada determinante son elementos de $\mathbb{O}_K$. Sólo nos falta hacer una observación de $|(b_{11}-1)|$. El menor de $b_{11}-1$ es de la forma $(-1)^n + r$ con $r \in J$. Entonces todo el determinante es de la forma $(-1)^n + s = 0$ donde $s \in J$.

Lo anterior implica que $(-1)^n = -s$ es un elemento de J, lo que significa que $J = \mathbb{O}_K$. □

PROPOSICIÓN 2.41. *Sean $I, J \subseteq \mathbb{O}_K$ ideales y supóngase que $\gamma \in \mathbb{O}_K$ es tal que $\gamma I = JI$. Entonces $\gamma\mathbb{O}_K = J$.*

DEMOSTRACIÓN. Primero demostraremos que $\frac{\beta}{\gamma} I \subseteq I$ con $\beta \in J$. Sea $\alpha \in I$. Entonces $\alpha\beta \in IJ = \gamma I$. Puesto que los elementos de γI son de la forma $\gamma\alpha'$ con $\alpha' \in I$, tenemos $\alpha\beta = \gamma\alpha'$ para algún $\alpha' \in I$. Debido a esto $\frac{\beta}{\gamma} = \alpha' \in I$ para todo $\alpha \in I$. Entonces $\frac{\beta}{\gamma} I \subseteq I$.

Usando el Lema 2.39 se observa que $\frac{\beta}{\gamma} \in \mathbb{O}_K$, y entonces $\beta \in \gamma\mathbb{O}_K$. De aquí se sigue que $J \subseteq \gamma\mathbb{O}_K$ y por esto $\gamma^{-1}J \subseteq \mathbb{O}_K$. Observemos que $\gamma^{-1}J$ es un ideal de $\mathbb{O}_K$. En efecto, un elemento de $\gamma^{-1}J$ es de la forma $\gamma^{-1}\beta$ con $\beta \in J$. Para $q \in \mathbb{O}_K$, se tiene $(\gamma^{-1}\beta)q = \gamma^{-1}(\beta q)$ y como $\beta \in J$, entonces $\beta q \in J$, por lo que $(\gamma^{-1}\beta)q \in \gamma^{-1}J$, así $\gamma^{-1}J$ es un ideal de $\mathbb{O}_K$.

Por hipótesis $\gamma I = IJ$, así que $I = \gamma^{-1}JI$. Por el Lema 2.40 $\gamma^{-1}J = \mathbb{O}_K$ y por lo tanto $J = \gamma\mathbb{O}_K$. □

A continuación definiremos una relación de equivalencia entre los ideales $\neq 0$ del anillo de enteros, la cual dará lugar a un grupo. Dos ideales $I, J \subseteq \mathbb{O}_K$ son equivalentes ($I \sim J$) si existen dos ideales principales $\alpha\mathbb{O}_K, \beta\mathbb{O}_K \subseteq \mathbb{O}_K$ tales que $(\alpha\mathbb{O}_K)I = (\beta\mathbb{O}_K)J$. Demostraremos que esta relación es de equivalencia. Las clases de equivalencia se llaman clases de ideales.

PROPOSICIÓN 2.42. *$\sim$ es de equivalencia.*

DEMOSTRACIÓN. Sean $I, J, K \subseteq \mathbb{O}_K$ ideales. La reflexividad y la simetría son evidentes. Para la transitividad supongamos que $I \sim J$ y $J \sim K$. Entonces existen ideales principales, $\alpha_1\mathbb{O}_K$, $\beta_1\mathbb{O}_K$, $\alpha_2\mathbb{O}_K$ y $\beta_2\mathbb{O}_K$, tales que $(\alpha_1\mathbb{O}_K)I = (\beta_1\mathbb{O}_K)J$ y $(\alpha_2\mathbb{O}_K)J = (\beta_2\mathbb{O}_K)K$. Multiplicando por α_2 la primera igualdad y por β_1 la segunda tenemos $(\alpha_2\alpha_1\mathbb{O}_K)I = (\alpha_2\beta_1\mathbb{O}_K)J$, $(\beta_1\alpha_2\mathbb{O}_K)J = (\beta_1\beta_2\mathbb{O}_K)K$. Por lo tanto $(\alpha_2\alpha_1\mathbb{O}_K)I = (\beta_1\alpha_2\mathbb{O}_K)J = (\beta_1\beta_2\mathbb{O}_K)K$, lo que implica que $I \sim K$, y por lo tanto la relación es transitiva. □

DEFINICIÓN 2.43. Sea $Cl(K) = \{\bar{I} : I \text{es ideal} \neq 0 \text{ de } \mathbb{O}_K\}$. El número de clase de K es la cardinalidad de $Cl(K)$ el cual denotaremos como h_K.

Vamos a mostrar que h_K es finito, pero antes necesitaremos del célebre Lema de Hurwitz.

LEMA 2.44. [Lema de Hurwitz] *Sea K un campo de números. Existe un entero positivo M, el cual depende únicamente del campo K y con*

la siguiente propiedad: dados $\alpha, \beta \in \mathbb{O}_K$ con $\beta \neq 0$, existe otro entero racional $1 \leq t \leq M$, y $\omega \in \mathbb{O}_K$ tal que

$$|N(t\alpha - \omega\beta)| < |N(\beta)|.$$

DEMOSTRACIÓN. Sea $\gamma = \dfrac{\alpha}{\beta} \in K$. Es suficiente probar que para todo $\gamma \in K$ existe M tal que $|N(t\gamma - \omega)| < 1$ para algún $1 \leq t \leq M$ y un $\omega \in \mathbb{O}_K$. Esto es cierto pues $|N(t\alpha - \omega\beta)| < |N(\beta)|$ si y sólo si $\dfrac{|N(t\alpha - \omega\beta)|}{N|\beta|} < \dfrac{|N(\beta)|}{N|\beta|}$. Por lo tanto $\left|N\left(\dfrac{t\alpha - \omega\beta}{\beta}\right)\right| < \left|N\left(\dfrac{\beta}{\beta}\right)\right|$ si y sólo si $|N(t\gamma - \omega)| < 1$.

Sea $\{\omega_1, \ldots, \omega_n\}$ una base entera de $\mathbb{O}_K$. Si $\gamma \in K$, $\gamma = \sum_{i=1}^{n} \gamma_i \omega_i$ con $\gamma_i \in \mathbb{Q}$. El valor absoluto de la norma de γ cumple con

$$\begin{aligned}
|N(\gamma)| &= \left| \prod_{i=1}^{n} \left(\sum_{j=1}^{n} \gamma_i \omega_i^{(j)} \right) \right| \\
&\leq \prod_{i=1}^{n} \left(\sum_{j=1}^{n} \left| \gamma_i \omega_i^{(j)} \right| \right) \\
&= \prod_{i=1}^{n} \sum_{j=1}^{n} \left(|\gamma_i| \left| \omega_i^{(j)} \right| \right) \qquad (1.2) \\
&\leq \prod_{i=1}^{n} \sum_{j=1}^{n} \left[\left(\max_i |\gamma_i| \right) \left| \omega_i^{(j)} \right| \right] \\
&= \left[\prod_{j=1}^{n} \left(\sum_{i=1}^{n} \left| \omega_i^{(j)} \right| \right) \right] \left(\max_i |\gamma_i| \right)^n
\end{aligned}$$

Definimos

$$C = \prod_{j=1}^{n} \left(\sum_{i=1}^{n} \left| \omega_i^{(j)} \right| \right),$$

y m al menor número entero tal que $m > \sqrt[n]{C}$ y $M = m^n$.

Sea $\delta \in K$. Entonces $\delta = \sum_{i=1}^{n} \delta_i \omega_i$. Escribimos $\delta_i = a_i + b_i$ donde $a_i \in \mathbb{Z}$ y $0 \leq b_i < 1$. Si $[\delta] = \sum_{j=1}^{n} a_i \omega_i$ y $\{\delta\} = \sum_{i=1}^{n} b_i \omega_i$ entonces

$$\delta = [\delta] + \{\delta\} = \sum_{j=1}^{n} a_i \omega_i + \sum_{i=1}^{n} b_i \omega_i = \sum_{j=1}^{n} (a_i \omega_i + b_i \omega_i) = \sum_{j=1}^{n} \delta_i \omega_i.$$

Además, como $a_i \in \mathbb{Z}$ y $\{\omega_1, \ldots, \omega_n\}$ es una base entera, entonces $[\delta] \in \mathbb{O}_K$ y $\{\delta\}$ tiene coordenadas entre 0 y 1.

Sea $\Phi : K \to \mathbb{R}^n$ definido como $\Phi(\delta) = (\delta_1, \delta_2, \ldots, \delta_n)$. Observemos que

$$\Phi(\{\delta\}) = (b_1, \ldots, b_n)$$

está en un cubo unitario de dimensión n. Dividimos a este cubo en m^n subcubos de lado $1/m$.

Por el principio de Dirichlet, existen $k < k'$con $1 \leq k, k' \leq m^n + 1$ tales que $\Phi(k\delta)$ y $\Phi(k'\delta)$ están en el mismo subcubo.

Si $t = k' - k$, entonces $t\delta = k'\delta - k\delta = t[\delta] + \{k'\delta\} - \{k\delta\}$. Observemos que $\delta' = \{k'\delta\} - \{k\delta\}$ tiene coordenadas en valor absoluto menores o iguales a $1/m$ pues están en el mismo subcubo. Además

$$1 \leq k \leq m^n + 1 \quad \text{y} \quad 1 \leq k' \leq m^n + 1, \tag{1.3}$$

$$-1 \geq -k' \geq -m^n - 1 \tag{1.4}$$

Sumando las desigualdades (1.3) y (1.4) se obtiene $-m^n \leq k - k' \leq m^n$. Por lo tanto $|t| \leq m^n = M$. Tambíen notemos que $\omega = t[\delta] \in \mathbb{O}_K$ pues t es un entero y $[\delta]$ un entero algebraico.

Por (1.2) tenemos que

$$|N(\delta)| \leq C \max\{\delta_i\}^n \leq C(1/m)^n = 1$$

y como $t\delta = \omega + \phi$, entonces $\phi = t\delta - \omega$ y finalmente $|N(t\delta - \omega)| \leq |N(\delta)| \leq 1$ que es el resultado buscado. □

El concepto de número de clase es tal vez, uno de los más importantes en teoría de números algebraicos.

TEOREMA 2.45. $h_K < \infty$.

DEMOSTRACIÓN. La idea de la demostración consiste en probar que un ideal dado, sólo puede ser equivalente a uno de una lista finita de ideales.

Sea I un ideal de $\mathbb{O}_K$. Para cada base entera en I se tiene que $N(\alpha) \in \mathbb{Z}$ para todo $\alpha \in I$. Por lo tanto, $|N(\alpha)| \geq 0$. Elegimos $\beta \in I$, $\beta \neq 0$, tal que $|N(\beta)|$ es mínimo. Por el Lema de Hurwitz, existe t con $1 \leq t \leq M$ y M como se definió en el mismo Lema de Hurwitz, de tal forma que para $\alpha \in I$ se cumple

$$|N(t\alpha - \omega\beta)| < |N(\beta)|,$$

para algún $\omega \in \mathbb{O}_K$. Puesto que $|N(\beta)|$ es mínimo, entonces $N(t\alpha - \omega\beta) = 0$ y así $t\alpha = \omega\beta$. Como $1 \leq t \leq M$, entonces de la igualdad $t\alpha = \omega\beta$ se tiene que $M!I \subseteq \beta\mathbb{O}_K$. Es claro que $J = \dfrac{1}{\beta}M!I$ es un

ideal y $J \subseteq \mathbb{O}_K$. Entonces $\beta J = \beta\frac{1}{\beta}M!I = M!I$ y por tanto, los ideales I, J están relacionados. Notemos que cualquier elemento de J es de la forma $\frac{1}{\beta}M!\delta$, para $\delta \in I$, en particular, si $\delta = \beta$ temenos que $M! \in J$. Si $I \neq J$, entonces $\mathbb{O}_K/I \neq \mathbb{O}_K/J$. Como $\mathbb{O}_K/\langle M!\rangle$ es finito, solamente hay un número finito de subanillos de $\mathbb{O}_K/\langle M!\rangle$, entonces solamente hay un número finito de ideales que contienen a $\langle M!\rangle$ que son los mismos que tienen a $M!$ como elemento.

Sean $J_1, J_2, \ldots, J_r$ los ideales de $\mathbb{O}_K$ tal que $M! \in J_i$ con $1 \leq i \leq r$. Hemos probado que $I \sim J_s$ para algún $1 \leq s \leq r$. Por lo tanto hay un número finito de clases de ideales.

□

COROLARIO 2.46. *Para todo ideal I de $\mathbb{O}_K$, existe un entero $1 \leq k \leq h_K$ tal que I^k es un ideal principal.*

DEMOSTRACIÓN. Dado un ideal I de $\mathbb{O}_K$, consideremos el conjunto de ideales

$$\mathcal{J} = \{I^i : 1 \leq i \leq h_K + 1\}.$$

Por el principio de Dirichlet, existen ideales I^i, I^j tales que $I^i \sim I^j$, con $1 \leq i < j \leq h_F + 1$. Así que, para ciertos $\alpha, \beta \in \mathbb{O}_K \setminus \{0\}$ tenemos:

$$(\alpha\mathbb{O}_K)I^i = (\beta\mathbb{O}_K)I^j \tag{1.5}$$

Mostraremos que I^{j-i} es principal. Multiplicando ambos lados de la igualdad (1.5) por β^{-1} obtenemos que

$$\frac{\alpha}{\beta}I^i = I^j.$$

Por lo anterior $I^j \subseteq I^i$, es decir, $\frac{\alpha}{\beta}I^i = I^j \subseteq I^i$. Si $\gamma = \frac{\alpha}{\beta}$, por el Lema 2.39, $\gamma \in \mathbb{O}_K$. Como $\gamma I^i = I^j = I^{j-i}I^i$, entonces por la Proposición 2.41, $\gamma\mathbb{O}_K = I^{j-i}$ y por lo tanto, si $k = j - 1$, I^k es un ideal principal. □

Sea $Cl(K) = \{\overline{I} : I \neq \{0\}$ es ideal de $\mathbb{O}_K\}$. Definimos un producto en $Cl(K)$: para $\overline{I}, \overline{J} \in Cl(K)$ tenemos $\overline{I}\,\overline{J} = \overline{IJ}$. La operación está bien definida pues si $\overline{I} = \overline{I'}$ y $\overline{J} = \overline{J'}$, entonces existen $\alpha, \alpha', \beta, \beta' \in \mathbb{O}_K$ tales que

$$(\alpha\mathbb{O}_K)I = (\alpha'\mathbb{O}_K)I' \quad \text{y} \quad (\beta\mathbb{O}_K)J = (\beta'\mathbb{O}_K)J'.$$

Así $(\alpha\beta\mathbb{O}_K)IJ = (\alpha'\beta'\mathbb{O}_K)I'J'$, y por lo tanto, $\overline{I}\,\overline{J} = \overline{I'}\,\overline{J'}$. Notemos que este producto es asociativo pues el producto de ideales lo es. La clase $\overline{\mathbb{O}_K}$ satisface que $\overline{I}\,\overline{\mathbb{O}_K} = \overline{I}$. Puesto que cualesquiera dos ideales principales están relacionados y por tanto $\overline{\langle\alpha\rangle} = \overline{\mathbb{O}_K}$, del corolario 2.46 $\overline{I^{k-1}}$ es el inverso de $\overline{I}$. Como el anillo de enteros es conmutativo, entonces $Cl(K)$ es un grupo abeliano finito. Por el Teorema de Lagrange y el Corolario 2.46, I^{h_F} es un ideal principal para cualquier I.

DEFINICIÓN 2.47. El grupo $Cl(K)$ lo llamaremos el grupo de clases de ideales de K.

COROLARIO 2.48. *$h_K = 1$ si y sólo si $\mathbb{O}_K$ es un dominio de ideales principales.*

DEMOSTRACIÓN. Sea $I \neq \{0\}$ ideal de $\mathbb{O}_K$. Si $h_K = 1$, entonces para ciertos $\alpha, \beta \in \mathbb{O}_K$ se cumple que $\alpha I = \beta\mathbb{O}_K$, así $I = \alpha^{-1}\beta\mathbb{O}_K$. Por lo tanto $\alpha^{-1}\beta \in I$ y $\alpha^{-1}\beta I \subseteq I$. Por el Lema 2.39 $\alpha^{-1}\beta \in \mathbb{O}_K$ y $I = \alpha^{-1}\beta\mathbb{O}_K = \langle \alpha^{-1}\beta \rangle$. Recíprocamente, sean I, J dos ideales de $\mathbb{O}_K$. Entonces $I = \gamma\mathbb{O}_K, J = \delta\mathbb{O}_K$ para ciertos $\gamma, \delta \in \mathbb{O}_K$. Como $\langle \delta \rangle I = \langle \gamma \rangle J$, entonces cualesquiera dos ideales $\neq \{0\}$ de $\mathbb{O}_K$ están relacionados, por lo tanto $h_K = 1$. □

2.5. Factorización en un campo de números

Ya vimos en el caso de $\mathbb{Z}[\sqrt{10}]$ que para encontrar los ideales primos basta con factorizar los ideales de la forma $\langle p \rangle$ para todos los primos p de $\mathbb{Z}$. Lo mismo sucede en todos los anillos de enteros. Ya vimos cómo se factorizan estos ideales en el caso de los campos cuadráticos. El siguiente resultado nos ayuda a resolver este problema de una forma mucho más general.

TEOREMA 2.49. [Teorema de Kummer] *Sean $K = \mathbb{Q}(\alpha)$ un campo de números de grado n con*

$$\mathbb{O}_K = \mathbb{Z}[\alpha] = \mathbb{Z} + \alpha\mathbb{Z} + \alpha^2\mathbb{Z} + \cdots + \alpha^{n-1}\mathbb{Z},$$

p un primo en $\mathbb{Z}$ y $f(x)$ el irreducible de α en $\mathbb{Q}$ y $\overline{f}(x)$ el polinomio f considerado en $\mathbb{Z}/p\mathbb{Z}$ usando el mapeo natural. Entonces $f(x)$ se puede factorizar como

$$\overline{f}(x) = \overline{g_1}(x)^{e_1} \cdots \overline{g_r}(x)^{e_r},$$

donde $\overline{g_1}(x), \ldots, \overline{g_r}(x)$ son polinomios mónicos irreducibles distintos en $\mathbb{Z}/p\mathbb{Z}[x]$ y $e_1, \ldots, e_e$ son enteros. Para cada i tomemos un polinomio $g_i(x)$ en $\mathbb{Z}[x]$ tal que el mapeo natural manda $g_i(x)$ a $\overline{g_i}(x)$, y definamos

$$P_i = \langle p, g_i(\alpha) \rangle.$$

Todos los P_i son ideales primos con norma $N(P_i) = p^{gr(g_i)}$, y además podemos factorizar al ideal $\langle p \rangle$ como

$$\langle p \rangle = P_1^{e_1} \cdot P_2^{e_1} \cdots P_r^{e_r}.$$

En los campos cuadráticos, podemos aplicar el resultado anterior y obtener:

PROPOSICIÓN 2.50. *Sea $p \in \mathbb{Z}$ un primo impar y δ_K el discriminante de $K = \mathbb{Q}(\sqrt{d})$.*

i) *Si* $p \nmid \delta_K$ *y la congruencia* $x^2 \equiv d \pmod{p}$ *tiene solución en* $\mathbb{Z}$*, entonces* $\langle p \rangle = P_1 P_2$ *donde* P_1, P_2 *son dos ideales primos distintos.*
ii) *Si* $p \nmid \delta_K$ *y la congruencia* $x^2 \equiv d \pmod{p}$ *no tiene solución en* $\mathbb{Z}$*, entonces* $\langle p \rangle$ *es un ideal primo.*
iii) *Si* $p \mid \delta_K$ *entonces* $\langle p \rangle = P^2$*, para un ideal primo* P*.*

PROPOSICIÓN 2.51. *Sea* $p = 2$ *y* δ_K *el discriminante de* K*.*

i) *Si* $2 \nmid \delta_K$ *y* $d \equiv 1 \pmod{8}$*, entonces* $\langle 2 \rangle = P_1 P_2$ *donde* P_1, P_2 *son dos ideales primos distintos.*
ii) *Si* $2 \nmid \delta_K$ *y* $d \equiv 5 \pmod{8}$*, entonces* $\langle 2 \rangle$ *es primo.*
iii) *Si* $2 \mid \delta_K$*, esto es,* $d \equiv 2, 3 \pmod{4}$*, entonces* $\langle 2 \rangle = P^2$ *donde* P *es un ideal primo.*

Para demostrar estos dos resultados, podemos usar el hecho de que la base de un campo cuadrático es de la forma $1, \alpha$, y por lo tanto, cumple la hipótesis del Teorema de Kummer.

Podemos dar los generadores de los ideales primos que nos indican las dos proposiciones anteriores. Por ejemplo, si $d \equiv 1 \pmod{8}$,

$$\langle 2 \rangle = \left\langle 2, \frac{1+\sqrt{d}}{2} \right\rangle \left\langle 2, \frac{1-\sqrt{d}}{2} \right\rangle,$$

y si $d \equiv 2 \pmod{4}$, $\langle 2 \rangle = \langle 2, \sqrt{d} \rangle^2$; y finalmente, si $d \equiv 3 \pmod{4}$ entonces

$$\langle 2 \rangle = \langle 2, 1 + \sqrt{2} \rangle^2.$$

En el caso de los primos impares, si existe $a \in \mathbb{Z}$ tal que $a^2 \equiv d \pmod{p}$, entonces

$$\langle p \rangle = \langle p, a + \sqrt{d} \rangle \langle p, a - \sqrt{d} \rangle.$$

Y si $p \mid \delta_K$ entonces $p \mid d$ y

$$\langle p \rangle = \langle p, \sqrt{d} \rangle^2.$$

Por ejemplo, el anillo de enteros de $K = \mathbb{Q}(\sqrt{10})$ es $\mathbb{Z}[\sqrt{10}]$. En $\mathbb{O}_K$,

$$\langle 2 \rangle = \langle 2, \sqrt{10} \rangle^2, \quad \langle 5 \rangle = \langle 5, \sqrt{10} \rangle^2.$$

Si $p = 3$, $1^2 \equiv 10 \pmod{3}$, entonces

$$\langle 3 \rangle = \langle 3, 1 + \sqrt{10} \rangle \langle 3, 1 - \sqrt{10} \rangle.$$

Finalmente, $x^2 \equiv 10 \pmod{7}$ no tiene solución, entonces $\langle 7 \rangle$ es un ideal primo.

Ahora consideremos el campo $K = \mathbb{Q}(\xi)$, donde $\xi = e^{2\pi i/5}$. Ya mencionamos que una base entera de K es $1, \xi, \xi^2, \xi^3$, por lo que

podemos utilizar el Teorema de Kummer. El polinomio irreducible de ξ es

$$f(x) = x^4 + x^3 + x^2 + x + 1.$$

Así, si queremos encontrar la factorización de $\langle 2\rangle$, debemos de factorizar $f(x)$ en $\mathbb{Z}/2\mathbb{Z}[x]$. En este caso, el polinomio sigue siendo irreducible, por lo tanto $\langle 2\rangle$ es un ideal primo. Lo mismo sucede con $\langle 3\rangle$. Por otro lado, en $\mathbb{Z}/5\mathbb{Z}[x]$, el polinomio se factoriza como:

$$x^4 + x^3 + x^2 + x + 1 = (4 + x)^4.$$

El teorema nos dice que, en este caso,

$$\langle 5\rangle = \langle 5, 4 + \xi\rangle^4.$$

Por otro lado, en $\mathbb{Z}/11\mathbb{Z}[x]$

$$x^4 + x^3 + x^2 + x + 1 = (2 + x)(6 + x)(7 + x)(8 + x),$$

entonces

$$\langle 11\rangle = \langle 11, 2 + \xi\rangle\langle 11, 6 + \xi\rangle\langle 11, 7 + \xi\rangle\langle 11, 8 + \xi\rangle.$$

En $\mathbb{Z}/19\mathbb{Z}[x]$

$$x^4 + x^3 + x^2 + x + 1 = (1 + 5x + x^2)(1 + 5x + x^2),$$

por lo que

$$\langle 19\rangle = \langle 1 + 5\xi + \xi^2\rangle\langle 1 + 15\xi + \xi^2\rangle.$$

Ahora hagamos algunos ejemplos en el anillo de enteros de $\mathbb{Q}(\sqrt[3]{5})$, que como ya dijimos, una base entera de este campo es $1, \sqrt[3]{5}, \sqrt[3]{25}$, y cumple las condiciones del Teorema de Kummer. El polinomio irreducible de $\sqrt[3]{5}$ es $x^3 - 5$, así que tenemos que factorizar este polinomio en algunos campos finitos para poder factorizar los primos de $\mathbb{Z}$. Por ejemplo, módulo 2

$$x^3 - 5 = (1 + x)(1 + x + x^2)$$

y por lo tanto

$$\langle 2\rangle = \langle 2, 1 + \sqrt[3]{5}\rangle\langle 2, 1 + \sqrt[3]{5} + \sqrt[3]{25}\rangle.$$

En $\mathbb{Z}/3\mathbb{Z}$, $x^3 - 5 = (1 + x)^3$ por lo que

$$\langle 3\rangle = \langle 3, 1 + \sqrt[3]{5}\rangle^3.$$

Módulo 7, el polinomio $x^3 - 5$ es irreducible, entonces $\langle 7\rangle$ es un ideal primo. Y en $\mathbb{Z}/13\mathbb{Z}[x]$ el polinomio se factoriza

$$x^3 - 5 = (2 + x)(5 + x)(6 + x),$$

así que

$$\langle 13\rangle = \langle 13, 2 + \sqrt[3]{5}\rangle\langle 13, 5 + \sqrt[3]{5}\rangle\langle 13, 6 + \sqrt[3]{5}\rangle.$$

2.6. Grupo de unidades en anillos de enteros de campos cuadráticos

En esta sección vamos a estudiar el grupo de unidades del anillo de enteros de un campo cuadrático. Sea $K = \mathbb{Q}(\sqrt{d})$. El primer caso que estudiaremos será cuando d es negativo. En este caso el grupo de unidades es un grupo finito. Posteriormente veremos lo que sucede en el caso d positivo. Iniciamos dando un criterio para identificar unidades en un anillo de enteros.

PROPOSICIÓN 2.52. *Sea $K = \mathbb{Q}(\sqrt{d})$ y $\alpha \in \mathbb{O}_K$. Entonces α es una unidad si y sólo si $|N(\alpha)| = 1$.*

DEMOSTRACIÓN. La demostración es igual que la que dimos en $\mathbb{Z}[\sqrt{10}]$, por lo que se deja como ejercicio. □

Ya que tenemos un criterio para saber si un entero algebraico es unidad, procederemos a encontrar el grupo de unidades de los anillos de enteros que nos interesan. Empezaremos con el caso $d < 0$ y libre de cuadrados. Denotemos al grupo de unidades de $\mathbb{O}_K = \mathbb{Q}(\sqrt{d})$ como U_d.

PROPOSICIÓN 2.53. *Sea $d < 0$ un entero racional libre de cuadrados. Entonces*

i) $U_{-1} = \{\pm 1, \pm i\}$.

ii) $U_{-3} = \{\pm 1, \pm\omega, \pm\omega^2\}$ *donde* $\omega = \dfrac{-1+\sqrt{-3}}{2}$.

iii) $U_d = \{\pm 1\}$ *para* $d = -2$ *ó* $d < -1$.

DEMOSTRACIÓN. En el caso $d \equiv 2, 3 \pmod 4$ sabemos que $\mathbb{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, por lo que cualquier unidad α se puede escribir como $\alpha = a + b\sqrt{d}$ con $a, b \in \mathbb{Z}$. Si $d = -1$, sabemos que el valor absoluto de la norma de α es igual a 1 si y sólo si $a^2 + b^2 = 1$. Las soluciones enteras de esta ecuación son $a = \pm 1, b = 0$ y $a = 0, b = \pm 1$. Por lo tanto,

$$U_{-1} = \{\pm 1, \pm i\}.$$

Si $d < -1$, tenemos que $a^2 + |d|b^2 = 1$. Así que necesariamente $b = 0$. Por lo tanto, las únicas soluciones son $a = \pm 1, b = 0$. Esto justifica la afirmación iii) cuando $d \equiv 2, 3 \pmod 4$.

Si $d \equiv 1 \pmod 4$, $\mathbb{O}_K = \mathbb{Z} + \mathbb{Z}\left(\dfrac{1+\sqrt{d}}{2}\right)$. Entonces las unidades las podemos escribir como

$$\alpha = \frac{a + b\sqrt{d}}{2}$$

con $a, b \in \mathbb{Z}$ y $a \equiv b \pmod 2$. Ahora, $|N(\alpha)| = 1$ si y sólo si $a^2 + |d|b^2 = 4$.

Si $d = -3$ tenemos que resolver la ecuación, $a^2 + 3b^2 = 4$. Las únicas soluciones enteras son $a = \pm 2, b = 0$ y $a = \pm 1, b = \pm 1$. Si $a = \pm 2, b = 0$ entonces ± 1 son unidades. Si $a = -1$ y $b = 1$, entonces

$$\omega = \frac{-1 + \sqrt{-3}}{2}$$

es unidad y por lo tanto $\pm\omega, \pm\omega^2 \in U_{-3}$.

Si $d < -3$ tenemos la igualdad $a^2 + |d|b^2 = 4$. Como $|d| > 4$, necesariamente $b = 0$. Por lo tanto $a = \pm 2$, lo que nos da el resultado iii) con $d \equiv 1 \pmod 4$. □ □

Notemos que en los tres casos, el grupo de unidades es cíclico. Ahora encontraremos el grupo de unidades de un anillo de enteros de un campo cuadrático real. Estos dependen de una unidad a la que llamaremos *unidad fundamental*.

PROPOSICIÓN 2.54. *Sea $K = \mathbb{Q}(\sqrt{d})$ con $d > 0$ y libre de cuadrados. Existe una unidad $\epsilon > 1$ (unidad fundamental) tal que $U(\mathbb{O}_K) = \{\pm\epsilon^n : n \in \mathbb{Z}\}$.*

DEMOSTRACIÓN. Esta demostración se deja como ejercicio. Se deben de seguir los siguientes pasos.

i) Vamos a dar por hecho que la Ecuación de Pell, $x^2 - dy^2 = 1$, tiene al menos una solución en $\mathbb{Z}$ con $x \geq 1$ y $y \geq 1$ (ver [**37**], pag. 88).
ii) Usando estos valores, podemos garantizar que existe una unidad $M = x + y\sqrt{d}$ que es mayor que 1.
iii) Demostrar que en el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ hay un número finito de elementos α tales que $-M \leq \alpha \leq M$.
iv) Sea $\mu = a + b\sqrt{d}$ ó $\mu = \dfrac{a + b\sqrt{d}}{2}$ una unidad. Pruebe que $a - b\sqrt{d}$, $-a + b\sqrt{d}$ y $-a - b\sqrt{d}$ también son unidades (en el segundo caso, dividiendo entre 2). Además, pruebe que exactamente una de éstas es mayor que 1.
v) Usando la información anterior, podemos asegurar que hay un número finito de unidades μ tales que $1 < \mu \leq M$.
vi) Sea ϵ la menor de las unidades que se encuentran en este intervalo (¿Por qué existe una mínima?).
vii) Use el procedimiento que se usó en $\mathbb{Z}[\sqrt{10}]$ para demostrar que en el anillo de enteros de $\mathbb{Q}(\sqrt{d})$, cualquier unidad es de la forma $\pm\epsilon^n$ (ϵ es la unidad fundamental).

□

K	Unidad fundamental de $\mathbb{O}_K$
$\mathbb{Q}(\sqrt{2})$	$1+\sqrt{2}$
$\mathbb{Q}(\sqrt{3})$	$2+\sqrt{3}$
$\mathbb{Q}(\sqrt{7})$	$8+3\sqrt{7}$
$\mathbb{Q}(\sqrt{11})$	$10+3\sqrt{11}$
$\mathbb{Q}(\sqrt{15})$	$4+\sqrt{15}$
$\mathbb{Q}(\sqrt{22})$	$197+42\sqrt{22}$
$\mathbb{Q}(\sqrt{31})$	$1520+273\sqrt{31}$
$\mathbb{Q}(\sqrt{94})$	$2143295+221064\sqrt{94}$
$\mathbb{Q}(\sqrt{165})$	$\frac{13+\sqrt{165}}{2}$
$\mathbb{Q}(\sqrt{166})$	$1700902565+132015642\sqrt{22}$

Capítulo 3

Campos cuadráticos de funciones

En este capítulo estudiaremos otra clase de campos cuadráticos, similares a los campos de números. Nuestro objetivo será mostrar herramienta suficientes para poder encontrar todas las factorizaciones de un elemento en el anillo de enteros de alguno de estos campos.

DEFINICIÓN 3.1. Consideremos un campo k. El campo de funciones racionales en una variable con coeficientes en k se define como

$$F = k(x) = \left\{ \frac{p_1(x)}{p_2(x)} : p_1(x), p_2(x) \in k[x], p_2(x) \neq 0 \right\}.$$

Al campo k le llamaremos el campo de constantes.

En otras palabras, los elementos de un campo de funciones racionales son cocientes de polinomios con constantes en un campo.

DEFINICIÓN 3.2. Un *campo de funciones algebraicas* K es una extensión finitamente generada sobre un campo de funciones racionales F.

DEFINICIÓN 3.3. K es un campo de funciones congruente en una variable si, con la notación anterior, $k = \mathbb{F}_q$ el campo finito con q elementos, $F = \mathbb{F}_q(x)$ y K es una extensión finita de F.

Observemos que la definición de campo de funciones congruentes es similar a la de campo de números, usando al campo de funciones racionales en lugar del campo de los números racionales. La razón por la que nos concentraremos en esta familia de campos de funciones es debido a que existe un gran parecido con los campos de números.

Si F es un campo de funciones racionales denotaremos por $\mathbb{O}_F$ al anillo de polinomios en una variable de F, es decir $\mathbb{O}_F = \mathbb{F}_q[x]$.

DEFINICIÓN 3.4. Sea K un campo de funciones congruente sobre un campo de funciones racionales F. El anillo de enteros de K es la cerradura entera de $\mathbb{O}_F$ en K, es decir, los elementos $\alpha \in K$ tales que existe un polinomio mónico $f(T)$ con coeficientes en $\mathbb{O}_F$ tal que $f(\alpha) = 0$. A este anillo lo denotaremos con $\mathbb{O}_K$.

EJEMPLO 3.5. Sea $F = \mathbb{F}_3(x)$. Algunos elementos de este campo son

$$x^2 + x + 1, \quad \frac{2x^2 + x + 2}{x^3 + 2x + 1} \quad \text{y} \quad \frac{1}{x^5 + x^4 + x^2 + 2x}.$$

Consideremos el polinomio $f(T) = T^2 + 2x + 2$ con coeficientes en $\mathbb{O}_F$. Una raíz de este polinomio es la función

$$y = \sqrt{x + 1},$$

así que el campo

$$K = F(y)$$

es una extensión finita sobre F, es decir, K es un campo de funciones congruente. Los elementos

$$x^3 + x^2 + 2x + (x + 1)\sqrt{x + 1} \quad \text{y} \quad \frac{x^2 + \sqrt{x + 1}}{2x^3 + x + 2 + (x^4 + x^2 + 2)\sqrt{x + 1}}$$

están en K.

EJEMPLO 3.6. Sea $F = \mathbb{F}_5(x)$ y consideremos el polinomio

$$f(T) = T^4 + xT^3 + (3x^2 + 1)T^2 + 4x^5T + x^2 + 4x + 2,$$

y sea y una función tal que $f(y) = 0$. Observemos que los coeficientes del polinomio $f(T)$ son, a su vez, polinomios con variable x y coeficientes en $\mathbb{F}_5$. Así, el coeficiente del término de grado 2 de $f(T)$ es $3x^2 + 1$ y el término independiente es $x^2 + 4x + 2$.

Tomemos el campo $K = F(y)$. Como la función y es raíz de un polinomio de grado 4, entonces la extensión K/F es una extensión de grado menor o igual a 4. De esta forma, K es un campo de funciones congruente.

Nos enfocaremos en casos similares al que tenemos en el Ejemplo 3.5, es decir, en los campos cuadráticos.

Una propiedad importante de los anillos de polinomios con coeficientes en un campo es la siguiente:

PROPOSICIÓN 3.7. *Sea F un campo. Entonces $F[x]$ es un dominio de factorización única.*

3.1. Campos cuadráticos de funciones

En la definición que sigue, el– lector podrá notar alguna similitud con los campos de números cuadráticos.

DEFINICIÓN 3.8. Un campo de funciones cuadrático es un campo de funciones congruente K sobre un campo de funciones racionales $F = \mathbb{F}_q(x)$ tal que q es impar y el grado de la extensión K/F es 2. Además, agregaremos la condición de que los campos de constantes de K y F son iguales.

En la definición anterior pedimos que los campos de constantes de K y F sean iguales debido a que, por ejemplo, la extensión de campos K/F con $F = \mathbb{F}_2(x)$ y $K = \mathbb{F}_4(x)$ es una extensión de grado 2 y además K también es un campo de funciones racionales. De esta forma, la condición sirve para que la intersección de los campos de funciones racionales y los campos de funciones cuadráticos sea vacía.

La razón por la que agregamos la condición de que el campo de constantes sea de característica impar es debido a que si $q = 2^r$ entonces la extensión K/F no es una extensión de Galois. Sin embargo, el estudio de campos de funciones de característica 2 también es interesante, pero en el caso de los campos cuadráticos suele hacerse por separado.

El Ejemplo 3.5 es un campo de funciones cuadrático. En ese caso consideramos el polinomio $d(x) = x + 1$ y agregamos una raíz de

$$p(T) = T^2 - d(x),$$

es decir

$$y = \sqrt{d(x)}.$$

Un elemento genérico de $K = F(y)$ es de la forma $a(x) + b(x)y$ con $a(x)$ y $b(x)$ polinomios con coeficientes en $\mathbb{F}_3$.

Todo campo cuadrático de funciones es de esta forma, es decir, tomamos $d(x) \in \mathbb{O}_F$ un polinomio no constante libre de cuadrados. Definimos el elemento $y = \sqrt{d(x)}$ y $K = \mathbb{F}_q(x)(y)$.

PROPOSICIÓN 3.9. *La cerradura entera de $\mathbb{O}_F$ en K es*

$$\mathbb{O}_K = \mathbb{O}_F + y\mathbb{O}_F.$$

DEMOSTRACIÓN. Sea $\alpha = a(x) + b(x)y \in K$. El polinomio irreducible de α con coeficientes en F es

$$p(T) = T^2 - 2a(x)T + a(x)^2 - d(x)b(x)^2.$$

Notemos que el polinomio anterior tiene dos variables, T y x. Recordemos que los elementos de K y F son funciones que están en términos de la variable x, mientras que T es la variable del polinomio $p(T)$, donde sustituimos α obteniendo $p(\alpha) = 0$. Para que α esté en la cerradura entera de $\mathbb{O}_F$ en K, entonces los coeficientes de $p(T)$ deben de estar en $\mathbb{O}_F$. Como 2 es un elemento distinto de cero del campo de constantes $\mathbb{F}_q$, entonces $2a(x) \in \mathbb{O}_F$ si y solamente si $a(x) \in \mathbb{O}_F$ multiplicando por 2^{-1}. Ahora, $a(x)^2 - d(x)b(x)^2 \in \mathbb{O}_F$ si y solamente si $-d(x)b(x)^2 \in \mathbb{O}_F$. Supongamos que $b(x) = \dfrac{b_1(x)}{b_2(x)}$ con $b_1(x), b_2(x)$ polinomios con coeficientes en $\mathbb{F}_q$, primos relativos entre sí. Para que $-d(x)b(x)^2$ sea un polinomio, es necesario que todo lo que está en el denominador se cancele con una parte del numerador. Supongamos que $c(x) \in \mathbb{O}_F$ es un polinomio irreducible que divide a $b_2(x)$, entonces

$c(x)^2 \mid -d(x)b_1(x)^2$ y como $b_1(x)$ y $b_2(x)$ son primos relativos, entonces $c(x)^2 \mid d(x)$, lo que no es posible pues $d(x)$ es libre de cuadrados. Por lo tanto, $a(x), b(x) \in \mathbb{O}_F$. □

Así, el anillo de enteros de K es $\mathbb{O}_K = \mathbb{O}_F + y\mathbb{O}_F$. Al igual que en el caso de los campos cuadráticos sobre $\mathbb{Q}$, podemos definir la traza y la norma de un elemento de K como

$$tr(a(x) + b(x)y) = 2a(x), \quad N(a(x) + b(x)y) = a(x)^2 - d(x)b(x)^2,$$

funciones que satisfacen las mismas propiedades que fueron enunciadas en la Proposición 2.14.

EJEMPLO 3.10. Sea $F = \mathbb{F}_3(x)$, $d(x) = x^3 + x = x(x^2 + 1)$, $y = \sqrt{d(x)}$ y $K = F(y)$. El siguiente polinomio tiene dos factorizaciones distintas en irreducibles:

$$x^2 + x = x(x^2 + 1) = y^2.$$

Por lo tanto, $\mathbb{O}_K$ no es un DFU.

El ejemplo anterior es similar al que vimos en el primer capítulo en el anillo $\mathbb{Z}[\sqrt{10}]$, donde $10 = (2)(5) = (\sqrt{10})^2$. El lector podrá observar que nos encaminamos a usar herramientas de factorización similares a las estudiadas en los anillos de enteros de campos de números.

3.2. Factorización en campos cuadráticos de funciones

La factorización de los ideales en este caso es básicamente idéntica a la que tenemos en el caso de los campos de números. A partir de ahora supongamos que $F = \mathbb{F}_q(x)$ es un campo de funciones racionales sobre un campo finito y que $K = F(\sqrt{d(x)})$ es un campo cuadrático de funciones con $d(x)$ libre de cuadrados.

TEOREMA 3.11. *Sea K un campo cuadrático de funciones y $\mathbb{O}_K$ su anillo de enteros. Todo ideal distinto de cero de $\mathbb{O}_K$ se puede factorizar de forma única como producto de ideales primos.*

La definición de norma de un ideal $I \subseteq \mathbb{O}_K$ es distinta a la de su equivalente en campos de números. Sea

$$J = \langle N(\alpha) : \alpha \in I \rangle,$$

es decir, el ideal de $\mathbb{O}_F$ generado por las normas de los elementos del ideal I. Como $\mathbb{O}_F$ es un anillo de ideales principales, entonces J es un ideal principal. La norma de I se define como el único generador de J que es un polinomio mónico. Aunque está definido de forma distinta, esta norma es, de cierta forma, equivalente a la que dimos en el caso de los campos de números, pues, si definimos de forma análoga el ideal J, en el caso de los campos de números J es generado por la norma de I.

EJEMPLO 3.12. Sea $F = \mathbb{F}_5(x)$ y $K = F(\sqrt{2x+1})$. Para encontrar la norma del ideal $\langle x \rangle$ es necesario conocer el ideal

$$J = \langle N(\alpha) : \alpha \in I \rangle.$$

Los elementos de $\langle x \rangle$ son de la forma $\alpha = x\beta$ para algún $\beta \in \mathbb{O}_K$ y

$$N(\alpha) = x^2 N(\beta).$$

Toda norma es un múltiplo de x^2 y x^2 es un elemento del ideal J, por lo que $J = \langle x^2 \rangle$. Los generadores de J son: x^2, $2x^2$, $3x^2$ y $4x^2$. De éstos, el único que es mónico es x^2, así que

$$N(\langle x \rangle) = x^2.$$

Ahora consideremos el ideal $I_2 = \langle \sqrt{2x+1} \rangle$. De nuevo,

$$J = \langle N(\alpha) : \alpha \in I_2 \rangle$$

y cada $\alpha \in I_2$ es de la forma $\alpha = \sqrt{2x+1}\beta$ con norma $N(\alpha) = (2x+1)N(\beta)$. Así que toda norma es múltiplo de $2x+1$ y este elemento está en J, por lo que $J = \langle 2x+1 \rangle$. Los generadores de J se obtienen multiplicando $2x+1$ por las constantes distintas de cero, es decir: $2x+1$, $2(2x+1) = 4x+2$, $3(2x+1) = x+3$ y $4(2x+1) = 3x+4$. De éstos, el único generador mónico es $x+3$, por lo tanto,

$$N(\langle \sqrt{2x+1} \rangle) = x+3.$$

La norma de un ideal principal está relacionada con la norma de sus generadores.

PROPOSICIÓN 3.13. *Si un ideal de $\mathbb{O}_K$ es principal, digamos $I = \langle \alpha \rangle$, entonces $N(I) = aN(\alpha)$ para algún $a \in \mathbb{F}_q$.*

EJEMPLO 3.14. Retomemos los ideales del Ejemplo 3.12. En el primer caso tenemos $N(x) = x^2$, $N(\langle x \rangle) = x^2$ y $N(x) = N(\langle x \rangle)$. Por otro lado,

$$N(\sqrt{2x+1}) = -(\sqrt{2x+1})^2 = 3x+4 \quad \text{y} \quad N(\langle \sqrt{3x+4} \rangle) = x+3,$$

de donde $x+3 = 2(3x+4)$, lo que satisface la proposición anterior.

Otra propiedad importante de la norma que también es valida en el caso de los campos de funciones es que es multiplicativa.

PROPOSICIÓN 3.15. *Sean K un campo de funciones, $\mathbb{O}_K$ su anillo de enteros. Si J_1, J_2 son ideales de $\mathbb{O}_K$, entonces $N(J_1J_2) = N(J_1)N(J_2)$. Si $\alpha, \beta \in \mathbb{O}_K$, entonces $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Al igual que en el caso de los campos de números, para encontrar todos los ideales primos de $\mathbb{O}_K$, basta con extender los ideales primos de $\mathbb{O}_F$ hasta $\mathbb{O}_K$ y factorizarlos. La siguiente proposición nos ayuda a identificar si un primo en $\mathbb{O}_F$ se ramifica, es inerte o se descompone en

$\mathbb{O}_K$. La regla es la misma que siguen los campos cuadráticos en el caso en el que están sobre el campo $\mathbb{Q}$.

PROPOSICIÓN 3.16. *Sean $F = \mathbb{F}_q(x)$, $\mathbb{O}_F = \mathbb{F}_q[x]$, $K = F(\sqrt{d(x)})$ con $d(x) \in \mathbb{O}_F$ libre de cuadrados y $\mathbb{O}_K$ la cerradura entera de $\mathbb{O}_F$ en K.*

i) *Si no existe $a(x) \in \mathbb{O}_F$ tal que $a(x)^2 \equiv p(x) \pmod{d(x)}$, entonces $p(x)$ es inerte, es decir $\langle p(x)\rangle$ es un ideal primo en $\mathbb{O}_K$.*
ii) *Si $p(x) \mid d(x)$, entonces $p(x)$ se ramifica, esto es $\langle p(x)\rangle = P^2$ para algún ideal primo P.*
iii) *Si $p(x) \nmid d(x)$ y existe $a(x) \in \mathbb{O}_F$ tal que $a(x)^2 \equiv p(x) \pmod{d(x)}$, entonces $p(x)$ se descompone, es decir $\langle p(x)\rangle = P_1P_2$ para dos ideales primos distintos.*

La demostración es similar a la del resultado análogo en campos de números en la Proposición 2.50. En el curso de la prueba se da explícitamente la factorización del ideal $\langle p(x)\rangle$. Si $p(x)$ se descompone, entonces

$$\langle p(x)\rangle = \langle p(x), a(x) + \sqrt{d(x)}\rangle\langle p(x), a(x) - \sqrt{d(x)}\rangle$$

y si se ramifica entonces

$$\langle p(x)\rangle = \langle p(x), \sqrt{d(x)}\rangle^2.$$

EJEMPLO 3.17. Sean $F = \mathbb{F}_5(x)$ y $K = F(\sqrt{x+1})$. El único ideal ramificado de K es

$$\langle x+1\rangle = \langle x+1, \sqrt{x+1}\rangle^2 = \langle \sqrt{x+1}\rangle^2.$$

El polinomio irreducible $x^2 + x + 1$ se descompone en K, pues

$$(3x)^2 \equiv 4x^2 + (x^2 + x + 1) \equiv x + 1 \pmod{x^2 + x + 1},$$

así que

$$\langle x+1\rangle = \langle x+1, 3x + \sqrt{x+1}\rangle\langle x+1, 3x - \sqrt{x+1}\rangle.$$

Finalmente, el ideal $\langle x^3 + 2x^2 + 1\rangle$ es un ideal primo en $\mathbb{O}_K$, pues los cuadrados módulo $x^3 + 2x^2 + 1$ que tienen residuo de grado 1 son:

$$x, x+2, x+4, 2x+1, 2x+2, 3x+3, 3x+4, 4x, 4x+1, 4x+3.$$

El ideal no se descompone pues $x + 1$ no es el producto de una constante por un cuadrado. La razón por la que no se ramifica es que $x^3 + 2x^2 + 1 \nmid x + 1$.

3.3. Unidades

Los campos cuadráticos de funciones se clasifican en tres tipos. Los campos imaginarios ramificados, los campos imaginarios inertes y los campos reales. Los términos ramificado e inertes se refieren a la descomposición del primo al infinito, un concepto que no trataremos en este texto.

DEFINICIÓN 3.18. Sea $K = F(\sqrt{d(x)})$ con $d(x)$ libre de cuadrados:

i) K es un campo cuadrático imaginario ramificado si $\deg(d(x))$ es impar.
ii) K es un campo cuadrático imaginario inerte si $\deg(d(x))$ es par y el coeficiente del término de grado mayor de $d(x)$ no es un cuadrado en $\mathbb{F}_q$.
iii) K es un campo cuadrático real si $\deg(d(x))$ es par y el coeficiente del término de grado mayor de $d(x)$ es un cuadrado en $\mathbb{F}_q$.

Supongamos que el coeficiente del término líder de $d(x)$ es a. En el caso iii), $a = b^2$ para algún $b \in \mathbb{F}_q$, si multiplicamos $b^{-1}\sqrt{d(x)} = \sqrt{b^{-2}d(x)}$. De esta forma, podemos cambiar $d(x)$ por un polinomio mónico. En el caso ii) esto no sucede. No existe ninguna constante que al multiplicarla por $\sqrt{d(x)}$ nos quede un polinomio mónico en el radicando.

EJEMPLO 3.19. Sea $F = \mathbb{F}_9(x)$. Los elementos del campo finito $\mathbb{F}_9$ son: 0, 1, 2, g, $g+1$, $g+2$, $2g$, $2g+1$, $2g+2$, donde g es un elemento tal que $g^2 = g + 1$ y $2 + 1 = 0$.

i) El campo $K_1 = F(\sqrt{x^3 + x + g})$ es un campo cuadrático imaginario ramificado, pues el grado del radicando es impar. El polinomio $x^3 + x + g$ es irreducible en $\mathbb{F}_9[x]$.
ii) Consideremos la expresión $(2g+1)x^4 + (2g+2)x^3 + (g+2)x^2 + 2x + 2g + 2 = (2g+1)(x + 2g + 1)(x^3 + 2x + 1)$. Como $2g + 1$ no es un cuadrado en $\mathbb{F}_9$, entonces

$$K_2 = F(\sqrt{(2g+1)x^4 + (2g+2)x^3 + (g+2)x^2 + 2x + 2g + 2})$$

es un campo cuadrático imaginario inerte.
iii) En el anillo $\mathbb{F}_9[x]$ tenemos

$$2x^2 + 2gx + 2g + 1 = 2(x + 1)(x + g + 2),$$

así que $2x^2 + 2gx + 2g + 1$ es libre de cuadrados. En el campo $\mathbb{F}_q$ observamos que $(g+1)^2 = 2$, así que 2 es un cuadrado. Sea $K_3 = F(\sqrt{2x^2 + 2gx + 2g + 1}) = F(\sqrt{x^2 + gx + g + 2})$. Éste es un campo cuadrático real.

Al igual que en el caso de los campos de números, los campos cuadráticos imaginarios únicamente tienen un número finito de unidades, mientras que los campos cuadráticos reales poseen una infinidad de elementos de este tipo.

LEMA 3.20. *Sea $F = \mathbb{F}_q(x)$ y K un campo cuadrático sobre F. Un elemento $\mu \in \mathbb{O}_K$ es una unidad si y solamente si $N(\mu) \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.*

PROPOSICIÓN 3.21. *Sean $F = \mathbb{F}_q(x)$ y $K = F(\sqrt{d(x)})$ para algún $d(x) \in \mathbb{O}_F$ libre de cuadrados.*

i) *Si K es un campo cuadrático real, entonces existe una unidad $\mu \in \mathbb{O}_K$ tal que el grupo de unidades de $\mathbb{O}_K$ es $U(\mathbb{O}_K) = \{a\mu^m : a \in \mathbb{F}_q^*, m \in \mathbb{Z}\}$.*
ii) *Si K es un campo cuadrático imaginario, entonces $U(\mathbb{O}_K) = \mathbb{F}_q^*$.*

En el caso de los campos de funciones cuadráticos imaginarios, es fácil ver que un elemento es unidad si y solamente si es una constante distinta de cero. Si

$$\alpha = a(x) + b(x)\sqrt{d(x)},$$

entonces

$$N(\alpha) = a(x)^2 - d(x)b(x)^2.$$

Si $d(x)$ tiene grado impar, entonces el grado de $a(x)^2$ es par y el de $-d(x)b(x)^2$ es impar, por lo que el grado de la norma es igual al máximo de los dos grados anteriores. Si $b(x) \neq 0$, entonces $\deg(N(\alpha)) \geq 1$, por lo que $N(\alpha) = a(x)^2$. Ahora, si $a(x) \notin \mathbb{F}_q$, entonces el grado de $N(\alpha) \geq 2$. Finalmente, 0 claramente no tiene inverso. Por lo tanto, las únicas unidades de $\mathbb{O}_K$ son los elementos de $\mathbb{F}_q^*$.

Si $d(x)$ es par pero el coeficiente del término líder no es un cuadrado, sí es posible que $\deg(a(x)^2) = \deg(d(x)b(x)^2)$. Sin embargo, $\deg(N(\alpha)) = \max(\deg(a(x)^2), \deg(d(x)b(x)^2))$, ya que, si son iguales, los términos de grado mayor no se eliminan pues el de $a(x)^2$ es un cuadrado y el de $d(x)b(x)^2$ no lo es, así que son distintos y no se cancelan. A partir de aquí procedemos de forma similar al caso anterior.

El caso de los campos cuadráticos reales de funciones es similar a los campos cuadráticos reales en campos de números. La demostración es casi idéntica.

EJEMPLO 3.22. Retomemos los campos K_1, K_2 y K_3 del Ejemplo 3.19. Las unidades de K_1 y K_2 son los elementos distintos de cero de $\mathbb{F}_9$, así que, al igual que en el caso de los campos de números, un campo cuadrático imaginario tiene un número finito de unidades.

En K_3, $\mu = x+2g+\sqrt{x^2+gx+g+2}$ es una unidad, pues $N(\mu) = 2$. Su inverso es $\mu^{-1} = 2x+g+\sqrt{x^2+gx+g+2}$, que se obtiene multiplicando el conjugado de μ por el inverso de 2 en $\mathbb{F}_q$ que es el mismo 2. μ es la

unidad fundamental de K_3 y cualquier unidad de $\mathbb{O}_K$ se puede escribir como $a\mu^m$ para algún $a \in \mathbb{F}_q^*$ y algún $m \in \mathbb{Z}$. Esto, obviamente, implica que $\mathbb{F}_q^* \subseteq U(\mathbb{O}_K)$.

3.4. Grupo de clases de ideales

Existen dos grupos de clases que suelen definirse en los campos de funciones. El más usual en los libros es el grupo de clases de divisores. Nosotros no trataremos este tema, pero recomendamos los siguientes libros al lector interesado [**3**], [**49**], [**50**] . Por otro lado, se puede definir, de la misma forma que en campos de números, el grupo de clases de ideales. Sea F un campo de funciones racionales, K un campo de funciones y $\mathbb{O}_K$ su anillo de enteros. Diremos que dos ideales I, J distintos de cero están relacionados si existen $\alpha, \beta \in \mathbb{O}_K \setminus \{0\}$ tales que

$$\alpha I = \beta J.$$

Esta relación es de equivalencia y el conjunto de clases de equivalencia forma un grupo con el producto natural. A este grupo lo llamaremos el *grupo de clases de ideales* de K . En general, el grupo de clases de ideales de un campo de funciones no siempre es finito, pero si el campo de constantes es finito entonces:

TEOREMA 3.23. *Sea $F = \mathbb{F}_q(x)$ un campo de funciones racionales sobre un campo finito y K una extensión algebraica sobre F. El grupo de clases de ideales de K es finito y a su cardinalidad le llamaremos el número de clase de K.*

En particular, los campos cuadráticos que hemos estado trabajando a lo largo de este capítulo tienen grupo de clases de ideales finito.

El comportamiento del grupo de clases de ideales de un campo cuadrático de funciones es similar al de su análogo en campos de números. La clase neutra es la que contiene a todos los ideales principales, a la que denotaremos $\overline{\mathbb{O}_K}$, y el número de clase es 1 si y solamente si el anillo de enteros es de factorización única.

EJEMPLO 3.24. Sean $F = \mathbb{F}_7(x)$ y $K = F(\sqrt{x-1})$. El campo K es cuadrático imaginario ramificado ya que el grado de $x - 1$ es impar, entonces las unidades de $\mathbb{O}_K$ son los elementos de $\mathbb{F}_7^*$. En este caso, todos los ideales están relacionados, así que el número de clase es 1. Al igual que en el caso de los campos de números, esto significa que el anillo $\mathbb{O}_K$ es un dominio de ideales principales y por lo tanto un dominio de factorización única.

En la siguiente sección estudiaremos un ejemplo en el que incluiremos todos los conceptos vistos en este capítulo, ahí veremos un caso en

donde el grupo de clases de ideales no es trivial. Cuando esto sucede, el anillo de enteros no es un dominio de factorización única.

3.5. Un ejemplo

A continuación usaremos lo que hemos estudiado en las secciones anteriores para factorizar un elemento de un campo de funciones cuadrático. A partir de ahora trabajaremos con $F = \mathbb{F}_5(x)$, $K = F(\sqrt{x^3+3x^2+2x})$. Observemos que $x^3+3x^2+2x = x(x+1)(x+2)$. Con la información que tenemos sabemos que K es un campo cuadrático imaginario ramificado, así que las únicas unidades de $\mathbb{O}_K$ son 1, 2, 3 y 4. Hay tres ideales ramificados ya que $d(x) = x^3+3x^2+2x$ tiene tres factores:

$$\begin{aligned}\langle x\rangle &= \langle x, \sqrt{x^3+3x^2+2x}\rangle^2,\\ \langle x+1\rangle &= \langle x+1, \sqrt{x^3+3x^2+2x}\rangle^2,\\ \langle x+2\rangle &= \langle x+2, \sqrt{x^3+3x^2+2x}\rangle^2.\end{aligned}$$

Llamemos $I_1 = \langle x, \sqrt{x^3+3x^2+2x}\rangle$, $I_2 = \langle x+1, \sqrt{x^3+3x^2+2x}\rangle$ y finalmente $I_3 = \langle x+2, \sqrt{x^3+3x^2+2x}\rangle$. Para probar que estos ideales no son principales, hay que usar la Proposición 3.13. Las normas de los ideales son:

$$N(I_1) = x, \quad N(I_2) = x+1, \quad N(I_3) = x+2.$$

Para que I_1 sea principal, debe existir un elemento con norma ax para algún $a \in \mathbb{F}_5^*$. Digamos

$$\alpha = a(x) + b(x)\sqrt{x^3+3x^2+2x}$$

con

$$N(\alpha) = a(x)^2 - b(x)^2(x^3+3x^2+2x) = x.$$

Debido a que el grado de $a(x)^2$ es par y el grado de $-b(x)^2(x^3+3x^2+2x)$ es impar, entonces los grados son distintos y tenemos

$$1 = \deg(N(\alpha)) = \max(\deg(a(x)^2), \deg(-b(x)^2(x^3+3x^2+2x))).$$

Si $b(x)$ es distinto de cero, entonces el grado de $-b(x)^2(x^3+3x^2+2x)$ es mayor o igual a 3, por lo que $b(x) = 0$ y $N(\alpha) = (a(x))^2 = x$, pero esto tampoco es posible pues $(a(x))^2$ tiene grado par y x tiene grado 1. Por lo tanto, no existe ningún elemento con norma x. Análogamente, no existe ningún elemento con norma $2x$, $3x$ ó $4x$, lo que implica que el ideal $I_1 = \langle x, \sqrt{x^3+3x^2+2}\rangle$ no es un ideal principal. De la misma forma podemos ver que los ideales I_2, I_3 tampoco son principales.

Hemos encontrado tres ideales no principales, ahora falta ver si los tres están en la misma clase o si hay más de una clase con ideales no principales. Como $I_1^2 = \langle x\rangle$, $I_2^2 = \langle x+1\rangle$ e $I_3^2 = \langle x+2\rangle$, entonces las clases $\overline{I_1}$, $\overline{I_2}$, $\overline{I_3}$ tienen orden 2 en el grupo de clases de ideales, ya

que cada ideal al cuadrado es principal. Lo anterior significa que el inverso de la clase $\overline{I_1}$ es la misma clase $\overline{I_1}$, así que si $\overline{I_1} = \overline{I_2}$, entonces $\overline{I_1}^2 = \overline{I_1 I_2} = \overline{\mathbb{O}_K}$.

Consideremos los ideales I_1, I_2. Si $I_1 I_2$ es un ideal principal, entonces debe de existir un elemento con norma $ax(x+1)$ para algún $a \in \mathbb{F}_5^*$. Igual que antes, si $I_1 I_2 = \langle \alpha \rangle$ con $\alpha = a(x) + b(x)\sqrt{x^3+3x^2+2x}$, entonces $b(x) = 0$, $a(x)^2 = ax(x+1)$ lo que no es posible pues $ax(x+1)$ no es un cuadrado. Por lo tanto $\overline{I_1} \neq \overline{I_2}$. De la misma forma se puede demostrar que $\overline{I_1} \neq \overline{I_3}$ y que $\overline{I_2} \neq \overline{I_3}$. Así, tenemos al menos cuatro clases, las tres anteriores y $\overline{\mathbb{O}_K}$.

Por otra parte, $N(\sqrt{x^3+3x^2+2x}) = -(x^3+3x^2+2x)$. Además, únicamente existe un ideal con norma x^3+3x^2+2x, este es $I_1 I_2 I_3$, de donde

$$\overline{I_1 I_2 I_3} = \overline{\mathbb{O}_K}.$$

Como el orden de $\overline{I_1}$, $\overline{I_2}$ y $\overline{I_3}$ es 2, lo anterior nos indica que $\overline{I_1} = \overline{I_2 I_3}$, $\overline{I_2} = \overline{I_1 I_3}$ y finalmente $\overline{I_3} = \overline{I_1 I_2}$.

De esta información, tenemos que el grupo de clases de ideales contiene un subgrupo isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$.

Ahora consideremos el polinomio irreducible $x+3$. Los cuadrados módulo $x+3$ son $0, 1, 4$ y

$$x^3+3x^2+2x = (x^2+2)(x+3)+4 \equiv 4 = 2^2 \pmod{x+3}.$$

Así que

$$\langle x+3 \rangle = \langle x+3, 2+\sqrt{x^3+3x^2+2x} \rangle \langle x+3, 2-\sqrt{x^3+3x^2+2x} \rangle.$$

Ninguno de los dos ideales del lado derecho de la igualdad es principal, pues, igual que con $x, x+1, x+2$, no existe ningún elemento con norma $a(x+3)$ con $a \in \mathbb{F}_5^*$. Concentrémonos en $I = \langle x+3, 2+\sqrt{x^3+3x^2+2x} \rangle$, denotando al otro ideal de la factorización como I'. Los únicos elementos con norma $a(x+3)^2$ para algún $a \in \mathbb{F}_5^*$ son

$$N(x+3) = N(4x+2) = (x+3)^2 \quad \text{y} \quad N(2x+1) = N(3x+4) = 4(x+3)^2.$$

Ninguno de estos genera a I^2 pues sabemos que todos generan a $II' = \langle x+3 \rangle$, que es un ideal distinto ya que se factoriza de forma distinta. Tampoco existen elementos con norma $a(x+3)^3$. Sin embargo, existen varios elementos con norma $(x+3)^4$. Estos son:

$$(x+3)^2, \quad x^2+3x+1+2\sqrt{x^3+3x^2+2x}, \quad x^2+3x+1+3\sqrt{x^3+3x^2+2x},$$

y los tres anteriores multiplicados por 4. Vamos a verificar que

$$\gamma = x^2+3x+1+3\sqrt{x^3+3x^2+2x}$$

es el generador de I^4.

Sea $J = \langle \alpha, \beta \rangle$ un ideal con dos generadores. La potencia cuarta de J es:

$$J^4 = \langle \alpha^4, \alpha^3\beta, \alpha^2\beta^2, \alpha\beta^3, \beta^4 \rangle.$$

Para que γ sea el generador de J^4, es necesario que γ divida a cada uno de los cinco generadores de J^4 que aparecieron en la expresión de arriba y que además γ genere al ideal, esto último se cumple si tenemos la primera condición y además tenemos que $N(\gamma) = aN(J^4)$ para algún $a \in \mathbb{F}_5^*$. Para saber si γ divide a un elemento, digamos β^4, tenemos que racionalizar la división:

$$\frac{\beta^4}{\gamma} = \frac{\beta^4\gamma'}{\gamma\gamma'} = \frac{\beta^4\gamma'}{N(\gamma)} = \frac{\beta^4\gamma'}{(x+3)^4}.$$

De esta forma, en el numerador tenemos un elemento de $\mathbb{O}_K$, digamos $a(x) + b(x)\sqrt{x^3+3x^2+2x}$, y en el denominador un elemento de $\mathbb{O}_F$, digamos $c(x)$. Si se tiene la situación anterior, el resultado va a estar en $\mathbb{O}_K$ si y solamente si

$$\frac{a(x)}{c(x)} \in \mathbb{O}_F \quad \text{y} \quad \frac{b(x)}{c(x)} \in \mathbb{O}_F.$$

Así, la división de elementos de $\mathbb{O}_K$ se puede reducir a dos divisiones de polinomios, lo que es más sencillo, ya que podemos usar los métodos usuales para conseguir esto, como la división larga o la división sintética cuando es posible.

Vamos a verificar que γ genera a I^4. A continuación $\beta = 2 + \sqrt{x^3+3x^2+2x}$:

$$\begin{aligned}
(x+3)^4 &= \gamma(x^2+3x+1+2\sqrt{x^3+3x^2+2x})^4,\\
(x+3)^3\beta &= \gamma(2x^2+2x+4+x\sqrt{x^3+3x^2+2x}),\\
(x+3)^2\beta^2 &= \gamma(x^3+x+1+(2x+3)\sqrt{x^3+3x^2+2x}),\\
(x+3)\beta^3 &= \gamma(2x^3+3x+4+(x^2+2x+4)\sqrt{x^3+3x^2+2x}),\\
\beta^4 &= \gamma(x^4+2x^3+x+1+(2x^2+x+4)\sqrt{x^3+3x^2+2x}).
\end{aligned}$$

Por lo anterior, γ divide a cada uno de los generadores de I^4 y

$$N(\gamma) = (x+3)^4 = N(I^4).$$

Entonces,

$$\langle x+3, 2+\sqrt{x^3+3x^2+2x}\rangle^4 = \langle x^2+3x+1+3\sqrt{x^3+3x^2+2x}\rangle.$$

De esta forma, la clase $\overline{I}$ del grupo de clases de ideales tiene orden 4, ya que I, I^2, I^3 no son principales pero I^4 sí lo es. Análogamente se puede verificar que el orden de la clase $\overline{I'}$ es 4. Pero II' es principal, así que

$$\overline{I}^{-1} = \overline{I}^3 = \overline{I'}.$$

Observemos que

$$\overline{I}^2 = \overline{I}^2\overline{y} = \overline{I}^6 = \left(\overline{I}^3\right)^2 = \overline{I'}^2.$$

Además, existen elementos con norma $(x+3)^2(x+1)$, estos son:

$$2x+2+2\sqrt{x^3+3x^2+2x}, \quad 2x+2+3\sqrt{x^3+3x^2+2x},$$
$$2x+3+2\sqrt{x^3+3x^2+2x}, \quad 2x+3+3\sqrt{x^3+3x^2+2x}.$$

Como solamente hay un ideal con norma $x+1$, al que habíamos llamado I_2, y dos ideales con norma $x+3$, I e I', entonces al menos uno de los ideales I_2I^2, $I_2I'^2$ ó I_2II' es principal. $I_2II' = I_2\langle y\rangle$, y como I_2 no es un ideal principal, entonces este queda descartado. Por otro lado, $\overline{I_2I^2} = \overline{I_2I'^2}$, así que ambos son principales y tenemos que

$$\overline{I_2} = \overline{I^2} = \overline{I'^2}.$$

Así que ahora podemos decir que el grupo de clases de ideales contiene a un grupo isomorfo al grupo $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$. Notemos que $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ tiene ocho elementos:

$$(0,0), \quad (0,1), \quad (0,2), \quad (0,3),$$
$$(1,0), \quad (1,1), \quad (1,2), \quad (1,3).$$

Tres de éstos tienen orden 2: $(0,2)$, $(1,0)$ y $(1,2)$, donde el tercero es la suma de los dos primeros. Hay cuatro elementos con orden 4: $(0,1)$, $(0,3)$, $(1,1)$ y $(1,3)$. Si conocemos uno de estos cuatro, los otros tres se pueden obtener sumándole los tres elementos de orden 2, así:

$$(0,1)+(0,2) = (0,3),$$
$$(0,1)+(1,0) = (1,1),$$
$$(0,1)+(1,2) = (1,3).$$

También es importante notar que $2(0,1) = 2(0,3) = 2(1,1) = 2(1,3) = (0,2)$. Usaremos esta información para analizar el grupo de clases de ideales de K.

Siguiendo un argumento análogo al que usamos con $x+3$, podemos concluir que $x+4$ se descompone y que si J, J' son los dos ideales con norma $x+4$, entonces $J, J^2, J^3, J', J'^2, J'^3$ no son ideales principales, pero J^4 y J'^4 sí lo son. Igual que con I,

$$\overline{J}^2 = \overline{J'}^2 = \overline{I_2}.$$

De esta forma, $\overline{I_2}$ es el elemento que corresponde a $(0,2)$ en $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$. Es fácil verificar que no existe ningún elemento con norma $a(x+3)(x+4)$, por lo que los ideales I, I', J y J' pertenecen a clases de ideales distintas y todas sus clases tienen orden 4. Además, se puede ver que $\overline{I} \times \overline{I_2} = \overline{I}^3 = \overline{I'}$, y realizando un análisis similar a lo hecho anteriormente llegamos a que $\overline{I} \times \overline{I_1} = \overline{J}$ y $\overline{I} \times \overline{I_3} = \overline{J'}$. Así que I, I', J y J' son las clases de orden 4.

Hasta este momento hemos demostrado que el grupo de clases de ideales contiene un subgrupo isomorfo a $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$, de hecho, el grupo de clases de ideales es isomorfo a este grupo, así que el número de clase es 8. Demostrar que no hay más clases de ideales es algo que queda fuera de los objetivos de este trabajo.

En la siguiente sección vamos a usar el grupo de clases que acabamos de encontrar para trabajar con elementos de $\mathbb{O}_K$ que tienen distintas factorizaciones.

3.6. Distintas factorizaciones de un elemento

Seguiremos trabajando en los campos

$$F = \mathbb{F}_5(x) \quad \text{y} \qquad K = F(\sqrt{x^3 + 3x^2 + 2x}).$$

A partir de ahora usaremos $y = \sqrt{x^3 + 3x^2 + 2x}$.

Para saber si un ideal I es principal, primero debemos de factorizarlo como producto de ideales primos, para conseguirlo, debemos de factorizar la norma y usar la factorización como guía para saber cuáles son los posibles ideales primos que dividen a I.

PROPOSICIÓN 3.25. *Sean $\mathbb{F}_q(x)$ un campo de funciones racionales, K un campo de funciones sobre F, $\mathbb{O}_K$ el anillo de enteros de K. Si I, J son dos ideales de $\mathbb{O}_K$, entonces $I \mid J$ si y sólo si $I \supseteq J$.*

Una vez que factorizamos al ideal como producto de ideales primos, digamos $I = P_1 P_2 \cdots P_t$, tomamos el conjunto de índices $A = \{1, 2, \ldots, t\}$. Para denotar una partición de A usaremos $\{A_1|A_2|\ldots|A_r\}$, donde los conjuntos A_i, con $i =, 1, 2, \ldots, r$, son las clases de la partición. Diremos que $\{A_1|A_2|\ldots|A_r\}$ es una partición principal de A si para cada A_i, con $i = 1, 2, \ldots, r$, se tiene que el producto de los elementos de A_i es principal, esto es

$$\prod_{j \in A_i} P_j = \langle \gamma_i \rangle$$

para algún $\gamma_i \in \mathbb{O}_K$. Si cada uno de los elementos γ_i de una partición principal es generado por un elemento irreducible, entonces la partición nos da una factorización como producto de irreducibles de γ:

$$\gamma = \gamma_1 \gamma_2 \cdots \gamma_r \mu,$$

donde μ es una unidad de $\mathbb{O}_K$.

PROPOSICIÓN 3.26. *Sean $\mathbb{F}_q(x)$ un campo de funciones racionales, K un campo de funciones sobre F, $\mathbb{O}_K$ el anillo de enteros de K. Sea $\gamma \in \mathbb{O}_K$ y $\langle \gamma \rangle = P_1 P_2 \cdots P_t$ la factorización de este ideal como producto de ideales primos. Entonces, γ es irreducible si y solamente si la única partición principal de $A = \{1, 2, \ldots, t\}$ es la que tiene una única clase.*

En nuestro ejemplo encontraremos todas las posibles factorizaciones distintas de

$$\alpha = x^3 + 2x^2 + 4 = (x+1)(x+3)^2.$$

En este caso $\alpha \in \mathbb{O}_F$ y tenemos su factorización en $\mathbb{O}_F$, así que es fácil dar la factorización del ideal $\langle \alpha \rangle$ en $\mathbb{O}_K$:

$$\langle \alpha \rangle = \langle x+1, y \rangle^2 \langle x+3, 2+y \rangle^2 \langle x+3, 2-y \rangle^2.$$

Ya tenemos una factorización, $(x+1)(x+3)^2$.

Vamos a demostrar que el polinomio $x+1$ es irreducible en $\mathbb{O}_K$. Sabemos que $\langle x+1 \rangle = \langle x+1, y \rangle^2$, entonces $A = \{1,2\}$ y sus particiones son $\{1|2\}$ y $\{1,2\}$. La partición $\{1|2\}$ no es principal pues el ideal $\langle x+1, y \rangle$ no es principal, así $x+1$ es irreducible. De la misma forma, usando $\langle x+3 \rangle = \langle x+3, 2+y \rangle \langle x+3, 2-y \rangle$ llegamos a que la única partición irreducible del conjunto de índices es $\{1,2\}$. Así que la factorización que conocemos de α en $\mathbb{O}_F$ es una factorización en irreducibles en $\mathbb{O}_K$. Sin embargo, no es la única.

Recordemos que el grupo de clases de ideales es isomorfo a $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$, donde el ideal $\langle x+1, y \rangle$ está en la clase correspondiente a $(0,2)$ y los ideales $\langle x+3, 2+y \rangle$ y $\langle x+3, 2-y \rangle$ están en clases de orden cuatro con

$$\overline{\langle x+3, 2+y \rangle} = \overline{\langle x+3, 2-y \rangle}^{-1},$$

digamos $(0,1)$ y $(0,3)$ vistos como clases de $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ (otra posibilidad válida hubiera sido $(1,1)$ y $(1,3)$). Así que en el grupo de clases de ideales, esta factorización es

$$(0,2) + (0,2) + (0,1) + (0,1) + (0,3) + (0,3).$$

Ordenemos la factorización de $\langle \alpha \rangle$ como

$$P_1 = P_2 = \langle x+1, y \rangle, \quad P_3 = P_4 = \langle x+3, 2+y \rangle, \quad P_5, P_6 \langle x+3, 2-y \rangle,$$

con conjunto de índices $A = \{1,2,3,4,5,6\}$. Las particiones principales de A con elementos irreducibles son:

$$\{1,2|3,5|4,6\},$$
$$\{1,2|3,6|4,5\},$$
$$\{1,3,4|2,5,6\},$$
$$\{1,5,6|2,3,4\}.$$

Cualquier otra partición de A no es principal o incluye algún elemento que no es irreducible. Por ejemplo, la partición $\{1,2,3,4,5,6\}$ es principal, pero la factorización que obtenemos es y, que no es un producto de elementos irreducibles. En la primera partición obtenemos la factorización, $(P_1P_2)(P_3P_5)(P_4P_6)$, P_1P_2 es principal pues corresponden a $(0,2) + (0,2) = (0,0)$ en $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$. P_3P_5 y P_4P_6 corresponden a $(0,1) + (0,3) = (0,0)$ en $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$, así que son principales.

Para demostrar que son irreducibles usamos el mismo método con el que probamos que $x+1$ es irreducible. La segunda partición produce la misma factorización que la primera pues $P_3 = P_4$ y $P_5 = P_6$. En la tercera partición, el primer factor es de la forma $(2,0)+(1,0)+(1,0) = (4,0) = (0,0)$ en $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ y el segundo es de la forma $(2,0)+(3,0)+(3,0) = (8,0) = (0,0)$, por lo que los dos productos de ideales que surgen son principales. De nuevo, la cuarta partición genera la misma factorización que la tercera. Así que básicamente hay dos factorizaciones distintas:

$$\langle \alpha \rangle = (P_1P_2)(P_3P_5)(P_4P_6) = (P_1P_3P_4)(P_2P_5P_6).$$

Únicamente falta encontrar los generadores de los ideales. En el caso de la primera factorización ya sabemos que $P_1P_2 = \langle x+1 \rangle$ y $P_3P_5 = P_4P_6 = \langle x+3 \rangle$. Para encontrar los generadores de $P_1P_3P_4$ y $P_2P_5P_6$ hay que buscar elementos cuya norma sea igual a $N(P_1P_3P_4) = N(P_2P_5P_6) = (x+1)(x+3)^2 = x^3 + 2x^2 + 4$ o bien a este polinomio multiplicado por una constante. Recordemos que la norma de $a(x) + b(x)y$ es

$$N(a(x) + b(x)y) = a(x)^2 - b(x)^2(x^3 + 3x^2 + 2x),$$

si queremos que sea $x^3 + 2x^2 + 4$, entonces $b(x)$ tiene que estar en $\mathbb{F}_5^*$ y $a(x)$ debe tener grado menor o igual a 1, de lo contrario, el grado de la norma es distinto de 3. Probando todas las posibilidades encontramos que los elementos con norma $x^3 + 2x^2 + 4$ son:

$$\begin{aligned} &2x + 2 + 2\sqrt{x^3 + 3x^2 + 2x}, \\ &2x + 2 + 3\sqrt{x^3 + 3x^2 + 2x}, \\ &3x + 3 + 2\sqrt{x^3 + 3x^2 + 2x}, \\ &3x + 3 + 3\sqrt{x^3 + 3x^2 + 2x}. \end{aligned}$$

Los elementos con norma $4(x^3+2x^2+4)$ son estos mismos multiplicados por 3 y no existen elementos con norma $a(x^3 + 2x^2 + 4)$ para $a = 2, 3$. Alguno de estos elementos debe generar a $P_1P_3P_4$ y algún otro a $P_2P_5P_6$. Probamos todas las posibilidades hasta encontrar

$$x^3 + 2x^2 + 4 = (2x + 2 + 2\sqrt{x^3 + 3x^2 + 2x})(2x + 2 + 3\sqrt{x^3 + 3x^2 + 2x}).$$

Por lo tanto, las dos factorizaciones en irreducibles distintas de $x^3 + 2x^2 + 4$ en $\mathbb{O}_K$ son la anterior y $(x+1)(x+3)^2$. Con esto concluimos nuestro ejemplo.

Bibliografía

[1] Adams W. W., and Goldstein L. J., *Introduction to Number Theory*. Prentice-Hall 1976.

[2] Andrews G. E., *Number Theory*. Dover 1994.

[3] Deuring M., *Lectures on the Theory of Algebraic Function of One Variable*. LNM 314, Springer-Verlag, 1973.

[4] Ellison W.J., Ellison J.P. *et al.* The diophantine equation $y^2 + k = x^3$. J. Number Theory **4** (1972), 107-117.

[5] Enzenberger H. M., *El diablo de los Números*. Siruela 1998.

[6] Finkelstein R., London H., On Mordell's equation $y^2 - k = x^3$: an interesting case of Sierpinski. J. Number Theory **2**, 310-321 (1970).

[7] Flannery D., *The square root of 2: a dialogue concerning a number and a sequence*. Copernicus-Springer-Verlag, 2006.

[8] Gallian J. A. and Winters S., Modular Arithmetic in the Marketplace. American Mathematical Montly, **95** No. 6, 548-551 (1988).

[9] Gardner M., On Expressing Integers as the Sums of Cubes and Other Unsolved Number-Theory Problems. Scientific American, **229**, 118-121 (1973).

[10] Gauss K. F., *Disquisitiones Arithmeticae*. Traducción del latín al español por Hugo Barrantes Campos, Michael Josephy y Ángel Ruiz Zúñiga. Colección *Enrique Pérez Arbelaéz*, **10**, Academia Colombiana de Ciencias Exactas, Físicas y Naturales, Bogotá, 1995.

[11] Granville A. It is easy to determine whether a given integer is prime. American Mathemathical Montly, **42**, 3-38 (2005).

[12] Guy Richard K. *Unsolved Problems in Number Theory*. Problem Books in Mathematics. Springer, New York 2004.

[13] Hardy G.H., Wright E.M. *An introduction to the theory of numbers*. Oxford University Press, Oxford 1979.

[14] Hoffman P., *Archimedes' revenge*. Norton, New York, 1988.

[15] Ireland K., M. Rosen., *A classical introduction to modern number theory*. GTM **84** Springer Verlag 1982.

[16] Ivorra Castillo C., *Teoría de Números*. Publicación electrónica `http://www.uv.es/ivorra/`.

[17] Jones J.P., *et al.* Diophantine representation of the set of prime numbers. American Mathematical Montly, **83**, No. 6, 449-464 (1976).

[18] LeVeque William J., *Fundamentals of Number Theory*. Dover 1996.

[19] McCarty, Paul J., *Algebraic extensions of fields*. Dover Books 1991.

[20] Nair M.A., A note on the equation $x^2 - y^3 = k$. Quart. J. Math. Oxford (2) **29**, 483-487 (1978).

[21] Nahin P.J., *An imaginary tale: The story of* $\sqrt{-1}$. Princeton University Press, Princeton, NJ, 1998.

[22] Narkiewicz, W., *Elementary and analitic theory of algebraic numbers*. Third edition. Springer-Verlag 2004.

[23] Niven I., Zuckerman S., Montgomery H.L., *An Introduction to the Theory of Numbers*. 5th ed., John Wiley, New York, 1991.
[24] Ore O., *Number Theory and its history*. Reimpresión de la versión original de 1948. Dover 1988, New York.
[25] Pineda-Ruelas. M., *Enteros, cuadrados, Gaussianos y teoría de grupos finitos*. 2013. Por aparecer.
[26] Pomerance C., Very Short Primality Proofs. Mathematics of Computation **48**, no. 177, 315-322 (1987).
[27] Proyecto GIMPS (Great Internet Mersenne Prime Search). `http://www.mersenne.org/prime.htm`
[28] Quine, W.J., Fermat's Last Theorem in combinatorial form. American Mathematical Montly, **95**, No. 7, 305-319 (1988).
[29] Ribenboim P., *Algebraic Numbers*, Wiley, New York 1972
[30] Ribenboim P., El famoso polinomio generador de primos de Euler y el número de clase de los cuerpos cuadráticos imaginarios. Revista Colombiana de Matemáticas, vol. **21**, 263-284 (1987).
[31] Ribenboim P., *Números primos: mistérios e recordes*. Coleção Matemática Universitaria, Rio de Janeiro: IMPA 2001.
[32] Ribenboim P., *The new book of prime number records*. Springer Verlag, New York (1996).
[33] Ribenboim P., *Classical Theory of Algebraic Numbers*. Universitext, Springer, New York (2001).
[34] Rivest R., Shamir A., Adleman L., A method for obtain digital signatures and public-key cryptosystems. Comm. of the ACM, **21**, 120-126 (1978).
[35] Rosen K.H., *Elementary Number Theory and its Applications*. Third ed., Addison Wesley, Paris 1993.
[36] Shanks D., *Solved and Unsolved Problems in Number Theory*. Chelsea, New York, 2002.
[37] Sierpiński W., *Elementary theory of numbers*. North-Holland, Amsterdan 1988.
[38] Silverman J. H., *A friendly Introduction to number theory*. Prentice-Hall, 3 edition, New Jersey 2005.
[39] Schroeder M.R., *Number Theory in Science and Communication: With applications in cryptography, physics, digital information, computing, and self-similarity*. Springer Series in Information Sciences, 7. Fourth edition. Springer Verlag, Berlin 2006.
[40] Stewart I., *De aquí al infinito; Las matemáticas de hoy*. Crítica, Barcelona 2004.
[41] Stewart I., Tall D., *Algebraic Number Theory and Fermat Last Theorem*. A K Peters, third edition, 2002.
[42] Stillwell J., *Elements of Number Theory*, Undergraduate Texts in Mathematics, Springer Verlag, New York 2003.
[43] Sylvester J.J., El estudio que no sabe nada de la observación. Colección Sigma. El Mundo de las Matemáticas, Vol. 5 Grijabo, España 1968.
[44] The Prime Pages. http://primes.utm.edu/
[45] Thompson J., A method for finding primes. American Mathematical Monthly, **60**, No. 3, 175 (1953).
[46] Uspensky J.V., A method for finding units in cubic orders of a negative discriminat, Trans. Amer. Math. Soc., **33**, 1-22 (1931).
[47] Uspensky J.V., *Teoría de ecuaciones*. Limusa, 2002.
[48] Vardi I., Archimedes' Cattle Problem. American Mathematical Montly, **105**, No. 4, 305-319 (1998).
[49] Villa-Salvador G.D., *Introducción a la teoría de las funciones algebraicas*, Fondo de Cultura Económica, 2002.

[50] Villa-Salvador D.G., *Topics in the Theory of Algebraic Function Fields*, Birkhauser, 2006.
[51] Wagon S., The evidence: primality testing. Math. Intellingencer **8**, no.3, 58-61 (1986).
[52] Weil A., *Two lectures on number theory, past and present*, Enseignement Math. **20**, 87-110 (1974).
[53] Weil A., *Number theory: An approach through history from Hummurapi to Legendre*, Birkhäuser, Boston, 1984.
[54] Weyl H., El modo matemático de pensar. Colección Sigma. El Mundo de las Matemáticas, Vol. 5 Grijabo, España 1968.
[55] Williams H.C., Holte R., Computation of the solutions of $x^3 + dy^3 = 1$. Math. Comp. **31** no. 139, 778-785 (1977).
[56] Williams Kenneth S., Note on Non-Euclidean Principal Ideal Domains. Mathematics Magazine, **48**, No. 3, 176-177 (1975).