Universidad
de La Laguna

Introducción a la teoría algebraica de números

Introduction to algebraic number theory

Luis José Santana Sánchez

Trabajo de Fin de Grado

Álgebra

Sección de Matemáticas

Facultad de Ciencias

Universidad de La Laguna

La Laguna, 17 de junio de 2015

Dr. Dña. **María Victoria Reyes Sánchez**, con N.I.F. 42.040.774-V profesora titular de Álgebra adscrita al Departamento de Matemáticas, Estadística e Investigación Operativa de la Universidad de La Laguna

C E R T I F I C A

Que la presente memoria titulada:

"*Introducción a la teoría algebraica de números.*"

ha sido realizada bajo su dirección por D. **Luis José Santana Sánchez**, con N.I.F. 54.133.393-H.

Y para que así conste, en cumplimiento de la legislación vigente y a los efectos oportunos firma la presente en La Laguna a 17 de junio de 2015

Agradecimientos

A Mª Victoria Reyes Sánchez,
por su dedicación, apoyo y consejos,
no solo en la elaboración de esta memoria,
sino en el transcurso de mi paso por la universidad.

A mi familia y amigos.

Resumen

El objetivo de esta memoria es el estudio de los anillos de enteros cuadráticos, la existencia de factorización única de ideales en estos anillos y el cálculo del grupo de clases para la determinación de anillos de enteros cuadráticos con factorización única de elementos.

En primera instancia se definen los anillos de enteros cuadráticos, se estudian sus elementos notables y se prueba la existencia de factorización aunque no siempre única. Posteriormente, consideramos ideales en lugar de elementos y se prueba que existe factorización única de ideales en lo que se denominan dominios de Dedekind. Finalmente, se determina el grupo de clases como un grupo cociente de ideales fraccionarios y se computa un algoritmo para el cálculo de estos grupos en el caso de cuerpos cuadráticos.

Palabras clave: Dominio de factorización única, Enteros cuadráticos, Dominios de Dedekind, Grupo de clases.

Abstract

This essay aims at the studying of quadratic integer rings, the unique factorization of ideals and the calculation of the ideal class group to determinate whether or not a quadratic integer rings is a unique factorization domain.

We first define quadratic integer rings, we study its main elements and we show the existence of factorization although it is not always unique. Following, we replace elements by ideals and we show there is unique factorization of ideals in Dedekind domains. Finally, we define the ideal class group as a quotient group of fractional ideals and we describe an algorithm to find the ideal class group of quadratic fields.

Keywords: *Unique factorization domain, Quadratic integers, Dedekind domains, Ideal calss group.*

Índice general

Introducción

La teoría de números que se conoce hoy en día nace en la antigua Grecia de la mano del que muchos consideran el padre del álgebra, Diofanto de Alejandría. En su obra *Arithmetica*, Diofanto reúne una colección de problemas sobre la existencia de soluciones enteras para las que, en su honor, se denominan ecuaciones diofánticas.

Es en el margen de una página del libro II de esta obra, donde el matemático Pierre de Fermat enuncia su famoso último teorema que afirma que dado n natural mayor que 2, no existen enteros positivos x, y, z, que cumplan la igualdad

$$x^n + y^n = z^n.$$

Aunque no es hasta 1995 cuando Andrew Wiles demuestra este teorema, otros matemáticos se embarcan con éxito en la prueba para valores determinados de n. Gauss mismo usa los enteros de Eisenstein y demuestra el teorema para $n = 3$.

En esta memoria de introducción a la teoría algebraica de números se estudian los anillos de enteros cuadráticos, que surgen como una generalización del anillo de enteros $\mathbb{Z}$. El anillo formado por los enteros de Eisenstein es un ejemplo de este tipo de anillos, los cuales son de gran utilidad a la hora de resolver ecuaciones diofánticas.

Fermat, por ejemplo, enuncia y demuestra que las únicas soluciones enteras de la ecuación $y^2 + 2 = x^3$ son exactamente $y = \pm 5$, $x = 3$. Para ello, utiliza el anillo de enteros cuadráticos $\mathbb{Z}[\sqrt{-2}]$.

Tanto la prueba realizada por Gauss como la realizada por Fermat se sustentan en la existencia de factorización única de elementos en los anillos que utilizaron. Sin embargo, no es cierto que todos los anillos de enteros cuadráticos sean dominio de factorización única y es ésta una de las principales diferencias que presentan respecto al anillo $\mathbb{Z}$.

Para resolver el problema de la factorización única, Dedekind sugiere considerar ideales en lugar de elementos y demuestra la existencia de factorización única de ideales como producto de ideales primos.

Finalmente, a través de los ideales se define el grupo de clases de ideales, que proporciona una caracterización de los anillos de enteros cuadráticos con factorización única de elementos.

Esta memoria se divide en tres capítulos. En el primer capítulo se definen los anillos de enteros cuadráticos, se estudian sus elementos notables y se prueba que existe factorización aunque no necesariamente única; además se observan algunas propiedades de sus ideales. En el segundo capítulo se introducen los dominios de Dedekind como la versión global de los dominios de valoración discreta y se demuestra que los ideales se descomponen de forma única como producto de ideales primos. En el tercer y último capítulo se definen los ideales fraccionarios, se prueba que forman un grupo multiplicativo en los dominios de Dedekind y se define el grupo de clases de ideales como un grupo cociente de ideales fraccionarios; se observa que en los cuerpos cuadráticos el grupo de clases de ideales es siempre finito y se obtiene un algoritmo para su cálculo.

En cada uno de los capítulos se ha incluído ejemplos de los resultados probados para una mejor comprensión de los mismos.

Capítulo 1

Anillos de enteros de cuerpos cuadráticos

Este primer capítulo está dedicado a introducir los anillos de enteros cuadráticos, formados por elementos de una extensión de $\mathbb{Q}$ de grado dos cuyo polinomio mínimo tiene coeficientes enteros. Se determina por completo cuáles son sus elementos y se comprueba que existe factorización de elementos aunque no única. Además, se estudian propiedades de los ideales de estos anillos que se usarán en capítulos posteriores.

1.1. Cuerpos cuadráticos

Todo subcuerpo K de los números complejos $\mathbb{C}$, por ser cuerpo, contiene a $1_{\mathbb{C}}$, luego debe contener tanto al anillo de los enteros $\mathbb{Z}$ como a su cuerpo de fracciones $\mathbb{Q}$. Esto quiere decir que podemos ver K como un $\mathbb{Q}-$espacio vectorial y podemos definir los cuerpos cuadráticos como sigue.

Definición 1.1.1. Se dice que K subcuerpo de $\mathbb{C}$ es un *cuerpo cuadrático* si es un $\mathbb{Q}-$espacio vectorial de dimensión 2.

En particular, si tomamos $\alpha \in K \setminus \mathbb{Q}$, se tiene que $\{1, \alpha\}$ es una $\mathbb{Q}$-base de K y por lo tanto si $z \in K$, existen $x, y \in \mathbb{Q}$ tales que $z = x + y\alpha$.

Denotando $\mathbb{Q}[\alpha] = \{\, g(\alpha) \in \mathbb{C} : g(X) \in \mathbb{Q}[X]\}$ es inmediato ver que $K = \mathbb{Q}[\alpha]$. Consecuentemente, $\mathbb{Q}[\alpha]$ es un cuerpo y coincide con su cuerpo de fracciones que denotamos por $\mathbb{Q}(\alpha)$. En concreto, se tiene el siguiente resultado.

Proposición 1.1.1. *Todos los cuerpos cuadráticos son de la forma*

$$\mathbb{Q}(\sqrt{m}) = \mathbb{Q}[\sqrt{m}] = \left\{x + y\sqrt{m} : x, y \in \mathbb{Q}\right\},$$

con $m \in \mathbb{Z}$ libre de cuadrados. Más aún, todos ellos son no isomorfos dos a dos.

Demostración.

Sea $m \in \mathbb{Z}$ libre de cuadrados. El polinomio mónico $f(X) = X^2 - m \in \mathbb{Q}[X]$ anula a $\sqrt{m}$, por ello, $\sqrt{m}$ es algebraico sobre $\mathbb{Q}$ y $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}(\sqrt{m})$ es una extensión de $\mathbb{Q}$. Además, como $\sqrt{m} \notin \mathbb{Q}$, $f(X)$ es irreducible y, por tanto, $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 2$, esto es, $\mathbb{Q}(\sqrt{m})$ es un $\mathbb{Q}-$espacio vectorial de dimensión dos.

Veamos que son no isomorfos dos a dos. Sean m, n enteros libres de cuadrados con $m \neq n$ y supongamos que existe un isomorfismo $\sigma : \mathbb{Q}(\sqrt{n}) \longrightarrow \mathbb{Q}(\sqrt{m})$. Por su condición de homomorfismo, $\sigma(x) = x$ para cualquier elemento $x \in \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{n})$. En particular,

$$\sigma\left(\left(\sqrt{n}\right)\right)^2 = \sigma\left(\left(\sqrt{n}\right)^2\right) = \sigma(n) = n.$$

Luego, $\sigma(\sqrt{n}) = \pm\sqrt{n} \in \mathbb{Q}(\sqrt{m})$ que no puede ser.

Recíprocamente, si K es cuerpo cuadrático y $\alpha \in K \setminus \mathbb{Q}$ podemos escribir $K = \mathbb{Q}(\alpha)$. Al ser 1, α, α^2 linealmente dependientes y $\{1, \alpha\}$ un sistema libre, existen a, b, $c \in \mathbb{Q}$ con $a \neq 0$ tales que

$$a\alpha^2 + b\alpha + c = 0.$$

Suponemos sin pérdida de generalidad que a, b, $c \in \mathbb{Z}$, entonces

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Si ponemos $n = b^2 - 4ac$, n es entero no nulo y no es un cuadrado perfecto, pues si lo fuera tendríamos que $\alpha \in \mathbb{Q}$ en contra de lo supuesto. Llegamos a que $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}(\alpha) = K$. Por último, podemos escribir $n = k^2 m$ con $m \in \mathbb{Z}$ libre de cuadrados y así $K = \mathbb{Q}(\sqrt{m})$.

□

De aquí en adelante consideramos los cuerpos cuadráticos como $K = \mathbb{Q}(\sqrt{m})$ y m un entero libre de cuadrados.

Definición 1.1.2. Decimos que un cuerpo cuadrático $K = \mathbb{Q}(\sqrt{m})$ es *real* si está contenido en $\mathbb{R}$ o, equivalentemente, si $m > 0$. En caso contrario decimos que es *imaginario*.

Si $\alpha = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m})$, con x, $y \in \mathbb{Q}$, definimos el *conjugado* de α como

$$\overline{\alpha} = x - y\sqrt{m}.$$

Se sigue de la definición que, para $\alpha, \beta \in \mathbb{Q}(\sqrt{m})$,

1. $\overline{(\overline{\alpha})} = \alpha$
2. $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$
3. $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$

A través del conjugado se define, para un elemento $\alpha = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m})$, la traza y la norma como

$$Tr(\alpha) = \alpha + \overline{\alpha} = 2x \in \mathbb{Q} \quad \text{y} \quad N(\alpha) = \alpha\overline{\alpha} = x^2 - y^2 m \in \mathbb{Q},$$

respectivamente. Se prueba que la traza es aditiva y la norma multiplicativa.

Además,

$$\alpha^2 = (x + y\sqrt{m})^2 = x^2 + y^2 m + 2xy\sqrt{m} =$$
$$= -x^2 + y^2 m + 2x(x + y\sqrt{m}) = -N(\alpha) + Tr(\alpha)\alpha$$

y por ello, α es raíz del polinomio mónico

$$f(X) := X^2 - Tr(\alpha)X + N(\alpha) \in \mathbb{Q}[X], \tag{1.1}$$

que al ser de grado dos es el polinomio mínimo de α cuando $\alpha \in K \setminus \mathbb{Q}$.

1.2. Enteros cuadráticos

Los enteros algebraicos de K son el análogo a lo enteros del cuerpo $\mathbb{Q}$. Éstos también constituyen un anillo y es el objeto de estudio de esta sección.

Definición 1.2.1. Un número complejo α se dice *entero algebraico* si es raíz de un polinomio mónico con coeficientes en $\mathbb{Z}$.

La prueba de que los enteros algebraicos forman un anillo se sigue teniendo en cuenta el siguiente resultado.

Proposición 1.2.1. *Un número complejo α es entero algebraico si, y solo si, $\mathbb{Z}[\alpha]$ es un $\mathbb{Z}-$módulo finitamente generado.*

Demostración.
"$\Longrightarrow$": Si α es un entero algebraico, existe $f(X) \in \mathbb{Z}[X]$ mónico tal que $f(\alpha) = 0$, esto es,

$$\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0\,, \quad a_i \in \mathbb{Z},$$

con lo que $\alpha^n = -\left(a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0\right)$. Luego $\{1, \alpha, ..., \alpha^{n-1}\}$ es un sistema generador de $\mathbb{Z}[\alpha]$ como $\mathbb{Z}-$módulo.

"$\Longleftarrow$": Supongamos que $\mathbb{Z}[\alpha] = \mathbb{Z}\alpha_1 + ... + \mathbb{Z}\alpha_n$ es finitamente generado, con $\alpha_i \in \mathbb{C}$. Es claro que $\alpha\mathbb{Z}[\alpha] \subseteq \mathbb{Z}[\alpha]$, por lo que para cualquier $i \in \{1, ..., n\}$, $\alpha\alpha_i \in \mathbb{Z}[\alpha]$ y por ello, $\alpha\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j$ con $a_{ij} \in \mathbb{Z}$. Sea $A = (a_{ij})$, tenemos que

$$A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \alpha \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix},$$

es decir, α es un autovalor de la matriz A y, por tanto, $det\,(\alpha I_n - A) = 0$. Expandiendo el determinante queda que $\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0$ con $a_0, ..., a_n \in \mathbb{Z}$, lo que quiere decir que α es un entero algebraico.

□

Corolario 1.2.2. *El conjunto de los enteros algebraicos forma un anillo.*

Demostración.

Veremos que es un subanillo de $\mathbb{C}$. En efecto, 1 es un entero algebraico y si α, β son enteros algebraicos, entonces $\mathbb{Z}[\alpha, \beta]$ es finitamente generado como $\mathbb{Z}-$módulo. En consecuencia, tanto $\mathbb{Z}[\alpha + \beta]$ como $\mathbb{Z}[\alpha\beta]$ están finitamente generados al estar contenidos en $\mathbb{Z}[\alpha, \beta]$. Se sigue que $\alpha + \beta$ y $\alpha\beta$ son enteros algebraicos.

□

A los enteros algebraicos de los cuerpos cuadráticos se les denomina enteros cuadráticos y al conjunto de los enteros cuadráticos de un cuerpo cuadrático K lo denotaremos por $\mathcal{O}_K$. Se sigue del Corolario 1.2.2 que $\mathcal{O}_K$ es un anillo, es más, es un dominio de integridad.

El objetivo de esta sección es determinar el anillo $\mathcal{O}_K$, que se conoce como el *anillo de enteros cuadráticos* de K. Para ello veremos primero que ser entero algebraico equivale a que el polinomio mínimo tiene sus coeficientes en $\mathbb{Z}$.

Proposición 1.2.3. *Un número complejo α es entero algebraico si, y solo si, es algebraico y su polinomio mínimo está en $\mathbb{Z}[X]$.*

Demostración.

Si $\alpha \in \mathbb{C}$ es un entero algebraico, existe $h(X) \in \mathbb{Z}[X]$ mónico tal que $h(\alpha) = 0$. Supongamos que $f(X) = Irr(\alpha, \mathbb{Q})$, entonces $h(X) = f(X)q(X)$, para algún polinomio $q(X) \in \mathbb{Q}[X]$. De aquí se sigue que $deg(h(X)) \geq deg(f(X))$.

- Si $deg(h(X)) = deg(f(X))$, tiene que ser $h(X) = f(X)$ pues ambos son mónicos, lo que implicaría que $f(X) \in \mathbb{Z}[X]$.
- Si $deg(h(X)) > deg(f(X))$, $h(X) \in \mathbb{Z}[X]$ es un polinomio reducible en $\mathbb{Q}[X]$ y, al ser primitivo, también lo es en $\mathbb{Z}[X]$. Con lo cual, $h(X) = g(X)r(X)$ con $g(X)$ y $r(X)$ polinomios mónicos de $\mathbb{Z}[X]$ y con grado menor al grado de $h(X)$. Además, $h(\alpha) = 0 = g(\alpha)r(\alpha)$. Podemos suponer que $g(\alpha) = 0$ y repetir el razonamiento hasta obtener un polinomio en $\mathbb{Z}[X]$ mónico, que anula a α y con el mismo grado que $f(X)$, es decir, su polinomio mínimo.

Recíprocamente si α es algebraico y su polinomio mínimo está en $\mathbb{Z}[X]$, α es entero algebraico.

□

Con este resultado, determinar cuándo un complejo α es entero algebraico se hace más sencillo. Por ejemplo, si $\alpha \in \mathbb{Q}$, su polinomio mínimo es $g(X) = X - \alpha$, que estará en $\mathbb{Z}[X]$ si, y solo si, $\alpha \in \mathbb{Z}$. Es decir, los enteros son los únicos enteros algebraicos racionales.

En el caso que nos concierne, ver cuándo $\alpha \in K \setminus \mathbb{Q}$ es entero algebraico se reduce a ver cuándo $Tr(\alpha)$ y $N(\alpha)$ están en $\mathbb{Z}$, pues sabemos que su polinomio mínimo es como en (1.1). Nuevamente, si denotamos $\mathbb{Z}[\alpha] = \{\, g(\alpha) \in \mathbb{C} \,:\, g(X) \in \mathbb{Z}[X]\}$, se cumple que

$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \,:\, a, b \in \mathbb{Z}\} \subseteq \mathcal{O}_K$, ya que si $\alpha = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ su polinomio mínimo es

$$X^2 - Tr(\alpha)X + N(\alpha) = X^2 - 2aX + a^2 - b^2 m \in \mathbb{Z}[X].$$

En general, se tiene el siguiente resultado que determina por completo los elementos de $\mathcal{O}_K$.

Proposición 1.2.4. *Sea $K = \mathbb{Q}(\sqrt{m})$. Entonces*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}] & si\ m \equiv 2,\, 3\ (mod\, 4) \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & si\ m \equiv 1\ (mod\, 4) \end{cases}$$

Demostración.

En primer lugar, sabemos que $\mathbb{Z}[\sqrt{m}] \subseteq \mathcal{O}_K$. Además, si $m \equiv 1\,(mod\,4)$ un elemento $\alpha = a + b\left(\frac{1+\sqrt{m}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ tiene traza

$$Tr(\alpha) = Tr\left(a + \frac{b}{2} + \frac{b}{2}\sqrt{m}\right) = 2\left(a + \frac{b}{2}\right) = 2a + b \in \mathbb{Z}$$

y norma

$$N(\alpha) = \left(a + \frac{b}{2}\right)^2 - \frac{b^2}{4}m = a^2 + ab + \frac{b^2}{4}(1 - m) \in \mathbb{Z}, \text{ al ser } m \equiv 1\,(mod\,4),$$

lo que implica que $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] \subseteq \mathcal{O}_K$.

Comprobemos que éstos son exactamente todos los elementos de $\mathcal{O}_K$. En efecto, dado $\alpha = x + y\sqrt{m} \in K$ será entero algebraico si, y solo si,

$$Tr(\alpha) = 2x \in \mathbb{Z} \text{ y } N(\alpha) = x^2 - y^2 m \in \mathbb{Z}.$$

Si $2x \in \mathbb{Z}$ o bien $x \in \mathbb{Z}$ o bien $x = \frac{a}{2}$ con a entero impar.

- Si $x \in \mathbb{Z}$, entonces $x^2 \in \mathbb{Z}$ y para que la norma sea entera debe ser $y^2 m \in \mathbb{Z}$. Así $y \in \mathbb{Z}$, pues en caso contrario sería $y = \frac{r}{s}$ con r, s enteros coprimos y s no unidad, cumpliendo que

  $$y^2 m = \frac{r^2}{s^2}m = q \in \mathbb{Z} \implies s^2 q = m r^2$$

  y como r y s son coprimos, tiene que ser $s^2 | m$, que no es cierto ya que m es libre de cuadrados.
  Luego si $x \in \mathbb{Z}$, entonces $y \in \mathbb{Z}$ y se tiene que

  $$\alpha = x + y\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$$

  y que

  $$\alpha = x + y\sqrt{m} = (x - y) + 2y\left(\frac{1 + \sqrt{m}}{2}\right) \in \mathbb{Z}\left[\frac{1 + \sqrt{m}}{2}\right].$$

- Si $x = \frac{a}{2}$ con a entero impar, la norma $\frac{a^2}{4} - y^2 m \in \mathbb{Z}$ si y solo si $a^2 - 4y^2 m \in 4\mathbb{Z}$, en particular $(2y)^2 m \in \mathbb{Z}$, es decir, $2y \in \mathbb{Z}$. Si $y \in \mathbb{Z}$, entonces $a^2 - 4my^2$ es impar en contra de lo supuesto. Por tanto, $y = \frac{b}{2}$ con b entero impar. En ese caso, $a^2 - mb^2 \in 4\mathbb{Z}$ luego debe ser $m \equiv 1\,(mod\,4)$ pues $a^2 \equiv b^2 \equiv 1\,(mod\,4)$ para cualesquiera a, b impares. De esta forma,

$$\alpha = x + y\sqrt{m} = \frac{a}{2} + \frac{b}{2}\sqrt{m} = \frac{a-b}{2} + b\left(\frac{1+\sqrt{m}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right].$$

□

Ejemplo 1. Los anillos de enteros cuadráticos más conocidos son los llamados enteros de Gauss y los enteros de Eisenstein. El primero se corresponde con el anillo de enteros cuadráticos del cuerpo $\mathbb{Q}(i)$ y son los elementos del anillo $\mathbb{Z}[i]$. El anillo de enteros de Eisenstein, por su parte, está formado por los enteros cuadráticos de $\mathbb{Q}(\sqrt{-3})$, que al ser $-3 \equiv 1\,(mod\,4)$, por la proposición anterior tenemos que es $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \mathbb{Z}[\omega]$, con $\omega \neq 1$ una raíz tercera primitiva de la unidad.

Para simplificar, denotaremos para $K = \mathbb{Q}(\sqrt{m})$

$$\omega_{_K} = \begin{cases} \sqrt{m} & si\ m \equiv 2,\ 3\,(mod\,4) \\ \frac{1+\sqrt{m}}{2} & si\ m \equiv 1\,(mod\,4) \end{cases} \tag{1.2}$$

y así, $\mathcal{O}_K = \mathbb{Z}[\omega_{_K}] = \{a + b\omega_{_K} \,:\, a,\, b \in \mathbb{Z}\}$.

Una vez determinado los anillos de enteros cuadráticos, lo natural es comprobar si tienen propiedades similares a la del anillo de los enteros $\mathbb{Z}$, en particular si existe o no factorización única. Para ello estudiamos los elementos notables de $\mathcal{O}_K$.

Se comienza viendo cómo son las unidades de $\mathcal{O}_K$. Teniendo en cuenta que la norma es multiplicativa y que la norma de un entero algebraico es un entero racional se tiene el siguiente resultado.

Proposición 1.2.5. *Sea $\varepsilon \in \mathcal{O}_K$, ε es unidad si y sólo si $N(\varepsilon) = \pm 1$.*

Ejemplo 2. Con esto, podemos ver que en el caso de los cuerpos cuadráticos imaginarios, el anillo de enteros cuadráticos siempre tendrá un número finito de unidades. En efecto, para cuerpos cuadráticos imaginarios, es decir, $K = \mathbb{Q}(\sqrt{m})$ con $m < 0$ y $N(\alpha) \geq 0$ para cualquier $\alpha \in K$, tenemos los dos casos siguientes:

1. $m \equiv 2,\ 3\,(mod\,4)$:
   En este caso $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$, luego $\varepsilon = a + b\sqrt{m} \in \mathcal{O}_K^{\times}$ si y solo si

   $$N(\varepsilon) = a^2 - b^2 m = 1$$

   con $a, b \in \mathbb{Z}$, con lo que $\mathbb{Z}[i]^{\times} = \{\pm 1,\, \pm\sqrt{-1}\}$ y $\mathbb{Z}[\sqrt{m}]^{\times} = \{\pm 1\}$ para $m \neq -1$.

2. $m \equiv 1\,(mod\,4)$:
   Entonces $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ y $\varepsilon = \frac{a+b\sqrt{m}}{2} \in \mathcal{O}_K^\times$ si y solo si

$$N(\varepsilon) = \frac{a^2 - b^2 m}{4} = \pm 1$$

   con $a, b \in \mathbb{Z}$, lo que nos lleva a que $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]^\times = \left\{\pm 1, \pm\frac{1+\sqrt{-3}}{2}, \pm\frac{1-\sqrt{-3}}{2}\right\}$ y $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]^\times = \{\pm 1\}$ para $m \neq -3$.

Existen anillos de enteros cuadráticos, empero, que tienen infinitas unidades. Este es el caso de $\mathbb{Z}[\sqrt{2}]$, en el que $1+\sqrt{2}$ es una unidad al ser $N(1+\sqrt{2}) = 1-2 = -1$ y además, por la multiplicidad de la norma, cualquier potencia de $1+\sqrt{2}$ es también una unidad y son todas distintas.

Para determinar los elementos irreducibles de $\mathcal{O}_K$ tenemos un resultado similar al de las unidades.

Proposición 1.2.6. *Si $\gamma \in \mathcal{O}_K$ satisface que $N(\gamma) = p$ es primo en $\mathbb{Z}$, entonces γ es un elemento irreducible de $\mathcal{O}_K$.*

Su prueba, al igual que con las unidades, se deduce de la propiedad multiplicativa de la norma y teniendo en cuenta que la norma de enteros algebraicos es un entero racional.

El recíproco no es cierto en general.

Ejemplo 3. En $\mathbb{Z}[\sqrt{-1}]$, 3 es irreducible pero $N(3) = 9$. Desde luego, si $3 = \alpha\beta$ tendríamos que α, $\beta \neq 0$ y $N(\alpha)N(\beta) = 9$. Como en $\mathbb{Z}[\sqrt{-1}]$ la norma es siempre positiva o cero, tiene que ser $N(\alpha) \in \{1, 3, 9\}$. Si fuera $N(\alpha) = 1$ o $N(\alpha) = 9$ entonces α o β serían unidad. Además, si $\alpha = a + b\sqrt{-1}$ con $a, b \in \mathbb{Z}$, nunca puede ser $N(\alpha) = a^2 + b^2 = 3$.

La Proposición 1.2.6 nos permite probar que existe factorización en los anillos $\mathcal{O}_K$.

Proposición 1.2.7. *Si $\alpha \notin \mathcal{O}_K^\times$ y $\alpha \neq 0$, entonces α se factoriza como producto de elementos irreducibles en $\mathcal{O}_K$.*

Demostración.
Para demostrarlo usamos inducción sobre $|N(\alpha)|$, con α como en la proposición. Si $|N(\alpha)| = 2$ entonces α es irreducible y ya estaría.
Supongamos que es cierto para todo elemento con $2 \leq |N(\alpha)| \leq n-1$.
Sea α tal que $|N(\alpha)| = n$ y no es irreducible entonces podemos poner $\alpha = \beta\gamma$ con β y γ no unidades. Entonces $|N(\beta)|$, $|N(\gamma)| \neq 1$ y son estrictamente menor a $|N(\alpha)|$. Aplicando la hipótesis de inducción

$$\beta = \pi_1 ... \pi_r \quad \text{y} \quad \gamma = \pi_1' ... \pi_s' \,,$$

con π_i y π_j' elementos irreducibles de $\mathcal{O}_K$. De aquí, $\alpha = \beta\gamma = \pi_1 ... \pi_r \pi_1' ... \pi_s'$.

□

En general, esta factorización en $\mathcal{O}_K$ no es única. De hecho, un mismo elemento puede tener dos factorizaciones con distinto número de factores irreducibles en ella.

Ejemplo 4. En $\mathbb{Z}[\sqrt{-14}]$

$$3^4 = 81 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14}).$$

Procediendo de forma similar al ejemplo 3 podemos ver que 3 es irreducible en $\mathbb{Z}[\sqrt{-14}]$. Veamos que $5 \pm 2\sqrt{-14}$ también son irreducibles. Supongamos que no lo son, por tanto, que existen α, $\beta \in \mathbb{Z}[\sqrt{-14}]$ tales que $5 \pm 2\sqrt{-14} = \alpha\beta$. Como ambos tienen norma igual a 81, se tiene que $N(\alpha) \in \{1, 3, 9, 27, 81\}$. Si ponemos $\alpha = a + b\sqrt{-14}$ entonces

$$N(\alpha) = a^2 + 14b^2$$

y de aquí se deduce que $N(\alpha) \neq 3, 27$. Por otra parte, los únicos elementos de $\mathbb{Z}[\sqrt{-14}]$ con norma igual a 9 son ± 3, que ninguno divide a $5 \pm 2\sqrt{-14}$. Se conluye que $N(\alpha) = 1$ o $N(\alpha) = 81$ y que, por tanto, α o β es una unidad, con lo que $5 \pm 2\sqrt{-14}$ son irreducibles.

Este ejemplo no solo muestra que no existe descomposición única en general en $\mathcal{O}_K$ sino que, al contrario que en el anillo de enteros $\mathbb{Z}$, ser irreducible no es condición suficiente para ser primo. En efecto, en $\mathcal{O}_K$ un entero $c \in \mathbb{Z}$ divide a un entero cuadrático $\alpha = a + b\omega_K$, con a, $b \in \mathbb{Z}$ si, y solo si, divide a a y a b. En nuestro caso, $3 \in \mathbb{Z}[\sqrt{-14}]$ es irreducible y divide a $81 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14})$, sin embargo, no divide a $5 \pm 2\sqrt{-14}$, por lo que no puede ser primo.

1.3. Ideales de anillos de enteros cuadráticos

Dedekind se percató que la factorización única podía salvaguardarse si en lugar de elementos consideramos los ideales generados por éstos. De hecho, en lo que se conocen como dominios de Dedekind, todo ideal puede ser expresado de forma única como producto de ideales primos.

La descomposición única de ideales es el motivo de estudio del próximo capítulo y veremos que existe en anillos de enteros cuadráticos. Para poder probar este resultado, se hace necesario estudiar algunas propiedades de los ideales en $\mathcal{O}_K$.

Proposición 1.3.1. *Todo ideal de $\mathcal{O}_K$ está generado a lo sumo por dos elementos.*

Demostración.
Un ideal en $\mathcal{O}_K$ puede verse como un subgrupo de $\mathcal{O}_K$. Como grupo aditivo $\mathcal{O}_K \cong \mathbb{Z}^2$, es decir, $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre de rango dos. Por tanto, cualquier subgrupo de $\mathcal{O}_K$ está generado a lo sumo por dos elementos. Esto implica que, como subgrupo de $\mathcal{O}_K$, cualquier ideal tiene a lo sumo dos generadores como $\mathbb{Z}$-módulo, con lo que también como ideal (es decir, como $\mathcal{O}_K$-módulo).

□

Con esto no pretendemos decir que un ideal de $\mathcal{O}_K$ no pueda estar generado por más de dos elementos sino que podemos encontrar dos que lo generen.

Corolario 1.3.2. *Sea K un cuerpo cuadrático y $\mathcal{O}_K$ el anillo de enteros cuadráticos de K. Entonces $\mathcal{O}_K$ es un anillo noetheriano.*

Proposición 1.3.3. *Dado $\mathfrak{a} \neq \{0\}$ ideal de $\mathcal{O}_K$ se tiene que $\mathcal{O}_K/\mathfrak{a}$ es un conjunto finito.*

Demostración.

Sea $\alpha \in \mathfrak{a} \setminus \{0\}$. El número $N(\alpha) = \alpha\alpha' \in \mathbb{Z}$ es no nulo y además está en $\mathfrak{a}$. De esta forma, el ideal $\langle N(\alpha)\rangle \subseteq \mathfrak{a}$ y se define el homomorfismo natural

$$\begin{aligned} \varphi : \mathcal{O}_K/\langle N(\alpha)\rangle &\longrightarrow \mathcal{O}_K/\mathfrak{a} \\ a + b\omega_{_K} + \langle N(\alpha)\rangle &\longmapsto a + b\omega_{_K} + \mathfrak{a} \end{aligned}$$

que resulta ser sobreyectivo. Probaremos que $\mathcal{O}_K/\langle N(\alpha)\rangle$ es un conjunto finito y así $\mathcal{O}_K/\mathfrak{a}$ tiene que ser finito también. Para ello, partimos de que $\mathcal{O}_K \cong \mathbb{Z}^2$ como grupo aditivo y veremos que $\mathbb{Z}^2/n\mathbb{Z}^2$ es finito, siendo $n = N(\alpha) \in \mathbb{Z}$.

Consideramos la proyección canónica $\pi_n : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ y definimos el epimorfismo $\Psi = \pi_n \times \pi_n : \mathbb{Z}^2 \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, cuyo núcleo es $Ker(\psi) = n\mathbb{Z}^2$. Por el primer teorema de isomorfía $\mathbb{Z}^2/n\mathbb{Z}^2 \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, luego $\mathcal{O}_K/(N(\alpha)) \cong \mathbb{Z}^2/n\mathbb{Z}^2$ tiene exactamente n^2 elementos.

□

Corolario 1.3.4. *Todo ideal primo no nulo $\mathfrak{p}$ de $\mathcal{O}_K$ es maximal, es decir, $\mathcal{O}_K$ es de dimensión 1.*

Demostración.

Si tomamos $\mathfrak{p} \neq \{0\}$ ideal primo de $\mathcal{O}_K$ entonces $\mathcal{O}_K/\mathfrak{p}$ es un dominio de integridad finito y, por lo tanto, cuerpo, lo que implica que $\mathfrak{p}$ es un ideal maximal de $\mathcal{O}_K$.

□

Capítulo 2

Dominios de Dedekind

En este capítulo se estudian los dominios de Dedekind, que generalizan las propiedades de los anillos de enteros cuadráticos vistas en el capítulo anterior y en los que se prueba que existe factorización única de ideales. Los dominios de Dedekind son la versión global de los dominios de valoración discreta, cuya definición y propiedades se estudian en las primeras secciones del capítulo. Finaliza el capítulo con el estudio de la factorización única de ideales para los anillos de enteros cuadráticos.

En lo que sigue de memoria, se consideran los anillos conmutativos y unitarios.

2.1. Dependencia entera y localización

Con esta sección se pretende únicamente introducir algunos conceptos y resultados del álgebra conmutativa a los que haremos alusión y con los que se trabajan en el resto del capítulo. Para un estudio más detallado se puede ver, por ejemplo, los Capítulos 3 y 5 de [1].

Definíamos en el Capítulo 1 de esta memoria los enteros algebraicos como los elementos de $\mathbb{C}$ que son raíz de algún polinomio mónico con coeficientes en el anillo $\mathbb{Z}$. En general, se puede definir un elemento entero como sigue.

Definición 2.1.1. Sea B un anillo y A un subanillo unitario de B. Un elemento α de B se dice que es entero sobre A si existe un polinomio mónico de $A[X]$ que anule a α, es decir, si α satisface una ecuación de la forma

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

donde $a_i \in A$ para cada i.

Los enteros algebraicos, por tanto, no son más que los elementos de $\mathbb{C}$ enteros sobre $\mathbb{Z}$.

Proposición 2.1.1. *El conjunto C de elementos de B que son enteros sobre A es un subanillo de B que contiene a A.*

De forma análoga al Corolario 1.2.2, la demostración se sigue de que un elemento $\alpha \in B$ es entero sobre A si, y solo si, $A[\alpha]$ es un $A-$módulo de generación finita. Además, los elementos de A siempre son enteros sobre A.

A este anillo C se le denomina la clausura íntegra de A en B. Si $C = A$, se dice que A es *íntegramente cerrado* en B.

Definición 2.1.2. Un dominio de integridad A se dice que es *íntegramente cerrado* si es íntegramente cerrado en su cuerpo de fracciones.

Ejemplo 5. Se seguía de la Proposición 1.2.3 que los elementos de $\mathbb{Q}$ enteros sobre $\mathbb{Z}$ son exactamente los propios elementos de $\mathbb{Z}$. En otras palabras, $\mathbb{Z}$ es íntegramente cerrado.

Ejemplo 6. Dado un cuerpo cuadrático K, el anillo de enteros cuadráticos $\mathcal{O}_K$ es, por construcción, íntegramente cerrado.

La localización es un proceso asociado a la construcción de anillos de fracciones. Recibe el nombre de localización pues los anillos que se obtienen tras este proceso son locales, es decir, poseen un único ideal maximal.

Definición 2.1.3. Un *subconjunto multiplicativamente cerrado* de A es un subconjunto S de A tal que $1 \in S$ y para cualesquiera dos elementos s, t de S, su producto se queda en S.

Sea A un anillo y S un subconjunto multiplicativamente cerrado de A. Definimos en $A \times S$ la relación de equivalencia

$$(a, s)\mathcal{R}(b, t) \Leftrightarrow \text{ existe } u \in S \text{ tal que } u(at - bs) = 0.$$

Se obtiene así el conjunto cociente

$$A \times S/\mathcal{R} = \left\{ \frac{a}{s} \ : \ a \in A,\, s \in S \right\},$$

al que denotamos por $S^{-1}A$, donde $\frac{a}{s}$ indica la clase del par (a, s). A este conjunto se le puede dotar de una estructura de anillo definiendo una adición y una multiplicación como sigue:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

Cuando se considera $S = A \setminus \mathfrak{p}$, siendo $\mathfrak{p}$ un ideal primo de A, el anillo de fracciones que resulta se escribe $A_{\mathfrak{p}}$ y se llama la localización de A en $\mathfrak{p}$. Este anillo tiene un único ideal maximal y es

$$\mathfrak{p}A_{\mathfrak{p}} = \left\{ \frac{a}{s} \ : \ a \in \mathfrak{p},\, s \notin \mathfrak{p} \right\}$$

Los ideales de $A_{\mathfrak{p}}$ están en correspondencia con los ideales de A contenidos en $\mathfrak{p}$. Esto es, los ideales de $A_{\mathfrak{p}}$ son los

$$\mathfrak{a}A_{\mathfrak{p}} := \left\{ \frac{a}{s} \ : \ a \in \mathfrak{a},\, s \notin \mathfrak{p} \right\}$$

donde $\mathfrak{a}$ es un ideal de A contenido en $\mathfrak{p}$. En esta correspondencia los ideales primos se corresponden con los primos, al igual que lo hacen los primarios.

Definición 2.1.4. Una propiedad P de un $A-$módulo I se dice que es una propiedad local si es cierto lo siguiente: I tiene $P \Leftrightarrow I_{\mathfrak{p}}$ tiene P, para cada ideal primo $\mathfrak{p}$ de A.

Un ejemplo de propiedad local se establece en lo siguiente:

Proposición 2.1.2. *Sea A un dominio de integridad. Entonces A es íntegramente cerrado si, y solo si, $A_{\mathfrak{p}}$ es íntegramente cerrado para cada ideal primo $\mathfrak{p}$ de A.*

Algunas propiedades de la localización que se usarán en el próximo capítulo son:

Proposición 2.1.3. *Sea M un $A-$módulo y sean I, J dos $A-$submódulos de M, entonces:*

1. $(I\,J)_{\mathfrak{p}} = I_{\mathfrak{p}} J_{\mathfrak{p}}$
2. $(I : J)_{\mathfrak{p}} = (I_{\mathfrak{p}} : J_{\mathfrak{p}})$, *si J es de generación finita.*

2.2. Dominios de valoración discreta

Para poder probar la factorización única de ideales en los dominios de Dedekind, usaremos los resultados de descomposición primaria en anillos noetherianos, que pueden encontrarse en el Capítulo 7 de [1] y algunos resultados sobre anillos de valoración discreta que comenzamos estudiando y se encuentran en [6].

Definición 2.2.1. Si A es un dominio de integridad y K su cuerpo de fracciones, se dice que A es un *anillo de valoración* de K si para cada $\alpha \in K^{\times}$ se tiene que $\alpha \in A$ o $\alpha^{-1} \in A$.

Proposición 2.2.1. *Si A es un anillo de valoración de K, entonces:*

1. *A es un anillo local.*
2. *A es íntegramente cerrado en su cuerpo de fracciones K.*

Demostración.

1. Para ver que A es anillo local veremos que $\mathfrak{m} = A \setminus A^{\times}$ es un ideal (ver Proposición 1.6. de [1]). Nótese que $\alpha \in \mathfrak{m}$ si, y solo si, $\alpha = 0$ o $\alpha^{-1} \notin A$.

   a) Si $a \in A$ y $\alpha \in \mathfrak{m}$, entonces $a\alpha \in \mathfrak{m}$ pues si no fuera así entonces $(a\alpha)^{-1} = b \in A$, por lo que $\alpha^{-1} = ab \in A$ que es absurdo.

b) Si $\alpha, \beta \in \mathfrak{m} \setminus \{0\}$, entonces, como A es anillo de valoración, $\alpha\beta^{-1} \in A$ o $\alpha^{-1}\beta \in A$. Suponemos sin pérdida de generalidad que $\alpha\beta^{-1} \in A$ y tomando $a = 1 + \alpha\beta^{-1} \in A$ en el apartado anterior,

$$\alpha + \beta = (1 + \alpha\beta^{-1})\beta \in \mathfrak{m}.$$

2. Si $\alpha \in K$ es entero sobre A, entonces satisface una ecuación de la forma

$$\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0 \quad \text{con } a_j \in A.$$

Si $\alpha \in A$ ya estaría. Si $\alpha \notin A$, entonces $\alpha^{-1} \in A$ y así $\alpha^{1-n}, \alpha^{2-n}, ..., \alpha^{-1} \in A$. Si multiplicamos la expresión anterior por α^{1-n} queda que

$$\alpha + a_{n-1} + ... + a_1\alpha^{2-n} + a_0\alpha^{1-n} = 0$$

con lo que

$$\alpha = -(a_{n-1} + ... + a_1\alpha^{2-n} + a_0\alpha^{1-n}) \in A,$$

que es una contradicción.

□

Definición 2.2.2. Sea K cuerpo, una *valoración discreta* de K es una aplicación sobreyectiva $\nu : K^\times \to \mathbb{Z}$ tal que, para $\alpha, \beta \in K^\times$

(*i*) $\nu(\alpha\beta) = \nu(\alpha) + \nu(\beta)$.

(*ii*) $\nu(\alpha + \beta) \geq \text{mín}\{\nu(\alpha), \nu(\beta)\}$.

Como consecuencia de su definición se obtienen las siguientes propiedades que serán de gran utilidad para posteriores demostraciones.

Lema 2.2.2. *Sea K un cuerpo con una valoración discreta ν. Entonces:*

1. $\nu(1) = 0$.
2. $\nu(-\alpha) = \nu(\alpha)$ *para todo* $\alpha \in K$.
3. $\nu(\alpha^{-1}) = -\nu(\alpha)$ *para todo* $\alpha \in K^\times$.

Cada valoración discreta de K tiene asociado un anillo de valoración.

Lema 2.2.3. *Si K es un cuerpo, y ν una valoración de K, entonces:*

1. *El conjunto* $\mathcal{O}_\nu := \{\alpha \in K : \nu(\alpha) \geq 0 \text{ o } \alpha = 0\}$ *es un anillo de valoración de K cuyo ideal maximal es* $\mathfrak{m}_\nu := \{\alpha \in K : \nu(\alpha) > 0 \text{ o } \alpha = 0\}$.
2. *El conjunto de unidades del anillo* $\mathcal{O}_\nu$ *es el núcleo del homomorfirmo* $\nu : K^\times \to \mathbb{Z}$, *es decir,* $\mathcal{O}_\nu^\times := \{\alpha \in K : \nu(\alpha) = 0\}$.

Demostración.

Por una parte tenemos que $1, 0 \in \mathcal{O}_\nu$. Además si $\alpha, \beta \in \mathcal{O}_\nu$ entonces

- $\alpha \pm \beta \in \mathcal{O}_\nu$ al ser $\nu(\alpha \pm \beta) \geq \text{mín}\{\nu(\alpha), \nu(\beta)\} \geq 0$.
- $\alpha\beta \in \mathcal{O}_\nu$ pues $\nu(\alpha\beta) = \nu(\alpha) + \nu(\beta) \geq 0$.

Además $\mathcal{O}_\nu$ es dominio de integridad ya que es subanillo de K.

Veamos que es un anillo de valoración. Si $\alpha \in K$ y $\alpha \notin \mathcal{O}_\nu$ entonces $\nu(\alpha) < 0$ y por tanto $\nu(\alpha^{-1}) = -\nu(\alpha) > 0$, luego $\alpha^{-1} \in \mathcal{O}_\nu$.

Al ser anillo de valoración, por la proposicion 2.2.1, es local y su ideal maximal es $\mathfrak{m}_\nu = \mathcal{O}_\nu \setminus \mathcal{O}_\nu^\times$.

Para ver que $\mathfrak{m}_\nu$ es como en (1) basta ver que el grupo de unidades del anillo es como en (2).

En efecto, si $\alpha \in K$ es tal que $\nu(\alpha) = 0$, y $\beta \in K^\times$ es tal que $\alpha\beta = 1$, entonces $0 = \nu(1) = \nu(\alpha) + \nu(\beta) = \nu(\beta)$, teniendo que $\beta \in \mathcal{O}_\nu$ y, por tanto, $\alpha \in \mathcal{O}_\nu^\times$.

Recíprocamente, si $\alpha \in \mathcal{O}_\nu^\times$ entonces $\alpha^{-1} \in \mathcal{O}_\nu$ y como $\nu(\alpha^{-1}) = -\nu(\alpha)$ con ambos $\nu(\alpha), \nu(\alpha^{-1}) \geq 0$, debe ser $\nu(\alpha) = \nu(\alpha^{-1}) = 0$.

□

Definición 2.2.3. Decimos que un dominio de integridad A es un *anillo de valoración discreta* si, para su cuerpo de fracciones K, existe una valoración discreta ν, tal que su anillo de valoración es $\mathcal{O}_\nu = A$.

Si A es un dominio de valoración discreta y $\mathfrak{a}$ es un ideal no nulo de A, entonces el conjunto $\{\nu(\alpha) : \alpha \in \mathfrak{a} \setminus \{0\}\} \subseteq \mathbb{N}$ tiene un primer elemento $k \in \mathbb{Z}$, es decir, existe $\alpha \in \mathfrak{a}$ tal que $\nu(\alpha) = k$ y para todo $\beta \in \mathfrak{a} \setminus \{0\}$, $\nu(\beta) \geq \nu(\alpha) = k$. Recíprocamente, si $\beta \in A$ y $\nu(\beta) \geq \nu(\alpha)$ entonces $\nu(\beta) - \nu(\alpha) = \nu(\beta\alpha^{-1}) \geq 0$ luego $\beta\alpha^{-1} \in A$ y $\beta = (\beta\alpha^{-1})\alpha \in \mathfrak{a}$. Más concretamente, $\beta \in \langle\alpha\rangle$, por lo tanto si $\alpha \in \mathfrak{a}$ con $\nu(\alpha) = k$ entonces

$$\mathfrak{a} = \{\beta \in A : \nu(\beta) \geq k \ o \ \beta = 0\} = \langle\alpha\rangle,$$

es decir, A es un dominio de ideales principales.

En particular, si $\mathfrak{a} = \mathfrak{m} = A \setminus A^\times = \{\alpha \in K : \nu(\alpha) \geq 1 \ o \ \alpha = 0\}$, al ser $\nu : K^\times \longrightarrow \mathbb{Z}$ sobreyectiva, existe $\pi \in K^\times$ tal que $\nu(\pi) = 1$ y así $\mathfrak{m} = \langle\pi\rangle$.

Además $\nu(\pi^k) = k\nu(\pi) = k$ y cualquier ideal de A es de la forma

$$\mathfrak{a} = \{a \in A : \nu(a) \geq k \ o \ a = 0\} = \langle\pi^k\rangle = \mathfrak{m}^k.$$

De esta forma el único ideal primo se obtiene cuando $k = 1$, esto es, el único ideal primo no nulo es el maximal y por ello $dim A = 1$.

El siguiente teorema caracteriza los dominios de valoración discreta y es fundamental para demostrar resultados sobre dominios de Dedekind, en particular, la factorización única de ideales. Dada su importancia, se incluye la prueba del mismo.

Teorema 2.2.4. *Sea A un dominio de integridad con cuerpo de fracciones K. Son equivalentes:*

1. *A es un anillo de valoración discreta.*
2. *A es un anillo noetheriano local de dimensión 1 íntegramente cerrado.*
3. *A es un anillo noetheriano local cuyo ideal maximal $\mathfrak{m}$ es principal.*
4. *A es un dominio de ideales principales local.*
5. *A es un dominio de factorización única con un único elemento irreducible π, salvo unidades.*

Demostración.
(1) $\implies$ (2): A es noetheriano al ser dominio de ideales principales y de dimensión 1 por lo anterior y, según la Proposición 2.2.1, es local e íntegramente cerrado.

(2) $\implies$ (3): Queda probar que $\mathfrak{m}$ es principal. Notemos que al ser A de dimensión 1, A no puede ser cuerpo y, por tanto, su ideal maximal $\mathfrak{m}$ es no nulo. Por otra parte, A es noetheriano luego $\mathfrak{m}$ es de generación finita y por el lema de Nakayama $\mathfrak{m} \neq \mathfrak{m}^2$. Esto nos asegura que existe $\pi \in \mathfrak{m} \setminus \mathfrak{m}^2$. Pretendemos demostrar que $\mathfrak{m} = \langle \pi \rangle$.
Por ser A noetheriano existe descomposición primaria minimal de $\langle \pi \rangle$ y sabemos que A es local y de dimensión 1, por lo que $\mathfrak{m}$ es el único ideal primo no nulo de A. Consecuentemente, $\langle \pi \rangle$ es $\mathfrak{m}-$primario y existe $n \geq 1$ tal que

$$\mathfrak{m}^n \subseteq \langle \pi \rangle \subseteq \mathfrak{m}.$$

Sea $n \in \mathbb{Z}^+$ el menor entero que cumple lo anterior y probemos que n=1.
Si $n > 1$, entonces $\mathfrak{m}^{n-1} \not\subseteq \langle \pi \rangle$, es decir, existe $x \in \mathfrak{m}^{n-1} \setminus \langle \pi \rangle$. Tomamos $\alpha = x\pi^{-1} \in K$, siendo K el cuerpo de fracciones de A, y probamos que α es un elemento entero sobre A. Primero observamos que, como $x\mathfrak{m} \subseteq \mathfrak{m}^n \subseteq \langle \pi \rangle$, entonces para todo $m \in \mathfrak{m}$, existe $t \in A$ tal que $xm = \pi t$, con lo que para todo $m \in \mathfrak{m}$, $\alpha m = xm\pi^{-1} = t \in A$ y así $\alpha\mathfrak{m} \subseteq A$. Este contenido es estricto, pues si fuera $\alpha\mathfrak{m} = A$ existiría $m \in \mathfrak{m}$ tal que $\alpha m = 1$ y se tendría que

$$\pi = \pi 1 = \pi\alpha m = xm \in \mathfrak{m}^n \subseteq \mathfrak{m}^2$$

que contradice la elección de $\pi \in \mathfrak{m} \setminus \mathfrak{m}^2$. De esta forma $\alpha\mathfrak{m} \subsetneq A$ es un ideal propio de A y está contenido en el ideal maximal. Nuevamente, por ser A noetheriano, existen $m_1, m_2, ..., m_k$ generadores de $\mathfrak{m}$ y se tiene que, para cada $i \in \{1, ..., k\}$,

$$\alpha m_i = \sum_{j=1}^{k} a_{ij} m_j \ \text{ con } \ a_{ij} \in A.$$

Si $M = (a_{ij})$ y consideramos la matriz $N = (\alpha I_k - M)$, la expresión anterior se reduce a

$$N \begin{pmatrix} m_1 \\ \vdots \\ m_k \end{pmatrix} = 0,$$

que es un sistema homogéneo con solución no trivial, lo que implica que $det(N) = 0$ y desarrollando el determinante se obtiene una ecuación de dependencia entera para α. Se concluye que α es entero sobre A y como A es íntegramente cerrado, $\alpha \in A$. Pero, entonces $x = \alpha\pi \in \langle\pi\rangle$, que no es cierto. Por tanto, debe ser $n = 1$.

(3) $\implies$ (4): Primero veamos que $\bigcap_{k\geq 1} \mathfrak{m}^k = \{0\}$. En efecto, si no fuera nulo, al ser $\mathfrak{m}$ su radical y A noetheriano, existiría $r \in \mathbb{Z}^+$ tal que

$$\mathfrak{m}^r \subseteq \bigcap_{k\geq 1} \mathfrak{m}^k \subseteq \mathfrak{m},$$

pero $\bigcap_{k\geq 1} \mathfrak{m}^k \subseteq \mathfrak{m}^r$, luego para cualquier $n \geq r$, $\mathfrak{m}^r = \mathfrak{m}^n$. En particular, se tiene que $\mathfrak{m} = \mathfrak{m}^{r+1} = \mathfrak{m}\mathfrak{m}^r$. Como A es noetheriano, $\mathfrak{m}^r$ es finitamente generado y por el lema de Nakayama $\mathfrak{m}^r = \{0\}$, en contra de lo supuesto.

Por hipótesis, el ideal maximal de A es principal, sea $\mathfrak{m} = \langle\pi\rangle$. Si $\mathfrak{a}$ es un ideal propio de A, entonces $\mathfrak{a} \subseteq \mathfrak{m}$. Además, $\mathfrak{a} \nsubseteq \bigcap_{k\geq 1} \mathfrak{m}^k = \{0\}$, pues es un ideal propio. Esto implica que existe $n \in \mathbb{Z}^+$ tal que $\mathfrak{a} \nsubseteq \mathfrak{m}^n$. Sea n el menor entero positivo que cumple lo anterior. Entonces $\mathfrak{a} \subseteq \mathfrak{m}^{n-1} = \langle\pi^{n-1}\rangle$. Por otra parte, $\mathfrak{m}^n \subseteq \mathfrak{m}^{n-1} = \langle\pi^{n-1}\rangle$ y si tomamos $x \in \mathfrak{m}^{n-1} \setminus \mathfrak{m}^n$, tenemos que $x = u\pi^{n-1}$ con $u \notin \mathfrak{m} = A \setminus A^\times$, con lo que queda que $\pi^{n-1} = u^{-1}x \in \mathfrak{a}$ y así $\langle\pi^{n-1}\rangle \subseteq \mathfrak{a}$.

(4) $\implies$ (5): Todo dominio de ideales principales es de factorización única. Además, un ideal $\langle\pi\rangle$ es maximal si, y solo si, π es irreducible. Dado que A es local, los elementos irreducibles de A generan al ideal maximal $\mathfrak{m}$ y por ello están asociados.

(5) $\implies$ (1): Si π es el único elemento irreducible de A y A es un dominio de factorización única, entonces para cada $\alpha \in A$, $\alpha = u\pi^n$, con u una unidad y $n \geq 0$. Definimos de esta forma $\nu(\alpha) := n$ y lo extendemos a su cuerpo de fracciones K mediante $\nu(\alpha/\beta) = \nu(\alpha) - \nu(\beta)$. Por construcción ν es una valoración discreta de K y su anillo de valoración es A.

□

Corolario 2.2.5. *Si A es un dominio de integridad noetheriano e íntegramente cerrado de dimensión 1, entonces para todo ideal $\mathfrak{p} \subseteq A$ el localizado $A_\mathfrak{p}$ es un anillo de valoración discreta.*

Demostración.

Los ideales primos de $A_\mathfrak{p}$ se corresponden biyectivamente con los ideales primos de A contenidos en $\mathfrak{p}$, con lo que $dimA = 1$ si y solo si $dimA_\mathfrak{p} = 1$ para todo ideal primo $\mathfrak{p}$. Además, $A_\mathfrak{p}$ es un dominio de integridad noetheriano, por la correspondencia entre los ideales de A y $A_\mathfrak{p}$ señalada en la Sección 2.1 de este capítulo, es local y es íntegramente cerrado por la Proposición 2.1.2. Por tanto, se obtiene el resultado según el teorema anterior.

□

2.3. Dominios de Dedekind

La versión global de los dominios de valoración discreta son los dominios de Dedekind.

Definición 2.3.1. Un dominio de integridad A se dice que es un dominio de Dedekind si satisface las siguientes propiedades:

1. A es un dominio noetheriano.
2. A es íntegramente cerrado.
3. Todo ideal primo no nulo de A es maximal, es decir, A es de dimensión 1.

Ejemplo 7. Para un cuerpo cuadrático K, el anillo de enteros cuadráticos es un anillo de Dedekind en tanto que es íntegramente cerrado y es noetheriano y de dimensión 1 por los resultados 1.3.1 y 1.3.4 vistos al final del capítulo 1.

Proposición 2.3.1. *Si A es un dominio noetheriano de dimensión 1, entonces todo ideal no nulo $\mathfrak{a} \subseteq A$ se puede expresar, en forma única, como producto de ideales primarios cuyos radicales son todos diferentes.*

Demostración.

Dado que A es noetheriano, $\mathfrak{a}$ tiene una descomposición primaria minimal, esto es, $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ con $\mathfrak{q}_i$ ideales $\mathfrak{p}_i$-primarios y $\mathfrak{p}_i \neq \mathfrak{p}_j$ para $i \neq j$. Al ser $dimA = 1$ y para cada $i \in \{1, ..., n\}$ $\mathfrak{p}_i \supseteq \mathfrak{q}_i \supseteq \mathfrak{a} \neq \{0\}$, tenemos que los $\mathfrak{p}_i$ son primos maximales y distintos, con lo que son coprimos dos a dos y así, para $i \neq j$

$$\sqrt{\mathfrak{q}_i + \mathfrak{q}_j} = \sqrt{\sqrt{\mathfrak{q}_i} + \sqrt{\mathfrak{q}_j}} = \sqrt{\mathfrak{p}_i + \mathfrak{p}_j} = \sqrt{\langle 1 \rangle} = \langle 1 \rangle$$

lo que implica $\mathfrak{q}_i + \mathfrak{q}_j = \langle 1 \rangle$ y $\mathfrak{a} = \mathfrak{q}_1 \cap ... \cap \mathfrak{q}_n = \mathfrak{q}_1 ... \mathfrak{q}_n$.

Esta descomposición, además, es única pues cada $\mathfrak{p}_i$ es un primo aislado al ser maximal y las componentes primarias asociadas a primos aislados son únicas.

□

Notemos que si los ideales primarios son potencia de ideales primos entonces todo ideal se expresaría de forma única como producto de ideales primos. Vamos a demostrar que esto es lo que ocurre en los dominios de Dedekind.

Proposición 2.3.2. *Sea A un dominio de integridad. Entonces, A es un dominio de Dedekind si, y solo si, A es noetheriano y para cada primo $\mathfrak{p}$, el anillo $A_{\mathfrak{p}}$ es un anillo de valoración discreta.*

Demostración.

Si A es un dominio de Dedekind, es noetheriano y por el Corolario 2.2.5 $A_{\mathfrak{p}}$ es un anillo de valoración discreta.

Recíprocamente, vimos en el Corolario 2.2.5 que $dimA = 1$ si, y solo si, $dimA_{\mathfrak{p}} = 1$ para todo ideal primo $\mathfrak{p}$. Además, A es noetheriano y es íntegramente cerrado, pues ser íntegramente cerrado es una propiedad local, como indicamos en la Proposición 2.1.2.

□

Corolario 2.3.3. *Sea A dominio de Dedekind. Entonces todo ideal primario de A es la potencia de un ideal primo.*

Demostración.

A es un dominio de Dedekind luego es noetheriano, de dimensión 1 y para cada ideal primo $\mathfrak{p}$, $A_{\mathfrak{p}}$ es un dominio de valoración discreta y por el Teorema 2.2.4 los ideales de $A_{\mathfrak{p}}$ son potencia de su ideal maximal $\mathfrak{p}A_{\mathfrak{p}}$. En particular, si $\mathfrak{q}$ es un ideal $\mathfrak{p}-$primario de A, $\mathfrak{q} \subseteq \mathfrak{p}$ y

$$\mathfrak{q}A_{\mathfrak{p}} = (\mathfrak{p}A_{\mathfrak{p}})^n = \mathfrak{p}^n A_{\mathfrak{p}}$$

para algún $n \in \mathbb{N}$. Esto implica que $\mathfrak{q} = \mathfrak{p}^n$.

□

Corolario 2.3.4. *Todo ideal no nulo $\mathfrak{a}$ de un dominio de Dedekind A se puede descomponer como un producto de ideales primos en forma única:*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_r^{e_r}$$

donde los $\mathfrak{p}_i$ son ideales primos distintos y $e_i > 0$ son enteros. Los $\mathfrak{p}_i$ son los ideales primos que contienen a $\mathfrak{a}$ y los exponentes e_i están unívocamente determinados.

Demostración.

Por la Proposición 2.3.1 todo ideal no nulo de A se descompone de forma única como producto de primarios y por el corolario anterior éstos son potencias de primos.

Además, si para algún ideal primo $\mathfrak{p}$, $\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_r^{e_r} \subseteq \mathfrak{p}$, entonces existe $i \in \{1, ..., r\}$ tal que $\mathfrak{p}_i \subseteq \mathfrak{p}$, luego $\mathfrak{p} = \mathfrak{p}_i$ al ser A de dimensión 1.

□

Se observa en el siguiente ejemplo cómo al considerar ideales, se garantiza la factorización única.

Ejemplo 8.

En $\mathbb{Z}[\sqrt{-14}]$, $15 = 3 \cdot 5 = (1 + \sqrt{-14})(1 - \sqrt{-14})$ son dos factorizaciones distintas de 15. Si ahora nos fijamos en los ideales que generan dichos elementos tenemos que

$$\mathfrak{p} = \langle 3, 1 + \sqrt{-14} \rangle \text{ y } \mathfrak{q} = \langle 5, 1 + \sqrt{-14} \rangle$$

son dos ideales primos de $\mathbb{Z}[\sqrt{-14}]$. En efecto, sea el epimorfismo

$$\begin{aligned} \varphi : \mathbb{Z}[\sqrt{-14}] &\longrightarrow \mathbb{Z}_3 \\ a + b\sqrt{-14} &\longmapsto [a - b] \end{aligned}$$

donde $[a - b]$ denota la clase de $a - b$ en $\mathbb{Z}_3$. El núcleo de φ es

$$\begin{aligned} Ker(\varphi) &= \{a + b\sqrt{-14} \ : \ [a - b] = [0]\} \\ &= \{a + b\sqrt{-14} \ : \ a = b + 3q, \ q \in \mathbb{Z}\} \\ &= \{3q + b(1 + \sqrt{-14}) \ : \ b, \ q \in \mathbb{Z}\} \\ &= \langle 3, 1 + \sqrt{-14} \rangle \end{aligned}$$

Por el primer teorema de isomorfía $\mathbb{Z}[\sqrt{-14}]/\langle 3, 1+\sqrt{-14}\rangle \cong \mathbb{Z}_3$ que es cuerpo, lo que implica que $\mathfrak{p}$ es maximal y, por tanto, primo. De forma análoga se tiene que $\mathfrak{q}$ es primo. Observemos que

$$\begin{aligned}\mathfrak{p}\overline{\mathfrak{p}} &= \langle 3, 1+\sqrt{-14}\rangle\langle 3, 1-\sqrt{-14}\rangle \\ &= \langle 9, 3-3\sqrt{-14}, 3+3\sqrt{-14}, 15\rangle = \langle 3\rangle.\end{aligned}$$

Esta última igualdad se tiene al ser $3 = 9-(3-3\sqrt{-14})-(3+3\sqrt{-14})$ y porque 3 es un divisor de 9, $3-3\sqrt{-14}$, $3+3\sqrt{-14}$ y 15. De forma similar podemos comprobar que $\langle 5\rangle = \mathfrak{q}\overline{\mathfrak{q}}$, $\langle 1+\sqrt{-14}\rangle = \mathfrak{p}\mathfrak{q}$ y $\langle 1-\sqrt{-14}\rangle = \overline{\mathfrak{p}}\overline{\mathfrak{q}}$. Esto nos asegura que

$$\langle 15\rangle = \langle 3\rangle\langle 5\rangle = \mathfrak{p}\overline{\mathfrak{p}}\mathfrak{q}\overline{\mathfrak{q}}$$

y a su vez

$$\langle 15\rangle = \langle 1+\sqrt{-14}\rangle\langle 1-\sqrt{-14}\rangle = \mathfrak{p}\mathfrak{q}\overline{\mathfrak{p}}\overline{\mathfrak{q}}.$$

En efecto esa es la descomposición en ideales primos del ideal $\langle 15\rangle$ a pesar de que 15 pueda factorizarse de dos formas distintas.

La factorización única de ideales nos permite probar resultados como el siguiente.

Proposición 2.3.5. *Un dominio de Dedekind es un dominio de ideales principales si, y solo si, es un dominio de factorización única.*

Demostración.

Todo dominio de ideales principales es dominio de factorización única. Recíprocamente, sea A un dominio de factorización única, $\mathfrak{p}$ un ideal primo no nulo de A y $0 \neq \alpha \in \mathfrak{p}$. Por factorización única $\alpha = \pi_1 ... \pi_n$ con los π_i irreducibles y al ser $\mathfrak{p}$ primo, existe algún factor irreducible $\pi := \pi_i \in \mathfrak{p}$, esto es, $\langle\pi\rangle \subseteq \mathfrak{p}$. Al ser A dominio de factorización única $\langle\pi\rangle$ es primo y, por tanto, maximal, pues $dim A = 1$. Luego $\mathfrak{p} = \langle\pi\rangle$ y de esta forma todo ideal primo de A es principal. Como todo ideal no nulo $\mathfrak{a}$ de A se descompone como producto de ideales primos y éstos son principales, entonces $\mathfrak{a}$ es principal.

□

Ejemplo 9.

En $\mathbb{Z}[\sqrt{-14}]$ el ideal $\mathfrak{a} = \langle 2, \sqrt{-14}\rangle$ no es principal. En efecto, si fuera principal existiría $\alpha \in \mathbb{Z}[\sqrt{-14}]$ tal que $\langle\alpha\rangle = \langle 2, \sqrt{-14}\rangle$, entonces $\alpha|2$ y $\alpha|\sqrt{-14}$ luego, aplicando normas, $N(\alpha)|4$ y $N(\alpha)|14$, tiene que ser $N(\alpha) = 1$ o $N(\alpha) = 2$. Si ponemos $\alpha = a + b\sqrt{-14}$ con $a, b \in \mathbb{Z}$ tenemos que $N(\alpha) = a^2 + 14b^2 \neq 2$. Tiene que ser $N(\alpha) = 1$ pero entonces $\langle 2, \sqrt{-14}\rangle = \langle 1\rangle$, que no es cierto. Se concluye que $\mathbb{Z}[\sqrt{-14}]$ no es un dominio de ideales principales y por la Proposición 2.3.5 tampoco será dominio de factorización única. De hecho, habíamos visto que $3^4 = 81 = (5+2\sqrt{-14})(5-2\sqrt{-14})$ son dos factorizaciones distintas de 81 en irreducibles.

Lo que resta de capítulo lo dedicaremos a ver cómo se factorizan los ideales en anillos de enteros cuadráticos $\mathcal{O}_K$, que al ser dominios de Dedekind tienen factorización única de ideales.

2.4. Factorización de ideales en anillos de enteros cuadráticos

Para estudiar la factorización única de ideales en los anillos $\mathcal{O}_K$ se hace necesario hablar de divisibilidad de ideales y usar una serie de resultados de prueba sencilla y que, por lo tanto, omitiremos algunas de sus demostraciones. Para indagar más en la factorización de ideales en cuerpos cuadráticos véase [4].

Definición 2.4.1. Sean $\mathfrak{a}$, $\mathfrak{b}$ ideales de $\mathcal{O}_K$. Diremos que $\mathfrak{a}$ divide a $\mathfrak{b}$ y escribimos $\mathfrak{a}|\mathfrak{b}$ si existe un ideal $\mathfrak{c}$ de $\mathcal{O}_K$ tal que $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.

Como consecuencia tenemos que si $\mathfrak{a}|\mathfrak{b}$, entonces $\mathfrak{b} \subseteq \mathfrak{a}$. Probaremos más adelante que el recíproco también es cierto.

Al igual que con los elementos de $\mathcal{O}_K$ podemos definir el conjugado de un ideal que, teniendo en cuenta las propiedades de la conjugación de un elemento, resulta ser también un ideal de $\mathcal{O}_K$.

Definición 2.4.2. Sea $\mathfrak{a}$ ideal de $\mathcal{O}_K$. Definimos el ideal conjugado de $\mathfrak{a}$ como
$$\overline{\mathfrak{a}} = \{\overline{\alpha} \,:\, \alpha \in \mathfrak{a}\}.$$

Se cumplen las mismas propiedades que las del conjugado de un elemento, esto es, si $\mathfrak{a}$, $\mathfrak{b}$ son ideales de $\mathcal{O}_K$, entonces:

1. $\overline{\overline{\mathfrak{a}}} = \mathfrak{a}$
2. $\overline{\mathfrak{a}} + \overline{\mathfrak{b}} = \overline{\mathfrak{a} + \mathfrak{b}}$
3. $\overline{\mathfrak{a}}\overline{\mathfrak{b}} = \overline{\mathfrak{a}\mathfrak{b}}$

Además, un ideal $\mathfrak{a}$ es primo si, y solo si, su conjugado $\overline{\mathfrak{a}}$ es primo.

Dicho esto, en lo que nos concierne, los ideales son finitamente generados y si $\mathfrak{a} = \langle \alpha_1, ..., \alpha_n \rangle$ es un ideal con $\alpha_1, ..., \alpha_n \in \mathcal{O}_K$, su conjugado viene dado por $\overline{\mathfrak{a}} = \langle \overline{\alpha}_1, ..., \overline{\alpha}_n \rangle$.

Sin embargo, no solo hemos señalado que $\mathcal{O}_K$ es noetheriano sino que todos sus ideales se generan a lo sumo por 2 elementos. Luego si α, $\beta \in \mathcal{O}_K$ son los generadores de un ideal el siguiente teorema nos dice exactamente quién es $\mathfrak{a}\overline{\mathfrak{a}}$.

Teorema 2.4.1. *Sea $\mathfrak{a} = \langle \alpha, \beta \rangle$ ideal de $\mathcal{O}_K$. Entonces*
$$\mathfrak{a}\overline{\mathfrak{a}} = \langle N(\alpha), Tr(\alpha\overline{\beta}), N(\beta) \rangle.$$

Demostración.
En general, $\mathfrak{a}\overline{\mathfrak{a}} = \langle \alpha, \beta \rangle \langle \overline{\alpha}, \overline{\beta} \rangle = \langle \alpha\overline{\alpha}, \alpha\overline{\beta}, \overline{\alpha}\beta, \beta\overline{\beta} \rangle = \langle N(\alpha), \alpha\overline{\beta}, \overline{\alpha}\beta, N(\beta) \rangle$. Lo que queremos ver es que
$$\langle N(\alpha), \alpha\overline{\beta}, \overline{\alpha}\beta, N(\beta) \rangle = \langle N(\alpha), Tr(\alpha\overline{\beta}), N(\beta) \rangle.$$

La inclusión $\langle N(\alpha), \alpha\overline{\beta}, \overline{\alpha}\beta, N(\beta)\rangle \supseteq \langle N(\alpha), Tr(\alpha\overline{\beta}), N(\beta)\rangle$ se tiene porque

$$Tr(\alpha\overline{\beta}) = \alpha\overline{\beta} + \overline{\alpha\overline{\beta}} = \alpha\overline{\beta} + \alpha\overline{\beta}.$$

Para probar la otra inclusión debemos tener en cuenta que como α, β y $\alpha\overline{\beta}$ son enteros algebraicos, sus normas y trazas son enteros y si $d \in \mathbb{Z}^+$ es el máximo común divisor de $N(\alpha)$, $Tr(\alpha\overline{\beta})$ y $N(\beta)$ se tiene que $\langle d\rangle = \langle N(\alpha), Tr(\alpha\overline{\beta}), N(\beta)\rangle$, con lo que la inclusión se obtiene si $\alpha\overline{\beta}$, $\overline{\alpha}\beta \in d\mathcal{O}_K$. Veremos que $\alpha\overline{\beta} \in d\mathcal{O}_K$ o, equivalentemente, que $\frac{\alpha\overline{\beta}}{d} \in \mathcal{O}_K$. Para ello probaremos que $Tr(\frac{\alpha\overline{\beta}}{d})$ y $N(\frac{\alpha\overline{\beta}}{d})$ son enteros racionales. En efecto,

$$Tr\left(\frac{\alpha\overline{\beta}}{d}\right) = \frac{\alpha\overline{\beta} + \overline{\alpha}\beta}{d} = \frac{Tr(\alpha\overline{\beta})}{d} \in \mathbb{Z}$$

pues $d|Tr(\alpha\overline{\beta})$ y

$$N\left(\frac{\alpha\overline{\beta}}{d}\right) = \frac{\alpha\overline{\beta}\overline{\alpha}\beta}{d^2} = \frac{N(\alpha)}{d}\frac{N(\beta)}{d} \in \mathbb{Z}$$

pues $d|N(\alpha)$ y $d|N(\beta)$.

De forma similar se prueba que $\overline{\alpha}\beta \in d\mathcal{O}_K$.

□

Notar que también hemos probado que $\mathfrak{a}\overline{\mathfrak{a}}$ es siempre principal y está generado por un entero positivo. Según esto definimos la norma de un ideal como sigue.

Definición 2.4.3. Para un ideal no nulo $\mathfrak{a}$ en $\mathcal{O}_K$, definimos la norma de $\mathfrak{a}$ y la denotamos por $N\mathfrak{a}$ como el entero positivo que genera a $\mathfrak{a}\overline{\mathfrak{a}}$, esto es:

$$\mathfrak{a}\overline{\mathfrak{a}} = \langle N\mathfrak{a}\rangle,\ N\mathfrak{a} \in \mathbb{Z}^+.$$

Observaciones.

1. Esta definición de norma es compatible con la de norma de un elemento en tanto que si $\mathfrak{a} = \langle\alpha\rangle$ es el ideal generado por $\alpha \in \mathcal{O}_K$ entonces $N\mathfrak{a} = |N(\alpha)|$.

2. Al igual que ocurría con la norma de un elemento, la norma de un ideal es multiplicativa, es decir, dados $\mathfrak{a}$, $\mathfrak{b}$ ideales no nulos de $\mathcal{O}_K$ entonces $N\mathfrak{a}\mathfrak{b} = N\mathfrak{a}N\mathfrak{b}$.

Como consecuencia tenemos que si $\mathfrak{a}|\mathfrak{b}$ entonces $N\mathfrak{a}|N\mathfrak{b}$, aunque el recíproco no es cierto en general.

Ejemplo 10. En $\mathbb{Z}[\sqrt{-14}]$ los ideales $\mathfrak{a} = \langle 1 + \sqrt{-14}\rangle$ y $\mathfrak{b} = \langle 1 - \sqrt{-14}\rangle$ tienen la misma norma pero $\mathfrak{a}$ no divide a $\mathfrak{b}$.

Como adelantamos, probaremos que si $\mathfrak{b} \subseteq \mathfrak{a}$ entonces $\mathfrak{a}|\mathfrak{b}$. Esto se obtiene a partir de los siguientes resultados.

Proposición 2.4.2. *Sea γ un elemento no nulo de $\mathcal{O}_K$ y $\mathfrak{a}$, $\mathfrak{b}$ dos ideales de $\mathcal{O}_K$. Si $\mathfrak{a}\langle\gamma\rangle = \mathfrak{b}\langle\gamma\rangle$ entonces $\mathfrak{a} = \mathfrak{b}$ y decimos que $\langle\gamma\rangle$ es cancelable.*

Demostración.

Observemos que $\langle\gamma\rangle\mathfrak{a} = \gamma\mathfrak{a}$, es el conjunto de elementos de $\mathfrak{a}$ multiplicados por γ. Al ser A dominio de integridad, podemos cancelar γ y por ello, las igualdades $\gamma\mathfrak{a} = \gamma\mathfrak{b}$ y $\mathfrak{a} = \mathfrak{b}$ son equivalentes.

□

Proposición 2.4.3. *Sea $\alpha \in \mathcal{O}_K$ y $\mathfrak{b} = \langle\beta_1, \beta_2\rangle$ un ideal de $\mathcal{O}_K$, las siguientes afirmaciones son equivalentes:*

1. $\langle\alpha\rangle|\mathfrak{b}$
2. $\alpha|\beta_j$ *para* $j = 1, 2$
3. $\mathfrak{b} \subseteq \langle\alpha\rangle$

Demostración.

Si $\langle\alpha\rangle|\mathfrak{b}$, entonces $\mathfrak{b} = \langle\alpha\rangle\mathfrak{c}$ para cierto ideal $\mathfrak{c} = \langle\gamma_1, \gamma_2\rangle$ de $\mathcal{O}_K$ y por lo tanto $\langle\beta_1, \beta_2\rangle = \langle\alpha\gamma_1, \alpha\gamma_2\rangle$ que implica que α divide a todo elemento de $\mathfrak{b}$, en particular, divide a β_1 y a β_2.

Que $\alpha|\beta_1, \beta_2$ significa que $\beta_1, \beta_2 \in \langle\alpha\rangle$ con lo que $\mathfrak{b} \subseteq \langle\alpha\rangle$.

Por último, si $\mathfrak{b} \subseteq \langle\alpha\rangle$ se tiene que $\alpha|\beta_1, \beta_2$, esto es, $\beta_1 = \alpha\gamma_1$ y $\beta_2 = \alpha\gamma_2$ con $\gamma_1, \gamma_2 \in \mathcal{O}_K$. Se concluye que $\mathfrak{b} = \langle\alpha\rangle\langle\gamma_1, \gamma_2\rangle$, es decir, $\langle\alpha\rangle|\mathfrak{b}$.

□

Proposición 2.4.4. *Sea $\mathcal{O}_K$ un anillo de enteros cuadráticos y sean $\mathfrak{a}, \mathfrak{b}$ ideales de $\mathcal{O}_K$, entonces $\mathfrak{a}|\mathfrak{b}$ si, y solo si, $\mathfrak{b} \subseteq \mathfrak{a}$.*

Demostración.

El caso $\mathfrak{a} = \langle 0\rangle$ es claro. Supongamos que $\mathfrak{a}$ es no nulo.

Si $\mathfrak{b} \subseteq \mathfrak{a}$, entonces $\mathfrak{b}\overline{\mathfrak{a}} \subseteq \mathfrak{a}\overline{\mathfrak{a}} = \langle N\mathfrak{a}\rangle$. Por la Proposición 2.4.3, $\langle N\mathfrak{a}\rangle|\mathfrak{b}\overline{\mathfrak{a}}$, es decir, existe un ideal $\mathfrak{c}$ tal que $\langle N\mathfrak{a}\rangle\mathfrak{c} = \mathfrak{b}\overline{\mathfrak{a}}$. Multiplicando por $\mathfrak{a}$,

$$\langle N\mathfrak{a}\rangle\mathfrak{c}\mathfrak{a} = \mathfrak{b}\langle N\mathfrak{a}\rangle$$

y cancelando $\langle N\mathfrak{a}\rangle$, según la Proposición 2.4.2, se obtiene que $\mathfrak{b}|\mathfrak{a}$.

□

Corolario 2.4.5. *Sea $\mathfrak{p}$ un ideal de $\mathcal{O}_K$. Entonces $\mathfrak{p}$ es un ideal primo no nulo si, y solo si, $\mathfrak{p}$ es un ideal propio tal que si $\mathfrak{p}|\mathfrak{a}\mathfrak{b}$, entonces $\mathfrak{p}|\mathfrak{a}$ o $\mathfrak{p}|\mathfrak{b}$.*

Demostración.

Si $\mathfrak{p} \nmid \mathfrak{a}$ el ideal $\mathfrak{p} + \mathfrak{a}$ contiene a $\mathfrak{p}$ y a $\mathfrak{a}$, es decir, es un divisor común de $\mathfrak{p}$ y $\mathfrak{a}$. Como los únicos divisores de $\mathfrak{p}$ son $\mathfrak{p}$ y $\langle 1\rangle$ y $\mathfrak{p}$ no divide a $\mathfrak{a}$, se deduce que $\mathfrak{p} + \mathfrak{a} = \langle 1\rangle$, esto es, $1 = \pi + \alpha$ para algún $\pi \in \mathfrak{p}$ y $\alpha \in \mathfrak{a}$. De esta forma, para cualquier $\beta \in \mathfrak{b}$,

$$\beta = 1 \cdot \beta = \pi\beta + \alpha\beta \in \mathfrak{p} + \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$$

y por ello $\mathfrak{b} \subseteq \mathfrak{p}$ que equivale a que $\mathfrak{p}|\mathfrak{b}$.

Recíprocamente, sean α, $\beta \in \mathcal{O}_K$ tales que $\alpha\beta \in \mathfrak{p}$. Entonces $\langle\alpha\rangle\langle\beta\rangle \subseteq \mathfrak{p}$, es decir, $\mathfrak{p}|\langle\alpha\rangle\langle\beta\rangle$, lo que implica que $\mathfrak{p}|\langle\alpha\rangle$ o $\mathfrak{p}|\langle\alpha\rangle$, esto es, $\alpha \in \mathfrak{p}$ o $\beta \in \mathfrak{p}$.

□

De esta forma, si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_K$ tal que $\mathfrak{p}\overline{\mathfrak{p}} = \langle N\mathfrak{p}\rangle$, podemos factorizar $N\mathfrak{p}$ en $\mathbb{Z}$, pongamos $N\mathfrak{p} = p_1...p_r$ con $p_1, ..., p_r$ primos de $\mathbb{Z}$. Entonces

$$\mathfrak{p}\overline{\mathfrak{p}} = \langle p_1...p_r\rangle = \langle p_1\rangle...\langle p_r\rangle,$$

es decir, $\mathfrak{p}|\langle p_1\rangle...\langle p_r\rangle$ en particular existe $i \in \{1, ..., r\}$ tal que $\mathfrak{p}|\langle p_i\rangle$.

Además este primo es único. En efecto, sea $p = p_i$ y supongamos que existe q primo de $\mathbb{Z}$, $q \neq p$, de forma que $\mathfrak{p}|\langle q\rangle$. Tenemos que $\mathfrak{p}|\langle p\rangle$ y $\mathfrak{p}|\langle q\rangle$, lo que quiere decir que $\langle p\rangle \subseteq \mathfrak{p}$ y que $\langle q\rangle \subseteq \mathfrak{p}$, esto implica que p, $q \in \mathfrak{p}$ siendo p, q coprimos, entonces $\mathfrak{p} = \langle 1\rangle$ en contra de la hipótesis de que $\mathfrak{p}$ es un ideal primo.

De esto se deduce que cualquier ideal primo $\mathfrak{p}$ no nulo de $\mathcal{O}_K$ tiene norma p o p^2 para algún primo $p \in \mathbb{Z}$. Desde luego, sea $\mathfrak{p} \neq \{0\}$ un ideal primo de $\mathcal{O}_K$ y $p \in \mathbb{Z}$ el único primo tal que $\mathfrak{p}|\langle p\rangle$. Tomando normas, $N\mathfrak{p}|N(\langle p\rangle)$ y como $N(\langle p\rangle) = |N(p)| = p^2$ tiene que ser $N\mathfrak{p} = p$ o $N\mathfrak{p} = \mathfrak{p}^2$.

Es más, si p es un número primo de $\mathbb{Z}$ y $\langle p\rangle = \mathfrak{p}_1...\mathfrak{p}_r$ es la descomposición en ideales primos del ideal generado por p, se tiene que $N(\langle p\rangle) = p^2 = N\mathfrak{p}_1...N\mathfrak{p}_r$ que nos asegura que $r \leq 2$. Es más, si $r = 1$ entonces $\langle p\rangle = \mathfrak{p}$ con $N\mathfrak{p} = p^2$ y si $r = 2$ entonces $\langle p\rangle = \mathfrak{p}\overline{\mathfrak{p}}$ pues si $\mathfrak{p}$ divide a $\langle p\rangle$ también lo hace su conjugado $\overline{\mathfrak{p}}$.

Así, si $p \in \mathbb{Z}$ es primo, el ideal $\langle p\rangle$ se factoriza de alguna de las siguientes formas:

$$\langle p\rangle = \begin{cases} \mathfrak{p}\overline{\mathfrak{p}} & con\, \mathfrak{p} \neq \overline{\mathfrak{p}} \\ \mathfrak{p} & con\, \mathfrak{p} = \overline{\mathfrak{p}} \\ \mathfrak{p}^2 & con\, \mathfrak{p} = \overline{\mathfrak{p}} \end{cases}$$

El siguiente teorema nos dice cómo va a factorizar dicho ideal $\langle p\rangle$. Cuando escribamos $\overline{f(X)}$, estaremos denotando al polinomio de $\mathbb{Z}_p[X]$ cuyos coeficientes son la clase en $\mathbb{Z}_p$ de los coeficientes del polinomio $f(X)$ de $\mathbb{Z}[X]$.

Teorema 2.4.6. *Sea $K = \mathbb{Q}(\sqrt{m})$ y $\mathcal{O}_K = \mathbb{Z}[\omega_K]$ con $f(X)$ el polinomio mínimo de ω_K:*

$$f(X) = \begin{cases} X^2 - m & si\ m \equiv 2,\, 3\ (mod\, 4) \\ X^2 - X + \frac{1-m}{4} & si\ m \equiv 1\ (mod\, 4). \end{cases}$$

Para cada número primo $p \in \mathbb{Z}$, la forma en la que el ideal $\langle p\rangle$ se factoriza en $\mathcal{O}_K$ concuerda con la forma en la que $\overline{f(X)}$ se factoriza en $\mathbb{Z}_p[X]$, esto es:

1. *Si $\overline{f(X)}$ es irreducible entonces $\langle p\rangle$ es primo en $\mathcal{O}_K$ con norma p^2.*

2. *Si* $\overline{f(X)} = \overline{(X-c)}\,\overline{(X-c')}$ *con* $c \not\equiv c'\ (mod\, p)$ *entonces* $\langle p\rangle = \mathfrak{p}\overline{\mathfrak{p}}$ *con* $\mathfrak{p} \neq \overline{\mathfrak{p}}$ *y tanto* $\mathfrak{p}$ *como* $\overline{\mathfrak{p}}$ *tienen norma* p.

3. *Si* $\overline{f(X)} = \left(\overline{X-c}\right)^2$ *entonces* $\langle p\rangle = \mathfrak{p}^2$ *y* $N\mathfrak{p} = p$.

En particular, los ideales primos en $\mathcal{O}_K$ *tienen norma prima exceptuando los principales* $\langle p\rangle$ *donde* p *es un primo entero tal que* $\overline{f(X)}$ *es irreducible en* $\mathbb{Z}_p[X]$.

Demostración.

Sabemos que $\mathcal{O}_K = \mathbb{Z}[\omega_{_K}] \cong \mathbb{Z}[X]/\langle f(X)\rangle$, y de forma natural se tiene que

$$\mathcal{O}_K/\langle p\rangle \cong \mathbb{Z}[X]/\langle p, f(X)\rangle \cong (\mathbb{Z}/p\mathbb{Z})\,[X]/\langle\overline{f(X)}\rangle.$$

En este último isomorfismo se basa la demostración, donde comparamos la estructura de los anillos $\mathcal{O}_K/\langle p\rangle$ y $(\mathbb{Z}/p\mathbb{Z})\,[X]/\langle\overline{f(X)}\rangle$ para ver la forma en la que se factoriza $\langle p\rangle$.

1. Si $\overline{f(X)}$ es irreducible en $\mathbb{Z}[X]$ entonces $(\mathbb{Z}/p\mathbb{Z})\,[X]/\langle\overline{f(X)}\rangle$ es un cuerpo, luego $\mathcal{O}_K/\langle p\rangle$ también es cuerpo, con lo que $\langle p\rangle$ es maximal y por tanto primo. Recíprocamente si $\langle p\rangle$ es primo es maximal al ser $dim\mathcal{O}_K = 1$ y $(\mathbb{Z}/p\mathbb{Z})\,[X]/\langle\overline{f(X)}\rangle$ sería cuerpo, entonces $\langle\overline{f(X)}\rangle$ es maximal en $(\mathbb{Z}/p\mathbb{Z})\,[X]$ o lo que es lo mismo $\overline{f(X)}$ es irreducible en $\mathbb{Z}[X]$.

2. Si $\overline{f(X)} = \overline{(X-c)}\,\overline{(X-c')}$ con $c \not\equiv c'\, mod\, p$ entonces

$$\begin{aligned}(\mathbb{Z}/p\mathbb{Z})\,[X]/\langle\overline{f(X)}\rangle &\cong (\mathbb{Z}/p\mathbb{Z})\,[X]/\langle\overline{X-c}\rangle \times (\mathbb{Z}/p\mathbb{Z})\,[X]/\langle\overline{X-c'}\rangle\\ &\cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})\end{aligned}$$

   es producto cartesiano de dos cuerpos. Consecuentemente, no es cuerpo y no tiene elementos nilpotentes distintos del cero. Como no es cuerpo, $\langle p\rangle$ no es maximal y por tanto no es primo (nuevamente usamos que $dim\mathcal{O}_K = 1$), entonces se factoriza o bien como $\langle p\rangle = \mathfrak{p}\overline{\mathfrak{p}}$ o bien $\langle p\rangle = \mathfrak{p}^2$. Si fuera el segundo caso, $\mathcal{O}_K/\langle p\rangle = \mathcal{O}_K/\mathfrak{p}^2$ que tiene elementos nilpotentes no nulos, en concreto, la clase de los elementos de $\mathfrak{p} \setminus \mathfrak{p}^2$. Solo puede ser que $\langle p\rangle = \mathfrak{p}\overline{\mathfrak{p}}$ con $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Efectivamente, si ese fuera el caso $\mathcal{O}_K/\langle p\rangle = \mathcal{O}_K/\mathfrak{p}\overline{\mathfrak{p}}$ que no tiene elementos nilpotentes distintos del cero pues si $\alpha^m \equiv 0\ (mod\, \mathfrak{p}\overline{\mathfrak{p}})$ entonces tanto $\mathfrak{p}$ como $\overline{\mathfrak{p}}$ dividen a $\langle\alpha^m\rangle = \langle\alpha\rangle^m$, y al ser primos dividen a $\langle\alpha\rangle$, por lo tanto $\mathfrak{p}\overline{\mathfrak{p}}|\langle\alpha\rangle$ ya que $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Se concluye que $\langle p\rangle = \mathfrak{p}\overline{\mathfrak{p}}$ con $\mathfrak{p} \neq \overline{\mathfrak{p}}$.

3. Si $\overline{f(X)} = \left(\overline{X-c}\right)^2$ entonces $(\mathbb{Z}/p\mathbb{Z})\,[X]/\langle\overline{X-c}\rangle^2$ tiene un elemento nilpotente no nulo que es $\overline{X-c}\ (mod\ \left(\overline{X-c}\right)^2)$. Con esto, descartamos la posibilidad de que $\langle p\rangle$ sea primo y que $\langle p\rangle = \mathfrak{p}\overline{\mathfrak{p}}$ según lo visto antes. Solo puede ser $\langle p\rangle = \mathfrak{p}^2$ que como vimos, tiene elementos nilpotentes aparte del cero.

□

Corolario 2.4.7. *Si* $\langle p\rangle$ *no es un ideal primo en* $\mathcal{O}_K$ *y* $[c] \in \mathbb{Z}_p$ *es una raíz de* $\overline{f(X)}$, *entonces el ideal* $\langle p, \omega_{_K} - c\rangle$ *es uno de los ideales primos que dividen a* $\langle p\rangle$.

Demostración.

Según el teorema anterior $\langle p\rangle = \mathfrak{p}\overline{\mathfrak{p}}$ para cierto ideal primo $\mathfrak{p}$. Pongamos $\mathfrak{a} = \langle p, \omega_{_K} - c\rangle$. Como $p \in \mathfrak{a}$ tenemos que $\mathfrak{a}|\langle p\rangle$ y como $\omega_{_K} - c \notin \langle p\rangle$, $\mathfrak{a} \neq \langle p\rangle$ por lo que $\mathfrak{a}$ es o bien uno de los ideales primos que dividen a $\langle p\rangle$ o $\mathfrak{a} = \langle 1\rangle$. Probamos que $\mathfrak{a} \neq \langle 1\rangle$ viendo que $N\mathfrak{a} \neq 1$. Por el Teorema 2.4.1 $N\mathfrak{a}$ es el máximo común divisor de $N(p) = p^2$, $Tr(p(\overline{\omega_{_K}} - c)) = pTr(\overline{\omega_{_K}} - c)$ y de

$$N(\omega_{_K} - c) = w\overline{w} - (w + \overline{w})c + c^2 = N(w) - Tr(w)c + c^2 = f(c) \equiv 0 \ (mod\, p),$$

que son todos divisibles por p, con lo que $p|N\mathfrak{a}$. Se concluye que $\mathfrak{a} \neq \langle 1\rangle$ así que $\mathfrak{a}$ aparece en la descomposición de $\langle p\rangle$.

□

Si $p \neq 2$, la forma en la que se factoriza el polinomio $\overline{f(X)}$ viene determinado por su discriminante, a saber, si $f(X) = X^2 - m$ el discriminante es $4m$ y si $f(X) = X^2 - X + \frac{1-m}{4}$ el discriminante es m. Definimos el discriminante de K como

$$d_{_K} = \begin{cases} 4m & si\, m \equiv 2,\, 3\ (mod\, 4) \\ m & si\, m \equiv 1\ (mod\, 4) \end{cases} \tag{2.1}$$

con lo cual,

- si d_K es un cuadrado no nulo módulo p, entonces $\overline{f(X)}$ tiene dos raíces distintas
- si d_K no es un cuadrado módulo p, entonces $\overline{f(X)}$ no tiene raíces
- si d_K es 0 módulo p, entonces $\overline{f(X)}$ tiene una raíz doble

Esto puede expresarse mejor haciendo uso del símbolo de Legendre. Dados a, $p \in \mathbb{Z}$ con p primo, se define el símbolo de Legendre como

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divide a } a \\ 1 & \text{si } x^2 \equiv a\ (mod\, p) \text{ tiene solución y } p \nmid a \\ -1 & \text{si } x^2 \equiv a\ (mod\, p) \text{ no tiene solución y } p \nmid a \end{cases}$$

Así podemos reescribir el Teorema 2.4.6. Dado p un primo de $\mathbb{Z}$, la forma en la que se factoriza $\langle p\rangle$ viene dada por:

$$\langle p\rangle = \begin{cases} \mathfrak{p}\overline{\mathfrak{p}} & si\, \left(\frac{d_K}{p}\right) = 1 \\ \mathfrak{p} & si\, \left(\frac{d_K}{p}\right) = -1 \\ \mathfrak{p}^2 & si\, \left(\frac{d_K}{p}\right) = 0 \end{cases} \tag{2.2}$$

El caso $p = 2$ debemos estudiarlo aparte. Consideramos las posibles congruencias de m módulo 8 y nos fijamos en el polinomio mínimo de ω_K que era

$$f(X) = \begin{cases} X^2 - m & si\, m \equiv 2,\, 3\, (mod\, 4) \\ X^2 - X + \frac{1-m}{4} & si\, m \equiv 1\, (mod\, 4). \end{cases}$$

- Si $m \equiv 1\, (mod\, 8)$ entonces $m \equiv 1\, (mod\, 4)$ y podemos escribir $m = 8k + 1$ para cierto $k \in \mathbb{Z}$. Su polinomio mínimo sería $f(X) = X^2 - X - 2k$ que en $\mathbb{Z}_2[X]$ sería $\overline{f(X)} = \overline{X^2 + X} = \overline{X(X+1)}$, cuyas raíces son 0 y 1 y por el Teorema 2.4.6 $\langle 2\rangle = \mathfrak{p}\overline{\mathfrak{p}}$ con $\mathfrak{p} = \langle 2, \frac{1+\sqrt{m}}{2}\rangle$

- Si $m \equiv 5\, (mod\, 8)$ entonces $m \equiv 1\, (mod\, 4)$ y $m = 8k + 5$ para algún $k \in \mathbb{Z}$. Entonces $\overline{f(X)} = \overline{X^2 - X - (2k+1)} = \overline{X^2 + X + 1}$ que es irreducible. Luego $\langle 2\rangle = \mathfrak{p}$.

- Si $m \equiv 3,\, 7\, (mod\, 8)$ entonces $m \equiv 3\, (mod\, 4)$ y el polinomio mínimo $\overline{f(X)} = \overline{X^2 - m} = \overline{X^2 + 1} = (\overline{X+1})^2$ tiene una raíz doble en $\mathbb{Z}_2[X]$, lo que se traduce en que $\langle 2\rangle = \mathfrak{p}^2$ y $\mathfrak{p} = \langle 2, \sqrt{m} - 1\rangle$.

- Si m es par, entonces $m \equiv 2\, (mod\, 4)$ y $\overline{f(X)} = \overline{X^2 - m} = \overline{X}^2$ tiene una raíz doble y $\langle 2\rangle = \mathfrak{p}^2$ con $\mathfrak{p} = \langle 2, \sqrt{m}\rangle$

Esto se recoge en la siguiente tabla.

m módulo 8	$\langle 2\rangle$	$\mathfrak{p}$
1	$\mathfrak{p}\overline{\mathfrak{p}}$	$\langle 2, \frac{1+\sqrt{m}}{2}\rangle$
5	$\mathfrak{p}$	$\langle 2\rangle$
3, 7	$\mathfrak{p}^2$	$\langle 2, \sqrt{m} - 1\rangle$
par	$\mathfrak{p}^2$	$\langle 2, \sqrt{m}\rangle$

De esta forma, todos los ideales primos de $\mathcal{O}_K$ se obtienen a partir de elementos primos en $\mathbb{Z}$.

Cerramos el capítulo con un ejemplo de cómo aplicar este método para factorizar ideales en un anillo de enteros cuadráticos.

Ejemplo 11. Según la tabla anterior y haciendo uso del símbolo de Legendre computamos algunos ideales primos en $\mathbb{Z}[\sqrt{-14}]$. Tenemos la siguiente tabla para los primeros primos racionales.

p	$\langle p\rangle$	$\mathfrak{p}$
2	$\mathfrak{p}_2^2$	$\mathfrak{p}_2 = \langle 2, \sqrt{-14}\rangle$
3	$\mathfrak{p}_3\overline{\mathfrak{p}}_3$	$\mathfrak{p}_3 = \langle 3, \sqrt{-14}+1\rangle$
5	$\mathfrak{p}_5\overline{\mathfrak{p}}_5$	$\mathfrak{p}_5 = \langle 5, \sqrt{-14}+1\rangle$
7	$\mathfrak{p}_7^2$	$\mathfrak{p}_7 = \langle 7, \sqrt{-14}\rangle$
11	$\langle 11\rangle$	$\langle 11\rangle$
13	$\mathfrak{p}_{13}\overline{\mathfrak{p}}_{13}$	$\mathfrak{p}_{13} = \langle 13, \sqrt{-14}+5\rangle$
17	$\langle 17\rangle$	$\langle 17\rangle$
19	$\mathfrak{p}_{19}\overline{\mathfrak{p}}_{19}$	$\mathfrak{p}_{19} = \langle 19, \sqrt{-14}+9\rangle$
21	$\mathfrak{p}_{23}\overline{\mathfrak{p}}_{23}$	$\mathfrak{p}_{23} = \langle \sqrt{-14}+3\rangle$

A partir de aquí podemos empezar a factorizar ideales cuyos generadores no tienen por qué estar en $\mathbb{Z}$.

Si $\mathfrak{a} = \langle 2 + 3\sqrt{-14}\rangle$, su norma es $N\mathfrak{a} = 130 = 2{\cdot}5{\cdot}13$, entonces $\mathfrak{a}$ debe ser el producto de un ideal primo de norma 2, un ideal primo de norma 5 y uno de norma 13. Con esto, debe ser $\mathfrak{p}_2|\mathfrak{a}$. Los únicos ideales primos de norma 5 son $\mathfrak{p}_5$ y $\overline{\mathfrak{p}}_5$ y solo uno de ellos divide a $\mathfrak{a}$, como $2 + 3\sqrt{-14} = 5 - 3(1 - \sqrt{-14})$ entonces $\langle 2 + 3\sqrt{-14}\rangle \subseteq \langle 5, 1 - \sqrt{-14}\rangle$, luego $\overline{\mathfrak{p}}_5|\mathfrak{a}$. Además $2 + 3\sqrt{-14} = -13 + 3(5 + \sqrt{-14})$, lo que quiere decir que $\mathfrak{p}_{13}$ es el ideal de norma 13 que divide a $\mathfrak{a}$. Así, la factorización de $\mathfrak{a}$ en ideales primos es $\mathfrak{a} = \mathfrak{p}_2\overline{\mathfrak{p}}_5\mathfrak{p}_{13}$.

Capítulo 3

Grupo de clases de ideales

Determinar cuándo un dominio de Dedekind es dominio de factorización única no es, en principio, sencillo y depende, por lo probado en la Proposición 2.3.5 de si sus ideales son o no principales. En este sentido, en este capítulo vemos cómo se asocia a un dominio de Dedekind su grupo de clases de ideales, cuyo tamaño mide lo cerca que está de ser un dominio de factorización única. El grupo de clases se define a partir de los llamados ideales fraccionarios, que se estudian en la primera sección del capítulo, y se prueba que en dominios de Dedekind son invertibles y forman un grupo. En las dos últimas secciones se prueba que el grupo de clases de cuerpos cuadráticos es siempre finito y se presenta un algoritmo para su cálculo.

3.1. Ideal fraccionario

Definición 3.1.1. Sea A un dominio de integridad y sea K su cuerpo de fracciones. Un $A-$submódulo I de K es un *ideal fraccionario* de A si $\gamma I \subseteq A$ para algún $\gamma \in A \setminus \{0\}$, es decir, si I es un subconjunto no vacío de K con las siguientes propiedades:

1. $\alpha, \beta \in I \implies \alpha + \beta \in I$.
2. $\alpha \in I, r \in A \implies r\alpha \in I$.
3. Existe $\gamma \in A$, *con* $\gamma \neq 0$, tal que $\gamma I \subseteq A$.

Este elemento γ de A decimos que es un *denominador común* de I.

Notemos que cualquier ideal $\mathfrak{a}$ de A es un ideal fraccionario con denominador común $\gamma = 1$. En lo que resta, a estos ideales fraccionarios los denominaremos ideales enteros.

Ejemplo 12. Sea $A = \mathbb{Z}$ y sea

$$I = \left\{ \frac{n}{25} \,:\, n \in \mathbb{Z} \right\}.$$

I es un subconjunto no vacío de $\mathbb{Q}$, cumple las propiedades (1) y (2) y además $25I = \mathbb{Z}$. Por lo tanto, I es un ideal fraccionario de $\mathbb{Z}$.

Ejemplo 13. Sea $A = \mathbb{Z}$ y sea

$$I = \left\{ \frac{n}{5^m} \, : \, n \in \mathbb{Z}, \, m \in \mathbb{N} \right\}$$

I es un subconjunto no vacío de $\mathbb{Q}$ con las propiedades (1) y (2). Sin embargo, no existe $k \in \mathbb{Z}$ tal que $kI \subseteq \mathbb{Z}$. En este caso, I no es un ideal fraccionario.

De la definición se desprende que si γ es un denominador común de un ideal fraccionario $I \subseteq K$ entonces γI es un ideal entero de A. Luego todos los ideales fraccionarios son de la forma

$$I = \frac{1}{\gamma}\mathfrak{a} \tag{3.1}$$

con $\gamma \in A \setminus \{0\}$ y $\mathfrak{a}$ un ideal entero de A. Esta representación no es necesariamente única pues para $\delta \in A \setminus \{0\}$

$$I = \frac{1}{\gamma\delta}(\delta\mathfrak{a}).$$

Esto nos permite probar que, para I_1, I_2 ideales fraccionarios de A, $I_1 + I_2$ e $I_1 I_2$ son dos ideales fraccionarios de A. En efecto, si escribimos

$$I_1 = \frac{1}{\gamma}\mathfrak{a} \;\text{ e }\; I_2 = \frac{1}{\delta}\mathfrak{b},$$

donde $\gamma, \delta \in A \setminus \{0\}$ y $\mathfrak{a}$, $\mathfrak{b}$ ideales enteros de A, entonces $I_1 + I_2$ e $I_1 I_2$ son ideales fraccionarios con denominador común, por ejemplo, $\gamma\delta$.

Ejemplo 14. Cada elemento $\alpha = \frac{\beta}{\gamma} \in K$ genera un ideal fraccionario que se indica por $\langle\alpha\rangle = \{r\alpha \, : \, r \in A\}$ y se denomina principal. De hecho, γ es un denominador común de $\langle\alpha\rangle$.

Proposición 3.1.1. *Si I es un $A-$submódulo de K finitamente generado, entonces I es un ideal fraccionario de A. Además, si A es noetheriano, los ideales fraccionarios son los $A-$submódulos de K finitamente generados.*

Demostración.

Sean $\alpha_1, ..., \alpha_n \in K$ generadores de I. Al ser K el cuerpo de fracciones de A, cada α_i es el cociente de dos elementos de A. Sea $\gamma \in A$ el producto de los denominadores de estos cocientes, entonces podemos escribir $\alpha_i = \beta_i \gamma^{-1}$, con $\beta_i \in A$. Por lo tanto, I es un $A-$submódulo de K y existe $\gamma \in A \setminus \{0\}$ tal que $\gamma I \subseteq A$, esto es, I es un ideal fraccionario de A.

Si, además, A es noetheriano, se sigue de (3.1) que todo ideal fraccionario está finitamente generado, ya que lo están los ideales de A.

□

Recordemos que nuestro objetivo es probar que, en los dominios de Dedekind, los ideales fraccionarios forman un grupo multiplicativo. Se ha probado que el producto de dos ideales fraccionarios es un ideal fraccionario, queda ver que éstos tienen inverso. Para ello, debemos definir primero qué se entiende por inverso de un ideal fraccionario.

Definición 3.1.2. Un $A-$submódulo I de K se dice que es invertible si existe un submódulo J de K tal que $IJ = A$.

En caso de que exista tal módulo J entonces es único e igual a

$$(A : I) := \{\alpha \in K \, : \, \alpha I \subseteq A\}.$$

En efecto, $(A : I)$ es un $A-$submódulo de K y

$$J \subseteq (A : I) = (A : I)\, IJ \subseteq AJ = J$$

La relación entre los ideales fraccionarios e inversibles la da la siguiente proposición.

Proposición 3.1.2. *Si I es un $A-$submódulo invertible de K, entonces I es un ideal fraccionario.*

Demostración.

Probamos que I es finitamente generado y por la Proposición 3.1.1, I es un ideal fraccionario.

Desde luego, si $I\,(A : I) = A$ entonces existen $\alpha_1, \ldots, \alpha_n \in I$ y $\beta_1, \ldots, \beta_n \in (A : I)$ tales que

$$\alpha_1\beta_1 + \ldots + \alpha_n\beta_n = 1$$

y así, para cada $\alpha \in I$,

$$\alpha = \alpha(\alpha_1\beta_1 + \ldots + \alpha_n\beta_n) = (\beta_1\alpha)\alpha_1 + \ldots + (\beta_n\alpha)\alpha_n\,,$$

siendo $\beta_i\alpha \in A$ por definición de $(A : I)$. Por tanto, I está generado por $\alpha_1, \ldots, \alpha_n$.

□

Demostraremos que el recíproco es también cierto en los dominios de Dedekind.

Proposición 3.1.3. *Sea A un dominio de integridad e I un ideal fraccionario. Si I es de generación finita y, para cada ideal maximal $\mathfrak{m}$ de A, $I_{\mathfrak{m}}$ es invertible, entonces I es invertible.*

Demostración.

Sea $\mathfrak{a} = I\,(A : I)$ ideal entero de A. Entonces, para cada ideal maximal $\mathfrak{m}$ de A, se sigue de las propiedades de la localización (ver Proposición 2.1.3) y de que I es finitamente generado que,

$$\mathfrak{a}_{\mathfrak{m}} = (I\,(A : I)\,)_{\mathfrak{m}} = I_{\mathfrak{m}}\,(A_{\mathfrak{m}} : I_{\mathfrak{m}}) = A_{\mathfrak{m}}\,.$$

La última igualdad se sigue de que $I_{\mathfrak{m}}$ es invertible. Esto implica que $\mathfrak{a} \not\subseteq \mathfrak{m}$. Esto es, no hay ningún ideal maximal de A que contenga a $\mathfrak{a}$, luego tiene que ser $\mathfrak{a} = A$. Por consiguiente, I es invertible.

□

Proposición 3.1.4. *En un dominio de valoración discreta A todo ideal fraccionario no nulo es invertible.*

Demostración.

Al ser A dominio de valoración discreta, A es local y su ideal maximal $\mathfrak{m}$ es principal. Sea $\pi \in A$ un generador de $\mathfrak{m}$ e $I \neq \{0\}$ un ideal fraccionario, entonces existe $\gamma \in A$ tal que γI es un ideal entero de A, es decir, $\gamma I = \langle \pi^r \rangle$ para cierto $r \in \mathbb{N}$. Por ello, si $s = \nu(y)$,

$$\gamma I = \langle \gamma \rangle I = \langle \pi^s \rangle I = \langle \pi^r \rangle \,,$$

esto es, $I = \langle \pi^{r-s} \rangle$ y es invertible.

□

Proposición 3.1.5. *Sea A un dominio de Dedekind, entonces cada ideal fraccionario no nulo de A es invertible.*

Demostración.

Sea $I \neq \{0\}$ un ideal fraccionario de A. Para cada ideal primo no nulo $\mathfrak{p}$ de A el ideal $I_{\mathfrak{p}}$ es fraccionario en el dominio de valoración discreta $A_{\mathfrak{p}}$ y por la Proposición 3.1.4 invertible. Luego I es fraccionario, de generación finita por ser A noetheriano y para cada ideal primo no nulo $\mathfrak{p}$ (y por tanto, maximal) $I_{\mathfrak{p}}$ es invertible. Entonces I es invertible por la Proposición 3.1.3.

□

3.2. Grupo de clases de ideales

La sección anterior nos dice que los ideales fraccionarios no nulos de un dominio de Dedekind A con cuerpo de fracciones K, forman un grupo multiplicativo que denotaremos por $\mathfrak{I}(K)$. Ahora bien, si consideramos los ideales fraccionarios principales $\langle \alpha \rangle$ con $\alpha \in K^\times$, el conjunto $\mathfrak{P}(K)$ de ideales principales constituyen un subgrupo de $\mathfrak{I}(K)$ en cuanto que

$$\langle \alpha \rangle \langle \beta \rangle^{-1} = \langle \alpha \beta^{-1} \rangle \in \mathfrak{P}(K).$$

En lo que sigue, nos referimos a los ideales fraccionarios de A simplemente como ideales y los denotamos con letra gótica indistintamente de si son o no enteros. También diremos que el inverso de un ideal $\mathfrak{a}$ es $\mathfrak{a}^{-1}$.

Definición 3.2.1. Sea A un dominio de Dedekind con K su cuerpo de fracciones y sean $\mathfrak{I}(K)$ y $\mathfrak{P}(K)$ los grupos multiplicativos antes definidos. Se denomina *grupo de clases de ideales* de K, o simplemente grupo de clases, al grupo cociente $H(K) = \mathfrak{I}(K)/\mathfrak{P}(K)$.

Notemos que dos ideales $\mathfrak{a}$, $\mathfrak{b}$ de A están en la misma clase de $H(K)$ si, y solo si, $\mathfrak{a}\mathfrak{b}^{-1} \in \mathfrak{P}(K)$. De ello, todo ideal $\mathfrak{a}$ de A está en la misma clase de un ideal entero $\mathfrak{c}$, pues $\mathfrak{a} = \langle \gamma^{-1} \rangle \mathfrak{c}$ para cierto $\gamma \in A$, o lo que es lo mismo, $\mathfrak{a}\mathfrak{c}^{-1} = \langle \gamma^{-1} \rangle \in \mathfrak{P}(K)$.

Teorema 3.2.1. *Sea A un dominio de Dedekind y K su cuerpo de fracciones. Entonces A es un dominio de factorización única si, y solo si, $card(H(K)) = 1$.*

Demostración.

Si A es dominio de factorización única, es dominio de ideales principales por ser A de Dedekind, luego todos los ideales fraccionarios de A son principales y por ello $card(H(K)) = 1$. Recíprocamente si $card(H(K)) = 1$ entonces todos los ideales son principales y por tanto A es de factorización única.

□

3.3. Grupo de clases de cuerpos cuadráticos

Veremos en esta sección que en el caso de los cuerpo cuadráticos $K = \mathbb{Q}(\sqrt{m})$, el grupo de clases es siempre finito y al orden de tal grupo lo denotamos por $h_{_K}$ y lo llamamos *número de clases* de K. Esto se prueba a partir de los siguientes resultados.

Lema 3.3.1. *Para todo entero $t > 0$ existe una cantidad finita de ideales enteros $\mathfrak{a}$ de $\mathcal{O}_K$ tales que $N\mathfrak{a} < t$.*

Demostración.

Probaremos que existe un número finito de ideales primos $\mathfrak{p}$ tales que $N\mathfrak{p} < t$ y al ser la norma multiplicativa y existir factorización única de ideales queda asegurado el resultado para ideales enteros en general.

En la Sección 2.4 del capítulo anterior se obtuvo que los ideales primos de $\mathcal{O}_K$ vienen determinados por la forma en la que $\langle p \rangle$ se factoriza, con p un primo entero positivo. Por consiguiente, al haber un número finito de primos p tales que $p < t$, hay un número finito de ideales primos $\mathfrak{p}$ tales que $N\mathfrak{p} \leq t$.

□

Nos proponemos encontrar una cota de la norma de los representantes de cada clase. Para ello, son necesarias las proposiciones que probamos a continuación.

Proposición 3.3.2. *Sea $\mathfrak{a}$ un ideal entero de $\mathcal{O}_K$ tal que $\langle n \rangle$ no divide a $\mathfrak{a}$ para todo natural $n \geq 2$. Entonces existe $s \in \mathbb{Z}$ de forma que $s - \omega_{_K} \in \mathfrak{a}$.*

Demostración.

Sabemos que $\mathfrak{a}$ está generado a lo sumo por dos elementos, es decir,

$$\mathfrak{a} = \langle a_1 + a_2\omega_{_K}, b_1 + b_2\omega_{_K} \rangle \text{ con } a_1,\, a_2,\, b_1,\, b_2 \in \mathbb{Z}.$$

Que $\langle n \rangle$ no divida a $\mathfrak{a}$ para cualquier n natural mayor que 1, equivale a que

$$\langle a_1 + a_2\omega_{_K}, b_1 + b_2\omega_{_K} \rangle \not\subseteq \langle n \rangle$$

para cualquier $n \geq 2$, lo que implica,

$$n \nmid a_1 + a_2\omega_{_K} \quad \text{o bien} \quad n \nmid b_1 + b_2\omega_{_K}.$$

Al ser para cualquier natural mayor que 1, el maximo común divisor de a_1, a_2, b_1 y b_2 es necesariamente 1. Luego, haciendo uso de la identidad de Bézout podemos encontrar c, d, e, f enteros de forma que

$$ca_1 + da_2 + eb_1 + fb_2 = -1.$$

Es a partir de estos enteros que podemos asegurar la existencia de un elemento de la forma $s - \omega_{_K} \in \mathfrak{a}$ con $s \in \mathbb{Z}$. Distinguimos dos casos, según el valor de $\omega_{_K}$ (ver (1.2)).

- Si fuera $\omega_{_K} = \sqrt{m}$, entonces tomamos el elemento

$$(d + c\sqrt{m})(a_1 + a_2\sqrt{m}) + (f + e\sqrt{m})(b_1 + b_2\sqrt{m}) \in \mathfrak{a},$$

que multiplicando y reordenando queda

$$(a_1 d + ca_2 m + fb_1 + eb_2 m) + (ca_1 + da_2 + eb_1 + fb_2)\sqrt{m} =$$
$$= (a_1 d + ca_2 m + fb_1 + b_2 em) - \sqrt{m}.$$

- En caso de que $\omega_{_K} = \frac{1+\sqrt{m}}{2}$, tomamos

$$((d - c) + c\omega_{_K})(a_1 + a_2\omega_{_K}) + ((f - e) + e\omega_{_K})(b_1 + b_2\omega_{_K}) \in \mathfrak{a},$$

que si tenemos en cuenta que

$$\omega_{_K}^2 = \left(\frac{1+\sqrt{m}}{2}\right)^2 = \frac{m-1}{4} + \omega_{_K},$$

al multiplicar y reordenar se tiene

$$\left((d-c)a_1 + ca_2\tfrac{m-1}{4} + (f-e)b_1 + eb_2\tfrac{m-1}{4}\right) + (ca_1 + da_2 + eb_1 + fb_2)\,\omega_{_K} =$$
$$= \left((d-c)a_1 + (f-e)b_1 + (ca_2 + b_2 e)\tfrac{m-1}{4}\right) - \omega_{_K},$$

siendo el primer sumando entero, pues $m \equiv 1\,(mod\,4)$.

□

Proposición 3.3.3. *Sea $\mathfrak{b}$ un ideal de $\mathcal{O}_K$. Entonces existe un ideal entero $\mathfrak{a}$ en la clase de $\mathfrak{b}$ tal que $\langle n\rangle$ no divide a $\mathfrak{a}$ para todo natural $n \geq 2$.*

Demostración.

Todo ideal $\mathfrak{b}$ está en la clase de un ideal entero $\mathfrak{c} = \langle a_1 + a_2\omega_{_K}, b_1 + b_2\omega_{_K}\rangle$. Si éste no fuera como en las condiciones de la proposición entonces el máximo común divisor d de a_1, a_2, b_1, y b_2 es distinto de 1. Pongamos $a_i = da_i'$ y $b_i = db_i'$, entonces

$$\mathfrak{c} = \langle d\rangle\langle a_1' + a_2'\omega_{_K}, b_1' + b_2'\omega_{_K}\rangle.$$

Desde luego, el ideal $\mathfrak{a} = \langle d^{-1}\rangle\mathfrak{c}$ es entero, está en la clase de $\mathfrak{c}$, por tanto en la de $\mathfrak{b}$ y es tal que no existe un $\langle n\rangle$ que lo divida, para cualquier natural $n \geq 2$.

□

El discriminante d_K de un cuerpo cuadrático K venía dado por (2.1). En [5] se prueba que podemos considerar los representantes de las clases de $H(K)$ con norma menor a $C_{_K} := \sqrt{\frac{|d_k|}{3}}$. Presentamos a continuación este resultado, que probaremos aquí gracias a las Proposiciones 3.3.2 y 3.3.3

Lema 3.3.4. *En toda clase de ideales existe un representante* $\mathfrak{a} \subseteq \mathcal{O}_K$ *tal que* $N\mathfrak{a} \leq C_{_K}$.

Demostración.

Sea $\mathfrak{b}$ un ideal de $\mathcal{O}_K$. La Proposición 3.3.3 nos asegura la existencia de un ideal entero $\mathfrak{a}$ en la clase de $\mathfrak{b}$ y con las condiciones de la proposición 3.3.2. Por tanto, existe un entero s tal que $s - \omega_{_K} \in \mathfrak{a}$. Definimos

$$r = \begin{cases} s & si\, m \equiv 2,\, 3\, (mod\, 4) \\ \frac{2s-1}{2} & si\, m \equiv 1\, (mod\, 4) \end{cases}$$

Notemos que,

$$r - \frac{\sqrt{d_K}}{2} = s - \omega_{_K} \in \mathfrak{a}.$$

Por otra parte, si $N\mathfrak{a} = a$, al ser $\langle a \rangle = \mathfrak{a}\overline{\mathfrak{a}} \subseteq \mathfrak{a}$, se tiene que $a \in \mathfrak{a}$. De esta forma

$$r - na - \frac{\sqrt{d_K}}{2} \in \mathfrak{a}$$

para cualquier n entero. Esto nos permite elegir r tal que $|r| \leq \frac{a}{2}$. Además, dado que $r - \frac{\sqrt{|d_K|}}{2} \in \mathfrak{a}$, existe $\mathfrak{c}$ ideal entero tal que $\langle r - \frac{\sqrt{|d_K|}}{2} \rangle = \mathfrak{a}\mathfrak{c}$. Entonces,

$$N\mathfrak{a}N\mathfrak{c} = \left| \left(r - \frac{\sqrt{d_K}}{2} \right) \left(r + \frac{\sqrt{d_K}}{2} \right) \right| = \left| r^2 - \frac{d_K}{4} \right| \leq \frac{a^2}{4} + \frac{|d_K|}{4}$$

Si fuera $N\mathfrak{a} \leq N\mathfrak{c}$ entonces

$$(N\mathfrak{a})^2 \leq \frac{a^2}{4} + \frac{|d_K|}{4}$$

y si despejamos $N\mathfrak{a}$ (recordar que $N\mathfrak{a} = a$), se tiene $N\mathfrak{a} \leq \sqrt{\frac{|d_K|}{3}}$.

En caso contrario, dado que $\mathfrak{c}\,\overline{\mathfrak{c}} = \langle N\mathfrak{c} \rangle$ es un ideal principal al igual que $\mathfrak{a}\mathfrak{c}$, se deduce que

$$[\mathfrak{a}][\mathfrak{c}] = [\mathfrak{a}\mathfrak{c}] = [\mathfrak{c}\overline{\mathfrak{c}}] = [\mathfrak{c}][\overline{\mathfrak{c}}]$$

y por ello $[\mathfrak{a}] = [\overline{\mathfrak{c}}]$. Por otra parte $N\overline{\mathfrak{c}} = N\mathfrak{c} < N\mathfrak{a}$.

Además, si $\langle n \rangle | \overline{\mathfrak{c}}$, con n natural, se tiene que $\langle n \rangle | \mathfrak{c} | \langle s - \omega_{_K} \rangle$, esto es, $s - \omega_{_K} = n(a + b\omega_{_K})$, que implica $nb = -1$, es decir, $n = 1$ y $\overline{\mathfrak{c}}$ cumple las condiciones de la Proposición 3.3.2.

Se repite el proceso anterior con el ideal $\overline{\mathfrak{c}}$ y se obtiene así una sucesión decreciente de naturales la cual debe estabilizarse para cierto ideal entero con norma menor o igual a $C_{_K}$. □

Teorema 3.3.5. *El número de clases de un cuerpo cuadrático* K *es finito.*

Demostración.

Por el lema 3.3.4 toda clase de ideales tiene un representante $\mathfrak{a} \subseteq \mathcal{O}_K$ tal que $N\mathfrak{a} \leq C_{_K}$. Pero por el lema 3.3.1 existe un número finito de ideales enteros $\mathfrak{a}$ de $\mathcal{O}_K$ tales que $N\mathfrak{a} \leq \lfloor C_{_K} \rfloor + 1$. Luego hay un número finito de representantes y por tanto $h_{_K}$ es finito. □

3.4. Algoritmo y ejemplos

El procedimiento seguido para probar la finitud del número de clases de los cuerpos cuadráticos da un algoritmo para determinar los posibles representantes de clases de ideales en $H(K)$.

Sea $K = \mathbb{Q}(\sqrt{m})$ un cuerpo cuadrático. Los siguientes pasos determinan el grupo de clases de K:

1. Determinar el discriminante $d_{_K}$.
2. Computar la cota $C_{_K} = \sqrt{\frac{|d_{_K}|}{3}}$.
3. Determinar todos los números primos de $\mathbb{Z}^+$ menores a $C_{_K}$.
4. Determinar la factorización de cada ideal principal $\langle p \rangle$ de $\mathcal{O}_K$, siendo p un primo del paso 3.
5. Determinar los generadores de $H(K)$ a partir de los ideales primos obtenidos en el paso 4 de norma menor a $C_{_K}$.

En la literatura se encuentran otras cotas de la norma de los representantes de las clases de $H(K)$, igualmente válidas para computar el algoritmo, véase por ejemplo [2] y [3]. Se ha decidido tomar $C_{_K}$ pues es una cota más restrictiva para los cuerpos cuadráticos.

A partir de los resultados obtenidos en la memoria se ha implementado un programa en *dev C++* que computa los 4 primeros pasos del algoritmo. El código del programa puede encontrarse en el Apéndice A.

Finalizamos el capítulo usando el programa implementado para calcular el grupo de clases de algunos cuerpos cuadráticos.

Ejemplo 15. Probemos que el número de clases de $K = \mathbb{Q}(\sqrt{23})$ es $h_{_K} = 1$.
En este caso el discriminante es $d_{_K} = 92$, la cota es

$$C_{_K} = \sqrt{\frac{92}{3}} < 6$$

y los primos menors a 6 son $p = 2, 3$ y 5. Si computamos el algoritmo obtenemos las factorizaciones

$$\langle 2 \rangle = \langle 2, \sqrt{23} - 1 \rangle \langle 2, \sqrt{23} - 1 \rangle = \mathfrak{p}_2^2$$

$$\langle 3 \rangle = \mathfrak{p}_3 \text{ es primo}$$

$$\langle 5 \rangle = \mathfrak{p}_5 \text{ es primo}$$

y los posibles generadores del grupo de clases son, por tanto, 1 y $[\mathfrak{p}_2]$, ya que $N\mathfrak{p}_3 = 9 \not< 6$ y $N\mathfrak{p}_5 = 25 \not< 6$.

Sin embargo, notemos que

$$\langle 2, \sqrt{23} - 1\rangle = \langle 2, -5 + \sqrt{23}\rangle$$

en tanto que $5 = -2 \cdot 2 + (-1 + \sqrt{23})$ y

$$\langle 2, -5 + \sqrt{23}\rangle = \langle -5 + \sqrt{23}\rangle$$

pues $(-5 + \sqrt{23})(-5 - \sqrt{23}) = 2$.

Luego $[\mathfrak{p}_2] = [\langle 2, -5 + \sqrt{23}\rangle] = [1]$ y se deduce que el número de clases es $h_{_K} = 1$.

Ejemplo 16. Estudiemos el grupo de clases de $\mathbb{Q}[\sqrt{-14}]$ que, al no ser $\mathbb{Z}[\sqrt{-14}]$ dominio de factorización única, $h_{_K}$ no puede ser 1.

El discriminante es $d_{_K} = -56$ y la cota

$$C_{_K} = \sqrt{\frac{56}{3}} < 5.$$

Se tiene que $p = 2$, 3 son los primos menores a 5 y computando nuevamente el algoritmo,

$$\langle 2\rangle = \langle 2, \sqrt{-14}\rangle\langle 2, \sqrt{-14}\rangle = \mathfrak{p}_2^2$$

$$\langle 3\rangle = \langle 3, \sqrt{-14} - 2\rangle\langle 3, -\sqrt{-14} - 2\rangle = \mathfrak{p}_3\overline{\mathfrak{p}}_3$$

De esta forma, los generadores del grupo de clases son 1, $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$ y $[\overline{\mathfrak{p}}_3]$.

Notemos que $2 - \sqrt{-14} \in \mathfrak{p}_2$ y $2 - \sqrt{-14} \in \mathfrak{p}_3$, luego $\mathfrak{p}_2\mathfrak{p}_3|\langle 2 - \sqrt{-14}\rangle$ pues $\mathfrak{p}_2$ y $\mathfrak{p}_3$ son ideales primos. Esto implica que existe $\mathfrak{a}$ ideal entero tal que $\langle 2 - \sqrt{-14}\rangle = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{a}$ y aplicando normas

$$18 = N(\langle 2 - \sqrt{-14}) = N\mathfrak{p}_2 N\mathfrak{p}_3 N\mathfrak{a} = 6N\mathfrak{a}$$

entonces $N\mathfrak{a} = 3$ y debe ser $\mathfrak{a} = \mathfrak{p}_3$ o $\mathfrak{a} = \overline{\mathfrak{p}}_3$, pero esto último no es posible pues si fuera $\mathfrak{a} = \overline{\mathfrak{p}}_3$

$$\langle 2 - \sqrt{-14}\rangle = \mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_3 = \mathfrak{p}_2\langle 3\rangle$$

y sería $\langle 3\rangle|\langle 2 - \sqrt{-14}\rangle$ que no es cierto. Por ello $\mathfrak{a} = \mathfrak{p}_3$ y

$$[\mathfrak{p}_2][\mathfrak{p}_3]^2 = [\mathfrak{p}_2\mathfrak{p}_3^2] = [\langle 2 - \sqrt{-14}\rangle] = 1.$$

Si tenemos en cuenta que $[\mathfrak{p}_2]^2 = [\langle 2\rangle] = 1$, la expresión anterior equivale a $[\mathfrak{p}_3]^2 = [\mathfrak{p}_2]$, de lo que se deduce que $[\mathfrak{p}_3]^4 = 1$.

Además,

$$[\mathfrak{p}_3\overline{\mathfrak{p}}_3] = [\langle 3\rangle] = 1 = [\mathfrak{p}_3]^4$$

que nos lleva a que $[\mathfrak{p}_3]^3 = [\overline{\mathfrak{p}}_3]$.

Si probamos que $[\mathfrak{p}_3]^2 \neq 1$, tendríamos que

$$H(\mathbb{Q}(\sqrt{-14})) = \{1,\, [\mathfrak{p}_3],\, [\mathfrak{p}_3]^2,\, [\mathfrak{p}_3]^3\}$$

es un grupo cíclico de orden 4 generado por $[\mathfrak{p}_3]$.

En efecto, si fuera $[\mathfrak{p}_3]^2 = [\mathfrak{p}_2] = 1$, sería que $\langle 2, \sqrt{-14}\rangle = \langle a + b\sqrt{-14}\rangle$ para ciertos a, $b \in \mathbb{Z}$, aplicando normas

$$2 = N(\langle 2, \sqrt{-14}\rangle) = a^2 + 14b^2$$

que no es posible.

Conclusiones

En esta memoria se ha presentado una introducción a uno de los temas clásicos de la teoría algebraica de números, como es la factorización única en anillos y hemos visto que el problema de determinar si existe o no factorización única en los anillos de enteros cuadráticos, se resuelve con el cálculo del grupo de clases de su cuerpo cuadrático.

Los resultados incluidos en la memoria se generalizan para enteros algebraicos de extensiones de $\mathbb{Q}$ de grado n. Precisamente, usando anillos formados por estos enteros, Lamé expone en 1847 lo que cree que es una demostración del último teorema de Fermat. De inmediato, Liuouville cuestiona un paso en la demostración en el que Lamé había supuesto que estos anillos siempre presentan factorización única. Recalcamos así la importancia de la existencia o no de factorización única.

Señalamos por último que, a pesar de obtener un algoritmo para el cálculo del número de clases y, en definitiva, para determinar si un anillo de enteros cuadráticos es dominio de factorización única o no, aún se está lejos de determinar qué anillos de enteros cuadráticos son de factorización única.

Es más, Gauss conjetura que existen infinitos cuerpos cuadráticos reales con número de clases uno. Esto sigue siendo hoy en día un problema abierto.

Apéndice A

Algoritmo para el cálculo del grupo de clases

Siguiendo los pasos del algoritmo expuesto en la Sección 3.4 del Capítulo 3, se implementa un programa que devuelve la factorización de todos los ideales principales generados por números primos enteros menores a la cota C_K. El proceso de factorización de dichos ideales se desarrolla a partir de los resultados obtenidos en la Sección 2.4 del Capítulo 2.

A continuación se muestra el código del programa. La eficacia del mismo no ha sido testada, quedando propuesto para futuros trabajos.

```
##############################################################################
#include <stdio.h>
#include <math.h>
int primo(int n){  // Comprueba la primalidad de un entero
   int cont=0, i=2;
   while((cont==0)&&(i<=(int)sqrt(n))){
       if(n%i==0)
           cont=cont + 1;
       i=i+1;
   };
   if(cont==0)
       return 1;
   else
       return 0;
}
int cuentaprimos(int m){ // Cuenta el número de primos menores a cierto natural dado
   int cont, i;
   for(i=2;i<m;i++){
       if (primo(i)==1)
           cont=cont+1;
   }
   return cont;
}
int disc(int m){ // Halla el discriminante dk
   if ((m%4==1)||(m%4==-3))
        return m;
```

```
    else
        return 4*m;
}
int legendre(int dk, int p){ // Determina el símbolo de Legendre
   int cont=0, i=1, a;
   if(dk%p==0)
       return 0;
   do{
       a=dk-pow(i,2);
       if (a%p==0){
              cont=cont + 1;
       }
       i=i+1;
   }while((cont==0)&&(i<p));
   if(cont==0)
       return -1;
   else
       return 1;
}
int raiz(int p, int m, int dk){ // Halla una raíz del polinomio mínimo de wk
   int a=p-1, r, cont=0, aux;
   if (dk==m){
       do{
           aux=pow(a,2);
           if(((aux - a + (1-m)/4)%p)==0){
               cont=cont+1;
               r=a;
           }
           a=a-1;
       }while((cont==0)&&(a>=0));
   }
   else{
       do{
           aux=pow(a,2);
           if(((aux -m)%p)==0){
               cont=cont+1;
               r=a;
           }
           a=a-1;
       }while((cont==0)&&(a>=0));
   }
   return r;
}
void factdos(int m){ //Factoriza el ideal <2>
   int resto;
   if(m<0)
       resto=m%8+8;
   else
       resto=m%8;
   if(resto%2==0)
       printf("<2> = <2 , w> <2 , w> = p^2");
   if((resto==3)||(resto==7))
       printf("<2> = <2 , w - 1> <2 , w - 1> = p^2");
   if((resto==1))
```

```
        printf("<2> = <2 , w> <2 , w'>");
    if((resto==5))
        printf("<2> = p  es primo");
}
void fact(int p, int dk, int m){ // Factoriza un ideal <p> con p primo impar
    int leg, r;
    leg=legendre(dk,p);
    if (leg==1){
        r=raiz(p, m, dk);
        printf("<%d> = <%d , w - %d> <%d , w' - %d> = pp'", p, p, r, p, r);
    }
    if (leg==0){
        r=raiz(p,m, dk);
        printf("<%d> = <%d , w - %d> <%d , w - %d> = p^2", p, p, r, p, r);
    }
    if (leg==-1)
        printf("<%d> = p   es primo", p, p);
}
void programa(int m, int dk, int Ck){
    int i, j=0, dim;
    printf("m= %d, dk= %d, Ck= %d \n\n", m, dk, Ck);
    dim=cuentaprimos(Ck);
    int vprimos[dim];
    for(i=2;i<Ck;i++){          // Se define un vector de primos menores a Ck
        if (primo(i)==1){
            vprimos[j]=i;
            j=j+1;
        }
    }
    for(i=0;i<dim;i++){
        printf("\n");
        if(vprimos[i]==2)
            factdos(m);
        else
            fact(vprimos[i],dk, m);
        printf("\n");
    }
}
main() {
    int m, dk, Ck;
    printf("Por favor, introduzca el entero libre de cuadrados m: ");
    scanf("%d",&m);
    dk=disc(m);
    Ck=fabs(sqrt(abs(dk)/3))+1;   // Se computa la cota Ck
    programa(m, dk, Ck);
}

################################################################################
```

Bibliografía

[1] Atiyah, M.F. & Macdonald, I.G.. (1989). *Introducción al álgebra conmutativa*. Barcelona, España: Reverté.

[2] Alaca, S. & Williams, K. S.. (2003). *Introductory Algebraic Number Theory*. Nueva York, Estados Unidos: Cambridge University Press.

[3] Lauret, E.. (Julio 2012). *Anillos de enteros de cuerpos cuadráticos*. Sitio web: http://www.mate.uncor.edu/∼elauret/articulos/2012-06-26-curso-elena-FINAL.pdf

[4] Conrad, K. *Factoring in Quadratic Fields*. Sitio web: http://www.math.uconn.edu/∼kconrad/blurbs/gradnumthy/quadraticgrad.pdf

[5] Ivorra, C. *Álgebra*. Sitio web: http://www.uv.es/ivorra/Libros/Algebra.pdf

[6] Elizondo, J. *Anillos de valuación discreta y de Dedekind*. Sitio web: http://www.math.unam.mx/javier/cap5.pdf