ANILLOS DE ENTEROS DE CUERPOS CUADRÁTICOS

EMILIO LAURET

RESUMEN. En este breve curso introduciremos una simple generalización del anillo de los números enteros llamado *anillo de enteros cuadráticos*. Veremos cómo se comporta su aritmética estudiando sus semejanzas y diferencias con los enteros racionales. Finalizaremos con el concepto de *número de clase* de un dominio de integridad el cual mide cuán lejos está de ser dominio de factorización única.

ÍNDICE

INTRODUCCIÓN

Como todos sabemos, el cuerpo de cocientes del anillo de números enteros $\mathbb{Z}$ es el cuerpo de los números racionales $\mathbb{Q}$. En este curso consideraremos extensiones cuadráticas de $\mathbb{Q}$, es decir, subcuerpos K de $\mathbb{C}$ de dimensión dos como espacios vectoriales sobre $\mathbb{Q}$. Dentro de cada uno de ellos definiremos su anillo de enteros $\mathcal{O}_K$, que resultará ser un $\mathbb{Z}$-módulo libre de rango dos.

Los anillos $\mathcal{O}_K$ conservan algunas propiedades de $\mathbb{Z}$, como por ejemplo que todo elemento no nulo y no inversible se factoriza como producto de irreducibles, aunque tal factorización no es única en general.

Los ejemplos más conocidos son los *enteros de Gauss*

$$\mathbb{Z}[\sqrt{-1}] = \mathbb{Z} + \mathbb{Z}\sqrt{-1}$$

2010 *Mathematics Subject Classification.* 11R11.

y los *enteros de Eisenstein*

$$\mathbb{Z}[\tfrac{1+\sqrt{-3}}{2}] = \mathbb{Z} + \mathbb{Z}\,\tfrac{1+\sqrt{-3}}{2},$$

en los cuales existe un algoritmo de división (dominios Euclídeos) tal como en $\mathbb{Z}$. En general éste no será el caso, ya que por ejemplo en el anillo

$$\mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$$

ni siquiera se puede factorizar de manera única. También son enteros cuadráticos los anillos $\mathbb{Z}[\sqrt{2}]$ y $\mathbb{Z}[\sqrt{5}]$, los cuales contienen infinitas unidades (elementos inversibles) a diferencia de $\mathbb{Z}$.

La principal similitud entre $\mathbb{Z}$ y $\mathcal{O}_K$ es que en ambos todo ideal se factoriza de manera única (salvo orden) como producto de ideales primos. Sin embargo, $\mathcal{O}_K$ no necesariamente es un dominio de ideales principales, por lo tanto esta propiedad no asegura la factorización única de elementos.

Finalizaremos con el difícil concepto de *número de clase* de un anillo $\mathcal{O}_K$, tema en el que existen diversos problemas abiertos de enunciado entendible. Este número mide por cuánto el anillo $\mathcal{O}_K$ no es un dominio de factorización única.

Estos cuerpos K de grado dos sobre $\mathbb{Q}$ son un caso particular de los *cuerpos de números* (subcuerpos de $\mathbb{C}$ de dimensión finita con respecto a $\mathbb{Q}$). Además, sus respectivos anillos de enteros $\mathcal{O}_K$ son en particular lo que se llama *Dominios de Dedekind*, principal objeto de estudio en cualquier curso de *teoría algebraica de números*. Existe una vasta bibliografía que trata sobre ellos. Recomendamos los textos de Narasimhan [4] y Alaca-Williams [1]. Diversos ejemplos y pruebas fueron extraídos de las notas de Pacharoni [5] y Conrad [2].

Le agradezco a Fiorela Rossi Bertone por revisar las notas y al Comité Organizador del *VI Encuentro Nacional de Álgebra* por la invitación para dar el curso.

1. Aritmética en cuerpos cuadráticos

1.1. Cuerpos cuadráticos. Todo subcuerpo K de los números complejos $\mathbb{C}$ contiene al cuerpo de los números racionales $\mathbb{Q}$. Esto vale pues como el elemento 1 está en K, entonces

$$\pm m = \pm(\underbrace{1 + \cdots + 1}_{m \text{ veces}}) \in K,$$

es decir, los números enteros están contenidos en K, por lo tanto su cuerpo de cocientes —el cual es precisamente $\mathbb{Q}$— también lo está. Luego todo subcuerpo de $\mathbb{C}$ se puede ver como un espacio vectorial sobre $\mathbb{Q}$, lo que permite la siguiente definición con la que trabajaremos de aquí en más.

Definición 1.1. Llamaremos —en este curso— un *cuerpo cuadrático* a un subcuerpo de $\mathbb{C}$ de dimensión dos como $\mathbb{Q}$-espacio vectorial.

Para $\alpha \in \mathbb{C}$ denotaremos $\mathbb{Q}[\alpha] = \{g(\alpha) \in \mathbb{C} : g(x) \in \mathbb{Q}[x]\}$ y diremos que $f(x) \in \mathbb{Q}[x]$ es su *polinomio minimal* si es mónico, anula a α y es de grado mínimo con esta propiedad. Dicho polinomio es único e irreducible sobre $\mathbb{Q}$ (Ejercicio 1).

Sea K un cuerpo cuadrático. Si $\alpha \in \mathbb{Q} \subset K$ entonces su polinomio minimal es $x - \alpha$. Tomemos $\alpha \in K \smallsetminus \mathbb{Q}$, entonces $\{1, \alpha\}$ es una $\mathbb{Q}$-base de K, en particular $K = \mathbb{Q}[\alpha]$. Como $\alpha^2 \in K$ existen coeficientes $q, r \in \mathbb{Q}$ tales que

$$\alpha^2 = q \cdot \alpha + r \cdot 1,$$

o equivalentemente

$$f(x) = x^2 - qx - r \tag{1.1}$$

es el polinomio minimal de α (Ejercicio 2).

Proposición 1.2. *Todos los cuerpos cuadráticos son de la forma*

$$\mathbb{Q}[\sqrt{m}] = \mathbb{Q} + \mathbb{Q}\sqrt{m},$$

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

Demostración. Dado $m \in \mathbb{Z}$ libre de cuadrados, fácilmente podemos ver que $\mathbb{Q}[\sqrt{m}]$ es un cuerpo cuadrático y que son no isomorfos de a pares (Ejercicio 3). Veamos ahora que son todos. Sean K un cuerpo cuadrático y $\alpha \in K \setminus \mathbb{Q}$, entonces $K = \mathbb{Q}[\alpha]$. Como $\dim_{\mathbb{Q}}(K) = 2$ tenemos que $1, \alpha, \alpha^2$ son linealmente dependientes, por lo tanto existen $a, b, c \in \mathbb{Q}$ tales que $a \neq 0$ y

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

Sin pérdida de la generalidad, podemos suponer que $a, b, c \in \mathbb{Z}$. Multiplicando por $4a$ tenemos que

$$(2a\alpha + b)^2 = b^2 - 4ac.$$

Denotemos $\beta = 2a\alpha + b$ y $n = b^2 - 4ac \in \mathbb{Z}$. Luego $\mathbb{Q}[\sqrt{n}] \subset \mathbb{Q}[\beta]$ y $\mathbb{Q}[\beta] = K$. Además $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{n}] = 2$ por lo que $K = \mathbb{Q}[\sqrt{n}]$. Finalmente, $K = \mathbb{Q}[\sqrt{m}]$ donde $n = k^2 m$ con $m \in \mathbb{Z}$ libre de cuadrados. □

A partir de ahora, a menos que aclaremos lo contrario, cuando escribamos $\mathbb{Q}[\sqrt{m}]$ estaremos asumiendo que m es un entero libre de cuadrados, por lo tanto $\mathbb{Q}[\sqrt{m}]$ es un cuerpo cuadrático.

Definición 1.3. Un cuerpo cuadrático $K = \mathbb{Q}[\sqrt{m}]$ es llamado *real* si $K \subset \mathbb{R}$ ($\iff$ $m > 0$) e *imaginario* si $K \nsubseteq \mathbb{R}$ ($\iff$ $m < 0$).

Sea $\sigma : \mathbb{Q}[\sqrt{m}] \to \mathbb{Q}[\sqrt{m}]$ definido por $\sigma(1) = 1$ y $\sigma(\sqrt{m}) = -\sqrt{m}$ extendiendo de manera $\mathbb{Q}$-lineal. Se ve que σ es un morfismos de cuerpos (Ejercicio 4). Si $\alpha \in \mathbb{Q}[\sqrt{m}]$ llamaremos a $\sigma(\alpha)$ el *conjugado* de α y lo denotaremos por α'. Observemos que si $m < 0$ entonces el conjugado coincide con el conjugado complejo (Ejercicio 4) y que el mapeo identidad y σ son los únicos morfismos de cuerpos de $\mathbb{Q}[\sqrt{m}]$ a $\mathbb{C}$. En otras palabras, σ es el elemento no trivial del grupo de Galois de la extensión $\mathbb{Q} \subset \mathbb{Q}[\sqrt{m}]$.

Si $\alpha = r + s\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ denotamos

$$\mathrm{Tr}_K(\alpha) = \alpha + \alpha' = 2r \qquad \text{y} \qquad \mathrm{N}_K(\alpha) = \alpha\alpha' = p^2 - mr^2.$$

Abreviaremos por $\mathrm{Tr}(\alpha)$ y $\mathrm{N}(\alpha)$ cuando no quepa lugar a dudas. El operador Tr resulta aditivo y N multiplicativo (Ejercicio 5). Notemos que

$$\begin{aligned} \alpha^2 = (r + s\sqrt{m})^2 &= r^2 + ms^2 + 2rs\sqrt{m} \\ &= -r^2 + ms^2 + 2r(r + s\sqrt{m}) \\ &= 2r\alpha - (r^2 - ms^2), \end{aligned}$$

por lo tanto

$$f(x) := x^2 + \mathrm{Tr}(\alpha)\, x - \mathrm{N}(\alpha) \tag{1.2}$$

anula a α, es mónico y de grado dos. Esto nos asegura que si $\alpha \notin \mathbb{Q}$ entonces $f(x)$ es su polinomio minimal.

Se puede definir la traza y la norma como sigue. Para $\alpha \in K$, el mapeo $L_\alpha : K \to K$ de multiplicar por izquierda, i. e. $L_\alpha(\beta) = \alpha\beta$, es una transformación lineal del $\mathbb{Q}$-espacio vectorial K. Entonces (Ejercicio 6)

$$\mathrm{Tr}(\alpha) = \mathrm{Tr}(L_\alpha) \quad \text{y} \quad \mathrm{N}(\alpha) = \mathrm{Tr}(L_\alpha). \tag{1.3}$$

1.2. Enteros cuadráticos.

Definición 1.4. Un número complejo α se dice un *entero algebraico* si es raíz de un polinomio mónico en $\mathbb{Z}[x]$.

Se puede ver que los enteros algebraicos forman un anillo (Ejercicio 7). Luego también lo hace el conjunto de *enteros cuadráticos* $\mathcal{O}_K$ formado por los enteros algebraicos en un cuerpo cuadrático K. Más aún, $\mathcal{O}_K$ es un *dominio de integridad*, es decir, un anillo conmutativo con unidad sin divisores de cero.

Nuestro siguiente paso es determinar $\mathcal{O}_K$ para cuerpos cuadráticos K. Es claro que $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ (Ejercicio 8). Para $\alpha \in \mathbb{C}$ denotemos $\mathbb{Z}[\alpha] = \{g(\alpha) \in \mathbb{C} : g(x) \in \mathbb{Z}[x]\}$. Se prueba que $\mathbb{Z}[\sqrt{m}] \subset \mathcal{O}_K$ (Ejercicio 8). El siguiente resultado determina completamente a $\mathcal{O}_K$.

Proposición 1.5. *Sea $K = \mathbb{Q}[\sqrt{m}]$. Entonces*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{si } m \equiv 2, 3 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & \text{si } m \equiv 1 \pmod 4. \end{cases}$$

Observación 1.6. Notemos que

$$\mathbb{Z}[\sqrt{m}] = \mathbb{Z} + \sqrt{m}\,\mathbb{Z} = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\},$$
$$\mathbb{Z}[\tfrac{1+\sqrt{m}}{2}] = \mathbb{Z} + \tfrac{1+\sqrt{m}}{2}\,\mathbb{Z} = \left\{ \tfrac{a+b\sqrt{m}}{2} : a, b \in \mathbb{Z},\ a \equiv b \pmod 2 \right\}$$

con $m \equiv 1 \pmod 4$ en el segundo caso.

Demostración. Un número complejo es algebraico si y sólo si su polinomio minimal tiene coeficientes enteros (Ejercicio 9). Si $\alpha \in K \setminus \mathbb{Q}$, hemos visto que su polinomio minimal está dado por (1.2). Luego, si $m \equiv 2, 3 \pmod 4$ y $\alpha = r + s\sqrt{m} \in K$, entonces $\alpha \in \mathcal{O}_K$ si y sólo si $\mathrm{Tr}(\alpha) = 2r \in \mathbb{Z}$ y $\mathrm{N}(\alpha) = r^2 - ms^2 \in \mathbb{Z}$. Supongamos que $r \notin \mathbb{Z}$, entonces $s \notin \mathbb{Z}$. Escribimos $r = r_1/2$ y $s = s_1/2$ con r_1 y s_1 impares, entonces $(r_1^2 - ms_1^2)/4 \in \mathbb{Z}$ o equivalentemente $r_1^2 \equiv ms_1^2 \pmod 4$. Como r_1 y s_1 son impares, $r_1^2 \equiv s_1^2 \equiv 1 \pmod 4$, lo cual nos lleva a una contradicción ya que $m \not\equiv 1 \pmod 4$. Luego r y s son enteros racionales y queda probado el primer caso.

Ahora supongamos $m \equiv 1 \pmod 4$ y tomemos $\alpha = r + s\sqrt{m} \in K$. Como antes, $\alpha \in \mathcal{O}_K$ si y sólo si $2r \in \mathbb{Z}$ y $r^2 - ms^2 \in \mathbb{Z}$. Esto último resulta equivalente a $r, s \in \mathbb{Z}$ o $r, s \in \mathbb{Z} + \frac{1}{2} := \{a + \frac{1}{2} : a \in \mathbb{Z}\}$. Finalmente notemos que

$$\begin{aligned} \alpha = r + s\sqrt{m} &= r + s\left(2\,\frac{1+\sqrt{m}}{2} - 1\right) \\ &= (r - s) + (2s)\,\frac{1+\sqrt{m}}{2}, \end{aligned}$$

por lo que $\alpha \in \mathcal{O}_K$ si y sólo si $r - s, 2s \in \mathbb{Z}$. □

Los enteros algebraicos $\mathbb{Z}[\sqrt{-1}]$ son comúnmente llamados *enteros de Gauss* y *enteros de Eisenstein* los de $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. Por comodidad denotaremos para $K=\mathbb{Q}[\sqrt{m}]$,

$$\omega_K = \begin{cases} \sqrt{m} & \text{si } m \equiv 2,3 \pmod 4, \\ \dfrac{1+\sqrt{m}}{2} & \text{si } m \equiv 1 \pmod 4, \end{cases} \tag{1.4}$$

por lo tanto tenemos que

$$\mathcal{O}_K = \mathbb{Z} + \omega_K \mathbb{Z}. \tag{1.5}$$

Se puede ver que $\mathrm{Tr}(\alpha)$ y $\mathrm{N}(\alpha)$ son enteros racionales si α es entero algebraico (Ejercicio 10).

1.3. Elementos destacados en $\mathcal{O}_K$. A continuación estudiaremos los conceptos de elementos inversibles, irreducibles y primos en los enteros cuadráticos $\mathcal{O}_K$, comparándolos con los propios de $\mathbb{Z}$.

Recordemos las siguientes definiciones en un dominio de integridad A:

- ε se llama *unidad* si existe $v \in A$ tal que $\varepsilon v = 1_A$ (se denota $v = \varepsilon^{-1}$);
- γ se llama *irreducible* si es no nulo, no es unidad y $\gamma = \alpha\beta$ implica que α o β es una unidad;
- π se llama *primo* si es no nulo, no es unidad y si $\pi \mid \alpha\beta$ entonces $\pi \mid \alpha$ o $\pi \mid \beta$.

Comencemos estudiando el conjunto $\mathcal{O}_K^\times$ de unidades de $\mathcal{O}_K$ para $K=\mathbb{Q}[\sqrt{m}]$. Supongamos que ε es una unidad, entonces

$$1 = \mathrm{N}(1) = \mathrm{N}(\varepsilon\varepsilon^{-1}) = \mathrm{N}(\varepsilon)\mathrm{N}(\varepsilon^{-1})$$

por lo tanto $\mathrm{N}(\varepsilon)$ es una unidad en $\mathbb{Z}$, es decir $\mathrm{N}(\varepsilon) = \pm 1$. Más aún, la recíproca es cierta ya que si $\pm 1 = \mathrm{N}(\varepsilon) = \varepsilon\varepsilon'$ entonces $\varepsilon^{-1} = \pm\varepsilon' \in \mathcal{O}_K$. Podemos enunciar lo siguiente:

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

Ejemplo 1.7. Con esta equivalencia calcularemos $\mathcal{O}_K^\times$ para cuerpos cuadráticos imaginarios $K=\mathbb{Q}[\sqrt{m}]$ $(m<0)$. Supongamos $m \equiv 2,3 \pmod 4$, por lo tanto $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$. Entonces $\varepsilon = a + b\sqrt{m} \in \mathcal{O}_K^\times$ $(a,b \in \mathbb{Z})$ si y sólo si

$$\mathrm{N}(\varepsilon) = a^2 - mb^2 = \pm 1.$$

Esto nos dice que $\mathbb{Z}[\sqrt{-1}]^\times = \{\pm 1, \pm\sqrt{-1}\}$ y $\mathbb{Z}[\sqrt{m}]^\times = \{\pm 1\}$ para $m \neq -1$.

Ahora tomemos $m \equiv 1 \pmod 4$, por lo tanto $\varepsilon = \frac{a+b\sqrt{m}}{2} \in \mathbb{Z}[\frac{1+\sqrt{m}}{2}]^\times$ $(a,b \in \mathbb{Z},\ a \equiv b \pmod 2)$ si y sólo si

$$\mathrm{N}(\varepsilon) = \frac{a^2 - mb^2}{4} = \pm 1.$$

Luego $\mathbb{Z}[m]^\times = \{\pm 1\}$ para $m \neq -3$ y $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]^\times = \left\{\pm 1,\ \pm\frac{1+\sqrt{-3}}{2},\ \pm\frac{1-\sqrt{-3}}{2}\right\}$.

El caso de cuerpos cuadráticos reales $K=\mathbb{Q}[\sqrt{m}]$ $(m>0)$ es muy diferente. Por ejemplo, notemos que $1+\sqrt{2}$ es una unidad de $\mathbb{Z}[\sqrt{2}]$ al igual que todas sus potencias, las cuales son distintas (Ejercicio 11), es decir, $\mathbb{Z}[\sqrt{2}]$ tiene infinitas unidades. Es notable esta diferencia con el caso imaginario en el que, como acabamos de ver, siempre existe una cantidad finita de unidades.

Supongamos que $m \equiv 2, 3 \pmod 4$. Notemos que si $\varepsilon = x + y\sqrt{m} \in \mathcal{O}_K$ $(x, y \in \mathbb{Z})$, entonces $\mathrm{N}(\varepsilon) = (x + y\sqrt{m})(x - y\sqrt{m}) = 1$ si y sólo si (x, y) es una solución de la *ecuación de Pell*

$$x^2 - my^2 = 1. \tag{1.6}$$

Luego, las soluciones de la ecuación de Pell están en correspondencia con las unidades en $\mathcal{O}_K$ de norma 1. En varios casos no existen unidades de norma -1, e. g. $m = 3$ (Ejercicio 12), por lo que la correspondencia llegaría a todas las unidades de $\mathcal{O}_K$.

Para cerrar el tema de las unidades en $\mathcal{O}_K$ para cuerpos cuadráticos reales K, enunciaremos el teorema que las caracteriza. Para la demostración de este teorema y un amplio estudio del tema, sugerimos ver el Capítulo 11 de [1].

Teorema 1.8. *Sea K un cuerpo cuadrático real y sea ε la menor unidad de $\mathcal{O}_K$ mayor a 1* (unidad fundamental)*. Entonces*

$$\mathcal{O}_K^\times \;=\; \{\pm\varepsilon^n : n \in \mathbb{Z}\}.$$

Ahora estudiemos los elementos irreducibles en $\mathcal{O}_K$. Supongamos que $\gamma \in \mathcal{O}_K$ es tal que $\mathrm{N}(\gamma) = p$ es un primo racional no necesariamente positivo. Si escribimos $\gamma = \alpha\beta$, entonces $p = \mathrm{N}(\alpha)\mathrm{N}(\beta)$ lo que implica que $\mathrm{N}(\alpha)$ o $\mathrm{N}(\beta)$ es ± 1, o equivalentemente α o β es unidad por (♣). Esto nos permite enunciar lo siguiente:

(♠) *si $\gamma \in \mathcal{O}_K$ satisface que $\mathrm{N}(\gamma) = p$ es primo en $\mathbb{Z}$, entonces γ es irreducible.*

Sin embargo la recíproca no es verdadera tal como lo muestra el siguiente ejemplo.

Ejemplo 1.9. El elemento 3 es irreducible en $\mathbb{Z}[\sqrt{-1}]$ mas $\mathrm{N}(3) = 9$. En efecto, si $3 = \alpha\beta$, tomando norma en ambos miembros obtenemos que $9 = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, lo cual implica que $\mathrm{N}(\alpha) \in \{\pm 1, \pm 3, \pm 9\}$. Pero $\mathrm{N}(\alpha) \geq 0$, si $\mathrm{N}(\alpha) = 1$ entonces α es unidad, si $\mathrm{N}(\alpha) = \pm 9$ entonces β es unidad, y $\mathrm{N}(\alpha)$ no puede valer 3 (Ejercicio 13), por lo tanto 3 es irreducible.

Es sabido que en un dominio de integridad, todo elemento primo es irreducible. Además, la recíproca es cierta en $\mathbb{Z}$ (más generalmente en todo dominio de ideales principales), pero no lo es en general en $\mathcal{O}_K$.

Ejemplo 1.10. El número 3 es un elemento irreducible en $\mathbb{Z}[\sqrt{-14}]$ (Ejercicio 14) que divide a $15 = (1 + \sqrt{-14})(1 - \sqrt{-14})$ pero no a $1 \pm \sqrt{-14}$. En general, un entero racional $c \in \mathbb{Z}$ divide un entero cuadrático $\alpha = a + b\omega_K$ $(a, b \in \mathbb{Z})$ si y sólo si c divide a a y b en $\mathbb{Z}$. Luego 3 no es primo en $\mathbb{Z}[\sqrt{-14}]$.

1.4. Factorización en $\mathcal{O}_K$. Recordemos las diferentes definiciones relacionadas con la factorización en un dominio de integridad A.

- A se dice de *factorización* si todo elemento α no nulo, no unidad, puede escribirse como $\alpha = \gamma_1 \dots \gamma_n$ con $\gamma_1, \dots, \gamma_n$ elementos irreducibles.
- A se dice *dominio de factorización única* (DFU) si es de factorización y además si $\alpha = \gamma_1 \dots \gamma_n = \delta_1 \dots \delta_m$ (γ_i, δ_i irreducibles) entonces $n = m$ y existe una permutación s de n elementos tal que γ_i es asociado a $\delta_{s(i)}$ para todo i (i. e. existe ε_i unidad tal que $\varepsilon_i\gamma_i = \delta_{s(i)}$).
- A se dice *dominio de ideales principales* (DIP) si todo ideal de A es principal, es decir, generado por un elemento.
- A se dice *dominio Euclídeo* (DE) si existe $\varphi : A \smallsetminus \{0\} \to \mathbb{N}$ tal que
  (i) si $\alpha, \beta \in A \smallsetminus \{0\}$ entonces $\varphi(\alpha) \leq \varphi(\alpha\beta)$;

(ii) si $\alpha, \beta \in A$ y $\beta \neq 0$ entonces existen $q, r \in A$ tales que $\alpha = \beta q + r$ donde $r = 0$, o $r \neq 0$ y $\varphi(r) < \varphi(\alpha)$.

Probemos primero que el anillo de enteros $\mathcal{O}_K$ de un cuerpo cuadrático K es de factorización a partir del siguiente enunciado:

($\heartsuit$) *todo $0 \neq \alpha \in \mathcal{O}_K$ no unidad se factoriza como producto de irreducibles en $\mathcal{O}_K$.*

Demostración. Si $\alpha \in \mathcal{O}_K$ no es nulo ni unidad, tiene un divisor irreducible γ_1 (Ejercicio 15), entonces $\alpha = \gamma_1\alpha_1$ con $1 \leq \mathrm{N}(\alpha_1) < \mathrm{N}(\alpha)$. Si α_1 no es irreducible y no es unidad —i.e. $\mathrm{N}(\alpha_1) \neq 1$— entonces $\alpha_1 = \gamma_2\alpha_2$, con γ_2 irreducible, obteniendo así una sucesión decreciente de números naturales $\mathrm{N}(\alpha)$, $\mathrm{N}(\alpha_1)$, $\mathrm{N}(\alpha_2), \ldots$, la cual en algún momento debe estabilizarse en 1, digamos $\mathrm{N}(\alpha_j) = 1$. Por lo tanto $\alpha = \gamma_1 \ldots \gamma_j\alpha_j$ con $\gamma_1, \ldots, \gamma_{j-1}, \gamma_j\alpha_j$ elementos irreducibles. □

Sin embargo, dicha factorización en $\mathcal{O}_K$ puede no ser única (salvo orden y unidades). En general, $\mathcal{O}_K$ no es DFU, más aún, la cantidad de elementos irreducibles en una factorización de un entero puede no ser siempre la misma.

Ejemplo 1.11. Notemos que

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

Ya vimos que 3 es irreducible en $\mathbb{Z}[\sqrt{-14}]$ (Ejercicio 14). Veamos que $5 \pm 2\sqrt{-14}$ también lo son. Ambos tienen norma igual a 81, por lo tanto si suponemos que $5 \pm 2\sqrt{-14} = \alpha\beta$ entonces $\mathrm{N}(\alpha) \in \{1, 3, 9, 27, 81\}$. Si escribimos $\alpha = a+b\sqrt{-14} \in \mathbb{Z}[\sqrt{-14}]$ tenemos

$$\mathrm{N}(\alpha) = a^2 + 14b^2.$$

Claramente $\mathrm{N}(\alpha) \neq 3, 27$. Además, los únicos elementos en $\mathbb{Z}[\sqrt{-14}]$ con norma igual a 9 son ± 3, los cuales no dividen a $5 \pm 2\sqrt{-14}$. Finalmente obtenemos que $\mathrm{N}(\alpha) = 1$ o $\mathrm{N}(\alpha) = 81$, es decir, α o β es unidad, por lo tanto $5 \pm 2\sqrt{-14}$ es irreducible.

Sabemos que todo dominio de ideales principales es un dominio de factorización única. Para nuestros anillos $\mathcal{O}_K$ con K un cuerpo cuadrático, la recíproca es cierta, lo cual demostraremos más adelante (Teorema 2.13). En particular $\mathbb{Z}[\sqrt{-14}]$ no es un dominio de ideales principales por Ejemplo 1.11.

Ejemplo 1.12. Veamos que el ideal $\mathfrak{a} = 2\mathcal{O}_K + \sqrt{-14}\mathcal{O}_K$ no es principal en $\mathbb{Z}[\sqrt{-14}]$. Supongamos que $\mathfrak{a} = \alpha\mathcal{O}_K$ para algún $\alpha \in \mathcal{O}_K$. Tenemos que $\alpha \mid 2$ entonces existe $\beta \in \mathcal{O}_K$ tal que $2 = \alpha\beta$. Tomando norma a ambos lados obtenemos que $4 = \mathrm{N}(\alpha)\mathrm{N}(\beta)$. De la misma manera, como $\alpha \mid \sqrt{-14}$ resulta que $\mathrm{N}(\alpha)$ divide a $\mathrm{N}(\sqrt{-14}) = 14$, por lo tanto $\mathrm{N}(\alpha)$ es 1 o 2. Escribiendo $\alpha = a + b\sqrt{-14}$ tenemos que $\mathrm{N}(\alpha) = a^2 + 14b^2 \neq 2$, entonces $\mathrm{N}(\alpha) = 1$. Así $\mathfrak{a} = \alpha\mathcal{O}_K = \mathcal{O}_K$ lo cual no es cierto.

Finalizaremos esta sección considerando los dominios Euclídeos. Supongamos que K es un cuerpo cuadrático imaginario, entonces es posible probar que $\mathcal{O}_K$ es dominio Euclídeo con respecto a una función $\varphi(\cdot)$ si y sólo si lo es con respecto a $\mathrm{N}(\cdot)$. Esto nos permite usar la siguiente propiedad

($\diamondsuit$) $\mathcal{O}_K$ *es DE con* $|\mathrm{N}(\cdot)|$ *si y sólo si* $\forall\, x \in K\ \exists \alpha \in \mathcal{O}_K$ *tal que* $\mathrm{N}(x - \alpha) < 1$.

La siguiente demostración, al igual que muchas otras, se encuentra en [5]. Además [1] recorre el tema exhaustivamente.

Demostración. Supongamos que $\mathcal{O}_K$ es dominio Euclídeo. Si $x \in K$ existe $c \in \mathbb{N}$ tal que $cx \in \mathcal{O}_K$, por lo tanto existen $\alpha, \gamma \in \mathcal{O}_K$ tales que $cx = c\alpha + \gamma$ con $|\mathrm{N}(\gamma)| < |\mathrm{N}(c)|$. Esto implica $|\mathrm{N}(x - \alpha)| = |\mathbb{N}(\gamma)|/|\mathrm{N}(c)| < 1$.

Recíprocamente, dados $\alpha \neq 0$ y β en $\mathcal{O}_K$, existe $x \in K$ tal que $|\mathrm{N}(\beta/\alpha - x)| < 1$, entonces $\beta = x\alpha + (\beta - x\alpha)$ y $|\mathrm{N}(\beta - x\alpha)| < |\mathrm{N}(\alpha)|$. □

Ejemplo 1.13. Usando ($\diamondsuit$) se puede probar (Ejercicio 16) que el anillo de enteros $\mathcal{O}_K$ de un cuerpo cuadrático imaginario $K = \mathbb{Q}[\sqrt{m}]$ ($m < 0$) es dominio Euclídeo si y sólo si

$$m = -1, -2, -3, -7, -11.$$

Ejemplo 1.14. Similarmente, el anillo de enteros $\mathcal{O}_K$ de un cuerpo cuadrático real $K = \mathbb{Q}[\sqrt{m}]$ ($m > 0$) es dominio Euclídeo con respecto a $|N(\cdot)|$ si y sólo si

$$m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Sin embargo no podemos afirmar que los enteros positivos libres de cuadrados m que no están en esta lista no sean dominio Euclídeos para alguna función $\varphi(\cdot)$. Por ejemplo para $m = 69$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{69}}{2}]$ es dominio Euclídeo con respecto a la función

$$\varphi(a + b\omega_K) = \begin{cases} |a^2 + ab - 17b^2| & \text{si } (a,b) \neq (10,3), \\ 26 & \text{si } (a,b) = (10,3). \end{cases}$$

Más aún, el número 26 puede ser reemplazado por cualquier entero mayor o igual a 26, por lo que $\mathbb{Z}[\frac{1+\sqrt{69}}{2}]$ es dominio Euclídeo con respecto a infinitas funciones distintas. El anillo $\mathbb{Z}[\sqrt{14}]$ también resulta dominio Euclídeo con respecto a una función distinta de $|\mathrm{N}(\cdot)|$.

Recomendamos [1] para ampliar el tema, en particular su *suggested reading* al final de Capítulo 2.

1.5. Ejercicios.

1. Sea $\alpha \in \mathbb{C}$ y $f(x)$ su polinomio minimal.
   a) Probar que $f(x)$ es irreducible en $\mathbb{Q}[x]$, es decir, si $f(x) = g(x)h(x)$ con $g(x), h(x) \in \mathbb{Q}[x]$, entonces $g(x)$ o $h(x)$ es constante.
   b) Probar que el conjunto de polinomios en $\mathbb{Q}[x]$ que anulan a α es el ideal generado por $f(x)$.
2. Sea $f(x) \in \mathbb{Q}[x]$ de grado dos. Probar que $f(x)$ es irreducible en $\mathbb{Q}[x]$ si y sólo si no tiene raíces racionales.
3. Sean m y n enteros libres de cuadrados distintos.
   a) Probar que $\mathbb{Q}[\sqrt{m}]$ es un cuerpo.
   b) Probar que 1 y $\sqrt{m}$ son linealmente independientes sobre $\mathbb{Q}$. Concluir que $\mathbb{Q}[\sqrt{m}]$ es un cuerpo cuadrático.
   c) Probar que $\mathbb{Q}[\sqrt{m}]$ y $\mathbb{Q}[\sqrt{n}]$ son no isomorfos. Ayuda: considerar la ecuación $\sqrt{m} = a + b\sqrt{n}$ con $a, b \in \mathbb{Q}$.
4. Sea $\sigma : \mathbb{Q}[\sqrt{m}] \to \mathbb{Q}[\sqrt{m}]$ dado por $\sigma(1) = 1$ y $\sigma(\sqrt{m}) = -\sqrt{m}$.
   a) Probar que σ es un isomorfismo de cuerpos.
   b) Probar que todos los morfismos de $\mathbb{Q}[\sqrt{m}]$ a $\mathbb{C}$ son Id y σ.
   c) Probar que si $m < 0$ entonces $\sigma(\alpha) = \overline{\alpha}$, donde la barra denota el conjugado complejo.
5. Probar que $\mathrm{Tr}(\alpha+\beta) = \mathrm{Tr}(\alpha)+\mathrm{Tr}(\beta)$ y $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$ para $\alpha, \beta \in \mathbb{Q}[\sqrt{m}]$.
6. Probar (1.3).

7. Probar los siguientes hechos.
   a) α es entero algebraico si y sólo si $\mathbb{Z}[\alpha]$ es finitamente generado como $\mathbb{Z}$-módulo.
   b) Si α y β son enteros algebraicos entonces también lo son $\alpha+\beta$ y $\alpha\beta$. Concluir que el conjunto de enteros algebraicos forman un subanillo de $\mathbb{C}$.
   c) Para todo $\alpha \in \mathbb{C}$ que es anulado por algún polinomio en $\mathbb{Q}[x]$ (*número algebraico*) existe $m \in \mathbb{Z}$ tal que $m\alpha$ es entero algebraico.
8. Probar las siguientes afirmaciones.
   a) Todo entero racional es entero algebraico.
   b) Los únicos números racionales que son enteros algebraicos son los enteros racionales.
   c) Los elementos en $\mathbb{Z}[\sqrt{m}] = \mathbb{Z} + \sqrt{m}\mathbb{Z}$ son enteros algebraicos.
9. Un polinomio $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ se dice *primitivo* si el máximo común divisor de $\{a_0, \ldots, a_n\}$ es 1. Probar los siguientes hechos.
   a) (*Lema de Gauss*) El producto de dos polinomios primitivos es primitivo.
   b) α es entero algebraico si y sólo si su polinomio minimal vive en $\mathbb{Z}[x]$.
10. Probar que $\mathrm{Tr}(\alpha), \mathrm{N}(\alpha) \in \mathbb{Z}$ para todo $\alpha \in \mathcal{O}_K$.
11. Probar que $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ y $(1+\sqrt{2})^n \neq 1$ para todo $n \neq 0$.
12. Probar que todas las unidades de $\mathbb{Z}[\sqrt{3}]$ tienen norma 1.
13. Probar que $\mathrm{N}(\alpha) \neq 3$ para todo $\alpha \in \mathbb{Z}[\sqrt{-1}]$.
14. Probar que 3 es un elemento irreducible en $\mathbb{Z}[\sqrt{-14}]$.
15. Probar que todo elemento no nulo y no unidad en $\mathcal{O}_K$ es divisible por un elemento irreducible en $\mathcal{O}_K$. [Ayuda: si $\gamma = \alpha\beta$ con $1 < \mathrm{N}(\alpha) < \mathrm{N}(\gamma)$, y α no es irreducible, entonces repitiendo el procedimiento, probar que en algún momento debe estabilizarse].
16. Probar la afirmación de Ejemplo 1.13. [Ayuda: ver [1, Thm. 2.2.3 y 2.2.5]]
17. Probar la afirmación de Ejemplo 1.14 únicamente para $m = 2, 3, 6$. [Ayuda: ver [1, Thm. 2.2.8]]

2. Teorema de factorización única de ideales

2.1. Ideales. Tomemos $\mathfrak{a}$ un ideal no nulo en $\mathcal{O}_K$, donde K como siempre denota un cuerpo cuadrático. Primero veamos que siempre contiene un entero racional no nulo. Sean $\alpha \in \mathfrak{a} \smallsetminus \{0\}$ y $f(x) = x^2 + bx + c \in \mathbb{Z}[x]$ su polinomio minimal. Notemos que $c \neq 0$ pues $f(x)$ es irreducible en $\mathbb{Q}[x]$. Como $f(\alpha) = 0$, tenemos

$$c = -\alpha\,(\alpha + b) \in \mathfrak{a},$$

por lo tanto $c \in \mathfrak{a} \cap \mathbb{Z}$. Además $\mathfrak{a} \cap \mathbb{Z}$ es un ideal de $\mathbb{Z}$, entonces $\mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$ para algún $a \in \mathbb{Z}$.

Sea $\mathfrak{p}$ un ideal primo no nulo de $\mathcal{O}_K$. Veamos que $\mathfrak{p}$ contiene exactamente un primo racional. Sea $a \in \mathfrak{p} \cap \mathbb{Z}$ y $a = p_1 \ldots p_k \in \mathbb{Z}$ su descomposición en primos (racionales), entonces como $\mathfrak{p}$ es un ideal primo tenemos que $p_i \in \mathfrak{p}$ para algún i. Ahora supongamos que p y q son dos primos distintos en $\mathfrak{p}$. Por ser coprimos existen $r, s \in \mathbb{Z}$ tales que $1 = pr + qs \in \mathfrak{p}$, por lo tanto $\mathcal{O}_K = \mathfrak{p}$, lo que contradice la hipótesis. Luego $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ para exactamente un primo racional $p \in \mathbb{Z}$.

Denotaremos $\langle \alpha_1, \ldots, \alpha_m \rangle$ al ideal generado por $\alpha_1, \ldots, \alpha_m$ en $\mathcal{O}_K$, es decir,

$$\langle \alpha_1, \ldots, \alpha_m \rangle = \alpha_1 \mathcal{O}_K + \cdots + \alpha_m \mathcal{O}_K.$$

Sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$. Recordemos que $\mathcal{O}_K = \mathbb{Z} + \omega_K \mathbb{Z}$ por Proposición 1.2, donde ω_K está dado por (1.4). En particular, $\mathfrak{a}$ es un $\mathbb{Z}$-submódulo de $\mathcal{O}_K$ de rango dos

(Ejercicio 1). Luego, por el teorema de subgrupos de grupos abelianos libres, existen $a, b, c \in \mathbb{Z}$, $a, c > 0$, tales que

$$\mathfrak{a} = a\mathbb{Z} + (b + c\,\omega_K)\mathbb{Z}. \tag{2.1}$$

En particular $\mathfrak{a} = \langle a, \alpha \rangle$ con $\alpha := b + c\,\omega_K$, es decir, todo ideal no nulo en $\mathcal{O}_K$ es generado por a lo sumo dos elementos.

Definición 2.1. Dado $\mathfrak{a}$ un ideal no nulo de $\mathcal{O}_K$, el cardinal del conjunto de coclases de $\mathcal{O}_K/\mathfrak{a}$ es llamado *norma* de $\mathfrak{a}$ y se denota $\mathrm{N}(\mathfrak{a})$ o simplemente $\mathrm{N}\mathfrak{a}$. Si $\mathfrak{a} = \{0\}$ entonces $\mathrm{N}\mathfrak{a} := 0$.

Se puede mostrar que $\mathrm{N}(\mathfrak{a}) = ac$ si $\mathfrak{a}$ es como en (2.1) (Ejercicio 2).

Proposición 2.2. *Para $\beta \in \mathcal{O}_K$ no nulo,* $\mathrm{N}\langle\beta\rangle = |\mathrm{N}(\beta)|$.

Demostración. Por un lado sabemos que $\langle\beta\rangle = a\mathbb{Z} + \alpha\mathbb{Z}$ por (2.1) donde $a, c \in \mathbb{N}$, $b \in \mathbb{Z}$ y $\alpha = b + c\,\omega_K$. Por (1.5) tenemos que $\langle\beta\rangle = \beta\mathbb{Z} + \beta\,\omega_K\mathbb{Z}$. Sea $R = (r_{ij}) \in \mathrm{GL}_2(\mathbb{Z})$ la matriz de cambio de bases entre $\{a, \alpha\}$ y $\{\beta, \beta\omega_K\}$ del $\mathbb{Z}$-módulo $\langle\beta\rangle$, más precisamente

$$\begin{pmatrix} \beta \\ \beta\omega_K \end{pmatrix} = \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix} \begin{pmatrix} a \\ \alpha \end{pmatrix}.$$

Sea $Q = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$, entonces $S := RQ$ es la matriz de la transformación lineal L_β (ver (1.3)) con respecto a la base $\{1, \omega\}$, pues

$$S \begin{pmatrix} 1 \\ \omega_K \end{pmatrix} = RQ \begin{pmatrix} 1 \\ \omega_K \end{pmatrix} = R \begin{pmatrix} a \\ \alpha \end{pmatrix} = \begin{pmatrix} \beta \\ \beta\omega_K \end{pmatrix}.$$

Finalmente por (1.3) tenemos que

$$\mathrm{N}\langle\beta\rangle = \det(Q) = |\det(R)|\,\det(Q) = |\det(S)| = |\mathrm{N}(\beta)|$$

pues $\det(R) = \pm 1$. □

Dados $\mathfrak{a}$ y $\mathfrak{b}$ ideales de $\mathcal{O}_K$, recordemos la definición de *suma*, *producto* y *conjugado* de ideales:

$$\begin{aligned} \mathfrak{a} + \mathfrak{b} &= \{\alpha + \beta : \alpha \in \mathfrak{a},\ \beta \in \mathfrak{b}\}, \\ \mathfrak{a}\mathfrak{b} &= \left\{ \sum_{i=1}^{m} \alpha_i\beta_i : \alpha_i \in \mathfrak{a},\ \beta_i \in \mathfrak{b} \text{ para todo } i \right\}, \\ \mathfrak{a}' &= \{\alpha' : \alpha \in \mathfrak{a}\}. \end{aligned}$$

Se puede ver (Ejercicio 3) que si $\mathfrak{a} = \langle\alpha_1, \ldots, \alpha_r\rangle$ y $\mathfrak{b} = \langle\beta_1, \ldots, \beta_s\rangle$ entonces $\mathfrak{a} + \mathfrak{b} = \langle\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s\rangle$, $\mathfrak{a}\mathfrak{b} = \langle\alpha_1\beta_1, \ldots, \alpha_i\beta_j, \ldots, \alpha_r\beta_s\rangle$ y $\mathfrak{a}' = \langle\alpha_1', \ldots, \alpha_r'\rangle$.

Ejemplo 2.3. En el anillo $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ tenemos

$$\begin{aligned} \langle 3, 2 + \sqrt{-5}\rangle\langle 3, 2 - \sqrt{-5}\rangle &= \langle 9, 6 + 3\sqrt{-5}, 6 - 3\sqrt{-5}, 9\rangle \\ &= \langle 3\rangle\langle 3, 2 + \sqrt{-5}, 2 - \sqrt{-5}\rangle \\ &= \langle 3\rangle \end{aligned}$$

pues $1 = (2 + \sqrt{-5}) + (2 - \sqrt{-5}) - 3 \in \langle 3, 2 + \sqrt{-5}, 2 - \sqrt{-5}\rangle$.

Se dice que $\mathfrak{a}$ *divide a* $\mathfrak{b}$ (se denota $\mathfrak{a} \mid \mathfrak{b}$) si existe un ideal $\mathfrak{c}$ de $\mathcal{O}_K$ tal que $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Notemos que si $\mathfrak{a} \mid \mathfrak{b}$ entonces $\mathfrak{b} = \mathfrak{a}\mathfrak{c} \subset \mathfrak{a}$. Veremos que la recíproca es cierta, (i. e. $\mathfrak{b} \subset \mathfrak{a} \Rightarrow \mathfrak{a} \mid \mathfrak{b}$) como consecuencia del teorema de factorización única de ideales.

Definición 2.4. Se llama *ideal fraccionario* de K a un $\mathcal{O}_K$-submódulo $\mathfrak{a}$ de K que satisface $b\mathfrak{a} \subset \mathcal{O}_K$ para algún $b \in \mathbb{N}$.

Un ideal de $\mathcal{O}_K$ es trivialmente un ideal fraccionario. A partir de ahora, a éstos los llamaremos *ideales enteros*. Es posible probar que si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales fraccionarios, entonces también lo son su suma y producto (Ejercicio 4).

Como corolario del teorema de factorización única de ideales veremos que todo ideal fraccionario no nulo tiene inverso (i. e. existe $\mathfrak{a}^{-1}$ ideal fraccionario tal que $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$). Por ahora sólo lo probaremos para ideales enteros primos.

Lema 2.5. *Todo ideal primo $\mathfrak{p}$ no nulo de $\mathcal{O}_K$ es inversible.*

Demostración. Sea $\mathfrak{q} = \{x \in K : x\mathfrak{p} \subset \mathcal{O}_K\}$. Claramente $\mathfrak{q}$ es un $\mathcal{O}_K$-módulo que contiene a $\mathcal{O}_K$. Si $a \in \mathfrak{p} \cap \mathbb{Z}$, entonces $a\mathfrak{q} \subset \mathfrak{q}\mathfrak{p} \subset \mathcal{O}_K$, por lo que $\mathfrak{q}$ es un ideal fraccionario. Por otro lado tenemos que $\mathfrak{p} \subset \mathfrak{p}\mathfrak{q} \subset \mathcal{O}_K$, pero como $\mathfrak{p}$ es un ideal maximal (Ejercicio 5) entonces $\mathfrak{p}\mathfrak{q} = \mathcal{O}_K$ o $\mathfrak{p}\mathfrak{q} = \mathfrak{p}$. El caso $\mathfrak{p}\mathfrak{q} = \mathfrak{p}$ no es posible (Ejercicio 6), lo cual completa la demostración. □

Teorema 2.6. *Todo ideal $\mathfrak{a}$ no nulo de $\mathcal{O}_K$ se descompone de manera única —salvo orden— como producto de ideales primos de $\mathcal{O}_K$.*

Demostración. Probemos primero la existencia de la factorización. Sea $\mathcal{T}$ el conjunto de ideales propios de $\mathcal{O}_K$ que no se factorizan como producto de ideales primos. Queremos ver que $\mathcal{T}$ es vacío. Supongamos $\mathcal{T} \neq \emptyset$. Puesto que $\mathcal{O}_K$ es Noetheriano (Ejercicio 7), $\mathcal{T}$ contiene un elemento maximal $\mathfrak{a}$ (Ejercicio 8). Como $\mathfrak{a}$ no es primo, está contenido en un ideal maximal $\mathfrak{p}$ (Ejercicio 8), que resulta primo (Ejercicio 5). Por Lema 2.5 existe $\mathfrak{p}^{-1}$ ideal fraccionario tal que $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$. Luego $\mathfrak{a}\mathfrak{p}^{-1}$ es un ideal propio de $\mathcal{O}_K$ que contiene propiamente a $\mathfrak{a}$ pues $\mathcal{O}_K \subsetneq \mathfrak{p}^{-1}$, por lo tanto $\mathfrak{a}\mathfrak{p}^{-1} \in \mathcal{T}$. Entonces $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ para ciertos $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ ideales primos, lo que implica $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \dots \mathfrak{p}_k \notin \mathcal{T}$ contradiciendo la hipótesis. Así $\mathcal{T} = \emptyset$.

Ahora veamos la unicidad. Sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$ tal que $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s$, con $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$ ideales primos de $\mathcal{O}_K$. Veamos que $\mathfrak{q}_1$ divide a $\mathfrak{p}_1 \dots \mathfrak{p}_r$, por lo tanto divide a alguno de ellos (Ejercicio 9), digamos $\mathfrak{p}_1$. Como todo ideal primo es maximal (Ejercicio 5), $\mathfrak{p}_1 = \mathfrak{q}_1$. Por Lema 2.5 tenemos que

$$\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{q}_1^{-1}\mathfrak{a} = \mathfrak{q}_2 \dots \mathfrak{q}_s.$$

Repitiendo este argumento se prueba que $r = s$ y que $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ coinciden con $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ salvo el orden. □

2.2. Consecuencias del teorema de factorización única. Ahora sí estamos en condiciones de demostrar que todo ideal fraccionario no nulo tiene inverso. En efecto, por Teorema 2.6 sabemos que $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$, y por Lema 2.5 se tiene que $\mathfrak{a}^{-1} = \mathfrak{p}_1^{-1} \dots \mathfrak{p}_r^{-1}$ es un ideal fraccionario. Más aún, Teorema 2.6 asegura que todo ideal fraccionario se descompone de manera única salvo orden como

$$\frac{\mathfrak{q}_1 \dots \mathfrak{q}_s}{\mathfrak{p}_1 \dots \mathfrak{p}_s},$$

donde escribimos $\dfrac{1}{\mathfrak{p}_i}$ en lugar de $\mathfrak{p}_i^{-1}$.

A continuación demostraremos que en el contexto de los ideales, contener es sinónimo de dividir.

Proposición 2.7. *Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales en $\mathcal{O}_K$, entonces $\mathfrak{a} \mid \mathfrak{b}$ si y sólo si $\mathfrak{b} \subset \mathfrak{a}$.*

Demostración. La ida es clara. Supongamos que $\mathfrak{b} \subset \mathfrak{a}$. El caso $\mathfrak{a} = \mathcal{O}_K$ es trivial. Si $\mathfrak{a} = \langle 0 \rangle$ tenemos que $\mathfrak{b} = \langle 0 \rangle$ y por lo tanto $\mathfrak{a} \mid \mathfrak{b}$. Asumamos entonces $\mathfrak{a}$ ideal entero propio. Por Teorema 2.6 podemos descomponer a $\mathfrak{a}$ y $\mathfrak{b}$ como

$$\mathfrak{a} = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_r^{a_r}, \qquad \mathfrak{b} = \mathfrak{p}_1^{b_1} \dots \mathfrak{p}_r^{b_r},$$

donde $a_1, b_1, \dots, a_r, b_r$ son enteros no negativos y $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ son ideales primos distintos.

Sólo resta probar que $b_j \leq a_j$ para todo j. Supongamos que esto no es cierto, digamos $b_1 > a_1$. Como $\mathfrak{b} \subset \mathfrak{a}$ se tiene

$$\mathfrak{p}_2^{a_2} \dots \mathfrak{p}_r^{a_r} \subset \mathfrak{p}_1^{-a_1}\mathfrak{a} \subset \mathfrak{p}_1^{-a_1}\mathfrak{b} \subset \mathfrak{p}_1^{b_1-a_1}\mathfrak{p}_2^{a_2} \dots \mathfrak{p}_r^{a_r}.$$

Sin embargo, el lado derecho es divisible por $\mathfrak{p}_1$ pues $b_1 - a_1 > 0$, mientras que el lado izquierdo no lo es por la unicidad de la factorización, lo cual es absurdo. Por lo tanto $b_1 \leq a_1$. □

A partir de la descomposición única de ideales se puede definir el *máximo común divisor* y el *mínimo común múltiplo* de dos ideales $\mathfrak{a} = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_r^{a_r}$ y $\mathfrak{b} = \mathfrak{p}_1^{b_1} \dots \mathfrak{p}_r^{b_r}$ $(a_i, b_i \geq 0)$ como

$$\operatorname{mcd}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{p}_1^{c_1} \dots \mathfrak{p}_r^{c_r} \quad \text{y} \quad \operatorname{mcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{p}_1^{d_1} \dots \mathfrak{p}_r^{d_r},$$

donde $c_i := \min(a_i, b_i)$ y $d_i := \max(a_i, b_i)$ para cada i. Se puede mostrar que $\operatorname{mcd}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ y $\operatorname{mcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$ (Ejercicio 10).

Otra consecuencia es

$$\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}\mathfrak{a}\,\mathrm{N}\mathfrak{b} \tag{2.2}$$

para ideales enteros $\mathfrak{a}$ y $\mathfrak{b}$. Recordemos que por Proposición 2.2 sabemos que $|\mathbb{N}(\alpha)| = \mathbb{N}\langle\alpha\rangle$ para cualquier $\alpha \in \mathcal{O}_K$, por lo tanto (2.2) vale para ideales principales. El caso general requiere algo más de trabajo (Ejercicio 11).

La propiedad (2.2) nos permite enunciar, de manera análoga a (♠), la siguiente condición para que un ideal sea primo.

Proposición 2.8. *Si $\mathfrak{p}$ es un ideal entero tal que $\mathrm{N}\mathfrak{p} = p$ es un primo racional entonces $\mathfrak{p}$ es un ideal primo.*

Demostración. (Ejercicio 12). □

Consideremos un ideal primo $\mathfrak{p}$ no nulo de $\mathcal{O}_K$. Sabemos que existe un único primo racional p en $\mathfrak{p}$, por lo tanto $\langle p \rangle \subset \mathfrak{p}$, o equivalentemente $\mathfrak{p}$ ocurre en la factorización de $\langle p \rangle = \mathfrak{p}_1 \dots \mathfrak{p}_r$ por Proposición 2.7. Aplicando norma a ambos lados obtenemos $p^2 = \mathrm{N}\mathfrak{p}_1 \dots \mathrm{N}\mathfrak{p}_r$, lo cual nos asegura que $r \leq 2$. Más aún, si $r = 2$ entonces $\mathrm{N}(\mathfrak{p}_i) = p$ para $i = 1, 2$. Esto implica que $\langle p \rangle = \mathfrak{p}$ $(r = 1)$ o $\langle p \rangle = \mathfrak{p}\mathfrak{p}'$ $(r = 2)$ pues si $\mathfrak{p}$ divide a $\langle p \rangle$ también lo hace $\mathfrak{p}'$. Luego, el ideal $\langle p \rangle$ se factoriza de una de las siguientes maneras (y p se denomina con respecto a K como sigue):

$$\langle p \rangle = \begin{cases} \mathfrak{p}\mathfrak{p}' & \text{con } \mathfrak{p} \neq \mathfrak{p}' \quad (p \textit{ se parte en } K), \\ \mathfrak{p} & \text{con } \mathfrak{p} = \mathfrak{p}' \quad (p \textit{ permanece primo en } K), \\ \mathfrak{p}^2 & \text{con } \mathfrak{p} = \mathfrak{p}' \quad (p \textit{ ramifica en } K). \end{cases} \tag{2.3}$$

Notemos que en todos los casos tenemos $\mathfrak{p}\mathfrak{p}' = \langle \mathrm{N}\mathfrak{p} \rangle$. Así, para cualquier ideal entero $\mathfrak{a}$, por (2.2) obtenemos

$$\mathfrak{a}\mathfrak{a}' = \langle \mathrm{N}(\mathfrak{a}) \rangle. \tag{2.4}$$

Con estas nuevas herramientas podemos trabajar con ejemplos explícitos.

Ejemplo 2.9. En Ejemplo 2.3 vimos que si $\mathfrak{p} = \langle 3, 2+\sqrt{-5}\rangle \subset \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, entonces $\mathfrak{p}\mathfrak{p}' = \langle 3\rangle$. Luego, $\mathrm{N}\mathfrak{p} = 3$ por (2.4) y $\mathfrak{p}$ es primo por Proposición 2.8. Más aún, $\mathfrak{p}$ no es principal pues si $\mathfrak{p} = \langle\alpha\rangle$ con $\alpha \in \mathcal{O}_K$, entonces $3 = \mathrm{N}\mathfrak{p} = |\mathrm{N}(\alpha)|$ lo cual no puede suceder pues $\mathrm{N}(a+b\sqrt{-5}) = a^2+5b^2 \neq 3$ para todo $a, b \in \mathbb{Z}$. Así, $\mathcal{O}_K$ no es un dominio de ideales principales.

Ejemplo 2.10. En Ejemplo 1.11 vimos que $3^4 = (5+2\sqrt{-14})(5-2\sqrt{-14})$ con 3, $\alpha := 5+2\sqrt{-14}$ y $\alpha' = 5-2\sqrt{-14}$ elementos irreducibles en $\mathbb{Z}[\sqrt{-14}]$. Si $\mathfrak{a} = \langle 3^4\rangle$, entonces tenemos dos factorizaciones distintas $\mathfrak{a} = \langle 3\rangle^4 = \langle\alpha\rangle\langle\alpha'\rangle$, pero no de ideales primos.

Sea $\mathfrak{p} = \langle 3, 1+\sqrt{-14}\rangle$, entonces

$$\mathfrak{p}\mathfrak{p}' = \langle 9, 3+\sqrt{-14}, 3-3\sqrt{-14}, 15\rangle = \langle 3\rangle.$$

En efecto, en la última igualdad claramente vale $\subset$ pues todos los elementos de $\mathfrak{p}\mathfrak{p}'$ son divisibles por 3. Además $3 = 2\cdot 9 - 15 \in \mathfrak{p}\mathfrak{p}'$ lo que asegura $\supset$. En particular $\mathrm{N}\mathfrak{p} = 3$ y $\mathfrak{p}$ es un ideal primo. Luego $\mathfrak{a} = \mathfrak{p}^4\mathfrak{p}'^4$ es su descomposición en ideales primos. Es posible comprobar que $\langle\alpha\rangle = \mathfrak{p}^4$ y $\langle\alpha'\rangle = \mathfrak{p}'^4$ (Ejercicio 13).

Para un cuerpo cuadrático $K = \mathbb{Q}[\sqrt{m}]$, llamaremos *discriminante* de K a

$$d_K = \begin{cases} 4m & \text{si } m \equiv 2,3 \pmod 4, \\ m & \text{si } m \equiv 1 \pmod 4. \end{cases}$$

Claramente se tiene que $K = \mathbb{Q}[\sqrt{d_K}]$. Más aún, $\{1, \frac{d_k+\sqrt{d_K}}{2}\}$ es una base del $\mathbb{Z}$-módulo $\mathcal{O}_K$ (Ejercicio 14). También haremos uso del conocido *símbolo de Legendre* el cual para un primo racional p impar y $a \in \mathbb{Z}$ se define por

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{si } p \nmid a \text{ y } x^2 \equiv a \pmod p \text{ tiene solución en } \mathbb{Z}, \\ -1 & \text{si } p \nmid a \text{ y } x^2 \equiv a \pmod p \text{ no tiene solución en } \mathbb{Z}, \\ 0 & \text{si } p \mid a. \end{cases}$$

Se puede ver que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ para todo $a, b \in \mathbb{Z}$ (Ejercicio 15).

El siguiente resultado da simples condiciones para que saber cómo se factoriza $\langle p\rangle$, para un número primo racional $p > 2$.

Teorema 2.11. *Sean p un primo racional impar y $K = \mathbb{Q}[\sqrt{m}]$ un cuerpo cuadrático con discriminante d_K. Entonces se tienen las siguientes equivalencias.*

(i) $\langle p\rangle = \mathfrak{p}^2$ *si y sólo si* $\left(\dfrac{d_K}{p}\right) = 0$.

(ii) $\langle p\rangle = \mathfrak{p}\mathfrak{p}'$ *con* $\mathfrak{p} \neq \mathfrak{p}'$ *si y sólo si* $\left(\dfrac{d_K}{p}\right) = +1$.

(iii) $\langle p\rangle = \mathfrak{p}$ *si y sólo si* $\left(\dfrac{d_K}{p}\right) = -1$.

Demostración. Comencemos suponiendo que $\langle p\rangle = \mathfrak{p}^2$. Entonces existe $\pi = a+b\,\frac{d_K+\sqrt{d_K}}{2} \in \mathfrak{p} \setminus \langle p\rangle$ con $a, b \in \mathbb{Z}$. Sin embargo,

$$\begin{aligned} \pi^2 &= \left(\frac{2a+bd_K}{2} + \frac{b}{2}\sqrt{d_K}\right)^2 \\ &= \tfrac{1}{4}\Big((2a+bd_K)^2 + d_K b^2\Big) + \tfrac{1}{2}(a+bd_K)b\sqrt{d_K} \in \langle p\rangle \end{aligned}$$

por lo tanto p divide (en $\mathbb{Z}$) a $(2a+bd_K)^2+d_Kb^2$ y a $(a+bd_K)b$. Si $p \mid b$ entonces $p \mid a$ y en consecuencia $p \mid \pi$ lo cual contradice la hipótesis. Esto implica que $p \mid a+bd_K$ y $p \nmid b$, sumado a que $p \mid (2a+bd_K)^2+d_Kb^2$, resulta $p \mid d_K$, es decir, $\left(\frac{d_K}{p}\right)=0$.

Ahora supongamos $p \mid d_K$. Consideremos $\mathfrak{p}=\langle p\rangle+\langle\sqrt{d_K}\rangle$, entonces (Ejercicio 16)

$$\mathfrak{p}^2=\langle p^2, p\sqrt{d_K}, d_K\rangle=\langle p\rangle, \tag{2.5}$$

con $\mathfrak{p}$ ideal primo por (2.4) y Proposición 2.8.

Supongamos que $\left(\frac{d_K}{p}\right)=1$, es decir, existe $a\in\mathbb{Z}$ tal que $a^2\equiv d_K \pmod p$. Si $\mathfrak{p}=\langle p, a+\sqrt{d}\rangle$ entonces (Ejercicio 16)

$$\mathfrak{p}\mathfrak{p}'=\langle p^2, p(a+\sqrt{d_K}), p(a-\sqrt{d_K}), a^2-d_K\rangle=\langle p\rangle \tag{2.6}$$

con $\mathfrak{p}$ y $\mathfrak{p}'$ ideales primos. Además $\mathfrak{p}\neq\mathfrak{p}'$ pues $\mathfrak{p}+\mathfrak{p}'=\mathcal{O}_K$.

Recíprocamente, si $\langle p\rangle=\mathfrak{p}\mathfrak{p}'$ con $\mathfrak{p}\neq\mathfrak{p}'$, entonces $\mathrm{N}(\mathfrak{p})=\mathrm{N}(\mathfrak{p}')=p$. Tomemos $\alpha=a+b\frac{d_K+\sqrt{d_K}}{2}\in\mathfrak{p}\smallsetminus\langle p\rangle$ donde $a,b\in\mathbb{Z}$ satisfacen que $p\nmid \mathrm{mcd}(a,b)$. Como $\langle\alpha\rangle\subset\mathfrak{p}$ se tiene $\mathfrak{p}\mid\langle\alpha\rangle$ por Proposición 2.7, por lo tanto $p=\mathrm{N}\mathfrak{p}$ divide a

$$\mathrm{N}\langle\alpha\rangle=|\mathrm{N}(\alpha)|=\left|\mathrm{N}\left(\tfrac{2a+bd_K}{2}+\tfrac{bd_K}{2}\sqrt{d_K}\right)\right|=\tfrac{1}{4}\left|(2a+bd_K)^2-b^2d_K\right|,$$

en particular $(2a+bd_K)^2\equiv b^2d_K \pmod p$. Si $p\mid b$ entonces $p\mid a$ lo cual contradice la hipótesis. Luego $p\nmid b$, entonces existe $c\in\mathbb{Z}$ tal que $bc\equiv 1 \pmod p$ (i. e. c es el inverso de b módulo p), por lo tanto $x^2\equiv d_K \pmod p$ tiene solución $x=(2a+bd_K)c$.

El último caso es inmediato a partir de los dos ítems anteriores. □

Existe una teoría similar para $p=2$ que utiliza el *símbolo de Kronecker*, la cual no abordaremos para no abultar el texto (ver [4]).

Para finalizar esta sección, veamos que en estos anillos todo DFU es necesariamente DIP. Necesitaremos el siguiente lema que tiene valor por sí mismo para entender los ideales primos en un DFU.

Lema 2.12. *Si $\mathcal{O}_K$ es un dominio de factorización única, entonces todo ideal primo en $\mathcal{O}_K$ es principal.*

Demostración. Primero veamos que dado π elemento irreducible en $\mathcal{O}_K$, el ideal $\langle\pi\rangle$ es maximal. Supongamos que $\langle\pi\rangle\subset\mathfrak{a}\subset\mathcal{O}_K$ y $\langle\pi\rangle\neq\mathfrak{a}$ para algún ideal entero $\mathfrak{a}$. Sea $\alpha\in\mathfrak{a}\smallsetminus\langle\pi\rangle$, escribimos $\langle\pi\rangle=\mathfrak{a}\mathfrak{b}$ por Proposición 2.7. Para todo $\beta\in\mathfrak{b}$ se tiene $\alpha\beta\in\langle\pi\rangle$, entonces $\pi\mid\alpha\beta$ y por lo tanto $\pi\mid\beta$ pues $\alpha\notin\langle\pi\rangle$. Esto nos dice que $\langle\pi\rangle=\mathfrak{b}$, de esta forma $\langle\pi\rangle=\langle\pi\rangle\mathfrak{a}$ lo que significa que $\mathfrak{a}=\mathcal{O}_K$ y $\langle\pi\rangle$ es maximal.

Tomemos $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$ y $\alpha\in\mathfrak{p}$ no nulo. Como $\mathcal{O}_K$ es dominio de factorización única, existen $\pi_1,\dots,\pi_r$ elementos irreducibles tales que $\alpha=\pi_1\dots\pi_r$. Esto nos dice que $\mathfrak{p}$ divide a $\langle\pi_1\rangle\dots\langle\pi_r\rangle$, por lo tanto divide a algún $\langle\pi_i\rangle$, i. e. $\langle\pi_i\rangle\subset\mathfrak{p}$. Por lo anterior $\langle\pi\rangle$ es maximal y en consecuencia vale la igualdad. □

Teorema 2.13. *El anillo de enteros $\mathcal{O}_K$ de un cuerpo cuadrático K es dominio de ideales principales si y sólo si es dominio de factorización única.*

Demostración. La ida vale en general. Sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$, veamos que es principal. Claramente podemos suponer que $\mathfrak{a}$ es propio. Descomponemos $\mathfrak{a}=\mathfrak{p}_1\dots\mathfrak{p}_r$ como producto de ideales primos $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ por Teorema 2.6. Por Lema 2.12, $\mathfrak{p}_i=\langle\pi_i\rangle$ para algún $\pi_i\in\mathcal{O}_K$, por lo tanto $\mathfrak{a}=\langle\pi_1\dots\pi_r\rangle$. □

Como consecuencia tenemos que $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única ya que en Ejemplo 2.9 vimos que no es dominio de ideales principales.

2.3. Ejercicios.

1. Probar que todo ideal $\mathfrak{a}$ de $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre de rango 2.
2. Probar que si $\mathfrak{a}$ es un ideal de $\mathcal{O}_K$ como en (2.1) entonces $\mathrm{N}\mathfrak{a} = ac$. [Ayuda: mostrar que un conjunto de representantes de $\mathcal{O}_K/\mathfrak{a}$ es $\{r + s\omega_K : 0 \leq r < a,\ 0 \leq s < c\}$.]
3. Probar que si $\mathfrak{a} = \langle \alpha_1, \ldots, \alpha_r \rangle$ y $\mathfrak{b} = \langle \beta_1, \ldots, \beta_s \rangle$ entonces:
   a) $\mathfrak{a} + \mathfrak{b} = \langle \alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \rangle$.
   b) $\mathfrak{a}\mathfrak{b} = \langle \alpha_1\beta_1, \ldots, \alpha_i\beta_j, \ldots, \alpha_r\beta_s \rangle$.
   c) $\mathfrak{a}' = \langle \alpha_1', \ldots, \alpha_r' \rangle$.
4. Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales fraccionarios. Probar que también lo son $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$, $\mathfrak{a}'$ y $c\,\mathfrak{a}$ para $c \in \mathbb{Q}$.
5. Probar que todo ideal primo es maximal. [Ayuda: todo dominio de integridad finito es un cuerpo.]
6. Probar que si $\mathfrak{p}$ y $\mathfrak{q}$ son ideales primos entonces $\mathfrak{p}\mathfrak{q} \neq \mathfrak{p}$.
7. Probar que $\mathcal{O}_K$ es Noetheriano, es decir, toda cadena ascendente $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$ de ideales en $\mathcal{O}_K$ debe estabilizarse en algún momento.
8. Probar las siguientes equivalencias para un anillo A.
   (i) A es Noetheriano.
   (ii) Todo subconjunto no vacío $\mathcal{T}$ de ideales en A contiene un elemento maximal, es decir, existe $\mathfrak{a} \in \mathcal{T}$ tal que $\mathfrak{a} \not\subset \mathfrak{b}$ para todo $\mathfrak{b} \in \mathcal{T}$ distinto de $\mathfrak{a}$.
   (iii) Todo ideal en A está contenido en un ideal maximal.
   (iv) Todo ideal en A es finitamente generado.
9. Probar que si un ideal primo $\mathfrak{p}$ divide a un producto de ideales $\mathfrak{a}\mathfrak{b}$, entonces $\mathfrak{p}$ divide a uno de ellos.
10. Probar que $\mathrm{mcd}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ y $\mathrm{mcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$. Generalizarlo para una cantidad finita de ideales.
11. Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales enteros en $\mathcal{O}_K$ de norma m y n respectivamente. Denotemos $\xi_1, \ldots, \xi_m$ y $\eta_1, \ldots, \eta_n$ los conjuntos de representantes de $\mathcal{O}_K/\mathfrak{a}$ y $\mathcal{O}_K/\mathfrak{b}$ respectivamente.
    a) Probar que existe $\gamma \in \mathcal{O}_K$ tal que $\mathrm{mcd}(\mathfrak{a}\mathfrak{b}, \langle\gamma\rangle) = \mathfrak{a}$.
    b) Probar que los elementos $\xi_i + \gamma\eta_j$ para $1 \leq i \leq m$ y $1 \leq j \leq n$ viven en clases distintas de $\mathcal{O}_K/\mathfrak{a}\mathfrak{b}$.
    c) Probar que los mn elementos del ítem anterior forman un conjunto completo de representantes de $\mathcal{O}_K/\mathfrak{a}\mathfrak{b}$.
12. Probar Proposición 2.8
13. Probar que $\langle 5 + 2\sqrt{-14} \rangle = \langle 3, 1 + \sqrt{-14} \rangle^4$ en $\mathbb{Z}[\sqrt{-14}]$.
14. Probar que $\mathcal{O}_K = \mathbb{Z} + \frac{d_K + \sqrt{d_K}}{2}\mathbb{Z}$.
15. Probar que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ para todo $a, b \in \mathbb{Z}$.
16. Probar (2.5) y (2.6)

3. Grupo de clases

3.1. Finitud del número de clases. Sea K un cuerpo cuadrático con anillo de enteros $\mathcal{O}_K$. Vimos al comenzar Subsección 2.2 que todo ideal fraccionario no nulo tiene inverso, lo que nos asegura que el conjunto de ideales fraccionarios no nulos forman un grupo multiplicativo (abeliano). Este grupo será denotado por Δ_K.

Notemos que si $\alpha \in K$ entonces $\langle\alpha\rangle := \{\alpha\beta : \beta \in \mathcal{O}_K\}$ es un ideal fraccionario en K. Los ideales fraccionarios de esta forma serán llamados naturalmente *principales*.

Claramente los ideales fraccionarios principales no nulos forman un subgrupo Π_K de Δ_K.

Definición 3.1. El grupo cociente $\mathfrak{I}_K = \Delta_K/\Pi_K$ es llamado el *grupo de clases de ideales* de K, o simplemente *grupo de clases*.

La intención es probar que el grupo $\mathfrak{I}_K$ es finito. El orden de tal grupo lo denotaremos por h_K y es llamado *número de clase* de K. Se puede ver que (Ejercicio 1)

$$h_K = 1 \iff \mathcal{O}_K \text{ es DFU.} \tag{3.1}$$

En general, el número h_K mide por cuánto $\mathcal{O}_K$ no es dominio de factorización única.

Dado $\mathfrak{a}$ un ideal fraccionario no nulo de K, denotaremos $[\mathfrak{a}]$ su clase en $\mathfrak{I}_K$. Notemos que $[\mathfrak{a}] = [\mathfrak{b}]$ equivale a $\mathfrak{a} = \langle\alpha\rangle\mathfrak{b}$ para algún $\alpha \in K$.

Lema 3.2. *Para todo entero $t > 0$ existe una cantidad finita de ideales enteros $\mathfrak{a}$ de $\mathcal{O}_K$ tales que $\mathrm{N}\mathfrak{a} < t$.*

Demostración. (Ejercicio 2). □

Lema 3.3. *Todo ideal entero no nulo $\mathfrak{a}$ contiene un elemento $\alpha \neq 0$ tal que*

$$|\mathrm{N}(\alpha)| \leq C_K\, \mathrm{N}\mathfrak{a},$$

donde $C_K = \big(1 + |\mathrm{N}(\omega_K)| + |\mathrm{Tr}(\omega_K)|\big)$.

Demostración. Sabemos que $\mathcal{O}_K = \mathbb{Z} + \omega_K\mathbb{Z}$ por (1.5). Sea t la parte entera de $(\mathrm{N}\mathfrak{a})^{1/2}$. Luego, entre los $(t+1)^2$ números de la forma $a + b\,\omega_K$ con $0 \leq a, b \leq t$ deben existir dos cuya diferencia esté en $\mathfrak{a}$ pues $\#\mathcal{O}_K/\mathfrak{a} = \mathrm{N}\mathfrak{a} < (t+1)^2$. Llamemos α a tal diferencia que podemos escribir como $\alpha = a + b\,\omega_K$ con $-t \leq a, b \leq t$. Entonces

$$\begin{aligned} |\mathrm{N}(\alpha)| &= |(a + b\omega_K)(a + b\omega'_K)| \\ &= |a^2 + b^2\mathrm{N}(\omega_K) + ab\mathrm{Tr}(\omega_K)| \\ &\leq t^2\,\big(1 + |\mathrm{N}(\omega_K)| + |\mathrm{Tr}(\omega_K)|\big), \end{aligned}$$

por lo que concluimos $|\mathrm{N}(\alpha)| \leq C_K\,\mathrm{N}\mathfrak{a}$. □

Lema 3.4. *En toda clase de ideales existe un representante $\mathfrak{a} \subset \mathcal{O}_K$ tal que $\mathrm{N}\mathfrak{a} \leq C_K$.*

Demostración. Consideremos la clase $[\mathfrak{b}]$ de un ideal fraccionario no nulo $\mathfrak{b}$. Podemos suponer que $\mathfrak{b}^{-1}$ es un ideal entero. Por Lema 3.3 existe $\beta \in \mathfrak{b}^{-1}$ tal que $|\mathrm{N}(\beta)| \leq C_K\,\mathrm{N}\mathfrak{b}^{-1}$. Sea $\mathfrak{a} = \langle\beta\rangle\mathfrak{b}$ en la clase $[\mathfrak{b}]$. Entonces $\mathrm{N}\mathfrak{a}\mathrm{N}\mathfrak{b}^{-1} = \mathrm{N}(\mathfrak{a}\mathfrak{b}^{-1}) = \mathrm{N}\langle\beta\rangle = |\mathrm{N}(\beta)| \leq C_K\mathrm{N}\mathfrak{b}^{-1}$, por lo tanto $\mathrm{N}\mathfrak{a} \leq C_K$. □

Estos tres lemas implican la finitud de h_K (Ejercicio 3).

Teorema 3.5. *El número de clase de K es finito.*

Fijado un cuerpo cuadrático K, el cálculo explícito del número h_K es generalmente complicado. En la actualidad se utilizan métodos computacionales para ello, sin embargo como veremos en la siguiente sección, aún no se entiende completamente su comportamiento.

Calculemos algunos de ellos usando Lema 3.4 y Teorema 2.11. La intención es dar un representante de cada clase de $\mathfrak{I}_K$. Por Lema 3.4 es suficiente buscar dentro de los ideales enteros de norma menor o igual a C_K. Más aún, gracias al teorema de

factorización única de ideales, podemos concentrarnos en los ideales primos. No es difícil chequear que (Ejercicio 4)

$$C_K = \begin{cases} 1+|m| & \text{si } m \equiv 2,3 \pmod 4, \\ \dfrac{2+|1-m|}{4} & \text{si } m \equiv 1 \pmod 4. \end{cases} \tag{3.2}$$

Ejemplo 3.6. Comencemos con el caso $K = \mathbb{Q}[\sqrt{2}]$ en donde $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$, $d_K = 8$ y $C_K = 3$. Sea $\mathfrak{p}$ un ideal entero con norma igual a 2 o 3, por lo tanto primo. Esto significa, por (2.4), que $\mathfrak{p}$ divide a $\langle 2\rangle$ o a $\langle 3\rangle$ respectivamente. Tenemos que $\langle 2\rangle = \langle\sqrt{2}\rangle^2$ y $\langle 3\rangle$ es primo pues $\left(\frac{d}{3}\right) = -1$ (ver Teorema 2.11), luego $\mathfrak{p} = \langle\sqrt{2}\rangle$ sólo puede ser igual al ideal principal $\langle 2\rangle$. Concluimos que todo ideal fraccionario es principal, o equivalentemente

$$h_{\mathbb{Q}[\sqrt{2}]} = 1.$$

Ejemplo 3.7. Sea $K = \mathbb{Q}[\sqrt{-1}]$ por lo tanto $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$, $d_K = -4$ y $C_K = 2$. En este caso $\langle 2\rangle = \langle 1+\sqrt{-1}\rangle^2$, entonces

$$h_{\mathbb{Q}[\sqrt{-1}]} = 1.$$

Para estos dos ejemplos ya sabíamos que $h_K = 1$ pues en ambos casos $\mathcal{O}_K$ es dominio de factorización única por ser dominio Euclídeo (ver Ejemplo 1.13 y Ejemplo 1.14). Con este mismo método se puede comprobar que $h_K = 1$ para los listados en Ejemplo 1.13 (Ejercicio 5) y en Ejemplo 1.14 (Ejercicio 6), aunque los cálculos necesarios aumentan significativamente a medida que d_K crece.

Ejemplo 3.8. Tomemos $K = \mathbb{Q}[\sqrt{-5}]$, así $\mathcal{O}_K = \mathbb{Z}[-5]$, $d_K = -20$ y $C_K = 6$. Sabemos por Ejemplo 2.9 que no es dominio de ideales principales, y en consecuencia tampoco es dominio de factorización única por Teorema 2.13, entonces $h_K \geq 2$. Tenemos (Ejercicio 7)

$$\begin{array}{rcll} \langle 2\rangle &=& \mathfrak{p}_2^2 & \text{donde} \quad \mathfrak{p}_2 = \langle 2, 1+\sqrt{-5}\rangle, \quad \mathfrak{p}_2 = \mathfrak{p}_2' \\ \langle 3\rangle &=& \mathfrak{p}_3\mathfrak{p}_3' & \text{donde} \quad \mathfrak{p}_3 = \langle 3, 1+\sqrt{-5}\rangle, \quad \mathfrak{p}_3 \neq \mathfrak{p}_3', \\ \langle 5\rangle &=& \mathfrak{p}_5^2 & \text{donde} \quad \mathfrak{p}_5 = \langle\sqrt{-5}\rangle, \quad \mathfrak{p}_5 = \mathfrak{p}_5'. \end{array} \tag{3.3}$$

Luego, todos los ideales enteros de norma menor o igual a 6 son

$$\mathfrak{p}_2, \quad \mathfrak{p}_3, \quad \mathfrak{p}_3', \quad \mathfrak{p}_2^2, \quad \mathfrak{p}_5, \quad \mathfrak{p}_2\mathfrak{p}_3 \quad \text{y} \quad \mathfrak{p}_2\mathfrak{p}_3'.$$

La primera factorización de (3.3) nos dice que $[\langle 1\rangle] = [\langle 2\rangle] = [\mathfrak{p}_2]^2$ por lo tanto $[\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2]$. Además se tiene que $\mathfrak{p}_2$ no puede ser principal y

$$\begin{aligned} \mathfrak{p}_2\mathfrak{p}_3 &= \langle 6,\, 2(1+\sqrt{-5}),\, 3(1+\sqrt{-5}), (1+\sqrt{-5})^2\rangle \\ &= \langle 1+\sqrt{-5}\rangle, \end{aligned}$$

lo que implica

$$\begin{array}{lll} [\mathfrak{p}_2\mathfrak{p}_3] = [\langle 1\rangle], & [\mathfrak{p}_3] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2], & [\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1} = [\mathfrak{p}_2], \\ [\mathfrak{p}_2\mathfrak{p}_3'] = [\langle 1\rangle], & [\mathfrak{p}_2^2] = [\langle 1\rangle], & [\mathfrak{p}_5] = [\langle 1\rangle]. \end{array}$$

Esto nos permite concluir

$$\mathfrak{I}_{\mathbb{Q}[\sqrt{-5}]} = \big\{[\langle 1\rangle],\ [\mathfrak{p}_2]\big\} \cong \mathbb{Z}_2 \qquad \text{y} \qquad h_{\mathbb{Q}[\sqrt{-5}]} = 2.$$

Con incluso menos cálculos es posible ver que $h_{\mathbb{Q}[\sqrt{-15}]} = 2$ (Ejercicio 8). Para el resto de los cuerpos con $h_K > 1$ la cantidad de posibilidades aumenta, aunque vale la pena mostrar que $h_{\mathbb{Q}[\sqrt{-23}]} = 3$ (Ejercicio 9).

3.2. Conjeturas de Gauss. El problema de determinar el número h_K se remonta a Gauss en su conocido tratado *Disquisitiones Arithmeticae* sobre formas binarias cuadráticas publicado en 1981. A pesar de que un gran número de prestigiosos matemáticos han trabajado en esta área, existen diversas cuestiones sobre el número h_K que aún no han resueltas. Daremos un breve recorrido sobre algunas ellas para el caso de cuerpos cuadráticos imaginarios. Un excelente resumen histórico hace Dorian Goldfeld [3], quien probó un importante teorema que veremos al fin de estas notas.

El primer avance significativo para entender el número h_K fue debido a Dirichlet en 1839. Este resultado es llamado *Dirichlet class number formula* y se puede escribir como sigue:

$$h_K = \begin{cases} \dfrac{w\sqrt{-d_K}}{2\pi}\, L(1,\chi) & \text{si } d_K < 0, \\ \dfrac{\sqrt{d_K}}{\log(\varepsilon)}\, L(1,\chi) & \text{si } d_K > 0, \end{cases} \tag{3.4}$$

donde d_K es el discriminante de K, w el número de unidades en $\mathcal{O}_K$, ε la unidad fundamental de $\mathcal{O}_K$ y $L(\cdot,\chi)$ la serie L correspondiente al carácter $\chi(n) := \left(\frac{d_K}{n}\right)$, i. e. $L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)\, n^{-s}$. Además dio una fórmula finita para el número $L(1,\chi)$, la cual desafortunadamente no es efectiva en la práctica.

Gauss hizo varias conjeturas en su tratado sobre el comportamiento de h_K, tal como

$$\lim_{m\to-\infty} h_{\mathbb{Q}[\sqrt{m}]} = \lim_{d_K\to-\infty} h_K = +\infty,$$

que fue probada por Helbronn en 1934. Además dejó listas de cuerpos cuadráticos imaginarios con números de clase menos a 6, afirmando además que estaban completas. Efectivamente lo estaban. Por ejemplo para $h_K = 1$ son

$$d_K = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

A decir verdad, ésta no es la nómina original de Gauss ya que su trabajo lo realizaba en el contexto de las formas cuadráticas binarias. Recién a mediados de la década del 60', Baker y Stark probaron independientemente que la lista estaba completa para $h_K = 1$, y luego para $h_K = 2$ a principios de los 70'.

La versión moderna de las listas conjeturadas por Gauss es el llamado *Gauss' class number problem* y se puede enunciar de la siguiente manera:

> *Encontrar un algoritmo efectivo para determinar todos los cuerpos cuadráticos imaginarios con número de clase dado.*

En la década del 70', Goldfeld publicó una serie de trabajos relacionando este problema con series L de curvas elípticas sobre $\mathbb{Q}$, y junto con los resultados de Gross y Zagier en esta área en 1985, se obtuvo el siguiente teorema.

Teorema 3.9 (Goldfeld-Gross-Zagier)**.** *Para todo $\varepsilon > 0$ existe una constante $c > 0$ calculable de manera efectiva tal que*

$$h_K > c\ (\log|d_K|)^{1-\varepsilon}$$

para todo cuerpo cuadrático imaginario K.

Este teorema resuelve —salvo una cantidad finita de cálculos— el problema de Gauss sobre el número de clases. De todas maneras, la "cantidad finita" de cálculos necesarios son exageradamente grandes, tanto que sólo se conocía para $h_K \leq 7$ hasta el 2004, año en el que Watkins determinó todos los cuerpos cuadráticos imaginarios con número de

clase menor o igual a 100. Para esto realizó modificaciones en los trabajos de Goldfeld obteniendo una mejor constante c, aunque aún así los cálculos demoraron siete meses dentro de la computadora. Como curiosidad, los cuerpos cuadráticos con número de clase igual a 100 son 1736, y el valor máximo de d_K para éstos es 1856563.

El caso cuadrático real es mucho menos entendido. Finalizamos estas notas con la siguiente conjetura de Gauss aún abierta.

Conjetura 3.10. (Gauss) *Existen infinitos cuerpos cuadráticos reales con número de clase uno.*

3.3. Ejercicios.

1. Sea K un cuerpo cuadrático. Probar que $\mathcal{O}_K$ es un dominio de factorización única si y sólo si $h_K = 1$.
2. Probar Lema 3.2 siguiendo los siguientes pasos.
   - Es suficiente demostrarlo para ideales primos.
   - Si $\mathfrak{p}$ es un ideal primo, entonces $\mathrm{N}\mathfrak{p}$ es p o p^2 para p un primo racional.
   - Concluir la demostración usando Teorema 2.11.
3. Probar Teorema 3.5 como una simple consecuencia de los Lema 3.2, Lema 3.3 y Lema 3.4.
4. Probar (3.2).
5. Probar que $h_K = 1$ para $K = \mathbb{Q}[\sqrt{m}]$ con $m = -2, -3, -7, -11$.
6. Probar que $h_K = 1$ para $K = \mathbb{Q}[\sqrt{m}]$ con $m = 2, 3, 5, 13$.
7. Probar (3.3).
8. Probar que $h_{\mathbb{Q}[\sqrt{-15}]} = 2$.
9. Probar que $h_{\mathbb{Q}[\sqrt{-23}]} = 3$ y dar los representantes de $\mathfrak{I}_{\mathbb{Q}[\sqrt{-23}]}$.

Referencias

[1] S. Alaca, K.S. Williams, *Introductory algebraic number theory*, Cambridge University Press (2004).

[2] K. Conrad, *Factoring in quadratic field*, notas incluidas en su página web.

[3] D. Goldfeld, *Gauss' class number problem for imaginary quadratic fields*, Bulletin of AMS **13**:1 (1985).

[4] R. Narasimhan, S. Raghavan, S. Rangachari, S. Lal, *Algebraic number theory*, Lecture notes of Tata Institute of Fundamental Research, Bombay (1966).

[5] M.I. Pacharoni, *Aritmética en cuerpos de números*, notas del elENA III, cursos para estudiantes (2006).

FaMAF — CIEM, Universidad Nacional de Córdoba; Medina Allende s/n, Ciudad Universitaria, 5000, Córdoba.

E-mail address: elauret@famaf.unc.edu.ar