Representación de números primos mediante formas cuadráticas

Elisa Mazuelos Jiménez

Representación de números primos mediante formas cuadráticas

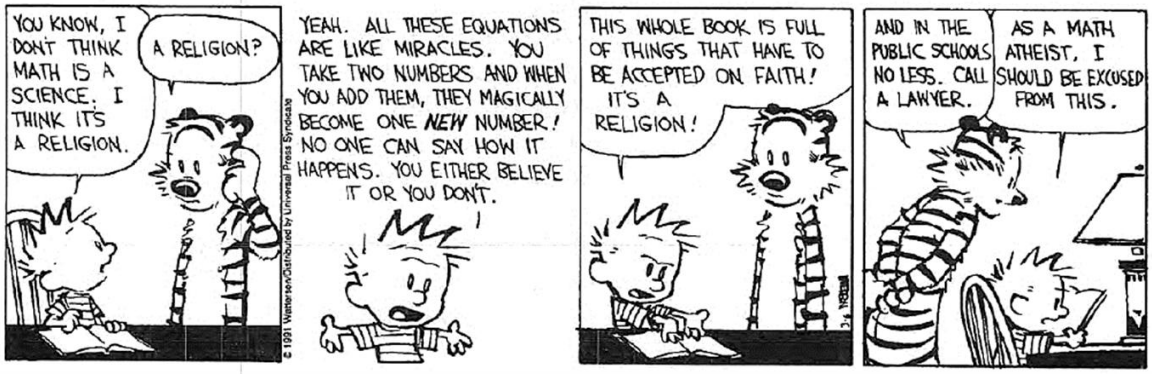
Elisa Mazuelos Jiménez

Memoria presentada como parte de los requisitos para la obtención del título de Grado en Matemáticas por la Universidad de Sevilla.

Tutorizada por Antonio Rojas León

21 de junio de 2017

Calvin and Hobbes **by Bill Watterson**



Índice

Abstract

The well-known seventeenth century mathematician Pierre de Fermat left some interesting results on integers and how to represent them as sums of powers – all of them unproved. In this dissertation we study the following problem: given an integer n, which prime numbers p can be expressed in the form

$$p = x^2 + ny^2,$$

where x and y are integers?

We will start with some basic notions of algebraic number theory, such as the ring of integers of a number field. Then, we will move forward to unique factorization of ideals and Dedekind domains, using the class number of a number field to help us look at a specific direction: rings of algebraic integers which are principal ideal domains.

We will close this dissertation by following the theory presented here and giving some examples of primes being expressed as the problem states.

Introducción

> *Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet.*
> *(He encontrado una prueba maravillosa de este teorema, la cual no cabe en este margen.)*
>
> — Pierre de Fermat

En el mundo matemático, es bien conocida la anécdota de Pierre de Fermat sobre la demostración no escrita por falta de espacio de su *a posteriori* nombrado último teorema:

> "Para n mayor o igual que 3, no existen x, y, z naturales que satisfagan la ecuación
>
> $$x^n + y^n = z^n.$$"

Este teorema, sin embargo, es el segundo de los cuarenta y ocho comentarios que Fermat anotó en su copia del *Arithmetica* de Diofanto. Así describía a su amigo el filósofo inglés Sir Kenelm Digby otros de sus descubrimientos:

> Todo número primo que sobrepasa en una unidad a un múltiplo de cuatro está compuesto por la suma de dos cuadrados. Son ejemplos 5, 13, 17, 29, 37, 41, etc.
>
> Todo número primo que sobrepasa en una unidad a un múltiplo de tres está compuesto por la suma de un cuadrado y el triple de otro cuadrado. Son ejemplos 7, 13, 19, 31, 37, 43, etc.

> Todo número primo que sobrepasa en una o tres unidades a un múltiplo de ocho está compuesto por la suma de un cuadrado y el doble de otro cuadrado. Son ejemplos 3, 11, 17, 19, 41, 43, etc.

El haber notado estos y otros comportamientos y relaciones particulares de los números primos ha otorgado a Fermat el título de *precursor* de la teoría de números moderna, a pesar de no haber demostrado propiamente sus intuiciones. Estos últimos resultados presentan la motivación de este trabajo, el cual tiene como objetivo trabajar el siguiente

Problema. *Dado $n \in \mathbb{Z}$, establecer condiciones sobre un número primo p para que pueda expresarse como*

$$p = x^2 + ny^2, \quad x, y \in \mathbb{Z}.$$

La resolución de este problema forma parte de la teoría algebraica de números clásica y ha motivado a lo largo de los últimos dos siglos importantes avances en esta disciplina. Podemos pues suponer por adelantado que no será tarea fácil ni podremos abarcar toda la casuística, como nos confirman las casi cuatrocientas páginas del libro de David Cox *Primes of the form* $x^2 + ny^2$ [Cox13]. Conforme avancemos en el trabajo, iremos delimitando nuestro campo de estudio hasta dar con éxito los resultados para ciertos n.

El primero de los enunciados de los que Fermat estaba convencido (el caso $n = 1$), se traduce como:

Proposición 0.0.1. Sea p un número primo impar tal que $p \equiv 1 \mod 4$. Entonces, existen $x, y \in \mathbb{Z}$ verificando

$$p = x^2 + y^2.$$

El primero en demostrar este y otros resultados provenientes del ingenio de Fermat fue el célebre Leonhard Euler. Su prueba, aunque perfectamente válida, se hace farragosa por la escasez de buenas herramientas. Pero, ¿cómo atacar un problema meramente aritmético que depende únicamente de números enteros?

Con el tiempo y el desarrollo de distintas ramas de las matemáticas se han dado multitud de pruebas diferentes a la proposición 0.0.1, una de ellas

constando de una única frase (véase [Zag90]). La que interesa al desarrollo de este trabajo es aquella con enfoque algebraico, que considera que la proposición 0.0.1 se puede traducir a ver que un primo congruente con 1 módulo 4 pierde su irreducibilidad en el anillo de enteros gaussianos

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

y factoriza como producto de dos elementos conjugados irreducibles $\alpha = x + yi$, $\overline{\alpha} = x - yi$, obteniendo

$$p = \alpha \cdot \overline{\alpha} = x^2 + y^2.$$

Esta idea encauza el inicio de este trabajo en tratar de descomponer un primo $p \in \mathbb{Z}$ en factores pertenecientes a lugares *parecidos* a $\mathbb{Z}$ dentro de ciertas extensiones algebraicas. En el caso anterior, la extensión donde queremos descomponer p es $\mathbb{Q}(\sqrt{-1})$, y el anillo que se comporta de manera parecida a $\mathbb{Z}$ es $\mathbb{Z}[i]$.

1 | Anillos de enteros

Caminante, no hay camino,
se hace camino al andar.

— Antonio Machado

El objetivo de este capítulo es encontrar la estructura similar a $\mathbb{Z}$ que se menciona en la introducción en otros cuerpos de números algebraicos, es decir, en extensiones finitas de $\mathbb{Q}$. En particular, las extensiones que nos interesan son las cuadráticas $\mathbb{Q}(\sqrt{m})$, con $m \in \mathbb{Z}$ libre de cuadrados.

Definiendo bien la estructura que juega el papel de $\mathbb{Z}$ en cuerpos de números algebraicos, podemos aspirar a encontrar unas propiedades de divisibilidad análogas a las que se dan en el anillo de los enteros $\mathbb{Z}$. Queremos, básicamente, encontrar un equivalente al teorema fundamental de la aritmética: buscamos descomponer elementos de $\mathbb{Q}(\sqrt{m})$ de manera única como producto de "objetos irreducibles" que cumplan el papel de los primos convencionales de $\mathbb{Z}$ en esa estructura misteriosa que necesitamos encontrar.

1.1 Módulos

En esta sección vamos a recordar el concepto de módulo y a probar algunas proposiciones necesarias para llegar a un resultado fundamental para el

desarrollo de este trabajo: dado un anillo, podemos encontrar un subanillo "parecido" a $\mathbb{Z}$ en sentido aritmético.

En adelante, consideraremos que un anillo es conmutativo, tiene elemento unidad y la imagen de éste a través de todos los homomorfismos de anillos es el elemento unidad del anillo de llegada.

Definición 1.1.1. Sea A un anillo. Un *A-módulo* es un grupo conmutativo M sobre el que se define una multiplicación por escalar, es decir, una aplicación de $A \times M$ en M (denotando la imagen de (x, m) como $x \cdot m$ o xm) que satisface:

(a) $(x + y) \cdot m = xm + ym$, con $x, y \in A$, $m \in M$.
(b) $x \cdot (m + n) = xm + xn$, con $x \in A$, $m, n \in M$.
(c) $(xy) \cdot m = x \cdot (ym)$, con $x, y \in A$, $m \in M$.
(d) $1_A \cdot m = m$, con $m \in M$ y 1_A la unidad multiplicativa de A.

Notamos pues que un A-módulo es la generalización del concepto de *espacio vectorial sobre un cuerpo*.

Ejemplos.
1. Un $\mathbb{Z}$-módulo es un grupo abeliano donde $(\pm x)m = \pm(m + \cdots + m)$ x veces, con $x \in \mathbb{Z}$, $x \geq 0$.
2. Si A es un cuerpo, un A-módulo es, como era de esperar, un espacio vectorial.

Definición 1.1.2. Dado un A-módulo M, se dirá que un subgrupo N de M es un *submódulo* si $am \in N$ para todo $a \in A$, $m \in N$. En particular, N es un A-módulo.

Ejemplo. Los ideales de un anillo A son submódulos del A-módulo $M = A$.

Definición 1.1.3. Se dice que un A-módulo M está *finitamente generado* si existen $g_1, \ldots, g_n \in M$ tales que, para todo elemento $x \in M$, existen $a_1, \ldots, a_n \in A$ satisfaciendo

$$x = a_1 g_1 + \cdots + a_n g_n,$$

y se escribe $M = \sum A g_i$.

Definición 1.1.4. Se dice que un A-módulo M es *libre de rango n* si existe una base $\mathcal{B} \subseteq M$ de n elementos que lo genera, es decir, un sistema generador con n elementos linealmente independientes.

Ejemplo. Un $\mathbb{Z}$-módulo libre es un grupo abeliano con una base.

Definición 1.1.5. Sean $a_1, \ldots, a_n \in A$, con A anillo, y B subanillo de A. Sea el homomorfismo de anillos $\varphi : B[X_1, \ldots, X_n] \to A$ que manda la variable X_i al valor a_i. La imagen de φ, denotada por $B[a_1, \ldots, a_n]$, es el menor subanillo de A que contiene a B y a $a_1, \ldots, a_n$, y su expresión explícita es

$$B[a_1, \ldots, a_n] = \left\{ \sum b_{(i)} a_1^{i_1} \cdots a_n^{i_n} \;\middle|\; b_{(i)} \in B \right\}.$$

1.2 Elementos enteros

Tal y como tenemos en el cuerpo de los racionales una aritmética basada en las propiedades de divisibilidad dentro del anillo de los números enteros, nuestro objetivo en esta sección es definir "los enteros" de un anillo cualquiera.

Definición 1.2.1. Sean A un anillo, B un subanillo de A. Decimos que un elemento $x \in A$ es *entero sobre B* cuando existen elementos $b_1, \ldots, b_n \in B$ tales que

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0.$$

Esta definición difiere de la noción usual de elemento *algebraico sobre un cuerpo* precisamente porque nuestra definición es sobre anillos, donde no todos los elementos son unidades. Así, si A y B son cuerpos, un elemento de A será entero sobre B si y sólo si es algebraico sobre B, ya que si $x \in A$ es solución de un polinomio con coeficientes en B, también es solución de un polinomio mónico con coeficientes en B (multiplicando por el inverso del coeficiente líder).

Definición 1.2.2. Sean A un anillo, B un subanillo de A. Diremos que A es *entero sobre B* cuando todo elemento de A es entero sobre B.

Conviene recordar que un dominio de integridad es un anillo conmutativo sin divisores propios de cero.

Definición 1.2.3. Sean A un anillo y B un subanillo de A. Si todo elemento de A entero sobre B pertenece a B, se dice que B es *integralmente cerrado* en A.
Si B es un dominio de integridad, $A = F(B)$ es su cuerpo de fracciones

$$A = F(B) = \left\{ \frac{a}{b} \;\middle|\; a, b \in B, b \neq 0 \right\},$$

y B es integralmente cerrado en A, decimos que B es un *Dominio Integralmente Cerrado* (DIC).

Definición 1.2.4. Sean A un anillo, B un subanillo. El anillo B' de todos los elementos de A enteros sobre B se llama *clausura entera de B en A*.

A partir de la definición 1.2.2 se puede derivar la definición que conocemos de *extensión algebraica de un cuerpo*: si A y B son cuerpos, A es una extensión algebraica de B si A es entero (o, equivalentemente, algebraico) sobre B.

Podemos ahora enunciar un resultado básico sobre elementos enteros.

Proposición 1.2.5. Sean A un subanillo de un dominio de integridad D, $x \in D$. Son equivalentes:

1. x es entero sobre A.
2. $A[x]$ es un A-módulo finitamente generado.
3. Existe un subanillo A' de D que contiene a $A[x]$ y está finitamente generado como A-módulo.

Demostración. [Ful89, § 1.9]. □

Proposición 1.2.6. Sean D un dominio de integridad, A un subanillo, y $x_1, \ldots, x_n \in D$. Si x_1 es entero sobre A, si x_2 es entero sobre $A[x_1]$, ..., si x_n es entero sobre $A[x_1, \ldots, x_{n-1}]$, entonces $A[x_1, \ldots, x_n]$ es un A-módulo finitamente generado.

Demostración. Por la proposición 1.2.5, $A[x_1]$ es un A-módulo finitamente generado y $A[x_1, x_2]$ es un $A[x_1]$-módulo finitamente generado, luego $A[x_1, x_2]$ es un A-módulo finitamente generado. El resto de la prueba es

similar. □

Las proposiciones 1.2.5 y 1.2.6 nos permiten enunciar uno de los resultados fundamentales del capítulo:

Proposición 1.2.7. Sea A un subanillo de un dominio de integridad D. El conjunto de elementos de D que son enteros sobre A es un subanillo de D que contiene a A, es integralmente cerrado en D y entero sobre A.

Demostración. Sea A' el conjunto de los elementos de D enteros sobre A. Es claro que $A \subseteq A'$, ya que todo elemento $a \in A$ es raíz del polinomio $X - a$.

Sean $a_1, a_2 \in A'$. De acuerdo con la definición 1.1.5, los elementos $a_1 \pm a_2$ y $a_1 \cdot a_2$ están en el anillo $A[a_1, a_2]$, luego $A[a_1 \pm a_2] \subset A[a_1, a_2]$, $A[a_1 \cdot a_2] \subset A[a_1, a_2]$. Por la proposición 1.2.6, $A[a_1, a_2]$ es un A-módulo finitamente generado, luego por la proposición 1.2.5 (3), $a_1 \pm a_2$, $a_1 \cdot a_2$ son enteros sobre A y por tanto pertenecen a A'. Esto implica que A' es un anillo.

El resto de detalles se pueden ver en el libro de Ribenboim [Rib01, § 5.1]. □

Las siguientes dos proposiciones pueden no parecer muy útiles en este capítulo, pero más adelante revelarán su verdadero propósito. Caminante, no hay camino.

Proposición 1.2.8. Sea D un dominio de integridad entero sobre un subanillo A. Si I es un ideal no nulo de D, entonces $I \cap A \neq 0$.

Demostración. Sea $x \in I$, $x \neq 0$. En particular, $x \in D$, luego existen $a_1, \ldots, a_n \in A$ tales que

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0.$$

Podemos suponer $a_n \neq 0$, ya que, si fuera nulo, podríamos sacar x como factor común (por ser D dominio de integridad) y obtendríamos la ecuación anterior con un subíndice y un exponente menos.

Por tanto,

$$a_n = -x(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}) \in I \cap A. \qquad \square$$

Proposición 1.2.9. Sea D un dominio de integridad entero sobre un subanillo A. Entonces, D es un cuerpo si, y sólo si, A también lo es.

Demostración. $\boxed{\Longrightarrow}$ Supongamos D cuerpo, y $x \in A$, $x \neq 0$. Como $x \in D$, consideramos x^{-1}, el inverso de x, para el cual existen $a_1, \ldots, a_n \in A$ tales que

$$(x^{-1})^n + a_1(x^{-1})^{n-1} + \cdots + a_{n-1}x^{-1} + a_n = 0,$$

por ser D entero sobre A. Multiplicando por x^{n-1} a ambos lados, obtenemos

$$x^{-1} + a_1 + a_2x + \cdots + a_nx^{n-1} = 0$$

$$\Longrightarrow\ x^{-1} = -(a_1 + a_2x + \cdots + a_nx^{n-1}) \in A,$$

luego A contiene a los inversos de sus elementos y por tanto es un cuerpo.

$\boxed{\Longleftarrow}$ Supongamos A cuerpo. Sea $x \in D$, con $x \neq 0$, y consideremos $\langle x \rangle \subseteq D$. Por la proposición 1.2.8, $A \cap \langle x \rangle \neq 0$, luego debe existir un elemento $a \in A$ en esa intersección, con $a = bx$, $b \in D$.

Sea $a^{-1} \in A$ el inverso de a. Como A es subanillo de D, $a^{-1} \in D$. Tenemos $1 = aa^{-1} = bxa^{-1} = (ba^{-1})x$, luego x tiene inverso en D, y D es un cuerpo. □

Observación 1.2.10. Conviene recordar la siguiente cadena de implicaciones:

$$\text{Dominio Euclídeo (DE)} \Longrightarrow \text{Dominio de Ideales Principales (DIP)} \Longrightarrow$$

$$\Longrightarrow \text{Dominio de Factorización Única (DFU).}$$

Proposición 1.2.11. Todo DFU es un DIC.

Demostración. Sean A un DFU, $K = F(A)$ su cuerpo de fracciones, $x \in K$, con $x \neq 0$. Tenemos por tanto $x = a/b$, con $a, b \in A$ y $a, b \neq 0$. Podemos suponer $\text{mcd}(a, b) = 1$, si no fuese así, se reduciría la fracción.

Si x es entero sobre A, existen $c_1, \ldots, c_n \in A$ tales que

$$\left(\frac{a}{b}\right)^n + c_1\left(\frac{a}{b}\right)^{n-1} + \cdots + c_{n-1}\left(\frac{a}{b}\right) + c_n = 0.$$

Multiplicando por b^n a ambos lados, obtenemos

$$a^n + c_1 a^{n-1} b + \cdots + c_{n-1} a b^{n-1} + c_n b^n = 0$$
$$\implies a^n = -b(c_1 a^{n-1} + \cdots + c_{n-1} a b^{n-2} + c_n b^{n-1}),$$

es decir, b divide a a^n. Como tenemos $\mathrm{mcd}(a, b) = 1$, a^n y b tampoco tienen factores comunes y por tanto $\mathrm{mcd}(a^n, b) = 1$. Esto no deja otra opción a b que ser la unidad multiplicativa, luego $x \in A$, y A es un DIC. □

1.3 Anillos de enteros algebraicos

En esta sección vamos a particularizar lo visto en la anterior para el caso de una extensión finita de $\mathbb{Q}$, a la que llamaremos K. ¿Existe una factorización análoga a la definida sobre $\mathbb{Z}$ en $\mathbb{Q}$? Si existe, ¿es única salvo orden y producto por unidades? Con estas preguntas empieza nuestro viaje por la teoría algebraica de números.

En adelante, trabajaremos dentro de un cuerpo de números K, al que le pediremos que sea una extensión de Galois.

Definición 1.3.1. Un número algebraico raíz de un polinomio mónico con coeficientes en $\mathbb{Z}$ se llama *entero algebraico*.

Los elementos de $\mathbb{Z}$, para no dar pie a confusión, se suelen llamar *enteros racionales*.

Observación 1.3.2. Los conjugados de un entero algebraico son enteros algebraicos.

Observación 1.3.3. Si denotamos por $\mathcal{O}_K$ al anillo de todos los enteros algebraicos de K (el obtenido a partir de la proposición 1.2.7), entonces $\mathcal{O}_K$ es un DIC, y $\mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$.

Definición 1.3.4. Dado $x \in K$, se definen su traza y su norma como

$$\mathrm{Tr}(x) = \sum_\sigma \sigma(x) \quad \text{y} \quad \mathrm{N}(x) = \prod_\sigma \sigma(x),$$

donde σ recorre los automorfismos de $\mathrm{Gal}(K/\mathbb{Q})$.

Observación 1.3.5. La definición anterior no debe asustarnos: la traza de un elemento $x \in K$ es la suma de sus conjugados, y la norma es el producto.

Observación 1.3.6. La traza y la norma de un entero algebraico son enteros racionales, ya que pertenecen a $\mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$.

En $\mathbb{Q}$ tenemos que todos los elementos de $\mathbb{Z}$ salvo el subconjunto $\{0, \pm 1\}$ se pueden descomponer en producto de primos de manera única salvo orden y producto por unidades (las unidades de los enteros racionales son $\{\pm 1\}$), ya que $\mathbb{Z}$ es un DFU. Ahora tenemos que identificar las unidades y los análogos a los números primos en K.

Proposición 1.3.7. Un entero algebraico x es una unidad si, y sólo si, $\mathrm{N}(x) = \pm 1$.

Demostración. $\boxed{\Longrightarrow}$ Sea $x \in \mathcal{O}_K$ unidad, es decir, tal que existe $x' \in \mathcal{O}_K$ con $xx' = 1$. Aplicando normas, $\mathrm{N}(xx') = \mathrm{N}(x)\,\mathrm{N}(x') = \mathrm{N}(1) = 1$, por lo que $\mathrm{N}(x)$ es una unidad de $\mathbb{Z}$, es decir, $\mathrm{N}(x) = \pm 1$.

$\boxed{\Longleftarrow}$ Supongamos $x \in \mathcal{O}_K$ tal que $\mathrm{N}(x) = \pm 1$. Sea x' el producto de todos los conjugados de x distintos de x, obteniendo $xx' = \pm 1$. Por la observación 1.3.2, $x' \in \mathcal{O}_K$, luego x divide a 1 en $\mathcal{O}_K$, y por tanto es una unidad. □

Lema 1.3.8. Sea D un dominio de integridad satisfaciendo la *condición de la cadena ascendente para ideales principales*: si

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots \subseteq \langle a_n \rangle \subseteq \cdots$$

es una cadena ascendente de ideales principales de D, existe un $n \in \mathbb{N}$ tal que

$$\langle a_n \rangle = \langle a_{n+1} \rangle = \cdots .$$

Entonces todo elemento distinto de cero y no unidad de D se puede escribir como producto de elementos irreducibles.

Demostración. Sea $a \in D$, $a \neq 0$ y no unidad. Entonces, o a es irreducible o existe un elemento $a_1 \in D$ dividiendo a a, es decir, tal que $\langle a \rangle \subset \langle a_1 \rangle$. Repitiendo el razonamiento para a_1, tenemos que, si no es irreducible, existe un $a_2 \in D$ tal que $\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle$. Por hipótesis, debemos llegar en algún

momento a un elemento $a_n \in D$ irreducible. Hemos probado por tanto que, dado un elemento $a \in D$, existe un $p_1 \in D$ irreducible tal que $p_1 \mid a$, y por tanto existe un $b_1 \in D$, $b_1 \neq 0$ tal que $a = p_1 b_1$, y $\langle a \rangle \subset \langle b_1 \rangle$. Si a no es irreducible, b_1 no es una unidad y, por tanto, repitiendo el razonamiento anterior, existe un elemento $p_2 \in D$ irreducible tal que $b_1 = p_2 b_2$, con $b_2 \in D$ y no nulo. Tenemos pues $a = p_1 p_2 b_2$, $\langle a \rangle \subset \langle b_1 \rangle \subset \langle b_2 \rangle$. Por hipótesis, debemos llegar a un $b_m \in D$ que sea unidad, luego $a = p_1 p_2 \cdots p_m b_m$, con p_i irreducible para todo $i = 1, \ldots, m$, es decir, $a \in D$, si no es irreducible, es producto de elementos irreducibles. □

Proposición 1.3.9. Sea $\mathcal{O}_K$ el anillo de enteros algebraicos de un cuerpo de números K. Entonces, dado $x \in \mathcal{O}_K$, $x \neq 0$ y no unidad, podemos escribirlo como producto de elementos irreducibles de $\mathcal{O}_K$.

Demostración. Sea $\langle x_1 \rangle \subseteq \langle x_2 \rangle \subseteq \cdots$ la cadena ascendente de ideales principales de $\mathcal{O}_K$. Por la inclusión de ideales, tenemos $x_1 = a x_2$, y tomando normas en K, $\mathrm{N}(x_1) = \mathrm{N}(a x_2) = \mathrm{N}(a)\,\mathrm{N}(x_2)$. Por la observación 1.3.6, las normas anteriores son enteros racionales, luego $\mathrm{N}(x_2)$ divide a $\mathrm{N}(x_1)$. Iterando este argumento, obtenemos que $\mathrm{N}(x_n)$ divide a $\mathrm{N}(x_1)$ para todo $n \geq 1$.

Por otra parte, un entero racional tiene un número finito de divisores, por lo tanto debe existir un n tal que $|\mathrm{N}(x_{n+1})| = |\mathrm{N}(x_n)|$, lo cual implica $x_n = c x_{n+1}$, con $c \in \mathcal{O}_K$ y $\mathrm{N}(c) = \pm 1$. Por la proposición 1.3.7, c es una unidad, luego $\langle x_n \rangle = \langle x_{n+1} \rangle$ y, en virtud del lema 1.3.8, todo elemento de $\mathcal{O}_K$ distinto de cero y no unidad se puede escribir como producto de elementos irreducibles. □

He aquí nuestra primera victoria: en una extensión finita de $\mathbb{Q}$, podemos encontrar un anillo tal que sus elementos se pueden descomponer en producto de irreducibles. Eso quiere decir, retrayéndonos a la introducción y al anillo de enteros gaussianos, que en $\mathbb{Z}[i]$ efectivamente podemos ver qué condiciones cumple un primo $p \in \mathbb{Z}$ para no ser primo en $\mathbb{Z}[i]$.

La victoria no es, sin embargo, tan dulce como se podría esperar. La proposición 1.3.9 nos asegura que, dado un elemento del anillo de enteros de una extensión, se puede encontrar una descomposición de éste en elementos irreducibles, pero no nos dice nada sobre la unicidad (entendiendo unici-

dad salvo orden y producto por unidades) de esa descomposición. En el caso particular de $\mathbb{Z}[i]$ no tenemos problema ya que es un DFU, pero en general no podemos asegurar la unicidad de descomposición en $\mathcal{O}_K$ para cualquier extensión K de $\mathbb{Q}$.

1.4 Enteros de extensiones cuadráticas

Como se expresó al principio de este capítulo, nuestro interés recae en extensiones cuadráticas de $\mathbb{Q}$. Para esta sección, por tanto, consideraremos $K = \mathbb{Q}(\sqrt{m})$, con $m \in \mathbb{Z}$ libre de cuadrados, y tendremos como objetivo obtener información sobre $\mathcal{O}_K$. Cabe recordar que un elemento de K es del tipo $a + b\sqrt{m}$, con $a, b \in \mathbb{Q}$.

Proposición 1.4.1. Un elemento $x = a + b\sqrt{m} \in K$ pertenece a $\mathcal{O}_K$ si, y sólo si, $2a = u \in \mathbb{Z}$, $2b = v \in \mathbb{Z}$, y $u^2 - mv^2 \equiv 0 \mod 4$.

Demostración. El truco de esta prueba está en utilizar que la traza y la norma de x son enteros racionales, y en notar que por tanto $u^2 = (2a)^2$ y $v^2 = (2b)^2$ implican $u^2 - mv^2 \in 4\mathbb{Z}$. Se puede encontrar con todos los detalles en el libro de Ribenboim [Rib01, § 5.4]. □

Este resultado se puede reformular obteniendo la siguiente

Proposición 1.4.2. Si $m \equiv 2 \mod 4$ o $m \equiv 3 \mod 4$, entonces

$$\mathcal{O}_K = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}.$$

Si $m \equiv 1 \mod 4$, entonces

$$\mathcal{O}_K = \left\{ \frac{u + v\sqrt{m}}{2} \,\middle|\, u, v \in \mathbb{Z},\ u \text{ y } v \text{ con la misma paridad} \right\}.$$

Demostración. Veamos qué ocurre caso por caso.

Supongamos $m \equiv 2 \mod 4$.

u	par	par	impar	impar	
v	par	impar	par	impar	
$u^2 - mv^2 \equiv$	0	2	1	3	mód 4

Sea $x = a + b\sqrt{m} \in \mathcal{O}_K$. Según la proposición anterior, debe ser $u^2 - mv^2 \equiv 0 \mod 4$, lo cual sólo se da si tanto $u = 2a$ como $v = 2b$ son pares. Esto ocurre si y sólo si a y b pertenecen a $\mathbb{Z}$.

Supongamos ahora $m \equiv 3 \mod 4$.

u	par	par	impar	impar	
v	par	impar	par	impar	
$u^2 - mv^2 \equiv$	0	1	1	2	mód 4

Observamos que este caso es análogo al anterior: a y b deben ser enteros racionales para que se satisfaga la condición de la proposición 1.4.1.

Por último, consideremos $m \equiv 1 \mod 4$.

u	par	par	impar	impar	
v	par	impar	par	impar	
$u^2 - mv^2 \equiv$	0	3	1	0	mód 4

Escribiendo $a = u/2$ y $b = v/2$, obtenemos el resultado. □

Para ilustrar la problemática de la no unicidad de factorización en una extensión cualquiera, consideremos el siguiente ejemplo:

Ejemplo 1.4.3. Sea $K = \mathbb{Q}(\sqrt{-5})$, con $\mathcal{O}_K = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{-5}]$ por el resultado anterior.

Podemos escribir

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right).$$

Veamos que 2, 3, $1 + \sqrt{-5}$ y $1 - \sqrt{-5}$ son irreducibles en $\mathbb{Z}[\sqrt{-5}]$. Supongamos $x, y \in \mathbb{Z}[\sqrt{-5}]$ no unidades tales que $2 = x \cdot y$. Tomando normas,

tenemos $4 = \mathrm{N}(x)\,\mathrm{N}(y)$. La única opción es $\mathrm{N}(x) = \mathrm{N}(y) = 2$, ya que la norma es un entero racional.

Sea $x = a + b\sqrt{-5}$ la expresión de x.

$$N(x) = a^2 + 5b^2 = 2,$$

lo cual es imposible si $a, b \in \mathbb{Z}$. El mismo razonamiento se puede seguir con el 3, para el cual tendríamos $\mathrm{N}(x) = \mathrm{N}(y) = 3$. En el caso de $(1 + \sqrt{-5})$ y $(1 - \sqrt{-5})$ tendríamos $\mathrm{N}(x) = 2$ y $\mathrm{N}(y) = 3$, o bien $\mathrm{N}(x) = 3$ y $\mathrm{N}(y) = 2$, y quedarían cubiertos sus casos por los del 2 y el 3.

Ahora tenemos que cerciorarnos de que estas dos descomposiciones son efectivamente distintas, es decir, que ninguno de esos elementos irreducibles está asociado con algún otro. Supongamos, por ejemplo, que 2 estuviera asociado con $(1 + \sqrt{-5})$, *i. e.*,

$$2 = u(1 + \sqrt{-5}), \quad u \text{ unidad de } K.$$

Esto implicaría, igualando de nuevo normas, $4 = \pm 6$, lo cual es absurdo. El razonamiento para el resto de combinaciones con $(1 - \sqrt{-5})$ y 3 es análogo. Concluimos por tanto que en $\mathbb{Q}(\sqrt{-5})$ podemos encontrar dos descomposiciones distintas para el elemento 6.

Resumen

1. Si K es una extensión finita de $\mathbb{Q}$, el conjunto de los enteros algebraicos sobre ella $\mathcal{O}_K$ es un anillo.

2. En $\mathcal{O}_K$ existe una descomposición en irreducibles para todo entero algebraico no unidad y distinto de 0, pero dicha descomposición no tiene por qué ser única, entendiéndose unicidad salvo orden y producto por unidades.

2 | Descomposición de ideales

L'algèbre est généreuse: elle done souvent plus que ce qu'on lui demande.
(El álgebra es generosa: siempre nos dice más de lo que le preguntamos.)

— Jean D'Alembert

En el capítulo anterior nos hemos topado con que en una extensión finita de $\mathbb{Q}$ la divisibilidad no se comporta en su anillo de enteros tan bien como en $\mathbb{Z}$. Para nuestro objetivo, que es estudiar la descomposición de números primos en el anillo de enteros de extensiones cuadráticas, esto supone un grave contratiempo: no tenemos garantías de que, dado un primo $p \in \mathbb{Z}$, éste tenga o no una descomposición en una extensión cuadrática que haga que p se pueda escribir como $p = x^2 + ny^2$, con $n, x, y \in \mathbb{Z}$, n fijado previamente.

Ernst Kummer, trabajando en la demostración del último teorema de Fermat y trasladando la prueba a extensiones algebraicas, notó el problema de la no unicidad de factorización. Su teoría era que, en el ejemplo 1.4.3, el número 6 no estaba del todo descompuesto; debían existir unos ciertos *elementos ideales* que descompusieran de manera única totalmente al 6. Estos elementos ideales fueron definidos por Richard Dedekind y son, como cabía esperar, los ideales que conocemos. La razón por la que nos ocupamos de ellos en este capítulo radica en la gran importancia que tienen en la teoría de números algebraica: los ideales del anillo de enteros de una extensión algebraica factorizan de manera única en ideales primos. Todos los detalles teóricos y del significado de esta unicidad se tratan de aquí en adelante.

2.1 Anillos noetherianos

En esta sección nos interesaremos por un tipo específico de anillo, noción necesaria para llegar al resultado que buscamos sobre descomposición de ideales. No obstante, antes de llegar al objeto de estudio en cuestión, necesitamos un poco de artillería algebraica que sirva para probar lo que concierne a esta sección.

Definición 2.1.1. Dado un anillo A, un A-módulo M se dice que es *noetheriano* si todo submódulo de M está finitamente generado.

Este tipo de módulos recibe su nombre en honor a Emmy Noether, gran contribuidora al estudio de las diferentes estructuras algebraicas y en particular de los módulos.

Un resultado bien conocido de álgebra conmutativa es la siguiente caracterización de módulos noetherianos:

Proposición 2.1.2. Sean A un anillo, M un A-módulo. Son equivalentes:

1. M es noetheriano.
2. Toda cadena ascendente $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ de submódulos de M es finita.
3. Toda familia no vacía de submódulos de M tiene un elemento maximal respecto a la relación de inclusión.

Demostración. $\boxed{1 \implies 2}$ Sea $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ una cadena ascendente de submódulos de M, y consideremos $N = \cup_j N_j$, unión de todos los submódulos de la cadena. Por hipótesis, N está finitamente generado por unos ciertos $g_1, \ldots, g_n \in N$, luego para cada $i \in \{1, \ldots, n\}$ debe existir un j_i tal que $g_i \in N_{j_i}$. Sea $m \geq j_i$ para todo $i \in \{1, \ldots, n\}$. Tenemos que $g_i \in N_m$ para todos los i anteriores, luego forzosamente debe ser $N = N_m$, *i. e.*, $N_m = N_{m+1} = \cdots$.

$\boxed{2 \implies 3}$ Sea $\mathcal{M}$ una familia no vacía de submódulos de M. Sea $N_1 \in \mathcal{M}$. Si N_1 no es maximal, existe un $N_2 \in \mathcal{M}$ tal que $N_1 \subseteq N_2$. Si N_2 no es maximal, repetimos el razonamiento. Este procedimiento es finito por hipótesis, luego debe existir un elemento maximal en $\mathcal{M}$.

$\boxed{3 \implies 1}$ Supongamos, por reducción al absurdo, que existe N submódulo de M no finitamente generado. Sea $\mathcal{M}$ la familia de todos los submódulos de M finitamente generados contenidos en N (esta familia es no vacía ya que $0 \in \mathcal{M}$). Sea N' el elemento maximal de $\mathcal{M}$, $N' \neq N$. Sea $x \in N$, con $x \notin N'$. El submódulo $N' + Ax \subseteq N$ está finitamente generado y por tanto pertenece a $\mathcal{M}$, sin embargo $N' \subset N' + Ax$, lo que contradice la maximalidad de N'. Concluimos que no existe tal submódulo N de M no finitamente generado. □

Corolario 2.1.3. Sea M un A-módulo noetheriano. Para todo N submódulo de M, se tiene que N y M/N son noetherianos.

Particularizando la definición 2.1.1 al caso del A-módulo $M = A$, obtenemos el objeto que buscábamos.

Definición 2.1.4. Un anillo A se dice *noetheriano* cuando todos sus ideales están finitamente generados.

Podemos por tanto reescribir la proposición 2.1.2 para obtener un resultado clásico de anillos noetherianos.

Proposición 2.1.5. Sea A un anillo. Son equivalentes:

1. A es noetheriano.
2. Toda cadena ascendente $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ de ideales de A es finita.
3. Toda familia no vacía de ideales de A tiene un elemento maximal respecto a la relación de inclusión.

Observación 2.1.6. Todo DIP es un anillo noetheriano.

Observación 2.1.7. Si I es un ideal de un anillo noetheriano A tal que $I \neq A$ (esto es, si I es un ideal propio de A), I está contenido en un ideal maximal.

Para llegar a un resultado importante de esta sección, necesitamos ver un par de detalles previos.

Proposición 2.1.8. Si A es un anillo noetheriano y M es un A-módulo finitamente generado, M es un módulo noetheriano.

Demostración. [Rib01, § 6.1]. □

Lema 2.1.9. Sean A un DIC, F su cuerpo de fracciones, K una extensión separable de grado n de F, B la clausura entera de A en K. Existen A-módulos libres M y M' de rango n tales que $M' \subseteq B \subseteq M$.

Demostración. [Rib01, § 6.1]. □

Ya estamos listos para enunciar y probar el resultado que queríamos mostrar en esta sección.

Proposición 2.1.10. El anillo de enteros de un cuerpo de números es noetheriano.

Demostración. Consideremos el DIC $\mathbb{Z}$, su cuerpo de fracciones $\mathbb{Q}$, K un cuerpo de números, y $\mathcal{O}_K$ el anillo de enteros de K (o sea, la clausura entera de $\mathbb{Z}$ en K). Por el lema 2.1.9, $\mathcal{O}_K \subseteq G$, con G grupo abeliano libre de rango finito. $\mathbb{Z}$ es un anillo noetheriano por ser DIP, luego por la proposición 2.1.8, G es un $\mathbb{Z}$-módulo noetheriano, y por el corolario 2.1.3, $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo noetheriano. Al tener $\mathbb{Z} \subseteq Ok$, todo $\mathcal{O}_K$-submódulo de $\mathcal{O}_K$ es a su vez un $\mathbb{Z}$-submódulo de $\mathcal{O}_K$, y como $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo noetheriano, cualquier cadena creciente de $\mathcal{O}_K$-submódulos de $\mathcal{O}_K$ es finita. Por la proposición 2.1.2, $\mathcal{O}_K$ es un $\mathcal{O}_K$-módulo noetheriano, o sea, un anillo noetheriano. □

2.2 Divisibilidad en ideales

En la sección anterior nos hemos preocupado por los generadores de los ideales del anillo de enteros de un cuerpo de números, y hemos concluido que son finitos. En esta sección vamos a ver qué condiciones necesitamos para que un ideal pueda ser descompuesto en producto de ideales primos.

En adelante consideraremos que un anillo es un dominio de integridad.

Definición 2.2.1. Sean A anillo, F su cuerpo de fracciones. Un A-módulo M contenido en F se dice que es un *ideal fraccional de* A cuando existe un elemento $a \in A$, $a \neq 0$, tal que $a \cdot M \subseteq A$.

Es evidente que todo ideal de un anillo A es fraccional, basta con tomar $a = 1$. Para evitar confusiones, a los ideales de A los llamaremos *ideales*

enteros.

Podemos asociar una operación de multiplicación a los ideales fraccionales como una extensión de la usual definida sobre ideales enteros. Sean $\mathcal{F}$ el conjunto de ideales fraccionales no nulos de un anillo A, y $M, M' \in \mathcal{F}$. Se define

$$M \cdot M' = \left\{ \sum_{i=1}^{n} x_i x_i' \mid n \geq 1, x_i \in M, x_i' \in M' \right\}.$$

Observación 2.2.2. La operación que acabamos de definir es cerrada: el producto de ideales fraccionales es a su vez un ideal fraccional. Además, esta operación es conmutativa, asociativa y tiene elemento neutro (el propio anillo A visto como ideal: $M \cdot A = M$).

Definición 2.2.3. Un ideal fraccional M de un anillo A se dice *invertible* cuando existe otro ideal fraccional M' tal que $M \cdot M' = A$.

Definición 2.2.4. Sean A un anillo, M y N ideales fraccionales de A. Se dice que M *divide a* N, escrito $M \mid N$, cuando existe un ideal entero $I \subseteq A$ tal que $M \cdot I = N$.

De estas definiciones se obtienen unas propiedades inmediatas y sencillas de probar.

Proposición 2.2.5. Sean M, M', M'' ideales fraccionales no nulos de un anillo A. Se verifican:

1. $M \mid M$.
2. Si $M \mid M'$ y $M' \mid M''$, entonces $M \mid M''$.
3. Si $M \mid M'$, entonces $M' \subseteq M$.
4. Si $M \mid M'$ y $M' \mid M$, entonces $M = M'$.

Demostración.

1. $M \cdot 1 = M$, luego $M \mid M$ por la definición 2.2.4.
2. Sean $I, J \subseteq A$ ideales enteros tales que $M \cdot I = M'$, $M' \cdot J = M''$. Claramente se tiene $I \cdot J \subseteq A$, y $M \cdot I \cdot J = M' \cdot J = M''$, luego $M \mid M''$.
3. Existe $I \subseteq A$ ideal entero tal que $M' = I \cdot M \subseteq A \cdot M = M$.
4. Por el apartado anterior, $M' \subseteq M$ y $M \subseteq M'$. Por doble contención, $M = M'$. □

Proposición 2.2.6. Sean A un anillo, F su cuerpo de fracciones. Dado I ideal no nulo de A, se define

$$I^{-1} = \{x \in F \mid xI \subseteq A\}.$$

Entonces:

1. I^{-1} es un ideal fraccional, $A \subseteq I^{-1}$, e $I \subseteq I \cdot I^{-1} \subseteq A$.
2. Si $I \subseteq A$ es un ideal no nulo, I será invertible si, y sólo si, $I \cdot I^{-1} = A$.

Demostración. 1. Veamos que I^{-1} forma un grupo con la suma.

   a) La operación es interna: sean $I, J \subseteq A$ tales que $xI \subseteq A$, $yJ \subseteq A$, con $x, y \in F$. Tenemos que $I \cdot J \subseteq A$, y evidentemente $(x+y)I \cdot J \subseteq A$, luego si $x, y \in I^{-1}$, se tiene $x + y \in I^{-1}$.
   b) La operación es asociativa: esta propiedad se hereda de que los elementos de I^{-1} provienen del cuerpo de fracciones de un anillo conmutativo.
   c) Existe elemento neutro: $0 \in I^{-1}$ ya que $\langle 0 \rangle \subseteq A$.
   d) Existe elemento simétrico: trivialmente, dados un ideal $I \subseteq A$ y un elemento $x \in F$, si $xI \subseteq A$, también se tendrá $(-x)I \subseteq A$.

   I^{-1} es por tanto un A-módulo de acuerdo con la definición 1.1.1, y si tomamos $a \in I$, tenemos que $aI^{-1} \subseteq I \cdot I^{-1} \subseteq A$, luego es un ideal fraccional de A. Como $1 \in I^{-1}$ de manera trivial, obtenemos que $A \subseteq I^{-1}$.

2. $\boxed{\Longleftarrow}$ Inmediato por la definición 2.2.3.

   $\boxed{\Longrightarrow}$ Supongamos I invertible, J el ideal fraccional tal que $I \cdot J = A$. La contención $I \cdot I^{-1} \subseteq A$ la tenemos por el apartado anterior. Veamos ahora la contraria. Sea $x \in A$, es decir,

$$x = \sum_{i=1}^{n} a_i b_i, \quad n \geq 1,\ a_i \in I,\ b_i \in J\ \forall i = 1, \ldots, n.$$

   Aquí, cada b_i está en F (por ser $J \subseteq F$), y es tal que $b_i \cdot I \subseteq A$. Así, $b_i \in I^{-1}$ para todo $i = 1, \ldots, n$, y por tanto $x \in I \cdot I^{-1}$, lo que prueba $A \subseteq I \cdot I^{-1}$. □

Observación 2.2.7. Dado I en las condiciones de la proposición 2.2.6, elevar I a potencias negativas no es más que operar, como intuitivamente podamos pensar,

$$I^{-n} = I^{-1} \cdots I^{-1} \quad n \text{ veces.}$$

Observación 2.2.8. Notemos que, en virtud de la proposición 2.2.5, la divisibilidad entre ideales fraccionales no nulos de un anillo es una relación de orden.

Observación 2.2.9. Dados $a, b \in F$, con F cuerpo de fracciones de un anillo A, a divide a b si, y sólo si, el ideal fraccional principal $\langle a \rangle$ divide al ideal fraccional principal $\langle b \rangle$.

Observación 2.2.10. Conviene recordar los siguientes resultados de cocientes entre anillos e ideales. Sean A un anillo (no necesariamente dominio de integridad), I un ideal de A.

$$I \text{ es primo} \iff {}^{A}\!/_{I} \text{ es un dominio de integridad,}$$
$$I \text{ es maximal} \iff {}^{A}\!/_{I} \text{ es un cuerpo.}$$

En $\mathbb{Z}$, los números primos juegan un papel básico no sólo en la divisibilidad numérica, sino también en la de ideales. Recordemos que los ideales primos de $\mathbb{Z}$ son de la forma $\langle p \rangle$, con p número primo. Además, $\mathbb{Z}/p\mathbb{Z}$ es cuerpo si p es primo, luego en particular $\langle p \rangle$ es maximal. En general, en un DIP, ser ideal primo no nulo es equivalente a ser maximal. Veamos qué ocurre en una extensión finita K.

Proposición 2.2.11. Sea $\mathcal{O}_K$ el anillo de enteros algebraicos de un cuerpo de números K. Todo ideal primo no nulo $\mathfrak{p} \subset \mathcal{O}_K$ es maximal, y contiene exactamente un número primo $p \in \mathbb{Z}$. Más aún, $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo finito conteniendo a $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Demostración. Sea $\mathfrak{p}$ un ideal primo no nulo de $\mathcal{O}_K$. Como $\mathcal{O}_K$ es entero sobre $\mathbb{Z}$, $\mathfrak{p} \cap \mathbb{Z}$ es un ideal no nulo de $\mathbb{Z}$ por la proposición 1.2.8, el cual es evidentemente primo. Por tanto, $\mathfrak{p} \cap \mathbb{Z} = \langle p \rangle$, para algún primo $p \in \mathbb{Z}$. El ideal $\mathfrak{p}$ no puede contener ningún otro primo p'; de ser así, por la identidad de Bézout, tendríamos $\alpha, \beta \in \mathbb{Z}$ tales que $1 = \alpha p + \beta p'$ y por tanto $1 \in \mathfrak{p}$, lo cual no puede ser ya que $\mathfrak{p} \subsetneq \mathcal{O}_K$.

Como $\mathcal{O}_K$ es entero sobre $\mathbb{Z}$ y $\langle p \rangle \subset \mathfrak{p}$, $\mathcal{O}_K/\mathfrak{p}$ es entero sobre $\mathbb{Z}/\langle p \rangle = \mathbb{F}_p$, el cual es un cuerpo. Por la proposición 1.2.9, $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo, y por tanto $\mathfrak{p}$ es maximal.

Para ver ahora que es finito, nos retrotraemos a la prueba de la proposición 2.1.10 hasta llegar a que $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo noetheriano. Escribámoslo en virtud de la definición 1.1.3 como $\mathcal{O}_K = \sum \mathbb{Z} g_i$, con g_i los generadores de $\mathcal{O}_K$, $i = 1, \ldots, n$. Al tener $\langle p \rangle \subset \mathfrak{p}$, obtenemos

$$\mathcal{O}_K\!/\mathfrak{p} \;\subset\; \mathcal{O}_K\!/\langle p \rangle \;=\; \sum \mathbb{Z} g_i\!/\langle p \rangle,$$

donde en el último cociente hay una cantidad finita de elementos (exactamente p^n). Concluimos así que $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo finito conteniendo a $\mathbb{F}_p$. □

Observación 2.2.12. La proposición 2.2.11 nos da una reformulación de la observación 2.1.7: todo ideal propio no nulo de $\mathcal{O}_K$ está contenido en un ideal primo $\mathfrak{p} \subset \mathcal{O}_K$.

2.3 Dominios de Dedekind

Hasta ahora hemos probado que el anillo de enteros de un cuerpo de números es noetheriano y tal que todo ideal primo no nulo del anillo es maximal. En esta sección vamos a ver cómo esas características hacen que podamos encontrar en él la descomposición que tantas carencias presenta la divisibilidad numérica usual.

Veamos algunos resultados necesarios para probar el teorema fundamental de esta sección. Recordamos que un anillo será dominio de integridad salvo que se especifique lo contrario.

Proposición 2.3.1. Sean A un anillo, $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ ideales primos invertibles de A, $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Entonces, si $I = \mathfrak{p}'_1 \cdots \mathfrak{p}'_s$, con $\mathfrak{p}'_i$ ideal primo para todo $i = 1, \ldots, s$, se tiene $s = r$ y, tras cierta permutación de subíndices, $\mathfrak{p}'_i = \mathfrak{p}_i$ para todo $i = 1, \ldots, r$.

Demostración. Sea $\mathfrak{p}_1$ el ideal minimal (con respecto a la inclusión) entre $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$. Por la proposición 2.2.5, $\mathfrak{p}_1 \supseteq I = \mathfrak{p}'_1 \cdots \mathfrak{p}'_s$, por lo que debe existir un subíndice, por ejemplo $i = 1$, tal que $\mathfrak{p}_1 \supseteq \mathfrak{p}'_1$. De la misma forma, $\mathfrak{p}'_1 \supseteq I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, por lo que $\mathfrak{p}'_1 \supseteq \mathfrak{p}_i$ para algún $i = 1, \ldots, r$, y por la minimalidad de $\mathfrak{p}_1$, tal subíndice es $i = 1$, luego $\mathfrak{p}_1 = \mathfrak{p}'_1$.

Como $\mathfrak{p}_1$ es invertible, multiplicando por $\mathfrak{p}_1^{-1}$, obtenemos $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{p}_1^{-1} \cdot I = \mathfrak{p}'_2 \cdots \mathfrak{p}'_s$, por lo que $\mathfrak{p}_1^{-1} \cdot I$ es un ideal entero y podemos seguir aplicando el procedimiento de manera inductiva hasta llegar al resultado deseado. □

Proposición 2.3.2. Si A es un anillo noetheriano e I es un ideal propio de A, existen ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ de A tales que $\mathfrak{p}_i \supseteq I$ para todo $i = 1, \ldots, r$, pero $I \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$.

Demostración. Si I es primo, se obtiene el resultado de manera inmediata. Sea $\mathcal{S}$ el conjunto de todos los ideales propios de A para los que no se cumple el resultado. Si $\mathcal{S} \neq \emptyset$, por ser A un anillo noetheriano, la proposición 2.1.5 nos dice que existe un ideal $I \in \mathcal{S}$ maximal en $\mathcal{S}$ con respecto a la inclusión, el cual no es primo ya que el resultado no se cumple para él. Existen por tanto elementos $a, a' \in A$ tales que $a, a' \notin I$, y $aa' \in I$. Sean $J = I + \langle a \rangle$, $J' = I + \langle a' \rangle$. Se tiene $I \subset J, J'$, por lo que $J, J' \notin \mathcal{S}$, y $J \cdot J' \subseteq I$. Como el resultado se cumple para J y J', existen ideales primos de A $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{p}'_1, \ldots, \mathfrak{p}'_s$ tales que $\mathfrak{p}_i \supseteq J \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$ y $\mathfrak{p}'_j \supseteq J' \supseteq \mathfrak{p}'_1 \cdots \mathfrak{p}'_s$ para todo $i = 1, \ldots, r$, $j = 1, \ldots, s$. Por lo tanto, $\mathfrak{p}_i, \mathfrak{p}'_j \supseteq I \supseteq J \cdot J' \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{p}'_1 \cdots \mathfrak{p}'_s$ para todo i, j recorriendo los valores anteriores, luego $I \notin \mathcal{S}$, lo que contradice la suposición inicial y concluye la prueba. □

Enunciamos ahora un teorema muy potente que abre el camino de la teoría algebraica de números.

Teorema 2.3.3 (Teorema de Dedekind). *Sea A un anillo. Son equivalentes:*

1. *A es noetheriano, integralmente cerrado y todo ideal primo no nulo de A es maximal.*

2. *Todo ideal entero no nulo de A se puede expresar de manera única como producto de ideales primos.*

3. *Todo ideal entero no nulo de A es igual al producto de ideales primos.*

4. *El conjunto de los ideales fraccionales no nulos de A forma un grupo multiplicativo.*

Demostración. $\boxed{1 \implies 2}$ Será esta implicación la que utilicemos más adelante, por tanto la que vamos a demostrar.

En las condiciones de (1), vamos a probar el siguiente

Lema 2.3.4. Todo ideal primo no nulo de A es invertible.

Sea $\mathfrak{p}$ ideal primo no nulo de A. Sabemos, por la proposición 2.2.6, $\mathfrak{p} \subseteq \mathfrak{p} \cdot \mathfrak{p}^{-1} \subseteq A$, y $A \subseteq \mathfrak{p}^{-1}$. Veamos primero que $\mathfrak{p}^{-1} \neq A$.

Sea $c \in \mathfrak{p}$ no nulo. Por la proposición 2.3.2, existen $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq A$ ideales primos tales que $\langle c \rangle \subseteq \mathfrak{p}_i$ para todo $i = 1, \ldots, r$, y $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \langle c \rangle$. Por ser $c \in \mathfrak{p}$, se tiene $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \langle c \rangle \subseteq \mathfrak{p}$. Vamos a fijar r como el mínimo que cumple la proposición 2.3.2.

Si $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}$, por ser $\mathfrak{p}$ primo, al menos algún $\mathfrak{p}_i$ debe estar contenido en $\mathfrak{p}$, digamos $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Por (1), $\mathfrak{p}$ y $\mathfrak{p}_1$ son maximales, luego $\mathfrak{p} = \mathfrak{p}_1$.

Como r es mínimo, tenemos $\mathfrak{p}_2 \cdots \mathfrak{p}_r \nsubseteq \langle c \rangle$, por lo que existe $a \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ tal que $a \notin \langle c \rangle$, luego, al no ser a múltiplo de c, $a/c \notin A$. Este elemento a/c está en $\mathfrak{p}^{-1}$, ya que $\mathfrak{p}_2 \cdots \mathfrak{p}_r \nsubseteq \mathfrak{p}$ y

$$\left(\frac{a}{c}\right) \mathfrak{p} \subseteq \left(\frac{1}{c}\right) \mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq A,$$

por lo que $A \subset \mathfrak{p}^{-1}$.

Veamos ahora que $\mathfrak{p}$ es efectivamente invertible, es decir, $\mathfrak{p} \cdot \mathfrak{p}^{-1} = A$. Tenemos

$$\mathfrak{p} = \mathfrak{p} \cdot A \subseteq \mathfrak{p} \cdot \mathfrak{p}^{-1} \subseteq A,$$

por lo que $\mathfrak{p} \cdot \mathfrak{p}^{-1}$ es un ideal entero de A que contiene a $\mathfrak{p}$. Las únicas opciones son $\mathfrak{p} \cdot \mathfrak{p}^{-1} = A$, o $\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{p}$.

Supongamos $\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{p}$. Esto implica que $\mathfrak{p} \cdot \mathfrak{p}^{-2} = (\mathfrak{p} \cdot \mathfrak{p}^{-1})\mathfrak{p}^{-1} = \mathfrak{p}$. Repitiendo el procedimiento, obtenemos $\mathfrak{p} \cdot \mathfrak{p}^{-n} = \mathfrak{p}$, para todo $n \geq 1$.

Sean $a \in \mathfrak{p}$, $b \in \mathfrak{p}^{-1}$, $a \cdot b^n \in \mathfrak{p} \cdot \mathfrak{p}^{-n} = \mathfrak{p}$, para todo $n \geq 1$. El ideal $I = \sum_{n=0}^{\infty} \langle ab^n \rangle$ está finitamente generado por ser A un anillo noetheriano, por lo que existen $c_0, \ldots, c_{n-1} \in A$ tales que $ab^n = \sum_{i=0}^{n-1} c_i ab^i$, y por tanto $b^n - \sum_{i=0}^{n-1} c_i b^i = 0$ y b es entero sobre A. Como A es un DIC por (1), $b \in A$ y concluimos que $\mathfrak{p}^{-1} \subseteq A$, lo cual es absurdo. Debe ser por tanto $\mathfrak{p} \cdot \mathfrak{p}^{-1} = A$, y queda probado que todo ideal primo de A es invertible.

Pasamos de lleno a la prueba que nos concierne. Si $I = A$, la condición (2) se cumple de manera trivial. Supongamos pues I ideal propio de A, y sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ ideales primos de A tales que, para todo $i = 1, \ldots, r$, $\mathfrak{p}_i \supseteq I \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$ (dichos ideales existen por la proposición 2.3.2). Supongamos $r \geq 1$ como el mínimo posible, y probemos por inducción en r que I puede expresarse como producto de ideales primos.

Para $r = 1$, $\mathfrak{p}_1 \supseteq I \supseteq \mathfrak{p}_1$, luego $I = \mathfrak{p}_1$ y tenemos lo deseado. Supongamos que el resultado se da para ideales que contienen un producto de a lo sumo $r - 1$ ideales primos. Sea $\mathfrak{p} \subset A$ ideal primo tal que $\mathfrak{p} \supseteq I$. De $\mathfrak{p} \supseteq I \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$, se tiene que $\mathfrak{p}$ contiene algunos ideales $\mathfrak{p}_i$: supongamos $\mathfrak{p} \supseteq \mathfrak{p}_r$. Por ser ideal primo, $\mathfrak{p}$ es maximal, luego $\mathfrak{p} = \mathfrak{p}_r$. Por el lema 2.3.4, tenemos $A = \mathfrak{p} \cdot \mathfrak{p}^{-1} \supseteq I \cdot \mathfrak{p}_r^{-1} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_{r-1}$. Por hipótesis de inducción, $I \cdot \mathfrak{p}_r^{-1} = \mathfrak{p}_1' \cdots \mathfrak{p}_s'$ tal que cada $\mathfrak{p}_j'$ es un ideal primo, y por tanto $I = I \cdot \mathfrak{p}_r^{-1} \cdot \mathfrak{p}_r = \mathfrak{p}_1' \cdots \mathfrak{p}_s' \cdot \mathfrak{p}_r$, y se tiene el resultado. La unicidad de descomposición la da la proposición 2.3.1.

$\boxed{2 \implies 3}$ Esta implicación es inmediata.

$\boxed{3 \implies 1}$ [Rib01, § 7.1]. □

En la sección anterior hemos probado que $\mathcal{O}_K$, el anillo de enteros algebraicos de un cuerpo de números K, satisface la condición (1) del teorema 2.3.3. Enunciamos por tanto el siguiente teorema.

Teorema 2.3.5. *Sea $\mathcal{O}_K$ el anillo de enteros algebraicos de un cuerpo de números de grado finito K. Entonces, todo ideal fraccional M de K es de la forma $M = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$, donde $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ son ideales primos distintos entre sí de $\mathcal{O}_K$ y $e_1, \ldots, e_r \in \mathbb{Z}^*$. Más aún, M es un ideal entero de $\mathcal{O}_K$ si, y sólo si, $e_i > 0$ para todo $i = 1, \ldots, r$.*

Demostración. Por definición de ideal fraccional, existe $a \in \mathcal{O}_K$ tal que $a \cdot M \subseteq \mathcal{O}_K$, por tanto $\langle a \rangle \cdot M$ es un ideal entero de $\mathcal{O}_K$. Por el teorema 2.3.3 (2), $\langle a \rangle$ y $\langle a \rangle \cdot M$ se pueden escribir de manera única como producto de ideales primos de $\mathcal{O}_K$, digamos

$$\begin{aligned} \langle a \rangle &= \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_s^{c_s},\ c_i \geq 0 \quad \forall i \in \{1, \ldots, s\}, \\ \langle a \rangle \cdot M &= \mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_s^{d_s},\ d_i > 0 \quad \forall i \in \{1, \ldots, s\}. \end{aligned}$$

Notemos que hemos fijado los ideales primos en ambas descomposiciones, por lo que consideramos que algún c_i puede ser 0.

Por el teorema 2.3.3 (4), $\langle a \rangle$ pertenece al grupo multiplicativo de los ideales fraccionales de $\mathcal{O}_K$, por lo que existe $\langle a \rangle^{-1}$ tal que $\langle a \rangle^{-1} \cdot \langle a \rangle = \mathcal{O}_K$, el elemento neutro del producto de ideales. Nos preguntamos qué expresión tiene $\langle a \rangle^{-1}$.

$$\begin{aligned} & \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_s^{c_s} \cdot \langle a \rangle^{-1} = \mathcal{O}_K \\ \Longrightarrow\ & \mathfrak{p}_2^{c_2} \cdots \mathfrak{p}_s^{c_s} \cdot \langle a \rangle^{-1} = \mathfrak{p}_1^{-c_1}, \end{aligned}$$

ya que $\mathfrak{p}_1$ pertenece también al grupo multiplicativo de los ideales fraccionales, y en virtud de la observación 2.2.7, el inverso de $\mathfrak{p}_1^{c_1}$ es $\mathfrak{p}_1^{-c_1}$. Procediendo con el resto de factores de $\langle a \rangle$, llegamos a

$$\langle a \rangle^{-1} = \mathfrak{p}_1^{-c_1} \cdots \mathfrak{p}_s^{-c_s},$$

y usando que $\langle a \rangle \cdot M \cdot \langle a \rangle^{-1} = M$ por la conmutatividad de la operación (véase observación 2.2.2),

$$M = \mathfrak{p}_1^{d_1 - c_1} \cdots \mathfrak{p}_s^{d_s - c_s},$$

de donde se concluye, eliminando exponentes iguales a 0 y renombrando los subíndices,

$$M = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}, \quad e_i \in \mathbb{Z}^* \quad \forall i \in \{1, \ldots, r\}.$$

Trivialmente, obtendremos que M es entero si en su descomposición no aparecen potencias negativas de ideales primos de $\mathcal{O}_K$. □

Definición 2.3.6. Se dice que un anillo A es un *dominio de Dedekind (DD)* si satisface las propiedades equivalentes del teorema de Dedekind.

La gran conclusión de esta sección, y de este capítulo, es que el anillo de enteros algebraicos de un cuerpo de números de grado finito K es un DD.

Vamos ahora a ver algo sobre la aritmética de los DD, conocimiento que nos será útil a la hora de buscar descomposiciones de ideales.

Definición 2.3.7. Un ideal entero I de un anillo A se dirá *irreducible* si $I \neq J \cdot J'$, con J, J' ideales enteros de A distintos de I.

Proposición 2.3.8. En un DD, un ideal es irreducible si, y sólo si, es primo.

Demostración. $\boxed{\Longrightarrow}$ Supongamos I irreducible. Al estar en un DD, tenemos dos opciones: I puede ser el ideal nulo (el cual es primo), o es producto de ideales primos. Como es irreducible, debe ser igual a un ideal primo.

$\boxed{\Longleftarrow}$ Procederemos por *modus tollens*. Supongamos I no irreducible, $I = J_1 \cdot J_2$. Por ser la divisibilidad de ideales una relación de orden (véase observación 2.2.8), $I \subset J_1$ e $I \subset J_2$, y por tanto existen $a_1 \in J_1$, $a_2 \in J_2$ tales que $a_1 \notin I$, $a_2 \notin I$. Tenemos $a_1 \cdot a_2 \in J_1 \cdot J_2 = I$, por lo tanto, I no puede ser primo. □

Proposición 2.3.9. Si $\mathfrak{p}$ es un ideal primo de un DD A, I, I' son ideales de A y $\mathfrak{p} \mid I \cdot I'$, entonces $\mathfrak{p} \mid I$ o $\mathfrak{p} \mid I'$.

Demostración. Como $\mathfrak{p} \mid I \cdot I'$, por definición, $I \cdot I' = \mathfrak{p} \cdot J$, con J ideal entero de A. Ambos miembros de la igualdad tienen una única descomposición en ideales primos, luego

$$\prod_{i=1}^{r} \mathfrak{p}_i = \mathfrak{p} \cdot \prod_{j=1}^{s} \mathfrak{p}'_j,$$

de lo que inmediatamente se deduce, por unicidad de descomposición, que $\mathfrak{p}$ debe estar entre los $\mathfrak{p}_i$ que descomponen a $I \cdot I'$. Debe ser, por tanto, $\mathfrak{p} \mid I$ o $\mathfrak{p} \mid I'$. □

Proposición 2.3.10. Sean M, M' ideales fraccionales no nulos de un DD A. M dividirá a M' si, y sólo si, $M \supseteq M'$.

Demostración. $\boxed{\Longrightarrow}$ Esta implicación la hemos cubierto por ser la divisibilidad de ideales una relación de orden (véase observación 2.2.8).

$\boxed{\Longleftarrow}$ Supongamos $M' \subseteq M$. Por el teorema 2.3.3, (4), M' y M pertenecen a un grupo multiplicativo y por tanto existe M^{-1} ideal fraccional con $M' \cdot M^{-1} \subseteq M \cdot M^{-1} = A$. Esto implica que $M' \cdot M^{-1}$ es un ideal entero de A tal que $(M' \cdot M^{-1})M = M'$, luego M divide a M' por definición. □

Proposición 2.3.11. Sea A un DD. Entonces, A será un DFU si, y sólo si, es un DIP.

Demostración. $\boxed{\Longleftarrow}$ Esta dirección es bien conocida, ya que todo DIP es un DFU (véase observación 1.2.10).

$\boxed{\Longrightarrow}$ Supongamos un anillo A que es DD y DFU. Por ser un DD, todo ideal propio de A se puede escribir de manera única como producto de ideales primos, luego bastará con probar que los ideales primos (maximales) de A son principales.

Sea $\mathfrak{p} \subset A$ ideal primo, y sea $a \in \mathfrak{p}$. Tenemos pues $\langle a \rangle \subseteq \mathfrak{p}$, lo que implica, por la proposición 2.3.10, $\langle a \rangle = \mathfrak{p} \cdot I$, con I ideal de A. Sea la descomposición de I en ideales primos

$$I = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}, \quad \alpha_i \in \mathbb{Z}_+ \ \forall i \in \{1, \dots, r\}$$

$$\Longrightarrow \ \langle a \rangle = \mathfrak{p} \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}.$$

Como A es un DFU, $a = x_1 \cdots x_s$, con x_j elemento irreducible de A para todo $j \in \{1, \dots, s\}$. Esto es, $\langle a \rangle = \langle x_1 \rangle \cdots \langle x_s \rangle$. Los ideales $\langle x_j \rangle$ son, de nuevo, irreducibles para todo $j \in \{1, \dots, s\}$, ya que A es un DFU. Por la proposición 2.3.8, estos ideales irreducibles son primos, y además, la igualdad

$$\langle x_1 \rangle \cdots \langle x_s \rangle = \mathfrak{p} \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}$$

implica, por unicidad de descomposición en un DD, que la descomposición en irreducibles del miembro izquierdo de la igualdad debe coincidir con la

del miembro derecho, por lo que los ideales primos de A son principales. □

Resumen

1. El anillo de enteros $\mathcal{O}_K$ de un cuerpo de números K es un dominio de Dedekind.
2. En K podemos encontrar una estructura llamada ideal fraccional que tiene una descomposición única en ideales primos de $\mathcal{O}_K$.
3. $\mathcal{O}_K$ sólo podrá ser dominio de factorización única si es dominio de ideales principales.

3 | Breve interludio algebraico

Wir müssen wissen. Wir werden wissen.
(Debemos saber. Sabremos.)

— David Hilbert

En nuestro viaje hasta ahora hemos visto y probado muchas propiedades del anillo de enteros de una extensión finita. En este capítulo vamos a ver ciertas nociones y varios resultados muy útiles a la hora de atacar el problema que nos concierne, en algunos casos.

El final del capítulo 2 sugiere una posible ruta. Obtuvimos que $\mathcal{O}_K$, el anillo de enteros del cuerpo de números K, es un dominio de factorización única si es un dominio de ideales principales. Naturalmente, trabajar en un DFU es bastante más cómodo que trabajar en lugares donde no se puede asegurar unicidad de factorización; además, en un DIP tenemos la ventaja de poder asociar números con ideales, y viceversa. Es por esto que en este capítulo vamos a centrarnos en encontrar extensiones cuadráticas tales que su anillo de enteros sea un DIP.

3.1 Grupo de clases y número de clases

En el capítulo anterior hemos visto que podemos aplicar una aritmética muy parecida a la numérica usual de $\mathbb{Z}$ a los ideales de $\mathcal{O}_K$. Cuando pasamos de

números a ideales, estamos "expandiendo" el objeto de trabajo, y ahora nos preguntamos en qué medida lo hacemos, cuánto difiere la divisibilidad en ideales respecto a la numérica y en qué casos concretos podremos trabajar con ideales de la misma forma que con números.

Puntualizamos, como hicimos en el capítulo anterior, que vamos a trabajar con anillos de enteros que serán siempre dominios de integridad.

Sea K un cuerpo de números. Vamos a denotar por $\mathcal{M}_K$ al grupo de ideales fraccionales de $\mathcal{O}_K$, y por $\mathcal{P}_K$ al subgrupo de ideales principales fraccionales del mismo.

Sean $I, J \in \mathcal{M}_K$. Definimos la siguiente relación: diremos que I es equivalente a J si existen $\alpha, \beta \in \mathcal{O}_K^*$ tales que

$$\alpha I = \beta J.$$

Proposición 3.1.1. La relación anterior es de equivalencia.

Demostración. La propiedad reflexiva es inmediata, basta con hacer $\alpha = \beta$. Para la simétrica, sólo hay que cambiar α por β. Para la transitiva,

$$\alpha I_1 = \beta I_2,\ \lambda I_2 = \mu I_3 \implies (\lambda\alpha) I_1 = (\lambda\beta) I_2 = (\beta\mu) I_3,$$

con $I_1, I_2, I_3 \in \mathcal{M}_K$, y $\alpha, \beta, \lambda, \mu \in \mathcal{O}_K^*$. □

Definición 3.1.2. El cociente del grupo $\mathcal{M}_K$ por la relación de equivalencia definida se llama *grupo de clases de ideales* o *grupo de clases*, y se denota por $Cl(K)$.

Proposición 3.1.3. $Cl(K) = \mathcal{M}_K / \mathcal{P}_K$.

Demostración. En $\mathcal{M}_K / \mathcal{P}_K$, dos ideales I y J (no nulos, ya que pertenecen a un grupo multiplicativo) pertenecerán a una misma clase de equivalencia si

$$I \cdot J^{-1} = \langle \alpha \rangle, \quad \alpha \in K^*$$
$$\implies I = \langle \alpha \rangle \cdot J.$$

Como K es el cuerpo de fracciones de $\mathcal{O}_K$, $\alpha = a/b$, para ciertos $a, b \in \mathcal{O}_K^*$, luego

$$I = \frac{\langle a \rangle}{\langle b \rangle} \cdot J \implies \langle b \rangle \cdot I = \langle a \rangle \cdot J \implies bI = aJ,$$

es decir, I y J son equivalentes (o están en la misma clase) por la relación de la definición 3.1.2. □

Definición 3.1.4. El grupo formado por las unidades de $\mathcal{O}_K$ se llama *grupo de unidades*, y se denota $\mathcal{O}_K^\times$.

Observación 3.1.5. A partir de la definición anterior y la proposición 3.1.3, es claro que el grupo de clases encaja en la sucesión exacta

$$1 \longrightarrow \mathcal{O}_K^\times \longrightarrow K^* \longrightarrow \mathcal{M}_K \longrightarrow Cl(K) \longrightarrow 1,$$

siendo la aplicación del centro la dada por $\alpha \mapsto \langle \alpha \rangle$.

Veamos ahora un resultado útil para el cálculo de descomposiciones en el caso de extensiones cuadráticas imaginarias.

Proposición 3.1.6. Sea $K = \mathbb{Q}(\sqrt{m})$, con $m \in \mathbb{Z}$, $m < 0$ y libre de cuadrados.

- Para $m \neq -1, m \neq -3$, $\mathcal{O}_K^\times = \{1, -1\}$.
- Para $m = -1$, $\mathcal{O}_K^\times = \{1, -1, i, -i\}$.
- Para $m = -3$, $\mathcal{O}_K^\times = \{1, -1, (1+\sqrt{-3})/2, (1-\sqrt{-3})/2, (-1+\sqrt{-3})/2, (-1-\sqrt{-3})/2\}$.

En cualquier caso, todas las unidades de K son raíces de la unidad.

Demostración. Para $m \equiv 2 \mod 4$ y $m \equiv 3 \mod 4$, por la proposición 1.4.2, $\mathcal{O}_K = \{a + b\sqrt{m},\ a, b \in \mathbb{Z}\}$. Dado $x = a + b\sqrt{m} \in \mathcal{O}_K$, tenemos, al ser su conjugado $\overline{x} = a - b\sqrt{m}$, $\mathrm{N}(x) = a^2 - b^2 m$. Por la proposición 1.3.7, x será unidad si $\mathrm{N}(x) = \pm 1$. Como $m < 0$, x será unidad si, y sólo si,

$$a^2 - b^2 m = 1.$$

Las opciones que tenemos son $a = \pm 1$ y $b = 0$, o $m = -1$, $b = \pm 1$ y $a = 0$.

Para $m \equiv 1 \mod 4$, por la proposición 1.4.2, $\mathcal{O}_K = \{(a + b\sqrt{m})/2,\ a, b \in \mathbb{Z},\ a, b$ con la misma paridad$\}$. Repitiendo el razonamiento, tenemos que $x = (a + b\sqrt{m})/2 \in \mathcal{O}_K$ será unidad si, y sólo si,

$$a^2 - b^2 m = 4.$$

Esta ecuación se cumple si $a = \pm 2$ y $b = 0$, o si $m = -3$, $b = \pm 1$ y $a = \pm 1$. Esto concluye la casuística y prueba el resultado. □

El grupo de clases y el grupo de unidades son objetos fundamentales en la teoría algebraica de números. La siguiente proposición ilustra en qué sentido interesa el primero para la búsqueda de extensiones cuadráticas cuyo anillo de enteros es un DIP.

Proposición 3.1.7. Sea K un cuerpo de números. Son equivalentes:

1. $Cl(K)$ está compuesto únicamente por el elemento neutro.
2. El anillo de enteros algebraicos $\mathcal{O}_K$ es un DIP.
3. Todo elemento no nulo de $\mathcal{O}_K$ factoriza en producto de elementos primos de manera única salvo orden y producto por unidades.

Demostración. $\boxed{1 \implies 2}$ Si $Cl(K)$ es únicamente el elemento neutro, quiere decir que todos los elementos de $\mathcal{M}_K$ pertenecen a una misma clase de equivalencia, *i. e.*, son todos ideales fraccionales principales.

Si en $\mathcal{M}_K$ todos los ideales son principales, al estar compuesto por los ideales fraccionales de $\mathcal{O}_K$, existe para cada $M \in \mathcal{M}_K$ un $a \in \mathcal{O}_K$ tal que $a \cdot M \subseteq \mathcal{O}_K$, luego los ideales de $\mathcal{O}_K$ también son principales.

$\boxed{2 \implies 3}$ Por la proposición 2.3.11, $\mathcal{O}_K$ es un DFU y por tanto todo elemento no nulo factoriza en producto de elementos primos de manera única salvo orden y producto por unidades.

$\boxed{3 \implies 1}$ De nuevo por la proposición 2.3.11, $\mathcal{O}_K$ es un DIP. Los ideales fraccionales de $\mathcal{M}_K$ son tales que, multiplicados por un elemento de $\mathcal{O}_K$, pasan a ser ideales enteros de $\mathcal{O}_K$, los cuales son todos principales. Es claro por tanto que los ideales de $\mathcal{M}_K$ deben ser también principales, luego al hacer cociente sobre $\mathcal{P}_K$ obtenemos una única clase de equivalencia. □

Ejemplo. Si $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$, $Cl(\mathbb{Q})$ tiene un único elemento y $\mathbb{Z}^\times = \{\pm 1\}$.

La proposición 3.1.7 da una nueva escritura de la proposición 2.3.11: $\mathcal{O}_K$ será un DFU si $Cl(K)$ tiene un único elemento. Parece pues interesante saber más sobre el grupo de clases, sobre todo respecto al número de elementos que puede tener. Esto motiva uno de los principales teoremas de la teoría

algebraica de números, presentado a continuación.

Teorema 3.1.8. *El grupo de clases de un cuerpo de números es finito.*

Demostración. [Neu99, § I.6]. □

Definición 3.1.9. El orden del grupo de clases de un cuerpo de números K se llama *número de clases de* K, denotado h_K.

El número de clases de un cuerpo de números K guarda cierta relación con L-funciones de Dirichlet, gracias a lo cual es posible computarlo (que no sencillo). Esto, sin embargo, se sale de los objetivos del trabajo y por tanto no nos pararemos en ello, remitiendo al lector al libro de Kato, Kurokawa y Saito [KKS00, § 4.3] para más detalles en el caso de extensiones cuadráticas imaginarias, y al artículo de Mollin y Williams [MW92] para el caso de extensiones cuadráticas reales.

Ahora sabemos que nos interesan, por la proposición 3.1.7, extensiones cuadráticas de $\mathbb{Q}$ con número de clases igual a 1. En los cuerpos de números que cumplen esto, obtenemos que "no hay diferencia" entre trabajar con ideales y con números: podemos hacer corresponder números con ideales principales y trabajar de manera análoga a como lo hacemos en $\mathbb{Z}$. Sin embargo, hay ciertas diferencias que debemos notar entre extensiones cuadráticas reales e imaginarias.

Vayámonos primero al caso de extensiones cuadráticas imaginarias. Un resultado bien conocido de teoría algebraica de números es la siguiente

Proposición 3.1.10. Sea $K = \mathbb{Q}(\sqrt{m})$, con $m \in \mathbb{Z}$, $m < 0$ y libre de cuadrados. Entonces,

$$h_K = 1 \iff m = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Demostración. [Sta67]. □

Como consecuencia de la *muy* finita cantidad de extensiones cuadráticas imaginarias cuyo anillo de enteros es un DIP, en el capítulo siguiente comentaremos la casuística en cada una de ellas.

¿Qué ocurre con las extensiones cuadráticas reales con número de clases

uno? A pesar de los avances llevados a cabo en esta rama, aún sigue sin demostración la siguiente

Conjetura 3.1.11. *Existen infinitas extensiones cuadráticas reales con número de clases uno.*

Esta intuición se remonta a Gauss, a quien la autora de este trabajo no se atrevería nunca a contradecir. Es por esto que, en el siguiente capítulo, sólo veremos algunos ejemplos de descomposición de ideales en el anillo de enteros de extensiones cuadráticas reales con número de clases uno.

3.2 Reciprocidad cuadrática

Una vez vista la idiosincrasia teórica de este trabajo, debemos pasar a cuestiones más técnicas. En esta sección hablaremos del *theorema aureum* enunciado por Leonhard Euler, demostrado erróneamente por Adrien-Marie Legendre y demostrado ocho veces (correctamente) por Karl F. Gauss. Con este fascinante teorema nos convertiremos en *Oompa Loompas* y procederemos a mancharnos las manos atacando la factorización de primos en los cuerpos de números que nos esperan.

En adelante denotaremos como p a un número primo impar. La problemática que pretendemos resolver es la siguiente: dado $a \in \mathbb{Z}$, determinar qué condiciones debe darse a p para que la ecuación en congruencias

$$x^2 \equiv a \mod p$$

tenga solución.

Definición 3.2.1. Se dirá que $a \in \mathbb{Z}$ es un *residuo cuadrático módulo* p si existe $x \in \mathbb{Z}/p\mathbb{Z}$ satisfaciendo la ecuación anterior.

Vamos a definir ahora un objeto tremendamente útil a la hora de tratar con residuos cuadráticos.

Definición 3.2.2. Definimos el *símbolo de Legendre de a y p* como

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ es un residuo cuadrático mód } p, \\ -1 & \text{si } a \text{ no es un residuo cuadrático mód } p, \\ 0 & \text{si } p \mid a. \end{cases}$$

La siguiente proposición nos da unas cuantas propiedades del símbolo de Legendre que nos serán de ayuda a la hora de calcularlo.

Proposición 3.2.3. Sea $a \in \mathbb{Z}$.

(a) $a^{(p-1)/2} \equiv (a/p) \mod p$.
(b) $(ab/p) = (a/p)(b/p)$.
(c) Si $a \equiv b \mod p$, $(a/p) = (b/p)$.

Demostración. [IR90, § 5.1]. □

Corolario 3.2.4. Hay tantos residuos cuadráticos no nulos módulo p como no residuos cuadráticos, exactamente $(p-1)/2$.

Demostración. [IR90, § 5.1]. □

Enunciaremos ahora el ya mencionado *theorema aureum*, bautizado así por Gauss por ser uno de los resultados más profundos y bonitos de la teoría de números, el primero de varios teoremas de reciprocidad.

Teorema 3.2.5 (Ley de reciprocidad cuadrática). *Sean p y q primos impares de $\mathbb{Z}$. Entonces*

(a) $(-1/p) = (-1)^{(p-1)/2}$.
(b) $(2/p) = (-1)^{(p^2-1)/8}$.
(c) $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$.

Demostración. [IR90, § 5.3]. □

Observación 3.2.6. La ley de reciprocidad cuadrática puede enunciarse de manera equivalente de la siguiente forma: dados p y q primos impares, las

congruencias

$$x^2 \equiv q \mod p$$
$$x^2 \equiv p \mod q$$

son ambas resolubles o ambas irresolubles excepto si p y q son congruentes con 3 módulo 4, caso en el cual una de ellas tiene solución y la otra no. Tras esta reformulación, podemos apreciar lo impresionante del resultado y cómo el símbolo de Legendre es un objeto tremendamente útil y profundo.

Ilustremos la potencia del teorema 3.2.5 con el siguiente

Ejemplo. Sean $p = 9907$, $a = 1001$. Por la proposición 3.2.3 (b),

$$\left(\frac{1001}{9907}\right) = \left(\frac{7}{9907}\right)\left(\frac{11}{9907}\right)\left(\frac{13}{9907}\right).$$

Por el teorema 3.2.5 (c),

$$\left(\frac{7}{9907}\right)\left(\frac{9907}{7}\right) = (-1)^{(6\cdot 9906)/4} = -1$$

Por la proposición 3.2.3 (c),

$$\left(\frac{9907}{7}\right) = \left(\frac{2}{7}\right),$$

y, por el teorema 3.2.5 (b),

$$\left(\frac{2}{7}\right) = (-1)^6 = 1 \implies \left(\frac{7}{9907}\right) = -1.$$

Notemos que podemos simplificar la escritura al aplicar la ley de reciprocidad cuadrática. En el caso anterior, como $(7/9907)(9907/7) = -1$, multiplicando en ambos lados por $(9907/7)$ obtenemos $(7/9907) = -(9907/7)$, ya que un símbolo de Legendre distinto de cero al cuadrado siempre es 1. Así,

$$\left(\frac{11}{9907}\right) = -\left(\frac{9907}{11}\right) = -\left(\frac{7}{11}\right)$$

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right),$$

y, como $2^2 \equiv 4 \mod 7$, $(4/7) = 1$ y por tanto $(7/11) = -1$, luego

$$\left(\frac{11}{9907}\right) = 1.$$

Por último,

$$\left(\frac{13}{9907}\right) = \left(\frac{9907}{13}\right) = \left(\frac{1}{13}\right) = 1.$$

Obtenemos así

$$\left(\frac{1001}{9907}\right) = -1,$$

y 1001 no es un residuo cuadrático módulo 9907.

3.3 Condiciones de descomposición

Ya sabemos a dónde vamos a restringirnos para estudiar el problema enunciado en la introducción de este trabajo. En esta sección vamos a dar un resultado muy interesante que nos proporcionará una condición necesaria para que, dado un primo $p \in \mathbb{Z}$, éste pueda escribirse como $x^2 + ny^2$, con $n, x, y \in \mathbb{Z}$, con n previamente fijado.

Antes de hablar de él, sin embargo, haremos unas cuantas observaciones acerca de la acción de automorfismos de Galois sobre ideales en una extensión.

Sean L una extensión de Galois de grado finito de un cuerpo de números K, $\mathcal{O}_L$ y $\mathcal{O}_K$ sus respectivos anillos de enteros. Los automorfismos de $\mathrm{Gal}(L/K)$ dejan fijos a los elementos de K y transforman en sus conjugados a los de L. En particular, $\sigma(\mathcal{O}_L) \subseteq \mathcal{O}_L$ para todo $\sigma \in \mathrm{Gal}(L/K)$, y, a su vez, $\mathcal{O}_L = \sigma(\sigma^{-1}(\mathcal{O}_L)) \subseteq \sigma(\mathcal{O}_L)$, luego $\mathcal{O}_L = \sigma(\mathcal{O}_L)$. Se deriva la siguiente

Observación 3.3.1. Sean I ideal de $\mathcal{O}_L$, $\sigma \in \mathrm{Gal}(L/K)$. Entonces, $\sigma(I) \subseteq \mathcal{O}_L$ es un ideal, y $\sigma(I) \cap \mathcal{O}_K = I \cap \mathcal{O}_K$.

Tras estas puntualizaciones, enunciamos un resultado interesante que usaremos más adelante.

Proposición 3.3.2. Sean L una extensión de Galois de grado n de un cuerpo de números K, y $\mathcal{O}_L$, $\mathcal{O}_K$ sus respectivos anillos de enteros. Si $\mathfrak{p}$, $\mathfrak{p}'$ son ideales primos de $\mathcal{O}_L$ tales que $\mathfrak{p} \cap \mathcal{O}_K = \mathfrak{p}' \cap \mathcal{O}_K \neq 0$, existe un automorfismo $\sigma \in \mathrm{Gal}(L/K)$ tal que $\sigma(\mathfrak{p}) = \mathfrak{p}'$.

Demostración. [Rib01, § 11.1]. □

Damos ahora el teorema anunciado al principio de la sección sobre descomposición de ideales primos en extensiones de Galois, el cual es, cuanto menos, impresionante.

Teorema 3.3.3. *Sean K un cuerpo de números, L una extensión de Galois de K, $\mathcal{O}_K$ y $\mathcal{O}_L$ sus respectivos anillos de enteros, $\mathfrak{p} \subset \mathcal{O}_K$ ideal primo no nulo. Supongamos que existe un elemento primitivo $t \in L$ tal que $\mathcal{O}_L = \mathcal{O}_K[t]$, y llamemos F al polinomio mínimo de t sobre K. Sea $\overline{F}$ la proyección natural de F en $\mathcal{O}_K/\mathfrak{p}$, $\overline{F} = \prod_{i=1}^{r} \overline{G_i}^{e_i}$ su descomposición en polinomios irreducibles sobre $\mathcal{O}_K/\mathfrak{p}$, $\overline{G_i} \in \mathcal{O}_K[X]$, $e_i \in \mathbb{N}$ para todo $i = 1, \ldots, r$. Entonces, $\mathcal{O}_L\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$, con $\mathfrak{q}_i \subset \mathcal{O}_L$ ideales primos no nulos distintos para todo $i = 1, \ldots, r$.*

Demostración. [Rib01, § 11.1]. □

El resultado anterior se puede enunciar de manera aún más potente relacionando la descomposición de $\overline{F}$ con la de $\mathcal{O}_L\mathfrak{p}$, pero no nos interesa llegar tan lejos. Nos es suficiente con lo que tenemos para enunciar la siguiente

Proposición 3.3.4. Sean $K = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}$ libre de cuadrados, $p \in \mathbb{Z}$ primo impar. Entonces,

- Si $(m/p) = 1$, entonces $\langle p \rangle = \mathfrak{p} \cdot \mathfrak{q}$, con $\mathfrak{p}$ y $\mathfrak{q}$ ideales primos distintos de $\mathcal{O}_K$, y se dice que *p se descompone totalmente* en K.
- Si $(m/p) = -1$, entonces $\langle p \rangle$ es un ideal primo, y decimos que p es *inerte* en K.
- Si $(m/p) = 0$, entonces $\langle p \rangle = \mathfrak{p}^2$, con $\mathfrak{p}$ ideal primo de $\mathcal{O}_K$, y se dice que p *ramifica* en K.

Demostración. Tomamos, en el teorema 3.3.3, $K = \mathbb{Q}(\sqrt{m})$ extensión de Galois de $\mathbb{Q}$, $\mathbb{Z}$ y $\mathcal{O}_K$ los anillos de enteros de $\mathbb{Q}$ y K respectivamente, $t = \sqrt{m}$ si $m \equiv 2,3 \mod 4$, $t = (1+\sqrt{m})/2$ si $m \equiv 1 \mod 4$, $\langle p \rangle$ ideal primo de $\mathbb{Z}$, F definido como

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

Vayamos primero al caso en el que $m \equiv 2,3 \mod 4$, y veamos cómo se descompone F en $\mathbb{Z}/p\mathbb{Z}$.

$$X^2 - m \mod p = \begin{cases} (X+\sqrt{m})(X-\sqrt{m}) & \text{si } \left(\frac{m}{p}\right) = 1, \\ X^2 - m & \text{si } \left(\frac{m}{p}\right) = -1, \\ X^2 & \text{si } \left(\frac{m}{p}\right) = 0. \end{cases}$$

Si $m \equiv 1 \mod 4$, las raíces de F son

$$X_1 = \frac{1+\sqrt{m}}{2}, \quad X_2 = \frac{1-\sqrt{m}}{2},$$

a partir de lo cual se obtiene

$$X^2 - X + \frac{1-m}{4} \mod p = \begin{cases} (X-X_1)(X-X_2) & \text{si } \left(\frac{m}{p}\right) = 1, \\ X^2 - X + \frac{1-m}{4} & \text{si } \left(\frac{m}{p}\right) = -1, \\ (X-\frac{1}{2})^2 & \text{si } \left(\frac{m}{p}\right) = 0. \end{cases}$$

En ambos casos, por el teorema 3.3.3, se obtiene la descomposición deseada. □

Resumen

El objetivo de este trabajo, que es dar condiciones a un número primo p para que se pueda escribir como $x^2 + ny^2$, con $n, x, y \in \mathbb{Z}$ y n fijado, va a restringirse sólo a ciertos n dentro de la lista de los que cumplen que $\mathbb{Q}(\sqrt{n})$ tiene número de clases uno.

4 | Cuerpos de números

In an ideal world, primes would start at 3.
(En un mundo ideal, los primos empezarían en el 3.)

— Number theory professor

En este capítulo final vamos a ver cómo todo lo visto hasta ahora ayuda de manera contundente a responder a la pregunta inicial restringida a algunos casos motivados por el capítulo anterior.

La proposición 3.3.4 nos indica que nos interesará, dados una extensión cuadrática K con $h_K = 1$ y un primo $p \in \mathbb{Z}$, delimitar las condiciones sobre las que p se descompone totalmente en K. Por ser $h_K = 1$, $\mathcal{O}_K$ es un DIP, y con esto vamos a sacar unas cuantas conclusiones.

Observación 4.0.1. Sean p primo tal que éste se descompone totalmente en K, extensión cuadrática de $\mathbb{Q}$, $\langle p \rangle = \mathfrak{p} \cdot \mathfrak{q}$ su descomposición en ideales primos. Trivialmente, tenemos

$$\langle p \rangle \subseteq \mathfrak{p} \cap \mathbb{Z},$$
$$\langle p \rangle \subseteq \mathfrak{q} \cap \mathbb{Z}.$$

Notemos que estamos cometiendo un abuso de notación: en las contenciones que hemos expresado, estamos considerando $\langle p \rangle$ como ideal primo de $\mathbb{Z}$, no como ideal de $\mathcal{O}_K$. Al ser $\langle p \rangle$ un ideal primo de $\mathbb{Z}$, éste es maximal, y por ser $\mathfrak{p} \cap \mathbb{Z}$ y $\mathfrak{q} \cap \mathbb{Z}$ ideales primos, debe ser

$$\mathfrak{p} \cap \mathbb{Z} = \mathfrak{q} \cap \mathbb{Z} = \langle p \rangle.$$

Observación 4.0.2. Sea $K = \mathbb{Q}(\sqrt{m})$ extensión de Galois de $\mathbb{Q}$, $m \in \mathbb{Z}$ y libre de cuadrados. Es claro que, por ser K una extensión cuadrática, $\mathrm{Gal}(K/\mathbb{Q})$ tendrá dos elementos: el automorfismo identidad, al que denotaremos id, y el automorfismo que manda un elemento de K a su conjugado, al que denotaremos σ.

Las observaciones 4.0.1 y 4.0.2 nos indican que estamos en las condiciones de aplicar la proposición 3.3.2, que nos lleva al fantástico resultado

$$\langle p \rangle = \mathfrak{p} \cdot \mathfrak{q} \implies \mathfrak{p} = \langle \alpha \rangle,\ \mathfrak{q} = \langle \overline{\alpha} \rangle,$$

con $\alpha \in \mathcal{O}_K$, $\overline{\alpha} = \sigma(\alpha) \in \mathcal{O}_K$. Ahora bien, como $\mathcal{O}_K$ es un DIP, se tiene la igualdad

$$p = u \cdot \alpha\overline{\alpha}, \quad u \in \mathcal{O}_K^{\times},$$

y, como p y $\alpha\overline{\alpha}$ son enteros racionales,

$$p = \pm\alpha\overline{\alpha}. \tag{4.1}$$

Este producto de elementos de $\mathcal{O}_K$ nos dará una forma cuadrática, lo que concluye el porqué del interés en este caso.

Cuando p ramifique en K, estudiaremos su expresión en cada extensión de forma particular.

4.1 Extensiones cuadráticas imaginarias

Vimos en el capítulo anterior que el conjunto de extensiones de este tipo con número de clases uno era bastante reducido (véase proposición 3.1.10). Es por esto que las vamos a estudiar una a una, no sin antes hacer la siguiente

Observación 4.1.1. Si $\alpha \in \mathcal{O}_K$, con $\mathcal{O}_K$ anillo de enteros de una extensión cuadrática imaginaria K con número de clases uno,

$$\alpha\overline{\alpha} \geq 0,$$

por lo que la igualdad (4.1) se traduce por

$$p = \alpha\overline{\alpha},$$

ya que suponemos $p > 0$.

4.1.1 $\mathbb{Q}(\sqrt{-1})$ y $\mathbb{Q}(\sqrt{-2})$

En estos cuerpos de números tenemos que los radicandos son congruentes con 3 y 2 módulo 4, respectivamente. La proposición 1.4.2 nos dice que $\mathcal{O}_{\mathbb{Q}(\sqrt{-1})} = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ y $\mathcal{O}_{\mathbb{Q}(\sqrt{-2})} = \mathbb{Z}[\sqrt{-2}]$.

Veamos primero la casuística de los primos que ramifican. En el caso de $K_{-1} = \mathbb{Q}(\sqrt{-1})$, no hay primos impares que ramifiquen ya que deberían dividir a 1. Estudiemos el caso del primo que nos falta por separado.

Sea $p = 2$. Por el teorema 3.3.3, 2 ramificará en K_{-2} si $F = X^2 + 1$ se descompone como un polinomio irreducible al cuadrado módulo 2; y obtenemos que, efectivamente, ese es el caso, ya que

$$X^2 + 1 = (X + 1)^2 \mod 2,$$

por lo que 2 ramifica en K_{-1}, y podemos escribir

$$2 = 1^2 + 1^2.$$

En el caso de $K_{-2} = \mathbb{Q}(\sqrt{-2})$, el polinomio mínimo de $\sqrt{-2}$ es $F = X^2 + 2$, y por ser

$$\overline{F} \equiv X^2 \mod 2,$$

obtenemos de nuevo que $p = 2$ ramifica, y además podemos escribir

$$2 = 0^2 + 2 \cdot 1^2.$$

Ahora, busquemos primos impares que descompongan totalmente en las extensiones en cuestión.

Por la proposición 3.3.4, en K_{-1}, tenemos

$$p \text{ se descompone totalmente en } K_{-1} \iff \left(\frac{-1}{p}\right) = 1.$$

¿Qué condiciones debe cumplir un primo p para que se dé la igualdad anterior? Aplicando lo visto en la sección 3.2,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2},$$

por tanto, la condición que debemos imponer es que $(p-1)/2$ sea par. Esto será así si, y sólo si, $p \equiv 1 \mod 4$.

De manera análoga, en K_{-2} necesitamos $(-2/p) = 1$.

$$\left(\frac{-2}{p}\right) = (-1)^{(p-1)/2} \cdot (-1)^{(p^2-1)/8}.$$

Aquí tenemos dos opciones: que ambos exponentes sean pares a la vez, o impares a la vez.

$$\begin{aligned}
\frac{p-1}{2} \text{ par} &\implies p \equiv 1 \mod 4, \\
\frac{p^2-1}{8} \text{ par} &\implies p \equiv 1,7 \mod 8, \\
\frac{p-1}{2} \text{ impar} &\implies p \equiv 3 \mod 4, \\
\frac{p^2-1}{8} \text{ impar} &\implies p \equiv 3 \mod 8.
\end{aligned}$$

Aplicando teoría de congruencias básica, obtenemos $p \equiv 1,3 \mod 8$.

Queda ahora la pregunta más importante: ¿lo que hemos hecho resuelve nuestro problema? En los casos de K_{-1} y K_{-2}, la respuesta es sí. Al ser $\mathcal{O}_{K_{-1}} = \mathbb{Z}[i]$ y $\mathcal{O}_{K_{-2}} = \mathbb{Z}[\sqrt{-2}]$, y con p cumpliendo las condiciones que hemos concluido en cada caso, la descomposición en ideales será tal que

$$\begin{aligned}
p = \alpha_1 \cdot \overline{\alpha_1} = a_1^2 + b_1^2, \quad \alpha_1 = a_1 + b_1 i \in \mathcal{O}_{K_{-1}}, \\
p = \alpha_2 \cdot \overline{\alpha_2} = a_2^2 + b_2^2, \quad \alpha_2 = a_2 + b_2\sqrt{-2} \in \mathcal{O}_{K_{-2}}.
\end{aligned}$$

En resumen,

$$\begin{aligned}
p = x^2 + y^2, \quad x, y \in \mathbb{Z} &\iff p = 2 \text{ o } p \equiv 1 \mod 4, \\
p = x^2 + 2y^2, \quad x, y \in \mathbb{Z} &\iff p = 2 \text{ o } p \equiv 1,3 \mod 8.
\end{aligned}$$

4.1.2 $\mathbb{Q}(\sqrt{-3})$ y $\mathbb{Q}(\sqrt{-7})$

En K_{-1} y K_{-2} teníamos la suerte de que las expresiones de los enteros algebraicos, junto a las condiciones derivadas de la proposición 3.3.4, concluían bajo qué suposiciones un primo podía escribirse como $x^2 + y^2$ y

$x^2 + 2y^2$, respectivamente, con $x, y \in \mathbb{Z}$. En los casos de $K_{-3} = \mathbb{Q}(\sqrt{-3})$ y $K_{-7} = \mathbb{Q}(\sqrt{-7})$, la proposición 1.4.2 nos dice

$$\mathcal{O}_{K_{-3}} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right], \quad \mathcal{O}_{K_{-7}} = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right],$$

así que en principio no lo tendremos tan fácil.

Vamos a empezar estudiando la descomposición de nuestro primo menos favorito, $p = 2$, en ambas extensiones. En K_{-3},

$$F = X^2 - X + 1 \equiv X^2 + X + 1 \mod 2,$$

y, al ser $\overline{F} = X^2 + X + 1$ irreducible sobre $\mathbb{Z}/2\mathbb{Z}[X]$, obtenemos que $\langle 2 \rangle$ es primo en $\mathcal{O}_{K_{-3}}$. En K_{-7},

$$F = X^2 - X + 2 \equiv X^2 + X \mod 2,$$

y $\overline{F} = X(X+1)$ se descompone en dos polinomios irreducibles, *i. e.*, 2 se descompone totalmente en K_{-7} y existen $\alpha, \overline{\alpha} \in \mathcal{O}_{K_{-7}}$ tales que

$$2 = \alpha\overline{\alpha}.$$

Veremos más adelante quiénes son estos enteros de $\mathcal{O}_{K_{-7}}$, cuando estudiemos la forma cuadrática que cumplen los primos que se descomponen totalmente en esta extensión.

Pasemos a los primos impares. En K_{-3} ramifica $p = 3$, en K_{-7} ramifica $p = 7$, y en ambos casos es trivial su escritura como suma de un cuadrado por 3 (respectivamente 7) veces otro cuadrado. Veamos pues los primos (impares) que se descomponen totalmente.

En K_{-3},

$$\left(\frac{-3}{p}\right) = (-1)^{(p-1)/2} \cdot (-1)^{(p-1)/2}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

En $\mathbb{Z}/3\mathbb{Z}$, el único residuo cuadrático (no nulo) es 1, luego $(p/3) = 1$ implica que la condición que hay que imponerle a p es ser congruente con 1 módulo 3. Como es evidente, excluimos el caso $p \equiv 0 \mod 3$ ya que el único primo que cumple esto es $p = 3$, ya estudiado.

En K_{-7},

$$\left(\frac{-7}{p}\right) = (-1)^{(p-1)/2}\left(\frac{7}{p}\right),$$

$$\left(\frac{7}{p}\right)\left(\frac{p}{7}\right) = (-1)^{(p-1)3/2} \implies \left(\frac{7}{p}\right) = (-1)^{(p-1)3/2}\left(\frac{p}{7}\right)$$

$$\implies \left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right).$$

En $\mathbb{Z}/7\mathbb{Z}$ los residuos cuadráticos no nulos son 1, 2 y 4, luego $(-7/p) = 1$ se dará si, y sólo si, $p \equiv 1, 2, 4 \mod 7$.

Una vez obtenidas las condiciones necesarias en cada caso, estudiemos qué más debemos pedir para poder escribir $p = x^2 + 3y^2$ y $p = x^2 + 7y^2$, respectivamente, con $x, y \in \mathbb{Z}$.

Empecemos estudiando el caso en K_{-3}. Sean p primo tal que $p \equiv 1 \mod 3$, $\alpha = a + b(1 + \sqrt{-3})/2 \in \mathcal{O}_{K_{-3}}$ el generador de uno de los ideales en los que se descompone $\langle p \rangle$. Entonces,

$$p = \left(a + b\left(\frac{1+\sqrt{-3}}{2}\right)\right)\left(a + b\left(\frac{1-\sqrt{-3}}{2}\right)\right) = a^2 + ab + b^2. \quad (4.2)$$

La expresión como forma cuadrática de p dada por (4.2) nos asegura que a y b no pueden ser pares a la vez, ya que en ese caso p no sería primo, pero esta pista es insuficiente. Nos será de ayuda la siguiente

Observación 4.1.2. Sean A un anillo, I un ideal de A, $u \in A$ una unidad. Se tiene

$$uI = I.$$

Esta observación nos permite afirmar que, en el cuerpo de números K_{-3},

$$\langle p \rangle = \langle u_1\alpha \rangle \cdot \langle u_2\overline{\alpha} \rangle,$$

con $\alpha = a + b(1 + \sqrt{-3})/2$, $\overline{\alpha} = a + b(1 - \sqrt{-3})/2 \in \mathcal{O}_{K_{-3}}$, $u_1, u_2 \in \mathcal{O}_{K_{-3}}^{\times}$, lo que traducimos por

$$p = (u_1\alpha)(u_2\overline{\alpha}), \quad \text{con } u_1u_2 = 1.$$

Esto nos da la idea de "jugar" con las unidades de $\mathcal{O}_{K_{-3}}^{\times}$ dadas en la proposición 3.1.6 para ver si podemos asegurar la existencia de $x, y \in \mathbb{Z}$ tales que $p = x^2 + 3y^2$.

Sean pues $\alpha = a + b(1+\sqrt{-3})/2$, $\overline{\alpha} = a + b(1-\sqrt{-3})/2$. Si b fuera par, habríamos acabado, ya que tendríamos

$$\alpha = \left(a + \frac{b}{2}\right) + \frac{b}{2}\sqrt{-3}, \quad a, \frac{b}{2} \in \mathbb{Z},$$

$$\overline{\alpha} = \left(a + \frac{b}{2}\right) - \frac{b}{2}\sqrt{-3}, \quad a, \frac{b}{2} \in \mathbb{Z},$$

y estaríamos en la misma situación que en el caso de K_{-1} y K_{-2}. Si, en lugar de b, fuera a par, al multiplicar por las unidades $u_1 = (1-\sqrt{-3})/2$, $u_2 = (1+\sqrt{-3})/2$,

$$u_1\alpha = a\left(\frac{1-\sqrt{-3}}{2}\right) + b,$$

$$u_2\overline{\alpha} = a\left(\frac{1+\sqrt{-3}}{2}\right) + b,$$

podríamos intercambiar a por b sin ningún problema, y nos remitiríamos al caso anterior.

Supongamos pues a y b impares. Sean $u_1 = (1+\sqrt{-3})/2$, $u_2 = (1-\sqrt{-3})/2$.

$$u_1\alpha = a\left(\frac{1+\sqrt{-3}}{2}\right) + b\left(\frac{-1+\sqrt{-3}}{2}\right) = \frac{a-b}{2} + \frac{a+b}{2}\sqrt{-3},$$

$$u_2\overline{\alpha} = a\left(\frac{1-\sqrt{-3}}{2}\right) + b\left(\frac{-1-\sqrt{-3}}{2}\right) = \frac{a-b}{2} - \frac{a+b}{2}\sqrt{-3}.$$

Al ser a y b impares, tanto $a+b$ como $a-b$ son pares y hemos encontrado unos enteros racionales $x = (a-b)/2$, $y = (a+b)/2$ tales que

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

Esto quiere decir que no hay que imponer más restricciones a p además de ser congruente con 1 módulo 3 para poderse escribir de la manera deseada.

Procedamos de manera análoga para el caso en K_{-7}. Sean p primo tal que $p \equiv 1, 2, 4 \mod 7$ (atención: $p = 2$ está al acecho), $\alpha = a + b(1+\sqrt{-7})/2 \in \mathcal{O}_{K_{-7}}$ el generador de uno de los ideales en los que se descompone $\langle p \rangle$. Tenemos

$$p = \left(a + b\left(\frac{1+\sqrt{-7}}{2}\right)\right)\left(a + b\left(\frac{1-\sqrt{-7}}{2}\right)\right) = a^2 + ab + 2b^2. \quad (4.3)$$

Si $p = 2$, trivialmente, obtenemos

$$2 = 0^2 + 0 \cdot 1 + 2 \cdot 1^2,$$

luego $\alpha = (1+\sqrt{-7})/2$ y $\overline{\alpha} = (1-\sqrt{-7})/2$ son los enteros de $\mathcal{O}_{K_{-7}}$ tales que su producto es igual a 2. Es imposible, sin embargo, encontrar $x, y \in \mathbb{Z}$ tales que

$$2 = x^2 + 7y^2,$$

luego $p = 2$ nos la ha vuelto a jugar.

Consideremos ahora p primo impar, y estudiemos la paridad de a y b según la expresión dada por (4.3). Evidentemente, a y b no pueden ser pares a la vez. Tampoco podrían ser impares a la vez, ya que la suma sería par, luego la única opción es que uno sea par y el otro impar. La conclusión es que b debe ser par, ya que de la otra forma (a par), la suma seguiría siendo par. Por tanto,

$$p = (x + y\sqrt{-7})(x - y\sqrt{-7}) = x^2 + 7y^2,$$

con $x = a + b/2$, $y = b/2$ enteros racionales, y en este caso no tenemos que imponer condiciones extra.

En resumen,

$$p = x^2 + 3y^2, \quad x, y \in \mathbb{Z} \iff p = 3 \text{ o } p \equiv 1 \mod 3,$$
$$p = x^2 + 7y^2, \quad x, y \in \mathbb{Z} \iff p = 7 \text{ o } p \equiv 1, 2, 4 \mod 7,\ p \neq 2.$$

4.1.3 $\mathbb{Q}(\sqrt{-n})$, $n \in \{11, 19, 43, 67, 163\}$

Veamos los cinco casos restantes derivados de la proposición 3.1.10. Denotemos, como anteriormente, $K_{-n} = \mathbb{Q}(\sqrt{-n})$, con $n \in \{11, 19, 43, 67, 163\}$.

Tenemos que todos los radicandos son congruentes con 1 módulo 4, por lo que

$$\mathcal{O}_{K_{-n}} = \mathbb{Z}\left[\frac{1+\sqrt{-n}}{2}\right], \quad n = 11, 19, 43, 67, 163.$$

De nuevo, como en los casos de K_{-3} y K_{-7}, volvemos a no tenerlo fácil.

Si $p = 2$,

$$F = \begin{cases} X^2 - X + 3 \equiv X^2 + X + 1 \mod 2 & \text{en } K_{-11}, \\ X^2 - X + 5 \equiv X^2 + X + 1 \mod 2 & \text{en } K_{-19}, \\ X^2 - X + 11 \equiv X^2 + X + 1 \mod 2 & \text{en } K_{-43}, \\ X^2 - X + 17 \equiv X^2 + X + 1 \mod 2 & \text{en } K_{-67}, \\ X^2 - X + 41 \equiv X^2 + X + 1 \mod 2 & \text{en } K_{-163}, \end{cases}$$

luego, por el teorema 3.3.3, $\langle 2 \rangle$ es primo en cada $\mathcal{O}_{K_{-n}}$.

En cada K_{-n} ramifica el primo $p = n$ y, de manera análoga a los casos anteriores,

$$p = 0^2 + n \cdot 1^2.$$

Pasamos por tanto al caso de los primos impares que se descomponen totalmente en cada K_{-n} estudiando el signo de $(-n/p)$.

Observación 4.1.3. Para $n \in \{11, 19, 43, 67, 163\}$,

$$\left(\frac{-n}{p}\right) = (-1)^{(p-1)/2} \cdot (-1)^{(p-1)k_n/2} \left(\frac{p}{n}\right),$$

donde $k_n \equiv 1 \mod 4$ para cada n. Por tanto,

$$\left(\frac{-n}{p}\right) = \left(\frac{p}{n}\right).$$

La observación anterior nos facilita enormemente el cálculo de $(-n/p)$ en cada caso, ya que sólo tenemos que buscar los residuos cuadráticos módulo un primo conocido. Para ello, podemos ayudarnos de la herramienta computacional SageMath y el comando `quadratic_residues(n)`. Así,

- $\left(\frac{-11}{p}\right) = 1 \iff p \equiv 1,3,4,5,9 \mod 11$.

- $\left(\frac{-19}{p}\right) = 1 \iff p \equiv 1,4,5,6,7,9,11,16,17 \mod 19$.

Se puede apreciar que la lista de congruencias aumentará considerablemente para los casos restantes; de hecho, por el corolario 3.2.4, para $n = 43$ tendremos una lista de veintiún números con los que puede ser congruente p, para $n = 67$ la lista será de treinta y tres, y para $n = 163$, de ochenta y uno. Escribir estas listas de congruencias carece de interés matemático, por lo que hablaremos de los casos $n = 11$ y $n = 19$ ya expuestos y trasladaremos las conclusiones al resto.

Intentemos, pues, hacer en K_{-11} algo parecido a lo que hicimos en los casos de K_{-3} y K_{-7}. Sea p primo tal que $p \equiv 1,3,4,5,9 \mod 11$, $\alpha = a + b(1+\sqrt{-11})/2 \in \mathcal{O}_{K_{-11}}$ el generador de uno de los ideales primos en los que se descompone $\langle p \rangle$. Entonces,

$$p = \left(a + b\left(\frac{1+\sqrt{-11}}{2}\right)\right)\left(a + b\left(\frac{1-\sqrt{-11}}{2}\right)\right) = a^2 + ab + 3b^2. \tag{4.4}$$

La expresión como forma cuadrática de p dada por (4.4), como pasaba con la de (4.2), sólo nos asegura que a y b no pueden ser pares a la vez. En este caso, sin embargo, no tenemos una forma sencilla de buscar enteros que satisfagan $p = x^2 + 11y^2$ de la misma forma en la que lo hicimos en K_{-3}, ya que las unidades de $\mathcal{O}_{K_{-11}}$ son únicamente 1 y -1 (véase proposición 3.1.6).

Lo mismo ocurre en K_{-19}, donde $\mathcal{O}_{K_{-19}}^{\times} = \{\pm 1\}$ y, si p se descompone totalmente, satisface la forma cuadrática

$$p = \left(a + b\left(\frac{1+\sqrt{-19}}{2}\right)\right)\left(a + b\left(\frac{1-\sqrt{-19}}{2}\right)\right) = a^2 + ab + 5b^2, \tag{4.5}$$

por lo que de nuevo sólo sabemos que a y b no son pares a la vez.

Para el resto de casos,

$$\begin{aligned} p &= a^2 + ab + 11b^2 \quad \text{si } p \text{ se descompone totalmente en } K_{-43}, \\ p &= a^2 + ab + 17b^2 \quad \text{si } p \text{ se descompone totalmente en } K_{-67}, \\ p &= a^2 + ab + 41b^2 \quad \text{si } p \text{ se descompone totalmente en } K_{-163}, \end{aligned}$$

tenemos las mismas dificultades que en los dos casos previos. Lamentablemente, no tenemos las herramientas teóricas necesarias para seguir avanzando; para ver más lejos hay que subirse a hombros de gigantes como David Hilbert.

Teorema 4.1.4. *Sean $n > 0$ un entero racional, $h(-n)$ el número de clases del cuerpo de números $K = \mathbb{Q}(\sqrt{-n})$. Entonces, existe un polinomio mónico irreducible $f_n(x) \in \mathbb{Z}[x]$ de grado $h(-4n)$ tal que, si un primo impar p no divide a n ni al discriminante de $f_n(x)$, entonces*

$$p = x^2 + ny^2 \iff \begin{cases} (-n/p) = 1 \text{ y } f_n(x) \equiv 0 \mod p \\ \textit{posee una solución entera.} \end{cases}$$

Demostración. [Cox13, § 2.9]. □

Este teorema se engloba en la teoría de los cuerpos de clases de Hilbert, caso concreto a su vez de la teoría de cuerpos de clases, donde se tiene como objetivo clasificar las extensiones abelianas de un cuerpo. La expresión del polinomio $f_n(x)$ mencionado en el teorema se obtiene del polinomio mínimo de una extensión particular del cuerpo de números $K = \mathbb{Q}(\sqrt{-n})$.

La potencia de este teorema es tal, que las condiciones expuestas son suficientes para *cualquier* $n > 0$, por lo que, como es natural, no es tarea fácil encontrar el polinomio $f_n(x)$ y por tanto dar unas condiciones necesarias y suficientes para que un primo impar p se pueda escribir como $x^2 + ny^2$, con $x, y \in \mathbb{Z}$, $n \in \mathbb{N}$.

Nosotros, por tanto, nos quedamos con los resultados

$$
\begin{aligned}
&p = x^2 + xy + 3y^2, \quad x, y \in \mathbb{Z} \iff p \equiv 1, 3, 4, 5, 9 \mod 11, \\
&p = x^2 + xy + 5y^2, \quad x, y \in \mathbb{Z} \iff p \equiv 1, 4, 5, 6, 7, 9, 11, 16, 17 \mod 19, \\
&p = x^2 + xy + 11y^2 \quad x, y \in \mathbb{Z} \iff \left(\frac{p}{43}\right) = 1, \\
&p = x^2 + xy + 17y^2 \quad x, y \in \mathbb{Z} \iff \left(\frac{p}{67}\right) = 1, \\
&p = x^2 + xy + 41y^2 \quad x, y \in \mathbb{Z} \iff \left(\frac{p}{163}\right) = 1.
\end{aligned}
$$

4.2 Extensiones cuadráticas reales

Sea $K = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}$, $m > 0$ y libre de cuadrados.

Las extensiones cuadráticas tienen una particularidad que las distingue notablemente de las imaginarias. Sea

$$x^2 - ny^2 = 1 \tag{4.6}$$

la ecuación de Pell, con $n \in \mathbb{N}$ y distinto de un cuadrado perfecto. En estas condiciones, Joseph Louis Lagrange demostró que dicha ecuación tiene infinitas soluciones para $x, y \in \mathbb{Z}$ (véase [Wei07, § II.XIV]). De este resultado se puede inferir que el anillo de enteros de $\mathbb{Q}(\sqrt{n})$ tiene infinitas unidades. Esto hace que, si encontramos una solución a la ecuación $p = \pm(x^2 - ny^2)$, se puedan construir infinitas expresiones para dicha igualdad.

La conjetura 3.1.11 nos obliga, para tristeza de todos, a dar sólo algunos ejemplos de descomposición de primos de $\mathbb{Z}$ en extensiones cuadráticas reales. Para $m = 2, 3$, se tiene $h_K = 1$, así que veamos cómo se procede en $\mathbb{Q}(\sqrt{2})$ y en $\mathbb{Q}(\sqrt{3})$.

4.2.1 $\mathbb{Q}(\sqrt{2})$

Sea $K_2 = \mathbb{Q}(\sqrt{2})$. Por la proposición 1.4.2, $\mathcal{O}_{K_2} = \mathbb{Z}[\sqrt{2}]$.

Como en el caso imaginario, empecemos por $p = 2$, el primo especial. Sea $F = X^2 - 2$ el polinomio mínimo de $\sqrt{2}$ en K_2.

$$F \equiv X^2 \quad \text{mód } 2,$$

luego 2 ramifica en K_2 por el teorema 3.3.3, y podemos escribir

$$2 = 2^2 - 2 \cdot 1^2, \quad \text{y} \;\; 2 = 2 \cdot 3^2 - 4^2$$

Veamos ahora qué condiciones debe cumplir un primo impar p para descomponerse totalmente en K_2, es decir, qué debe cumplir p para que se dé $(2/p) = 1$.

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Aprovechamos el calculote hecho en el caso de $\mathbb{Q}(\sqrt{-2})$ para concluir

$$\left(\frac{2}{p}\right) = 1 \iff p \equiv 1, 7 \quad \text{mód } 8.$$

Concluimos por tanto

$$p = \begin{cases} x^2 - 2y^2 \\ \quad \text{o} \\ 2y^2 - x^2 \end{cases} \qquad x, y \in \mathbb{Z} \iff p = 2 \text{ o } p \equiv 1, 7 \quad \text{mód } 8.$$

Veamos la construcción de las infinitas expresiones de p como $\pm(x^2 - 2y^2)$ a partir de soluciones de la ecuación de Pell (4.6), con $n = 2$. Sea $a^2 - 2b^2$ una expresión de p, con $a, b \in \mathbb{Z}$. Entonces, si (x, y) es una solución entera racional de (4.6) con $n = 2$,

$$p = (a^2 - 2b^2)(x^2 - 2y^2) = (ax + 2by)^2 - 2(ay + bx)^2, \tag{4.7}$$

y mediante esa construcción se obtienen infinitas expresiones de p, una por solución de (4.6) con $n = 2$.

Comprobemos que, efectivamente, la fórmula del miembro derecho de la igualdad en (4.7) genera expresiones de p. Hemos visto

$$2 = 2^2 - 2 \cdot 1^2,$$

luego sean $a = 2$, $b = 1$. Una solución para $n = 2$ de (4.6) es $x = 3$, $y = 2$. Sustituimos en (4.7) y obtenemos

$$(6 + 4)^2 - 2(4 + 3)^2 = 10^2 - 2 \cdot 7^2 = 2,$$

y hemos generado otra expresión de $p = 2$ como un entero racional al cuadrado menos dos veces el cuadrado de otro entero racional.

Sea ahora $2b^2 - a^2$ una expresión de p, con $a, b \in \mathbb{Z}$. Aplicando el mismo razonamiento,

$$p = (2b^2 - a^2)(x^2 - 2y^2) = 2(bx + ay)^2 - (2by + ax)^2, \tag{4.8}$$

y el miembro derecho de (4.8) genera infinitas expresiones de p a partir de soluciones de (4.6) con $n = 2$ una vez que encontramos una.

4.2.2 $\mathbb{Q}(\sqrt{3})$

Sean $K_3 = \mathbb{Q}(\sqrt{3})$, $\mathcal{O}_{K_3} = \mathbb{Z}[\sqrt{3}]$ por la proposición 1.4.2.

Veamos qué se trama $p = 2$ en esta extensión. Sea $F = X^2 - 3$ el polinomio mínimo de $\sqrt{3}$ en K_3. Tenemos

$$F \equiv X^2 + 1 \equiv (X + 1)^2 \mod 2,$$

por lo que 2 ramifica en K_3 por el teorema 3.3.3, y podemos escribir

$$2 = 3 \cdot 3^2 - 5^2.$$

Pasemos a los primos impares. En K_3, $p = 3$ ramifica, y podemos expresarlo como

$$3 = 3 \cdot 1^2 - 0^2.$$

Veamos para finalizar qué primos se descomponen totalmente.

$$\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right).$$

Combinamos la paridad del exponente $(p-1)/2$ con el signo de $(p/3)$, y obtenemos

$$\begin{aligned} \frac{p-1}{2} \text{ par} &\implies p \equiv 1 \mod 4, \\ \left(\frac{p}{3}\right) = 1 &\implies p \equiv 1 \mod 3, \\ \frac{p-1}{2} \text{ impar} &\implies p \equiv 3 \mod 4, \\ \left(\frac{p}{3}\right) = -1 &\implies p \equiv 2 \mod 3. \end{aligned}$$

Aplicando el teorema chino del resto, obtenemos que la condición para que p se descomponga totalmente en K_3 es $p \equiv 1, 11 \mod 12$.

Así, concluimos

$$p = \begin{cases} x^2 - 3y^2 \\ \text{o} \\ 3y^2 - x^2 \end{cases} \qquad x, y \in \mathbb{Z} \iff p = 2,\ p = 3 \text{ o } p \equiv 1, 11 \mod 12.$$

Vamos a dar una expresión explícita, como hicimos en K_2, de las infinitas expresiones de un primo si se puede escribir como $x^2 - 3y^2$ o como $3y^2 - x^2$ a partir de soluciones de la ecuación de Pell (4.6) para $n = 3$.

Si $p = a^2 - 3b^2$ es una expresión de p, con $a, b \in \mathbb{Z}$, y (x, y) es una solución entera racional de (4.6) para $n = 3$,

$$p = (a^2 - 3b^2)(x^2 - 3y^2) = (ax + 3by)^2 - 3(ay + bx)^2.$$

Si $p = b^2 - 3a^2$, en las mismas condiciones,

$$p = (b^2 - 3a^2)(x^2 - 3y^2) = 3(bx + ay)^2 - (3by + ax)^2.$$

Conclusiones

El problema que hemos abordado en este trabajo, por simple que pudiere parecer, nos ha hecho sumergirnos en sitios muy concretos de la teoría algebraica de números. Hemos visto cómo, por intentar resolver lo que aquí hemos tocado sin el cuidado que merece, se han creado nuevas herramientas y hecho descubrimientos tan fascinantes como el teorema de Dedekind, la ley de reciprocidad cuadrática o el teorema de descomposición de ideales primos en extensiones de Galois. A partir de una idea escrita en los márgenes de un libro, una intuición que pudiera parecer anecdótica, se ha abierto paso una rama de estudio que de tan majestuosa puede incluso antojarse terrorífica.

Mi viaje por la teoría algebraica de números ha estado lleno de asombro y frustraciones, siendo sin duda una profunda fascinación por el misterio de los números primos lo que ha acabado primando. Así, la verdadera conclusión es que siempre hay un paso más allá que dar, porque, caminante, no hay camino, se hace camino al andar.

Bibliografía

[AM69] MICHAEL F. ATIYAH y IAN G. MACDONALD. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[Bos11] JOHAN BOSMAN. *Algebraic Number Theory*. Free Software Foundation, 2011.

[Cox13] DAVID A. COX. *Primes of the Form $x^2 + ny^2$*. Second. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, 2013 (vid. págs. 4, 57).

[DF04] DAVID S. DUMMIT y RICHARD M. FOOTE. *Abstract Algebra*. Third. John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[Ful89] WILLIAM FULTON. *Algebraic Curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989 (vid. pág. 10).

[IR90] KENNETH IRELAND y MICHAEL ROSEN. *A Classical Introduction to Modern Number Theory*. Second. Vol. 84. Graduate Texts in Mathematics. Springer-Verlag, New York, 1990 (vid. pág. 41).

[KKS00] KAZUYA KATO, NOBUSHIGE KUROKAWA y TAKESHI SAITO. *Number Theory 1: Fermat's Dream*. Vol. 186. Translations of Mathematical Monographs. American Mathematical Society, Providence, RI, 2000 (vid. pág. 39).

[KKS11] KAZUYA KATO, NOBUSHIGE KUROKAWA y TAKESHI SAITO. *Number Theory 2: Introduction to Class Field Theory*. Vol. 240. Translations of Mathematical Monographs. American Mathematical Society, Providence, RI, 2011.

[MW92] RICHARD A. MOLLIN y HUGH C. WILLIAMS. «Computation of the class number of a real quadratic field». En: *Utilitas Math.* 41 (1992) (vid. pág. 39).

[Neu99] JÜRGEN NEUKIRCH. *Algebraic Number Theory*. Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 1999 (vid. pág. 39).

[Rib01] PAULO RIBENBOIM. *Classical Theory of Algebraic Numbers*. Universitext. Springer-Verlag, New York, 2001 (vid. págs. 11, 16, 21, 22, 29, 44).

[Sta67] HAROLD M. STARK. «A complete determination of the complex quadratic fields of class-number one». En: *Michigan Math. J.* 14 (1967) (vid. pág. 39).

[Ste12] PETER STEVENHAGEN. *Number Rings*. 2012.

[Wei07] ANDRÉ WEIL. *Number Theory*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007 (vid. pág. 58).

[Zag90] DON B. ZAGIER. «A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares». En: *Amer. Math. Monthly* 97.2 (1990) (vid. pág. 5).