Representación de primos mediante formas cuadráticas

Álvaro Domínguez Gutiérrez

Representación de primos mediante formas cuadráticas

Álvaro Domínguez Gutiérrez

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

Tutorizado por

Antonio Rojas León

Índice general

Resumen

Este trabajo busca dar una primera idea de la teoría algebraica de números y de su método. Partimos de una premisa sencilla: estudiar qué primos se pueden escribir en la forma $p = x^2 + ny^2$ para un n dado. La teoría algebraica de números busca expandir el mundo de los números para responder este tipo de preguntas.

Comenzaremos con una sección dedicada a explicar los rudimentos de esta teoría. Generalizaremos la noción de número entero en lo que llamaremos *entero algebraico* y les daremos estructura de anillo y veremos las ricas propiedades que tienen sus ideales. Más adelante, como parece natural en cualquier curso de álgebra, pasaremos a estudiar sus extensiones. Veremos cómo se comportan los enteros, y sus ideales, dentro del anillo de enteros de un cuerpo de números. También dedicaremos un momento a darles estructura de grupo a los ideales de los anillos de enteros, y veremos que, igual que los números, también se pueden factorizar.

Después aplicaremos esta teoría al caso particular de las extensiones cuadráticas, aquellas de la forma $K = \mathbb{Q}[\sqrt{d}]$, con d libre de cuadrados. Veremos entonces un buen ejemplo de cómo actúa la teoría algebraica de números: para estudiar la ecuación $p = x^2 + ny^2$, estudiaremos cómo se comportan los ideales primos de $\mathbb{Z}$ en el anillo de enteros de K. Resulta que si p factoriza como producto de dos primos en K, se podrá escribir de esa manera.

Abstract

In this essay, we are aiming to give a first impression of algebraic number theory and its method. We start from a relatively simle question: given a positive integer n, which primes p can be expressed in the form $p = x^2 + ny^2$?

First, we will develop the building blocks of algebraic number theory. We will define algebraic integers and study their properties, we will see that they have ring structure, and study their ideals. Then, we will study extensions of the so called *number fields*, and how do the ideals of the ring of integers $\mathbb{Z}$ behave in a bigger ring. Later, we will prove that the ideals of an algebraic number ring have a multiplicative structure, and that they can be factores.

Finally, we will apply all of this theory to the special case of quadratic field extensions: those of the form $K = \mathbb{Q}[\sqrt{d}]$, with d a squarefree integer. It turns out that studying the equation $p = x^2 + ny^2$ can be reduced to studying how prime ideals of $\mathbb{Z}$ decompose into prime ideals in K.

0 | Introducción

Muchos cursos de álgebra prueban un conocido resultado de Fermat que dice que, para un primo impar p,

$$p = x^2 + y^2 \iff p \equiv 1 \mod 4.$$

Pero Fermat también estudió qué primos se pueden escribir en la forma $p = x^2 + 2y^2$, o en la forma $p = x^2 + 3y^2$. Es natural entonces plantearse la siguiente pregunta:

Pregunta. *Dado un entero positivo n, ¿qué primos p se pueden expresar en la forma*

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

con x e y números enteros?

La figura de Fermat es muy interesante porque en sus estudios comienzan muchas de las preguntas que más han hecho avanzar la teoría de números, y la matemática en general.

Figura 1: Pierre de Fermat (1601-1665).

Es conocido que uno de los problemas más importante de la historia de las matemáticas es el famoso último teorema de Fermat.

Teorema 0.1 (Último teorema de Fermat). *La ecuación*

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

no tiene soluciones con $x, y, z \in \mathbb{Z}$, $xyz \neq 0$, *cuando* $n \leq 3$.

Los intentos por demostrarlo dieron grandes avances a la matemática, y en especial a la teoría algebraica de números. Un famoso, pero fallido, intento de demostración fue dado en 1847, por el matemático Gabriel Lamé ante la Academia de París. El esquema de su prueba es el siguiente:

Primero, hacemos una simplifiación del problema. No es difícil ver que basta probarlo para $n = 4$ y para $n = p \geq 3$ primo. La prueba para $n = 4$ fue dada por el propio Fermat, usando su método del descenso. La idea de Lamé era factorizar $x^p + y^p$. Llegó a la siguiente expresión:

$$x^p + y^p = \prod_{i=0}^{p-1} \left(x + \zeta_p^i y \right), \tag{1}$$

donde ζ_p es una raíz $p-$ésima primitiva de la unidad.

La ecuación (1) es una factorización de $x^p + y^p$ sobre el siguiente anillo:

$$\mathbb{Z}[\zeta_p] = \{a_0 + a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1}\}.$$

Aquí aparece un ejemplo de anillo de enteros. Ya estamos en el territorio de la teoría algebraica de números. Después, Lamé llegó a una contradicción usando que en este anillo, dos elementos $x + y\zeta_p^i$, $x + y\zeta_p^j$ son relativamente primos siempre que $i \neq j$, y la ecuación (1). Sin embargo, Liouville encontró un problema: esta prueba dependía de que $\mathbb{Z}[\zeta_p]$ fuera un dominio de factorización única, cosa que no es cierta. La prueba no era correcta.

Se decía que esta prueba era lo primero que se le ocurriría a un matemático mínimamente competente. De hecho, el propio Kummer ya había intentado esta estrategia, dándose cuenta del fallo. Intentó salvar la dificultad de la no factorización única definiendo lo que llamó *números ideales*, que más adeltante llegaron a ser lo que hoy conocemos como los ideales de un anillo. Probó que se puede definir un producto entre los ideales, y que entre los ideales sí que se mantiene la factorización única entre ideales primos.

En este trabajo seguiremos los pasos de Gauss y Lagrange y centraremos nuestros esfuerzo en las formas cuadráticas, ecuaciones de la forma

$$f(x, y) = ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{Z}.$$

Se suele prestar más atención a las formas cuadráticas *primitivas*, aquellas donde a, b y c son relativamente primos.

Diremos que un entero m es representado por una forma cuadrática f si $m = f(x, y)$ tiene solución entera en x, y. Estudiaremos entonces qué primos se pueden representar según la forma cuadrática $x^2 + ny^2$. Dada una forma cuadrática $f(x, y) = ax^2 + bxy + cy^2$, definimos su *discriminante* como $D = b^2 - 4ac$. Hay una condición necesaria y suficiente para que un número m se represente mediante una forma cuadrática de discriminante D:

Proposición 0.2 ([Cox11, Lema 2.5]). Sea $D \equiv 0, 1 \mod 4$ un entero y m un entero relativamente primo con D. Entonces m se representa mediante una forma cuadrática primitiva de discriminante D si y sólo si D es un residuo cuadrático módulo m.

Con este resultado, una respuesta a esta pregunta en términos puramente de formas cuadráticas es:

Corolario 0.3 ([Cox11, Corolario 2.6]). Sea n un entero y p un primo impar que no divide a n. Entonces $\left(\frac{-n}{p}\right) = 1$ si y sólo si p se representa mediante una forma primitiva de discriminante $-4n$, donde $\left(\frac{\cdot}{p}\right)$ denota el símbolo de Legendre.

A lo largo del trabajo veremos conceptos muy parecidos a estos, desde el punto de vista de la teoría algebraica de números, y de su lenguaje: los ideales. Este problema está resuelto para cualquier n, usando lo que se conoce como teoría de cuerpos de clases, pero no llegaremos tan lejos, sólo hasta donde podamos con las herramientas elementales de la descomposición en ideales. La ecuación $p = x^2 + ny^2$ se puede factorizar como

$$x^2 + ny^2 = \left(x + y\sqrt{-n}\right)\left(x - y\sqrt{-n}\right),$$

así que parece natural estudiar las extensiones cuadráticas. Eso es exactamente lo que haremos: estudiar un objeto algebraico, la extensión $\mathbb{Q}[\sqrt{-n}]$, para responder a una pregunta sobre formas cuadráticas.

1 Generalidades de la teoría algebraica de números

1.1 Traza, norma y discriminante.

Sea L/K una extensión de cuerpos finita, con $[L : K] = n$, y tomemos una base $\alpha_1, ..., \alpha_n$ de L/K. Sea $\alpha \in L$ y consideremos el homomorfismo $\alpha\cdot : L \to L$ dado por la multiplicación por α. Digamos que las imágenes de los elementos de la base vienen dadas por $\alpha\alpha_i = \sum_j a_{ij}\alpha_j$, entonces la matriz del endomorfismo respecto de esa base es $A = (a_{ij})$.

Definición 1.1. *La **traza** de α, $t_{L/K}(\alpha)$, se define como $a_{11}+a_{22}+...+a_{nn}$. La **norma** de α, $N_{L/K}(\alpha)$, se define como* $\det(a_{ij})$.

Observación 1.2. Cabe destacar que esta definición no depende de la base escogida, puesto que en general el determinante y la traza de un endomorfismo no lo hacen.

Proposición 1.3 (Propiedades de la traza y la norma.). Se deducen de la definición las siguientes propiedades:
(a) $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$, $\quad t_{L/K}(\alpha + \beta) = t_{L/K}(\alpha) + t_{L/K}(\beta)$.
(b) $N_{L/K}(a\beta) = a^n N_{L/K}(\beta)$, $\quad t_{L/K}(a\alpha) = at_{L/K}(\alpha)$.
(c) $N_{L/K}(\alpha^{-1}) = N_{L/K}(\alpha)^{-1}$.
Donde $\alpha, \beta \in L, a \in K$.

Observación 1.4. En el polinomio característico del endomorfismo definido antes, $f_\alpha(t) = \det(t\,\mathrm{Id} - A) = t^n - a_1 t^{n-1} + ... + (-1)^n a_n \in K[t]$, se pueden ver la traza y la norma como:

$$a_1 = t_{L/k}(\alpha), \qquad a_n = N_{L/k}(\alpha).$$

Con esto, tenemos que la traza y la norma de un elemento de L pertenecen al cuerpo base K.

Si L/K es separable y de grado n, por el teorema del elemento primitivo podemos escribir $L = K[\alpha]$ para algún $\alpha \in L$. Por ser separable, el polinomio mínimo de α no tiene raíces múltiples. Ahora, si denotamos por $\sigma^{(i)} : L \longrightarrow \overline{K}$ las distintas inmersiones de L en la clausura algebraica de K que fijan K, para $\gamma \in K$ denotamos $\gamma^{(i)} := \sigma_i(\gamma)$ a los distintos conjugados de γ, una definición alternativa y más cómoda es tomar $N_{L/K}(\gamma) = \gamma^{(1)}\gamma^{(2)}...\gamma^{(n)}$ y $t_{L/K}(\gamma) = \gamma^{(1)} + \gamma^{(2)} + ... + \gamma^{(n)}$. Más adelante trabajaremos con extensiones de Galois. Por fijar ideas, en este caso los σ_i serán los automorfismos de la extensión.

A partir de ahora vamos a omitir los subíndices en la traza y la norma por aligerar la notación.

Otro aspecto a destacar es que si L/K es separable, entonces la traza no es idénticamente nula. Por ejemplo, en cuerpos de característica 0, que son los que vamos a tratar, $t(1) = n \neq 0$

Definición 1.5. *Si tomamos elementos $\alpha_1, \dots, \alpha_n \in L$, definimos el* ***discriminante*** $\Delta(\alpha_1, \dots, \alpha_n) := \det\left(t(\alpha_i\alpha_j)\right)$.

Proposición 1.6. Si $\Delta(\alpha_1, ...\alpha_n) \neq 0$, entonces $\alpha_1, ..., \alpha_n$ es una base de L sobre K. Además, si L/K es separable y $\alpha_1, ..., \alpha_n$ es una base de L sobre K, entonces su discriminante $\Delta(\alpha_1, ...\alpha_n) \neq 0$.

Demostración. Supongamos que $\alpha_1, ..., \alpha_n$ son linealmente dependientes, entonces existen $a_1, ..., a_n \in K$ no todos nulos tales que $\sum a_i\alpha_i = 0$. Multiplicando por α_j y tomando traza:

$$\sum_i a_i t(\alpha_i\alpha_j) = 0, \quad j = 1, 2...., n$$

Es decir, la matriz $\left(t\left(\alpha_i\alpha_j\right)\right)$ tiene tiene determinante nulo, lo que contradice que $\Delta(\alpha_1, ...\alpha_n) \neq 0$.

Ahora, si $\alpha_1, ..., \alpha_n$ es una base, supongamos que $\Delta(\alpha_1, ...\alpha_n) = 0$. Entonces, el sistema de ecuaciones lineales

$$\sum_i x_i t(\alpha_i\alpha_j) = 0 \quad j = 1, ..., n$$

Tiene solución no trivial $x_i = a_i$, $j = 1, ..., n$. Si $\alpha = \sum a_i\alpha_i$, que es no nulo, entonces $t(\alpha\alpha_j) = 0$, $j = 1, ..., n$ por las propiedades de la traza.
Como $\alpha_1, ..., \alpha_n$ es una base, se deduce que $t(\alpha\beta) = 0$ para todo $\beta \in L$, y esto implica que la traza es idénticamente nula. Como L/K es separable, esto no puede ocurrir.

Proposición 1.7. Supongamos que $\alpha_1, ..., \alpha_n$ y $\beta_1, ..., \beta_n$ son bases para L/K, con $\alpha_i = \sum_j a_{ij}\beta_j,\ a_{ij} \in K$. Entonces $\Delta(\alpha_1, ...\alpha_n) = \det\left(a_{ij}\right)^2 \Delta(\beta_1, ...\beta_n)$

Demostración. Tomemos traza en ambos lados de la igualdad $\alpha_i\alpha_j = \sum_j \sum_l a_{ij}a_{kl}\beta_j\beta_l$.

Sean las matrices $A = \left(t(\alpha_i\alpha_j)\right)$, $B = \left(t(\beta_i\beta_j)\right)$, $C = \left(a_{ij}\right)$. Se tiene la igualdad matricial $A = C^t BC$. Basta tomar determinantes a ambos lados para tener lo que se quiere probar. ∎

La siguiente proposición da una forma más cómoda de calcular discriminantes.

Proposición 1.8. Sea L/K una extensión separable de grado n y $\alpha_1, \alpha_2, ..., \alpha_n \in L$. Sean $\sigma_1, \ldots, \sigma_n$ las inmersiones de L en una clausura algebraica de K. Si denotamos $\sigma_j(\alpha_i) = \alpha_i^{(j)}$, entonces:

$$\Delta(\alpha_1, ...\alpha_n) = \det\left(\alpha_i^{(j)}\right)^2.$$

Demostración. Sabemos que $t(\alpha_i\alpha_j) = \alpha_i^{(1)}\alpha_j^{(1)} + \alpha_i^{(2)}\alpha_j^{(2)} + ... + \alpha_i^{(n)}\alpha_j^{(n)}$. Sean las matrices $A = \left(t(\alpha_i\alpha_j)\right)$ y $B = (\alpha_i^{(k)})$. Entonces, $A = BB^t$. Tomando determinantes se tiene lo que se quiere probar. ∎

Proposición 1.9. Supongamos que β es un elemento primitivo de L sobre K. Sea $f(x) \in K[x]$ el polinomio mínimo de β sobre K. Si L/K es separable, entonces,

$$\Delta\left(1, \beta, ..., \beta^{n-1}\right) = (-1)^{(n(n-1))/2} N\left(f'(\beta)\right),$$

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

Demostración. La matriz $\left(\left(\beta^{(j)}\right)^i\right)$ con $j = 1, ..., n$ e $i = 0, ..., n-1$ es una matriz de Vandermonde, luego su determinante viene dado por:

$$\prod_{i<j}\left(\beta^{(j)} - \beta^{(i)}\right).$$

Entonces, tenemos:

$$\Delta\left(1, \beta, ..., \beta^{n-1}\right) = (-1)^{(n(n-1))/2} \prod_{i\neq j}\left(\beta^{(j)} - \beta^{(i)}\right).$$

Ahora, $f(x) = \prod_i \left(x - \beta^{(i)}\right)$, y entonces $f'(\beta^{(j)}) = \prod_i \left(\beta^{(j)} - \beta^{(i)}\right)$ con $i \neq j$. Como $f'(\beta^{(j)}) = (f'(\beta))^{(j)}$, tomando el producto en j se obtiene lo que se quiere probar. ∎

1.2 Cuerpos de números y anillos de enteros.

Comencemos la sección con algunas definiciones básicas.

Definición 1.10. *Llamamos* ***cuerpo de números*** *a una extensión finita $K/\mathbb{Q}$. Los elementos de K se llaman* ***números algebraicos****.*

Definición 1.11. *Sea R un anillo, y $A \subseteq R$ un subanillo. Decimos que un elemento $x \in R$ es* ***entero*** *sobre A si existen elementos $a_1, ..., a_n \in A$ tales que:*

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

Si K es un cuerpo de números, los elementos de K que son enteros sobre $\mathbb{Z}$ se dicen ***enteros algebraicos****. El conjunto de los enteros algebraicos de K se denotará por $\mathcal{O}_K$.*

Una observación interesante es el hecho de que esto generaliza la situación que tenemos entre $\mathbb{Q}$ y $\mathbb{Z}$: los enteros algebraicos de $\mathbb{Q}$ son precisamente los números enteros, como ilustramos en la siguiente proposición.

Proposición 1.12. Un número racional $r \in \mathbb{Q}$ es un entero algebraico si y sólo si $r \in \mathbb{Z}$

Demostración. Si $r \in \mathbb{Z}$, verifica la ecuación $x - r = 0$, pero esto es decir que es entero algebraico.

Si $r \in \mathbb{Q}$ es un entero algebraico, verifica la ecuación $x^n + b_1 x^{n-1} + ... + b_{n-1} x + b_n$,con los $b_1, ..., b_n \in \mathbb{Z}$. Escribimos $r = \frac{c}{d}$, con $d \neq 0$ y c, d relativamente primos. Sustituyendo en la ecuación y multiplicando en ambos lados por d^n queda:

$$c^n + b_1 c^{n-1} d + b_2 c^{n-2} d^2 + ... + b_{n-1} c d^{n-1} + b_n d^n = 0,$$

de donde se deduce despejando que $d \mid c^n$, pero como $\gcd(c, d) = 1$, debe ser $d = \pm 1$, luego $r \in \mathbb{Z}$.

Proposición 1.13. Sea R un anillo, A un subanillo de R, y $x \in R$. Son equivalentes:
(1) x es entero sobre A.
(2) El anillo $A[x]$ es un $A-$módulo finitamente generado.
(3) Existe un subanillo B de R tal que $A[x] \subseteq B$ y B es un $A-$módulo finitamente generado.

Demostración. (1) $\Rightarrow$ (2) : Como x es entero sobre A, verifica un polinomio mónico $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ con $a_1, \ldots, a_n \in A$. Veamos que $\{1, x, \ldots, x^{n-1}\}$ es un sistema generador del $A-$módulo $A[x]$. Como $x^n = -\left(a_1 x^{n-1} + \cdots + a_n\right)$, podemos

expresar cualquier potencia superior a x^n como una combinación de $1, x, ..., x^{n-1}$ con los coeficientes en A.
(2) $\Rightarrow$ (3) : Basta tomar $B = A[x]$.
(3) $\Rightarrow$ (1) : Sea $B = Ay_1 + ... + Ay_n$. Como $x, y_i \in B$, entonces podemos escribir su producto como $xy_i = \sum_{j=1}^{n} a_{ij} y_j$ con los $a_{ij} \in A$. Despejando, tenemos $\sum_{j=1}^{n} \left(\delta_{ij} x - a_{ij}\right) y_j = 0$ para todo $i = 1, ..., n$. En otras palabras, el sistema de ecuaciones lineales $\sum_{j=1}^{n} \left(\delta_{ij} x - a_{ij}\right) Y_j = 0$ con $i = 1, ..., n$ tiene como solución a $(y_1, ..., y_n)$.

Sea d el determinante de la matriz $\left(\delta_{ij} x - a_{ij}\right)_{i,j}$. Recordemos que cuando tenemos una igualdad matricial $M \cdot \underline{x} = 0$, multiplicando por la matriz adjunta traspuesta de M, obtenemos $\det(M) \cdot \underline{x} = 0$. En nuestro caso tenemos que $d\, y_j = 0$ para $j = 1, \dots, n$.

Como $1 \in B$, lo podemos escribir en la forma $1 = \sum_{j=1}^{n} c_j y_j$, con $c_j \in A$. Entonces $d = d \cdot 1 = \sum_{j=1}^{n} c_j d y_j = 0$. Calculando d explícitamente:

$$d = \det \begin{pmatrix} x - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & x - a_{22} & \dots & -a_{2n} \\ \vdots & \vdots & & \vdots \\ -a_{n1} & -a_{n2} & \dots & x - a_{nn} \end{pmatrix},$$

se deduce que d es de la forma $0 = d = x^n + ... + b_1 x^{n-1} + ... + b_n$ con cada $b_i \in A$, es decir, x es entero sobre A.

Esto se puede generalizar con n elementos de R: el anillo $A[a_1, ..., a_n]$ es finitamente generado como $A-$módulo si y sólo si los generadores son enteros sobre A.

Corolario 1.14. El conjunto B de elementos de R que son enteros sobre A es un subanillo de R que contiene a A.

Demostración. Sean $x, y \in B$, entonces $A[x, y]$ es un $A-$módulo finitamente generado, y por lo tanto $x + y$, xy son enteros sobre A.

Definición 1.15. *El conjunto B del corolario anterior se llama **clausura íntegra** de A en R. Si $B = A$, decimos que A es **íntegramente cerrado** en R. Diremos que A es íntegramente cerrado si lo es en su cuerpo de fracciones.*

El objetivo de esta sección es ver que el anillo de enteros de un cuerpo de números K es lo que llamamos un *dominio de Dedekind*. Presentamos este concepto en la siguiente definición:

Definición 1.16. *Un **dominio de Dedekind** es un dominio de integridad $\mathcal{O}_K$ tal que:*

1. *Es noetheriano.*
2. *Todo ideal primo no nulo es maximal.*
3. *$\mathcal{O}_K$ es íntegramente cerrado*

Lema 1.17. Sea $\beta \in K$. Existe un $b \in \mathbb{Z}$ no nulo tal que $b\beta \in \mathcal{O}_K$.

Demostración. Como $\beta \in K$, cumple la ecuación $a_0\beta^n + a_1\beta^{n-1} + ... + a_n = 0$ con los $a_i \in \mathbb{Z}$ y $a_0 \neq 0$. Multiplicando en ambos lados de la ecuación por a_0^{n-1} queda: $\left(a_0\beta\right)^n + a_1\left(a_0\beta\right)^{n-1} + ... + a_n a_0^{n-1} = 0$, es decir, $a_0\beta$ verifica un polinomio mónico con coeficientes enteros, luego $a_0\beta \in \mathcal{O}_K$.

Como consecuencia podemos sacar que, dada una base de K sobre $\mathbb{Q}$, podemos obtener siempre una base que consista de enteros algebraicos, multiplicando por el mínimo común múltiplo de los enteros descritos en el lema anterior.

Proposición 1.18. Todo ideal no nulo $\mathfrak{a}$ de $\mathcal{O}_K$ contiene una base de K sobre $\mathbb{Q}$.

Demostración. Tomemos $\beta_1, ..., \beta_n$ una base de K sobre $\mathbb{Q}$. Por el lema anterior, existe un $b \in \mathbb{Z}$ no nulo tal que $b\beta_1, ..., b\beta_n$ están en $\mathcal{O}_K$. Basta tomar un $\alpha \in \mathfrak{a}$ no nulo y los elementos $b\beta_1\alpha, ..., b\beta_n\alpha$ están en $\mathfrak{a}$ y son una base de K sobre $\mathbb{Q}$.

Observación 1.19. Vamos a considerar la extensión $K/\mathbb{Q}$, y sobre ella la traza y la norma. Se verifica para $\alpha \in K$, que su traza y su norma son números racionales, por la observación que hicimos sobre el polinomio característico. Ahora, si $\alpha \in \mathcal{O}_K$, como sus conjugados verifican el mismo polinomio, también son enteros algebraicos, y su suma y producto son enteros algebraicos. Entonces, la traza y la norma de α son enteros por la proposición 1.12. Como consecuencia, si $\alpha_1, ..., \alpha_n \in \mathcal{O}_K$ es una base de K sobre $\mathbb{Q}$, su discriminante también es entero.

Una propiedad muy importante del discriminante es que nos permite expresar los ideales de $\mathcal{O}_K$ de una forma muy útil.

Proposición 1.20. Sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$ y supongamos que $\alpha_1, ..., \alpha_n \in \mathfrak{a}$ es una base de $K/\mathbb{Q}$ con $\left|\Delta(\alpha_1, ..., \alpha_n)\right|$ mínimo. Entonces $\mathfrak{a} = \mathbb{Z}\alpha_1 + ... + \mathbb{Z}\alpha_n$, es decir, todo ideal de $\mathcal{O}_K$ es un $\mathbb{Z}-$módulo libre de rango n.

Demostración. Observamos que como $\left|\Delta(\alpha_1, ..., \alpha_n)\right|$ es un entero positivo, hay alguna base con tal cantidad mínima.

Sea $\alpha \in \mathfrak{a}$, con $\alpha = \gamma_1\alpha_1 + ... + \gamma_n\alpha_n, \quad \gamma_i \in \mathbb{Q}$. Hay que probar que $\gamma_i \in \mathbb{Z}$.

Supongamos que hay alguno que no, γ_1, y si no, basta reordenarlos. Entonces podemos escribir $\gamma_1 = m + \theta$ con $m \in \mathbb{Z}$ y $0 < \theta < 1$.

Sean $\beta_1 = \alpha - m\alpha_1,\ \beta_2 = \alpha_2, ...,\ \beta_n = \alpha_n$, que forman una base de $K/\mathbb{Q}$. Escribiendo $\beta_1 = \theta\alpha_1 + \gamma_2\alpha_2 + ... + \gamma_n\alpha_n$, nos damos cuenta de que la matriz de cambio de base entre $\{\alpha_i\}$ y $\{\beta_i\}$ es:

$$\begin{pmatrix} \theta & 0 & \dots & 0 \\ \gamma_2 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_n & 0 & \dots & 1 \end{pmatrix}$$

Y sabemos por la proposición 1.7 que $\Delta(\beta_1, ...\beta_n) = \theta^2\Delta(\alpha_1, ...\alpha_n)$. Recordemos que $\theta < 1$, así que esto contradicie la minimalidad del discriminante de $\alpha_1, ...\alpha_n$.

Definición 1.21. *Si $\alpha_1, ..., \alpha_n \in \mathfrak{a}$ es una base de $K/\mathbb{Q}$ tal que $\mathfrak{a} = \alpha_1\mathbb{Z} + ... + \alpha_n\mathbb{Z}$, decimos que es una **base entera** de $\mathfrak{a}$.*

Observación 1.22. Dos bases enteras de un ideal tienen el mismo discriminante, ya que deben tener el mismo valor absoluto y además, por la proposición 1.7, tienen el mismo signo. Esto permite definir $\Delta(\mathfrak{a}) := \Delta(\alpha_1, ..., \alpha_n)$, el discriminante de $\mathfrak{a}$. Para el caso $\mathfrak{a} = \mathcal{O}_K$, definimos $\delta_K := \Delta\left(\mathcal{O}_K\right)$ como el **discriminante de K**.

Observación 1.23 ([Rib13, Capítulo 6, Teorema L]). Dado un ideal $\mathfrak{a}$, utilizando la forma normal de Smith, existe una base entera $x_1, \dots, x_n$ de $\mathcal{O}_K$ y unos $f_1, \dots, f_n \in \mathbb{Z}$ tales que $f_1x_1, \dots, f_nx_n$ es una base entera de $\mathfrak{a}$. Más aún, los f_i se pueden escoger de tal forma que $f_1 \mid f_2 \mid \dots \mid f_n$.

Ahora pasaremos a ver una serie de propiedades importantes del anillo $\mathcal{O}_K$ y de sus ideales. A lo largo del desarrollo, sólo consideraremos ideales no nulos.

Lema 1.24. Si $\mathfrak{a} \subseteq \mathcal{O}_K$ es un ideal, entonces $\mathfrak{a} \cap \mathbb{Z} \neq 0$.

Demostración. Sea $\alpha \in \mathfrak{a}, \alpha \neq 0$. Entonces, verifica un polinomio mónico con coeficientes enteros $\alpha^m + a_1\alpha^{m-1} + ... + a_m = 0$. Como estamos trabajando en un cuerpo, podemos asumir que el polinomio tiene término independiente no nulo, ya que si no, basta multiplicar por α^{-1}. Despejando, $a_m = -\left(\alpha^m + a_1\alpha^{m-1} + ... + a_{m-1}\alpha\right) \in \mathfrak{a} \cap \mathbb{Z}$.

Proposición 1.25. Sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$. El cociente $\mathcal{O}_K/\mathfrak{a}$ es finito.

Demostración. Por el lema 1.24, existe un $a \in \mathfrak{a} \cap \mathbb{Z}$ no nulo. Sea $(a) \subseteq \mathfrak{a}$ el ideal generado por a. Como $\mathcal{O}_K/(a)$ se proyecta de forma sobreyectiva sobre $\mathcal{O}_K/\mathfrak{a}$, vamos a probar que el segundo es finito. De hecho, vamos a ver que tiene exactamente a^n elementos.

Por la proposición 1.20, podemos escribir $\mathcal{O}_K = \mathbb{Z}\omega_1 + ... + \mathbb{Z}\omega_n$. Sea el conjunto $S = \{\sum \gamma_i\omega_i \ : \ 0 \leq \gamma_i < a\}$. Vamos a probar que S es un conjunto de representantes de $\mathcal{O}_K/\mathfrak{a}$.

Sea $\omega = \sum m_i\omega_i \in \mathcal{O}_K$, y escribamos $m_i = q_i a + \gamma_i$ con $0 \leq \gamma_i < a$. Entonces, $w \equiv \sum \gamma_i\omega_i \mod a$, es decir, cada clase de equivalencia del cociente contiene un elemento de S.

Ahora, si $\sum \gamma_i\omega_i$ y $\sum \gamma_i'\omega_i$ están en la misma clase de equivalencia, veamos que $\gamma_i = \gamma_i'$. Como $\sum \gamma_i\omega_i \equiv \sum \gamma_i'\omega_i$, y los ω_i son linealmente independientes, entonces $a \mid \gamma_i - \gamma_i'$. Ahora, como $0 \leq \gamma_i, \gamma_i' < a$, necesariamente es $\gamma_i - \gamma_i' = 0$.

Por lo tanto, S es un conjunto de representantes de $\mathcal{O}_K/(a)$, con cardinal a^n, y el anillo cociente es finito. ∎

A partir de esta proposición se pueden sacar algunas conclusiones muy importantes:

Corolario 1.26. $\mathcal{O}_K$ es noetheriano.

Demostración. Sea $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots$ una cadena ascendente de ideales de $\mathcal{O}_K$. Como $\mathcal{O}_K/\mathfrak{a}_1$ es finito, por el teorema de la correspondencia, sólo puede haber una cantidad finita de ideales de $\mathcal{O}_K$ que contengan a $\mathfrak{a}_1$. ∎

Corolario 1.27. Todo ideal primo de $\mathcal{O}_K$ es maximal.

Demostración. Sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$. Entonces, $\mathcal{O}_K/\mathfrak{p}$ es un dominio de integridad finito, luego es un cuerpo, así que $\mathfrak{p}$ es maximal. ∎

Observación 1.28. $\mathcal{O}_K$ es íntegramente cerrado. En efecto, sea $\alpha \in K$ tal que, para algunos $a_1, \ldots, a_n \in \mathcal{O}_K$, tengamos $\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n = 0$. Queremos ver que $\alpha \in \mathcal{O}_K$, es decir, que es entero sobre $\mathbb{Z}$.

Consideremos el anillo $B = \mathcal{O}_K[\alpha] \subseteq K$. Desde luego, este anillo contiene a $\mathbb{Z}[\alpha]$. Vamos a probar que B es un $\mathbb{Z}-$módulo finitamente generado.

Sabemos que $\mathcal{O}_K = \mathbb{Z}u_1 + \ldots \mathbb{Z}u_n$ para alguna base entera. Desde luego, como $\alpha^n = -\left(a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n\right)$, B es un $\mathcal{O}_K-$módulo finitamente generado, y como $\mathcal{O}_K$ es un $\mathbb{Z}-$módulo finitamente generado, también lo es B. Por tanto, $\alpha \in \mathcal{O}_K$, y el anillo de enteros es íntegramente cerrado.

Hemos probado las tres propiedades que debe cumplir un dominio de Dedekind. Podemos afirmar entonces:

Corolario 1.29. $\mathcal{O}_K$ es un dominio de Dedekind.

Observación 1.30. Consideremos el cuerpo de números $\mathbb{Q}[i]$. Más adelante veremos que su anillo de enteros es $\mathbb{Z}[i]$, el anillo de los enteros de Gauss. Es conocido que este anillo es un dominio de factorización única (de hecho, es un dominio euclídeo). Sin embargo, esta situación no es para nada común. Por ejemplo, sea $K = \mathbb{Q}[\sqrt{-5}]$. de nuevo, en el capítulo 2 veremos que su anillo de enteros es $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Ocurre lo siguiente:

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

Usando la norma se puede probar que estas dos son factorizaciones en irreducibles distintas, así que K no es dominio de factorización única.

Ahora vamos a estudiar más en profundidad los dominios de Dedekind. Veremos que en este tipo de anillos, los ideales se pueden factorizar de forma única como producto de ideales primos, y esto será muy importante. Comencemos recordando la definición del producto de dos ideales.

Definición 1.31. *Si I, J son ideales de un anillo A, definimos el ideal IJ como el ideal generado por todos los productos ab con $a \in I$ y $b \in J$, es decir, es el conjunto de sumas finitas $\sum a_i b_i$ donde $a_i \in I$, $b_i \in J$.*

A partir de ahora, por no repetir demasiado, por *ideal* entenderemos ideal no nulo. Los resultados que probaremos serán válidos para cualquier dominio de Dedekind, y los denotaremos $\mathcal{O}_K$ donde K será su cuerpo de fracciones.

Proposición 1.32. Sea I un ideal en un dominio de Dedekind $\mathcal{O}_K$. Existe un ideal J tal que IJ es principal.

Para probar esta proposición usaremos dos lemas:

Lema 1.33. Todo ideal en un dominio de Dedekind contiene un producto de ideales primos.

Demostración. Supongamos que el resultado no es cierto. Entonces, si llamamos S al conjunto de los ideales de $\mathcal{O}_K$ que no contienen un producto de ideales primos, no es vacío. Como $\mathcal{O}_K$ es noetheriano, S contiene un elemento maximal M, el cual no puede ser primo porque está en S.

Como M no es primo, existen $\alpha, \beta \in \mathcal{O}_K$ tales que $\alpha\beta \in M$ pero ninguno de ellos está en M. Entonces, los ideales $M + (\alpha)$ y $M + (\beta)$ contienen estrictamente a M. Ahora bien, M era un elemento maximal de S, así que $M + (\alpha)$ y $M + (\beta)$ contienen

un producto de ideales primos, pues no pueden estar en S por la maximalidad de M. Entonces, $(M+(\alpha))(M+(\beta))$ también contiene un producto de ideales primos, y está contenido en M. Tendríamos que M contiene un producto de ideales primos, lo cual no es cierto.

Lema 1.34. Sea I un ideal propio en un dominio de Dedekind $\mathcal{O}_K$ cuyo cuerpo de fracciones es K. Existe un $\gamma \in K \setminus \mathcal{O}_K$ tal que $\gamma I \subseteq \mathcal{O}_K$.

Demostración. Sea $\alpha \in I$. Por el lema 1.33, (α) contiene un producto de ideales primos. Fijemos $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ tales que $\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq (\alpha)$, con r mínimo.

Como I es un ideal propio, está contenido en un ideal maximal, y por tanto primo, porque en los dominios de Dedekind, primo y maximal son equivalentes: $I \subseteq \mathfrak{p}$. Entonces, el producto $\mathfrak{p}_1 \dots \mathfrak{p}_r$ está contenido en $\mathfrak{p}$. De aquí se sigue que $\mathfrak{p} \supseteq \mathfrak{p}_i$ para algún i. Si no fuera así, tomemos $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$. Se verifica que $a_1 \dots a_r \in \mathfrak{p}$, y como es primo algún a_i debe estar en $\mathfrak{p}$, lo que es una contradicción.

Ahora, como ambos ideales son primos (y maximales) $\mathfrak{p} = \mathfrak{p}_i$. Vamos a tomar $i = 1$ por simplificar, pues basta reordenar el producto.

Recordemos que r fue tomado mínimo, así que $\mathfrak{p}_2 \dots \mathfrak{p}_r \subsetneq (\alpha)$. Tomemos $\beta \in \mathfrak{p}_2 \dots \mathfrak{p}_r \setminus (\alpha)$, y sea $\gamma = \beta/\alpha$. Este elemento verifica el enunciado:

$$(\beta/\alpha)I \subseteq (\beta/\alpha)\mathfrak{p} = (\beta/\alpha)\mathfrak{p}_1 \subseteq {}^{1}(\mathfrak{p}_2 \dots \mathfrak{p}_r)(\alpha^{-1})\mathfrak{p}_1 = \alpha^{-1}\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq \alpha^{-1}(\alpha) = \mathcal{O}_K.$$

Por último, observemos que $\gamma \notin \mathcal{O}_K$. De ser así, tendríamos $\beta/\alpha \in \mathcal{O}_K$, es decir, $\beta \in (\alpha)$, que no es cierto.

Demostración (de la proposición 1.32). Sea $\alpha \in I$ no nulo, y sea $J := \{\beta \in \mathcal{O}_K : \beta I \subseteq (\alpha)\}$. Entonces J es un ideal, y además es no nulo puesto que $\alpha \in J$. Es inmediato que $IJ \subseteq (\alpha)$.

Ahora, sea $A = \frac{1}{\alpha} IJ$, que está contenido en $\mathcal{O}_K$, pues $IJ \subseteq (\alpha)$, y es un ideal. Tenemos dos casos: Si $A = \mathcal{O}_K$, entonces, despejando: $IJ = (\alpha)$ y habríamos terminado. Si no, es un ideal propio, y podemos aplicar el lema 1.34: $\gamma A \subseteq \mathcal{O}_K$ para algún elemento $\gamma \in K \setminus \mathcal{O}_K$. Gracias a este γ, llegaremos a una contradicción. Usaremos que $\mathcal{O}_K$ es íntegramente cerrado, y encontraremos un polinomio mónico con coeficientes en $\mathcal{O}_K$ que tenga a γ como raíz.

Como $\alpha \in I$, se tiene que $\frac{1}{\alpha} IJ$ contiene a J. En efecto, si $x \in J$, basta escribir $x = \frac{1}{\alpha}\alpha x$, y esto está en $\frac{1}{\alpha} IJ$.

[1] Recordemos que $\beta \in \mathfrak{p}_2 \dots \mathfrak{p}_r$

Entonces, $\gamma J \subseteq \gamma A \subseteq \mathcal{O}_K$, y de aquí deducimos que $\gamma J \subseteq J$: Sea $\beta \in J$, luego $\gamma\beta \in \gamma J$. Veamos que $\gamma\beta \in J = \{x \in \mathcal{O}_K : xI \subseteq (\alpha)\}$. Sabemos que $\gamma A = (\gamma/\alpha)IJ \subseteq \mathcal{O}_K$, y en particular $(\gamma\beta/\alpha)I \subseteq \mathcal{O}_K$. Despejando, tenemos $(\gamma\beta)I \subseteq \alpha\mathcal{O}_K = (\alpha)$, luego $\gamma\beta \in J$ como queríamos probar.

Ahora, como $\mathcal{O}_K$ es noetheriano, podemos escribir $J = (\alpha_1, \dots, \alpha_m)$. Vamos a usar la relación $\gamma J \subseteq J$ para obtener el polinomio que buscábamos. Como $\gamma\alpha_i \in J$, podemos escribirlos en la forma $\gamma\alpha_i = a_{i1}\alpha_1 + \cdots + a_{im}\alpha_m$ para $i = 1, \dots, m$. Para $M = (a_{ij})$, esto se traduce en la ecuación matricial:

$$\gamma \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} \iff (\gamma I - M) \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = 0.$$

Como los α_i generan J, y este ideal es no nulo, no todos los generadores pueden ser nulos, pero entonces la matriz $\gamma I - M$ tiene determinante 0. Escribiendo el determinante queda un polinomio mónico en γ con coeficientes en $\mathcal{O}_K$, luego γ es entero sobre $\mathcal{O}_K$, y como es íntegramente cerrado, $\gamma \in \mathcal{O}_K$, lo que es una contradicción. ∎

La siguiente definición va a ser central en el desarrollo de nuestra teoría.

Definición 1.35. *Dos ideales $A, B \subseteq \mathcal{O}_K$ se dicen equivalentes ($A \sim B$) si existen $\alpha, \beta \in \mathcal{O}_K$ tales que $\alpha A = \beta B$. Esta relación es de equivalencia, y a las clases de equivalencia las llamaremos* ***clases de ideales****.*

Observación 1.36. $\mathcal{O}_K$ es un dominio de ideales principales si y sólo si sólo hay una clase de ideales. En efecto, si $\mathcal{O}_K$ es un dominio de ideales principales, sea (α) un ideal, entonces es claro que está relacionado con $\mathcal{O}_K$, pues basta escribir $(\alpha) = \alpha\mathcal{O}_K$. Recíprocamente, sea I un ideal de $\mathcal{O}_K$, y veamos que es principal. Como $I \sim \mathcal{O}_K$, existen $\alpha, \beta \in \mathcal{O}_K$ tales que $\alpha I = \beta\mathcal{O}_K$, es decir, $I = (\beta/\alpha)$, es un ideal principal. De aquí deducimos que **el número de clases de ideales mide, en cierto modo, cómo de lejos está un anillo de ser dominio de ideales principales**.

Observación 1.37. El producto de ideales se puede extender de forma natural a las clases de ideales: $\overline{I} \cdot \overline{J} = \overline{IJ}$. A priori, este producto dota a las clases de ideales de estructura de monoide conmutativo. Para los dominios de Dedekind, la proposición 1.32 les da estructura de grupo, pues implica que toda clase de ideales tenga un elemento inverso.

Podemos seguir explotando la proposición 1.32 para deducir algunas propiedades buenas del producto de ideales, como son la siguientes:

Proposición 1.38 (Ley de cancelación). Si A, B, C son ideales en un dominio de Dedekind $\mathcal{O}_K$ tales que $AB = AC$, entonces $B = C$.

Demostración. Sabemos que existe un ideal J tal que $AJ = (\alpha)$, luego:

$$AJB = AJC \Rightarrow \alpha B = \alpha C \Rightarrow B = C.$$

Proposición 1.39. Sean A, B ideales en un dominio de Dedekind $\mathcal{O}_K$. Entonces, $A \mid B$ si y sólo si $B \subseteq A$.

Demostración. Supongamos que $A \mid B$, entonces $B = AC$ para algún ideal C. Sea $x \in B = AC$, entonces $x = \sum a_i c_i \in A$, luego $B \subseteq A$.

Supongamos ahora que $B \subseteq A$, y veamos que $A \mid B$. Sea J un ideal tal que $AJ = (\alpha)$, y denotemos $C = (1/\alpha)BJ$. Es un ideal de $\mathcal{O}_K$, y además:

$$AC = A(1/\alpha)BJ = (1/\alpha)AJB = (1/\alpha)(\alpha)B = B,$$

como queríamos.

Ahora podemos probar el resultado estrella de los dominios de Dedekind:

Teorema 1.40. *Todo ideal en un dominio de Dedekind se puede escribir de manera única como producto de ideales primos.*

Demostración. Veamos primero la existencia de esa representación. Sea S el conjunto de los ideales (propios) que no se pueden escribir como producto de ideales primos, y supongamos que $S \neq \emptyset$. Como $\mathcal{O}_K$ es noetheriano, S contiene un elemento maximal $M \neq \mathcal{O}$. Existe un ideal maximal (y por tanto, primo) P que contiene a M, luego $M = PI$ para algún ideal I. Entonces, I contiene a M, y la contención es estricta: supongamos que $I = M$, entonces $\mathcal{O}_K M = M = PM$, y por la ley de cancelación, tendríamos $\mathcal{O}_K = P$, lo que contradice la primalidad de P. Como I contiene estrictamente a M, no puede estar en S por la maximalidad de M, luego se puede escribir como producto de ideales primos. Pero entonces, $M = PI$ un producto de ideales primos, lo que es una contradicción.

Ahora veamos la unicidad: supongamos que $P_1 \dots P_r = Q_1 \dots Q_s$ con P_i, Q_i ideales primos no necesariamente iguales. Entonces, $P_1 \supseteq Q_1 \dots Q_s$ por la proposición 1.39, de donde deducimos que $P_1 \supseteq Q_i$ para algún i, siguiendo el mismo razonamiento de la prueba del lema 1.34.

Podemos suponer que $i = 1$, pues basta reordenar el producto. Así, $Q_1 \subseteq P_1$, y como son ideales primos en un dominio de Dedekind, también son maximales, y debe

ser $P_1 = Q_1$. Usando la ley de cancelación, tenemos $Q_2 \dots Q_s = P_2 \dots P_r$. Basta repetir este proceso, y llegamos a que $r = s$ y $P_i = Q_i$ para todo i, luego la factorización es única. ∎

Proposición 1.41. Un dominio de Dedekind $\mathcal{O}_K$ es un dominio de factorización única si y sólo si es un dominio de ideales principales.

Demostración. Primero, sabemos que todo dominio de ideales principales es un dominio de factorización única. Recíprocamente, sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$. Como $\mathcal{O}_K$ es noetheriano, $\mathfrak{p} = (a_1, \dots, a_n)$. Ahora, $\mathcal{O}_K$ es un dominio de factorización única, así que tiene sentido el máximo común divisor. Sea $d = \gcd(a_1, \dots, a_n)$, entonces $\mathfrak{p} = (a_1, \dots, a_n) = (d)$, pues $\mathfrak{p} \subseteq (d)$, y como $\mathcal{O}_K$ es dominio de Dedekind, $\mathfrak{p}$ es maximal. Hemos probado que todo ideal primo es principal en $\mathcal{O}_K$, si es un dominio de factorización única.

Ahora, sea I un ideal de $\mathcal{O}_K$. Por el teorema 1.40, $I = \mathfrak{p}_1 \dots \mathfrak{p}_r$ con $\mathfrak{p}_i$ ideales primos de $\mathcal{O}_K$. Pero todos estos ideales son principales, así que I es un producto de ideales principales, es decir, I es principal. ∎

Observación 1.42. En la observación 1.30 vimos que al extender la noción de número entero a los enteros algebraicos de un cuerpo de números, podíamos perder la unicidad de la factorización en irreducibles. El teorema que acabamos de demostrar es precisamente esto: aunque la factorización no sea única en los elementos de $\mathcal{O}_K$, sí que lo es en sus ideales. Si volvemos al caso de $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, se tienen las siguientes factorizaciones de ideales:

$$
\begin{aligned}
(2) &= \left(2, 1+\sqrt{-5}\right)^2 \\
(3) &= \left(3, 1+\sqrt{-5}\right)\left(3, 2+\sqrt{-5}\right) \\
\left(1+\sqrt{-5}\right) &= \left(2, 1+\sqrt{-5}\right)\left(3, 1+\sqrt{-5}\right) \\
\left(1-\sqrt{-5}\right) &= \left(3, 1+\sqrt{-5}\right)\left(3, 2+\sqrt{-5}\right)
\end{aligned}
$$

Observamos que, ya que $\mathcal{O}_K$ no es dominio de factorización única, las nociones de primo e irreducible no son equivalentes.

Un resultado que nos va a resultar muy útil es el conocido teorema chino del resto:

Teorema 1.43 (Teorema chino del resto). *Sean $\mathfrak{a}_1, \dots \mathfrak{a}_n$ ideales en un anillo A comaximales, es decir, que $\mathfrak{a}_i + \mathfrak{a}_j = A$ si $i \neq j$. Supongamos que $\mathfrak{a} = \cap_{i=1}^n \mathfrak{a}_i$. Entonces:*

$$A/\mathfrak{a} \cong \bigoplus_{i=1}^{n} A/\mathfrak{a}_i.$$

Resulta que cuando dos ideales son comaximales, su intersección y su producto coincide. Si un ideal $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$, el teorema chino del resto nos permite escribir el cociente $A/\mathfrak{a} \cong \bigoplus_{i=1}^n A/\mathfrak{p}_i^{e_i}$. Veamos la potencia de este resultado para demostrar propiedades relevantes sobre este concepto que vamos a introducir:

Definición 1.44. *Sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$. Definimos la **norma** de $\mathfrak{a}$ como el índice de $\mathfrak{a}$ en $\mathcal{O}_K$, es decir,*

$$\mathfrak{N}(\mathfrak{a}) := \left[\mathcal{O}_K : \mathfrak{a}\right] = |\mathcal{O}_K/\mathfrak{a}|.$$

Observación 1.45. Recordemos que, por la proposición 1.25, el cociente $\mathcal{O}_K/\mathfrak{a}$ es finito.

Una propiedad esperable de la norma de un ideal es que la norma de un producto de ideales sea el producto de sus normas.

Proposición 1.46. Si $\mathfrak{a}, \mathfrak{b}$ son ideales de $\mathcal{O}_K$, entonces $\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$.

Demostración. Si $\mathfrak{a}$ y $\mathfrak{b}$ son relativamente primos, es muy sencillo pues:

$$\mathcal{O}_K/\mathfrak{ab} \cong \mathcal{O}_K/\mathfrak{a} \times \mathcal{O}_K/\mathfrak{b},$$

y basta tomar norma. Por tanto, es suficiente demostrar que $\mathfrak{N}(\mathfrak{p}^m) = \mathfrak{N}(\mathfrak{p})^m$, para $\mathfrak{p}$ un primo no nulo.

Tenemos una cadena de ideales $\mathcal{O}_K \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \dots \supseteq \mathfrak{p}^m$. Podemos usar el tercer teorema de isomorfía para $\mathcal{O}_K-$módulos: $\mathfrak{p}^m \subseteq \mathfrak{p}^{m-1} \subseteq \mathcal{O}_K$, luego:

$$\frac{\mathcal{O}_K/\mathfrak{p}^m}{\mathfrak{p}^{m-1}/\mathfrak{p}^m} \cong \mathcal{O}_K/\mathfrak{p}^{m-1},$$

y comparando el número de elementos:

$$\frac{\mathfrak{N}(\mathfrak{p}^m)}{|\mathfrak{p}^{m-1}/\mathfrak{p}^m|} = \mathfrak{N}(\mathfrak{p}^m).$$

Mediante un proceso inductivo llegamos a que

$$\mathfrak{N}(\mathfrak{p}^m) = |\mathcal{O}_K/\mathfrak{p}| \cdot |\mathfrak{p}/\mathfrak{p}^2| \dots |\mathfrak{p}^{m-1}/\mathfrak{p}^m|.$$

Nos gustaría saber qué valores tienen los índices $|\mathfrak{p}^k/\mathfrak{p}^{k+1}|$. De hecho, veremos algo mejor algo mejor: $\mathcal{O}_K/\mathfrak{p}$ y $\mathfrak{p}^k/\mathfrak{p}^{k+1}$ son isomorfos como $\mathcal{O}_K-$módulos para cada k. Para ver esto, sea $\alpha \in \mathfrak{p}^k - \mathfrak{p}^{k+1}$ y el siguiente homomorfismo:

$$\begin{aligned} \mathcal{O}_K &\to \mathfrak{p}^k/\mathfrak{p}^{k+1} \\ x &\mapsto \alpha x + \mathfrak{p}^{k+1} \end{aligned}$$

Su núcleo es $\mathfrak{p}$, pues si tomamos $x \in \mathfrak{p}$, entonces $\alpha x \in \mathfrak{p}^{k+1}$, y como $\mathfrak{p}$ es primo, es maximal, y coincide con el núcleo. Además, es sobreyectivo, pues $\mathfrak{p}^k = \mathfrak{p}^{k+1} + \alpha\mathcal{O}_K$. Esto último es gracias a la factorización única. Es claro que $\mathfrak{p}^{k+1} \subsetneq \mathfrak{p}^{k+1} + \alpha\mathcal{O}_K \subseteq \mathfrak{p}^k$, y si hubiera un ideal $\mathfrak{p}^{k+1} \subsetneq \mathfrak{b} \subseteq \mathfrak{p}^k$, sabemos que tiene que ser divisor de $\mathfrak{p}^{k+1}$, luego $\mathfrak{b} = \mathfrak{p}^k$. Entonces, como cada elemento de $\mathfrak{p}^k$ es la suma de un elemento de $\mathfrak{p}^{k+1}$ y un múltiplo de α, al reducir módulo $\mathfrak{p}^{k+1}$ tenemos que los elementos del cociente son precisamente múltiplos de α. Esto demuestra que es sobreyectiva.

Por el primer teorema de isomorfía se deduce que $\mathcal{O}_K/\mathfrak{p}$ y $\mathfrak{p}^k/\mathfrak{p}^{k+1}$ son isomorfos, y esto concluye la prueba. ∎

Por último vamos a relacionar la norma de un elemento $\alpha \in \mathcal{O}_K$ con la norma del ideal que genera. Precisamente este resultado justifica el nombre que le hemos puesto a la norma de un ideal. Merece la pena destacar que $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$, así que esto tiene sentido. Antes usaremos un lema:

Lema 1.47. Sea $\mathfrak{a}$ un ideal no nulo de $\mathcal{O}_K$, $\{y_1, \dots, y_n\}$ una base de $\mathfrak{a}$ como grupo libre abeliano, y δ_K el discriminante de K. Entonces:

$$\mathfrak{N}(\mathfrak{a})^2 = \frac{\Delta(y_1, \dots, y_n)}{\delta_K}.$$

Demostración. Por la observación 1.23, existen una base entera $x_1, \dots, x_n$ de $\mathcal{O}_K$ y enteros $f_1, \dots, f_n$ tales que $x_1 f_1, \dots, x_n f_n$ es base de $\mathfrak{a}$. Es decir, podemos escribir $\mathcal{O}_K = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n$ y $\mathfrak{a} = \mathbb{Z}x_1 f_1 \oplus \cdots \oplus \mathbb{Z}x_n f_n$. Resulta que $\mathcal{O}_K/\mathfrak{a} \cong \prod \mathbb{Z}/\mathbb{Z}f_i$, mediante el isomorfismo inducido por

$$\begin{aligned} \mathcal{O}_K &\to \prod \mathbb{Z}/\mathbb{Z}f_i \\ \sum a_i x_i &\mapsto (a_i \mod f_i)_{1\le i\le n}, \end{aligned}$$

cuyo núcleo es $\mathfrak{a}$ y es sobreyectivo. Entonces, $\mathfrak{N}(\mathfrak{a}) = \prod_{i=1}^n f_i$. Usando la proposición 1.7 y dándonos cuenta de que $\prod_{i=1}^n f_i$ es el determinante de la matriz diagonal con entradas f_i, tenemos:

$$\Delta(f_1 x_1, \dots f_n x_n) = \left(\prod_{i=1}^n f_i\right)^2 \cdot \delta_K.$$

Como los discriminantes de dos bases enteras de $\mathfrak{a}$ son iguales, tenemos

$$\Delta(y_1, \dots y_n) = \mathfrak{N}(\mathfrak{a})^2 \cdot \delta_K \Rightarrow \mathfrak{N}(\mathfrak{a})^2 = \frac{\Delta(y_1, \dots, y_n)}{\delta_K}.$$

Proposición 1.48. Sea $\alpha \in \mathcal{O}_K$ no nulo. Entonces, $\mathfrak{N}(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|$.

Demostración. Sea $\{x_1, \dots x_n\}$ una base entera de $\mathcal{O}_K$. Entonces, $\{\alpha x_1, \dots \alpha x_n\}$ es una base de $\alpha\mathcal{O}_K$, y por el lema anterior:

$$\mathfrak{N}(\alpha\mathcal{O}_K)^2 = \frac{\Delta(\alpha x_1, \dots, \alpha x_n)}{\delta_K}.$$

Ahora, sean $\sigma_1, \dots, \sigma_n$ las inmersiones de K en una clausura algebraica de $\mathbb{Q}$. Operando y usando las propiedades del discriminante:

$$\begin{aligned}\Delta(\alpha x_1 \dots, \alpha x_n) &= \det\left(\sigma_i(\alpha x_j)\right)^2 \\ &= \det\left(\sigma_i(\alpha\delta_{ij})\right)^2 \cdot \det\left(\sigma_i x_j\right)^2 \\ &= N_{K/\mathbb{Q}}(\alpha)^2 \cdot \delta_K.\end{aligned}$$

Como $\mathfrak{N}(\alpha\mathcal{O}_K) > 0$, tomando raíz cuadrada tenemos $\mathfrak{N}(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|$.

1.3 Ramificación de primos

En esta sección vamos a estudiar en mayor profundidad un fenómeno bien conocido. Comenzaremos con un ejemplo para ponernos en situación. Si consideramos la extensión $\mathbb{Z} \subseteq \mathbb{Z}[i]$, sabemos que hay algunos números primos en $\mathbb{Z}$ que dejan de ser irreducibles en $\mathbb{Z}[i]$. De hecho, tenemos una caracterización: el 2 y todos los primos congruentes con 1 módulo 4. Además, esto permite escribir tales números primos como $p = x^2 + y^2$, lo que resuelve nuestra pregunta para el caso $n = 1$. A lo largo de esta sección, por "primo de $\mathcal{O}_K$" nos referimos a "ideal primo no nulo", siguiendo el paralelismo con $\mathbb{Z}$.

En general, vamos a estudiar cómo se comportan los ideales primos (no nulos) de $\mathbb{Z}$ cuando los vemos en el anillo de enteros $\mathcal{O}_K$ de un cuerpo de números K. Si tomamos un ideal primo $(p) = p\mathbb{Z}$ de $\mathbb{Z}$, su ideal extendido en $\mathcal{O}_K$ tendrá una factorización en ideales primos de $\mathcal{O}_K$:

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}.$$

A los exponentes e_i los llamamos **índice de ramificación** de $\mathfrak{p}_i$ en p. Se denota con $e\left(\mathfrak{p}_i \mid p\right)$.

Si un primo $\mathfrak{p}$ de $\mathcal{O}_K$ divide a $p\mathcal{O}_K$, diremos que $\mathfrak{p}$ está sobre de p, o que p está debajo de $\mathfrak{p}$. No es difícil ver que $\mathfrak{p}$ esté sobre p es equivalente a que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Observamos que cada primo $\mathfrak{p}$ de $\mathcal{O}_K$ está sobre al menos un primo $p \in \mathbb{Z}$, porque la contracción de ideales preserva primalidad. Además debe de ser único, pues de contener a dos primos $p, q \in \mathbb{Z}$, contendría a 1 y $\mathfrak{p}$ no sería primo.

Hay otro número que se le puede asociar a los ideales de $\mathcal{O}_K$ que dividen a p. Podemos ver el cuerpo $\mathbb{Z}/p\mathbb{Z}$ como un subcuerpo de $\mathcal{O}_K/\mathfrak{p}_i$. Si el grado de la extensión de cuerpos es f_i (es decir, $\mathcal{O}_K/\mathfrak{p}_i$ es **el** cuerpo finito con p^{f_i} elementos), al número f_i lo llamamos **grado de inercia** de $\mathfrak{p}_i$ sobre p, y se denota con $f\left(\mathfrak{p}_i \mid p\right)$. El siguiente teorema nos da una relación muy importante entre estos dos números y el grado de la extensión.

Teorema 1.49. *Sea $n = [K : \mathbb{Q}]$ y sea $p \in \mathbb{Z}$ primo cuya factorización en $\mathcal{O}_K$ es $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$, y donde los correspondientes grados de inercia e índices de ramificación son, respectivamente $e_1 \dots e_r$ y $f_1 \dots f_r$. Entonces:*

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

Demostración. Sabemos que $p\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$. Por la propiedad del producto de las normas tenemos:

$$\mathfrak{N}\left(p\mathcal{O}_K\right) = \prod_{i=1}^{r} \mathfrak{N}\left(\mathfrak{p}_i\right)^{e_i} = \prod_{i=1}^{r} \left(p^{f_i}\right)^{e_i}.$$

Por otro lado, en la proposición 1.25 vimos que el cardinal de $\mathcal{O}_K/p\mathcal{O}_K$ era p^n, pero esto por definición es $\mathfrak{N}\left(p\mathcal{O}_K\right)$. Igualando exponentes llegamos a $\sum_{i=1}^{r} e_i f_i = n$, como queríamos ver. ∎

Si la extensión $K/\mathbb{Q}$ es de Galois, podemos fortalecer el teorema anterior. Si $\mathfrak{a}$ es un ideal y $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, denotamos $\sigma\mathfrak{a} = \{\sigma a : a \in \mathfrak{a}\}$, y es un ideal. Además, es fácil ver que $\sigma\mathcal{O}_K = \mathcal{O}_K$, y si $\mathfrak{p}$ es un ideal primo, como σ induce un isomorfismo $\mathcal{O}_K/\sigma\mathfrak{p} = \sigma\mathcal{O}_K/\sigma\mathfrak{p} \cong \mathcal{O}_K/\mathfrak{p}$, se deduce que $\sigma\mathfrak{p}$ sigue siendo un ideal primo.

Proposición 1.50. Sea $(p) = p\mathbb{Z}$ un ideal primo, y supongamos que $\mathfrak{p}_i$ y $\mathfrak{p}_j$ son ideales primos de $\mathcal{O}_K$ que dividen a $\mathfrak{p}$. Entonces, existe $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ tal que $\sigma\mathfrak{p}_i = \mathfrak{p}_j$.

Demostración. Supongamos que hay un ideal primo $\mathfrak{p}_j$ que contiene a $p\mathcal{O}_K$ pero que no está en el conjunto $\{\sigma\mathfrak{p}_i : \sigma \in \mathrm{Gal}(K/\mathbb{Q})\}$. Por el teorema chino del resto, existe un $\alpha \in \mathcal{O}_K$ tal que $\alpha \equiv 0 \mod \mathfrak{p}_j$ y $\alpha \equiv 1 \mod \sigma\mathfrak{p}_i$ para todo $\sigma \in G = \mathrm{Gal}(K/\mathbb{Q})$.

Entonces, $N(\alpha) = \prod_{\sigma\in G} \sigma\alpha \in \mathfrak{p}_j \cap \mathbb{Z} = (p)$, porque $id(\alpha) = \alpha \in \mathfrak{p}_j$, y como $\alpha \in \mathcal{O}_K$, su norma es un número entero. Además, también se sigue que $N(\alpha) \in \mathfrak{p}_i$, y como $\mathfrak{p}_i$ es primo, $\sigma\alpha \in \mathfrak{p}_i$ para algún $\sigma \in G$, es decir, $\alpha \in \sigma^{-1}\mathfrak{p}_i$, pero no puede ocurrir porque $\alpha \equiv 1 \mod \sigma^{-1}\mathfrak{p}_i$, y hemos llegado a una contradicción.

Ahora vamos a probar la mejora del teorema 1.49 en el caso en que la extensióm $K/\mathbb{Q}$ es de Galois.

Teorema 1.51. *Supongamos que $K/\mathbb{Q}$ es Galois y de grado n, y sea $p \in \mathbb{Z}$ un primo, cuya factorización en $\mathcal{O}_K$ es $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$. Entonces $e_1 = e_2 = \cdots = e_r$ y $f_1 = f_2 = \cdots = f_r$. Si denotamos e y f a esos valores, entonces $efr = n$.*

Demostración. Para un índice i, existe $\sigma \in G = \mathrm{Gal}(K/\mathbb{Q})$ tal que $\sigma\mathfrak{p}_1 = \mathfrak{p}_i$. Ahora, como σ induce un isomorfismo $\mathcal{O}_K/\mathfrak{p}_1 \cong \mathcal{O}_K/\sigma\mathfrak{p}_1 = \mathcal{O}_K/\mathfrak{p}_i$, los grados de inercia f_i son todos iguales.

Ahora aplicamos σ en ambos lados de la igualdad $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}\mathfrak{p}_r^{e_r}$. Desde luego, $\sigma p\mathcal{O}_K = p\mathcal{O}_K$. Tenemos la siguiente igualdad:

$$\left(\sigma\mathfrak{p}_1\right)^{e_1} \dots \left(\sigma\mathfrak{p}_r\right)^{e_r} = p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}.$$

Por un lado, el exponente de $\sigma\mathfrak{p}_1$ es e_1, y por otro lado es e_i, pues $\sigma\mathfrak{p}_1 = \mathfrak{p}_i$. Por la unicidad de la factorización en ideales primos, debemos tener $e_i = e_1$, y se sigue que todos los índices de ramificación e_i son iguales.

Por último, como $\sum_{i=1}^{r} e_i f_i = n$, tenemos que $efr = n$, como queríamos.

Definición 1.52. *Dado un cuerpo de números $K/\mathbb{Q}$, decimos que un primo $p \in \mathbb{Z}$* ***ramifica*** *si $e_i > 1$ para algún i y que no ramifica si $e_i = 1$ para todo i. Si p satisface $e_i = f_i = 1$ para todo i, diremos que p se* ***descompone completamente*** *en $\mathcal{O}_K$. Si $r = 1$ y $e = 1$ (y por tanto $f = n$), $p\mathcal{O}_K$ es un ideal primo, y p se dice* ***inerte****.*

Cabe destacar que si $p \in \mathbb{Z}$ es un primo que se descompone completamente, entonces no ramifica y además se descompone como un producto de $n = [K : \mathbb{Q}]$ primos distintos en $\mathcal{O}_K$.

Ahora vamos a ver una herramienta muy potente para obtener la factorización de un primo $p \in \mathbb{Z}$ en $\mathcal{O}_K$. Recordemos la notación: K es un cuerpo de números con grado $[K : \mathbb{Q}] = n$, y anillo de enteros $\mathcal{O}_K$. Sea $\alpha \in \mathcal{O}_K$ un elemento primitivo de $K/\mathbb{Q}$, es decir, $K = \mathbb{Q}[\alpha]$. Un detalle que hay que tener en cuenta es que en general no es cierto que $\mathcal{O}_K = \mathbb{Z}[\alpha]$[2]. Lo que sí ocurre es que $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$ como subgrupos

aditivos, y el índice $|\mathcal{O}_K : \mathbb{Z}[\alpha]|$ es finito, al ser ambos grupos abelianos libres del mismo rango.

Veremos que, para todos los primos $p \in \mathbb{Z}$ salvo una cantidad finita, la factorización de $p\mathbb{Z}$ en $\mathcal{O}_K$ se puede determinar simplemente reduciendo módulo p un cierto polinomio. Esto será posible si p no divide al índice $|\mathcal{O}_K : \mathbb{Z}[\alpha]|$. Además, si se verifica que $\mathcal{O}_K = \mathbb{Z}[\alpha]$, nos valdrá para todos.

Vamos a fijar la siguiente notación: Sea $p \in \mathbb{Z}$, y sea $h \in \mathbb{Z}[x]$ un polinomio. Denotaremos con $\bar{h}$ al polinomio en $\mathbb{Z}/p\mathbb{Z}$ que se obtiene reduciendo los coeficientes de h módulo p.

Sea g el polinomio mínimo de α sobre $\mathbb{Q}$ que es mónico, y cuyos coeficientes son enteros. Por tanto, podemos considerar $\bar{g} \in \mathbb{Z}/p\mathbb{Z}[x]$. Su factorización será de la forma:

$$\bar{g} = \bar{g}_1^{e_1} \bar{g}_2^{e_2} \dots \bar{g}_r^{e_r}.$$

Teorema 1.53. *Con las notaciones anteriores, supongamos además que p no divide al índice $|\mathcal{O}_K : \mathbb{Z}[\alpha]|$. Entonces, la factorización de $p\mathbb{Z}$ en $\mathcal{O}_K$ es:*

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

donde $\mathfrak{p}_i$ es el ideal $\big(p, g_i(\alpha)\big)$ en $\mathcal{O}_K$, es decir, $\mathfrak{p}_i = p\mathcal{O}_K + (g_i(\alpha))$. Además, $f\left(\mathfrak{p}_i \mid p\right)$ es el grado de $\bar{g}_i$.

Demostración. Sea f_i el grado de cada polinomio g_i (y también de $\bar{g}_i$, pues g es mónico). Probaremos lo siguiente:

1. Para cada i, o bien $\mathfrak{p}_i = \mathcal{O}_K$, o bien $\mathcal{O}_K/\mathfrak{p}_i$ es un cuerpo de $|\mathbb{Z}/p\mathbb{Z}|^{f_i} = p^{f_i}$ elementos.
2. $\mathfrak{p}_i + \mathfrak{p}_j = \mathcal{O}_K$ si $i \neq j$.
3. $p\mathcal{O}_K \mid \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$.

Veremos primero, suponiendo ciertos estos resultados, cómo se deduce de ellos el teorema. Digamos que $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ son los ideales de la lista que no son $\mathcal{O}_K$ y que $\mathfrak{p}_{s+1}, \dots, \mathfrak{p}_r = \mathcal{O}_K$. Al final veremos que $r = s$. $\mathfrak{p}_1, \dots \mathfrak{p}_s$ son ideales primos de $\mathcal{O}_p$ y están sobre p, porque lo contienen. Con esto, tenemos que $f\left(\mathfrak{p}_i \mid p\right) = f_i$ para $i \leq s$

[2] De hecho, en la siguiente sección veremos un ejemplo para extesiones cuadráticas en el que no son iguales.

por el apartado (1). Por el segundo apartado sabemos que son todos distintos, y el tercero se reduce a $p\mathcal{O}_K \mid \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_s^{e_s}$. Por tanto, la factorización de p será $p\mathcal{O}_K = \mathfrak{p}_1^{d_1} \dots \mathfrak{p}_r^{d_r}$ con $d_i \leq e_i$ para $i = 1, \dots, s$.

Por el teorema 1.49 sabemos que $n = d_1 f_1 + \cdots + d_s f_s$. Por otro lado, n es el grado de g, así que $n = e_1 f_1 + \cdots + e_r f_r$. De aquí se sigue que $s = r$ y que $d_i = e_i$ y habríamos terminado. Falta probar (1), (2) y (3).

Prueba de (1): Un cuerpo con cardinal p^{f_i} es, por el teorema de clasificación de cuerpos finitos:

$$\mathbb{F}_i = \left(\mathbb{Z}/p\mathbb{Z}\right)[x] \Big/ \left(\bar{g}_i\right).$$

Vamos a relacionar $\mathcal{O}_K/\mathfrak{p}_i$ y $\mathbb{F}_i$ apoyándonos en $\mathbb{Z}[x]$ y en el primer teorema de isomorfía. Primero, definimos el homomorfismo natural $\mathbb{Z}[x] \to \mathbb{F}_i$, primero reduciendo los coeficientes módulo p y luego reduciendo módulo el ideal $\left(\bar{g}_i\right)$. Este homomorfismo es claramente sobreyectivo y además su núcleo es el ideal generado por p (su extensión en el anillo de polinomios) y $\left(g_i\right)$. Entonces, $\mathbb{Z}[x]/\left(p, g_i\right) \cong \mathbb{F}_i$.

Ahora consideramos el homomorfismo $\mathbb{Z}[x] \to \mathcal{O}_K$ definido por la sustitución $x \mapsto \alpha$. Componiendo con la proyección al cociente por $\mathfrak{p}_i$ tenemos el siguiente homomorfismo:

$$\begin{aligned} \mathbb{Z}[x] &\to \mathcal{O}_K/\mathfrak{p}_i \\ f(x) &\mapsto f(\alpha) + \mathfrak{p}_i. \end{aligned}$$

Es claro que el ideal $\left(p, g_i\right)$ está contenido en su núcleo. Ahora, como $\mathbb{Z}[x]/\left(p, g_i\right)$ es un cuerpo, dicho ideal es maximal, así que o bien coincide con el núcleo, o bien el núcleo es todo $\mathbb{Z}[x]$.

Más aún, el homomorfismo es sobreyectivo. Para ello veremos que $\mathcal{O}_K \subseteq \mathbb{Z}[\alpha] + \mathfrak{p}_i$. De hecho, vamos a probar que $\mathcal{O}_K = \mathbb{Z}[\alpha] + p\mathcal{O}_K$. Primero, $p \in \mathfrak{p}_i$, luego $p\mathcal{O}_K \subseteq \mathfrak{p}_i$. El índice de $\mathbb{Z}[\alpha] + p\mathcal{O}_K$ en $\mathcal{O}_K$ es divisor común de los índices de $\mathbb{Z}[\alpha]$ y $p\mathcal{O}_K$ en $\mathcal{O}_K$, pero $p \nmid |\mathcal{O}_K/\mathbb{Z}[\alpha]|$, y $|\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]|$ es una potencia de p, así que necesariamente dicho índice debe ser 1. Así, $\mathcal{O}_K = \mathbb{Z}[\alpha] + p\mathcal{O}_K$ y el homomorfismo es sobreyectivo.

Recordando las dos posibilidades que teníamos para su núcleo, si es $\mathbb{Z}[x]$, el cociente es el anillo nulo, así que $\mathfrak{p}_i = \mathcal{O}_K$, y si es el ideal $\left(p, g_i\right)$, entonces $\mathcal{O}_K/\mathfrak{p}_i \cong \mathbb{F}_i$, un cuerpo con p^{f_i} elementos, y hemos terminado la prueba de (1).

Prueba de (2): Los $\bar{g}_i$ son polinomios mónicos, distintos e irreducibles en el dominio de ideales principales $\left(\mathbb{Z}/p\mathbb{Z}\right)[x]$, así que por la identidad de Bézout, para $i \neq j$

existen polinomios $h, k \in \mathbb{Z}[x]$ tales que

$$\bar{g}_i\bar{h} + \bar{g}_j\bar{k} = \bar{1}, \text{ es decir,}$$
$$g_i h + g_j k \equiv 1 \mod p.$$

En la segunda ecuación estamos tomando módulo el ideal generado por p extendido en $\mathbb{Z}[x]$. Ahora, cambiando x por α, tenemos:

$$g_i(\alpha)h(\alpha) + g_j(\alpha)k(\alpha) \equiv 1 \mod p\mathcal{O}_K,$$

y de aquí se sigue que $1 \in \big(p, g_i(\alpha), g_j(\alpha)\big) = \mathfrak{p}_i + \mathfrak{p}_j$, probando (2).

Prueba de (3): Para simplificar notación, llamemos $\gamma_i = g_i(\alpha)$, y así, $\mathfrak{p}_i = \big(p, \gamma_i\big)$. Es fácil ver que el producto $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ está contenido en el ideal $\big(p, \gamma_1^{e_1} \dots \gamma_r^{e_r}\big)$, y por tanto es divisible por él. Resulta que este último ideal es igual a $p\mathcal{O}_K$. Para verlo, basta probar que $\gamma_1^{e_1} \dots \gamma_r^{e_r} \in p\mathcal{O}_K$.

Sabemos que $\bar{g} = \bar{g}_1^{e_1}\bar{g}_2^{e_2} \dots \bar{g}_r^{e_r}$, luego

$$g_1^{e_1} g_2^{e_2} \dots g_r^{e_r} \equiv g \mod p,$$

con p el ideal extendido en $\mathbb{Z}[x]$. Como antes, sustituyendo x por α, tenemos:

$$\gamma_1^{e_1} \dots \gamma_r^{e_r} \equiv 0 \mod p\mathcal{O}_K,$$

luego $\gamma_1^{e_1} \dots \gamma_r^{e_r} \in p\mathcal{O}_K$ y habríamos terminado la prueba de (3), y del teorema. ∎

Ejemplo 1.54. Veamos cómo hemos obtenido las factorizaciones de los ideales en la observación 1.42, por ejemplo la del ideal (2). Más adelante veremos que el anillo de enteros de $\mathbb{Q}[\sqrt{-5}]$ es $\mathbb{Z}[\sqrt{-5}]$. El polinomio mínimo de $\sqrt{-5}$ sobre $\mathbb{Q}$ es $x^2 + 5$, así que en virtud del teorema anterior, debemos estudiar su factorización módulo 2.

$$x^2 + 5 \equiv x^2 + 1 \equiv (x+1)^2 \mod 2.$$

Entonces 2 ramifica en $\mathbb{Q}[\sqrt{-5}]$ y su factorización es, por la segunda parte del teorema anterior:

$$2\mathcal{O}_K = \left(2, 1 + \sqrt{-5}\right)^2.$$

1.4 El grupo de clases de ideales.

Recordemos que en un cuerpo de números K con anillo de enteros $\mathcal{O}_K$, las clases de equivalencia por la relación definida en la definición 1.35 forman un grupo, que

habíamos llamado grupo de clases de ideales. El objetivo de esta sección es probar que ese grupo es finito, y su orden nos permitirá definir un invariante de los cuerpos de números: el número de clase. Comencemos por algunas consideraciones previas.

Proposición 1.55. Sea K un cuerpo de números y $\mathcal{O}_K$ su anillo de enteros. Existe un número real positivo λ_K[3], dependiente exclusivamente de K, tal que cada ideal no nulo $\mathfrak{a}$ de $\mathcal{O}_K$ contiene un elemento α verificando

$$|N_{\mathbb{Q}}^K(\alpha)| \leq \lambda_K \|\mathfrak{a}\|.$$

Demostración. Sea $\alpha_1, \dots, \alpha_n$ una base entera de $\mathcal{O}_K$ y sean $\sigma_1, \dots, \sigma_n$ las inmersiones de K en $\mathbb{C}$. Afirmamos que se puede tomar

$$\lambda_K = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i \alpha_j|.$$

En efecto, para un ideal I, sea m el único entero tal que $m^n \leq \|I\| < (m+1)^n$. Sean $\sum_{j=1}^{n} m_j \alpha_j$ con $0 \leq m_j \leq m$, que son $(m+1)^n$ elementos de $\mathcal{O}_K$. Por tanto, al menos dos de ellos deben ser congruentes módulo I, pues hay más que $\|I\|$. Tomemos dos, y consideremos su resta $\alpha = \sum m_j \alpha_j \in I$, con $|m_j| \leq m$. Ahora:

$$|N_{\mathbb{Q}}^K(\alpha)| = \prod_{i=1}^{n} |\sigma_i \alpha| \leq \prod_{i=1}^{n} \sum_{j=1}^{n} m_j |\sigma_i \alpha_j| \leq m^n \lambda \leq \|I\| \lambda.$$

Corolario 1.56. Cada clase de ideales de $\mathcal{O}_K$ contiene un ideal J cumpliendo $\|J\| \leq \lambda_K$.

Demostración. Tomemos una clase de ideales C y su inversa C^{-1}. Ahora, sea $I \in C^{-1}$, y $\alpha \in I$ que verifique la cota de la proposición anterior. El ideal (α) está contenido en I, y por tanto es divisible por I, es decir $(\alpha) = IJ$. Pero necesariamente $J \in C$. Veamos que este ideal cumple el enunciado:

Operando con la norma de α, tenemos $|N_{\mathbb{Q}}^K(\alpha)| = \|(\alpha)\| = \|I\| \cdot \|J\|$. Como $|N_{\mathbb{Q}}^K(\alpha)| \leq \lambda_K \|I\|$, se deduce que $\|J\| \leq \lambda_K$, como queríamos.

[3] En algunos textos se da un valor explícito de esta cota. Si $\sigma_1, \overline{\sigma_1}, \dots, \sigma_s, \overline{\sigma_s}$ son las inmersiones de K en $\mathbb{C}$, se puede tomar $\lambda_K = \left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|}$, donde δ_K es el discriminante de K. Para más información, se puede consultar [Neu13, págs. 35-36].

Corolario 1.57. Hay un número finito de clases de ideales en $\mathcal{O}_K$

Demostración. Dado un primo $p \in \mathbb{Z}$, sólo puede haber una cantidad finita de ideales primos $\mathfrak{p} \subseteq \mathcal{O}_K$ sobre él, pues esto es equivalente a $\mathfrak{p} \mid p$. Entonces, dada una constante M, sólo puede haber una cantidad finita de ideales primos con norma acotada por M: los ideales primos de $\mathcal{O}_K$ que dividen a los primos menores o iguales que M. Más aún, sólo hay una cantidad finita de ideales $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ con norma acotada por M, pues $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{e_1} \dots \mathfrak{N}(\mathfrak{p}_r)^{e_r}$, y sabemos que se cumple para ideales primos. Basta tomar la constante $M = \lambda_K$, y sólo puede haber un número finito de clases de ideales, pues por el corolario anterior, cada clase contiene un ideal con norma acotada por λ_K.

Con este resultado podemos definir el siguiente invariante algebraico:

Definición 1.58. *El número de clases de ideales de un cuerpo de números K se llama* ***número de clase*** *de K, y lo denotaremos h_K.*

Observación 1.59. El hecho de que sólo haya un número finito de clases de ideales resulta tranquilizador en cierto modo. Pasar de estudiar números a estudiar ideales no nos ha hecho entrar en un nuevo territorio infinito.

2 | Extensiones cuadráticas

Para fijar ideas, vamos a aplicar la teoría que acabamos de desarrollar a las extensiones cuadráticas. Sabemos que las extensiones cuadráticas son de la forma $K = \mathbb{Q}[\sqrt{N}]$ con $N \neq 0, 1$ entero libre de cuadrados. Siempre son extensiones de Galois, y su grupo de Galois está formado por id y $\sigma : \sqrt{d} \mapsto -\sqrt{d}$. Un elemento $\alpha \in K$ es de la forma $\alpha = a + b\sqrt{d}$ con $a, b \in \mathbb{Q}$. Conociendo el grupo de Galois podemos calcular la traza y la norma:

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

Además, el polinomio mínimo de α es $p_\alpha(x) = x^2 - t(\alpha)x + N(\alpha)$. Queremos caracterizar el anillo de enteros de K. Recordemos que la traza y la norma de enteros algebraicos es un número entero, por lo que $\alpha \in \mathcal{O}_K$ si y sólo si $t(\alpha), N(\alpha) \in \mathbb{Z}$. Si $\alpha = a + b\sqrt{d}$ tenemos:

$$\alpha = a + b\sqrt{d} \in \mathcal{O}_K \iff 2a, a^2 - db^2 \in \mathbb{Z}.$$

Vamos a mejorar el lado de la derecha. Resulta que:

$$2a, a^2 - db^2 \in \mathbb{Z} \iff 2a = u \in \mathbb{Z}, 2b = v \in \mathbb{Z} \text{ y } u^2 - dv^2 \equiv 0 \mod 4.$$

En efecto, si $\alpha \in \mathcal{O}_K$ su traza ($u = 2a$) y su norma son enteros y $(2a)^2 - d(2b)^2$ es múltiplo de 4. Como $(2a)^2$ es entero, también lo es $(2b)^2 d$, pero al ser d libre de cuadrados, debe ser $v = 2b \in \mathbb{Z}$.
Recíprocamente, sabemos que $t(\alpha) = 2a \in \mathbb{Z}$. Falta ver que $N(\alpha) = a^2 - db^2 \in \mathbb{Z}$, pero usando que $(2a)^2 - d(2b)^2 = 4(a^2 - db^2) \in 4\mathbb{Z}$, deducimos que $a^2 - db^2 \in \mathbb{Z}$, luego $\alpha \in \mathcal{O}_K$.

Está claro que $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$, pero la otra contención depende de la congruencia de d módulo 4. Observamos que no puede ser $d \equiv 0 \mod 4$ porque d es libre de cuadrados. Analizaremos cada caso por separado:

- Si $d \equiv 2 \mod 4$, sea $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$. Entonces $u^2 - dv^2 \equiv u^2 - 2v^2 \mod 4$, luego $u^2 \equiv 2v^2 \mod 4$, es decir, $u^2 = 2v^2 + 4n = 2(v^2 + 2n)$, un número par. Entonces $u = 2a$ es par, y $a \in \mathbb{Z}$. Falta ver que $b \in \mathbb{Z}$. Sabemos que $a^2 - db^2 \in Z$ y que $a^2 \in \mathbb{Z}$, luego debe ocurrir que $db^2 \in \mathbb{Z}$. Como antes, dado que d es libre de cuadrados, $b \in \mathbb{Z}$. Hemos visto que $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, luego en este caso $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.
- Si $d \equiv 3 \mod 4$, sea $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$. Haciendo cálculos igual que antes llegamos a que $u^2 + v^2 \equiv 0 \mod 4$. Esto sólo se da cuando u y v son ambos pares. Como antes, esto implica que $a, b \in \mathbb{Z}$ y $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.
- Si $d \equiv 1 \mod 4$, sea $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$, llegamos a que $u^2 \equiv v^2 \mod 4$. Esto sólo se cumple si u y v tienen la misma paridad, y entonces $\alpha = \frac{u+v\sqrt{d}}{2}$. Si ambos son pares, $u = 2a$, $v = 2b$ tenemos

$$\frac{u + v\sqrt{d}}{2} = a + b\sqrt{d} = (a - b) \cdot 1 + 2b \cdot \left(\frac{1 + \sqrt{d}}{2}\right).$$

Si son impares, $u - 1, v - 1$ son pares y entonces:

$$\frac{u + v\sqrt{d}}{2} = \frac{1 + \sqrt{d}}{2} + \left(\frac{u - 1}{2} + \frac{v - 1}{2}\sqrt{d}\right).$$

En cualquier caso, los sumandos son combinaciones de 1 y $\frac{1+\sqrt{d}}{2}$ con coeficientes en $\mathbb{Z}$. Hemos probado el siguiente resultado:

Proposición 2.1. Sea $d \neq 0, 1$ un entero libre de cuadrados. El anillo de enteros del cuerpo de números $K = \mathbb{Q}[\sqrt{d}]$ es $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ si $d \equiv 2, 3 \mod 4$ y $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ si $d \equiv 1 \mod 4$.

Naturalmente, una base entera en el primer caso es $\left\{1, \sqrt{d}\right\}$ y $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ en el segundo. Ahora que tenemos una base entera podemos calcular el discriminante. Un simple cálculo nos da:

$$\delta_K = \begin{cases} d & \text{si } d \equiv 1 \mod 4 \\ 4d & \text{si } d \equiv 2, 3 \mod 4 \end{cases}$$

Podemos usar el discriminante para expresar el anillo de enteros de una forma más compacta:

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{\delta_K + \sqrt{\delta_K}}{2}\right].$$

2.1 Reciprocidad cuadrática

Vamos a desviarnos un momento del objetivo principal para ver en profundidad una herramienta que nos servirá más adelante. Queremos estudiar la ecuación:

$$x^2 \equiv a \mod p,\ p \text{ primo.}$$

Nos preguntamos si existe solución, y de qué manera dependen de a y de p. Gauss estudió este problema y desarrolló lo que hoy conocemos como reciprocidad cuadrática, culminando con su conocida ley de reciprocidad cuadrática. Hay muchas pruebas de este resultado, y nosotros daremos una que usará sumas de Gauss y cuerpos de números, y nos servirá como una primera aplicación de la teoría que hemos desarrollado.

Definición 2.2. *Sea p un primo impar. Diremos que $a \in \mathbb{Z}$ es un **residuo cuadrático módulo** p si es congruente a un cuadrado perfecto módulo p, es decir, si existe solución de la ecuación:*

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

Proposición 2.3. Sea $a \in \mathbb{Z}$ no múltiplo de p. Entonces a es un residuo cuadrático módulo p si y sólo si $a^{(p-1)/2} \equiv 1 \mod p$.

Demostración. Supongamos que existe un x_0 tal que $x_0^2 \equiv a \mod p$. Entonces:

$$a^{(p-1)/2} \equiv x_0^{p-1} \equiv 1 \mod p,$$

donde en la última igualdad hemos usado el pequeño teorema de Fermat. Recíprocamente, en particular tenemos que $a \not\equiv 0 \mod p$, así que $a + p\mathbb{Z} \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times = \langle b \rangle$, que sabemos que es un grupo cíclico de orden $p-1$, luego $a \equiv b^k$ con $1 \leq k \leq p-1$. Aplicando la hipótesis tenemos:

$$a^{(p-1)/2} \equiv b^{k(p-1)/2} \equiv 1 \mod p.$$

Ahora bien, b es un generador de $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$, así que su orden es $p-1$ y por tanto $p-1 \mid k(p-1)/2$, de donde $2 \mid k$ y podemos escribir $k = 2k'$. Entonces:

$$a \equiv g^k \equiv g^{2k'} \equiv (g^{k'})^2 \mod p,$$

luego a es un residuo cuadrático módulo p como queríamos ver. ∎

Definición 2.4. *Sea p un primo impar. Definimos el **símbolo de Legendre** de la siguiente manera:*

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

Observación 2.5. Está claro que si $a \equiv b \mod p$, entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Proposición 2.6. Sea p un primo impar, y $a \in \mathbb{Z}$ no nulo. Entonces:

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \mod p.$$

Demostración. La idea es usar la proposición anterior. Primero, si $p \mid a$, es claro pues todo es 0. Si $p \nmid a$, por el pequeño teorema de Fermat, $a^{p-1} - 1 \equiv 0 \mod p$, luego:

$$\left(a^{(p-1)/2} - 1\right)\left(a^{(p-1)/2} + 1\right) \equiv 0 \mod p.$$

Es decir, $a^{(p-1)/2} \equiv \pm 1 \mod p$. Si $a^{(p-1)/2} \equiv 1 \mod p$, es un residuo cuadrático y $\left(\frac{a}{p}\right) = 1$. Si $a^{(p-1)/2} \equiv -1 \mod p$, no lo es y $\left(\frac{a}{p}\right) = -1$. En cualquier caso, se tiene la igualdad que se quería probar. ∎

Observación 2.7. Como la ecuación $a^{(p-1)/2} \equiv 1 \mod p$ tiene $(p-1)/2$ soluciones, deducimos que hay $(p-1)/2$ residuos cuadráticos módulo p, sin contar el 0, y $(p-1)/2$ no residuos cuadráticos módulo p. En particular tenemos la igualdad $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$.

Proposición 2.8 (Primera ley suplementaria de la reciprocidad cuadrática.). Sea p un primo impar, entonces:

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

Demostración. Por la proposición 2.6, tenemos $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p$, y como $p \neq 2$, es $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ ∎

Proposición 2.9.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Demostración. Si p divide a a o b, el resultado se verifica. Supongamos que p no divide a ninguno de los dos. Usando la proposición 2.6, tenemos:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \mod p, \quad \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p, \quad \left(\frac{b}{p}\right) \equiv b^{(p-1)/2} \mod p.$$

Es decir,

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p,$$

pero en este caso el símbolo de Legendre toma los valores ± 1, luego la ecuación de arriba es, de hecho, una igualdad. ∎

Observación 2.10. Esta proposición implica que el producto de dos residuos cuadráticos es un residuo cuadrático, y que el producto de dos no residuos cuadráticos sí que es un residuo cuadrático.

Proposición 2.11 (Segunda ley suplementaria de la reciprocidad cuadrática.). Sea p un primo impar. Entonces:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1,7 \mod 8, \\ -1 & \text{si } p \equiv 3,5 \mod 8. \end{cases}$$

Se puede escribir de forma más compacta como $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Demostración. Vamos a trabajar en $\mathbb{Z}[i]$ e ilustrar la potencia que tiene la teoría algebraica de números. Sabemos que $(1+i)^2 = 2i$. Ahora,

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

Además, $(1+i)^p \equiv 1 + i^p \mod p\mathbb{Z}[i]$. Juntando todos tenemos:

$$2^{\frac{p-1}{2}}(1+i)i^{\frac{p-1}{2}} \equiv 1 + i^p \mod p\mathbb{Z}[i] \tag{2.1}$$

Vamos a estudiar la ecuación (2.1) en función de la congruencia módulo 8 de p.

- Si $p \equiv 1 \mod 8$, entonces $i^p = i^{8k+1} = i$, e $i^{(p-1)/2} = 1$. Entonces la ecuación (2.1) se escribe:

  $$2^{\frac{p-1}{2}}(1+i) \equiv (1+i) \mod p\mathbb{Z}[i] \Rightarrow 2^{\frac{p-1}{2}} \equiv 1 \mod p\mathbb{Z}[i].$$

  Como $p\mathbb{Z}[i]$ es el ideal extendido de p, también tenemos $2^{\frac{p-1}{2}} \equiv 1 \mod p$ y por la proposición 2.6, $\left(\frac{2}{p}\right) = 1$.
- Si $p \equiv -1 \mod 8$, $i^p = -i$, $i^{(p-1)/2} = -i$, y la ecuación (2.1) queda:

  $$1 - i \equiv -i(1+i)2^{\frac{p-1}{2}} \mod p\mathbb{Z}[i].$$

  Siguiendo el mismo razonamiento de antes, tenemos que $\left(\frac{2}{p}\right) = 1$.
- Si $p \equiv 3 \mod 8$, entonces $i^p = -i$, $i^{(p-1)/2} = i$ y operando como antes resulta $\left(\frac{2}{p}\right) = -1$.
- Si $p \equiv 5 \mod 8$, entonces $i^p = i$, $i^{(p-1)/2} = -1$, y de nuevo sale $\left(\frac{2}{p}\right) = -1$.

Además, para llegar a la segunda forma del enunciado basta sustituir en $(-1)^{\frac{p^2-1}{8}}$ en cada congruencia módulo 8.

Para probar el resultado estrella de esta sección usaremos una herramienta muy importante en la teoría de números: las sumas de Gauss. Aunque se pueden definir de forma más general, nosotros usaremos el símbolo de Legendre:

Definición 2.12 (Suma de Gauss). *Sea p un primo impar, y denotemos por ζ_p una raíz $p-$ésima primitiva de la unidad. Definimos la* ***suma de Gauss*** *como:*

$$S = \sum_{a \bmod p} \left(\frac{a}{p}\right) \zeta_p^a.$$

Proposición 2.13.

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

Demostración.

$$S^2 = S \cdot S = \left(\sum_{a \bmod p} \left(\frac{a}{p}\right) \zeta_p^a\right) \cdot \left(\sum_{b \bmod p} \left(\frac{b}{p}\right) \zeta_p^b\right) = \left(\sum_{a,b \bmod p} \left(\frac{ab}{p}\right) \zeta_p^{a+b}\right).$$

Escribimos $b = ca$, con $(c, p) = 1$:

$$S^2 = \sum_{(a,p)=1} \sum_{(c,p)=1} \left(\frac{a^2 c}{p}\right) \zeta_p^{a(1+c)} = \sum_{(c,p)=1} \left(\frac{c}{p}\right) \left(\sum_{(a,p)=1} \zeta_p^{a(1+c)}\right),$$

donde hemos usado que el símbolo de Legendre es multiplicativo y que a^2 es un residuo cuadrático módulo p.

Ahora observamos que, ya que p es primo, $(1 + c, p) = 1$ o $(1 + c, p) = p$, y este último caso pasa si $c = p - 1$. Vamos a estudiar el sumatorio interior en estos dos casos:

- Si $(c + 1, p) = 1$, entonces:

$$\left(\sum_{(a,p)=1} \zeta_p^{a(1+c)}\right) = \zeta_p^{1+c} + \zeta_p^{2(1+c)} + \cdots + \zeta_p^{(p-1)(1+c)} = -1.$$

- Si $(c + 1, p) = p$, entonces:

$$\left(\sum_{(a,p)=1} \zeta_p^{a(1+c)}\right) = 1 + 1^2 + \cdots + 1^{p-1} = p - 1.$$

Así que, separando el sumatorio en estos casos:

$$\begin{aligned} S^2 &= \sum_{(c,p)=1} \left(\frac{c}{p}\right) \left(\sum_{(a,p)=1} \zeta_p^{a(1+c)} \right) \\ &= \sum_{1\leq c\leq p-2} \left(\frac{c}{p}\right)(-1) + \left(\frac{p-1}{p}\right)(p-1) \\ &= (-1)\left(\sum_{1\leq c\leq p-1} \left(\frac{c}{p}\right) - \left(\frac{p-1}{p}\right)\right) + \left(\frac{p-1}{p}\right)(p-1) \\ &= \left(\frac{p-1}{p}\right) + \left(\frac{p-1}{p}\right)(p-1) = \left(\frac{-1}{p}\right) p. \end{aligned}$$

Hemos usado la igualdad de la observación 2.7 y que $p-1 \equiv -1 \mod p$ en las igualdades anteriores.

Proposición 2.14. Sea q un primo impar. Entonces:

$$S^q \equiv \left(\frac{q}{p}\right) S \mod q.$$

Demostración. Vamos a trabajar en el cuerpo de números $K = \mathbb{Q}[\zeta_p]$, donde ζ_p es una raíz primitiva $p-$ésima de la unidad. Sea $\mathcal{O}_K$ su anillo de enteros.

$$S^q = \left(\sum_{a \mod p} \left(\frac{a}{p}\right) \zeta_p^a \right)^q \equiv \sum_{a \mod p} \left(\frac{a}{p}\right)^q \zeta_p^{aq} \mod q\mathcal{O}_K.$$

Como q es un primo impar, $\left(\frac{a}{p}\right)^q = \left(\frac{a}{p}\right)$. Por otro lado,

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{q^2}{p}\right) = \left(\frac{aq^2}{p}\right).$$

Juntando todo nos queda:

$$S^q \equiv \sum_{a \mod p} \left(\frac{aq^2}{p}\right) \zeta_p^{aq} \equiv \left(\frac{q}{p}\right) \sum_{a \mod p} \left(\frac{aq}{p}\right) \zeta_p^{aq} \mod q\mathcal{O}_K.$$

Ahora, si a recorre todas las clases módulo p, aq también, así que podemos reescribir la ecuación de la siguiente manera:

$$S^q \equiv \left(\frac{q}{p}\right) S \mod q\mathcal{O}_K.$$

Por último, como $q\mathcal{O}_K$ es el ideal extendido de q, esta ecuación también será válida módulo q, luego:

$$S^q \equiv \left(\frac{q}{p}\right) S \quad \text{mód } q.$$

Teorema 2.15 (Ley de reciprocidad cuadrática). *Sean p y q dos primos impares. Entonces:*

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

Demostración. De la proposición 2.14, tenemos

$$S^q \equiv \left(\frac{q}{p}\right) S \quad \text{mód } q,$$

y cancelando S en ambos lados de la ecuación nos da:

$$S^{q-1} \equiv \left(\frac{q}{p}\right) \quad \text{mód } q.$$

Ahora, como q es un primo impar, $2 \mid q-1$, así que podemos escribir:

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

donde en la última igualdad hemos usado la proposición 2.13. Ahora usamos la proposición 2.8, y 2.6 y tenemos:

$$\left(\frac{q}{p}\right) \equiv p^{(q-1)/2}(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \quad \text{mód } p.$$

Pero como $q \neq 2$ y en la ecuación todos los términos son ± 1, es de hecho una igualdad:

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

Una vez estudiado en profundidad el símbolo de Legendre y la ley de reciprocidad cuadrática, nos preguntamos si se puede generalizar a residuos cuadráticos módulo un número entero n. De manera natural surge la siguiente definición:

Definición 2.16. *Sean $a \in \mathbb{Z}$ no nulo y n un entero positivo impar, coprimo con a. Definimos el **símbolo de Jacobi** $\left(\frac{a}{n}\right)$ como el producto de los símbolos de Legendre correspondientes a la factorización de n. Es decir, si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$:*

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{\alpha_1} \dots \left(\frac{a}{p_k}\right)^{\alpha_k}.$$

El símbolo de Jacobi es una buena generalización del símbolo de Legendre, pues cumple las propiedades esperables, en especial la ley de reciprocidad cuadrática y las leyes suplementarias. Lo bueno es que su prueba se remite a descomponer el símbolo de Jacobi con su definición y aplicar el resultado para el símbolo de Legendre:

Teorema 2.17 (Ley de reciprocidad cuadrática para el símbolo de Jacobi). *Con la notación de la definición anterior, tenemos las leyes suplementarias:*

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} \qquad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}},$$

y la ley de reciprocidad cuadrática, para a, n enteros positivos, impares y coprimos, se tiene:

$$\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)(-1)^{\frac{a-1}{2}\cdot\frac{n-1}{2}}.$$

2.2 Descomposición de primos en extensiones cuadráticas.

En esta sección usaremos las herramientas que hemos desarrollado para estudiar el comportamiento de los primos de $\mathbb{Z}$ en el anillo de enteros de una extensión cuadrática. Sea $K = \mathbb{Q}[\sqrt{d}]$ con d libre de cuadrados, y sea p un número primo. Queremos estudiar la descomposición de $p\mathcal{O}_K$ en función de los primos de $\mathcal{O}_K$. Como las extensiones cuadráticas siempre son de Galois, en virtud del teorema (1.51), como $n = [K : \mathbb{Q}] = 2$, puede darse uno de los 3 siguientes escenarios:

1. Si $r = 2, e = 1, f = 1$, $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ con $\mathfrak{p}_1 \neq \mathfrak{p}_2$, y p se descompone completamente en $\mathcal{O}_K$.
2. Si $r = 1, e = 1, f = 2$, $p\mathcal{O}_K$ es un ideal primo y p es inerte en $\mathcal{O}_K$.
3. Si $r = 1, e = 2, f = 1$, $p\mathcal{O}_K = \mathfrak{p}^2$ y p ramifica en $\mathcal{O}_K$.

Vamos a estudiar, según el valor de d, cuándo ocurre cada caso. Usaremos el teorema 1.53 para deducir el comportamiento de los primos enteros en $\mathcal{O}_K$. Denotaremos:

$$\omega = \frac{1+\sqrt{d}}{2}, \qquad c = \frac{1-d}{4}.$$

El polinomio mínimo de $\sqrt{d}$ o de ω, dependiendo de la congruencia de d módulo 4 es el siguiente:

$$f(x) = \begin{cases} x^2 - d & \text{si } d \equiv 2, 3 \mod 4, \\ x^2 - x + c & \text{si } d \equiv 1 \mod 4. \end{cases}$$

Como de costumbre, el primo $p = 2$ es conflictivo así que lo estudiaremos aparte. Resulta que la congruencia de p módulo δ_K determina la descomposición de p en K:

Proposición 2.18. Sea $p \in \mathbb{Z}$ un primo impar. Entonces:

- p ramifica en $\mathbb{Q}[\sqrt{d}]$ si y sólo si $\left(\frac{d}{p}\right) = 0$.
- p es inerte en $\mathbb{Q}[\sqrt{d}]$ si y sólo si $\left(\frac{d}{p}\right) = -1$.
- p se descompone completamente en $\mathbb{Q}[\sqrt{d}]$ si y sólo si $\left(\frac{d}{p}\right) = 1$.

Demostración. Primero veamos el caso en que $d \equiv 2, 3 \mod 4$. Tenemos que estudiar la factorización del polinomio $x^2 - d$ módulo p. Si $\left(\frac{d}{p}\right) = 0$, es decir $p \mid d$, entonces $x^2 - d \equiv x^2 \mod p$ y por el teorema 1.53 p ramifica en $\mathbb{Q}[\sqrt{d}]$. Si $\left(\frac{d}{p}\right) = -1$, el polinomio $x^2 - d$ es irreducible en $\mathbb{F}_p[x]$ y por tanto, p es inerte en $\mathbb{Q}[\sqrt{d}]$. Por último, si $\left(\frac{d}{p}\right) = 1$, tenemos

$$x^2 - d \equiv \left(x - \sqrt{d}\right)\left(x + \sqrt{d}\right) \mod p,$$

y p se descompone completamente en $\mathbb{Q}[\sqrt{d}]$.

Ahora veamos el caso $d \equiv 1 \mod 4$. En primer lugar, si $\left(\frac{d}{p}\right) = 1$, existe $\alpha \in \mathbb{Z}$ tal que $d \equiv \alpha^2 \mod p$. Por tanto, el polinomio $x^2 - x + c$ factoriza en $\mathbb{F}_p[x]$ como

$$x^2 - x + c \equiv (x - \omega)(x - \hat{\omega}) \mod p, \quad \hat{\omega} = \frac{1 - \alpha}{2},$$

luego p se descompone completamente en $\mathbb{Q}[\sqrt{d}]$. Ahora queremos ver cuándo se da la siguiente situación:

$$x^2 - x + \bar{c} \equiv \left(x^2 + \bar{a}\right)^2 \equiv x^2 + 2\bar{a}x + \bar{a}^2, \mod p$$

para caracterizar cuándo p ramifica en $\mathbb{Q}[\sqrt{d}]$. Igualando coeficientes tenemos:

$$2\bar{a} = -\bar{1} \qquad\qquad \bar{a}^2 = \bar{c}.$$

Despejando de $c = \frac{1-d}{4}$ tenemos $d = 1 - 4c$, y reduciendo módulo p

$$\bar{d} = \bar{1} - (\overline{2a})^2 = \bar{1} - \bar{1} = \bar{0},$$

así que si p ramifica en $\mathbb{Q}[\sqrt{d}]$, entonces $p \mid d$.
Recíprocamente, si $p \mid d$, entonces $4c = 1 - d \equiv 1 \mod 4$, luego:

$$4(x^2 - x + c) \equiv 4x^2 - 4x + 1 = (2x-1)^2 \mod p.$$

El polinomio $x^2 - x + c = \left(x - \frac{1}{2}\right)^2$ factoriza como un cuadrado en $\mathbb{F}_p[x]$ (una vez más vemos la importancia de que $p \neq 2$) y por tanto p ramifica en $\mathbb{Q}[\sqrt{d}]$ si y sólo si $\left(\frac{d}{p}\right) = 0$. Por último, razonando por exclusión, p es inerte en $\mathbb{Q}[\sqrt{d}]$ cuando $\left(\frac{d}{p}\right) = -1$ y esto termina la prueba. ∎

Proposición 2.19. El primo 2 ramifica en $\mathbb{Q}[\sqrt{d}]$ si y sólo si $d \equiv 2, 3 \mod 4$, es inerte en $\mathbb{Q}[\sqrt{d}]$ si y sólo si $d \equiv 5 \mod 8$ y se descompone completamente en $\mathbb{Q}[\sqrt{d}]$ si y sólo si $d \equiv 1 \mod 4$.

Demostración. Comencemos estudiando el caso de $d \equiv 2, 3 \mod 4$. Recordemos que $\mathcal{O}_\mathcal{K} = \mathbb{Z}[\sqrt{d}]$. Puede ocurrir que $\bar{d} = \bar{0}$ o que $\bar{d} = \bar{1}$.

$$\begin{cases} \bar{d} = \bar{0} & \Rightarrow x^2 - \bar{d} = x^2. \\ \bar{d} = \bar{1} & \Rightarrow x^2 - \bar{d} = \left(x - \bar{1}\right)^2. \end{cases}$$

En cualquier caso, el polinomio mínimo de $\sqrt{d}$ factoriza en $\mathbb{F}_2[x]$ como un cuadrado, luego 2 ramifica en $\mathbb{Q}[\sqrt{d}]$.

Para el caso en que $d \equiv 1 \mod 4$, recordemos que el polinomio que tenemos que estudiar es $x^2 - x + c$, con $c = \frac{1-d}{4}$. Veamos su comportamiento módulo 2:

- Si $c \equiv 1 \mod 2$, es decir, $\frac{1-d}{2} = 2k+1$, despejando tenemos que $d = -8k-3$, o lo que es lo mismo, $d \equiv -3 \equiv 5 \mod 8$, y en este caso el polinomio $x^2 - x + \bar{1} = x^2 + x + \bar{1}$ es irreducible en $\mathbb{F}_2[x]$, luego 2 es inerte en $\mathbb{Q}[\sqrt{d}]$.
- Si $c \equiv 0 \mod 2$, es decir, $\frac{1-d}{2} = 2k$, despejando como antes tenemos que $d \equiv 1 \mod 8$, y el polinomio $x^2 - x + \bar{c} = x^2 + x = x(x+1)$ factoriza en $\mathbb{F}_2[x]$ como dos factores lineales. Es decir, 2 descompone completamente en $\mathbb{Q}[\sqrt{2}]$. ∎

Cuando calculamos el discriminante, obtuvimos que $\delta_K = d$ si $d \equiv 1 \mod 4$ y $\delta_K = 4d$ si $d \equiv 2, 3 \mod 4$. Combinando las dos proposiciones anteriores deducimos:

Proposición 2.20. $p \in \mathbb{Z}$ ramifica en $K = \mathbb{Q}[\sqrt{d}]$ si y sólo si $p \mid \delta_K$. En particular, sólo una cantidad finita de primos ramifican en $\mathbb{Q}[\sqrt{d}]$.

Como curiosidad, se puede probar que este resultado es válido para cualquier cuerpo de números, no sólo las extensiones cuadráticas.

Ejemplo 2.21. En $K = \mathbb{Q}[i]$, como $-1 \equiv 3 \mod 4$, el discriminante es $\delta_K = -4$. Entonces, el único primo que ramifica es el $2 = i(1-i)^2$.

Gracias al símbolo de Jacobi y a su reciprocidad cuadrática, podremos caracterizar el comportamiento de p viendo si es un cuadrado módulo cierto número (d o $d/2$, según el caso). Si $d \equiv 1 \mod 4$, hacemos lo siguiente:

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

Si $d \equiv 3 \mod 4$,

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

Y si $d \equiv 2 \mod 4$, en este caso d es par y hay que tener más cuidado: $d = 2e$ con e un número impar y hacemos:

$$\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{e}{p}\right) = (-1)^{\frac{p^2-1}{8}}(-1)^{\frac{p-1}{2}\cdot\frac{d-2}{4}} \left(\frac{p}{e}\right).$$

Corolario 2.22. Si $p \equiv p' \mod |\delta_K|$, entonces p y p' tienen la misma descomposición en $K = \mathbb{Q}[\sqrt{d}]$.

3 El estudio de las formas cuadráticas

En este capítulo vamos a explotar la teoría de las extensiones cuadráticas para estudiar las formas cuadráticas.

3.1 La ecuación $p = x^2 + ny^2$.

Sea $K = \mathbb{Q}[\sqrt{-n}]$, con $n > 0$ y $-n \equiv 2, 3 \mod 4$, es decir, que $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$. Supongamos que el número de clase $h_K = 1$, es decir, que $\mathcal{O}_K$ es un dominio de ideales principales.

Vamos a hacer un breve comentario sobre las unidades en los anillos de enteros. Gracias al carácter multiplicativo de la norma deducimos:

Proposición 3.1. Sea K un cuerpo de números y $\mathcal{O}_K$ su anillo de enteros. Un elemento $u \in \mathcal{O}_K$ es unidad si y sólo si $|N(u)| = 1$.

Demostración. Si u es una unidad, $uu^{-1} = 1$. Tomando norma, $N(u)N(u^{-1}) = 1$, y como u es un entero algebraico, su norma es un número entero y necesariamente debe ser $N(u) = \pm 1$. Recíprocamente, si $|N(u)| = 1$, y digamos que $[K : \mathbb{Q}] = 1$, denotamos con $\sigma^{(i)} : K \to \overline{\mathbb{Q}}$ a las distintas inmersiones de K en una clausura algebraica de $\mathbb{Q}$ que fijan $\mathbb{Q}$, y por $u^{(i)} = \sigma^{(i)}(u)$, entonces $N(u) = u^{(1)} \dots u^{(n)} = \pm 1$, donde $u^{(1)} = u$. El elemento $u^{(2)} \dots u^{(n)}$ es el inverso de u, así que es unidad. ∎

Resulta que p verifica la ecuación $p = x^2 + ny^2$ si y sólo si p se descompone completamente en K. En efecto, si $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, con $\mathfrak{p}_1 \neq \mathfrak{p}_2$, como $\mathcal{O}_K$ es un dominio de ideales principales, $\mathfrak{p}_1 = \left(x + y\sqrt{-n}\right)\mathcal{O}_K$. Ahora bien, tanto $\mathfrak{p}_1$ como $\mathfrak{p}_2$ están

encima de p. Por la proposición 1.50, existe un $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ tal que $\mathfrak{p}_2 = \sigma\mathfrak{p}_1$. Pero como K es una extensión cuadrática, y $\mathfrak{p}_1 \neq \mathfrak{p}_2$, necesariamente σ es la conjugación

$$\sigma : \sqrt{-n} \mapsto -\sqrt{-n},$$

de donde $\mathfrak{p}_2 = \left(x - y\sqrt{-n}\right)\mathcal{O}_K$. Entonces:

$$p\mathcal{O}_K = \left(x + y\sqrt{-n}\right)\mathcal{O}_K \left(x - y\sqrt{-n}\right)\mathcal{O}_K = (x^2 + ny^2)\mathcal{O}_K,$$

de donde tenemos la ecuación $p = u(x^2 + ny^2)$, pues puede aparecer una unidad u. Esto no supone mucho problema, pues despejando de la ecuación queda que u debe ser un número racional, y las únicas unidades racionales son ± 1. Además, como el lado derecho de la igualdad es positivo, dicha unidad debe ser 1, y tenemos la ecuación que queríamos: $p = x^2 + ny^2$.

Recíprocamente, si $p = x^2 + ny^2$, esta ecuación se puede escribir en $\mathcal{O}_K$ como $p = \left(x + y\sqrt{-n}\right) \cdot \left(x - y\sqrt{-n}\right)$. Entonces $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ debe ser la factorización en ideales primos de $p\mathcal{O}_K$, al ser K una extensión de grado 2, y al haberlo escrito como producto de dos factores. Por el teorema 1.51, esa expresión no se puede seguir factorizando, y por tanto descompone completamente en K.

Por tanto, el estudio de la ecuación $p = x^2+ny^2$ se reduce a estudiar los primos que descomponen completamente en las extensiones cuadráticas imaginarias con número de clase 1. Por suerte, sabemos exactamente cuáles son:

Proposición 3.2 ([Neu13, pág. 37]). Las extensiones cuadráticas imaginarias con número de clases 1 son de la forma $\mathbb{Q}[\sqrt{d}]$ con $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.

De las extensiones cuadráticas anteriores, sólo -1 y -2 son congruentes con 2 y 3 módulo 4. Estos son los más sencillos de estudiar. También haremos un estudio del resto de casos, veremos que algo podemos decir.

3.1.1 Primos de la forma $p = x^2 + y^2$

En este caso la clave es estudiar la extensión $K = \mathbb{Q}[\sqrt{-1}]$. Como $-1 \equiv 3 \mod 4$, su anillo de enteros es $\mathcal{O}_K = \mathbb{Z}[i]$. Es conocido que este anillo es un dominio de ideales principales, así que estamos en las condiciones anteriores. Como $\delta_K = -4$, 2 divide al discriminante y entonces ramifica. Además, es el único primo que ramifica en K, y lo podemos escribir fácilmente como $2 = 1^2 + 1^2$.

Sabemos que $p = x^2 + y^2$ siempre que p se descomponga completamente en K, es decir, si $\left(\frac{-1}{p}\right) = 1$. Gracias a la proposición 2.8 podemos determinar cuáles son:

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \iff \frac{p-1}{2} \text{ es par.}$$

Con un simple cálculo se ve: $\frac{p-1}{2} = 2k$ si $p - 1 = 4k$, es decir, si $p \equiv 1 \mod 4$. Entonces, hemos deducido el siguiente resultado:

$$\boxed{p = x^2 + y^2 \iff p = 2,\ p \equiv 1 \mod 4.}$$

Ejemplo 3.3. Podemos escribir $5 = 1^2 + 2^2$.

Observación 3.4. Estamos identificando los generadores de dos ideales. ¿Hasta qué punto multiplicar por unidades cambia la solución? Lo que puede pasar es que se nos cambie el orden de x e y, o que cambie el signo.

3.1.2 Primos de la forma $p = x^2 + 2y^2$

En este caso la clave es estudiar la extensión $K = \mathbb{Q}[\sqrt{-2}]$. Como $-2 \equiv 2 \mod 4$, su anillo de enteros es $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$. Se puede probar que este anillo es un dominio euclídeo, y por tanto un dominio de ideales principales.

Como antes, $\delta_K = -8$, luego 2 ramifica y lo podemos escribir como $2 = 0^2 + 2 \cdot 1^2$. Vamos a caracterizar los primos que se descomponen completamente en K. Esto pasa si $\left(\frac{-2}{p}\right) = 1$, es decir:

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

Para que sea 1 debe ocurrir que ambos exponentes tengan la misma paridad. Recordamos que la proposición 2.11 se puede escribir de la siguiente manera:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1, 7 \mod 8, \\ -1 & \text{si } p \equiv 3, 5 \mod 8. \end{cases}$$

Vamos a ver cuándo ambos exponentes son positivos primero: si $p \equiv 1 \mod 8$, es decir, $p = 1 + 8k$, en particular $p \equiv 1 \mod 4$ luego $(-1)^{(p-1)/2} = 1$, y es suficiente pedir lo primero. Si $p \equiv 7 \mod 8$, entonces $p \equiv 3 \mod 4$ y no son ambos positivos.

Ahora cuando los dos son negativos. Si $p \equiv 3 \mod 8$, en también es $p \equiv 3 \mod 4$ y ambos signos son negativos. Pero si $p \equiv 5 \mod 8$, entonces $p \equiv 1 \mod 4$ y tienen signos diferentes. En resumen:

$$p = x^2 + 2y^2 \iff p = 2,\ p \equiv 1, 3 \mod 8.$$

Ejemplo 3.5. Veamos algunos ejemplos. Primero, el caso especial de $p = 2$, pues ramifica: $2 = 0^2 + 2 \cdot 1^2$. Ahora, para un caso más común, $11 = 3^2 + 2 \cdot 1^2$.

3.2 El caso $d \equiv 1 \mod 4$

Sea $K = \mathbb{Q}[\sqrt{-n}]$, con $-n \equiv 1 \mod 4$, es decir, que $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-n}}{2}\right]$. Supongamos que el número de clase $h_K = 1$, es decir, que $\mathcal{O}_K$ es un dominio de ideales principales. Como antes, podremos escribir los números primos que se descomponen completamente en K en función de una cierta forma cuadrática. Repitiendo el razonamiento anterior, sea p que se descomponga completamente en K, veamos cómo queda la ecuación:

$$p = \left(x + y \cdot \frac{1+\sqrt{-n}}{2}\right) \cdot \left(x + y \cdot \frac{1-\sqrt{-n}}{2}\right) = x^2 + xy + y^2 \cdot \frac{1+n}{4}. \tag{3.1}$$

Así que, a priori, podemos sacar el siguiente resultado:

$$p \text{ se descompone completamente en } K \iff p = x^2 + xy + y^2 \cdot \frac{1+n}{4}$$

Vamos a hacer un par de cálculos que nos serán de utilidad más adelante:

Observación 3.6. Supongamos que $-n \equiv 1 \mod 4$, y sea p un primo impar. Entonces:

$$\left(\frac{-n}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{n}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{n-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{n}\right) = \left(\frac{p}{n}\right). \tag{3.2}$$

Observación 3.7. Vamos a calcular una expresión de la norma en $K = \mathbb{Q}[\sqrt{-n}]$ cuando $-n \equiv 1 \mod 4$. Sea $\alpha = \frac{x+y\sqrt{-n}}{2} \in \mathcal{O}_K$, entonces:

$$N(\alpha) = \frac{x + y\sqrt{-n}}{2}\frac{x - y\sqrt{-n}}{2} = \frac{x^2 + ny^2}{4}.$$

En virtud de la proposición 3.1, α es unidad si y sólo si $x^2 + ny^2 = 4$.

3.2.1 Primos de la forma $p = x^2 + 3y^2$

Vamos a estudiar la descomposición de primos en $K = \mathbb{Q}[\sqrt{-3}]$. Observamos que el anillo de enteros es $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ y parece que no vamos a conseguir una expresión en esta forma. Primero, como $\delta_K = -3$, el 3 es el único primo que ramifica, y lo podemos escribir como $3 = 0^2 + 3 \cdot 1^2$. Veamos cuáles son los primos que se descomponen completamente en K. Recordemos que son los primos p que verifican que $\left(\frac{-3}{p}\right) = 1$. Aplicando la ecuación (3.2), podemos ver cuándo $\left(\frac{p}{3}\right) = 1$, y esto es muy sencillo, pues el único residuo cuadrático módulo 3 es 1. De aquí deducimos entonces:

Proposición 3.8. p descompone completamente en K si y sólo si $p \equiv 1 \mod 3$.

Ahora veremos que el hecho de que el anillo de enteros de K sea $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ no supone demasiado problema. Nuestra idea es multiplicar convenientemente por unidades para que los ideales en los que se descompone p en K estén generados por elementos de la forma $x + y\sqrt{-3}$, y poder escribir $p = x^2 + 3y^2$. Veamos cuáles son las unidades de $\mathcal{O}_K$[1]. Sea $\alpha = x + y\frac{1+\sqrt{-3}}{2} \in \mathcal{O}_K$. Por la proposición 3.1, las unidades están caracterizadas por verificar $x^2 + 3y^2 = 4$. Por suerte, como x e y son enteros, tenemos sólo una cantidad finita de soluciones: si $x = \pm 2$ y $y = 0$ si $x, y = \pm 1$. Más concretamente, las unidades de $\mathcal{O}_K$ son:

$$\pm 1, \frac{1 + \sqrt{-3}}{2}, \frac{-1 + \sqrt{-3}}{2}, \frac{1 - \sqrt{-3}}{2}, \frac{-1 - \sqrt{-3}}{2}.$$

Recordamos entonces que buscamos escribir $x + y\frac{1+\sqrt{-3}}{2}$ como $a + b\sqrt{-3}$ con a y b

[1]Existe un teorema que caracteriza perfectamente cuáles son las unidades del anillo de enteros de cualquier cuerpo de números, y se debe a Dirichlet. En el caso de las extensiones imaginarias podemos usaremos método más rudimentario. Para más información, consultar [Neu13, Capítulo 7]

enteros. Un primer caso muy simple es si y es par:

$$x + y\frac{1+\sqrt{-3}}{2} = x + \frac{y}{2} + \frac{y}{2}\sqrt{-3}, \quad x + y\frac{1-\sqrt{-3}}{2} = x + \frac{y}{2} - \frac{y}{2}\sqrt{-3}$$

de donde tomando $a = x + \frac{y}{2}$, $b = \frac{y}{2}$, se tiene la expresión deseada:

$$p = \left(a + b\sqrt{-3}\right)\left(a - b\sqrt{-3}\right) = a^2 + 3b^2.$$

Ahora vamos al caso en que x sea par, e y sea impar (no pueden ser los dos pares a la vez: como p verifica la ecuación (3.1), p sería un número par). Aquí hay que multiplicar por unidades para expresar los generadores de los ideales en los que factoriza p de forma conveniente:

$$\left(x + y\frac{1+\sqrt{-3}}{2}\right)\left(\frac{1-\sqrt{-3}}{2}\right) = \frac{x}{2} + y + \frac{-x}{2}\sqrt{-3} = a + b\sqrt{-3},$$
$$\left(x + y\frac{1-\sqrt{-3}}{2}\right)\left(\frac{1+\sqrt{-3}}{2}\right) = \frac{x}{2} + y + \frac{x}{2}\sqrt{-3} = a - b\sqrt{-3}.$$

Tomando $a = \frac{x}{2} + y$ y $b = \frac{-x}{2}$, podemos escribir $p = a^2 + 3b^2$.

Ahora el caso en el que tanto x como y sean impares. De nuevo, multiplicando por una unidad adecuada:

$$\left(x + y\frac{1+\sqrt{-3}}{2}\right)\left(\frac{1+\sqrt{-3}}{2}\right) = \frac{x-y}{2} + \frac{x+y}{2}\sqrt{-3} = a + b\sqrt{-3},$$
$$\left(x + y\frac{1-\sqrt{-3}}{2}\right)\left(\frac{1-\sqrt{-3}}{2}\right) = \frac{x-y}{2} + \frac{-(x+y)}{2}\sqrt{-3} = a - b\sqrt{-3}.$$

En conclusión, siempre que p se descomponga completamente en $\mathbb{Q}[\sqrt{-3}]$, podemos multiplicar por una unidad para que el generador de los ideales en los que se descompone sea de la forma que nos conviene. En conclusión:

$$p = x^2 + 3y^2 \iff p = 3,\ p \equiv 1 \mod 3.$$

Ejemplo 3.9. Podemos escribir $7 = 2^2 + 3 \cdot 1^2$, o $13 = 1^2 + 3 \cdot 2^2$.

Observación 3.10. En este caso, multiplicar por unidades tampoco cambia la solución. De hecho, para obtener $p = x^2 + 3y^2$, hemos tenido que multiplicar minuciosamente por ciertas unidades. Para la ecuación $p = x^2 + xy + y^2$ tampoco importa multiplicar por las otras unidades.

3.2.2 Primos de la forma $p = x^2 + 7y^2$

Estudiemos la factorización en $\mathbb{Q}[\sqrt{-7}]$. Como $-7 \equiv 1 \mod 4$, el anillo de enteros es $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$, y el discriminante es $\delta_K = -7$. En K, el 7 ramifica, y se puede escribir como $7 = 0^2 + 7 \cdot 1^2$.

A priori, los primos que se descompongan completamente en K se escribirán en la forma

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

Estudiemos los primos que se descomponen completamente en K. Como de costumbre, el primo $p = 2$ es un poco especial: se puede escribir $2 = 0^2 + 0 \cdot 1 + 2 \cdot 1^2$, pero no como $2 = x^2 + 7y^2$. Sea entonces $p \neq 2, 7$:

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

Un cálculo rápido nos da que los residuos cuadráticos módulo 7 son $1, 2, 4$, luego p se descompone completamente en K si y sólo si $p \equiv 1, 2, 4 \mod 7$.

Vamos a calcular las unidades de $\mathcal{O}_K$, a ver si podemos hacer el mismo razonamiento que antes para obtener $p = x^2 + 7y^2$. Calculemos la expresión de la norma, sea $\alpha = \frac{x+y\sqrt{-7}}{2} \in \mathcal{O}_K$:

$$N(\alpha) = \frac{x + y\sqrt{-7}}{2} \cdot \frac{x - y\sqrt{-7}}{2} = \frac{x^2 + 7y^2}{4},$$

de donde α es unidad si y sólo si $x^2 + 7y^2 = 4$, pero esta ecuación no tiene soluciones enteras distintas de ± 1, así que no aparecen unidades nuevas en $\mathcal{O}_K$. Sin embargo, veremos que aún así podemos llegar a la ecuación $p = x^2 + 7y^2$. Partimos de la ecuación $p = x^2 + xy + 2y^2$, donde $p \neq 2, 7$. Una primera observación es que x e y no pueden tener la misma paridad, pues la suma sería un número par en ambos casos. Si y es par, ya está, pues basta escribir:

$$x + y \cdot \frac{1 + \sqrt{-7}}{2} = \left(x + \frac{y}{2}\right) + \frac{y}{2}\sqrt{-7} = a + b\sqrt{-7},$$

lo que nos llevaría al caso $p = a^2 + 7b^2$ directamente.

Resulta que el caso en que x es par e y es impar no se puede dar, pues este caso, $x^2 + xy + 2y^2$ sería un número par. De hecho, esto pasa en general siempre y cuando

$n \equiv -1 \mod 8$, digamos $n = 8k - 1$:

$$x^2 + xy + y^2 \cdot \frac{1+n}{4} = x^2 + xy + 2ky^2,$$

el caso en que x es par no puede darse. Por tanto, el único caso que puede ocurrir es x impar e y par, el cual hemos llevado a la forma que nos interesa:

$$p = x^2 + 7y^2 \iff p = 7,\ p \equiv 1, 2, 4 \mod 7.$$

Ejemplo 3.11. Podemos escribir $11 = 2^2 + 7 \cdot 1^2$, o $29 = 1^2 + 7 \cdot 2^2$.

3.3 Extensiones reales

Vamos a ver qué partido se le pueden sacar a las extensiones cuadráticas reales en el estudio de las formas cuadráticas. Aunque parezca sorprendente, son un poco más complicadas que las imaginarias. La primera diferencia está en el número de clase, el caso 1 es mucho más común, y de hecho no se sabe si hay una cantidad infinita de ellas. Para $2 \leq n \leq 100$ son las siguientes, según [BS86, págs. 422-424]:

$$\begin{aligned} n = &2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, 43, \\ &46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97. \end{aligned}$$

Nos limitaremos a las extensiones $\mathbb{Q}[\sqrt{n}]$ con número de clase 1 y $n \equiv 2, 3 \mod 4$. Siguiendo un razonamiento similar al apartado anterior, si p es un primo que se descompone completamente en $K = \mathbb{Q}[\sqrt{n}]$, entonces se puede escribir como $p = u(x^2 - ny^2)$, donde u es una unidad. Otra complicación de las extensiones reales es que esa unidad, si bien debe ser racional, ahora puede ser -1. Tenemos entonces:

$$p \text{ se descompne completamente en } K \iff p = \pm(x^2 - ny^2).$$

Aún no hemos terminado con las complicaciones de las extensiones reales. Ahora, los anillos de enteros pueden tener infinitas unidades ([Neu13, Capítulo 7]), y esto implicará que no habrá solución única para la ecuación $p = \pm(x^2 - ny^2)$. Ante la dificultad de la situación, veremos un ejemplo concreto:

3.3.1 La extensión $\mathbb{Q}[\sqrt{2}]$

Estudiando esta extensión vamos a ver qué primos se pueden escribir de la siguiente manera:

$$p = x^2 - 2y^2, \qquad p = 2x^2 - y^2.$$

El anillo de enteros es $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$, y el discriminante es $\delta_K = 8$. Por tanto, el 2 es el único primo que ramifica en K. Lo podemos escribir como $2 = 2^2 - 2 \cdot 1^2 = 2 \cdot 3^2 - 4^2\cdot$, así que ya comenzamos a ver que las soluciones de la ecuación no son únicas. Sea ahora p un primo impar, veamos cuándo se descompone completamente. Por la proposición 2.11 directamente, p se descompone completamente en K si y sólo si $p \equiv 1, 7 \mod 8$, luego:

$$p = \pm(x^2 - 2y^2) \iff p = 2,\ p \equiv 1, 7 \mod 8.$$

Ejemplo 3.12. En este ejemplo vamos a ilustrar cómo se pueden conseguir tantas soluciones de la ecuación como se desee. Sea $u = 1 + \sqrt{2}$, y $\bar{u} = 1 - \sqrt{2}$ dos unidades de $\mathcal{O}_K$. Vamos a hacer un razonamiento similar al de la sección 3.2.1, multiplicar por las unidades de manera conveniente. Tomemos $p = 17$, que descompone completamente en K. Lo podemos escribir como $17 = 5^2 - 2 \cdot 2^2$, y esto es equivalente a que $17\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, con $\mathfrak{p}_1 = \left(5 + 2\sqrt{2}\right)\mathcal{O}_K, \mathfrak{p}_2 = \left(5 - 2\sqrt{2}\right)\mathcal{O}_K$. Como antes, multiplicar por una unidad el generador de los ideales no los altera, y por tanto no alterará la ecuación (salvo quizá un signo), es decir:

$$-17 = \left(1 + \sqrt{2}\right)\left(5 + 2\sqrt{2}\right)\left(1 - \sqrt{2}\right)\left(5 - 2\sqrt{2}\right) = \left(9 + 7\sqrt{2}\right)\left(9 - 7\sqrt{2}\right) = -(9^2 - 2 \cdot 7^2).$$

Si bien no hemos conseguido exactamente otra solución, pues aparece un -1, basta multiplicar de nuevo por las unidades:

$$17 = \left(1 + \sqrt{2}\right)^2\left(5 + 2\sqrt{2}\right)\left(1 - \sqrt{2}\right)^2\left(5 - 2\sqrt{2}\right) = \left(23 + 16\sqrt{2}\right)\left(23 - 16\sqrt{2}\right) = 23^2 - 2 \cdot 16^2,$$

y esta vez sí que deberíamos estar convencidos de que la solución no es única.

4 Conclusión

Tras mucho trabajo, hemos resuelto la pregunta de qué primos se pueden escribir como $p = x^2 + ny^2$ para los n que las herramientas básicas nos han permitido. Con técnicas más sofisticadas se puede resolver para una cantidad infinita de $n > 0$. El resultado es el siguiente:

Teorema 4.1 ([Cox11, Teorema 5.1]). *Sea $n \equiv 1, 2 \mod 4$ un entero positivo y libre de cuadrados. Entonces, existe un polinomio irreducible $f_n(x) \in \mathbb{Z}[x]$ tal que, para un primo p que no divida ni a n ni al discriminante de f_n, se tiene:*

$$p = x^2 + ny^2 \iff \begin{array}{l} \left(\frac{-n}{p}\right) = 1, \text{ y la ecuación} \\ f_n(x) \equiv 0 \mod p \text{ tiene solución entera.} \end{array}$$

El enunciado puede sonar no demasiado complicado, pero el polinomio f_n es el polinomio mínimo de un elemento primitivo de una extensión muy importante de $K = \mathbb{Q}[\sqrt{-n}]$: el *cuerpo de clase de Hilbert* de K. Este teorema, aunque sirve para una cantidiad infinita de casos, por desgracia no resuelve la pregunta para todos los $n > 0$. No es válido en aquellos en los que $\mathbb{Z}[\sqrt{-n}]$ no es el anillo de enteros de K. Hay que dar un paso más allá y estudiar los anillos $\mathbb{Z}[\sqrt{-n}]$, lo que da lugar al concepto de *orden* de un cuerpo de números cuadrático imaginario.

El cuerpo de clase de Hilbert es un objeto muy interesante, y estudiarlo es la continuación natural de este trabajo. Dado un cuerpo de números K, su cuerpo de clase de Hilbert es su *extensión abeliana no ramificada maximal*. Veremos qué significa esto: la parte de abeliana está clara. Para hablar de qué es una extensión no ramificada, tenemos que hablar de primos finitos e infinitos. Dada una extensión $K \subseteq L$, los primos finitos simplemente son los ideales primos de $\mathcal{O}_K$.

Un *primo infinito real* es una inmersión $\sigma : K \to \mathbb{R}$, mientras que un *primo infinito complejo* es un par de inmersiones complejas conjugadas $\sigma, \bar{\sigma} : K \to \mathbb{C}$. Un primo

infinito σ de K ramifica en L si es real pero tiene una extensión a L que es compleja. Por ejemplo, el primo infinito de $\mathbb{Q}$ no ramifica en $\mathbb{Q}[\sqrt{2}]$, pero sí ramifica en $\mathbb{Q}[\sqrt{-2}]$. Entonces, una extensión $K \subseteq L$ se dice **no ramificada** si es no ramificada en todos los primos, finitos e infinitos. Ya podemos definir el cuerpo de clase de Hilbert:

Teorema 4.2 ([Cox11, Teorema 5.18]). *Dado un cuerpo de números K, existe una extensión finita y de Galois L/K tal que:*

1. *L es una extensión de K abeliana y no ramificada.*
2. *Cualquier extensión abeliana y no ramificada de K está contenida en L.*

*El cuerpo L se denomina **cuerpo de clase de Hilbert** de K.*

El cuerpo de clase de Hilbert tiene multitud de propiedades interesantes. Una de ellas es que conocemos muy bien su grupo de clases de ideales:

Proposición 4.3 ([Cox11, Teorema 5.23]). Dado un cuerpo de números K con cuerpo de clase de Hilbert L, el grupo de clases de ideales de L es isomorfo a $\mathrm{Gal}(L/K)$.

El estudio de la descomposición de primos en L es la clave para saber cuáles se pueden escribir como $p = x^2 + ny^2$. La siguiente proposición es crucial en la prueba del teorema 4.1, que se puede encontrar en [Cox11]:

Proposición 4.4 ([Cox11, Teorema 5.26]). Sea L el cuerpo de clase de Hilbert de $K = \mathbb{Q}[\sqrt{-n}]$, con $n \not\equiv 3 \mod 4$ y libre de cuadrados, es decir, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$. Si p es un primo impar que no divide a n, entonces:

$$p = x^2 + ny^2 \iff p \text{ se descompone completamente en } L.$$

Este resultado es el que relaciona nuestra pregunta con el cuerpo de clase de Hilbert, y es lo que motiva su estudio.

En este trabajo queríamos responder una pregunta que a priori parece puramente sobre formas cuadráticas, y hemos acabado explorando el amplio mundo de la teoría algebraica de números. Ahora, resulta que tampoco hemos terminado del todo, y es que en este área siempre se puede ir más allá.

Bibliografía

[Alu21] Paolo Aluffi. *Algebra: chapter 0*. Vol. 104. American Mathematical Soc., 2021.

[BS86] Z. I. Borevich e I. R. Shafarevich. *Number theory*. Academic press, 1986.

[Cox11] David A. Cox. *Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication*. Vol. 34. John Wiley & Sons, 2011.

[IR90] Kenneth Ireland y Michael Rosen. *A classical introduction to modern number theory*. Vol. 84. Springer Science & Business Media, 1990.

[KKS00] Kazuya Kato, Nobushige Kurokawa y Takeshi Saito. *Number Theory 1: Fermat's Dream. Translations of Mathematical Monographs*. 2000.

[Loz12] Álvaro Lozano-Robledo. «Desde Fermat, Lamé, y Kummer hasta Iwasawa: Una introducción a la teoría de Iwasawa». En: *La Gaceta de la RSME* 15.2 (2012), págs. 251-276.

[Mar18] Daniel A. Marcus. *Number Fields*. Springer, 2018.

[ME05] M. Ram Murty y Jody Esmonde. *Problems in algebraic number theory*. Vol. 190. Springer Science & Business Media, 2005.

[Neu13] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Springer Science & Business Media, 2013.

[Rib13] Paulo Ribenboim. *Classical theory of algebraic numbers*. Springer Science & Business Media, 2013.