Departamento de Matemáticas, Facultad de Ciencias
Universidad Autónoma de Madrid

Órdenes en cuerpos de números

Trabajo de fin de grado

Grado en Matemáticas

Autor: Álvaro Hernández Herrera
Tutor: Enrique González Jiménez

Curso 2023-2024

Resumen

Sea K un cuerpo de números. Un *orden* en K es un subanillo $\mathcal{O}$ del anillo de enteros de K que contiene una base de la extensión $K/\mathbb{Q}$. Los órdenes generalizan la noción del anillo de enteros, y en este trabajo estudiaremos estos objetos desde sus propiedades algebraicas básicas (anillo noetheriano de dimensión 1 cuyos cocientes por ideales no nulos son finitos) hasta todas las cuestiones aritméticas que les atañen.

Más concretamente, nos centraremos en estudiar el *grupo de Picard* de un orden y su *conductor*. Dicho grupo es una generalización del grupo de clases de ideales asociado al anillo de enteros y contiene información relevante sobre la artimética de ideales en el orden; demostraremos varias fórmulas para el número de elementos de este grupo (una para órdenes arbitrarios en cuerpos de números y otras más explícitas en órdenes más particulares) y encontraremos a través del conductor una estrecha relación entre éste y el grupo de clases de idesles, lo que permitirá aplicar *Teoría de Cuerpos de Clases* a órdenes. Por otra parte, el conductor veremos que captura información geométrica (sobre la regularidad de ideales primos) y que ésta se traduce en información aritmética (sobre la invertibilidad de éstos).

Por último, nos adentraremos en dos problemas clásicos: el *problema del número de clases* de Gauss y la Multiplicación Compleja (*Jugendtraum* de Kronecker). Para el primero desarrollaremos un algoritmo para clasificar órdenes en función del número de clases; para el segundo demostraremos la integralidad de los *módulos singulares*.

Abstract

Let K be a number field. An *order* in K is a subring $\mathcal{O}$ of the ring of integers of K that contains a basis of the extension $K/\mathbb{Q}$. Orders generalise the ring of integers, and in this project we shall study these objects from its basic algebraic properties (one-dimensional Noetherian rings with finite quotients by nonzero ideals) to its arithmetic properties.

In particular, we shall focus on the study of the *Picard group* of an order and its *conductor*. This group generalises the ideal class group attached to the ring of integers, and it contains relevant information regarding the ideal arithemtic of the order; in this regard, we shall prove various formulae for the number of elements of this group (one for arbitrary orders in number fields and others for more particular cases), and we shall find, by means of the conductor, a close connection between this group and the ideal class group, which provides the framework to apply Class Field Theory to orders. On the other hand, we shall see how the conductor captures geometric information of the order (concerning the regularity of prime ideals) and how this translates to arithmetic information (regarding the invertibility of prime ideals).

Lastly, we shall delve into two classical problems: Gauss' *class number problem* and *complex multiplication* (Kronecker's *Jugendtraum*). For the first one, we shall develop an algorithm which classifies imaginary quadratic orders in terms of their class number; for the latter, we shall prove the integrality of *singular modules*.

Índice general

Notación y tabla de símbolos

El término *anillo* se usará siempre para referirse a un anillo conmutativo y unitario y todos los homomorfismos de anillos llevan la unidad en la unidad. Introducimos a continuación los símbolos más frecuentes en el texto:

$\mathbb{N}$	Números naturales (sin incluir 0).
$\subseteq, \subset$	Inclusión e inclusión propia.
$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{A}$	Ideales de un anillo.
$\mathfrak{p}, \mathfrak{q}, \mathfrak{P}, \mathfrak{Q}$	Ideales primos de un anillo.
$\mathfrak{m}, \mathfrak{M}$	Ideales maximales de un anillo.
$A^\times$	Grupo de unidades del anillo A.
$S^{-1}A$	Localización de A en un subconjunto multiplicativo $S \subseteq A$.
$A_\mathfrak{p}$	Localización de A en $S = A \setminus \mathfrak{p}$.
$[G : H]$	Índice del subgrupo H en el grupo G.
L/K	Extensión de cuerpos.
$[L : K]$	Grado de la extensión L/K.
$\mathrm{Gal}(L/K)$	Grupo de Galois de L/K.
$\mathrm{Tr}_{L/K}$	Traza de L/K.
$\mathrm{N}_{L/K}$	Norma de L/K.
$\mathcal{O}_K$	Anillo de enteros del cuerpo de números K.
$\mathcal{O}$	Orden en un cuerpo de números K.
$\mathfrak{f}$	Conductor de un orden.
$J_K, J(\mathcal{O})$	Grupo de ideales fraccionarios no nulos de $\mathcal{O}_K$, resp. de $\mathcal{O}$.
$P_K, P(\mathcal{O})$	Grupo de ideales fraccionarios principales no nulos de $\mathcal{O}_K$, resp. de $\mathcal{O}$.
Cl_K	Grupo de clases de ideales de $\mathcal{O}_K$.
$Cl_K(\mathfrak{f})$	Grupo de clases de ideales relativo al conductor.
$\mathrm{Pic}(\mathcal{O})$	Grupo de Picard de $\mathcal{O}$.
$\mathrm{Pic}(\mathcal{O}, \mathfrak{f})$	Grupo de Picard relativo al conductor.
$h_K, h(\mathcal{O})$	Número de clases de K, resp. de $\mathcal{O}$.
$\mathfrak{N}$	Norma de ideales.
$j(\mathfrak{a})$	j-invariante del ideal fraccionario $\mathfrak{a}$ de un orden imaginario cuadrático.
$\mathcal{L}_\mathcal{O}$	Conjunto de retículos con multiplicación compleja por $\mathcal{O}$ salvo homotecia.
$\mathrm{End}(\Lambda)$	Endomorfismos del retículo Λ.

Introducción

Uno de los objetos fundamentales de la Teoría Algebraica de Números es el *anillo de enteros* $\mathcal{O}_K$ asociado a un cuerpo de números K (es decir, una extensión finita $K/\mathbb{Q}$), formado por todos los números complejos que sean raíz de un polinomio mónico con coeficientes enteros. Estos son ejemplos de dominios de Dedekind (esto es, dominios noetherianos y normales en los que todo ideal primo no nulo es maximal, cf. A.1.3). Nos centraremos en dos cuestiones: los ideales de este anillo y sus unidades.

Los ideales de $\mathcal{O}_K$ formalizan la noción de *número ideal* propuesta por Ernst Kummer para probar el último teorema de Fermat para primos regulares. Con ellos se construye un grupo abeliano Cl_K, denominado el *grupo de clases de ideales* (o *grupo de clases*), que mide lo lejos que están los números ideales de ser números en el sentido usual; en términos modernos, miden la obstrucción de los ideales de $\mathcal{O}_K$ para ser principales, teniéndose que $\mathcal{O}_K$ es un dominio de ideales principales si y sólo si Cl_K es el grupo trivial. Uno de los resultados más importantes acerca de este grupo es que es un grupo finito (Teorema A.52); su número de elementos h_K se denomina el *número de clases*.

Además, si K es un cuerpo cuadrático, su discriminante d_K es 0 ó 1 módulo 4 y $d_K/4$ (resp. d_K) es libre de cuadrados, por lo que es un *discriminante fundamental*; recíprocamente, para cada discriminante fundamental podemos encontrar un cuerpo cuadrático ($\mathbb{Q}(\sqrt{d_K})$ ó $\mathbb{Q}(\sqrt{d_K/4})$) con dicho discriminante. De hecho, tenemos un isomorfismos entre el grupo de clases Cl_K de un cuerpo cuadrático imaginario y el grupo de formas cuadráticas[1] binarias primitivas definidas positivas de discriminante d_K bajo una relación de equivalencia definida por una acción de $\mathrm{SL}_2(\mathbb{Z})$. Esto permitiría estudiar las formas cuadráticas binarias y la representabilidad de enteros por ellas mediante los anillos de enteros; sin embargo, sólo abarcaría las formas con discriminante fundamental.

Por otra parte, el Teorema de unidades de Dirichlet (Teorema A.54) determina la estructura de grupo de las unidades de $\mathcal{O}_K$, teniéndose que $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$, donde $\mu(K)$ es el grupo de las raíces de la unidad contenidas en K, r es el número de morfismos reales y s es el número de pares conjugados de morfismos complejos.

Estos dos grupos entran en conjunción para describir los números ideales mediante la sucesión exacta de grupos abelianos

$$1 \longrightarrow \mathcal{O}_K^\times \longrightarrow K^\times \longrightarrow J_K \longrightarrow Cl_K \longrightarrow 1,$$

[1] Recordemos que una forma cuadrática binaria es de la forma $f(x,y) = ax^2 + bxy + cy^2$ para ciertos $a, b, c \in \mathbb{Z}$. Su discriminante es $b^2 - 4ac$, se dice primitiva si el máximo común divisor de a, b y c es 1 y se dice definida positiva si toma valores positivos para $(x,y) \neq 0$. Dos formas cuadráticas binarias f y g se dicen equivalentes si existe $A \in \mathrm{SL}_2(\mathbb{Z})$ tal que $f(x,y) = g(A(x,y))$.

donde J_K es el grupo de *ideales fraccionarios* de K, que podemos entender como los números ideales de K. Es decir, las unidades determinan la pérdida de información al pasar a números ideales (recordemos que todas las unidades de un anillo generan el mismo ideal) y el grupo de clases mide *cuántos* números ideales no son números de K.

No obstante, fijado un cuerpo de números K, digamos $K = \mathbb{Q}(i)$ por concretitud, el anillo de enteros $\mathcal{O}_K = \mathbb{Z}[i]$ no es el único subanillo de interés de K. ¿Qué podemos decir de $\mathbb{Z}[i/3]$ y $\mathbb{Z}[i/2]$ ó de $\mathbb{Z}[2i]$ y $\mathbb{Z}[3i]$? Los dos primeros se pueden obtener como localizaciones de $\mathcal{O}_K$, que siguen siendo dominios de Dedekind y se pueden estudiar de forma similar; los segundos, sin embargo, son una clase distinta de anillos: los *órdenes*. Estos ya no serán dominios de Dedekind (en concreto perderán la propiedad de ser normales), lo que dificultará su estudio al no poder aplicarse resultados como el Teorema de factorización única de ideales (Teorema A.29) o el Teorema de invertibilidad de ideales (Teorema A.27). Además, como veremos más adelante, los órdenes en cuerpos cuadráticos alcanzan todos los posibles discriminantes de formas binarias cuadráticas (es decir los enteros congruentes con 0 ó 1 módulo 4) y, aunque no lo estudiaremos, es posible extender a ellos la equivalencia con dichas formas cuadráticas (cf. [6, II. Teorema 7.7.]) y dar un tratamiento moderno de los estudios de Carl Friedrich Gauss sobre éstas en sus *Disquisitiones Arithmeticae*.

En el Capítulo 1, demostraremos las propiedades principales de los órdenes y construiremos un grupo análogo al grupo de clases, que denominaremos *grupo de Picard*. Al igual que el grupo de clases, éste nos dará información sobre la aritmética de ideales en un orden y, de hecho, este grupo de Picard estará estrechamente relacionado con el grupo de clases del cuerpo de fracciones del orden. Encontraremos una fórmula explícita para el número de clases del grupo de Picard de un orden en términos del número de clases de su cuerpo de fracciones y otras cantidades asociadas a ellos. Entre estas, destacamos el grupo de unidades del orden, que como veremos tiene el mismo rango que el del anillo de enteros, y el *ideal conductor*, que es un ideal que captura información relevante sobre la aritmética de ideales en el orden. Posteriormente estudiaremos este ideal conductor en más detalle, entendiendo a través de él qué ideales del orden tienen factorización única, cuáles son los primos *regulares* del orden y estableciendo cierta correspondencia entre los ideales del orden y del anillo de enteros, además de sus correspondientes normas de ideales.

En el Capítulo 2, estudiaremos en mayor profundidad el caso particular de los órdenes de la forma $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$, que generalizan el caso cuadrático, para los que podremos obtener información más detallada sobre su estructura de ideales y grupo de Picard, llegando a una forma más explícita de la fórmula del número de clases obtenida anteriormente para órdenes en cuerpos de números que depende de la factorización en $\mathcal{O}_K$ de los ideales principales generados por primos de $\mathbb{Z}$ que dividen al conductor. Posteriormente, aplicaremos esta fórmula del número de clases al caso cuadrático, para el que podremos obtener la factorización de los primos de $\mathbb{Z}$ en términos del símbolo de Kronecker; con esto, será posible dar un algoritmo que permite clasificar de forma eficaz todos los órdenes imaginarios cuadráticos con un número de clases dado. Este algoritmo ha sido desarrollado por el autor de esta memoria en base a un trabajo de Janis Klaise [11] y supone una mejora sustancial en cuanto a eficiencia con respecto a los previamente existentes. Usaremos dicho algoritmo y la clasificación de todos los anillos de enteros con números de clases ≤ 100 de Mark Watkins ([23], [24]) para clasificar usando `SageMath` [22] todos los órdenes en cuerpos cuadráticos imaginarios con número de clases ≤ 100; además, calcularemos numéricamente usando `Magma` [3] un polinomio $H(x)$ asociado a cada uno de estos órdenes en función de

su grupo de Picard y la *función modular elíptica* j, que le asocia un número complejo a cada una de sus clases (Tablas 2.1, B.1 y B.2).

En el Capítulo 3, veremos por qué los polinomios $H(x)$ asociados a cada orden imaginario cuadrático son mónicos con coeficientes enteros, lo que nos da que, para cada ideal $\mathfrak{a}$ del orden, $j(\mathfrak{a})$ es un entero algebraico con grado igual al número de clases del orden. Para ello, comenzaremos presentando brevemente la teoría de retículos en $\mathbb{C}$ y daremos las principales propiedades de la función j; posteriormente, se estudiará la relación entre los grupos de Picard de órdenes en cuerpos cuadráticos imaginarios y cierta clase de retículos (los que tienen *multiplicación compleja*), lo que nos permitirá demostrar la algebricidad de $j(\mathfrak{a})$. No obstante, la demostración de la integralidad de $j(\mathfrak{a})$ no la podremos dar en su totalidad y usaremos para ella el Teorema principal de la Multiplicación Compleja, que explica el *Jugendtraum* de Leopold Kronecker [12].

Por último, se han incluido todos los resultados necesarios de Álgebra Conmutativa y Teoría Algebraica de Números (en su mayoría con demostración) en el Apéndice A y todo el código utilizado, así como las tablas mencionadas anteriormente para números de clases 2 y 3 en el Apéndice B.

Cabe mencionar, que por motivos de extensión, se han exluido otros temas de interés y algunas de las demostraciones del Capítulo 3; entre ellas, destacamos la demostración del Teorema principal de la Multiplicación Compleja y la integralidad de j sobre retículos con multiplicación compleja, para lo cual nos referimos a [18, Capítulo II]. Por otra parte, entre los temas excluidos destacamos ahondar en la aplicación de la *Teoría de Cuerpos de clases* a órdenes, el desarrollo de una fórmula de clases analítica (en términos del residuo de una función zeta) y profundizar en el estudio geométrico de los órdenes.

CAPÍTULO 1
Órdenes en cuerpos de números

> Why are numbers beautiful? It's like asking why is Beethoven's Ninth Symphony beautiful. If you don't see why, someone can't tell you. I know numbers are beautiful. If they aren't beautiful, nothing is.
>
> Paul Erdős

En este capítulo estudiaremos en general los órdenes en cuerpos de números, usando para ello primero su estructura algebraica de anillo noetheriano unidimensional, concluyendo a partir de ella una fórmula explícita para el *número de clases*, y a continuación trataremos de entender en mayor profundidad sus propiedades aritméticas mediante un ideal particular: el *conductor*.

1.1. Definición y propiedades básicas

A lo largo de esta sección, K denotará un cuerpo de números de grado n con anillo de enteros $\mathcal{O}_K$ (cf. A.40).

Definición 1.1. Un *orden* $\mathcal{O}$ en K es un subanillo de $\mathcal{O}_K$ que tiene rango n como $\mathbb{Z}$-módulo (i.e., contiene una base entera de n elementos).

Observación 1.2. *Los órdenes se pueden definir de forma más general en anillo arbitrarios y se podrían estudiar con mayor generalidad (entre estos podemos destacar por ejemplo los órdenes en álgebras de cuaternios, que surgen de forma natural en el estudio de curvas elípticas sobre cuerpos de característica positiva).*

Vemos en primer lugar que esta noción extiende la de anillo de enteros, pues $\mathcal{O}_K$ admite una base entera de longitud n (por Proposición A.39), por lo que es un orden de K, que, al ser todos los órdenes subanillos de éste, es el *orden maximal* u *orden principal* de K.

Ejemplos 1.3.

(a) Sea $f > 1$ un entero y consideremos $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$; escogiendo una base entera de $\mathcal{O}_K$ que contenga el 1 (por ejemplo $\{1, \theta, ..., \theta^{n-1}\}$ con $\theta \in \mathcal{O}_K$ un elemento

primitivo de $K/\mathbb{Q}$), tenemos que $\mathcal{O}$ está generado sobre $\mathbb{Z}$ por 1 y los elementos distintos de 1 de esta base multiplicados por f. Por lo que $\mathcal{O}$ es un subanillo de $\mathcal{O}_K$ que contiene una base entera de n elementos, i.e., es un orden no maximal de K. Esto incluye en particular los que denominaremos *órdenes cuadráticos*: $\mathcal{O} = \mathbb{Z} + f\mathbb{Z}[\sqrt{D}]$ u $\mathcal{O} = \mathbb{Z} + f\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ en función de la congruencia módulo 4 de D (cf. A.55).

(b) Si en lugar de un sólo entero f consideramos $m_1, ..., m_{n-1}$ enteros positivos y $1, \omega_1, ..., \omega_{n-1}$ una base entera de $\mathcal{O}_K$, por la misma argumentación de antes $\mathcal{O} = \mathbb{Z} + \mathbb{Z}m_1\omega_1 + ... + \mathbb{Z}m_{n-1}\omega_{n-1}$ es un orden en K.

Aunque parezca que hemos perdido mucha estructura al permitir otros subanillos de $\mathcal{O}_K$, los órdenes generalizan al anillo de enteros sin perder todas las propiedades deseables de los dominios de Dedekind; sólo dejan de ser normales:

Proposición 1.4. *Sea $\mathcal{O}$ un orden en K; $\mathcal{O}$ es noetheriano y de dimensión (de Krull) 1.*

Demostración. Es análoga a la demostración para el anillo de enteros (cf. Teorema A.43): Como $\mathcal{O}$ es un $\mathbb{Z}$-módulo finitamente generado, es un $\mathbb{Z}$-módulo Noetheriano, por lo que todo ideal $\mathfrak{a}$ de $\mathcal{O}$ es finitamente generado como $\mathbb{Z}$-módulo y, por lo tanto, como $\mathcal{O}$-modulo; luego $\mathcal{O}$ es un anillo Noetheriano.
Si $\mathfrak{p} \neq 0$ es un primo de $\mathcal{O}$, $\mathfrak{p} \cap \mathbb{Z} \neq 0$ (pues si $a \in \mathfrak{p} \subseteq \mathcal{O}_K$ es no nulo, existe una ecuación mónica con coeficientes enteros que satisface con término independiente no nulo, por lo que el término independiente es un entero en $\mathfrak{p}$), por lo que $\mathfrak{p} \cap \mathbb{Z}$ es maximal y por la Proposición A.22 tenemos que $\mathfrak{p}$ es maximal. □

Ahora bien, si $\mathcal{O}$ es normal, tendría que ser el orden maximal $\mathcal{O}_K$ (si $\alpha \in \mathcal{O}_K$, α es un entero algebraico por definición de $\mathcal{O}_K$ y, como $\mathcal{O}$ es normal, $\alpha \in \mathcal{O}$). Por lo que en general $\mathcal{O}$ no va a ser un dominio de factorización única (pues esto implicaría que es normal por la Proposición A.20) y ni siquiera un dominio de Dedekind, por lo que tampoco habrá factorización única de ideales ni todos sus ideales serán invertibles (cf. Teorema A.29).

Observamos por otra parte que las localizaciones de un $\mathcal{O}_K$ son dominios de Dedekind (por lo que son dominios noetherianos unidimensionales[1] normal), pero que en general ya no serán enteras sobre $\mathbb{Z}$; por el contrario, como hemos visto, los órdenes son dominios noetherianos unidimensionales que siguen siendo enteros sobre $\mathbb{Z}$, pero ya no son normal. Así pues, estudiaremos en la siguiente sección los dominios noetherianos unidimensionales, que es una generalización de ambos conceptos, con el objetivo de dar una fórmula para el *número de clases* de un orden. No obstante, antes de concluir esta sección veremos alguna otra propiedad fundamental de los órdenes:

Proposición 1.5. *Sea $\mathcal{O}$ un orden en K y sea $\mathfrak{a} \neq 0$ un ideal de $\mathcal{O}$. $\mathcal{O}/\mathfrak{a}$ es un anillo finito.*

Demostración. Sea $a \in \mathfrak{a}$ un elemento no nulo; entonces $a \mid \mathrm{N}_{K/\mathbb{Q}}(a)$ (por definición de la norma) y, así, $(\mathrm{N}_{K/\mathbb{Q}}(a)) \subseteq \mathfrak{a}$ por lo que

$$\#(\mathcal{O}/\mathfrak{a}) \leq \#(\mathcal{O}/(a)) \leq \#(\mathcal{O}/\mathrm{N}_{K/\mathbb{Q}}(a)\mathcal{O}) = \#(\mathbb{Z}^n/\mathrm{N}_{K/\mathbb{Q}}(a)\mathbb{Z}^n),$$

donde $n = [K : \mathbb{Q}]$, que es un grupo finito. □

[1] Excluimos aquí el caso $S = \mathcal{O}_K \setminus \{0\}$.

Con esto, el Teorema de correspondencia para anillos nos da el siguiente corolario:

Corolario 1.6. *Sea $\mathcal{O}$ un orden en K y sea $\mathfrak{a} \neq 0$ un ideal de $\mathcal{O}$. Entonces hay a lo sumo un número finito de ideales primos de $\mathcal{O}$ que contienen a $\mathfrak{a}$.*

1.2. Dominios noetherianos unidimensionales

En esta sección, $\mathcal{O}$ denotará un dominio noetheriano unidimensional con cuerpo de fracciones K, $\tilde{\mathcal{O}}$ denotará su normalización, que suponemos finita como $\mathcal{O}$-módulo, y $\mathcal{O}_\mathfrak{p}$ su localización en $S = \mathcal{O} \setminus \mathfrak{p}$ (cf. Ejemplo A.7).

1.2.1. Propiedades básicas

Comenzamos demostrando una versión del Teorema chino del resto[2]:

Proposición 1.7. *Si $\mathfrak{a} \neq 0$ es un ideal de $\mathcal{O}$,*

$$\mathcal{O}/\mathfrak{a} \cong \bigoplus_{\mathfrak{p}} \mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p} = \bigoplus_{\mathfrak{p} \supseteq \mathfrak{a}} \mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p}.$$

Demostración. Sea $\tilde{\mathfrak{a}}_\mathfrak{p} = \mathcal{O} \cap \mathfrak{a}\mathcal{O}_\mathfrak{p}$. Observamos en primer lugar que $\mathfrak{a} \subseteq \mathfrak{p}$ sólo para un número finito de primos $\mathfrak{p}$ (por el Corolario 1.6) y, para el resto, $\mathfrak{a}\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ (por la Proposición A.9), de forma que $\tilde{\mathfrak{a}}_\mathfrak{p} = \mathcal{O}$. Además, si $a \in \bigcap_\mathfrak{p} \tilde{\mathfrak{a}}_\mathfrak{p} = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}} \tilde{\mathfrak{a}}_\mathfrak{p}$, el ideal $\mathfrak{b} = \{x \in \mathcal{O} \,|\, xa \in \mathfrak{a}\}$ no está contenido en ningún ideal maximal $\mathfrak{p}$, por lo que $\mathfrak{b} = \mathcal{O}$ y, por tanto, $a = 1 \cdot a \in \mathfrak{a}$, luego $\bigcap_\mathfrak{p} \tilde{\mathfrak{a}}_\mathfrak{p} = \mathfrak{a}$ (el otro contenido se sigue de que $\mathfrak{a} \subseteq \tilde{\mathfrak{a}}_\mathfrak{p}$ para todo primo $\mathfrak{p}$). Con esto, aplicando la correspondencia de ideales primos de $\mathcal{O}$ y de $\mathcal{O}_\mathfrak{p}$ (Corolario A.10), para cada $\mathfrak{p} \supseteq \mathfrak{a}$, $\mathfrak{p}$ es el único ideal primo de $\mathcal{O}$ que contiene a $\tilde{\mathfrak{a}}_\mathfrak{p}$. Por lo que si $\mathfrak{p}$ y $\mathfrak{q}$ son ideales primos (no nulos) distintos de $\mathcal{O}$, $\tilde{\mathfrak{a}}_\mathfrak{p} + \tilde{\mathfrak{a}}_\mathfrak{q}$ no puede estar contenido en ningún ideal maximal de $\mathcal{O}$ y, por tanto, $\tilde{\mathfrak{a}}_\mathfrak{p} + \tilde{\mathfrak{a}}_\mathfrak{q} = \mathcal{O}$ (i.e., son coprimos). Así, el Teorema chino del resto[3] (Teorema A.2) nos da que

$$\mathcal{O}/\mathfrak{a} \cong \bigoplus_{\mathfrak{p} \supseteq \mathfrak{a}} \mathcal{O}/\tilde{\mathfrak{a}}_\mathfrak{p}$$

Por último, por la Proposición A.9 y el Corolario A.10, $\mathcal{O}/\tilde{\mathfrak{a}}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p}$ y el teorema se sigue. □

Ahora, si $\mathcal{O}$ no es un dominio de Dedekind, no todos sus ideales serán invertibles (cf. Teorema A.27), por lo que en general el grupo de ideales no contendrá todos los ideales fraccionarios de $\mathcal{O}$; no obstante, sigue teniendo sentido (cf. Definición A.28) el grupo de ideales invertibles $J(\mathcal{O})$. De hecho, el inverso sigue teniendo la misma forma:

Proposición 1.8. *Si $\mathfrak{a} \subset \mathcal{O}$, $\{x \in K : x\mathfrak{a} \subseteq \mathcal{O}\} \supset \mathcal{O}$; además, si $\mathfrak{a}$ es un ideal fraccionario invertible, $\mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subseteq \mathcal{O}\}$.*

[2] Si tomamos $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \ldots \mathfrak{p}_r^{\nu_r}$ con los $\mathfrak{p}_j$ ideales primos no nulos distintos, entonces $\mathcal{O}_{\mathfrak{p}_j}/\mathfrak{a}\mathcal{O}_{\mathfrak{p}_j} = \mathcal{O}_{\mathfrak{p}_j}/\mathfrak{p}_j\mathcal{O}_{\mathfrak{p}_j} = \mathcal{O}/\mathfrak{p}_j$ y recuperamos la versión usual (cf. Teorema A.2).

[3] Nótese que hemos usado que sólo hay un número finito de primos que contienen a $\mathfrak{a}$ y la suma directa es finita.

Demostración. La demostración es esencialmente igual al caso de dominios de Dedekind: Si $\mathfrak{a}$ es invertible, $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$, por lo que $\mathfrak{a}^{-1} \subseteq \{x \in K : x\mathfrak{a} \subseteq \mathcal{O}\}$ y, multiplicando por $\mathfrak{a}$, $\mathcal{O} \subseteq \mathfrak{a}\{x \in K : x\mathfrak{a} \subseteq \mathcal{O}\} \subseteq \mathcal{O}$. Por otra parte, si $\mathfrak{a} \subset \mathcal{O}$, tomamos un ideal maximal $\mathfrak{p} \supseteq \mathfrak{a}$, de forma que $\{x \in K : x\mathfrak{p} \subseteq \mathcal{O}\} \subseteq \{x \in K : x\mathfrak{p} \subseteq \mathcal{O}\}$, por lo que basta probarlo para $\mathfrak{p}$; pero si $\{x \in K : x\mathfrak{p} \subseteq \mathcal{O}\} = \mathcal{O}$, tenemos que $\mathfrak{p}\{x \in K : x\mathfrak{p} \subseteq \mathcal{O}\} = \mathfrak{p}$, que es una contradicción: tomamos $a \in \mathfrak{p}$ y $\mathfrak{p}_1...\mathfrak{p}_r \subseteq (a)$ ideales primos no nulos con r minimal (existen por ser $\mathcal{O}$ noetheriano), entonces por primalidad existe j tal que $\mathfrak{p}_j \subseteq \mathfrak{p}$ y, por ser $\mathcal{O}$ de dimensión 1, $\mathfrak{p}_j = \mathfrak{p}$, digamos $j = 1$; así, como r es minimal $\mathfrak{p}_2...\mathfrak{p}_r \not\subseteq (a)$, por lo que existe $b \in \mathfrak{p}_2...\mathfrak{p}_r$ tal que $b \notin (\mathfrak{a})$ y, por tanto, $a^{-1}b \notin \mathcal{O}$, pero $a^{-1}b \in \{x \in K : x\mathfrak{p} \subseteq \mathcal{O}\}$ y, por tanto, $\{x \in K : x\mathfrak{p} \subseteq \mathcal{O}\} \neq \mathcal{O}$. □

Además, la invertibilidad se puede caracterizar localmente:

Proposición 1.9. *Un ideal fraccionario $\mathfrak{a}$ de $\mathcal{O}$ es invertible si y sólo si $\mathfrak{a}_\mathfrak{p} = \mathfrak{a}\mathcal{O}_\mathfrak{p}$ es un ideal principal de $\mathcal{O}_\mathfrak{p}$ para todo ideal primo no nulo $\mathfrak{p}$ de $\mathcal{O}$.*

Demostración. Sea $\mathfrak{a}$ un ideal invertible de $\mathcal{O}$ y tomemos $\mathfrak{b}$ otro ideal fraccionario invertible tal que $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. Existen $a_1, ..., a_r \in \mathfrak{a}$ y $b_1, ..., b_r \in \mathfrak{b}$ tales que

$$1 = a_1b_1 + ... + a_rb_r.$$

Además, para cierto i, $a_ib_i \notin \mathfrak{p}\mathcal{O}_\mathfrak{p}$, por lo que $a_ib_i \in \mathcal{O}_\mathfrak{p}^\times$, y, por tanto, dado $x \in \mathfrak{a}_\mathfrak{p}$, $xb_i \in \mathfrak{a}_\mathfrak{p}\mathfrak{b} = \mathcal{O}$, luego $x = xb_i(b_ia_i)^{-1}a_i \in a_i\mathcal{O}_\mathfrak{p}$. Concluimos así que $\mathfrak{a}_\mathfrak{p} = a_i\mathcal{O}_\mathfrak{p}$, i.e., es principal. Recíprocamente, supongamos que $\mathfrak{a}_\mathfrak{p}$ es principal para todo $\mathfrak{p}$, digamos $\mathfrak{a}_\mathfrak{p} = a_\mathfrak{p}\mathcal{O}_\mathfrak{p}$ para cierto $a_\mathfrak{p} \in K^\times$. Podemos suponer además que $a_\mathfrak{p} \in \mathfrak{a}$. Si $\mathfrak{a}\mathfrak{a}^{-1} \neq \mathcal{O}$, existiría un ideal maximal $\mathfrak{p}$ de $\mathcal{O}$ con $\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{p} \subset \mathcal{O}$. Sean $a_1, ..., a_n \in \mathfrak{a}$ generadores de $\mathfrak{a}$ (recordemos que $\mathcal{O}$ es noetheriano, por lo que todo ideal es finitamente generado), y tomemos $s_i \in \mathcal{O} \setminus \mathfrak{p}$, $b_i \in \mathcal{O}$ tales que $a_i = a_pb_i/s_i$ ($a_i \in \mathfrak{a} \subseteq \mathfrak{a}_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}\mathcal{O}_\mathfrak{p}$), luego $s_ia_i \in \mathfrak{a}_\mathfrak{p}\mathcal{O}$. Por lo que si definimos $s = s_1...s_n$, $sa_\mathfrak{p}^{-1}\mathfrak{a} \subseteq \mathcal{O}$ y $sa_\mathfrak{p}^{-1} \in \mathfrak{a}^{-1}$; así, $s \in \mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathfrak{p}$, que contradice que $s \in \mathcal{O} \setminus \mathfrak{p}$. Luego $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$, i.e., $\mathfrak{a}$ es invertible. □

1.2.2. Grupo de Picard y unidades

Nuestro propósito ahora es estudiar el *grupo de Picard* de los anillos noetherianos unidimensionales, que definimos de forma análoga al caso de anillo de enteros: El *grupo de Picard* (o grupo de clases de ideales) $\mathrm{Pic}(\mathcal{O})$ de un anillo noetheriano unidimensional $\mathcal{O}$ se define como el cociente de los ideales fraccionarios invertibles $J(\mathcal{O})$ con el subgrupo de ideales fraccionarios principales[4] $P(\mathcal{O})$; también denotaremos por $h(\mathcal{O}) = \#\,\mathrm{Pic}(\mathcal{O})$ al número de clases. Para ello seguiremos el desarrollo de Neukirch [15, I.§12.] y culminaremos este apartado demostrando para la finitud de este grupo en caso de órdenes con una fórmula (algebraica) explícita del número de clases. Sin embargo, antes de comenzar con la labor teórica, cabe observar que hay diferencias notables con el grupo de clases usual, pues si $\mathcal{O}$ es un DIP, obtenemos inmediatamente que $h(\mathcal{O}) = 1$, pero el recíproco no es cierto, ya que sólo estamos considerando los ideales invertibles, es decir, sólo tenemos el siguiente resultado:

Proposición 1.10. *$h(\mathcal{O}) = 1$ si y sólo si todo ideal invertible de $\mathcal{O}$ es principal.*

[4] Estos son trivialmente invertibles, pues si $\alpha \in K^\times$, $\alpha^{-1} \in K^\times$ y $(\alpha\mathcal{O})(\alpha^{-1}\mathcal{O}) = \mathcal{O}$.

Un ejemplo de esto es el orden $\mathcal{O} = \mathbb{Z} + 2\mathbb{Z}[i]$, que tiene número de clases 1 como veremos más adelante (cf. Ejemplo 1.23) y, sin embargo, $(2, 2i)$ es un ideal primo de $\mathcal{O}$ que se puede comprobar que no es principal, por lo que $(2, 2i)$ no es invertible.

Estudiaremos ahora, por medio de la localización, la estructura de los ideales fraccionarios de $\mathcal{O}$.

Proposición 1.11. *La correspondencia $\mathfrak{a} \mapsto (\mathfrak{a}_\mathfrak{p})_\mathfrak{p}$ induce un isomorfismo de grupos abelianos $J(\mathcal{O}) \cong \bigoplus_\mathfrak{p} P(\mathcal{O}_\mathfrak{p})$ (donde $\mathfrak{p}$ reccore los ideales primos de $\mathcal{O}$). Así, identificando $P(\mathcal{O})$ con su imagen, tenemos que* $\mathrm{Pic}(\mathcal{O}) \cong (\bigoplus_\mathfrak{p} P(\mathcal{O}_\mathfrak{p}))/P(\mathcal{O})$.

Demostración. Sea $\mathfrak{a} \in J(\mathcal{O})$; por la Proposición 1.9, $\mathfrak{a}_\mathfrak{p} = \mathfrak{a}\mathcal{O}_\mathfrak{p}$ es principal y se tiene que $\mathfrak{a}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ para todos salvo un número finito de primos $\mathfrak{p}$, luego el homomorfismo $J(\mathcal{O}) \to \bigoplus_\mathfrak{p} P(\mathcal{O}_\mathfrak{p})$ dado por $\mathfrak{a} \mapsto (\mathfrak{a}_\mathfrak{p})_\mathfrak{p}$ está bien definido.
Si la imagen de $\mathfrak{a}$ es trivial, i.e., $\mathfrak{a}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ para todo primo $\mathfrak{p}$ y $\mathfrak{a} \neq 0$, tenemos por la Proposición 1.7 que $\mathcal{O}/\mathfrak{a}$ es el anillo trivial, por lo que $\mathfrak{a} = \mathcal{O}$, luego la aplicación es inyectiva.
Sea ahora $(a_\mathfrak{p}\mathcal{O}_\mathfrak{p}) \in \bigoplus_\mathfrak{p} P(\mathcal{O}_\mathfrak{p})$, entonces el $\mathcal{O}$-submódulo $\mathfrak{a} = \bigcap_\mathfrak{p} a_\mathfrak{p}\mathcal{O}_\mathfrak{p}$ de K es un ideal fraccionario (pues $a_\mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ para casi todo $\mathfrak{p}$ y, por tanto, podemos tomar $c \in \mathcal{O}$ tal que $ca_\mathfrak{p}\mathcal{O}_\mathfrak{p} \subseteq \mathcal{O}_\mathfrak{p}$ para todo $\mathfrak{p}$; luego $c\mathfrak{a} \subseteq \bigcap_\mathfrak{p} \mathcal{O}_\mathfrak{p} = \mathcal{O}$). Ahora, si $d \in \mathcal{O} \setminus \{0\}$ es tal que $da_\mathfrak{p}^{-1}a_\mathfrak{q} \in \mathcal{O}$ para los $\mathfrak{q}$ tales que $a_\mathfrak{p}^{-1}a_\mathfrak{q} \notin \mathcal{O}$ (recordemos que sólo hay un número finito de estos), tenemos (por la Proposición 1.7) que existe un $a \in \mathcal{O}$ tal que $a \equiv d \pmod{\mathfrak{p}}$ y $a \in da_\mathfrak{p}^{-1}a_\mathfrak{q}\mathcal{O}_\mathfrak{q}$ para $\mathfrak{q} \neq \mathfrak{p}$, de forma que $\varepsilon = ad^{-1}$ es una unidad de $\mathcal{O}_\mathfrak{p}$ y $a_\mathfrak{p}\varepsilon \in \bigcap_\mathfrak{q} a_\mathfrak{q}\mathcal{O}_\mathfrak{q} = \mathfrak{a}$; luego $a_\mathfrak{p}\mathcal{O}_\mathfrak{p} = (a_\mathfrak{p}\varepsilon)\mathcal{O}_\mathfrak{p} \subseteq \mathfrak{a}\mathcal{O}_\mathfrak{p}$. Así, $\mathfrak{a}\mathcal{O}_\mathfrak{p} = a_\mathfrak{p}\mathcal{O}_\mathfrak{p}$ para todo $\mathfrak{p}$ y, por tanto, la aplicación es suprayectiva. Llegamos, pues a que $J(\mathcal{O}) \cong \bigoplus_\mathfrak{p} P(\mathcal{O}_\mathfrak{p})$; tomando cocientes por $P(\mathcal{O})$ se sigue el resultado. □

Sabemos que $\tilde{\mathcal{O}}$ es normal y se puede comprobar de forma similar a la Proposición 1.4; no obstante, que sea un anillo noetheriano no es inmediato y es un caso particular del sigueinte resultado:

Teorema 1.12 (Krull-Akizuki)**.** *Sea L/K una extensión finita y sea $\tilde{\mathcal{O}}$ la clausura entera de $\mathcal{O}$ en L. La clausura entera de $\mathcal{O}$ en L es un dominio de Dedekind.*

Tomando $L = K$ en este teorema obtenemos directamente que $\tilde{\mathcal{O}}$ es un dominio de Dedekind; no obstante, como el caso que nos interesa es el de órdenes en cuerpos de números, en el cual $\tilde{\mathcal{O}} = \mathcal{O}_K$, no demostraremos este resultado y para su demostración nos referimos a [15, I. Proposición 12.8].

Observación 1.13. *En todos los resultados anteriores, la condición de que $\tilde{\mathcal{O}}$ sea un $\mathcal{O}$-módulo finito es innecesaria; sin embargo, en lo sucesivo será de fundamental importancia.*

Proposición 1.14. *Hay una sucesión exacta de grupos abelianos*

$$1 \longrightarrow \mathcal{O}^\times \longrightarrow \tilde{\mathcal{O}}^\times \longrightarrow \bigoplus_\mathfrak{p} \tilde{\mathcal{O}}_\mathfrak{p}^\times/\mathcal{O}_\mathfrak{p}^\times \longrightarrow \mathrm{Pic}(\mathcal{O}) \longrightarrow \mathrm{Pic}(\tilde{\mathcal{O}}) \longrightarrow 1.$$

donde $\mathfrak{p}$ reccore los ideales primos no nulos de $\mathcal{O}$ y $\tilde{\mathcal{O}}_\mathfrak{p}$ denota la clausura entera de $\mathcal{O}_\mathfrak{p}$ en K.

Demostración. Si $\tilde{\mathfrak{p}}$ recorre los ideales primos de $\tilde{\mathcal{O}}$, por la Proposición 1.11, tenemos un isomorfismo

$$(*) \qquad J(\tilde{\mathcal{O}}) \cong \bigoplus_{\tilde{\mathfrak{p}}} P(\tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}).$$

Si $\mathfrak{p}$ es un primo no nulo de $\mathcal{O}$, como $\tilde{\mathcal{O}}$ es un dominio de Dedekind por el Teorema de Krull-Akizuki, tenemos que $\mathfrak{p}\tilde{\mathcal{O}} = \tilde{\mathfrak{p}}_1^{e_1}...\tilde{\mathfrak{p}}_r^{e_r}$ (Teorema A.29), por lo que hay un número finito de ideales de $\tilde{\mathcal{O}}$ sobre $\mathfrak{p}$; análogamente, dado un ideal primo de $\mathcal{O}_{\mathfrak{p}}$ hay un número finito de ideales sobre éste en $\tilde{\mathcal{O}}_{\mathfrak{p}}$. Como todo ideal no nulo de $\tilde{\mathcal{O}}_{\mathfrak{p}}$ está sobre $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ (pues es el único ideal primo de $\mathcal{O}_{\mathfrak{p}}$), tenemos que $\tilde{\mathcal{O}}_{\mathfrak{p}}$ es un anillo de Dedekind con un número finito de ideales, y, por tanto, un DIP (por la Proposición A.30) y, usando de nuevo la Proposición 1.11,

$$(**) \qquad P(\tilde{\mathcal{O}}_{\mathfrak{p}}) = J(\tilde{\mathcal{O}}_{\mathfrak{p}}) \cong \bigoplus_{\tilde{\mathfrak{p}} \supseteq \mathfrak{p}} P(\tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}).$$

Y, juntando $(*)$ y $(**)$, llegamos a

$$J(\tilde{\mathcal{O}}) \cong \bigoplus_{\mathfrak{p}} \bigoplus_{\tilde{\mathfrak{p}} \supseteq \mathfrak{p}} P(\tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}) \cong \bigoplus_{\mathfrak{p}} P(\tilde{\mathcal{O}}_{\mathfrak{p}}),$$

donde $\mathfrak{p}$ recorre los primos de $\mathcal{O}$ y $\tilde{\mathfrak{p}}$ los de $\tilde{\mathcal{O}}$. Ahora, como para cualquier dominio A con cuerpo de fracciones K se tiene el isomorfismo natural $P(R) \cong K^\times/A^\times$, obtenemos el diagrama conmutativo de grupos abelianos con filas exactas

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times/\mathcal{O}^\times & \longrightarrow & \bigoplus_{\mathfrak{p}} K^\times/\mathcal{O}_{\mathfrak{p}}^\times & \longrightarrow & \mathrm{Pic}(\mathcal{O}) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & K^\times/\tilde{\mathcal{O}}^\times & \longrightarrow & \bigoplus_{\mathfrak{p}} K^\times/\tilde{\mathcal{O}}_{\mathfrak{p}}^\times & \longrightarrow & \mathrm{Pic}(\tilde{\mathcal{O}}) & \longrightarrow & 1, \end{array}$$

donde α, β y γ son las aplicaciones naturales inducidas por la inclusión. Por lo que podemos aplicar el Lema de la serpiente (Lema A.4) para obtener una sucesión exacta de grupos abelianos

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \ker\alpha & \longrightarrow & \ker\beta & \longrightarrow & \ker\gamma & & \\ & & & & & \overset{\delta}{\swarrow} & & & \\ & & \mathrm{coker}\,\alpha & \longrightarrow & \mathrm{coker}\,\beta & \longrightarrow & \mathrm{coker}\,\gamma & \longrightarrow & 1. \end{array}$$

Y, por una parte, α y β (y, por tanto γ) son suprayectivas, por lo que sus conúcleo son triviales; además, $\ker\alpha \cong \tilde{\mathcal{O}}^\times/\mathcal{O}^\times$ y $\ker\beta \cong \bigoplus_{\mathfrak{p}} \tilde{\mathcal{O}}_{\mathfrak{p}}^\times/\mathcal{O}_{\mathfrak{p}}^\times$, por lo que llegamos a la sucesión exacta

$$1 \longrightarrow \tilde{\mathcal{O}}^\times/\mathcal{O}^\times \longrightarrow \bigoplus_{\mathfrak{p}} \tilde{\mathcal{O}}_{\mathfrak{p}}^\times/\mathcal{O}_{\mathfrak{p}}^\times \longrightarrow \ker\gamma \xrightarrow{\delta} 1.$$

Por suprayectividad de γ y el primer teorema de isomorfía tenemos la sucesión exacta corta canónica

$$1 \longrightarrow \ker\gamma \longrightarrow \mathrm{Pic}(\mathcal{O}) \xrightarrow{\gamma} \mathrm{Pic}(\tilde{\mathcal{O}}) \longrightarrow 1,$$

que podemos componer con la anterior, llegando a

$$1 \longrightarrow \mathcal{O}^\times \longrightarrow \tilde{\mathcal{O}}^\times \longrightarrow \bigoplus_{\mathfrak{p}} \tilde{\mathcal{O}}_{\mathfrak{p}}^\times/\mathcal{O}_{\mathfrak{p}}^\times \longrightarrow \mathrm{Pic}(\mathcal{O}) \longrightarrow \mathrm{Pic}(\tilde{\mathcal{O}}) \longrightarrow 1,$$

como queríamos probar. □

Estudiaremos ahora este término central, para lo cual necesitaremos entender mejor las localizaciones en primos de estos anillos; para esto será necesario ver qué sucede en los primos *malos*, es decir, en los que impiden que $\mathcal{O}$ sea un dominio de Dedekind, o lo que es lo mismo, en los que $\mathcal{O}_\mathfrak{p}$ no es un anillo de valoración discreta (cf. Teorema A.27).

Definición 1.15. Decimos que un primo $\mathfrak{p} \neq 0$ de $\mathcal{O}$ es *regular* si $\mathcal{O}_\mathfrak{p}$ es normal (en virtud de las Proposición A.11 y el Corolario A.10 esto basta para que $\mathcal{O}_\mathfrak{p}$ sea un anillo de valoración discreta por el Teorema A.16).

Ahora, si $\mathfrak{p}$ es un primo regular, $\mathcal{O}_\mathfrak{p}$ es un anillo de valoración discreta y, en particular, $\tilde{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$, de donde se sigue que los sumandos correspondientes a primos regulares en el término intermedio de la sucesión exacta anterior son triviales.

Por otra parte, el ideal que nos servirá para estudiar los primos irregulares se denomina el *conductor*:

Definición 1.16. Definimos el *conductor* de $\mathcal{O}$ por $\mathfrak{f} = \{a \in \tilde{\mathcal{O}} \mid a\tilde{\mathcal{O}} \subseteq \mathcal{O}\}$.

Observación 1.17. *Por una parte, como $\tilde{\mathcal{O}}$ es un $\mathcal{O}$-módulo finitamente generado, $\mathfrak{f} \neq 0$; por otra, el conductor es el ideal más grande de $\tilde{O}$ contenido en $\mathcal{O}$ (si $\mathfrak{a}$ es un ideal de $\tilde{\mathcal{O}}$ y $\mathfrak{a} \subseteq \mathcal{O}$, para todo $a \in \mathfrak{a}$ $a\mathcal{O}_K \subseteq \mathfrak{a} \subseteq \mathcal{O}$, luego $a \in \mathfrak{f}$).*

Tenemos con esto el siguiente criterio:

Proposición 1.18. *Un ideal primo $\mathfrak{p} \neq 0$ de $\mathcal{O}$ es regular si y sólo si $\mathfrak{f} \not\subseteq \mathfrak{p}$. Además, si $\mathfrak{p}$ es regular, $\tilde{\mathfrak{p}} = \mathfrak{p}\tilde{\mathcal{O}}$ es un ideal primo de $\mathcal{O}$ y $\mathcal{O}_\mathfrak{p} = \tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}$.*

Demostración.
($\Longrightarrow$): Supongamos que $\mathfrak{f} \not\subseteq \mathfrak{p}$ y sea $t \in \mathfrak{f} \setminus \mathfrak{p}$. Por definición del conductor, $t\tilde{\mathcal{O}} \subseteq \mathcal{O}$, por lo que $\tilde{\mathcal{O}} \subseteq t^{-1}\mathcal{O} \subseteq \mathcal{O}_\mathfrak{p}$. Ahora, si $\mathfrak{m} = \mathfrak{p}\mathcal{O}_\mathfrak{p}$ es el ideal maximal de $\mathcal{O}_\mathfrak{p}$, $\tilde{\mathfrak{p}} = \mathfrak{m} \cap \tilde{\mathcal{O}}$ es un ideal primo de $\tilde{\mathcal{O}}$ tal que $\mathfrak{p} \subseteq \tilde{\mathfrak{p}} \cap \mathcal{O}$, por lo que por maximalidad $\mathfrak{p} = \tilde{\mathfrak{p}} \cap \mathcal{O}$; así, $\mathcal{O}_\mathfrak{p} \subseteq \tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}$. Si $a/s \in \tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}$ con $a \in \tilde{\mathcal{O}}$ y $s \in \tilde{\mathcal{O}} \setminus \tilde{\mathfrak{p}}$, entonces $ta \in \mathcal{O}$ y $ts \in \mathcal{O} \setminus \mathfrak{p}$, por lo que $a/s = (ta)/(ts) \in \tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}$ y concluimos así que $\mathcal{O}_\mathfrak{p} = \tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}$. Como $\tilde{\mathcal{O}}$ es un dominio de Dedekind, tenemos que $\tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}} = \mathcal{O}_\mathfrak{p}$ es un dominio de valoración discreta (por el Teorema A.27) y, por tanto, $\mathfrak{p}$ es un primo regular.
Tenemos en este caso que si $\tilde{\mathfrak{q}}$ es otro ideal de $\tilde{\mathcal{O}}$ sobre $\mathfrak{p}$, $\tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}} = \mathcal{O}_\mathfrak{p} \subseteq \tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}$ y, por tanto, $\tilde{\mathfrak{p}} = \tilde{\mathcal{O}} \cap \tilde{\mathfrak{p}}\tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}} \subseteq \tilde{\mathcal{O}} \cap \mathfrak{q}\tilde{\mathcal{O}}_{\tilde{\mathfrak{q}}} = \tilde{\mathfrak{q}}$, luego $\tilde{\mathfrak{p}} = \tilde{\mathfrak{q}}$ (por maximalidad). Por lo que tenemos la factorización en primos $\mathfrak{p}\tilde{\mathcal{O}} = \tilde{\mathfrak{p}}^e$ con $e \geq 1$ y con esto, usando que se tiene que $\mathfrak{m} = \mathfrak{p}\mathcal{O}_\mathfrak{p} = (\mathfrak{p}\tilde{\mathcal{O}})\mathcal{O}_\mathfrak{p} = \tilde{\mathfrak{p}}^e\mathcal{O}_\mathfrak{p} = \mathfrak{m}^e$, concluimos que $e = 1$ y, así, $\tilde{\mathfrak{p}} = \mathfrak{p}\tilde{\mathcal{O}}$.
($\Longleftarrow$): Supongamos ahora que $\mathfrak{p}$ es un primo regular (i.e., $\mathcal{O}_\mathfrak{p}$ es un dominio de valoración discreta). Tenemos entonces que $\mathcal{O}_\mathfrak{p}$ es normal y, como $\tilde{\mathcal{O}}$ es entero sobre $\mathcal{O}$, $\tilde{\mathcal{O}} \subseteq \mathcal{O}_\mathfrak{p}$. Sea $x_1, ...x_n$ un sistema de generadores de $\tilde{\mathcal{O}}$ como $\mathcal{O}$-módulo y tomemos $a_i \in \mathcal{O}$ y $s_i \in \mathcal{O} \setminus \mathfrak{p}$ tales que $x_i = a_i/s_i$; luego, si definimos $s = s_1...s_n$, $s\tilde{\mathcal{O}} \subseteq \mathcal{O}$, lo que implica que $s \in \mathfrak{f} \setminus \mathfrak{p}$ y, por tanto, $\mathfrak{f} \not\subseteq \mathfrak{p}$. □

Como corolario inmediato tenemos por que hay a lo sumo un número finito de primos no regulares:

Corolario 1.19. *Hay un número finito de primos irregulares en $\mathcal{O}$.*

Demostración. Por el Corolario 1.6, hay un número finito de primos que contienen al conductor y por la proposición anterior (Proposición 1.18) los primos irregulares son exactamente los que contienen al conductor. □

Ejemplo 1.20. Siguiendo con el ejemplo $\mathcal{O} = \mathbb{Z} + 2\mathbb{Z}[i]$, tenemos que su conductor es $\mathfrak{f} = \{\alpha \in \mathbb{Z}[i] : \alpha\mathbb{Z}[i] \subseteq \mathcal{O}\} = 2\mathbb{Z}[i]$ (pues $(a+bi)\mathbb{Z}[i] \subseteq \mathcal{O}$ si y sólo si se cumple que $(a+bi)(c+di) = (ac-bd)+(ad+bc)i \in \mathcal{O}$ para todo $c, d \in \mathbb{Z}$, lo que es equivalente a que $2 \mid a$ y $2 \mid b$, i.e., $a + bi \in 2\mathbb{Z}[i]$). Esto no es algo particular de este orden, de hecho, todos los órdenes de la forma $\mathbb{Z} + f\mathcal{O}_K$ tienen conductor $\mathfrak{f} = f\mathcal{O}_K$, como veremos en el siguiente capítulo, en el que estudiaremos esta clase de órdenes en detalle. Con esto, la Proposición 1.18 nos da que los primos regulares de $\mathcal{O}$ son exactamente los que no contienen a 2; en particular, el ideal primo $(2, 2i)$ es irregular y, como mencionamos anteriormente, tampoco es invertible. Veremos más adelante que para ideales primos estas nociones son equivalentes (cf. Teorema 1.27).

Usando esta nueva herramienta, podemos simplificar el término central de la sucesión exacta de 1.14 con la siguiente proposición:

Proposición 1.21. $\bigoplus_{\mathfrak{p}} \tilde{\mathcal{O}}_{\mathfrak{p}}^{\times}/\mathcal{O}_{\mathfrak{p}}^{\times} \cong (\tilde{\mathcal{O}}/\mathfrak{f})^{\times}/(\mathcal{O}/\mathfrak{f})^{\times}$.

Demostración. Por la Proposición 1.7, obtenemos un isomorfismo:

$$(*) \qquad \mathcal{O}/\mathfrak{f} \cong \bigoplus_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}/\mathfrak{f}\mathcal{O}_{\mathfrak{p}},$$

donde $\mathfrak{p}$ recorre los primos no regulares de $\mathcal{O}$. La clausura entera de $\mathcal{O}_{\mathfrak{p}}$, $\tilde{\mathcal{O}}_{\mathfrak{p}}$, tiene como únicos primos los primos $\tilde{\mathfrak{p}}$ de $\tilde{\mathcal{O}}$ sobre $\mathfrak{p}$ (cf. Corolario A.10) y $\tilde{\mathcal{O}}_{\mathfrak{p}} = \tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}$, por lo que $\mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}} = \mathfrak{f}\mathcal{O}_{\mathfrak{p}}$. Así, aplicamos la Proposición 1.7 dos veces (primero con $\mathfrak{a} = \mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}}$ y luego con $\mathfrak{a} = \mathfrak{f}$) para obtener

$$\tilde{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}} \cong \bigoplus_{\tilde{\mathfrak{p}} \supseteq \mathfrak{p}} \tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}/\mathfrak{f}\tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}$$

y

$$(**) \qquad \tilde{\mathcal{O}}/\mathfrak{f} \cong \bigoplus_{\mathfrak{p}} \bigoplus_{\tilde{\mathfrak{p}} \supseteq \mathfrak{p}} \tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}/\mathfrak{f}\tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}} \cong \bigoplus_{\mathfrak{p}} \tilde{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}}.$$

Luego si consideramos los grupos de unidades de $(*)$ y $(**)$ y tomamos su cociente, obtenemos

$$(\tilde{\mathcal{O}}/\mathfrak{f})^{\times}/(\mathcal{O}/\mathfrak{f})^{\times} \cong \bigoplus_{\mathfrak{p}} (\tilde{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}})^{\times}/(\mathcal{O}_{\mathfrak{p}}/\mathfrak{f}\mathcal{O}_{\mathfrak{p}})^{\times}.$$

Definimos ahora para los primos no regulares el homomorfismo de grupos natural $\psi : \tilde{\mathcal{O}}_{\mathfrak{p}}^{\times} \to (\tilde{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}})^{\times}/(\mathcal{O}_{\mathfrak{p}}/\mathfrak{f}\mathcal{O}_{\mathfrak{p}})^{\times}$. Si $u \pmod{\mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}}}$ es una unidad de $\tilde{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}}$, u no está contenido en ningún ideal maximal de $\tilde{\mathcal{O}}_{\mathfrak{p}}$ (pues $\mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}} \subseteq \mathfrak{p}\tilde{\mathcal{O}}_{\mathfrak{p}}$) y es, por tanto, una unidad de este anillo, por lo que ψ es suprayectiva. Además, $\mathcal{O}_{\mathfrak{p}}^{\times} \subseteq \ker\psi \subseteq \mathcal{O}_{\mathfrak{p}}$ (y es un subgrupo de $\tilde{\mathcal{O}}_{\mathfrak{p}}^{\times}$), por lo que $\ker\psi = \mathcal{O}_{\mathfrak{p}}^{\times}$ y, usando el primer teorema de isomorfía, llegamos a que

$$\tilde{\mathcal{O}}_{\mathfrak{p}}^{\times}/\mathcal{O}_{\mathfrak{p}}^{\times} \cong (\tilde{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}})^{\times}/(\mathcal{O}_{\mathfrak{p}}/\mathfrak{f}\mathcal{O}_{\mathfrak{p}})^{\times} \quad \text{y} \quad \bigoplus_{\mathfrak{p}} \tilde{\mathcal{O}}_{\mathfrak{p}}^{\times}/\mathcal{O}_{\mathfrak{p}}^{\times} \cong (\tilde{\mathcal{O}}/\mathfrak{f})^{\times}/(\mathcal{O}/\mathfrak{f})^{\times}$$

como queríamos probar. □

Culminamos el estudio del grupo de Picard aplicando los resultados obtenidos sobre dominios noetherianos unidimensionales al caso que nos motivó a estudiarlos: los órdenes en cuerpos de números. Pues con todas las herramientas de las que disponemos, podemos formular una generalización del Teorema de unidades de Dirichlet (Teorema A.54) y el Teorema de finitud del número de clases (Teorema A.52) en un sólo resultado para órdenes:

Teorema 1.22. *Sea $\mathcal{O}$ un orden en un cuerpo de números K, $\mathcal{O}_K$ el orden maximal y $\mathfrak{f}$ el conductor de $\mathcal{O}$. Entonces los grupos $\mathcal{O}_K^\times/\mathcal{O}^\times$ y $\mathrm{Pic}(\mathcal{O})$ son finitos y tenemos la fórmula explícita*

$$h(\mathcal{O}) = \frac{h_K \cdot \#(\mathcal{O}_K/\mathfrak{f})^\times}{|\mathcal{O}_K^\times : \mathcal{O}^\times| \cdot \#(\mathcal{O}/\mathfrak{f})^\times}.$$

En particular, el rango de $\mathcal{O}^\times$ coincide con el de $\mathcal{O}_K^\times$ (y es, por el Teorema de unidades de Dirichlet, $r+s-1$, con la notación usada en dicho teorema).

Demostración. Como en el orden maximal todos los ideales fraccionarios no nulos son invertibles (por el Teorema A.29), tenemos que $\mathrm{Pic}(\mathcal{O}_K) = Cl_K$, y, aplicando la sucesión exacta de la Proposición 1.14 junto a la fórmula para el término central dada en la Proposición 1.21, llegamos a la sucesión exacta

$$1 \longrightarrow \mathcal{O}_K^\times/\mathcal{O}^\times \longrightarrow (\mathcal{O}_K/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times \longrightarrow \mathrm{Pic}(\mathcal{O}) \longrightarrow Cl_K \longrightarrow 1.$$

Por lo que

$$\#\,\mathrm{Pic}(\mathcal{O}) = \frac{\#\,\mathrm{Pic}(\mathcal{O}_K)}{\frac{\#(\mathcal{O}_K/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times}{\#\mathcal{O}_K^\times/\mathcal{O}^\times}} = \frac{h_K \cdot \#(\mathcal{O}_K/\mathfrak{f})^\times}{|\mathcal{O}_K^\times : \mathcal{O}^\times| \cdot \#(\mathcal{O}/\mathfrak{f})^\times}.$$

Cabe mencionar que se usa implícitamente el Teorema de finitud del número de clases (Teorema A.52). □

Con esta fórmula podemos retomar el ejemplo $\mathcal{O} = \mathbb{Z} + 2\mathbb{Z}[i]$ y comprobar que, en efecto, tiene número de clases 1:

Ejemplo 1.23. Sea $\mathcal{O} = \mathbb{Z} + 2\mathbb{Z}[i]$ ($K = \mathbb{Q}(i)$ y $\mathcal{O}_K = \mathbb{Z}[i]$). Es sabido que los enteros gaussianos $\mathcal{O}_K$ son un dominio euclídeo (tomando como función euclídea la norma) y, en particular, un dominio de ideales principales, por lo que $h_K = 1$. Por otra parte, como vimos en el Ejemplo 1.20, $\mathfrak{f} = 2\mathcal{O}_K$, por lo que tenemos

$$\begin{aligned}\mathcal{O}/\mathfrak{f} &= \{a + 2bi + 2\mathcal{O}_K \,:\, a, b \in \mathbb{Z}\} = \{0 + 2\mathcal{O}_K, 1 + 2\mathcal{O}_K\},\ \text{y}\\ \mathcal{O}_K/\mathfrak{f} &= \{0 + 2\mathcal{O}_K, 1 + 2\mathcal{O}_K, i + 2\mathcal{O}_K, 1 + i + 2\mathcal{O}_K\},\end{aligned}$$

y podemos ver entonces que

$$(\mathcal{O}/\mathfrak{f})^\times = \{1 + 2\mathcal{O}_K\} \ \text{y}\ (\mathcal{O}_K/\mathfrak{f})^\times = \{1 + 2\mathcal{O}_K, i + 2\mathcal{O}_K\}.$$

Por último, por la Proposición A.56, $\mathcal{O}_K^\times = \{1, -1, i, -i\}$ y $\mathcal{O}^\times = \{1, -1\}$, por lo que podemos calcular explícitamente con el Teorema 1.22

$$h(\mathcal{O}) = \frac{1 \cdot 2}{2 \cdot 1} = 1.$$

Seguiremos estudiando este tipo de órdenes en el siguiente capítulo, donde sacaremos provecho de la fórmula del teorema anterior dando un algoritmo para clasificar órdenes cuadráticos imaginarios con número de clase dado.

1.3. El conductor

Retomamos ahora nuestro objeto central: los órdenes. En esta sección estudiaremos el conductor siguiendo parcialmente el desarrollo de K. Conrad [5]. En esta sección $\mathcal{O}$ denotará un orden no maximal en un cuerpo de números K con conductor $\mathfrak{f}$ y $\mathcal{O}_K$ su orden maximal.

1.3.1. Ideales invertibles e ideales coprimos con el conductor

En primer lugar, damos un criterio de invertibilidad para ideales enteros basado en el conductor, para lo cual necesitaremos dos lemas:

Lema 1.24. *Si $\mathfrak{a} \neq 0$ es un ideal de $\mathcal{O}$ coprimo con $\mathfrak{f}$, entonces $\mathcal{O} = \{x \in K \mid x\mathfrak{a} \subseteq \mathfrak{a}\}$.*

Demostración. Sea $x \in K$ tal que $x\mathfrak{a} \subseteq \mathfrak{a}$; como $\mathfrak{a}$ es un $\mathcal{O}$-módulo finitamente generado (por ser $\mathcal{O}$ noetheriano), y $\mathcal{O}$ es un $\mathbb{Z}$-módulo finitamente generado, tenemos que $\mathfrak{a}$ es un $\mathbb{Z}$-módulo y, por tanto, x es entero sobre $\mathbb{Z}$ (luego $x \in \mathcal{O}_K$). Por coprimalidad, podemos tomar $a \in \mathfrak{a}$ y $b \in \mathfrak{f}$ tales que $1 = a + b$; luego $xa \in \mathfrak{a} \subseteq \mathcal{O}$ por hipótesis y $xb \in \mathcal{O}$, de donde concluimos que $x = ax + bx \in \mathcal{O}$. La otra inclusión se sigue de la definición de ideal. □

Lema 1.25. *Sea $\mathfrak{a} \neq 0$ un ideal de $\mathcal{O}$. Si $\mathfrak{a}$ es invertible, $\mathcal{O} = \{x \in K \mid x\mathfrak{a} \subseteq \mathfrak{a}\}$. Además, si $\mathfrak{a}$ es primo, se tiene el recíproco.*

Demostración. Sea $\mathfrak{a}$ un ideal invertible de $\mathcal{O}$ y sea $x \in K$ tal que $x\mathfrak{a} \subseteq \mathfrak{a}$, luego multiplicando por $\mathfrak{a}^{-1}$ llegamos a $x\mathcal{O} \subseteq \mathcal{O}$ y, por tanto, $x \in \mathcal{O}$.
Supongamos ahora que el ideal primo $\mathfrak{a}$ no es invertible; entonces el producto de ideales $\mathfrak{p} \cdot \{x \in K \mid x\mathfrak{p} \subseteq \mathcal{O}\} \neq \mathcal{O}$. Podemos tomar así $x \in K \setminus \mathcal{O}$ tal que $x\mathfrak{p} \subseteq \mathcal{O}$; luego

$$\mathfrak{p} \subseteq (\mathcal{O} + x\mathcal{O})\mathfrak{p} \subseteq \mathfrak{p} + x\mathfrak{p} \subseteq \mathcal{O}.$$

Así, por maximalidad de $\mathfrak{p}$, o bien $(\mathcal{O} + x\mathcal{O})\mathfrak{p} = \mathfrak{p}$ o bien $(\mathcal{O} + x\mathcal{O})\mathfrak{p} = \mathcal{O}$, siendo esta última imposible al ser $\mathfrak{p}$ no invertible; llegamos así a que $x\mathfrak{p} \subseteq \mathfrak{p}$ pero $x \notin \mathcal{O}$. □

Con esto ya estamos preparados para demostrar el siguiente teorema:

Teorema 1.26. *Todo ideal $\mathfrak{a} \neq 0$ de $\mathcal{O}$ coprimo con el conductor $\mathfrak{f}$ es producto de primos invertibles; en particular, $\mathfrak{a}$ es invertible.*

Demostración. Sea $\mathfrak{a} \neq 0$ un ideal coprimo con el conductor; si $\mathfrak{a}$ es primo, por los lemas 1.24 y 1.25 tenemos que $\mathfrak{a}$ es invertible. Probamos ahora por inducción en $|\mathcal{O} : \mathfrak{a}|$ que todo ideal coprimo con el conductor factoriza como producto finito de primos invertibles: supongamos que $\mathfrak{a}$ es coprimo con $\mathfrak{f}$ pero no es primo y tomemos $\mathfrak{p}$ un ideal maximal que contenga a $\mathfrak{a}$; de esta forma, $\mathcal{O} = \mathfrak{a} + \mathfrak{f} \subseteq \mathfrak{p} + \mathfrak{f} \subseteq \mathcal{O}$, por lo que $\mathfrak{p}$ es coprimo con $\mathcal{O}$ y es un ideal primo, luego es invertible. Sea $\mathfrak{a}' = \mathfrak{p}^{-1}\mathfrak{a} (\subseteq \mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O})$. Por una parte, como $\mathfrak{a} \neq \mathfrak{p}$, $\mathfrak{a}' \neq \mathcal{O}$; por la otra, la inclusión $\mathfrak{p}\mathfrak{a}' \subset \mathfrak{a}$ es estricta (pues si $\mathfrak{p}\mathfrak{a}' = \mathfrak{a}'$, para cada $k \geq 0$ $\mathfrak{a}' = \mathfrak{p}^k\mathfrak{a}' \subseteq \mathfrak{p}^k$, luego $|\mathcal{O} : \mathfrak{a}'| = |\mathcal{O} : \mathfrak{p}^k|$ para todo $k \geq 0$, que es imposible), por lo que $|\mathcal{O} : \mathfrak{a}'| < |\mathcal{O} : \mathfrak{a}|$ y, por hipótesis inductiva, tenemos que $\mathfrak{a}'$ es producto finito de primos invertibles. Luego $\mathfrak{a} = \mathfrak{p}\mathfrak{a}'$ nos da la factorización buscada. □

Esto en general es falso si $\mathfrak{a}$ no es coprimo con el conductor, pues si $\mathfrak{a}$ es cualquier primo que divide al conductor $\mathfrak{a}$ no es invertible como veremos a continuación.

Teorema 1.27. *Sea $\mathfrak{p} \neq 0$ un ideal primo de $\mathcal{O}$. Son equivalentes:*

(i) *$\mathfrak{p}$ es invertible.*

(ii) *$\mathfrak{p}$ es coprimo con $\mathfrak{f}$.*

(iii) *$\mathfrak{p}$ es regular.*

Demostración. Por la Proposición 1.18, $\mathfrak{p}$ regular $\iff \mathfrak{f} \not\subseteq \mathfrak{p} \iff \mathfrak{p}$ coprimo con $\mathfrak{f}$, es decir, tenemos $(ii) \iff (iii)$. Además, el Teorema 1.26 nos da $(ii) \implies (i)$. Basta, pues, probar $(i) \implies (ii)$:
Supongamos que $\mathfrak{p}$ es invertible; por la Proposición 1.9, $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ es un ideal principal de $\mathcal{O}_\mathfrak{p}$, por lo que $\mathcal{O}_\mathfrak{p}$ es un anillo local con ideal maximal principal y, por tanto, un anillo de valoración discreta (por la Proposición A.15) y, por tanto, $\mathfrak{p}$ es regular.

□

1.3.2. Teorema de correspondencia y norma absoluta

Con lo que hemos visto en este capítulo, conocemos muchas de las propiedades de los órdenes en cuanto anillos (son noetherianos y unidimensionales, tenemos una caracterización local de la invertibilidad y una medida de la no principalidad de los ideales fraccionarios, el grupo de Picard, entre otras). Sin embargo, tenemos exigua información sobre su estructura de ideales (enteros). Este problema en general es complicado; sin embargo, podemos dilucidar el caso de ideales coprimos con el conductor relacionándolos con ideales del orden maximal:

Teorema 1.28 (Teorema de correspondencia)**.** *Se tienen las siguientes correspondencias:*

(i) *Para cada ideal $\mathfrak{a}$ de $\mathcal{O}_K$ coprimo (en $\mathcal{O}_K$) con $\mathfrak{f}$, $\mathfrak{a} \cap \mathcal{O}$ es un ideal de $\mathcal{O}$ coprimo (en $\mathcal{O}$) con $\mathfrak{f}$ y el homomorfismo de anillos natural $\mathcal{O}/(\mathfrak{a}\cap\mathcal{O}) \to \mathcal{O}_K/\mathfrak{a}$ es un isomorfismo.*

(ii) *Para cada ideal $\mathfrak{a}$ de $\mathcal{O}$ coprimo con $\mathfrak{f}$, $\mathfrak{a}\mathcal{O}_K$ es un ideal de $\mathcal{O}_K$ coprimo con el conductor y el homomorfismo de anillos natural $\mathcal{O}/\mathfrak{a} \to \mathcal{O}_K/\mathfrak{a}\mathcal{O}_K$ es un isomorfismo.*

(iii) *Los ideales no nulos de $\mathcal{O}$ coprimos con el conductor están en correspondencia biyectiva con los ideales no nulos de $\mathcal{O}_K$ coprimos con el conductor mediante $\mathfrak{a} \to \mathfrak{a} \cap \mathcal{O}$ y $\mathfrak{b} \to \mathfrak{b}\mathcal{O}_K$; además, estas biyecciones son multiplicativas.*

Demostración.

(i) Si $\mathfrak{a}$ es un ideal de $\mathcal{O}_K$ y $\mathfrak{a} + \mathfrak{f} = \mathcal{O}_K$, usando que $\mathfrak{f}$ es un ideal de $\mathcal{O}$, tenemos que $\mathcal{O} = \mathcal{O} \cap (\mathfrak{a}+\mathfrak{f}) \subseteq \mathfrak{a} \cap \mathcal{O} + \mathfrak{f} \subseteq \mathcal{O}$, por lo que $\mathfrak{a}\cap\mathcal{O}$ es coprimo con $\mathfrak{f}$. El homomorfismo de anillos inducido por la inclusión, $\mathcal{O} \to \mathcal{O}_K/\mathfrak{a}$, es suprayectivo (pues la imagen de $\mathfrak{f} \subseteq \mathcal{O}$ en este es todo el anillo por coprimalidad) y tiene núcleo $\mathfrak{a} \cap \mathcal{O}$, por lo que el primer teorema de isomorfía para anillos nos da el resultado.

(ii) Si $\mathfrak{a}$ es un ideal de $\mathcal{O}$ y $\mathfrak{a}+\mathfrak{f}=\mathcal{O}$, usando ahora que $\mathfrak{f}$ es un ideal de $\mathcal{O}_K$ y $1\in\mathcal{O}$, $\mathcal{O}_K=\mathcal{O}\mathcal{O}_K=(\mathfrak{a}+\mathfrak{f})\mathcal{O}_K=\mathfrak{a}\mathcal{O}_K+\mathfrak{f}$, por lo que $\mathfrak{a}\mathcal{O}_K$ y $\mathfrak{f}$ son coprimos y $\mathfrak{a}\subseteq\mathfrak{a}\mathcal{O}_K\cap\mathcal{O}=(\mathfrak{a}\mathcal{O}_K\cap\mathcal{O})\mathcal{O}\subseteq\mathfrak{a}(\mathfrak{a}+\mathfrak{f})\subseteq\mathfrak{a}$, lo que implica que $\mathfrak{a}\mathcal{O}_K\cap\mathcal{O}=\mathfrak{a}$. Así, el homomorfismo de anillos inducido por la inclusión $\mathcal{O}\to\mathcal{O}_K/\mathfrak{a}\mathcal{O}_K$ es suprayectivo (pues de nuevo la imagen de $\mathfrak{f}$ es todo el anillo) y tiene núcleo $\mathfrak{a}\mathcal{O}_K\cap\mathcal{O}=\mathfrak{a}$. Así que usando otra vez el primer teorema de isomorfía llegamos al resultado.

(iii) Si $\mathfrak{a}$ es un ideal de $\mathcal{O}_K$ coprimo con el conductor, tenemos por (i) que $\mathfrak{b}=\mathfrak{a}\cap\mathcal{O}$ es coprimo con el conductor en $\mathcal{O}$, por lo que

$$\mathfrak{a}=\mathfrak{a}\mathcal{O}=\mathfrak{a}(\mathfrak{b}+\mathfrak{f})\subseteq\mathfrak{a}\mathfrak{b}+\mathfrak{a}\mathfrak{f}\subseteq\mathfrak{b}\mathcal{O}_K+\mathfrak{b}\mathcal{O}_K\subseteq\mathfrak{a},$$

y, por tanto, $\mathfrak{b}\mathcal{O}_K=\mathfrak{a}$. Recíprocamente, si $\mathfrak{b}$ es un ideal de $\mathcal{O}$ coprimo con $\mathfrak{f}$, por (ii) tenemos que $\mathfrak{a}=\mathfrak{b}\mathcal{O}_K$ es coprimo con $\mathfrak{f}$ en $\mathcal{O}_K$ y $\mathfrak{a}\cap\mathcal{O}=\mathfrak{b}$. Por lo que en efecto tenemos una biyección y, como $(\mathfrak{b}\mathcal{O}_K)(\mathfrak{b}'\mathcal{O}_K)=\mathfrak{b}\mathfrak{b}'\mathcal{O}_K$, tenemos la multiplicatividad.

□

Además, la hipótesis de coprimalidad es imprescindible, pues $\mathfrak{f}$ es un ideal tanto de $\mathcal{O}_K$ como de $\mathcal{O}$ y, por tanto, $\mathfrak{f}\cap\mathcal{O}=\mathfrak{f}$ y $\mathfrak{f}\mathcal{O}_K=\mathfrak{f}$, pero en general $\mathcal{O}/\mathfrak{f}\ncong\mathcal{O}_K/\mathfrak{f}$ (salvo si $\mathcal{O}=\mathcal{O}_K$).

Con este teorema, podemos generalizar a órdenes en cuerpos de números una importante herramienta de la Teoría Algebraica de Números: *la norma absoluta*. Recordemos que la norma absoluta para un anillo de enteros se define como el índice $|\mathcal{O}_K:\mathfrak{a}|$ para ideales enteros $\mathfrak{a}$ de $\mathcal{O}_K$ y se extiende, tras haber probado que es multiplicativa a todos los ideales fraccionarios de K, definiendo así un homomorfismo de grupos $J_K\to\mathbb{Q}_{>0}^{\times}$ (cf. Teorema A.46). Imitaremos este procedimiento para órdenes:

Definición 1.29. Sea $\mathcal{O}$ un orden en K y $\mathfrak{a}$ un ideal de $\mathcal{O}$; se define la *norma absoluta* de $\mathfrak{a}$ por $\mathfrak{N}(\mathfrak{a})=|\mathcal{O}:\mathfrak{a}|$ (para referirnos a la norma de $\mathcal{O}_K$ escribiremos $\mathfrak{N}_K(\mathfrak{a})$).

En primer lugar, el Teorema de correspondencia (Teorema 1.28) relaciona la norma $\mathfrak{N}$ con $\mathfrak{N}_K$:

Proposición 1.30. *Si $\mathfrak{a}$ es un ideal de $\mathcal{O}_K$ coprimo con el conductor en $\mathcal{O}_K$, entonces $\mathfrak{N}(\mathfrak{a}\cap\mathcal{O})=\mathfrak{N}_K(\mathfrak{a})$; recíprocamente, si $\mathfrak{b}$ es un ideal de $\mathcal{O}$ coprimo con el conductor en $\mathcal{O}$, $\mathfrak{N}_K(\mathfrak{b}\mathcal{O}_K)=\mathfrak{N}(\mathfrak{b})$.*

Demostración. El mencionado Teorema de correspondencia nos da isomorfismos de anillos $\mathcal{O}/(\mathfrak{a}\cap\mathcal{O})\cong\mathcal{O}_K/\mathfrak{a}$ y $\mathcal{O}/\mathfrak{b}\cong\mathcal{O}_K/\mathfrak{b}\mathcal{O}_K$, de donde se sigue el resultado. □

Imitando el caso de $\mathcal{O}_K$, nos gustaría probar la multiplicatividad de la norma para ideales de $\mathcal{O}_K$; no obstante, esta demostración pasa por usar factorización única de ideales, algo que, en general, no tenemos en $J(\mathcal{O})$; sin embargo, para extender dicha demostración podemos restringirnos al subgrupo de $J(\mathcal{O})$ generado por los ideales coprimos con el conductor $\mathfrak{f}$ (que recordemos que son invertibles por el Teorema 1.26): $J(\mathcal{O},\mathfrak{f})$.

Proposición 1.31. *$\mathfrak{N}$ satisface las siguientes propiedades:*

(i) *Si $\alpha\in\mathcal{O}$ es tal que $\alpha\mathcal{O}+\mathfrak{f}=\mathcal{O}$, $\mathfrak{N}(\alpha\mathcal{O})=|\,\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$, donde $\mathrm{N}_{K/\mathbb{Q}}$ es la norma de la extensión $K/\mathbb{Q}$ (cf. Definición A.31).*

(ii) $\mathfrak{N}$ *se extiende a un homomorfismo de grupos de* $J(\mathcal{O},\mathfrak{f})$.

Demostración. Si $\alpha \in \mathcal{O}$ es coprimo con el conductor en $\mathcal{O}$, usando la Proposición 1.30, $\mathfrak{N}(\alpha\mathcal{O}) = \mathfrak{N}_K(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|$ (por la Proposición A.45). Ahora, si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales coprimos con el conductor, usamos de nuevo la Proposición 1.30 y la multiplicatividad de $\mathfrak{N}_K$ (Teorema A.46) para obtener que

$$\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}_K((\mathfrak{a}\mathcal{O}_K)(\mathfrak{b}\mathcal{O}_K) = \mathfrak{N}_K(\mathfrak{a}\mathcal{O}_K)\,\mathfrak{N}_K(\mathfrak{b}\mathcal{O}_K) = \mathfrak{N}(\mathfrak{a})\,\mathfrak{N}(\mathfrak{b}).$$

Por lo que $\mathfrak{N}$ es una aplicación multiplicativa en un conjunto generador de $J(\mathcal{O},\mathfrak{f})$, extendiéndose así a un homomorfismo de $J(\mathcal{O},\mathfrak{f})$. □

1.3.3. El grupo de Picard relativo al conductor

De forma completamente análoga a lo que hicimos para definir el grupo de Picard de un orden, definimos el grupo de Picard relativo al conductor mediante los grupos $J(\mathcal{O},\mathfrak{f})$ y $P(\mathcal{O},\mathfrak{f})$, donde $P(\mathcal{O},\mathfrak{f})$ es el subgrupo de $J(\mathcal{O},\mathfrak{f})$ generado por los ideales principales coprimos con el conductor, respectivamente. Así, definimos el grupo de Picard relativo al conductor por $\mathrm{Pic}(\mathcal{O},\mathfrak{f}) = J(\mathcal{O},\mathfrak{f})/P(\mathcal{O},\mathfrak{f})$.

Empezamos observando que la inclusión $J(\mathcal{O},\mathfrak{f}) \hookrightarrow J(\mathcal{O})$ induce una aplicación (al componer con la proyección en el cociente) $J(\mathcal{O},\mathfrak{f}) \xrightarrow{\Psi} \mathrm{Pic}(\mathcal{O})$ cuyo núcleo es $J(\mathcal{O},\mathfrak{f}) \cap P(\mathcal{O})$ y que tenemos el siguiente resultado:

Lema 1.32. *Dado un ideal* $\mathfrak{c} \neq 0$*, en cada clase de* $\mathrm{Pic}(\mathcal{O})$ *existe un ideal entero de* $\mathcal{O}$ *coprimo con* $\mathfrak{c}$.

Demostración. Si $\mathfrak{c} = \mathcal{O}$, todos los ideales de $\mathcal{O}$ son coprimos con $\mathfrak{c}$, por lo que el resultado es trivial; supongamos, pues, que $\mathfrak{c} \neq \mathcal{O}$. Sean $\mathfrak{p}_1, ..., \mathfrak{p}_k$ los ideals primos de $\mathcal{O}$ que contienen a $\mathfrak{c}$; sea $C \in \mathrm{Pic}(\mathcal{O})$ y tomemos un ideal fraccionario $\mathfrak{a}$ de $\mathcal{O}$ tal que $C = [\mathfrak{a}]^{-1}$. Para cada $x \in \mathfrak{a}$, $\mathfrak{c} \subseteq x\mathfrak{a}^{-1} + \mathfrak{c} \subseteq \mathcal{O}$; si $x\mathfrak{a}^{-1} + \mathfrak{c} = \mathcal{O}$, el ideal $\mathfrak{b} = x\mathfrak{a}^{-1}$ es entero, coprimo con $\mathfrak{c}$ y $[\mathfrak{b}] = C$. Si no, $x\mathfrak{a}^{-1} + \mathfrak{c}$ está contenido en un ideal maximal que también contiene a $\mathfrak{c}$, por lo que es alguno de los ideales $\mathfrak{p}_1, ..., \mathfrak{p}_r$, digamos $\mathfrak{p}_j$, y tenemos así que $x\mathfrak{a}^{-1} \subseteq \mathfrak{p}_j$ (por maximalidad); luego $x \in \mathfrak{a}\mathfrak{p}_j$. Por lo que basta encontrar un $x \in \mathfrak{a}$ tal que para cada $j = 1, ..., k$ $x \notin \mathfrak{a}\mathfrak{p}_j$, pues tendríamos que $\mathfrak{b} = x\mathfrak{a}^{-1} \subseteq \mathcal{O}$ (es decir, es un ideal entero) y $\mathfrak{b} + \mathfrak{c} = \mathcal{O}$:
Para cada $j = 1, ..., k$, tomamos $x_j \in \mathfrak{a} \setminus \mathfrak{a}\mathfrak{p}_j$ y, por el Teorema Chino del Resto A.2, tenemos que existe un $x \in \mathfrak{a}$ tal que $x \equiv x_i \pmod{\mathfrak{a}\mathfrak{p}_j}$ y, así, $x \notin \mathfrak{a}\mathfrak{p}_j$ para cada $j = 1, ..., k$, obteniendo el ideal entero buscado. □

Así, si $\mathcal{C} \in \mathrm{Pic}(\mathcal{O})$, podemos escoger un ideal $\mathfrak{a}$ de $\mathcal{O}$ coprimo con $\mathfrak{f}$ tal que $\mathfrak{a} \in \mathcal{A}$, de forma que $\Psi(\mathfrak{a}) = A$ y Ψ es suprayectiva, obteniendo por el primer teorema de isomorfía:

Teorema 1.33. *Hay un isomorfismo de grupos abelianos* $J(\mathcal{O},\mathfrak{f})/\ker\Psi \cong \mathrm{Pic}(\mathcal{O})$. *En particular, como* $P(\mathcal{O},\mathfrak{f}) \subseteq J(\mathcal{O},\mathfrak{f}) \cap P(\mathcal{O}) = \ker\Psi$*, tenemos un homomorfismo suprayectivo* $\mathrm{Pic}(\mathcal{O},\mathfrak{f}) \longrightarrow \mathrm{Pic}(\mathcal{O})$.

Probaremos en el próximo capítulo que, para una clase de órdenes (los de la forma $\mathbb{Z} + f\mathcal{O}_K$) se tiene que esta aplicación es inyectiva y, por tanto, un isomorfismo de grupos abelianos.

1.4. Geometría de los órdenes

En esta sección discutiremos brevemente cómo interpretar los órdenes en un sentido geométrico, aunque por cuestiones de espacio y como esto no será necesario para nada en lo sucesivo, no entraremos en mucho detalle ni definiremos todos los términos, y las demostraciones serán todas relegadas a la bibliografía.

Sea $\mathcal{O}$ un orden en un cuerpo de números K (más generalmente podríamos seguir tratando con dominios noetherianos unidimensionales, como hemos hecho en secciones previas). $\mathcal{O}$ tiene asociado el *esquema afín*[5] $X = \operatorname{Spec}\mathcal{O}$, que es el conjunto de ideales primos de $\mathcal{O}$ dotado de la *topología de Zariski*, esto es, la que tiene por cerrados los conjuntos

$$V(\mathfrak{a}) = \{\mathfrak{p} \in X \,:\, \mathfrak{p} \supseteq \mathfrak{a}\}, \quad \text{para } \mathfrak{a} \text{ un ideal de } \mathcal{O},$$

y de un *haz* de anillos (para ver que esto es un haz nos referimos a [15, I. Proposición 13.3])

$$\mathcal{O}(U) = S^{-1}\mathcal{O}, \quad \text{donde } U \text{ es un abierto de } X \text{ y } S = \mathcal{O} \setminus \bigcup_{\mathfrak{p}\in U} \mathfrak{p}.$$

La idea fundamental es considerar X como un espacio cuyas funciones regulares en el abierto U son los elementos de $\mathcal{O}(U)$, para lo cual es conveniente definir $\kappa(\mathfrak{p}) = \mathcal{O}/\mathfrak{p}$ y pensar en los elementos $f \in \mathcal{O}$ como funciones en X mediante

$$f(\mathfrak{p}) = f \pmod{\mathfrak{p}} \in \kappa(\mathfrak{p}).$$

Por simplicidad diremos que un punto $\mathfrak{p} \in X$ es regular si el anillo local $\mathcal{O}_\mathfrak{p}$ es un dominio de valoración discreta. Con esta interpretación geométrica los órdenes maximales (más generalmente los dominios de Dedekind) serían *curvas no singulares* (cf. Teorema A.27(ii)) y los órdenes no maximales tendrían singularidades en los puntos que se corresponden a lo que hemos denominado anteriormente primos no regulares (cf. Definición 1.15). Así, podemos darle una interpretación geométrica al conductor, pues, en virtud de la Proposición 1.18 las singularidades de la curva $X = \operatorname{Spec}\mathcal{O}$ son exactamente los ideales primos que contienen al conductor, y de hecho el Teorema 1.27 nos dice que los puntos no singulares son primos invertibles.

Por otra parte, la inclusión $\iota : \mathcal{O} \hookrightarrow \mathcal{O}_K$ induce un *morfismo*[6] $\operatorname{Spec}\mathcal{O}_K \to \operatorname{Spec}\mathcal{O}$ por $\mathfrak{P} \mapsto \mathfrak{P} \cap \mathcal{O}$ que *resuelve* las singularidades de $\mathcal{O}$. De hecho, si $\mathfrak{p}$ es un punto de $\operatorname{Spec}\mathcal{O}$, podemos considerar su factorización $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1}...\mathfrak{P}_r^{e_r}$, de modo que $\mathfrak{P}_1, ..., \mathfrak{P}_r$ son los puntos de $\operatorname{Spec}\mathcal{O}_K$ que tienen imagen $\mathfrak{p}$, y $\mathfrak{p}$ es regular si y sólo si $r = 1$, $e_1 = 1$ y $[\mathcal{O}_K/\mathfrak{P} : \mathcal{O}/\mathfrak{p}] = 1$ (cf. Sección 13 de [15, Capítulo I]).

Por último, cabe mencionar que nuestra definición del grupo de Picard (en términos de ideales invertibles) también se puede entender geométricamente (como se explica en la sección 6 de [8, Capítulo II]) y se pueden definir otros grupos de interés geométrico asociados al orden $\mathcal{O}$, como el *grupo de clases de divisores*, que es el cociente del grupo abeliano libre generado por los ideales primos por cierto subgrupo (formado por los llamados *divisores principales*), como se puede ver en [15, I. Definición 12.13], que en el caso del orden maximal coincide de nuevo con el grupo de clases de ideales de K (cf. [15, I. Proposición 12.14]).

[5] Para la definición precisa nos referimos a la Sección 2 de [8, Capítulo II].
[6] Para la definición precisa nos referimos a la Sección 2 de [8, Capítulo II].

CAPÍTULO 2

Órdenes de la forma $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$

En 1801, C. F. Gauss propuso en su libro *Disquistiones Arithmeticæ* tres conjeturas relacionadas al número de clases de formas binarias cuadráticas, una de las cuales ([7, Art. 303]) es una clasificación completa de los discriminantes con número de clases 1. En este capítulo retomaremos esta conjetura mediante la formulación moderna de los órdenes y daremos un algoritmo para determinar todos los discriminantes negativos con un número de clases dado, digamos h, supuesto que se conoce la solución para órdenes maximales con número de clases h' para cada $h' \mid h$.

Antes de ello, generalizaremos los resultados sobre órdenes cuadráticos de [6, II.§7.] a una clase algo más general, los órdenes de la forma $\mathbb{Z} + f\mathcal{O}_K$; en particular, estudiaremos el grupo de Picard relativo definido al final del capítulo anterior para estos órdenes y obtendremos una fórmula del número de clases para ellos, para luego especializarlo al caso cuadrático.

Veamos antes de comenzar que los órdenes que estudiaremos en efecto generalizan el caso cuadrático, es decir, que todos los órdenes en cuerpos cuadráticos son de esta forma:

Proposición 2.1. *Sea K un cuerpo cuadrático, digamos $K = \mathbb{Q}(\sqrt{D})$ con $D \in \mathbb{Z}$ libre de cuadrados y $\mathcal{O}$ un orden en K. Si tomamos $f = |\mathcal{O}_K : \mathcal{O}|$, entonces el conductor de $\mathcal{O}$ es $\mathfrak{f} = f\mathcal{O}_K$ y $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = \mathbb{Z} + f\omega\mathbb{Z}$, donde $\omega = \sqrt{D}$ si $D \equiv 2, 3 \pmod 4$ y $\omega = \frac{1+\sqrt{D}}{2}$ si $D \equiv 1 \pmod 4$.*

Demostración. En primer lugar observamos que, como $\mathcal{O}_K$ y $\mathcal{O}$ son $\mathbb{Z}$-módulos finitamente generados del mismo rango, $\mathcal{O}_K/\mathcal{O}$ es un grupo abeliano finito. Ahora, por la Proposición A.55, tenemos que $1, \omega$ es una base entera de $\mathcal{O}_K$. Además, $f\omega \in \mathcal{O}$ (pues $\mathcal{O}_K/\mathcal{O}$ es un grupo abeliano de orden f, por lo que $f\mathcal{O}_K/\mathcal{O} = 0$); luego podemos escoger $c \in \mathbb{N}$ minimal tal que $c\omega \in \mathcal{O}$.
Así, si tomamos $\alpha = a + b\omega \in \mathcal{O}$ (con $a, b \in \mathbb{Z}$), entonces $b\omega = \alpha - a \in \mathcal{O}$ y, por tanto, $c|b$; luego $\mathcal{O} = \mathbb{Z} + c\omega\mathbb{Z}$ y, así, $\mathcal{O}_K/\mathcal{O}$ tiene orden c. Luego $c = f$ y concluimos que $\mathcal{O} = \mathbb{Z} + f\omega\mathbb{Z}$. Como $f\mathcal{O}_K \subseteq \mathcal{O}$, por definición de conductor, $f\mathcal{O}_K \subseteq \mathfrak{f}$. Por otra parte, tenemos que si $\alpha = a + bf\omega \in \mathfrak{f}$ (con $a, b \in \mathbb{Z}$), $\alpha\omega = a\omega + bf\omega^2 = c + (a + bfd)\omega \in \mathcal{O} = \mathbb{Z} + f\omega\mathbb{Z}$ (con $c, d \in \mathbb{Z}$), luego $f|a + bdf$ y, por tanto, $f|a$ y $\alpha \in f\mathcal{O}_K$. Por lo que $\mathfrak{f} = f\mathcal{O}_K$. □

A lo largo de este capítulo K denotará siempre un cuerpo de números de grado $n > 1$ con anillo de enteros $\mathcal{O}_K$ y $\mathcal{O}$ un orden (en general no maximal) en K con conductor $\mathfrak{f}$.

2.1. Propiedades básicas

Una de las principales ventajas de los órdenes de la forma $\mathbb{Z} + f\mathcal{O}_K$, es que podremos determinar explícitamente su conductor y que éste será un ideal principal en $\mathcal{O}_K$ (generado por un entero), lo cual nos permitirá mejorar algunos de los resultados del capítulo anterior.

Lema 2.2. *Sea $\mathfrak{a} \neq 0$ un ideal de $\mathcal{O}_K$ y supongamos que $\mathcal{O} = \mathbb{Z} + \mathfrak{a}$ es un orden. Sea $a \in \mathbb{Z}$ tal que $\mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$, entonces los ideales de $\mathcal{O}$ que contienen a $\mathfrak{a}$ son de la forma $d\mathbb{Z} + \mathfrak{a}$ para cierto entero $d \mid a$; en particular $\mathfrak{f} = d\mathbb{Z} + \mathfrak{a}$ con $d \mid a$ el mínimo entero positivo en $\mathfrak{f}$, que es el exponente[1] del grupo abeliano $\mathcal{O}_K/\mathcal{O}$.*

Demostración. Por el segundo teorema de isomorfía para anillos, $\mathcal{O}/\mathfrak{a} = (\mathbb{Z}+\mathfrak{a})/\mathfrak{a} \cong \mathbb{Z}/(\mathfrak{a} \cap \mathbb{Z}) = \mathbb{Z}/a\mathbb{Z}$; así, si $\mathfrak{b}$ es un ideal de $\mathcal{O}$ que contiene a $\mathfrak{a}$, por el teorema de correspondencia tenemos un ideal $\bar{\mathfrak{b}} = \{x + \mathfrak{a} \mid x \in \mathfrak{b}\}$ de $\mathcal{O}/\mathfrak{a}$ y usando el isomorfismo anterior lo podemos considerar como un ideal de $\mathbb{Z}/a\mathbb{Z}$, donde sería de la forma $d\mathbb{Z}/a\mathbb{Z}$ para cierto $d \mid a$ y, así, $\bar{\mathfrak{b}} = \overline{d\mathbb{Z} + \mathfrak{a}}$ y $\mathfrak{b} = d\mathbb{Z} + \mathfrak{a}$. Como $\mathfrak{a} \subseteq \mathbb{Z} + \mathfrak{a} = \mathcal{O}$, $\mathfrak{a}\mathcal{O}_K = \mathfrak{a} \subseteq \mathcal{O}$, por lo que $\mathfrak{a} \subseteq \mathfrak{f}$ y así $\mathfrak{f} = d\mathbb{Z} + \mathfrak{a}$ para cierto $d \mid a$. Ahora, como $\mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$ y $d \mid a$, $\mathfrak{f} \cap \mathbb{Z} = (d\mathbb{Z} \cap \mathbb{Z}) + (\mathfrak{a} \cap \mathbb{Z}) = d\mathbb{Z} + a\mathbb{Z} = d\mathbb{Z}$, d es el mínimo entero positivo de $\mathfrak{f}$. Por último, $d \in \mathfrak{f}$, $d\mathcal{O}_K \subseteq \mathcal{O}$, por lo que $d \cdot \mathcal{O}_K/\mathcal{O} = 0$ y por tanto, el exponente m de $\mathcal{O}_K/\mathcal{O}$ divide a d (en particular $m \leq d$); y, por otra parte, si m es el exponente de $\mathcal{O}_K/\mathcal{O}$, $m\mathcal{O}_K \subseteq \mathcal{O}$, luego $m \in \mathfrak{f}$ y $m \geq d$ por minimalidad. □

Ahora, para el caso $\mathfrak{a} = f\mathcal{O}_K$, tenemos el siguiente resultado:

Proposición 2.3. *Sea $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ para cierto entero $f > 1$; entonces $\mathfrak{f} = f\mathcal{O}_K$.*

Demostración. Por el lema anterior, tenemos que $\mathfrak{f} = d\mathbb{Z} + f\mathcal{O}_K$ con $d \mid f$ el exponente de $\mathcal{O}_K/\mathcal{O}$; sea $\omega_1, ..., \omega_n$ una base entera de $\mathcal{O}_K$ con $\omega_1 = 1$ y tomemos $a_1, ..., a_n \in \mathbb{Z}$ tales que $d\omega_2 = a_1 + fa_2\omega_2 + ... + fa_n\omega_n$, de forma que $0 = a_1 + (fa_2 - d)\omega_2 + fa_2 + ... + fa_n\omega_n$ y, como los ω_j forman una base, $fa_2 - d = 0$, por lo que $f \mid d$ y, así, $d = f$. Concluimos, pues, que $\mathfrak{f} = f\mathbb{Z} + f\mathcal{O}_K = f\mathcal{O}_K$. □

Observación 2.4. *Usando el Lema 2.2, si $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$, tenemos además que los ideales que contienen al conductor son exactamente los de la forma $d\mathbb{Z} + f\mathcal{O}_K$ con $d \mid f$; en particular, si f es primo el conductor es un ideal maximal.*

En lo que resta de capítulo consideraremos $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ para cierto entero $f > 1$ (de forma que $\mathfrak{f} = f\mathcal{O}_K$) y llamaremos indistintamente conductor al ideal $\mathfrak{f}$ y al entero positivo f.

Proposición 2.5. *Un ideal $\mathfrak{a}$ de $\mathcal{O}_K$ es coprimo (en $\mathcal{O}_K$) con el conductor si y sólo si $\mathfrak{N}_K(\mathfrak{a})$ es coprimo con f; similarmente, un ideal $\mathfrak{b}$ de $\mathcal{O}$ es coprimo (en $\mathcal{O}$) con el conductor si y sólo si $\mathfrak{N}(\mathfrak{b})$ es coprimo con f.*

Demostración. Sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$ y consideremos $\mu_f : \mathcal{O}_K/\mathfrak{a} \to \mathcal{O}_K/\mathfrak{a}$ la multiplicación por f. Si $\mathfrak{a}$ es coprimo con $\mathfrak{f}$, podemos tomar $a \in \mathfrak{a}$ y $\alpha \in \mathcal{O}_K$ tales que $a + f\alpha = 1$, por lo que dado $\beta + \mathfrak{a} \in \mathcal{O}_K/\mathfrak{a}$,

$$\mu_f(\alpha\beta + \mathfrak{a}) = f\alpha\beta + \mathfrak{a} = (1 - a)\beta + \mathfrak{a} = \beta + \mathfrak{a}$$

[1] Recordamos que el exponente de un grupo G es el mínimo entero m positivo tal que $G^m = 1$ (con notación aditiva $m \cdot G = 0$), y que siempre existe para grupos finitos.

y μ_f es suprayectiva. Recíprocamente, si μ_f es suprayectiva podemos tomar $\alpha+\mathfrak{a} \in \mathcal{O}_K/\mathfrak{a}$ tal que $\mu_f(\alpha+\mathfrak{a}) = 1+\mathfrak{a}$, por lo que existe $a \in \mathfrak{a}$ tal que $f\alpha = 1+a$, luego $\mathfrak{a}+\mathfrak{f} = \mathcal{O}_K$. Como $\mathcal{O}_K/\mathfrak{a}$ es un grupo abeliano finito y μ_f un homomorfismo de grupos, μ_f es suprayectiva si y sólo si es un isomorfismo de grupos abelianos. Además, por el Teorema de clasificación de los grupos abelianos finitos, μ_f es un isomorfismo si y sólo si f es coprimo con el orden del grupo, i.e., si y sólo si f y $\mathfrak{N}_K(\mathfrak{a})$ son coprimos.
Ahora, por el Teorema de correspondencia 1.28, $\mathfrak{b}$ es coprimo con el conductor si y sólo si $\mathfrak{b}\mathcal{O}_K$ es coprimo con el conductor; por la Proposición 1.30, $\mathfrak{N}(\mathfrak{b}) = \mathfrak{N}_K(\mathfrak{b}\mathcal{O}_K)$ y el resultado se sigue. □

Concluimos esta sección generalizando la relación entre el conductor y el índice en cuerpos cuadráticos dada en la Proposición 2.1:

Proposición 2.6. *Sea $\mathcal{O} = \mathbb{Z}+f\mathcal{O}_K$, entonces tenemos que $|\mathcal{O}_K : \mathcal{O}| = f^{n-1}$ y $\operatorname{disc}(\mathcal{O}) = (f^{n-1})^2 d_K = |\mathcal{O}_K : \mathcal{O}|^2 d_K$, donde $\operatorname{disc}(\mathcal{O})$ denota el discriminante de $\mathcal{O}$.*

Demostración. Fijada una base $\omega_1, ...\omega_n$ de $\mathcal{O}_K$ con $\omega_1 = 1$, consideramos el homomorfismo de grupos $\psi : \mathcal{O}_K \to (\mathbb{Z}/f\mathbb{Z})^{n-1}$ dada por $\psi(a_1+a_2\omega_2+...+a_n\omega_n) = (a_2, ..., a_n) \pmod{n}$. Si $\alpha \in \mathcal{O}$, existen $a_1, ..., a_n \in \mathbb{Z}$ tales que $\alpha = a_1+a_2f\omega_2+...+a_nf\omega_n$, por lo que $\psi(\alpha) = 0$; si $\alpha = a_1+a_2\omega_2+...+a_n\omega_n$ y $\psi(\alpha) = 0$, entonces para todo $j \in \{2, ..., n\}$ existe un $q_j \in \mathbb{Z}$ tal que $a_j = fq_j$, por lo que $\alpha \in \mathcal{O}$. Luego $\ker\psi = \mathcal{O}$ y el primer teorema de isomorfía para grupos nos da el resultado buscado.
Por último, $\operatorname{disc}(\mathcal{O}) = \operatorname{disc}(1, f\omega_2, ..., f\omega_n) = (f^{n-1})^2 d_K = |\mathcal{O}_K : \mathcal{O}|^2 d_K$. □

2.2. Grupo de Picard relativo

Antes de estudiar el grupo de Picard relativo, demostaremos un lema que nos será útil para relacionar $\operatorname{Pic}(\mathcal{O}, \mathfrak{f})$ con cierto grupo de clases de ideales del orden maximal:

Lema 2.7. *Si $\alpha \in \mathcal{O}_K$ es tal que $\alpha \equiv a \pmod{\mathfrak{f}}$, entonces $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \equiv a^n \pmod{f}$.*

Demostración. Como $\alpha \equiv a \pmod{\mathfrak{f}}$ y $\mathfrak{f} = f\mathcal{O}_K$, podemos escribir $\alpha = a + f\beta$ para cierto $\beta \in \mathcal{O}_K$, por lo que fijada una clausura algebraica de $\bar{\mathbb{Q}}$ de $\mathbb{Q}$ y dado un $\mathbb{Q}$-morfismo $\sigma : K \to \mathbb{Q}$, $\sigma\alpha = a + f\sigma\beta$, luego si $\sigma_1, ..., \sigma_n$ son los $\mathbb{Q}$-morfismos de K en $\bar{\mathbb{Q}}$, se tiene que $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \prod_{j=1}^n \sigma_j\alpha = \prod_{j=1}^n (a + f\sigma_j\beta) \equiv a^n \pmod{f}$. □

Retomamos ahora la aplicación Ψ definida en la sección 1.3.3, que según vimos en dicha sección es suprayectiva y tiene núcleo $J(\mathcal{O}, \mathfrak{f}) \cap P(\mathcal{O}) \supseteq P(\mathcal{O}, \mathfrak{f})$; para los órdenes de la forma $\mathbb{Z} + f\mathcal{O}_K$ de hecho se tiene la igualdad:

Lema 2.8. *Sea $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$, entonces $J(\mathcal{O}, \mathfrak{f}) \cap P(\mathcal{O}) = P(\mathcal{O}, \mathfrak{f})$.*

Demostración. Sea $\mathfrak{a} \in J(\mathcal{O}, \mathfrak{f}) \cap P(\mathcal{O})$; existe un $\alpha \in K$ e ideales enteros $\mathfrak{b}$ y $\mathfrak{c}$ de $\mathcal{O}$ coprimos con el conductor tales que $\mathfrak{a} = \alpha\mathcal{O} = \mathfrak{b}\mathfrak{c}^{-1}$. Así, por la Proposición 1.31, tenemos que $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{b})/\mathfrak{N}(\mathfrak{c})$, y, tomando $c = \mathfrak{N}(\mathfrak{c})$, tenemos que c es coprimo con f y, por tanto, $c\mathcal{O}$ es coprimo con el conductor (por la Proposición 2.5), por lo que $c\mathcal{O} \in P(\mathcal{O}, \mathfrak{f})$. Con esto, si definimos $\mathfrak{c}' = c\mathfrak{c}^{-1}$ (que es un ideal entero[2]), entonces $c\alpha\mathcal{O} = c\mathfrak{b}\mathfrak{c}^{-1} = \mathfrak{b}\mathfrak{c}' \subseteq \mathcal{O}$, por lo que $c\alpha\mathcal{O} \in P(\mathcal{O}, \mathfrak{f})$ y, por tanto, $\mathfrak{a} = \alpha\mathcal{O} = (c\alpha\mathcal{O})(c\mathcal{O})^{-1} \in P(\mathcal{O}, \mathfrak{f})$. □

[2]Si $\mathfrak{a}$ es un ideal entero de $\mathcal{O}$, como $\mathcal{O}/\mathfrak{a}$ es un grupo finito de orden $\mathfrak{N}(\mathfrak{a})$, $\mathfrak{N}(\mathfrak{a}) \cdot \mathcal{O}/\mathfrak{a} = 0$, por lo que $\mathfrak{N}(\mathfrak{a}) \in \mathfrak{a}$; en particular, $\mathfrak{N}(\mathfrak{a})\mathfrak{a}^{-1} \subseteq \mathcal{O}$.

Igual que definimos anteriormente subgrupos de $J(\mathcal{O})$ mediante ideales coprimos con el conductor, hacemos algo similar para el orden maximal: definimos $J_K(\mathfrak{f})$ como el subgrupo de J_K generado por los ideales enteros de $\mathcal{O}_K$ coprimos (en $\mathcal{O}_K$) con $\mathfrak{f}$ y $P_{K,\mathbb{Z}}(\mathfrak{f})$ como el subgrupo de J_K generado por los ideales principales de la forma $\alpha\mathcal{O}_K$ con $\alpha \equiv a \pmod{\mathfrak{f}}$ para algún $a \in \mathbb{Z}$ coprimo con f. Definimos así $Cl_K(\mathfrak{f}) = J_K(\mathfrak{f})/P_{K,\mathbb{Z}}(\mathfrak{f})$; que se relaciona con los grupos conocidos mediante el siguiente teorema:

Teorema 2.9. *Sea $\mathcal{O}$ un orden de la forma $\mathbb{Z}+f\mathcal{O}_K$. Hay isomorfismos de grupos abelianos* $\mathrm{Pic}(\mathcal{O}) \cong \mathrm{Pic}(\mathcal{O},\mathfrak{f}) \cong Cl_K(\mathfrak{f})$.

Demostración. Por los Lemas 1.32 y 2.8, tenemos que la inclusión $J(\mathcal{O},\mathfrak{f}) \hookrightarrow J(\mathcal{O})$ induce un isomorfismo de grupos abelianos $\mathrm{Pic}(\mathcal{O},\mathfrak{f}) \cong \mathrm{Pic}(\mathcal{O})$. Por otra parte, el teorema de correspondencia 1.28 nos da una biyección multiplicativa entre ideales (enteros) de $\mathcal{O}$ coprimos con el conductor e ideales (enteros) de $\mathcal{O}_K$ coprimos con el conductor dada por $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ y con inversa $\mathfrak{b} \mapsto \mathfrak{b} \cap \mathcal{O}$, por lo que se extiende a un isomorfismo de grupos abelianos $J(\mathcal{O},\mathfrak{f}) \xrightarrow{\sim} J_K(\mathfrak{f})$; sea P la imagen de $P(\mathcal{O},\mathfrak{f})$ bajo este isomorfismo. Basta, pues, probar que $P = P_K(\mathfrak{f})$:
Si $\alpha \in \mathcal{O}_K$ es tal que $\alpha \equiv a \pmod{\mathfrak{f}}$ con $a \in \mathbb{Z}$ coprimo con f, $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \equiv a^n \pmod{f}$ (por el Lema 2.7), luego $(\mathrm{N}_{K/\mathbb{Q}}(\alpha), f) = 1$ y, como $f\mathcal{O}_K \subseteq \mathcal{O}$, $\alpha = a + f\beta \in \mathcal{O}$. Recíprocamente, si $\alpha \in \mathcal{O}$ tiene norma coprima con f, escribiendo $\alpha = a + f\beta$ con $\beta \in \mathcal{O}_K$ y $a \in \mathbb{Z}$, llegamos a que $\alpha \equiv a \pmod{\mathfrak{f}}$ y $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \equiv a^m \pmod{f}$ (de nuevo usando el Lema 2.7) es coprimo con f, por lo que a es coprimo con f. Así, tenemos que $P(\mathcal{O},\mathfrak{f})$ está generado por los ideales de la forma $\alpha\mathcal{O}$ con $\alpha \in \mathcal{O}$ cuya norma es coprima con f, por lo que P está generado por los ideales $\alpha\mathcal{O}_K$ tales que $\alpha \in \mathcal{O}$ con norma coprima con f; como por definición $P_{K,\mathbb{Z}}(\mathfrak{f})$ está generado por los ideales $\alpha\mathcal{O}_K$ tales que $\alpha \equiv a \pmod{\mathfrak{f}}$ con $(a, f) = 1$, por lo visto anteriormente estos conjuntos generadores son iguales y, por tanto, $P = P_{K,\mathbb{Z}}(\mathfrak{f})$. □

Es decir, el grupo $\mathrm{Pic}(\mathcal{O},\mathfrak{f})$ nos ha permitido, por una parte, reducir el estudio de $\mathrm{Pic}(\mathcal{O})$ al de los ideales enteros de $\mathcal{O}$ coprimos con el conductor y, más aun, reducirlo al estudio de aquellos del anillo de enteros. De hecho, este isomorfismo nos permitiría aplicar *Teoría de Cuerpos de Clases* a estos órdenes viendo su grupo de clases como $Cl_K(\mathfrak{f})$; hacerlo en detalle excedería las posibilidades de este trabajo, pero veamos brevemente cómo:

Teorema 2.10 (Existencia de cuerpos de clases)**.** *Sea $\mathfrak{m}$ un ideal de $\mathcal{O}_K$ y sea H un subgrupo de congruencia*[3] *para $\mathfrak{m}$. Entonces existe una única extensión abeliana L/K cuyos primos ramificados*[4] *dividen a $\mathfrak{m}$ y un isomorfismo canónico*[5] *de grupos abelianos* $J_K(\mathfrak{m})/H \cong \mathrm{Gal}(L/K)$.

Podemos encontrar el resultado original de Takagi en [21, Satz 23], quien probaría en 1920 algunos de los resultados fundamentales de esta teoría; para la versión que enunciamos aquí nos referimos a [6, II. Teorema 8.5]. Con esto, podemos aplicar el teorema con $\mathfrak{m} = \mathfrak{f}$ y $H = P_{K,\mathbb{Z}}(\mathfrak{f})$ para obtener una extensión abeliana L/K tal que

$$\mathrm{Pic}(\mathcal{O}) \cong Cl_K(\mathfrak{f}) = J_K(\mathfrak{f})/P_{K,\mathbb{Z}}(\mathfrak{f}) \cong \mathrm{Gal}(L/K).$$

[3] Un subgrupo de $J_K(\mathfrak{m})$ que contiene a todos los ideales principales generados por elementos $1 \pmod{\mathfrak{m}}$.
[4] Si $\mathfrak{p}$ es un ideal primo (no nulo) de $\mathcal{O}_K$, se dice que $\mathfrak{p}$ *ramifica* en L si en su factorización $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}...\mathfrak{P}_r^{e_r}$ hay algún exponente $e_j > 1$.
[5] Es inducido por la denominada *aplicación de Artin*, que no definiremos por brevedad.

Dicho L se denomina el *cuerpo de clases de anillo* del orden $\mathcal{O}$; en el caso del orden maximal ($\mathfrak{f} = \mathcal{O}_K$) se denomina el *cuerpo de clases de Hilbert* de K. Antes de concluir esta sección, destacamos que en el caso de que K sea un cuerpo cuadrático, estas construcciones se pueden hacer explícitas, como veremos en el próximo capítulo.

2.3. Fórmula del número de clases y clasificación

Comenzamos definiendo $\Phi_K : \{\text{ideales de } \mathcal{O}_K\} \longrightarrow \mathbb{N}$ por $\Phi_K(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})^\times$, cuyas propiedades principales están recogidas en la sección A.2.2 del Apéndice; en particular, el Corolario A.50 nos da la siguiente fórmula:

$$(\natural) \qquad \Phi_K(a\mathcal{O}_K) = |a|^n \prod_{\mathfrak{p}|a\mathcal{O}_K} \left(1 - \frac{1}{\mathfrak{N}_K(\mathfrak{p})}\right) = |a|^n \prod_{p|a} \prod_{\mathfrak{p}|p\mathcal{O}_K} \left(1 - \frac{1}{\mathfrak{N}_K(\mathfrak{p})}\right),$$

para $a \in \mathbb{Z}$, que depende únicamente de como se extienden los ideales primos de $\mathbb{Z}$ a $\mathcal{O}_K$ (y de la factorización de a).

Por otra parte, el valor de $\#(\mathcal{O}/\mathfrak{f})^\times$ es más fácil de calcular, pues tenemos el siguiente resultado:

Lema 2.11. *Sea $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$. Hay un isomorfismo de anillos $\mathcal{O}/\mathfrak{f} \cong \mathbb{Z}/f\mathbb{Z}$; en particular, tenemos que $(\mathcal{O}/\mathfrak{f})^\times \cong (\mathbb{Z}/f\mathbb{Z})^\times$ y $\#(\mathcal{O}/\mathfrak{f})^\times = \varphi(f)$, donde φ es la función φ de Euler.*

Demostración. Por el segundo Teorema de isomorfía para anillos,

$$\mathcal{O}/\mathfrak{f} = (\mathbb{Z} + f\mathcal{O}_K)/(f\mathcal{O}_K) \cong \mathbb{Z}/(f\mathcal{O}_K \cap \mathbb{Z}) = \mathbb{Z}/f\mathbb{Z};$$

tomando unidades obtenemos el resultado. □

Teorema 2.12. *Sea $\mathcal{O} = \mathbb{Z} + \mathcal{O}_K$. Tenemos la fórmula para el número de clases*

$$h(\mathcal{O}) = \frac{h_K \cdot f^{n-1}}{|\mathcal{O}_K^\times : \mathcal{O}^\times|} \left(\prod_{p|f} \left(1 - \frac{1}{p}\right)^{-1} \prod_{\mathfrak{p}|p\mathcal{O}_K} \left(1 - \frac{1}{\mathfrak{N}_K(\mathfrak{p})}\right)\right).$$

Demostración. Por la fórmula para el número de clases del Teorema 1.22, tenemos que

$$h(\mathcal{O}) = \frac{h_K \cdot \#(\mathcal{O}_K/\mathfrak{f})^\times}{|\mathcal{O}_K^\times : \mathcal{O}^\times| \#(\mathcal{O}/\mathfrak{f})^\times};$$

sustituyendo ($\natural$) con $a = f$ y usando que $\#(\mathcal{O}/\mathfrak{f})^\times = \#(\mathbb{Z}/f\mathbb{Z})^\times = \varphi(f)$ llegamos a la expresión buscada. □

2.3.1. Aplicación al caso cuadrático

Proposición 2.13. *Sea K un cuerpo cuadrático y sea $a \in \mathbb{Z}$ un entero no nulo. Entonces*

$$\#(\mathcal{O}_K/a\mathcal{O}_K)^\times = a^2 \prod_{p|a} \left(1 - \frac{1}{p}\right)\left(1 - \left(\frac{d_k}{p}\right)\frac{1}{p}\right).$$

Demostración. Sea p un primo; por la fórmula (♮) tenemos que

$$\Phi_K(p\mathcal{O}_K) = \mathfrak{N}_K(p\mathcal{O}_K) \prod_{\mathfrak{p}|p\mathcal{O}_K} \left(1 - \frac{1}{\mathfrak{N}_K(\mathfrak{p})}\right) = p^2 \prod_{\mathfrak{p}|p\mathcal{O}_K} \left(1 - \frac{1}{\mathfrak{N}_K(\mathfrak{p})}\right).$$

Usando la Proposición A.57, distinguimos en tres casos:
(i) $\left(\frac{d_K}{p}\right) = 0$, en cuyo caso p ramifica: $p\mathcal{O}_K = \mathfrak{p}^2$ con $\mathfrak{p} \neq 0$ un primo de $\mathcal{O}_K$ y $\mathfrak{N}_K(\mathfrak{p}) = p$, por lo que $\Phi_K(p\mathcal{O}_K) = p^2\left(1 - \frac{1}{p}\right) = p^2\left(1 - \frac{1}{p}\right)\left(1 - \left(\frac{d_K}{p}\right)\right)$.
(ii) $\left(\frac{d_K}{p}\right) = 1$, en cuyo caso p se decompone: $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ con $\mathfrak{p}_1 \neq \mathfrak{p}_2$ primos no nulos de $\mathcal{O}_K$ y $\mathfrak{N}_K(\mathfrak{p}_1) = \mathfrak{N}_K(\mathfrak{p}_2) = p$, luego $\Phi_K(p\mathcal{O}_K) = p^2\left(1 - \frac{1}{p}\right)^2 = p^2\left(1 - \frac{1}{p}\right)\left(1 - \left(\frac{d_K}{p}\right)\right)$.
(iii) $\left(\frac{d_K}{p}\right) = -1$, en cuyo caso p es inerte: $p\mathcal{O}_K = \mathfrak{p}$ con $\mathfrak{p} \neq 0$ un primo de $\mathcal{O}_K$ y $\mathfrak{N}_K(\mathfrak{p}) = p^2$; tenemos así que $\Phi_K(p\mathcal{O}_K) = p^2\left(1 - \frac{1}{p^2}\right)^2 = p^2\left(1 - \frac{1}{p}\right)\left(1 - \left(\frac{d_K}{p}\right)\right)$.
Por lo que, en cualquier caso, $\Phi_K(p\mathcal{O}_K) = p^2\left(1 - \frac{1}{p}\right)\left(1 - \left(\frac{d_K}{p}\right)\right)$. Así, usando de nuevo la fórmula (♮) y la multiplicatividad de Φ_K y de la norma:

$$\begin{aligned}\#(\mathcal{O}_K/a\mathcal{O}_K)^\times = \Phi_K(a\mathcal{O}_K) &= \mathfrak{N}(a\mathcal{O}_K) \prod_{\mathfrak{p}|a\mathcal{O}_K} \left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\right) = a^2 \prod_{\mathfrak{p}|a\mathcal{O}_K} \frac{\Phi_K(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})} \\ &= a^2 \prod_{p|a} \frac{\Phi_K(p\mathcal{O}_K)}{\mathfrak{N}(p)} = a^2 \prod_{p|a} \left(1 - \frac{1}{p}\right)\left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right).\end{aligned}$$

□

Con todo lo anterior, obtenemos la siguiente fórmula para el número de clases para órdenes en cuerpos cuadráticos:

Teorema 2.14. *Sea K un cuerpo cuadrático y $\mathcal{O}$ un orden en K. Entonces*

$$h(\mathcal{O}) = \frac{h_K \cdot f}{|\mathcal{O}_K^\times : \mathcal{O}^\times|} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right).$$

2.3.2. Órdenes imaginarios cuadráticos según su número de clases

En [11] se menciona la posibilidad de desarrollar un algoritmo para clasificar órdenes imaginarios cuadráticos según su número de clases mediante la fórmula del Teorema 2.14; pero no desarrollan el caso par y se utiliza en su lugar una cota superior para los conductores y los discriminantes con la que se calculan exhaustivamente todos los órdenes posibles. Aquí desarrollaremos dicha idea de aprovechar la fórmula del Teorema 2.14 para diseñar un algoritmo más eficiente que resuelva este problema (en comparación el algoritmo usado en [11] tarda aproximadamente[6] 19 horas y media en devolver un diccionario completo con todos los órdenes imaginarios cuadráticos con número de clases $h(\mathcal{O}) \leq 100$; el aquí presente realiza esta tarea en cuestión de segundos[7]). Describimos a continuación el algoritmo, cuya implementación en `SageMath` se puede encontrar en el Apéndice B.

[6] Ejecutado por John Cremona en la Universidad de Warwick.
[7] Menos de 20 segundos, ejecutado localmente en `SageMath` (versión 9.3).

Separaremos este problema en dos partes; la primera, dados dos enteros $m \geq 1$ y d, encontrar todas las soluciones enteras $f > 1$ a la ecuación

$$(*) \qquad m = f \prod_{p|f} \left(1 - \left(\frac{d}{p}\right) \frac{1}{p}\right).$$

Observemos en primer lugar, que factorizando f y multiplicando el lado derecho de la ecuación anterior, para cada $p \mid f$ se tiene que $p - (d/p) \mid m$, por lo que tenemos una restricción sobre los divisores primos de f y podemos determinar así todas las posibles f:

1. Eliminamos los casos directos:
   (i) Si $m = 1$, esto implica que $p = 2$ y $(d/p) = 1$; el producto queda $1/2$. De modo que si $(d/2) = 1$, añadimos la solución $f = 2$ a la lista.
   (ii) Si $m = 3$, las únicas posibilidades son $p = 2$ y $(d/2) = \pm 1$ ó $p = 3$ y $(d/p) = 0$. Así, en función de esto podemos calculamos el cociente entre m y el producto en $(*)$ y añadimos su cociente f cuando sea un entero.
   (iii) Si $m \neq 1, 3$ es impar, sólo es posible que $p = 2$ si $(d/2) = 1$ ó $(d/2) = -1$ y $3 \mid m$; y en otro caso es necesario que $(d/p) = 0$ y $p \mid m$. Por lo que los posibles primos son $p = 2$, si se satisfacen las correspondientes condiciones, y los factores primos de $\gcd(m, d)$; calculamos con esto los posibles productos en $(*)$ y añadimos f a la lista cuando sea un entero.
2. En el resto de casos m es un número par, que es donde se produce la mayor parte del gasto computacional, y el caso que no se considera en la propuesta de [11], por lo que aquí es donde realmente se produce la mejora con respecto al algoritmo de [11]. Observamos que como $p - (d/p) \mid m$ para cada $p \mid f$, todos los divisores primos p de f están a distancia (d/p) de un divisor de m. Con esto, lo que haremos será recorrer todos los divisores $r \mid m$ y comprobamos si $r+1$ es primo cuando $(d/r+1) = 1$, si r es primo cuando $(d/r) = 0$ y si $r-1$ es primo cuando $(d/r-1) = -1$, y añadiremos $r+1$, r y $r-1$ (respectivamente) a los posibles divisores primos de f. Como hemos hecho en los casos anteriores, a partir de aquí basta calcular todos los posibles productos en $(*)$ para las posibles combinaciones de primos en nuestra lista y añadir f a la lista de soluciones cuando sea un entero.

Una vez sabemos hallar todas las soluciones enteras a $(*)$ con m y d fijos, estamos en disposición de encontrar (condicionalmente) todos los órdenes con número de clases h: Fijemos un entero $h \geq 1$ y supongamos que conocemos todos los discriminantes de cuerpos imaginarios cuadráticos K con número de clase h_K para cada divisor $h_K \mid h$. Así, en vistas de la fórmula del Teorema 2.14, para encontrar todos los órdenes imaginarios cuadráticos con número de clases h, basta recorrer los divisores h' de h y posibles discriminantes d_K de cuerpos imaginarios cuadráticos K con $h_K = h'$, y usar el algoritmo anterior para encontrar todas las soluciones enteras a $(*)$ con $m = h \cdot |\mathcal{O}_K^\times : \mathcal{O}^\times| / h'$ y $d = d_K$.

Observemos que, por la Proposición A.56, $|\mathcal{O}_K^\times : \mathcal{O}^\times|$ sólo puede ser 1 (si $d_K \neq -3, -4$), 2 (si $d_K = -4$) o 3 (si $d_K = -3$), por lo que el único impedimento es tener una lista de todos los discriminantes con número de clase h' para cada $h' \mid h$, esto es, resolver el problema del número de clase de Gauss.

Aunque aún no haya una solución completa a éste, Heegner [9], en el año 1952, dio una clasificación completa de todos los cuerpos imaginarios cuadráticos con número de clase

1, cuya demostración contenía un error que fue solucionado posterioremente por Stark [20] en 1969; hubo, sin embargo, dos pruebas independientes de este resultado en 1967 por Baker [2] y por Stark [19]. Posteriormente, se fueron consiguiendo resultados similares para números de clase pequeños; en 2004 Watkins [24] dio una clasificación de todos los cuerpos cuadráticos con número de clase h para $h \leq 100$. Así, usando la clasificación de Watkins (que podemos encontrar en [23]) junto al algoritmo descrito anteriormente podemos clasificar todos los órdenes no maximales con número de clases h para $h \leq 100$. Para $h > 100$, el algoritmo sigue sirviendo para encontrar órdenes no maximales de número de clases h si nos restringimos al caso $h_K \mid h$ con $h_K \leq 100$.

Por otra parte, para cada ideal fraccionario $\mathfrak{a}$ de $\mathcal{O}$ definimos

$$j(\mathfrak{a}) = \frac{1728 g_2(\mathfrak{a})^3}{g_2(\mathfrak{a})^3 - 27 g_3(\mathfrak{a})^2}, \text{ donde } g_2(\mathfrak{a}) = 60 G_4(\mathfrak{a}),\ g_3(\mathfrak{a}) = 140 G_6(\mathfrak{a})$$
$$\text{y } G_{2k}(\mathfrak{a}) = \sum_{\omega \in \mathfrak{a} \setminus \{0\}} \frac{1}{\omega^{2k}},$$

que, como veremos en el siguiente capítulo, sólo depende de la clase de ideales de $\mathfrak{a}$. Se presenta a continuación la tabla con todos los órdenes (maximales y no maximales) con número de clases 1, junto al denominado *polinomio de clases de Hilbert*, $H(x) = \prod_{\mathfrak{a}}(x - j(\mathfrak{a}))$, donde $\mathfrak{a}$ recorre un sistema completo de representantes de $\mathrm{Pic}(\mathcal{O})$, que ha sido calculado con alta precisión en `Magma`. Siguiendo el mismo proceso se han calculado todos los órdenes

d_K	f	$H(x)$
-3	1	x
	2	$x - 54000$
	3	$x + 12288000$
-4	1	$x - 1728$
	2	$x - 287496$
-7	1	$x + 3375$
	2	$x - 16581375$
-8	1	$x - 8000$
-11	1	$x + 32768$
-19	1	$x + 884736$
-43	1	$x + 884736000$
-67	1	$x + 147197952000$
-163	1	$x + 262537412640768000$

Tabla 2.1: $h(\mathcal{O}) = 1$

con número de clases $h(\mathcal{O}) \leq 100$ junto al $H(x)$ correspondiente; incluimos también en el Apéndice B el código usado para calcular los $H(x)$, así como la clasificación y tablas análogas a la Tabla 2.1 para $h = 2$ y $h = 3$.

La principal observación que podemos hacer en las tablas (cf. Tabla 2.1, Tabla B.1 y Tabla B.2) es que todos los $H(x)$ son mónicos con coeficientes enteros y de grado $h(\mathcal{O})$, por lo que los $j(\mathfrak{a})$ son (conjeturalmente, pues los cáculos son numéricos) enteros algebraicos de grado $\leq h(\mathcal{O})$ (de hecho se puede comprobar que todos los polinomios son irreducibles, por lo que son enteros algebraicos de grado exactamente $h(\mathcal{O})$). La explicación de estos fenómenos reside en la *Teoría de la Multiplicación Compleja*, que será objeto del siguiente capítulo.

CAPÍTULO 3
Multiplicación compleja

Es handelt sich um meinen liebsten Jugendtraum, nämlich um den Nachweis, dass die Abel'schen Gleichungen mit Quadratwurzeln rationaler Zahlen durch die Transformations-Gleichungen elliptischer Functionen mit singulären Moduln grade so erschöpft werden, wie die ganzzahligen Abel'schen Gleichungen durch die Kreistheilungsgleichungen.

Se trata de mi más querido sueño de juventud, a saber, la demostración de que todas las ecuaciones abelianas con raices cuadradas de números racionales se agotan mediante las identidades de transformación de funciones elípticas con módulos singulares, al igual que las ecuaciones abelianas enteras se agotan mediante las divisiones de la circunferencia.
Extracto de una carta de L. Kronecker a R. Dedekind, 15 de marzo de 1880 [12, pág. 455].

El conocido Teorema de Kronecker-Weber clasifica todas las extensiones abelianas[1] de $\mathbb{Q}$ como subextensiones de algún cuerpo ciclotómico $\mathbb{Q}(e^{2\pi i/n})$ (al menos en el caso de extensiones finitas); es decir, las extensiones abelianas (finitas) de $\mathbb{Q}$ son de la forma $\mathbb{Q}(\alpha)$ para alguna combinación lineal con coeficientes racionales de raíces de la unidad α (por el Teorema del elemento primitivo). En su carta a Dedekind, Kronecker le expone su sueño de juventud: extender este teorema a extensiones abelianas de cuerpos cuadráticos (o en sus términos, ecuaciones abelianas con raíces cuadradas de números racionales) mediante *funciones elípticas* y *módulos singulares*.

Cabe mencionar que años más tarde este problema sería parte del décimosegundo problema de Hilbert (cf. [10, pp. 458–461]), que pide extender el mencionado Teorema de Kronecker-Weber a cuerpos de números arbitrarios.

Nuestro objetivo en este capítulo es estudiar (relegando muchas demostraciones a la bibliografía por motivos de espacio) el *Jugendtraum* de Kronecker, principalmente los *módulos singulares*, para poder explicar los fenomenos descubiertos al final del capítulo anterior.

[1] Recordemos que una extensión se dice abeliana si es de Galois y su grupo de Galois es abeliano.

3.1. Retículos y la función modular elíptica

Antes de comenzar con el estudio de la Multiplicación Compleja y su relación con los órdenes, necesitaremos introducir algunos conceptos básicos sobre *retículos* en $\mathbb{C}$, lo cual no debería sorprendernos si tenemos en cuenta que los órdenes –e incluso sus ideales fraccionarios– imaginarios cuadráticos (fijado un $\mathbb{Q}$-morfismo $K \hookrightarrow \mathbb{C}$) son de forma natural un retículo en los números complejos. Comenzaremos definiendo estos objetos y viendo cómo se relacionan con los ideales fraccionarios de un orden y el grupo de Picard, para lo cual seguiremos principalmente los Capítulos 1 y 2 de [18] y el Capítulo 3 de [6].

3.1.1. Definiciones y primeras propiedades

Podríamos definir con mayor generalidad un retículo en un espacio vectorial V como un subgrupo de V generado (sobre $\mathbb{Z}$) por un conjunto de vectores linealmente independientes, lo cual serviría para estudiar órdenes en cuerpos de números de grado superior; sin embargo, para el caso cuadrático podemos simplificar y definir:

Definición 3.1. Un *retículo* Λ es un subgrupo de $\mathbb{C}$ de la forma $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ con ω_1, ω_2 independientes sobre $\mathbb{R}$ (geométricamente estamos pidiendo que no sean colineales); (ω_1, ω_2) se denomina una base del retículo. Diremos además que dos retículos Λ_1, Λ_2 son homotéticos si existe un $\alpha \in \mathbb{C}^\times$ tal que $\Lambda_1 = \alpha\Lambda_2$ (es decir si se puede transformar uno en el otro mediante una rotación y una dilatación).

Una *función elíptica* es una función meromorfa f doblemente periódica, es decir, $f(z+\omega_1) = f(z+\omega_2) = f(z)$ para ciertos $\omega_1, \omega_2 \in \mathbb{C}$ independientes sobre $\mathbb{R}$. Por lo que podemos pensar en ellas como funciones definidas en $\mathbb{C}/\Lambda$. El principal ejemplo de función elíptica es la $\wp$ de Weierstrass

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\lambda\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right),$$

que es esencial para gran parte de esta teoría, pues las funcioens elípticas están generadas por $\wp$ y $\wp'$, es decir, son elementos de $\mathbb{C}(\wp, \wp')$; pero no entraremos en más detalles al respecto.

Los retículos en $\mathbb{C}$ son invariantes por ciertas homotecias (en el sentido de que $\alpha\Lambda \subseteq \Lambda$) y, en general, esto será cierto para todos las homotecias por elementos de $\mathbb{Z}$ (por definición). Estaremos interesados principalmente en aquellos retículos que tengan *más* homotecias que sólo los enteros:

Definición 3.2. Definimos el anillo[2] $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$. Diremos que Λ tiene *multiplicación compleja* (o *CM*) por $\mathcal{O}$ si $\mathcal{O} = \mathrm{End}(\Lambda) \neq \mathbb{Z}$.

Proposición 3.3. *Sea Λ un retículo con CM por $\mathcal{O}$; entonces $\mathcal{O}$ es un orden en un cuerpo cuadrático imaginario K. Además, Λ es homotético a un ideal fraccionario invertible de $\mathcal{O}$.*

[2] Si $a \in \mathbb{Z}$, $a\Lambda \subseteq \Lambda$, por lo que $\mathbb{Z} \subseteq \mathrm{End}(\Lambda)$; y si $\alpha, \beta \in \mathrm{End}(\Lambda)$, entonces $(\alpha\beta)\Lambda = \alpha(\beta\Lambda) \subseteq \alpha\Lambda \subseteq \Lambda$ y $(\alpha+\beta)\Lambda = \alpha\Lambda + \beta\Lambda \subseteq \Lambda + \Lambda = \Lambda$, luego $\alpha\beta, \alpha+\beta \in \mathrm{End}(\Lambda)$.

Demostración. Escribamos $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ con $\tau = \omega_2/\omega_1 \in \mathfrak{H}$ y sea $\Lambda' = \mathbb{Z} + \tau\mathbb{Z}$. Si $\alpha \in \mathcal{O} \setminus \mathbb{Z}$, entonces $\alpha\Lambda' = \frac{1}{\omega_1}(\alpha\Lambda) \subseteq \frac{1}{\omega_1}\Lambda = \Lambda'$, por lo que existen $a, b, c, d \in \mathbb{Z}$ tales que $\alpha = a + b\tau$ y $\alpha\tau = c + d\tau$; luego $\tau = (c + d\tau)/(a + b\tau)$ y obtenemos la ecuación cuadrática

$$b\tau^2 + (a - d)\tau - c = 0.$$

Como $\tau \notin \mathbb{R}$ (pues ω_1 y ω_2 no pueden estar alineados), necesariamente $b \neq 0$ y $K = \mathbb{Q}(\tau)$ es un cuerpo imaginario cuadrático. Así, dado $\beta \in \mathcal{O}$, se tiene que $\beta\Lambda' \subseteq \Lambda'$ y podemos tomar como antes $a', b' \in \mathbb{Z}$ tales que $\beta = a' + b'\tau$, por lo que $\beta \in K$ y tenemos que $\mathcal{O} = \{\beta \in K : \beta\Lambda \subseteq \Lambda\}$ es un orden en el cuerpo imaginario cuadrático K. Por último, observamos que Λ es homotético a $\Lambda' \subseteq K$. □

Discutiremos ahora brevemente la estructura de los retículos bajo la relación de homotecia: Como dado $z \in \mathbb{C} \setminus \mathbb{R}$, o bien $z \in \mathfrak{H}$ o bien $1/z \in \mathfrak{H}$, podemos suponer sin pérdida de generalidad que todas las bases están orientadas, esto es, que $\omega_1/\omega_2 \in \mathfrak{H}$, por lo que si $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ es un retículo, Λ es homotético a $\Lambda_\tau = \tau\mathbb{Z} + \mathbb{Z}$ con $\tau = \omega_1/\omega_2 \in \mathfrak{H}$. Tenemos con esto que si denotamos por $\mathcal{L}$ el conjunto de todos los retículos en $\mathbb{C}$ y $\mathcal{L}/\mathbb{C}^\times$ el conjunto cociente bajo la relación de homotecia, tenemos una aplicación suprayectiva $\mathfrak{H} \to \mathcal{L}/\mathbb{C}^\times$ dada por $\tau \mapsto \Lambda_\tau$. Por lo que para obtener una biyección basta ver cuando τ_1 y τ_2 dan lugar al mismo retículo ([18, I. Lema 1.2]):

Lema 3.4. *Sean $\tau_1, \tau_2 \in \mathfrak{H}$. Λ_{τ_1} y Λ_{τ_2} son homotéticos si y sólo si existe una matriz $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ tal que $\tau_2 = (a\tau_1 + b)/(c\tau_1 + d)$.*

Por lo que si definimos una acción de $\mathrm{SL}_2(\mathbb{Z})$ en $\mathfrak{H}$ por $\gamma\tau = \frac{a\tau+b}{c\tau+d}$ para cada $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, tenemos una biyección entre las órbitas de $\mathfrak{H}$ por la acción[3] de $\mathrm{SL}_2(\mathbb{Z})$ y $\mathcal{L}/\mathbb{C}^\times$.

3.1.2. La función modular elíptica

Pasamos ahora a la construcción de una *función modular*. Para cada retículo Λ definimos su *serie de Eisenstein* de peso $2k$, $k \geq 2$ por

$$G_{2k}(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^{2k}}.$$

Observamos que (al menos a nivel formal), $G_{2k}(\alpha\Lambda) = \alpha^{-2k} G_{2k}(\Lambda)$, por lo que si lo traducimos al lenguaje de $\mathfrak{H}$ con la acción de $\mathrm{SL}_2(\mathbb{Z})$ tenemos que, definiendo $G_{2k}(\tau) = G_{2k}(\Lambda_\tau)$ (de nuevo a nivel formal) se satisface la ley de transformación en $\mathfrak{H}$

$$G_{2k}(\gamma\tau) = G_{2k}(\Lambda_{\gamma\tau}) = G_{2k}((c\tau + d)^{-1}\Lambda_\tau) = (c\tau + d)^{2k} G_{2k}(\tau),\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Esta ley de transformación define una interesante clase de funciones en las que no profundizaremos aquí, pero daremos la siguiente definición:

[3] De hecho se puede hacer un poco mejor y usar el grupo modular $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$, pues -1 actúa como la identidad en $\mathfrak{H}$ y es fácil ver que esta nueva acción es transitiva. Pero esto no será necesario en lo sucesivo.

Definición 3.5. Sea $k \in \mathbb{Z}$, diremos que f es una *forma modular* de peso $2k$ si es una función holomorfa en $\mathfrak{H}$ acotada cuando $\tau \to i\infty$ tal que

$$f(\gamma\tau) = (c\tau + d)^{2k} f(\tau), \text{ para } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ y } \tau \in \mathfrak{H}.$$

Cabe mencionar que no incluimos peso impar porque la única posibilidad sería el 0 (al aplicar la matriz -1 obtenemos que $f(\tau) = (-1)^k f(\tau)$).

Proposición 3.6. *Para $k \geq 2$ la serie de Eisenstein de peso $2k$ define una función modular de peso $2k$ y $G_{2k}(\infty) = 2\zeta(2k)$, donde $\zeta(s)$ es la función zeta de Riemann.*[4]

Para una demostración de este resultado nos referimos a [18, I. Proposición 3.4.2]. Con esto, definiendo $g_2 = 60G_4$ y $g_3 = 140G_6$, tenemos que $\Delta = g_2^3 - 27g_3^2$ es una forma modular de peso 12 que se anula en el infinito (basta usar los valores conocidos $\zeta(4) = \pi^4/90$ y $\zeta(6) = \pi^6/945$ junto a la proposición anterior); y g_2^3 es una forma modular de peso 12, por lo que el j-invariante $j = 1728g_2^3/\Delta$ satisface (cuando está definida) la ley de transformación de una forma modular de peso 0 y tiene un polo en el infinito, de hecho Δ no se anula en $\mathfrak{H}$ (cf. [6, III. Proposición 10.7]), por lo que j es holomorfa en todo $\mathfrak{H}$, teniendo así una función holomorfa en $\mathfrak{H}$ que es invariante por la acción de $\mathrm{SL}_2(\mathbb{Z})$ y, usando la correspondencia con los retículos, podemos asignar a cada retículo una cantidad invariante por homotecia. De hecho, el recíproco también es cierto (cf. [6, III. Teorema 10.9]):

Teorema 3.7. *Λ_1 y Λ_2 son homotéticos si y sólo si $j(\Lambda_1) = j(\Lambda_2)$.*

3.1.3. Correspondencia con el grupo de Picard

Sea $\mathcal{O}$ un orden en un cuerpo imaginario cuadrático K y sea $\mathfrak{a}$ un ideal fraccionario de $\mathcal{O}$; fijada una inclusión $K \hookrightarrow \mathbb{C}$, podemos escribir $\mathfrak{a} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ con $\omega_1, \omega_2 \in K \subset \mathbb{C}$ tales que $\omega_1/\omega_2 \in \mathfrak{H}$ (por definición de ideal fraccionario), por lo que los ideales fraccionarios de $\mathcal{O}$ son de forma natural retículos en $\mathbb{C}$. Además, dados dos ideales fraccionarios $\mathfrak{a}$ y $\mathfrak{b}$ de $\mathcal{O}$ en la misma clase de $\mathrm{Pic}(\mathcal{O})$, existe un $c \in K \subset \mathbb{C}$ tal que $\mathfrak{a} = c\mathfrak{b}$, por lo que definen retículos homotéticos. En primer lugar, probamos el siguiente resultado:

Lema 3.8. *El retículo $\Lambda = \mathfrak{a}$, tiene multiplicación compleja por $\mathcal{O}$.*

Demostración. Sea $\mathcal{O}' = \mathrm{End}(\Lambda)$; $\mathcal{O}'$ es un orden en cierto cuerpo cuadrático K' (por la Proposición 3.3) tal que $\mathcal{O} \subseteq \mathcal{O}'$ (si $\alpha \in \mathcal{O}$, $\alpha\mathfrak{a} \subseteq \mathfrak{a}$), por lo que $K = K'$ y $\mathcal{O}' \subseteq \mathcal{O}_K$. Así, si $\alpha \in \mathcal{O}'$, $\alpha\mathfrak{a} \subseteq \mathfrak{a}$ y $\alpha \in \mathcal{O}_K$, luego $\alpha \in \mathfrak{f} \subseteq \mathcal{O}$, donde $\mathfrak{f}$ es el conductor de $\mathcal{O}$ (cf. 1.16). Así, $\mathrm{End}(\Lambda) = \mathcal{O}$. □

Definimos, igual que el producto de ideales, el producto de un ideal fraccionario por un retículo por

$$\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + ... + \alpha_r\Lambda_r \,:\, \alpha_j \in \mathfrak{a},\, \lambda_j \in \Lambda\}$$

Veremos a continuación que esto induce una acción transitiva de $\mathrm{Pic}(\mathcal{O})$ en los retículos de $\mathbb{C}$ con multiplicación compleja por $\mathcal{O}$.

[4] Por $f(\infty)$ entendemos $\lim\limits_{\substack{y\to\infty \\ y\in\mathbb{R}}} f(iy)$.

Proposición 3.9. *Sea $\mathcal{O}$ un orden en un cuerpo imaginario cuadrático, sea Λ un retículo en $\mathbb{C}$ con multiplicación compleja por $\mathcal{O}$ y sean $\mathfrak{a}$ y $\mathfrak{b}$ ideales fraccionarios invertibles de $\mathcal{O}$. Tenemos entonces que $\mathfrak{a}\Lambda$ es un retículo con multiplicación compleja por $\mathcal{O}$ y que $\mathfrak{a}\Lambda$ y $\mathfrak{b}\Lambda$ son homotéticos si y sólo si $\mathfrak{a}$ y $\mathfrak{b}$ están en la misma clase de* $\mathrm{Pic}(\mathcal{O})$.

Demostración. Como Λ tiene multiplicación compleja por $\mathcal{O}$, $\mathcal{O}\Lambda = \Lambda$, de forma que, tomando $c \in \mathbb{Z} \setminus \{0\}$ tal que $c\mathfrak{a} \subseteq \mathcal{O}$, $c\mathfrak{a}\Lambda \subseteq \Lambda$ y, por tanto, $\mathfrak{a}\Lambda \subseteq \frac{1}{c}\Lambda$. Tenemos así que $\mathfrak{a}\Lambda$ es un subgrupo discreto de $\mathbb{C}$. Por otra parte, tomando $d \in \mathbb{Z} \setminus \{0\}$ tal que $d\mathcal{O} \subseteq \mathfrak{a}$, $d\Lambda = d\mathcal{O}\Lambda \subseteq \mathfrak{a}\Lambda$, por lo que $\mathfrak{a}\Lambda$ genera $\mathbb{C}$ como $\mathbb{R}$-espacio vectorial y es, por tanto, un retículo en $\mathbb{C}$. Ahora, si $\alpha \in \mathbb{C}$, multiplicando por $\mathfrak{a}^{-1}$,

$$\alpha\mathfrak{a}\Lambda \subseteq \mathfrak{a}\Lambda \iff \alpha\mathcal{O}\Lambda \subseteq \mathcal{O}\Lambda \iff \alpha\Lambda \subseteq \Lambda; \text{ luego } \mathrm{End}(\mathfrak{a}\Lambda) = \mathrm{End}(\Lambda) = \mathcal{O}.$$

Por último, si $\mathfrak{a}\Lambda$ y $\mathfrak{b}\Lambda$ son homotéticos, existe un $c \in \mathbb{C}^\times$ tal que $\mathfrak{a}\Lambda = c\mathfrak{b}\Lambda$, luego $\mathfrak{a}(c\mathfrak{b})^{-1}$ y $\mathfrak{a}^{-1}(c\mathfrak{b})$ están contenidos en $\mathrm{End}(\Lambda) = \mathcal{O}$, por lo que necesariamente $\mathfrak{a}(c\mathfrak{b})^{-1} = \mathcal{O}$ y, por tanto, $\mathfrak{a} = c\mathfrak{b}$, teniéndose así que $c \in K^\times$ y que $\mathfrak{a}$ y $\mathfrak{b}$ definen la misma clase en $\mathrm{Pic}(\mathcal{O})$; el recíproco fue discutido anteriormente. □

Con esta proposición, si denotamos por $\mathcal{L}_\mathcal{O}$ el conjunto de retículos de $\mathbb{C}$ con multiplicación compleja por $\mathcal{O}$ módulo homotecias, la operación

$$[\mathfrak{a}] * \Lambda = \mathfrak{a}^{-1}\Lambda, \text{ con } [\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}),\ \Lambda \in \mathcal{L}_\mathcal{O},$$

está bien definida y es una acción de grupo de $\mathrm{Pic}(\mathcal{O})$ en $\mathcal{L}_\mathcal{O}$.

Proposición 3.10. *La acción de* $\mathrm{Pic}(\mathcal{O})$ *en* $\mathcal{L}_\mathcal{O}$ *es simplemente transitiva*[5].

Demostración. Sean Λ_1, Λ_2 retículos con CM por $\mathcal{O}$ y tomemos $\lambda_1 \in \Lambda_1 \setminus \{0\}$. Si definimos $\mathfrak{a}_1 = \lambda_1^{-1}\Lambda_1$, $\mathfrak{a}_1$, $\mathrm{End}(\mathfrak{a}_1)$ es un orden en un cuerpo cuadrático K' y $\mathfrak{a}_1 \subseteq K'$ (por la Proposición 3.3) y claramente $\mathcal{O} = \mathrm{End}(\Lambda_1) \subseteq \mathrm{End}(\mathfrak{a}_1)$, por lo que $K' = K$, donde K es el cuerpo de fracciones de $\mathcal{O}$. Además, $\mathfrak{a}_1$ es un $\mathcal{O}$-módulo finitamente generado (pues es finitamente generado como $\mathbb{Z}$-módulo y $\mathcal{O}\mathfrak{a}_1 = \mathfrak{a}_1$); luego $\mathfrak{a}_1$ es un ideal fraccionario de $\mathcal{O}$. Análogamente, tomando $\lambda_2 \in \Lambda_2 \setminus \{0\}$, $\mathfrak{a}_2 = \lambda_2^{-1}\Lambda_2$ es otro ideal fraccionario de $\mathcal{O}$; por lo que si definimos $\mathfrak{a} = \mathfrak{a}_2^{-1}\mathfrak{a}$,

$$[\mathfrak{a}] * \Lambda_1 = \mathfrak{a}_2\mathfrak{a}_1^{-1}\Lambda_1 = \frac{\lambda_1}{\lambda_2}\Lambda_2,$$

donde hemos usado para la última igualdad que $\lambda_2\lambda_1^{-1}\mathfrak{a}_2\mathfrak{a}_1^{-1}\Lambda_1 = \lambda_2\mathfrak{a}_2 = \Lambda_2$. Luego Λ_1 y Λ_2 son homotéticos y, por tanto, la acción es transitiva. Por último, si $\mathfrak{a} * \Lambda = \Lambda$, $\mathfrak{a}$ y $\mathfrak{a}^{-1}$ están contenidos en $\mathrm{End}(\Lambda) = \mathcal{O}$, por lo que $\mathfrak{a} = \mathcal{O}$. □

En particular, esto nos da el siguiente resultado:

Teorema 3.11. *Hay una correspondencia biyectiva natural entre* $\mathrm{Pic}(\mathcal{O})$ *y* $\mathcal{L}_\mathcal{O}$.

Demostración. Por la Proposición 3.9 con $\Lambda = \mathcal{O}$ (recordemos que Λ tiene multiplicación compleja por $\mathcal{O}$ por el Lema 3.8), tenemos la inclusión $\mathrm{Pic}(\mathcal{O}) \hookrightarrow \mathcal{L}_\mathcal{O}$ y, para cada $[\Lambda'] \in \mathcal{L}_\mathcal{O}$, por la Proposición 3.10 existe una única clase $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$ tal que $[\mathfrak{a}^{-1}] * [\Lambda] = [\Lambda']$, i. e., Λ' es homotético a $\mathfrak{a}\mathcal{O} = \mathfrak{a}$ y $[\Lambda'] = [\mathfrak{a}]$. □

[5] Recordemos que una acción de G en X se dice transitiva si dados $x, y \in X$ existe un $g \in G$ tal que $y = g \cdot x$; si además el g que relaciona x e y es único, la acción se dice simplemente transitiva.

3.2. Módulos singulares y multiplicación compleja

Con todo lo visto hasta ahora ya podemos explicar la segunda pieza del *Jugendtraum* de Kronecker: los *módulos singulares*, para lo cual seguiremos el Capítulo 2 de [18] y el Capítulo 3 de [6]. Diremos que un número complejo es un *módulo singular* (o *j-invariante singular*) si es el j-invariantes de un retículo con multiplicación compleja. Comenzaremos esta sección demostrando, mediante la teoría que hemos desarrollado y un ingrediente extra: las *curvas elípticas*, que los módulos singulares son números algebraicos. Concluiremos usando el Teorema Principal de la multiplicación compleja para demostrar que, de hecho, los módulos singulares son enteros algebraicos y dando exactamente su grado, con lo que podremos explicar completamente las Tablas 2.1, B.1 y B.2 y un curioso fenómeno de números irracionales (de hecho transcendentes) que son *casi* enteros.

3.2.1. Algebricidad de los módulos singulares

Queremos probar el siguiente teorema:

Teorema 3.12. *Sea $\mathcal{O}$ un orden en un cuerpo imaginario cuadrático K y sea $\mathfrak{a}$ un ideal fraccionario de $\mathcal{O}$. Entonces $j(\mathfrak{a})$ es un número algebraico de grado a lo sumo $h(\mathcal{O})$.*

Para ello necesitaremos desviarnos momentáneamente al mundo de las *curvas elípticas*, donde los órdenes surgen de forma natural como los endomorfismos de estos objetos. Por motivos de espacio sólo enunciaremos los resultados necesarios, cuyas demostraciones pueden ser encontradas en [17] y [18].

Definición 3.13. Definimos[6] una *curva elíptica* (sobre $\mathbb{C}$) como las soluciones en $\mathbb{C}$ a la ecuación

$$E : y^2 = 4x^3 - Ax - B, \quad \text{con } A, B \in \mathbb{C} \text{ y } 4A^3 - 27B^3 \neq 0.$$

junto a un *punto en el infinito* O. A estas curvas se les asocia la cantidad

$$j(E) = \frac{1728A^3}{4A^3 - 27B^2},$$

denominada el *j-invariante* de E.

Estas curvas tienen estructura de grupo abeliano mediante una construcción geométrica (cf. [17, III.§2.])[7]. Y, como podemos observar, si tenemos un retículo Λ en $\mathbb{C}$ y tomamos $A = g_2(\Lambda)$ y $B = g_3(\Lambda)$, $j(E) = j(\Lambda)$, por lo que estaremos interesados en curvas elípticas de la forma

$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda).$$

Recíprocamente, tenemos el siguiente resultado ([18, I. Corolario 4.3]):

Teorema 3.14 (Teorema de uniformización)**.** *Para cada curva elíptica E (sobre $\mathbb{C}$) existe un único retículo $\Lambda \subset \mathbb{C}$ tal que $E = E_\Lambda$ y un isomorfismo de grupos abelianos y de variedades complejas $E \cong \mathbb{C}/\Lambda$.*

[6] Se pueden definir en mayor generalidad como curvas algebraicas proyectivas suaves de género 1 sobre un cuerpo K junto a un punto K-racional y deducir de ahí mediante el Teorema de Rieman-Roch un modelo polinómico análogo al que describimos, denominado *modelo de Weierstrass* (cf. [17, III. Prop. 3.1]). Sin embargo, por motivos de extensión nos ceñiremos a este caso.

[7] Siguiendo la definición abstracta se puede obtener directamente y evitar largas comprobaciones (cf. [17, III. Proposición 3.4]).

Todo ello nos da una correspondencia entre curvas elípticas y retículos, teniéndose además que dos curvas elípticas son isomorfas si y sólo si sus correspondientes retículos son homotéticos, que $j(E) = j(\Lambda)$ y que el anillo de *endomorfismos*[8] de E, $\mathrm{End}(E)$, es isomorfo al de Λ; en particular, si $\mathrm{End}(E) \cong \mathbb{Z}$ o $\mathrm{End}(E) \cong \mathcal{O}$ con $\mathcal{O}$ un orden imaginario cuadrático.

Con esto, podemos concluir que si $\mathcal{O}$ es un orden en un cuerpo cuadrático imaginario, tenemos una biyección entre las curvas elípticas sobre $\mathbb{C}$ con endomorfismos por $\mathcal{O}$ (módulo isomorfismo de curvas sobre $\mathbb{C}$) y $\mathcal{L}_{\mathcal{O}}$. Así pues, dado un automorfismo $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$, si definimos E^σ como la curva elíptica resultante al cambiar A y B por $\sigma(A)$ y $\sigma(B)$, tenemos que $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E)$ (componiendo los endomorfismos con σ) y $j(E^\sigma) = \sigma(j(E))$. Pasamos así a la demostración del teorema:

Demostración del Teorema 3.12. Sea $E = E_{\mathfrak{a}}$ la curva elíptica correspondiente al retículo $\mathfrak{a} \subset \mathbb{C}$. Fijado $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$, $\mathrm{End}(E) \cong \mathrm{End}(E^\sigma) \cong \mathcal{O}$, por lo que E^σ sólo puede corresponder a un retículo de $\mathcal{L}_{\mathcal{O}}$ y, por el Teorema 3.11, hay exactamente $h(\mathcal{O})$ de ellos; luego $\sigma(j(\mathfrak{a})) = \sigma(j(E)) = j(E^\sigma)$ sólo puede tomar $h(\mathcal{O})$ valores distintos, por lo que $j(\mathfrak{a})$ es un número algebraico de grado a lo sumo $h(\mathcal{O})$. □

3.2.2. Integralidad de los módulos singulares

Comenzamos esta sección enunciando uno de los resultados centrales de la Teoría de la Multiplicación Compleja, cuya demostración se puede encontrar en [18, Teorema 8.2]:

Teorema 3.15 (Teorema Principal de la Multiplicación Compleja)**.** *Sea $\mathcal{O}$ un orden en el cuerpo imaginario cuadrático K y sea L el cuerpo de descomposición de $H(x)$ sobre K. Existe un isomorfismo de grupos*

$$\Psi : \mathrm{Gal}(L/K) \longrightarrow \mathrm{Pic}(\mathcal{O})$$

que conmuta con las acciones de $\mathrm{Pic}(\mathcal{O})$ y $\mathrm{Gal}(L/K)$ en $\mathcal{L}_{\mathcal{O}}$. En particular, L/K es una extensión abeliana que contiene todos los $j(\mathfrak{a})$.

El cuerpo de descomposición de $H(x)$ se denomina el *cuerpo de clases de anillo* de $\mathcal{O}$ y, en el caso $\mathcal{O} = \mathcal{O}_K$, el *cuerpo de clases de Hilbert* de K. Con esto, casi podemos probar nuestro objetivo final:

Teorema 3.16. *Sea $\mathcal{O}$ un orden imaginario cuadrático y sea $\mathfrak{a}$ un ideal fraccionario de $\mathcal{O}$. $j(\mathfrak{a})$ es un número algebraico de grado $h(\mathcal{O})$ y el polinomio de clases de Hilbert $H(x)$ (definido en el capítulo anterior) es su polinomio mínimo. Además, $L = K(j(\mathfrak{a}))$ para cada ideal fraccionario $\mathfrak{a}$ de $\mathcal{O}$.*

Demostración. Sea L el cuerpo de descomposición de $H(x)$. Por el Teorema anterior, $\#\,\mathrm{Gal}(L/K) = \#\,\mathrm{Pic}(\mathcal{O})$, que es por definición el grado de $H(x)$ y, por la Proposición 3.10 junto al Teorema anterior tenemos que $\mathrm{Gal}(L/K)$ actúa transitivamente en las raíces de $H(x)$, por lo que $H(x)$ es irreducible sobre K y cualquiera de sus raíces genera L. Esto nos da directamente que $[\mathbb{Q}(j(\mathfrak{a})) : \mathbb{Q}] = [K(j(\mathfrak{a})) : K] = [L : K] = h(\mathcal{O})$. □

[8] Esto es, un *morfismo de variedades* $\psi : E \to E$ tal que $\psi(O) = O$. La estructura de anillo viene inducida por la ley de grupo de E y la composición de funciones.

Por último, omitiremos la demostración de que $H(x)$ es un polinomio con coeficientes enteros por cuestiones de espacio; esta se puede encontrar en [18, II. §6.] ó [6, III.], pero con ello obtenemos el resultado que buscábamos:

Teorema 3.17. *Sea $\mathcal{O}$ un orden en un cuerpo imaginario cuadrático y sea $\mathfrak{a}$ un ideal fraccionario en $\mathcal{O}$. $j(\mathfrak{a})$ es un entero algebraico de grado $h(\mathcal{O})$.*

Esto, como mencionamos al final del capítulo anterior, nos permite calcular explícitamente los polinomios $H(x)$ mediante el cálculo numérico $\prod(x - j(\mathfrak{a}))$, donde $\mathfrak{a}$ recorre un sistema completo de representantes de $\mathrm{Pic}(\mathcal{O})$, usando suficiente precisión. En cualquier caso, usando `Magma` podemos generar una curva elíptica con el j-invariante dado y comprobar que en efecto se tiene multiplicación compleja, sirviendo así como segunda revisión de las tablas. Para ello usamos, respectivamente, las funciones `EllipticCurveFromjInvariant` y `HasComplexMultiplication`.

Por otra parte, la función $j(\tau) = j(\mathbb{Z} + \tau\mathbb{Z})$ es 1-periódica, por lo que tiene desarrollo de Fourier, cuyos primeros términos son (cf. [18, Observación 7.4.1])

$$j(\tau) = 1/q + 744 + 196884q + 21493760q^2 + \ldots \text{ donde } q = e^{2\pi i\tau}.$$

Esto explica, entre otras cosas, el conocido fenómeno de que $e^{\pi\sqrt{163}}$ sea *casi* un entero, pues como ya hemos visto, -163 es un discriminante con número de clases 1, por lo que usando el teorema anterior $j((1+\sqrt{-163})/2) \in \mathbb{Z}$ y, tomando $\tau = (1+\sqrt{-163})/2$, $q = -e^{-\pi\sqrt{163}}$ es del orden de 10^{-18}, teniéndose así que $1/q \approx j(\tau) - 744 \in \mathbb{Z}$.

Claramente no hay nada de especial en el -163 (salvo que es el discriminante más grande con número de clases 1), por lo que podríamos realizar un proceso similar con números de clase mayores para obtener más *casi enteros*. Por ejemplo, con el orden $\mathcal{O} = \mathbb{Z} + 5\mathbb{Z}[i]$ (cf. Tabla B.1), que tiene número de clases 2, podemos encontrar las raíces del polinomio mínimo de $j(\mathcal{O}) = j(5i)$ para llegar a que $j(5i) = 1728(12740595841 + 5697769392\sqrt{5})$, luego $j(5i) - 1728 \cdot 5697769392\sqrt{5} \in \mathbb{Z}$ y, en particular, tomando $q = e^{2\pi i\cdot(5i)} = e^{-10\pi}$ (del orden de 10^{-14}), obtenemos que

$$1/q - 1728 \cdot 5697769392\sqrt{5} \approx j(5i) - 1728 \cdot 5697769392\sqrt{5} - 744 \in \mathbb{Z}.$$

Haciendo el mismo juego con discriminantes más grandes (para obtener menor diferencia con respecto a un entero), podemos hacer lo mismo con el discriminante (fundamental) $d_K = -427$ y obtener que, tomando $q = e^{-\pi\sqrt{427}}$ (del orden de 10^{-29}),

$$1/q - 147197952000 \cdot 6789639488444631\sqrt{61} \approx j(\tau) - 744 \in \mathbb{Z}$$

De hecho, si calculamos estas cantidades numéricamente, obtenemos

$$\begin{aligned}
e^{\pi\sqrt{163}} &= 262537412640768743{,}99999999999925\ldots \\
e^{10\pi} - 1728 \cdot 5697769392\sqrt{5} &= 22015749612503{,}9999999955285\ldots \\
e^{\pi\sqrt{427}} - 147197952000 \cdot 6789639488444631\sqrt{61} &= 780572775626189195990630 4743{,}999999999999999999999987\ldots
\end{aligned}$$

APÉNDICE A

Resultados de Álgebra conmutativa y Teoría algebraica de números

A.1. Álgebra conmutativa

En la primera parte de este apéndice se enunciaran, y en su mayoría se demostrarán, algunos resultados fundamentales de Álgebra Conmutativa que han sido necesarios. Principalmente usaremos [1] y [14] para los resultados generales, y [15], [13] y [16] para los resultados sobre dependencia entera y dominios de Dedekind.

A.1.1. Resultados básicos y localización

Proposición A.1. *Todo anillo contiene un ideal maximal; además, si* $\mathfrak{a} \neq (1)$ *es un ideal, existe un ideal maximal que contiene a* $\mathfrak{a}$*.*

Demostración. Sea A un anillo. El conjunto de todos sus ideales distintos del total está parcialmente ordenado por inclusión, es no vacío (pues contiene a (0)) y todo subconjunto totalmente ordenado se puede acotar por su unión (que es de nuevo un ideal distinto del total, ya que 1 no está en ningún ideal propio de A); el resultado se sigue así del Lema de Zorn. Para la segunda parte basta aplicar la primera a $A/\mathfrak{a}$ y usar el teorema de correspondencia para anillos. □

Teorema A.2 (Teorema chino del resto)**.** *Sean* $\mathfrak{a}_1, ...\mathfrak{a}_n$ *ideales coprimos*[1] *dos a dos de un anillo* A *y sea* $\mathfrak{a} = \mathfrak{a}_1...\mathfrak{a}_n$*. Entonces existe un isomorfismo natural* $A/\mathfrak{a} \xrightarrow{\sim} \bigoplus_{i=1}^{n} A/\mathfrak{a}_i$ *dado por* $x \mapsto (x + \mathfrak{a}_1, ..., x + \mathfrak{a}_n)$*.*

Demostración. [1, Proposición 1.10] Primero se demuestra que, para dos ideales coprimos, el producto coincide con la intersección y por inducción lo mismo sucede para n ideales coprimos dos a dos; luego tomamos $a_i \in \mathfrak{a}_1$, $b_i \in \mathfrak{a}_i$ tales que $a_i + b_i = 1$, definimos $x = b_1...b_n$ y observamos que $x \equiv 1 \pmod{\mathfrak{a}_1}$ y $x \equiv 0 \pmod{\mathfrak{a}_i}$ para $i > 1$, por lo que el resultado se sigue del primer teorema de isomorfía para anillos. □

Definición A.3. Un conjunto de A-módulos (resp. grupos, anillos...) $\{M_n\}_n$ junto a homomorfismos de A-módulos (resp. grupos, anillos...) $\{f_n : M_n \to M_{n+1}\}_n$ se denomina una

[1] Recordemos que dos ideales $\mathfrak{a}$ y $\mathfrak{b}$ se dicen coprimos si $\mathfrak{a} + \mathfrak{b} = (1)$.

secuencia y se denota usualmente por

$$\ldots \to M_{n-1} \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \to \ldots$$

Una secuencia de A-módulos (resp. grupos, anillos...) se dice exacta si para cada n se tiene que $\ker f_n = \operatorname{Im} f_{n-1}$.

Lema A.4. *(Lema de la serpiente) Si tenemos un diagrama conmutativo de grupos abelianos (resp. anillos conmutativos o A-módulos)*[2] *con filas exactas*

$$\begin{array}{ccccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \end{array}$$

Existe un homomorfismo de grupos abelianos (resp. anillos conmutativos o A-módulos) $\ker c \xrightarrow{\delta} \operatorname{coker} a$ *que relaciona los núcleos y conúcleos en una sucesión exacta:*

$$\ker a \to \ker b \to \ker c \xrightarrow{\delta} \operatorname{coker} a \to \operatorname{coker} b \to \operatorname{coker} c.$$

Demostración. Sea $x \in \ker c$, como g es suprayectiva existe un $y \in B$ tal que $x = g(y)$ y, como el diagrama es conmutativo, $g'(b(y)) = c(x) = 0$, por lo que $b(y) \in \ker g'$. Como la fila inferior es exacta, $\ker g' = \operatorname{Im} f'$, teniendo así que $b(y) = f'(z)$ para cierto $z \in A'$; por inyectividad de f', este z es único. Definimos así $\delta(x) = z + \operatorname{Im} a$. Comprobar que δ es un homomorfismo bien definido y que la secuencia es exacta es rutinario (cf. [14, III. Lema 9.1]). □

Definición A.5. Sea A un anillo. Un subconjunto $S \subseteq A$ se dice *multiplicativo* si $xy \in S$ para todo $x, y \in S$ y $1 \in S$. En el conjunto $A \times S$ definimos la relación de equivalencia $(x, s) \sim (y, t)$ cuando $\exists r \in S : r(tx - sy) = 0$. Definimos la *localización* de A en S por $S^{-1}A = (A \times S)/\sim$ y denotamos $a/s = [(a, s)]$.

Proposición A.6. *La relación $\sim$ es, en efecto, una relación de equivalencia; las operaciones $\frac{a}{s} + \frac{b}{t} = \frac{ta+sb}{st}$ y $\frac{a}{s} \cdot \frac{b}{t}$ le dan a $S^{-1}A$ estructura de anillo y la aplicación natural $a \mapsto a/1$ es un homomorfismo de anillos. Además, si A es un dominio y $0 \notin S$, esta aplicación es inyectiva (por lo que identificamos A con un subanillo de $S^{-1}A$).*

Demostración. Ver la sección §4 de [14, Capítulo II]. □

Ejemplo A.7 (Localización en primos)**.** Sea A un dominio y $\mathfrak{p}$ un primo de A. El conjunto $S_\mathfrak{p} = A \setminus \mathfrak{p}$ es multiplicativo y obtenemos el anillo local de A en $\mathfrak{p}$, $A_\mathfrak{p} = S_\mathfrak{p}^{-1}A$.

Definición A.8. Definimos análogamente la localización de un A-módulo en un subconjunto multiplicativo S de A como $S^{-1}M = (M \times S)/\sim$, donde $(m, s) \sim (m', s')$ cuando $\exists t \in S : t(s'm - sm') = 0$, que se convierte en un $S^{-1}A$-módulo con las operaciones naturales. Cuando $S = A \setminus \mathfrak{p}$ usamos de nuevo la notación $M_\mathfrak{p}$.

[2] En mayor generalidad este resultado es cierto en *categorías abelianas*, pudiéndose demostrar además que la secuencia resultante es *natutral*; pero por simplicidad nos restringimos a los casos que necesitaremos.

Proposición A.9. *Sea A un anillo y S un sunbconjunto multiplicativo de A. Todo ideal de $S^{-1}A$ es de la forma $S^{-1}\mathfrak{a}$ para algún ideal $\mathfrak{a}$ de A; $S^{-1}\mathfrak{a} = S^{-1}A$ si y sólo si $\mathfrak{a} \cap S \neq \emptyset$; y hay una correspondencia biyectiva entre ideales primos de A que no intersecan a S e ideales primos de $S^{-1}A$ dada por $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ y con inversa $\mathfrak{P} \mapsto \mathfrak{P} \cap A$.*

Demostración. Ver (i) y (iv) de [1, Proposición 3.11]. □

Corolario A.10. *Sea $\mathfrak{p}$ un ideal primo de A. Los ideales primos de $A_\mathfrak{p}$ están en correspondencia biyectiva con los ideales primos de A contenidos en $\mathfrak{p}$; en particular, $A_\mathfrak{p}$ es un anillo local*[3]*. Además, si $\mathfrak{m}$ es un ideal maximal de A y $\mathfrak{m}_\mathfrak{p} = \mathfrak{m}A_\mathfrak{p}$, tenemos un isomorfismo natural $A/\mathfrak{p}^n \cong A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^n$ para todo $n \geq 1$.*

Demostración. Para la primera parte basta tomar $S = A \setminus \mathfrak{p}$ en la proposición anterior y observar que si $\mathfrak{m}$ es un ideal maximal de $A_\mathfrak{p}$, es primo, por lo que $\mathfrak{m} \cap A \subseteq \mathfrak{p}$, luego $\mathfrak{m} \subseteq S^{-1}\mathfrak{p}$ y $\mathfrak{m} = S^{-1}\mathfrak{p}$ por maximalidad. Para la segunda parte consideramos nos referimos a [15, I. Corolario 11.2]. □

Proposición A.11. *Si A es un dominio noetheriano y S un subconjunto multiplicativo, $S^{-1}A$ también es noetheriano.*

Demostración. Sea $\mathfrak{A}$ un ideal de $S^{-1}A$ y consideremos $\mathfrak{a} = \mathfrak{A} \cap A$; por la Proposición A.9, $\mathfrak{A} = S^{-1}\mathfrak{a}$, por lo que si $\mathfrak{a}$ es finitamente generado, $\mathfrak{A}$ también. Como en un anillo noetheriano todos los ideales son finitamente generados, concluimos que $S^{-1}A$ es noetheriano. □

A.1.2. Anillos de valoración discreta

Definición A.12. Un *anillo de valoración discreta* es un dominio de ideales principales A con un único ideal primo no nulo.

Observación A.13. *Como todo elemento $a \in A \setminus \mathfrak{p}$ es una unidad, si escribimos $\mathfrak{p} = (\pi)$, todos los elementos no nulos de A se escriben de forma única*[4] *como $u\pi^n$ con $u \in A^\times$ y $n \geq 0$. Así, todo elemento del cuerpo de fracciones K de A se expresa de forma única como $x = \varepsilon\pi^n$ con $\epsilon \in A^\times$ y $n \in \mathbb{Z}$. El exponente de π en la expresión anterior se denomina valoración de x y se denota $v(x)$, obteniendo así una función suprayectiva $v : K^\times \to \mathbb{Z}$ que, con la convención $v(0) = \infty$, cumple que para todo $x, y \in K$, $v(xy) = v(x) + v(y)$ y $v(x + y) \geq \min\{v(x), v(y)\}$.*

Proposición A.14. *Sea K un cuerpo y $v : K^\times \to \mathbb{Z}$ un homomorfismo suprayectivo tal que $v(x + y) \geq \min\{v(x), v(y)\}$, entonces $A = \{x \in K : v(x) \geq 0\} \cup \{0\}$ es un anillo de valoración discreta con cuerpo de fracciones K y valoración asociada v.*

Demostración. Basta tomar $\pi \in K^\times$ tal que $v(\pi) = 1$ (que es posible por suprayectividad) y observar que si $x \in A$, $x = 0$ o $v(x\pi^{-v(x)}) = 0$, por lo que $x = u\pi^n$ con $n = v(x) \geq 0$ y $u = x\pi^{-v(x)}$; esto nos da que todo ideal no nulo de A es de la forma (π^n), teniéndose así que es un dominio de valoración discreta. □

[3] Recordemos que un anillo se dice local si tiene un único ideal maximal.

[4] Todos los ideales no nulos de A o son todo A o están contenidos en el ideal $\mathfrak{p}$, por lo que son de la forma (π^n) para $n \geq 0$; si $u_1\pi^{n_1} = u_2\pi^{n_2}$, digamos con $n_1 \geq n_2$, $\pi^{n_2}(u_1\pi^{n_1-n_2} - u_2) = 0$, por lo que $\pi^{n_1-n_2} = u_1^{-1}u_2$ y necesariamente $n_1 = n_2$, luego $(u_1 - u_2)\pi^{n_1} = 0$ y $u_1 = u_2$.

Proposición A.15. *Sea A un anillo conmutativo. A es un dominio de valoración discreta si y sólo si es un anillo local noetheriano cuyo ideal maximal está generado por un nilpotente (esto en general, como trataremos con dominios, será simplemente pedir que sea un ideal principal).*

Demostración. La implicación directa es inmediata. Para el recíproco probaríamos primero que $\bigcap \mathfrak{m}^n = 0$ (donde $\mathfrak{m} = (\pi)$ es el ideal maximal de A), por lo que si $y \in A$ es un elemento no nulo, podemos escribir $y = u\pi^n$ para cierto $n \geq 0$ y $u \notin \mathfrak{m}$, que al igual que demostramos al definir la valoración asociada a un anillo de valoración discreta, se escribe así de forma única; luego definimos $v(y) = n$, que se comprueba que es una valoración y usamos la Proposición A.14. Los detalles se pueden encontrar en [16, I. Proposición 2]. □

Teorema A.16. *Sea A un dominio noetheriano. A es un dominio de valoración discreta si y sólo si A tiene un único ideal primo no nulo y todos los elementos $\alpha \in K$ tales que $f(\alpha) = 0$ para algún polinomio mónico (no nulo) $f \in A[x]$ pertenecen a A.*

Demostración. Si A es un dominio de valoración discreta, tiene un único ideal primo no nulo por definición; si $\alpha \in K$ es tal que

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

y $\alpha \notin A$, entonces $v(\alpha) = -m$ para cierto $m > 0$, de forma que $v(\alpha^n) = -nm$ y $v(a_j\alpha^j) \geq -(n-1)m > -nm$, de donde se llega a una contradicción usando que si $x_1, ..., x_n \in K$ y $v(x_j) > v(x_1)$ para todo $j \geq 2$ entonces $x_1 + ... + x_n \neq 0$. Una demostración de este último resultado y del recíproco se puede encontrar en [16, I. Proposición 3]. □

A.1.3. Dominios de Dedekind

Enteros algebraicos

Definición A.17. Sean $A \subseteq B$ anillos; $b \in B$ se dice *entero* (algebraico) sobre A si hay un polinomio mónico $f(x) \in A[x]$ no nulo con $f(b) = 0$. Si todos los elementos de B son enteros sobre A, B se dice entero sobre A.

Como podemos observar, al menos cuando B está contenido en un cuerpo (es decir, cuando A y B son dominios), los enteros algebraicos de B sobre A son algebraicos del cuerpo de fracciones de B sobre el de A; recíprocamente, podemos obtener enteros *quitando denominadores* a los algebraicos:

Proposición A.18. *Sea A un dominio con cuerpo de fracciones K y α algebraico sobre K; existe $a \in A \setminus \{0\}$ tal que $a\alpha$ es entero sobre A.*

Demostración. Sea α un número algebraico sobre K, digamos con polinomio mínimo

$$f(x) = x^n + c_{n-1}x^{n-1} + ... + c_1x + c_0,$$

escribimos $c_j = a_j/b_j$ con $a_j, b_j \in A$ y tomamos $a = b_0...b_{n-1}$, de forma que, multiplicando por a^n,

$$(a\alpha)^n + a_{n-1}(a\alpha)^{n-1} + aa_{n-2}(a\alpha)^{n-2} + ... + a^{n-2}a_1(a\alpha) + a^{n-1}a_0 = 0,$$

luego $a\alpha$ es entero sobre A. □

Como es natural, cabe esperar que esta clase de números tuviese más estructura, como mínimo de anillo (pues la suma y el producto de algebraicos son algebraicos). Esto no es inmediato a partir de la definición; para probarlo será útil trasladarnos al lenguaje de módulos:

Proposición A.19. *$b_1, ..., b_n \in B$ son enteros sobre A si y sólo si $A[b_1, ..., b_n]$ es un A-módulo finitamente generado. En particular si $b_1, b_2 \in B$ son enteros sobre A, $b_1 + b_2$ y $b_1 b_2$ también lo son y si C es entero sobre B y B es entero sobre A, C lo es sobre A.*

Demostración. Si $b \in B$ es entero sobre A, existe un $f \in A[x]$ mónico con $f(b) = 0$. Ahora, si $g \in A[x]$, existen $q, r \in A[x]$ tales que el grado de r es menor que el de f y $g = qf + r$, de forma que $g(b) = r(b)$, luego $\{1, b, ..., b^{n-1}\}$ (donde n es el grado de f) genera $A[b]$. El caso general se sigue por inducción. Recíprocamente, si $A[b_1, .., b_n]$ es finitamente generado como A-módulo, digamos por $\omega_1, ..., \omega_r$, entonces dado $b \in A[b_1, ..., b_n]$ existen $a_{ij} \in A$ tales que

$$b\omega_i = \sum_{j=1}^{r} a_{ij}\omega_j, \quad \text{para todo } i \in \{1, ..., r\}.$$

Así, $(bI - M)\omega_i = 0$, donde I es la matriz identidad de dimensión r y $M = (a_{ij})$, por lo que $\det(bI - M)\omega_i = 0$ para todo i (multiplicando por el adjunto), luego $\det(bI - M) = 0$, lo que nos da desarrollando el determinante una ecuación mónica para b con coeficientes en A. □

De esto deducimos que $\bar{A} = \{b \in B \mid b \text{ entero sobre } A\}$ es un anillo entero sobre A, que denominamos la *clausura entera* de A en B. Y, si A es un dominio que coincide con su clausura entera en su cuerpo de fracciones, decimos que A es *normal*.

Los ejemplos más sencillo de anillos normal son los dominios de factorización única; pero, como veremos más adelante, la factorización única es una propiedad que en general no tendremos.

Proposición A.20. *Si A es un dominio de factorización única, A es normal.*

Demostración. Sea K el cuerpo de fracciones de A y tomemos $\alpha \in K$ entero sobre A. Como A es un DFU, podemos escribir $\alpha = a/b$ con $a, b \in A$, $b \neq 0$ en mínimos términos (es decir, si $c \mid b$ y $c \mid a$, entonces $c \in A^\times$); así, por ser α entero sobre A, existen $a_0, ..., a_{n-1} \in A$ tales que

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

y, multiplicando por b^n a ambos miembros,

$$a^n + a_{n-1}a^{n-1}b + ... + a_1 a b^{n-1} + a_0 b^n = 0,$$

luego $b \mid a^n$, por lo que $b \mid a$ y $b \mid b$, teniéndose así que $b \in A^\times$ y, por tanto, $\alpha \in A$. □

Por otra parte, ser entero y, en particular, normal, es una propiedad que se preserva al localizar:

Proposición A.21. *Si A y B son dominios con B entero sobre A y S es un subconjunto multiplicativo de A, $S^{-1}B$ es entero sobre $S^{-1}A$; además, si A es normal, $S^{-1}A$ también.*

Demostración. Para la primera parte basta observar que si $\alpha \in S^{-1}B$, $s\alpha \in B$ para cierto $s \in S$, por lo que $s\alpha$ es entero sobre A y, escribiendo una ecuación mónica con coeficientes en A para $s\alpha$ y diviendo por s^n (donde n es el máximo exponente de la ecuación) obtenemos que α es entero sobre $S^{-1}A$, de forma que $S^{-1}B$ es entero sobre $S^{-1}A$. Por otra parte, si A es normal y $\alpha \in K$ satisface una ecuación mónica con coeficientes en $S^{-1}A$, procedemos como en la Proposición A.18 observando que ahora todos los denominadores están en S. □

Pasamos ahora a estudiar cómo se comportan los ideales primos en extensiones enteras:

Proposición A.22. *Sean A y B dominios con B entero sobre A y $\mathfrak{p}$ un ideal primo de A. Entonces $\mathfrak{p}B \neq B$ y existe un ideal primo $\mathfrak{P}$ de B tal que $\mathfrak{p} = \mathfrak{P} \cap A$.*

Demostración. Localizando en $\mathfrak{p}$ tenemos por la Proposición A.21 que $B_\mathfrak{p}$ es entero sobre $A_\mathfrak{p}$ y por el Corolario A.10, $A_\mathfrak{p}$ es un anillo local con ideal maximal $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$ y

$$\mathfrak{p}B_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}B_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}B_\mathfrak{p};$$

así, si $\mathfrak{p}B = B$, $\mathfrak{m}_\mathfrak{p}B_\mathfrak{p} = B_\mathfrak{p}$ y podemos escribir $1 = a_1b_1 + ... + a_nb_n$ con $a_j \in \mathfrak{m}_\mathfrak{p}$ y $b_j \in B_\mathfrak{p}$; luego tomando $B_0 = A_\mathfrak{p}[b_1, ..., b_n]$, B_0 es un $A_\mathfrak{p}$-módulo finitamente generado tal que $\mathfrak{m}_\mathfrak{p}B_0 = B_0$, luego el Lema de Nakayama nos da que $B_0 = 0$, que es una contradicción. Tenemos así que $\mathfrak{p}B \neq B$ y $\mathfrak{m}_\mathfrak{p}B_\mathfrak{p} \neq B_\mathfrak{p}$, por lo que existe un ideal maximal (por la Proposición A.1) $\mathfrak{M}$ de $B_\mathfrak{p}$ que contiene a $\mathfrak{m}_\mathfrak{p}B_\mathfrak{p}$, por lo que por maximalidad de $\mathfrak{m}_\mathfrak{p}$ en $A_\mathfrak{p}$, $\mathfrak{M} \cap A_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}$. Así pues, tomando $\mathfrak{P} = \mathfrak{M} \cap B$, $\mathfrak{P} \cap A = \mathfrak{p}$. □

Cuando $\mathfrak{p} = \mathfrak{P} \cap A$ como en la proposición anterior, diremos que $\mathfrak{P}$ *está sobre* $\mathfrak{p}$.

Proposición A.23. *Sean A y B dominios con B entero sobre A y sean $\mathfrak{P}$ un primo de B y $\mathfrak{p}$ un primo de A con $\mathfrak{p} = \mathfrak{P} \cap A$. $\mathfrak{P}$ es maximal si y sólo si $\mathfrak{p}$ es maximal.*

Demostración. Si $\mathfrak{p}$ es maximal, $A/\mathfrak{p}$ es un cuerpo y $B/\mathfrak{P}$ es un dominio entero sobre $A/\mathfrak{p}$, lo que implica que $B/\mathfrak{P}$ es un cuerpo[5] y, por tanto, $\mathfrak{P}$ es maximal. Recíprocamente, si $\mathfrak{P}$ es maximal, $B/\mathfrak{P}$ es un cuerpo entero sobre el dominio $A/\mathfrak{p}$, que si no fuese un cuerpo tendría un ideal maximal no nulo (por Proposición A.1) y, por la proposición anterior, existiría un ideal primo no nulo en $B/\mathfrak{P}$, contradiciendo que $B/\mathfrak{P}$ es un cuerpo. □

Por último, consideremos un dominio A normal con cuerpo de fracciones K, L/K una extensión de Galois finita y B la clausura entera de A en L. Si $\mathfrak{p}$ es un ideal maximal de A, el grupo de Galois $\mathrm{Gal}(L/K)$ actúa transitivamente sobre el conjunto de ideales sobre $\mathfrak{p}$, i.e., sobre los primos $\mathfrak{P}$ de B tales que $\mathfrak{P} \cap A = \mathfrak{p}$ (cf. [13, I. Proposición 11]) y obtenemos como corolario el siguiente resultado:

Proposición A.24. *Con la notación anterior, hay un número finito de ideales de B sobre $\mathfrak{p}$.*

Demostración. Basta usar que $\mathrm{Gal}(L/K)$ es un grupo finito que actúa transitivamente sobre los primos sobre B. □

[5] Si $\alpha \in B/\mathfrak{P}$ es distinto de 0, α es algebraico sobre el cuerpo $A/\mathfrak{p}$, por lo que $A/\mathfrak{p}[\alpha]$ es un cuerpo y α es invertible.

Factorización de ideales y grupo de clases

La idea principal es formalizar la noción de *número ideal* de Kummer mediante dominios; hoy los conocemos como ideales. Esta construcción pretende *solucionar* el problema de la factorización única y hacer aritmética con ellos; sin embargo, para dividir necesitamos una clase más grande de ideales:

Definición A.25. Sea A un dominio con cuerpo de fracciones K. Un *ideal fraccionario* $\mathfrak{a}$ de A (o de K sobre A) es un A-submódulo de K tal que $r\mathfrak{a} \subseteq A$ para cierto $r \in A \setminus \{0\}$ (observamos que si $\mathfrak{a}$ es finitamente generado, podemos tomar r como el producto de todos los denominadores de un conjunto finito de generadores de $\mathfrak{a}$; recíprocamente, si A es noetheriano esto implica que $r\mathfrak{a}$ es finitamente generado y, por tanto, $\mathfrak{a}$ también). Para cada ideal fraccionario $\mathfrak{a}$ de A definimos además el conjunto

$$\mathfrak{a}^{-1} = \{\alpha \in K \,:\, \alpha\mathfrak{a} \subseteq A\}.$$

Supondremos siempre que los ideales fraccionarios son no nulos y, para evitar confusión, a veces nos referiremos a los ideales usuales como *ideales enteros*.

Sin embargo, no es cierto que en todos los dominios estos ideales factoricen de forma única en primos, por lo que nos restringimos a los anillos que si lo cumplen:

Definición A.26. Un *dominio de Dedekind* es un dominio noetheriano, normal y de dimensión (de Krull[6]) 1.

Probaremos el siguiente resultado siguiendo la demostración de [4, I.§2. Proposición 1]:

Teorema A.27. *Sea A un dominio. Son equivalentes:*

(i) *A es un dominio de Dedekind.*

(ii) *A es noetheriano y para todo ideal primo no nulo $\mathfrak{p}$, $A_\mathfrak{p}$ es un anillo de valoración discreta.*

(iii) *Todos los ideales fraccionarios de A son invertibles*[7].

Demostración. Demostramos $(i) \implies (ii) \implies (iii) \implies (i)$:
$[(i) \implies (ii)]$ Sea A un dominio de Dedekind. Como A es noetheriano y normal, si $\mathfrak{p}$ es un ideal primo no nulo de A, $A_\mathfrak{p}$ también es noetheriano y normal por las Proposiciones A.11 y A.21 y, si $\mathfrak{P}$ es un ideal primo no nulo de $A_\mathfrak{p}$, $\mathfrak{P} \subseteq \mathfrak{m}_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$ (recordemos que por el Corolario A.10, $A_\mathfrak{p}$ es un anillo local con ideal maximal $\mathfrak{m}_\mathfrak{p}$), por lo que $\mathfrak{P} \cap A$ es un ideal primo no nulo contenido en $\mathfrak{p}$ y, como A tiene dimensión 1, $\mathfrak{P} \cap A = \mathfrak{p}$, de donde se sigue que $\mathfrak{P} = \mathfrak{m}_\mathfrak{p}$. Luego por el Teorema A.16, $A_\mathfrak{p}$ es un anillo de valoración discreta.
$[(ii) \implies (iii)]$ Sea $\mathfrak{a}$ un ideal fraccionario con generadores $a_1, ..., a_n$ y sea $\mathfrak{p}$ un ideal primo no nulo. Como $A_\mathfrak{p}$ es un anillo de valoración discreta, le corresponde una valoración $v_\mathfrak{p}$ y, podemos escoger así el a_j de valoración mínima, digamos a_1; tenemos entonces que $\mathfrak{a}A_\mathfrak{p} = a_1A_\mathfrak{p}$ y, por tanto, $a_1^{-1}a_i = x_iy_i^{-1}$ para ciertos $x_i \in A$, $y_i \in A \setminus \mathfrak{p}$, de forma que si

[6] En este caso quiere decir que no es un cuerpo y que todo ideal primo no nulo es maximal; en general la dimensión de Krull se define como el supremo de los n tales que podemos formar una cadena estricta de ideales primos $\mathfrak{p}_0 \subset ... \subset \mathfrak{p}_n$.

[7] Decimos que un ideal fraccionario $\mathfrak{a}$ es invertible si $\mathfrak{a}\mathfrak{a}^{-1} = (1)$.

definimos $y = y_1...y_n$, $ya_1^{-1}a_i \in A$ para todo i, luego $ya_1^{-1} \in \mathfrak{a}^{-1}$ y, por tanto, $y \in \mathfrak{a}\mathfrak{a}^{-1}$. Como $y \notin \mathfrak{p}$ concluimos que $\mathfrak{a}\mathfrak{a}^{-1} \not\subseteq \mathfrak{p}$ y, como esto es válido para todo ideal maximal $\mathfrak{p}$, necesariamente $\mathfrak{a}\mathfrak{a}^{-1} = A$.
$[(iii) \implies (i)]$ Sea $\mathfrak{a}$ un ideal fraccionario de A. Como $\mathfrak{a}\mathfrak{a}^{-1} = A$, existen $a_1, ..., a_n \in \mathfrak{a}$ y $b_1, ..., b_n \in \mathfrak{a}^{-1}$ tales que $a_1b_1 + ... + a_nb_n = 1$, por lo que si $x \in \mathfrak{a}$, $x = a_1(b_1x) + ...a_n(b_nx)$, pòr lo que $a_1, ..., a_n$ generan $\mathfrak{a}$ y podemos concluir así que A es noetheriano. Si $\alpha \in K$ es entero sobre A, por la Proposición A.19, $B = A[\alpha]$ es un A-submódulo de K finitamente generado y, por tanto, un ideal fraccionario de A, por lo que es invertible y, al ser también un anillo $BB = B$, por lo que $B = BA = B(BB^{-1}) = BB^{-1} = A$, teniéndose así que $\alpha \in A$ y que A es normal. Por último, si $\mathfrak{p}$ es un ideal primo no nulo de A y $\mathfrak{m}$ un ideal maximal que lo contiene, entonces $\mathfrak{p}\mathfrak{m}^{-1}$ es un ideal de A y $(\mathfrak{p}\mathfrak{m}^1)\mathfrak{m} = \mathfrak{a}$, por lo que o bien $\mathfrak{m} \subseteq \mathfrak{p}$ (en cuyo caso $\mathfrak{p} = \mathfrak{m}$ por maximalidad) o bien $\mathfrak{p}\mathfrak{m}^{-1} \subseteq \mathfrak{p}$, en cuyo caso $\mathfrak{m}^{-1} = (\mathfrak{p}^{-1}\mathfrak{p})\mathfrak{m}^{-1} \subseteq \mathfrak{p}^{-1}\mathfrak{p} = A$, lo que implica que $A \subseteq \mathfrak{m}$, que es imposible. □

La primera observación, es que esto nos da que los ideales fraccionarios de A forman un grupo abeliano (con el producto), por lo que podemos definir

Definición A.28. Definimos el *grupo de ideales* $J(A)$ de un dominio A como el conjunto de todos los ideales fraccionarios invertibles de A; en particular, si A es un dominio de Dedekind $J(A)$ consiste en todos los ideales fraccionarios (no nulos) de A. Definimos además el grupo de ideales principales $P(A)$ como el grupo formado por todos los ideales fraccionarios de la forma αA con $\alpha \in K^\times$ (observamos que todos los ideales de esta forma son invertibles, pues $(\alpha A)(\alpha^{-1}A) = A$). Con esto, podemos definir el *grupo de clases* o *grupo de Picard* de A como $\mathrm{Pic}(A) = J(A)/P(A)$; el número de elementos de este grupo se denomina *número de clases* y se denota por $h(A)$.

Probamos ahora que el grupo de ideales de un dominio de Dedekind es libre generado por los ideales primos no nulos, esto es, que hay factorización única de ideales en ideales primos:

Teorema A.29 (Factorización única de ideales)**.** *Sea A un dominio de Dedekind. Todo ideal entero propio y no nulo de A factoriza de forma única (salvo orden) como producto de primos; en particular, $J(A)$ es un grupo abeliano libre generado por los ideales primos no nulos de A.*

Demostración. Sea $\mathfrak{a} \neq 0$ un ideal propio de A. Tomemos $\mathfrak{p}_1$ un ideal maximal que contenga a $\mathfrak{a}$ (Proposición A.1), entonces tenemos que $\mathfrak{a} = \mathfrak{p}_1(\mathfrak{p}_1^{-1}\mathfrak{a})$; definimos $\mathfrak{b}_1 = \mathfrak{p}_1^{-1}\mathfrak{a}$ e iteramos este proceso (i.e., dado $\mathfrak{b}_n$ tomamos un ideal maximal $\mathfrak{p}_{n+1}$ que contenga a $\mathfrak{b}_n$ y definimos $\mathfrak{b}_{n+1} = \mathfrak{p}_{n+1}^{-1}\mathfrak{b}_n$), obteniendo así una cadena ascendente de ideales $\mathfrak{b}_1 \subseteq \mathfrak{b}_2 \subseteq ...$, que se tiene que estabilizar por ser A noetheriano, obteniendo así que $\mathfrak{a}$ es un producto finito de ideales primos no nulos. Para la unicidad observamos que si $\mathfrak{p}_1...\mathfrak{p}_n = \mathfrak{q}_1...\mathfrak{q}_m$, son dos factorizaciones en primos, $\mathfrak{q}_1...\mathfrak{q}_m \subseteq \mathfrak{p}_1$ y, entonces por primalidad[8] de $\mathfrak{p}_1$de $\mathfrak{p}_1$ $\mathfrak{q}_j \subseteq \mathfrak{p}_1$ para algún j y, por maximalidad de $\mathfrak{q}_j$, tenemos que $\mathfrak{q}_j = \mathfrak{p}_1$; multiplicamos por el inverso de estos dos elementos en la igualdad e iteramos el proceso, obtenemos así que $n = m$ y que existe un $\sigma \in S_n$ (el grupo simétrico en n elementos) tal que $\mathfrak{p}_i = \mathfrak{q}_{\sigma(i)}$ para todo i. □

Con este teorema podemos definir para cada ideal fraccionario $\mathfrak{a}$ de A y cada primo no nulo $\mathfrak{p}$ de A el entero $v_\mathfrak{p}(\mathfrak{a}) \in \mathbb{Z}$ como el exponente que tiene $\mathfrak{p}$ en la factorización de $\mathfrak{a}$.

[8] Si $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ y $\mathfrak{a} \not\subseteq \mathfrak{p}$, tomamos $a \in \mathfrak{a}$ tal que $a \notin \mathfrak{p}$, de forma que para todo $b \in \mathfrak{b}$ se tiene que $ab \in \mathfrak{p}$ y, por tanto, $b \in \mathfrak{p}$. El resultado para m ideales se sigue por inducción.

Por último, la estructura de dominio de Dedekind impone ciertas propiedades sobre la estructura de ideales del anillo:

Proposición A.30. *Sea A un dominio de Dedekind.*

(i) *Si A tiene un número finito de ideales primos, es un DIP.*

(ii) *Si $\mathfrak{a} \neq 0$ es un ideal de A, $A/\mathfrak{a}$ es un DIP.*

(iii) *Todo ideal $\mathfrak{a}$ de A se puede generar con hasta dos elementos.*

Demostración. (i) se sigue inmediatamente del Lema de aproximación y la factorización de ideales (cf. [16, I. pág. 12]); usando el teorema de correspondencia para anillos tenemos que (ii) se sigue de (i), dado que hay a lo sumo un número finito de ideales enteros que contienen a un ideal entero dado (por factorización única). Por último, si $\mathfrak{a} = 0$ es trivial; si no, tomamos $a_1 \in \mathfrak{a}$ no nulo y tenemos por (ii) que $A/(a_1)$ es un DIP, así que existe un $a_2 \in \mathfrak{a}$ tal que $\mathfrak{a} \leftrightarrow (a_2 + (a_1))$ bajo el teorema de correspondencia, de forma que $(a_1, a_2) \leftrightarrow 0$ y $\mathfrak{a} = (a_1, a_2)$. □

A.2. Teoría algebraica de números

A.2.1. Herramientas y objetos básicos

En esta sección daremos las definiciones de algunas herramientas útiles para el estudio de los enteros algebraicos, concluyendo con el objeto fundamental de la Teoría algebraica de números: el *anillo de enteros*. Seguiremos principalmente el desarrollo de [15, I.§2].

Norma, traza y discriminante

En primer lugar, recordamos algunas definiciones de Teoría de Galois:

Definición A.31. Sea L/K una extensión de cuerpos. Tenemos un endomorfismo K-lineal $T_x : L \to L$ definido por $T_x(\alpha) = x\alpha$ y definimos con éste la *norma* de L/K $\mathrm{N}_{L/K}(x) = \det(T_x)$ y la *traza* de L/K $\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(T_x)$. Obtenemos así homomorfismos $\mathrm{Tr}_{L/K} : L \to K$ y $\mathrm{N}_{L/K} : L^\times \to K^\times$.

La traza y la norma, al menos en el caso de extensiones finitas y separables, tienen una expresión útil en términos de los K-embeddings de L en una clausura algebraica:

Proposición A.32. *Si L/K es una extensión finita y separable y $\sigma : L \to \bar{K}$ reccore los K-morfismos de L en una clasura algebraica de K,*

(i) $\mathrm{Tr}_{L/K}(x) = \sum_\sigma \sigma(x)$

(ii) $\mathrm{N}_{L/K}(x) = \prod_\sigma \sigma(x)$

Demostración. Ver [15, I. Proposición 2.6]. □

Aquí podemos ver la potencial utilidad de la traza y la norma para estudiar los enteros algebraicos en una extensión, pues de esto se deduce que si A es un dominio normal con cuerpo de fracciones K, L/K una extensión separable finita y B la clausura entera de A en L, $\mathrm{Tr}_{L/K}(x)$, $\mathrm{N}_{L/K}(x) \in A$ para todo $x \in B$ (ya que ambos son elementos de K al estar fijados por todos los K-morfismos y son enteros sobre A, pues x satisface una ecuación con coeficientes en A y podemos aplicar σ a esta para cada K-morfismo).

Por otra parte, la norma y la traza respetan las extensiones de cuerpos (separables y finitas):

Corolario A.33. *Si L/K y M/L son extensiones finitas separables*[9]*, entonces tenemos las relaciones* $\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}$ *y* $\mathrm{N}_{L/K} \circ N_{M/L} = N_{M/K}$.

Demostración. Tenemos que $\sigma \sim \tau \iff \sigma\big|_L = \tau\big|_L$ define una relación de equivalencia en $\mathrm{Hom}_K(M, \bar{K})$ que da una partición en $m = [L : K]$ clases de equivalencia, digamos con representantes $\sigma_1, ..., \sigma_m$. Entonces $\mathrm{Hom}_K(L, \bar{K})$ consiste exactamente de estos elementos y

$$\begin{aligned}\mathrm{Tr}_{M/K}(x) &= \sum_{i=1}^{m} \sum_{\sigma \sim \sigma_i} \sigma x = \sum_{i=1}^{m} \mathrm{Tr}_{\sigma_i(M)/\sigma_i(L)}(\sigma_i x) = \sum_{i=1}^{m} \sigma_i(\mathrm{Tr}_{M/L}(x)) \\ &= \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(x)).\end{aligned}$$

Y exactamente igual para la norma. □

Pasamos ahora al discriminante:

Definición A.34. El *discriminante* de una base $\alpha_1, ..., \alpha_n$ de una extensión finita separable L/K se define por $\mathrm{disc}(\alpha_1, ..., \alpha_n) = \det((\sigma_i \alpha_j)_{i,j})^2$, donde $\sigma_1, ..., \sigma_n$ son los K-morfismos de L en una clausura algebraica de K.

Usando esta definición y que $(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)) = (\sigma_k \alpha_i)^t (\sigma_k \sigma_j)$, obtenemos la relación

Proposición A.35. $\mathrm{disc}(\alpha_1, ..., \alpha_n) = \det(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j))$

Por otra parte, usando el teorema del elemento primitivo y cambiando de la base $\{\alpha_1, ..., \alpha_n\}$ a la generada por el elemento primitivo y usando el determinante de Vandermonde obtenemos el siguiente resultado:

Proposición A.36. *Sea L/K una extensión separable y $\alpha_1, ..., \alpha_n$ una K-base de L, entonces* $\mathrm{disc}(\alpha_1, ..., \alpha_n) \neq 0$ *y* $\mathrm{Tr}_{L/K}(xy)$ *define una forma bilineal no degenerada en L.*

Demostración. Ver [15, I. Proposición 2.8]. □

Base entera y anillo de enteros

Definición A.37. Sea A un dominio enteramete cerrado con cuerpo de fracciones K y B la clausura entera de A en una extensión L/K. Una *base entera* de B sobre A (también A-base) es un conjunto de elementos $\omega_1, ..., \omega_n \in B$ tal que todo elemento $b \in B$ se expresa de forma única como combinación A-lineal de los ω_j.

[9] Esto también es cierto en el caso inseparable (cf. [15, I. Corolario 2.7]), pero no será necesario.

Encontrar estas bases en en general difícil y puede incluso que para ciertos anillos no las haya; pero en los casos que nos conciernen siempre habrá:

Lema A.38. *Sea $\alpha_1, ..., \alpha_n$ una K-base de L contenida en B y $d = \operatorname{disc}(\alpha_1, ..., \alpha_n)$. Entonces $dB \subseteq A\alpha_1 + ... + A\alpha_n$.*

Demostración. Dado $\alpha \in B$, podemos tomar $a_1, ..., a_n \in K$ tales que $\alpha = a_1\alpha_1 + ... + a_n\alpha_n$, de forma que los a_j son solución al sistema de ecuaciones

$$\operatorname{Tr}_{L/K}(\alpha_i\alpha) = \sum_{j=1}^{n} \operatorname{Tr}_{L/K}(\alpha_i\alpha_j)a,$$

que tiene coeficientes en A (pues $\operatorname{Tr}_{L/K}(x) \in A$ para todo $x \in B$) y determinante $\det(\operatorname{Tr}_{L/K}(\alpha_i\alpha_j)) = d$ (por la Proposición A.35), de forma que $da_j \in A$ para todo j y, por tanto, $d\alpha \in A\alpha_1 + ... + A\alpha_n$. □

Proposición A.39. *Con la notación de la definición anterior, si A es un dominio de ideales principales, todo B-submódulo finitamente generado de L es un A-módulo libre de rango $[L : K]$. En particular, B admite una base entera sobre A.*

Demostración. Sea $M \neq 0$ un B-submódulo finitamente generado de L y tomemos $\alpha_1, ..., \alpha_n \in L$ una K-base de L contenida en B (existe siempre una, pues tomamos cualquier K-base y usamos la Proposición A.18). Por el lema anterior $dB \subseteq A\alpha_1 + ... + A\alpha_n$, donde $d = \operatorname{disc}(\alpha_1, ..., \alpha_n)$, de forma que B tiene rango a lo sumo n y, como todo sistema de generadores de B como A-módulo será una K-base de L, necesariamente B tiene rango n. Por otra parte, si $x_1, ..., x_r \in M$ son generadores de M como B-módulo, $x_1, ..., x_r \in L$, por lo que usando la Proposición A.18, podemos tomar un $a \in A$, $a \neq 0$ tal que $ax_j \in B$ para todo j, de forma que

$$adM \subseteq dB \subseteq A\alpha_1 + ... + A\alpha_n,$$

y, por el teorema de estructura de módulos finitamente generados sobre DIPs podemos concluir que M es un A-módulo libre, con rango acotado por arriba por n y por debajo por el rango de B, que también es n. □

Llegamos ahora a la defincón de uno de los principales objeto de estudio de la Teoría algebraica de números es el anillo de enteros:

Definición A.40. Sea K un cuerpo de números; definimos su *anillo de enteros* $\mathcal{O}_K$ como la clausura entera de $\mathbb{Z}$ en K.

Observamos que, por la proposición anteorior, todo $\mathcal{O}_K$-submódulo $\mathfrak{a}$ de K admite una base entera, por lo que podemos en particular, el anillo de enteros y todos sus ideales fraccionarios admiten una base entera. Podemos además definir el discriminante de un ideal fraccionario $\mathfrak{a}$ como $\operatorname{disc}(\mathfrak{a}) = \operatorname{disc}(\alpha_1, ..., \alpha_n)$ como el de alguna de sus bases (no depende de la elección de base porque el cambio de $\mathbb{Z}$-bases viene dado por una matriz de $\mathrm{GL}_n(\mathbb{Z})$, que tiene determinante ± 1 y en la definición del discriminante aparecerá al cuadrado). Análogamente, definimos así el discriminante de K por $d_K = \operatorname{disc}(\mathfrak{a})$. Además, tenemos la siguiente relación entre discriminantes y el índice:

Proposición A.41. *Sea K un cuerpo de números. Si $\mathfrak{a} \subseteq \mathfrak{a}'$ son dos ideales fraccionarios, su índice $|\mathfrak{a}' : \mathfrak{a}|$ es finito y $\operatorname{disc}(\mathfrak{a}) = |\mathfrak{a}' : \mathfrak{a}|^2 \operatorname{disc}(\mathfrak{a}')$.*

Demostración. Ver [15, I. Proposición 2.12]. □

Lema A.42. *Sea K un cuerpo de números de grado n y sea $\alpha_1, ..., \alpha_n$ una $\mathbb{Q}$-base de K. Si $d = \operatorname{disc}(\alpha_1, ..., \alpha_n)$ es libre de cuadrados, entonces $\alpha_1, ..., \alpha_n$ es una base entera de $\mathcal{O}_K$.*

Demostración. Sea $\beta_1, ..., \beta_n$ una base entera de $\mathcal{O}_K$ y tomemos $a_{ij} \in \mathbb{Z}$ tales que

$$\alpha_j = \sum_{i=1}^{n} a_{ij}\beta_i, \quad A = (a_{ij}).$$

Esto nos da que, por definición del discriminante, $d = \det(A)^2 \operatorname{disc}(\beta_1, ..., \beta_n)$ y, como d es libre de cuadrados, necesariamente $\det(A) = \pm 1$, por lo que $\alpha_1, ..., \alpha_n$ generan $\mathcal{O}_K$ y son, por tanto, una base entera. □

Por último, concluimos esta sección viendo que el anillo de enteros es un dominio de Dedekind y, por tanto, podemos aplicarle todos los resultados de A.1.3:

Teorema A.43. *Sea K un cuerpo de números; su anillo de enteros $\mathcal{O}_K$ es un dominio de Dedekind.*

Demostración. $\mathcal{O}_K$ es normal por definición y noetheriano por ser todo ideal suyo un $\mathbb{Z}$-módulo finitamente generado en virtud de la Proposición A.39. Ahora, si $\mathfrak{p}$ es un ideal primo no nulo de $\mathcal{O}_K$, $\mathfrak{p} \cap \mathbb{Z}$ es un ideal primo no nulo de $\mathbb{Z}$ (pues si $y \in \mathfrak{p}$ es no nulo, y satisface una ecuación mónica con coeficientes enteros cuyo término independiente es no nulo y, por tanto, está en $\mathfrak{p} \cap \mathbb{Z}$), por lo que es un ideal maximal de $\mathbb{Z}$ y por la Proposición A.22, $\mathfrak{p}$ es maximal. □

Para anillos de enteros usamos la notación $J_K = J(\mathcal{O}_K)$, $P_K = P(\mathcal{O}_K)$, $Cl_K = Cl(\mathcal{O}_K)$ y $h_K = h(\mathcal{O}_K)$.

A.2.2. Algunas funciones aritméticas

Sea K un cuerpo de números y $\mathcal{O}_K$ su anillo de enteros.

Definición A.44. Definimos la *norma absoluta* (o *norma de ideales*) para cada ideal no nulo $\mathfrak{a}$ de $\mathcal{O}_K$ por $\mathfrak{N}(\mathfrak{a}) = |\mathcal{O}_K : \mathfrak{a}|$ (por la Proposición A.41 esta cantidad es siempre finita).

Proposición A.45. *Sea $\alpha \in \mathcal{O}_K \setminus \{0\}$; entonces $\mathfrak{N}((\alpha)) = |\operatorname{N}_{K/\mathbb{Q}}(\alpha)|$.*

Demostración. Sea $\omega_1, ..., \omega_n$ una base entera de $\mathcal{O}_K$; entonces $\alpha\omega_1, ..., \alpha\omega_n$ es una base entera de (α) y, si denotamos por $A = (a_{ij})$ la matriz tal que

$$\alpha\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j, \text{ para todo } 1 \leq i \leq n,$$

entonces $\operatorname{N}_{K/\mathbb{Q}}(\alpha) = \det(A)$ por definición de norma (cf. A.31) y, por otra parte, $|\det(A)| = |\mathcal{O}_K : (\alpha)|$, de donde se sigue el resultado. □

Teorema A.46. *Si* $\mathfrak{a} = \mathfrak{p}_1^{\nu_1}...\mathfrak{p}_r^{\nu_r}$ *es la factorización de* $\mathfrak{a} \neq 0$ *en ideales primos, entonces*

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1}... \mathfrak{N}(\mathfrak{p}_r)^{\nu_r};$$

en particular, $\mathfrak{N}$ *define una función completamente multiplicativa en los ideales enteros de* $\mathcal{O}_K$ *y, por tanto, define un homomorfismo de grupos* $\mathfrak{N} : J_K \longrightarrow \mathbb{Q}_{>0}$.

Demostración. Por el Teorema chino del resto (Teorema A.2),

$$\mathcal{O}_K/\mathfrak{a} \cong \mathcal{O}_K/\mathfrak{p}_1^{\nu_1} \oplus ... \oplus \mathcal{O}_K/\mathfrak{p}_r^{\nu_r},$$

por lo que

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1^{\nu_1})... \mathfrak{N}(\mathfrak{p}_r)^{\nu_r},$$

luego basta probar que si $\mathfrak{p}$ es un ideal primo no nulo de $\mathcal{O}_K$ y ν un entero positivo, entonces $\mathfrak{N}(\mathfrak{p}^\nu) = \mathfrak{N}(\mathfrak{p})^\nu$. Ahora, por factorización única de ideales (Teorema A.29), $\mathfrak{p}^j \neq \mathfrak{p}^{j+1}$ para todo j, por lo que $\mathfrak{p}^j/\mathfrak{p}^{j+1}$ es un $(\mathcal{O}_K/\mathfrak{p})$-espacio vectorial no trivial. Tomando $a \in \mathfrak{p}^j \backslash \mathfrak{p}^{j+1}$ y definiendo $\mathfrak{b} = (a) + \mathfrak{p}^{j+1}$, tenemos que $\mathfrak{p}^{j+1} \subset \mathfrak{b} \subseteq \mathfrak{p}^j$ y, así, $\mathfrak{b} = \mathfrak{p}^j$ (pues en caso contrario $\mathfrak{p} \subset \mathfrak{b}\mathfrak{p}^{-j} \subset \mathcal{O}_K$, que es imposible por maximalidad de $\mathfrak{p}$); luego a (mód $\mathfrak{p}^{j+1}$) genera $\mathfrak{p}^j/\mathfrak{p}^{j+1}$ como $(\mathcal{O}_K/\mathfrak{p})$-espacio vectorial y, por tanto, tiene dimensión 1 y $\mathfrak{p}^j/\mathfrak{p}^{j+1} \cong \mathcal{O}_K/\mathfrak{p}$. Con esto,

$$\mathfrak{N}(\mathfrak{p}^\nu) = |\mathcal{O}_K : \mathfrak{p}^\nu| = |\mathcal{O}_K : \mathfrak{p}||\mathfrak{p} : \mathfrak{p}^2|...|\mathfrak{p}^{\nu-1} : \mathfrak{p}^\nu| = \mathfrak{N}(\mathfrak{p})^\nu,$$

de donde se sigue el resultado. □

De forma similar a cómo hemos definido la norma absoluta, definiremos una generalización de la función φ de Euler a ideales. Si pensamos en esta función como la cantidad de números coprimos a un número dado (por debajo del mismo), no es obvio como llevar a cabo esta generalización; pero surge de forma natural si consideramos la definición alternativa

$$\varphi(a) = \#(\mathbb{Z}/a\mathbb{Z})^\times.$$

Definición A.47. Definimos la función de Euler generalizada

$$\Phi_K : \{\text{ideales enteros no nulos de } \mathcal{O}_K\} \longrightarrow \mathbb{N}$$

por $\Phi_K(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})^\times$.

Esta función, al igual que la φ usual, es multiplicativa (en coprimos) y se puede dar explícitamente en términos de la factorización del argumento:

Proposición A.48. *Sean* $\mathfrak{a}$ *y* $\mathfrak{b}$ *ideales coprimos no nulos de* $\mathcal{O}_K$. *Entonces se tiene que* $\Phi_K(\mathfrak{a}\mathfrak{b}) = \Phi_K(\mathfrak{a})\Phi_K(\mathfrak{b})$.

Demostración. Como $\mathfrak{a}$ y $\mathfrak{b}$ son coprimos, el Teorema chino del resto (Teorema A.2) nos da el isomorfismo de anillos

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

por lo que tenemos que sus unidades son

$$(\mathcal{O}_K/\mathfrak{a}\mathfrak{b})^\times \cong (\mathcal{O}_K/\mathfrak{a})^\times \times (\mathcal{O}_K/\mathfrak{b})^\times,$$

de donde se sigue inmediatamente el resultado. □

Teorema A.49. *Sea $\mathfrak{a}$ un ideal entero no nulo de $\mathcal{O}_K$. Se tiene la fórmula*

$$\Phi_K(\mathfrak{a}) = \mathfrak{N}(\mathfrak{a}) \prod_{\mathfrak{p}|\mathfrak{a}} \left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\right),$$

donde $\mathfrak{p}$ recorre los ideales primos no nulos de $\mathcal{O}_K$ que dividen a $\mathfrak{a}$.

Demostración. Usando la factorización única de ideales (Teorema A.29) y la proposición anterior, tenemos que

$$\Phi_K(\mathfrak{a}) = \prod_{\mathfrak{p}|\mathfrak{a}} \Phi_K(\mathfrak{p}^{\nu_\mathfrak{p}}).$$

Así, si probamos que $\Phi_K(\mathfrak{p}^\nu) = \mathfrak{N}(\mathfrak{p})^{\nu-1}(\mathfrak{N}(\mathfrak{p}) - 1)$, el resultado se sigue por multiplicatividad de la norma absoluta (Teorema A.46). Sea, pues, $\mathfrak{p}$ un ideal primo no nulo de $\mathcal{O}_K$ y $\nu \in \mathbb{N}$. Si $\nu = 1$, $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo (pues $\mathfrak{p}$ maximal) y es inmediato que $\Phi_K(\mathfrak{p}) = \mathfrak{N}(\mathfrak{p})-1$. Supongamos por inducción que el resultado es cierto para $\nu-1$ ($\nu > 1$). Probamos en primer lugar que la reducción natural

$$(\mathcal{O}_K/\mathfrak{p}^\nu)^\times \longrightarrow (\mathcal{O}_K/\mathfrak{p}^{\nu-1})^\times$$

es suprayectiva: Si $\alpha \pmod{\mathfrak{p}^{\nu-1}} \in (\mathcal{O}_K/\mathfrak{p}^{\nu-1})^\times$, entonces existe un $\beta \in \mathcal{O}_K$ tal que $\alpha\beta - 1 \in \mathfrak{p}^{\nu-1}$, de forma que $\alpha\beta = 1 + \gamma$ para cierto $\gamma \in \mathfrak{p}^{\nu-1}$ y

$$\alpha\beta(1 - \gamma) = 1 - \gamma^2 \equiv 1 \pmod{\mathfrak{p}^\nu},$$

luego $\alpha \in (\mathcal{O}_K/\mathfrak{p}^\nu)^\times$ como buscábamos. Fijemos ahora un $\gamma \in \mathfrak{p}^{\nu-1} \setminus \mathfrak{p}^\nu$. Dado $\alpha \in \mathcal{O}_K$, $(1 + \alpha\gamma)(1 - \alpha\gamma) = 1 - \alpha^2\gamma^2 \equiv 1 \pmod{\mathfrak{p}^\nu}$, por lo que $1 + \alpha\gamma \pmod{\mathfrak{p}^\nu} \in (\mathcal{O}_K/\mathfrak{p}^\nu)^\times$. Además, si $1 + \alpha\gamma \equiv 1 \pmod{\mathfrak{p}^\nu}$, entonces $\alpha \equiv 0 \pmod{\mathfrak{p}}$, de modo que obtenemos un homomorfismo de grupos inyectivo bien definido

$$\mathcal{O}_K/\mathfrak{p} \longrightarrow (\mathcal{O}_K/\mathfrak{p}^\nu)^\times.$$

Por otra parte, $1 + \alpha\gamma \equiv 1 \pmod{\mathfrak{p}^{\nu-1}}$ para cualquier $\alpha \in \mathcal{O}_K$ y, si $\beta \equiv 1 \pmod{\mathfrak{p}^{\nu-1}}$, entonces $\beta = 1 + \delta$ para cierto $\delta \in \mathfrak{p}^{\nu-1}$, luego $\alpha = \delta\gamma^{-1} \in \mathfrak{p}^{\nu-1}(\mathfrak{p}^{\nu-1})^{-1} = \mathcal{O}_K$ y $\beta = 1 + \alpha\gamma$. Por lo que la imagen del homomorfismos definido anteriormente coincide con el kernel de la reducción y tenemos por tanto la sucesión exacta corta de grupos abelianos

$$1 \longrightarrow \mathcal{O}_K/\mathfrak{p} \longrightarrow (\mathcal{O}_K/\mathfrak{p}^\nu)^\times \longrightarrow (\mathcal{O}_K/\mathfrak{p}^{\nu-1})^\times \longrightarrow 1.$$

Con esto podemos aplicar la hipótesis inductiva y ver que

$$\Phi_K(\mathfrak{p}^\nu) = \#(\mathcal{O}_K/\mathfrak{p}^\nu)^\times = \#(\mathcal{O}_K/\mathfrak{p}^{\nu-1})^\times \cdot \#(\mathcal{O}_K/\mathfrak{p}) = \Phi_K(\mathfrak{p}^{\nu-1})\,\mathfrak{N}(\mathfrak{p}) = \mathfrak{N}(\mathfrak{p})^\nu(\mathfrak{N}(\mathfrak{p}) - 1),$$

como queríamos probar. □

Corolario A.50. *Sea $a \in \mathbb{Z}$ un elemento no nulo. Entonces*

$$\Phi_K(a\mathcal{O}_K) = |a|^n \prod_{\mathfrak{p}|a\mathcal{O}_K} \left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\right) = a^n \prod_{p|a} \prod_{\mathfrak{p}|p\mathcal{O}_K} \left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\right),$$

donde n es el grado del cuerpo de números K.

Demostración. Basta usar en el teorema anterior que, por la Proposición A.45, se tiene que $\mathfrak{N}(a\mathcal{O}_K) = |\,\mathrm{N}_{K/\mathbb{Q}}(a)| = |a|^n$. □

A.2.3. Finitud del número de clases

Para demostrar la finitud del número de clase, necesitamos un lema previo que se sigue del Teorema de Minkowski sobre retículos ([15, I. Teorema 4.4]) aplicado a cuerpos de números (cf. [15, I. Teorema 5.3]), que no demostraremos por brevedad:

Lema A.51. *Sea $\mathfrak{a} \neq 0$ un ideal entero de $\mathcal{O}_K$. Existe un elemento no nulo $a \in \mathfrak{a}$ tal que*

$$|\,\mathrm{N}_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\,\mathfrak{N}(\mathfrak{a}),$$

donde s es el número de pares de $\mathbb{Q}$-morfismos $\sigma : K \longrightarrow \mathbb{C}$ con imagen no contenida en $\mathbb{R}$ (aunque realmente esto no será necesario, lo importante es la existencia de elementos acotados en norma).

Con esto, podemos probar dicho resultado:

Teorema A.52 (Finitud del número de clases)**.** *Sea K un cuerpo de números; su grupo de clases de ideales Cl_K es un grupo finito.*

Demostración. Si $\mathfrak{p}$ es un ideal primo no nulo de $\mathcal{O}_K$, existe un primo $p \in \mathbb{Z}$ tal que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, de forma que $\mathcal{O}_K/\mathfrak{p}$ es una extensión finita del cuerpo de p elementos $\mathbb{F}_p$, digamos de grado f, luego $\mathfrak{N}(\mathfrak{p}) = p^f$. Por otra parte, dado un primo p, hay un número finito de ideales primos $\mathfrak{p}$ de $\mathcal{O}_K$ tales que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, por lo que si fijamos una cota $R > 0$, hay a lo sumo un número finito de ideales primos de $\mathcal{O}_K$ con norma acotada por M. Así, por factorización única de ideales (Teorema A.29), hay a lo sumo un número finito de ideales enteros $\mathfrak{a}$ con $\mathfrak{N}(\mathfrak{a}) \leq M$. Luego si para cierto M conseguimos probar que cada clase de ideales de Cl_K contiene un ideal entero de norma menor que M tendríamos el resultado. Tomemos

$$M = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}.$$

Sea $\mathfrak{a}$ un representante arbitrario de una clase de Cl_K y tomemos $\gamma \in \mathcal{O}_K$ no nulo tal que $\mathfrak{b} = \gamma\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. Por el lema anterior, existe un $\alpha \in \mathfrak{b}$ no nulo tal que $|\,\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leq M\,\mathfrak{N}(\mathfrak{b})$; en particular, por la Proposición A.45 y la multiplicatividad de la norma (Teorema A.46),

$$\mathfrak{N}(\alpha\mathfrak{b}^{-1}) = \mathfrak{N}((\alpha))\,\mathfrak{N}(\mathfrak{b})^{-1} = \mathrm{N}_{K/\mathbb{Q}}(\alpha)\,\mathfrak{N}(\mathfrak{b})^{-1} \leq M,$$

de forma que $\mathfrak{a}_0 = \alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a}$ está en la misma clase que $\mathfrak{a}$ y tiene norma acotada por M, demostrando así el teorema. □

Por último, observamos que el número de clases nos da información artimética relevante sobre $\mathcal{O}_K$:

Proposición A.53. *Sea K un cuerpo de números; $h_K = 1 \iff K$ es un DFU.*

Y, así, podemos entender el grupo de clases como la obstrucción a la factorización única.

A.2.4. Unidades del anillo de enteros

Concluimos este Apéndice, enunciando sin demostración (pues ello requeriría desarrollar la Teoría de Minkowski para cuerpos de números) otro teorema fundamental de la Teoría Algebraica de Números: el *Teorema de unidades de Dirichlet*.

Sea K un cuerpo de números y sean $\sigma_1, ...\sigma_n : K \to \mathbb{C}$ los $\mathbb{Q}$-morfismos de K en $\mathbb{C}$. De estos habrá un número $r \geq 0$ de morfismos cuya imagen esté contenida en $\mathbb{R}$. Si $\sigma : K \to \mathbb{C}$ es un $\mathbb{Q}$-morfismo cuya imagen en $\mathbb{C}$ no está contenida en $\mathbb{C}$, la composición con la conjugación $\bar{\sigma}$ es otro $\mathbb{Q}$-morfismo distinto, por lo que hay un número par de estos morfismos, digamos $2s$ (de forma que $r+2s = n$). Definimos además las raíces de la unidad de K por $\mu(K) = \{x \in K^\times \mid x^n = 1, n \geq 1\}$ (es decir los elementos de torsión del grupo abeliano $K^\times$).

Teorema A.54 (Teorema de unidades de Dirichlet)**.** *Con la notación anterior, $\mathcal{O}_K^\times$ es el producto directo del grupo cíclico finito $\mu(K)$ y un grupo abeliano libre de rango $r+s-1$, i.e., $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$.*

Demostración. Ver [15, I. Teorema 7.4]. □

A.2.5. Cuerpos cuadráticos

Pasaremos ahora a probar algunos resultados elementales sobre cuerpos cuadráticos.

Proposición A.55. *Sea $K = \mathbb{Q}(\sqrt{D})$ un cuerpo cuadrático ($D \in \mathbb{Z}$ libre de cuadrados); K tiene discriminante*

$$d_K = \begin{cases} D, & D \equiv 1 \pmod 4 \\ 4D, & D \equiv 2, 3 \pmod 4 \end{cases}$$

y anillo de enteros

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

Demostración. En primer lugar, es evidente que los únicos $\mathbb{Q}$-morfimos posibles de K en $\mathbb{C}$ son los definidos por $\sqrt{D} \mapsto \pm\sqrt{D}$. Ahora, si $x = \alpha + \beta\sqrt{D} \in K$ es entero algebraico, por la Proposición A.18, $x = \frac{a+b\sqrt{D}}{c}$ con $a, b, c \in \mathbb{Z}$ y a y c, b y c coprimos. Luego por la Proposición A.32, $\mathrm{Tr}_{K/\mathbb{Q}}(x) = (\alpha + \beta\sqrt{D}) + (\alpha - \beta\sqrt{D}) = 2a/c \in \mathbb{Z}$ (por lo que $c = 1$ o $c = 2$) y $\mathrm{N}_{K/\mathbb{Q}}(x) = (\alpha + \beta\sqrt{D})(\alpha - \beta\sqrt{D}) = \alpha^2 - D\beta^2 \in \mathbb{Z}$. Así, si $c = 1$, $\alpha, \beta \in \mathbb{Z}$ y $x \in \mathbb{Z}[\sqrt{D}] \subset \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. Si $c = 2$, $\frac{a^2-db^2}{4} \in \mathbb{Z}$, luego $a^2 - Db^2 \equiv 0 \pmod 4$; por lo que si $D \equiv 2, 3 \pmod 4$, D no es un residuo cuadrático y, por tanto, la única solución es $a^2 \equiv b^2 \equiv 0 \pmod 4$, contradiciendo que a y c (y b y c) son coprimos. Si $D \equiv 1 \pmod 4$, $\frac{1+\sqrt{D}}{2} \in \mathcal{O}_K$ y $d(1, \frac{1+\sqrt{D}}{2}) = D$ es libre de cuadrados, por lo que tenemos, usando el Lema A.42,

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

Con discriminantes $d_K = D$ en el primer caso y $d_K = 4D$ en el segundo. □

Conocidos ya todos los anillos de enteros de cuerpos cuadráticos, pasemos a estudiar sus unidades; el teorema de unidades de Dirichlet (Teorema A.54) nos da que en el caso

imaginario cuadrático $\mathcal{O}_K^\times \cong \mu(K)$, por lo que bastaría encontrar las raíces de la unidad contenidas en K; en el caso real cuadrático, $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z} = \{\pm 1\} \times \langle u \rangle$. No obstante, podemos tratar el caso imaginario de forma elemental:

Proposición A.56. *Sea $K = \mathbb{Q}(\sqrt{D})$ un cuerpo imaginario cuadrático ($D < 0$ libre de cuadrados).*

$$\mathcal{O}_K^\times = \begin{cases} \{\pm 1, \pm i\}, & D = -1 \\ \{\pm 1, \pm\omega, \pm\omega^2\}, & D = -3 \\ \{\pm 1\}, & \text{en el resto,} \end{cases}$$

donde ω es una raíz cúbica primitiva de la unidad.

Demostración. Sea $\alpha = a + b\sqrt{D} \in \mathcal{O}_K^\times$ con $a, b \in \frac{1}{2}\mathbb{Z}$[10]. Usando la norma de $K/\mathbb{Q}$ tenemos que $1 = \mathrm{N}_{K/\mathbb{Q}}(\alpha) = a^2 - Db^2$, de donde descartamos inmediantamente las posibilidades $|a| > 1$ y, para $D \neq -1$, $|b| \geq 1$; así, si $D < -3$, $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \geq a^2 + 5b^2 \geq 5b^2$, por lo que $|b| \leq \frac{1}{\sqrt{5}} < \frac{1}{2}$, luego $b = 0$, $a = 1$ y, por tanto, $\mathcal{O}_K^\times = \{\pm 1\}$. Si $D = -2$, $1 \geq 2b^2$, por lo que $|b| = 0, \frac{1}{2}$, teniéndose que este último caso implica que $|a| = \frac{1}{\sqrt{2}}$, que es imposible, por lo que $\mathcal{O}_K^\times = \{\pm 1\}$.
Ahora, si $D = -1$, $|a| = \frac{1}{2}$ o $|b| = \frac{1}{2}$ nos da que $a \notin \frac{1}{2}\mathbb{Z}$ o $b \notin \frac{1}{2}\mathbb{Z}$, por lo que las únicas posibilidades son $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$, es decir $\mathcal{O}_K^\times = \{\pm 1, \pm i\}$. Por último, si $D = -3$, $b = 0$ o $|b| = \frac{1}{2}$: en el primer caso obtenemos $a = \pm 1$ y en el segundo $a = \pm\frac{1}{2}$, por lo que $\mathcal{O}_K^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$. □

Cabe mencionar que para el caso real se pueden obtener las unidades encontrando soluciones a la *ecuación de Pell* $x^2 - Dy^2 = \pm 1$; sin embargo, esto no lo utilizaremos.

Por último introduciremos el símbolo de Kronecker (que definiremos sólo sobre primos por simplicidad) para estudiar el comportamiento de los primos (de $\mathbb{Z}$) en extensiones cuadráticas:
Para cada primo p y $m \in \mathbb{Z}$ denotamos por $\left(\frac{m}{p}\right)$ el símbolo de Kronecker, que se define como el símbolo de Legendre[11] si $p \neq 2$ y, si $p = 2$,

$$\left(\frac{m}{2}\right) = \begin{cases} 0 & m \equiv 0, 4 \pmod 8 \\ 1 & m \equiv \pm 1 \pmod 8 \\ -1 & m \equiv \pm 3 \pmod 8 \end{cases}$$

Proposición A.57. *Sea $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ el automorfismo no trivial de la extensión cuadrática $K/\mathbb{Q}$ y sea $p \in \mathbb{Z}$ un número primo.*

(i) *Si $\left(\frac{d_K}{p}\right) = 0$, p ramifica, es decir, $p\mathcal{O}_K = \mathfrak{p}^2$ para cierto ideal primo no nulo de $\mathcal{O}_K$.*

(ii) *Si $\left(\frac{d_K}{p}\right) = 1$, p se descompone, i.e., $p\mathcal{O}_K = \mathfrak{p}\sigma(\mathfrak{p})$ con $\mathfrak{p}$ y $\sigma(\mathfrak{p})$ ideales primos no nulos de $\mathcal{O}_K$.*

(iii) *Si $\left(\frac{d_K}{p}\right) = -1$, p es inerte, esto es, $p\mathcal{O}_K$ es primo en $\mathcal{O}_K$.*

Demostración. Ver [6, II. Proposición 5.16]. □

[10] Permitimos semienteros para no tener que distinguir entre los casos $D \equiv 1 \pmod 4$ y $D \equiv 2, 3 \pmod 4$ (cf. Proposición A.55).
[11] Recordemos que éste vale 1 si m es un residuo cuadrático módulo p, -1 si es un no residuo módulo p y 0 si $p \mid m$.

APÉNDICE B

Implementación de los algoritmos y tablas

B.1. Código

Presentamos aquí los algoritmos descritos al final del Capítulo 2. Comenzamos con el algoritmo que, dados $m \geq 1$ y $d < 0$, encuentra todos los enteros $f > 1$ que satisfacen $(*)$.

```
def eq_h(m, d):
    F=set()

    if m==1:
        if kronecker(d,2)==1: F.add((d,2))

    elif m==3:
        P=set()
        if kronecker(d,2)!=0: P.add(2)
        if d%3==0: P.add(3)
        for x in powerset(P):
            if x!=[]:
                producto=prod([1-(kronecker(d,p))/p for p in x])
                f=m/producto
                if f in ZZ:
                    if set(x)==set([p[0] for p in f.factor()]):
                        F.add((d,f))

    elif m%2==1:
        P=set([p[0] for p in gcd(m,d).factor()])
        if d%8==1: P.add(2)
        if d%8==5 and m%3==0: P.add(2)
        for x in powerset(P):
            if x!=[]:
                producto=prod([1-(kronecker(d,p))/p for p in x])
                f=m/producto
                if f in ZZ:
                    if set(x)==set([p[0] for p in f.factor()]):
                        F.add((d,f))
    else:
        P=set()
        for div in m.divisors():
            if kronecker(d,div+1)==1:
                if (div+1).is_prime(): P.add(div+1)
            if kronecker(d,div)==0:
                if div.is_prime(): P.add(div)
            if kronecker(d,div-1)==-1:
                if (div-1).is_prime(): P.add(div-1)
        for x in powerset(P):
```

```
            if x!=[]:
                producto=prod([1-(kronecker(d,p))/p for p in x])
                f=m/producto
                if f in ZZ:
                    if set(x)==set([p[0] for p in f.factor()]):
                        F.add((d,f))
    return set(F)
```

Con esto, se pueden calcular (condicionalmente) todos los órdenes no maximales con número de clases como describimos al final del Capítulo 2:

```
def orders_with_class_number(h, dic):
    orders=set()
    for hK in h.divisors():
        for dK in dic[hK]:
            if dK==-3: orders=orders.union(eq_h(3*h, dK))
            elif dK==-4: orders=orders.union(eq_h(2*h, dK))
            else: orders=orders.union(eq_h(ZZ(h/hK), dK))
    return orders
```

Usando este código hemos obtenido todos los órdenes (maximales y no maximales) con número de clase $h \leq 100$ a partir de la clasificación de Watkins [23] en cuestión de segundos:

```
In [72]: orders=dict()
         import time
         a=time.time()
         for h in xsrange(1,101):
             orders[h]=orders_with_class_number(h, Watkins)
         print(time.time()-a)

         15.195063352584839
```

A partir de aquí podemos calcular los polinomios $H(x)$ descritos al final del mismo capítulo usando `Magma`, pues podemos usar las funciones de `PicardGroup` y `jInvariant` para realizar el trabajo restante:

```
jminpoly:=function(D,f, precision)
local B, C, R, K, O, G, T, p, tau;
C:=ComplexField(precision);
R<x>:=PolynomialRing(C);
K:=QuadraticField(D);
O:=sub<MaximalOrder(K) | f>;
G, map:=PicardGroup(O);
p:=1;
for g in G do
B:=[Conjugate(b,1 : Precision:=precision) : b in Basis(map(g))];
p:=p*(x-jInvariant(B));
end for;
p:=Polynomial([Re(c) : c in Coefficients(p)]);
return <D,f,Round(p)>;
end function;
```

B.2. Tablas

d_K	f	$H(x)$
-3	4	$x^2 - 2835810000x + 6549518250000$
	5	$x^2 + 654403829760x + 5209253090426880$
	7	$x^2 + 34848505552896000x + 11356800389480448000000$
-4	3	$x^2 - 153542016x - 1790957481984$
	4	$x^2 - 82226316240x - 7367066619912$
	5	$x^2 - 44031499226496x - 292143758886942437376$
-7	4	$x^2 - 274917323970000x + 1337635747140890625$
-8	2	$x^2 - 52250000x + 12167000000$
	3	$x^2 - 377674768000x + 232381513792000000$
-11	3	$x^2 + 37616060956672x - 56171326053810176$
-15	1	$x^2 + 191025x - 121287375$
	2	$x^2 - 37018076625x + 153173312762625$
-20	1	$x^2 - 1264000x - 681472000$
-24	1	$x^2 - 4834944x + 14670139392$
-35	1	$x^2 + 117964800 - 134217728000$
-40	1	$x^2 - 425692800x + 9103145472000$
-51	1	$x^2 + 5541101568x + 6262062317568$
-52	1	$x^2 - 6896880000x - 567663552000000$
-88	1	$x^2 - 6294842640000x + 15798135578688000000$
-91	1	$x^2 + 10359073013760x - 3845689020776448$
-115	1	$x^2 + 427864611225600x + 1{,}30231327260672000$
-123	1	$x^2 + 1354146840576000x + 148809594175488000000$
-148	1	$x^2 - 39660183801072000x - 7898242515936467904000000$
-187	1	$x^2 + 4545336381788160000x - 3845689020776448000000$
-232	1	$x^2 - 6047299578498913440000x$ $+ 1487107071315713714551200000000$
-235	1	$x^2 + 8231774194494259200000x + 1194662117046272340787200$
-267	1	$x^2 + 19683091854079488000000x$ $+ 53142966267262137689702400000$
-403	1	$x^2 + 24528113892293313919795200000x$ $- 10884420340249105583308800000$
-427	1	$x^2 + 15611455512523783919812608000x$ $+ 15504175622261891654693683200000$

Tabla B.1: $h(\mathcal{O}) = 2$

d_K	f	$H(x)$
-3	6	$x^3 - 151013228706000x^2 + 224179462188000000x$ $- 1879994705688000000000$
	9	$x^3 + 185576290573466419200 0x^2 - 375065736503309107200 0000x$ $+ 333858672467351961600 0000000$
-11	2	$x^3 - 1122662608x^2 + 270413882112x - 653249011576832$
-19	2	$x^3 - 784074438864x^2 + 1128678666363648x - 827237892283232256$
-23	1	$x^3 + 3491750x^2 - 5151296875x + 12771880859375$
	2	$x^3 - 12207823849750x^2 - 263033266852296875x$ $- 6267542200571287109375$
-31	1	$x^3 + 39491307x^2 - 58682638134x + 1566028350940383$
	2	$x^3 - 1559739536377947x^2 - 874125972104525910x$ $- 599530686551745232383$
-43	2	$x^3 - 782759106183330000x^2 + 1164707517403692000000x$ $- 692660810326239000000000000$
-59	1	$x^3 + 30197678080x^2 - 140811576541184x$ $+ 374643194001883136$
-67	2	$x^3 - 216672372920248567380 00x^2 + 322408427628582369720 00000x$ $- 318937643273692956938421600 0000000$
-83	1	$x^3 + 2691907584000x^2 - 41490055168000000x + 549755813888000000000$
-107	1	$x^3 + 129783279616000x^2 - 6764523159552000000x$ $+ 337618789203968000000000$
-139	1	$x^3 + 12183160834031616x^2 - 5304178675513766707 2x$ $+ 67408489017571610198016$
-163	2	$x^3 - 689258930361092798910856392869460 00x^2$ $+ 102561728837719322645921325412908000000x$ $- 180956256216655229536939508726752008926922480000000000$
-211	1	$x^3 + 658735872886300999 68x^2 + 277390576406111100862464x$ $+ 531082302140889869811764428 8$
-283	1	$x^3 + 896113233868328017920 00x^2 + 908392365354469294080 00000x$ $+ 201371843156955365376000000000$
-307	1	$x^3 + 805016812009981390848000x^2 - 508364642573414616268800 0000x$ $+ 898761963106062670233600 0000000$
-331	1	$x^3 + 664740473017379338646323 2x^2 + 368729929041040103875232661504x$ $+ 561762428403893982302184885945630 72$
-379	1	$x^3 + 364395404104624239018246144x^2$ $- 121567791009880876719538528321536x$ $+ 154436000476890119480246018074151485 44$
-499	1	$x^3 + 300510110807102620070672596992 0x^2$ $- 606371782549426639472239256001105 1008x$ $+ 467113318239995478279867315443744131094937 6$
-547	1	$x^3 + 812973955396316547216374784000 00x^2$ $- 139712328431787827943469744128000000x$ $+ 833039375706784039686352404480000 00000$
-643	1	$x^3 + 395455751627261340994924670115840 00x^2$ $- 630037850504724787649965179745075200 0000x$ $+ 308052554652302847380880841299197952000000000$
-883	1	$x^3 + 349039343410118190392242950119333928960 00x^2$ $- 151960111125245282033875619529124478976000000x$ $+ 167990285381627318187575520800123387904000000000$
-907	1	$x^3 + 123072080721198402394477590506838687744 000x^2$ $+ 391815942080148196175658115753763143680000 0x$ $+ 149161274746524841328545894969274007552000000000$

Tabla B.2: $h(\mathcal{O}) = 3$

Bibliografía

[1] Atiyah, M. F., and Macdonald, I. G. *Introduction to commutative algebra*. Addison-Wesley series in mathematics. Addison-Wesley, Reading, Mass. London, 1969.

[2] Baker, A. Linear forms in the logarithms of algebraic numbers. *Mathematika 13*, 2 (1966), 204–216.

[3] Bosma, W., Cannon, J., and Playoust, C. The Magma algebra system. I. The user language. *J. Symbolic Comput. 24*, 3-4 (1997), 235–265. Computational algebra and number theory (London, 1993). http://dx.doi.org/10.1006/jsco.1996.0125.

[4] Cassels, J. W. S., and Frölich, A., Eds. *Algebraic number theory: proceedings of an instructional conference organized by the London Mathematical Society (a Nato Advanced Study Institute) with the support of the International Mathematical Union*. Academic Press, London, 1967.

[5] Conrad, K. The conductor ideal of an order. https://kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf. Visitado el 28/01/2024.

[6] Cox, D. A. *Primes of the form $p = x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, second ed. Pure and applied mathematics. Addison-Wesley, 2013.

[7] Gauss, C. F. *Disquisitiones arithmeticae*, [english ed.] revised by william c. waterhouse, with the help of cornelius greither and a.w. grootendorst. ed. Springer-Verlag, Berlin [etc., 1986.

[8] Hartshorne, R. *Algebraic geometry*, vol. No. 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1977.

[9] Heegner, K. Diophantische Analyse und Modulfunktionen. *Mathematische Zeitschrift 56*, 3 (1952), 227–253.

[10] Hilbert, D. Mathematical problems. *Bull. Amer. Math. Soc. 8*, 10 (1902), 437–479.

[11] Klaise, J. *Orders in quadratic imaginary fields of small class number*. Trabajo de fin de grado, University of Warwick, 2012.

[12] Kronecker, L., and Hensel, K. *Leopold Kronecker's Werke*, vol. 5. Teubner, Leipzig, 1895 - 1931.

[13] Lang, S. *Algebraic Number Theory*, second ed. Graduate Texts in Mathematics 110. Springer-Verlag, New York, 2000.

[14] Lang, S. *Algebra*, third ed., vol. 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[15] Neukirch, J. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften 322. Springer-Verlag, Berlin Heidelberg, 1999.

[16] Serre, J.-P. *Local Fields*. Graduate texts in mathematics 67. Springer-Verlag, New York, 1979.

[17] Silverman, J. H. *The arithmetic of elliptic curves*. Graduate texts in mathematics 106. Springer-Verlag, New York, 1986.

[18] Silverman, J. H. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate texts in mathematics 151. Springer-Verlag, New York, 1994.

[19] Stark, H. A complete determination of the complex quadratic fields of class-number one. *Michigan Mathematical Journal 14*, 1 (1967), 1–27.

[20] Stark, H. On the "gap" in a theorem of Heegner. *Journal of Number Theory 1*, 1 (1969), 16–27.

[21] Takagi, T. *Über eine Theorie des relativ Abel'schen Zahlkörpers*. Springer Japan, Tokyo, 1990, pp. 73–167.

[22] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.3)*, 2021. https://www.sagemath.org.

[23] Watkins, M. Resolution of class number 100 for imaginary quadratic fields. list of fundamental discriminants. https://magma.maths.usyd.edu.au/~watkins/papers/CLASSNO.out. Visitado el 14/02/2024.

[24] Watkins, M. Class number of imaginary quadratic fields. *Mathematics of Computation 73*, 246 (2003), 907–938.