Primos de la forma $x^2 + ny^2$ y el cuerpo de clases de Hilbert

Javier Alfonso Moreno Carrillo
Código: 1032456375

Universidad Nacional de Colombia
Facultad de Ciencias
Departamento de Matemáticas
Bogotá, D.C.
Octubre 2016

Primos de la forma $x^2 + ny^2$ y el cuerpo de clases de Hilbert

Javier Alfonso Moreno Carrillo
Código: 1032456375

Trabajo de grado para obtener el título de
Magister en Ciencias-Matemáticas

Director
John Jaime Rodríguez V, Ph.D.
Profesor asociado

Línea de investigación
Álgebra y teoría de números

Universidad Nacional de Colombia
Facultad de Ciencias
Departamento de Matemáticas
Bogotá, D.C.
Octubre 2016

Título en español

Primos de la forma $x^2 + ny^2$ y el cuerpo de clases de Hilbert

Title in English

Primes of the form $x^2 + ny^2$ and the Hilbert class field

Resumen: En este trabajo estudiamos condiciones para que dado un primo p, este pueda ser representado por medio de una forma cuadrática binaria de la forma$x^2 + ny^2$ para infinitos n.

Abstract: In this work we study conditions for given a prime p, this can be represented by a binary quadratic form of the form $x^2 + ny^2$ for infinite n.

Palabras clave: Primos, formas cuadráticas, cuerpo de clases de Hilbert, órdenes, extensiones cuadráticas.

Keywords: Primes, quadratic forms, Hilbert class field, orders, quadratic extensions.

Dedicado a

A mis padres y mi gran motivación para seguir: Julieth.

Agradecimientos

Quiero expresar mis agradecimientos a mi director, Profesor John Jaime, por todo su apoyo y su paciencia durante la realización de este trabajo de grado. Mi respeto y admiración por su entrega hacia las matemáticas y todo lo que ello involucra.

Índice general

Índice general **I**

Introducción **II**

1. Preliminares. **1**

1.1. Algo de historia. 1

1.2. Ley de reciprocidad cuadrática. 3

1.3. Cuerpos cuadráticos. 5

1.4. Índice de ramificación y grado de inercia. 8

1.4.1. Teoría de Galois. 10

1.4.2. Descomposición de un número primo en un cuerpo cuadrático. 12

2. Órdenes en cuerpos cuadráticos. **15**

3. El cuerpo de clases de Hilbert. **29**

3.1. Solución de $p = x^2 + ny^2$ para infinitos n. 35

Bibliografía **40**

Introducción

Uno de los teoremas más famosos de la teoría de números es el siguiente: Un primo impar p puede escribirse como $p = a^2 + b^2$ si, y solo si $p \equiv 1 \pmod 4$. Esta afirmación realizada por Fermat y demostrada por Euler es sólo el inicio del problema más general, dar condiciones bajo las cuales un primo impar p puede representarse como $p = x^2 + ny^2$.

Euler demostró la afirmación de Fermat usando una estrategia de dos pasos, un paso de reciprocidad donde demuestra que si $p \equiv 1 \pmod 4$, entonces $p|x^2 + y^2$; y después un paso de descenso donde prueba que si $p|x^2 + y^2$, entonces $p = a^2 + b^2$. Euler logra generalizar estos métodos y así obtiene resultados análogos para los problemas $p = x^2 + 2y^2$ y $p = x^2 + 3y^2$. Debe señalarse aquí que gracias a esto Euler descubre la ley de reciprocidad cuadrática, y más adelante Lagrange y Legendre descubren que es necesario un estudio más detallado de las formas cuadráticas para un discriminante fijo.

Más adelante Gauss, siguiendo los pasos de Euler, Lagrange y Legendre desarrolla una teoría de composición de formas cuadráticas, y enuncia conjeturas importantes sobre el grupo de clases y el número de clases de formas. Aunque el trabajo de Gauss es sobre formas cuadráticas más adelante todos estos resultados se enuncian en el lenguaje de ideales como son conocidos hoy.

Con las herramientas desarrolladas por Gauss se pueden estudiar las ecuaciones $p = x^2 + 27y^2$, donde Gauss usa la ley de reciprocidad cúbica, y $p = x^2 + 64y^2$ donde usa la ley de reciprocidad bicuadrática. Estos métodos sin embargo solo funcionan para un número finito de formas $x^2 + ny^2$.

Es la teoría del cuerpo de clases de Hilbert la que logra unificar todo el trabajo realizado hasta ese momento y enuncia un interesante teorema que resuelve el problema de la representación $p = x^2 + ny^2$ para inifintos n. El objetivo de este trabajo es enunciar y probar ese teorema.

Teorema. *Sea $n > 0$ un entero que satisface la siguiente condición:*

$$n \text{ es libre de cuadrados, } n \not\equiv 3 \bmod 4.$$

Entonces existe un polinomio mónico irreducible $f_n(x) \in \mathbb{Z}[x]$ *de grado* $h(-4n)$ *tal que si un primo impar* p *no divide a* n *ni al discriminante de* $f_n(x)$*, entonces*

$$p = x^2 + ny^2 \Longleftrightarrow \begin{cases} (-n/p) = 1 \text{ y } f_n(x) \equiv 0 \text{ mod } p \\ \text{tiene una solución en los enteros.} \end{cases}$$

Además, $f_n(x)$ *puede ser tomado como el polinomio minimal de un entero algebraico real* α *para el cual* $L = K(\alpha)$ *es el cuerpo de clases de Hilbert de* $K = \mathbb{Q}(\sqrt{-n})$*.*

CAPÍTULO 1

Preliminares.

1.1. Algo de historia.

Fermat es el primero en empezar con el estudio de este problema. Él conjetura que un primo p es representado por una forma cuadrática $p = x^2 + ny^2$, con $x, y \in \mathbb{Z}$, si y solo si, $p \equiv 1 \bmod 4$. De Fermat no se conoce ninguna demostración, pero según los trabajos hechos posteriormente, sí se entiende que él sabía la demostración de dicha conjetura.

Euler, posteriormente, logra hacer una demostración de la afirmación de Fermat y además demuestra otras dos afirmaciones:

$$\begin{aligned} p = x^2 + 2y^2 &\iff p \equiv 1, 3 \bmod 8 \\ p = x^2 + 3y^2 &\iff p = 3 \text{ o } p \equiv 1 \bmod 3. \end{aligned}$$

El método utilizado por Euler en su demostración se basa en dos hechos muy conocidos: el paso del descenso y el paso de la reciprocidad. Gracias a este último, Euler descubre lo que se conoce hoy como la Ley de Reciprocidad Cuadrática.
Al momento de Euler querer hacer la prueba de $p = x^2 + 4y^2$ encuentra que el paso del descenso falla y nota que su demostración no puede ser generalizada.

El estudio de las formas cuadráticas se debe en gran medida a Lagrange y Legendre; son ellos quienes dan las siguientes definiciones, importantes durante esta parte del estudio de la solución a nuestro problema.

- Una forma cuadrática $f(x, y) = ax^2 + bxy + cy^2$ es primitiva si sus coeficientes son primos relativos; definida positiva, si ella solo representa números positivos; y reducida si
$$|b| \leq a \leq c, \text{ y si } |b| = a \text{ o } a = c, \ b \geq 0.$$

- El discriminante de una forma primitiva definida positiva es $D = b^2 - 4ac$.
- Dos formas $f(x, y)$ y $g(x, y)$ se dicen propiamente equivalentes si existen enteros p, q, r y s tales que $f(x, y) = g(px + qy, rx + sy)$ y $ps - qr = 1$.
- Toda forma primitiva definida positiva es propiamente equivalente a una única forma reducida.

Con esto lo que se busca es trabajar con las formas cuadráticas más sencillas, en el sentido de que tengan los coeficientes más pequeños. A continuación presentamos una tabla con las formas reducidas para un discriminante D dado. Aquí, $h(D)$ nota el número de formas cuadráticas primitivas definidas positivas reducidas de discriminante D.

D	$h(D)$	Formas reducidas de discriminante D
-4	1	$x^2 + y^2$
-8	1	$x^2 + 2y^2$
-12	1	$x^2 + 3y^2$
-20	2	$x^2 + 5y^2$, $2x^2 + 2xy + 3y^2$
-28	1	$x^2 + 7y^2$
-56	4	$x^2 + 14y^2$, $2x^2 + 7y^2$, $3x^2 \pm 2xy + 5y^2$
-108	3	$x^2 + 27y^2$, $4x^2 \pm 2xy + 7y^2$
-256	4	$x^2 + 64y^2$, $4x^2 + 4xy + 17y^2$, $5x^2 \pm 2xy + 13y^2$

TABLA 1.1. Tabla formas cuadraticas reducidas.

En el siguiente ejemplo se muestra una forma de determinar cuáles y cuantas formas cuadráticas primitivas reducidas se pueden obtener a partir de un discriminante dado.

Ejemplo 1.1. Suponga que $ax^2 + bxy + cy^2$ es una forma reducida de discriminante $D < 0$. Entonces $b^2 \leq a^2$ y $a \leq c$, luego

$$-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2$$

y así $a \leq \sqrt{(-D)/3}$.
Si se quiere saber cuantas formas cuadráticas con discriminante $D = -4$ note que lo que tenemos es que $a \leq \sqrt{-(-4)/3}$, es decir, $a = 1$.
Como la forma que queremos debe ser reducida, lo que tenemos es que $|b| \leq 1$, luego $b = 0$ o $b = 1$. De aquí que, como $-4 = D = b^2 - 4ac \equiv 0 \bmod 4$ tenemos que $b = 0$. De igual forma, de la definición del discriminante tenemos que $c = 1$. Por lo tanto la única forma reducida de discriminante $D = -4$ es $x^2 + y^2$.

Posterior a esto, surge el problema de saber cuáles formas representan a un número primo p cuando hay más de una forma reducida con discriminante D.

Gauss introduce la teoría de género en la cual dice que dos formas primitivas definidas positivas de discriminante D están el mismo género si ellas representan los mismos valores en $(\mathbb{Z}/D\mathbb{Z})^*$. Para el caso $n = 5$, cuyo discriminante es $D = -20$ hay dos formas reducidas, y gracias a la teoría de género se tiene que:

$$\begin{aligned} p = x^2 + 5y^2 &\iff p \equiv 1, 9 \bmod 20 \\ p = 2x^2 + 2xy + 3y^2 &\iff p \equiv 3, 7 \bmod 20. \end{aligned}$$

Aunque la teoría de género funciona muy bien en estos casos, cuando $n = 14$, esta teoría apenas logra separar las cuatro formas cuadráticas en dos géneros, lo cual no permite resolver nuestra pregunta inicial. El resultado que se tiene es:

$$\begin{aligned} p \equiv 1, 9, 15, 23, 25, 39 \bmod 56 &\iff p = x^2 + 14y^2 \text{ o } 2x^2 + 7y^2 \\ p \equiv 3, 5, 13, 19, 27, 45 \bmod 56 &\iff p = 3x^2 \pm 2xy + 5y^2. \end{aligned}$$

De aquí nace el interés por una nueva teoría que mejore estos resultados.

1.2. Ley de reciprocidad cuadrática.

Si p es un número primo, la discusión de la congruencia $x^2 \equiv a \bmod p$ es sencilla. Sabemos que tiene solución si, y solo si, $a^{(p-1)/2} \equiv 1 \bmod p$. Sin embargo, si la pregunta se cambia un poco el problema se torna mucho más difícil. Suponga que a es un entero. Para cuáles primos p la congruencia $x^2 \equiv a \bmod p$ tiene solución? La respuesta la provee la ley de reciprocidad cuadrática. Esta ley fue formulada por Euler y A. M. Legendre pero Gauss fue el primero en dar un prueba completa.

Definición 1.2. Si $(a, m) = 1$ diremos que a es un residuo cuadrático módulo m si la congruencia $x^2 \equiv a \bmod m$ tiene solución. De otro modo a no es un residuo cuadrático módulo m.

Nota 1.3. Sea $m = 2^e p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$ la descomposición en números primos de m y suponga que $(a, m) = 1$. Entonces $x^2 \equiv a \mod m$ tiene solución si, y solo si, la siguientes condiciones se satisfacen:

(a) Si $e = 2$, entonces $a \equiv 1 \bmod 4$.
Si $e \geq 3$, entonces $a \equiv 1 \bmod 8$.

(b) Para cada i tenemos que $a^{(p_i-1)/2} \equiv 1 \bmod p_i$.

La nota anterior nos traslada el problema a preguntarnos para cuáles primos p un entero a es residuo cuadrático. En lo que sigue en este trabajo p será un número primo impar a menos que se diga lo contrario.

Definición 1.4. El símbolo (a/p) tomará el valor 1 si a es un residuo cuadrático módulo p, -1 si a no es un residuo cuadrático módulo p, y cero si p divide a a. (a/p) es llamado el *símbolo de Legendre*.

El símbolo de Legendre es una herramienta extremadamente conveniente para discutir los residuos cuadráticos. Ahora listaremos algunas de sus propiedades.

Proposición 1.5. *(a)* $a^{(p-1)/2} \equiv (a/p) \ mod\ p.$

(b) $(ab/p) = (a/p)(b/p).$

(c) Si $a \equiv b \ mod\ p$, *entonces* $(a/p) = (b/p).$

Demostración. Si p divide a a o b, todas las afirmaciones son ciertas trivialmente. Supongamos que $p \nmid a$ y que $p \nmid b$.
Sabemos que $a^{p-1} \equiv 1 \bmod p$; así $(a^{(p-1)/2}+1)(a^{(p-1)/2}-1) = a^{p-1}-1 \equiv 0 \bmod p$. De aquí que $a^{(p-1)/2} \equiv \pm 1 \bmod p$. Por la nota anterior, $a^{(p-1)/2} \equiv 1 \bmod p$ si, y solo si, a es un residuo cuadrático módulo p. Esto prueba la parte (a).
Para probar el literal (b) aplicaremos la parte (a). $(ab)^{(p-1)/2} \equiv (ab/p) \bmod p$ y $(ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2} \equiv (a/p)(b/p) \bmod p$. Así $(ab/p) \equiv (a/p)(b/p) \bmod p$, lo cual implica que $(ab/p) = (a/p)(b/p)$.
Como $a \equiv b \bmod p$ existe $n \in \mathbb{Z}$ tal que $a = b + pn$. Note que $x^2 \equiv a \bmod p$ tiene solución si, y solo si, $x^2 \equiv b + pn \equiv b \bmod p$ tiene solución, lo cual prueba (c). □

Teorema 1.6 (Ley de reciprocidad cuadrática.)**.** *Sean p y q primos impares. Entonces* $(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}$.

Ahora daremos un par de lemas relacionados con algunas propiedades de las raíces n-ésimas de la unidad usados en la demostración de la Ley de reciprocidad cuadrática.

Lema 1.7. *Si n es un entero impar positivo y $f(z) = e^{2\pi iz} - e^{-2\pi iz}$, entonces*

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right).$$

Lema 1.8. *Si p es un primo impar, $a \in \mathbb{Z}$, y $p \nmid a$, entonces*

$$\prod_{l=1}^{(p-1)/2} f\left(\frac{la}{p}\right) = \left(\frac{a}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right).$$

Ahora sí procedemos a hacer la demostración de la ley de reciprocidad cuadrática.

Demostración. Sean p y q primos impares. Por el lema 1.8

$$\prod_{l=1}^{(p-1)/2} f\left(\frac{lq}{p}\right) = \left(\frac{q}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right).$$

Y por el lema 1.7

$$\frac{f(ql/p)}{f(l/p)} = \prod_{m=1}^{(q-1)/2} f\left(\frac{l}{p} + \frac{m}{q}\right) f\left(\frac{l}{p} - \frac{m}{q}\right).$$

Colocando estas dos ecuaciones en una sola tenemos que

$$\left(\frac{q}{p}\right) = \prod_{m=1}^{(q-1)/2} \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p} + \frac{m}{q}\right) f\left(\frac{l}{p} - \frac{m}{q}\right).$$

De la misma forma encontramos que

$$\left(\frac{p}{q}\right) = \prod_{m=1}^{(q-1)/2} \prod_{l=1}^{(p-1)/2} f\left(\frac{m}{q} + \frac{l}{p}\right) f\left(\frac{m}{q} - \frac{l}{p}\right).$$

Como $f(m/q - l/p) = -f(l/p - m/q)$ vemos que

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

Y por lo tanto

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

Esto completa la prueba. □

Como resultado complementario a la ley de reciprocidad cuadrática tenemos la siguiente proposición.

Proposición 1.9. *Sea p un primo impar.*

(a) $(-1)^{(p-1)/2} = (-1/p)$.

(b) $(2/p) = (-1)^{(p^2-1)/8}$.

1.3. Cuerpos cuadráticos.

Sea L/F una extensión algebraica finita de cuerpos. La dimensión de L/F, $[L : F]$, será denotada por n. Un subcuerpo F de los números complejos se dice un cuerpo de números algebraicos si $[F : \mathbb{Q}]$ es finito.

Definición 1.10. Suponga que $\alpha_1, \alpha_2, ..., \alpha_n$ es una base para L/F y $\alpha \in L$. Entonces $\alpha\alpha_i = \sum_j a_{ij}\alpha_j$, con $a_{ij} \in F$. Definimos la norma de α, $N_{L/F}$, como $\det(a_{ij})$. La traza de α, $t_{L/F}(\alpha)$, es $a_{11} + a_{22} + \cdots + a_{nn}$.

Nota 1.11. En el caso de una extensión cuadrática, es decir, $\alpha \in K = \mathbb{Q}(\sqrt{N})$, N no cuadrado, tenemos que $t(\alpha) = \alpha + \alpha'$ y $N(\alpha) = \alpha\alpha'$, donde $\alpha = r + s\sqrt{N}$ y $\alpha' = r - s\sqrt{N}$ con $r, s \in \mathbb{Q}$.

Un cuerpo de números algebraicos K se llama un cuerpo cuadrático si $[K : \mathbb{Q}] = 2$. Diremos que $\mathcal{O}_K \subset K$ es el anillo de enteros del cuerpo K si todo elemento $\alpha \in \mathcal{O}_K$

es raíz de un polinomio mónico con coeficientes enteros. Empezaremos mostrando que existe una base para $\mathcal{O}_K$.
Sea $K = \mathbb{Q}(\alpha)$ un cuerpo cuadrático. Entonces el elemento α satisface una ecuación cuadrática $ax^2 + bx + c = 0$, con $a, b, c \in \mathbb{Z}$. Así

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

Sea $N = b^2 - 4ac$. Entonces, $K = \mathbb{Q}(\sqrt{N})$. Sea $N = A_1^2 A_2$ donde $A_1, A_2 \in \mathbb{Z}$ y A_2 es libre de cuadrados. Sea $K = \mathbb{Q}(\sqrt{A_2})$. Cambiando la notación, hemos mostrado que todo cuerpo cuadrático tiene la forma $\mathbb{Q}(\sqrt{d})$ donde d es un entero libre de cuadrados.
Note ahora que si σ es cualquier isomorfismo de K que deja fijo a $\mathbb{Q}$ tendremos que $(\sigma(\sqrt{d}))^2 = d$. Así $\sigma(\sqrt{d}) = \pm\sqrt{d}$. De aquí se sigue que $K/\mathbb{Q}$ es una extensión de Galois cuyo grupo de Galois tiene dos elementos, la identidad y el automorfismo que toma $\sqrt{d}$ y lo envía en $-\sqrt{d}$.
Todo elemento de K tiene la forma $\alpha = r + s\sqrt{d}$ con $r, s \in \mathbb{Q}$. El automorfismo no trivial envía α en $\alpha' = r - s\sqrt{d}$. Así, $t(\alpha) = \alpha + \alpha' = 2r$ y $N(\alpha) = \alpha\alpha' = r^2 - ds^2$. Si $\gamma \in \mathcal{O}_K$ entonces $t(\gamma)$ y $N(\gamma) \in \mathbb{Z}$. Recíprocamente, si estas condiciones se cumplen, entonces γ satisface $0 = (x - \gamma)(x - \gamma') = x^2 - t(\gamma)x + N(\gamma) \in \mathbb{Z}[x]$ probando que $\gamma \in \mathcal{O}_K$. Así, $\gamma \in \mathcal{O}_K$ si, y solo si $t(\gamma)$ y $N(\gamma) \in \mathbb{Z}$.

Proposición 1.12. *Si $d \equiv 2, 3$ mod 4 entonces $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$.*
Si $d \equiv 1$ mod 4 entonces $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\left(\frac{-1 + \sqrt{d}}{2}\right)$.

Demostración. Suponga que $\gamma = r + s\sqrt{d}$, $r, s \in \mathbb{Q}$. Entonces $\gamma \in \mathcal{O}_K$ si y solo si $2r$ y $r^2 - s^2 d \in \mathbb{Z}$. Como $2r \in \mathbb{Z}$ tenemos de la segunda condición que $4s^2 d \in \mathbb{Z}$. Como d es libre de cuadrados tenemos que $2s \in \mathbb{Z}$. Sea $2r = m$ y $2s = n$. Entonces, $r^2 - ds^2 \in \mathbb{Z}$ implica que $m^2 - dn^2 \equiv 0 \bmod 4$.
Recuerde que un cuadrado es congruente a 0 o 1 módulo 4.
Si $d \equiv 2, 3 \bmod 4$ entonces $m^2 - dn^2 \equiv m^2 + 2n^2$ o $m^2 + n^2 \bmod 4$. La única forma para que $m^2 + 2n^2$ o $m^2 + n^2$ sean divisibles entre 4 es que m y n sean ambos pares. Es decir, si y solo si, r y s están en $\mathbb{Z}$. Esto prueba la primera afirmación.
Si $d \equiv 1 \bmod 4$ entonces $m^2 - dn^2$ es congruente a $m^2 - n^2$ módulo 4. Pero $m^2 - n^2 \equiv 0 \bmod 4$ si, y solo si, m y n tienen la misma paridad. Así $\mathcal{O}_K = \{(m + n\sqrt{d})/2 \ : \ m \equiv n \bmod 2\}$. Note que

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

Como $m \equiv n \bmod 2$, $(m + n)/2 \in \mathbb{Z}$. Así $\mathcal{O}_K \subset \mathbb{Z} + \mathbb{Z}(-1 + \sqrt{d})/2$. Para ver la otra contenencia, note que $(-1 + \sqrt{d})/2$ es raíz del polinomio $4x^2 + 4x + (1 - d) = 0$ y como $d \equiv 1 \bmod 4$ tenemos que el anterior polinomio es en realidad $x^2 + x + \frac{1 - d}{4} = 0$ y así $(-1 + \sqrt{d})/2 \in \mathcal{O}_K$. □

Nota 1.13. Para el caso en el que el grado de la extensión sea n, se puede ver que $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo de la forma $\mathcal{O}_K = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n$ para algunos $w_i \in \mathcal{O}_K$.

A continuación daremos un par de definiciones importantes en las cuales el $\mathcal{O}_K$, anillo de enteros de una extensión cuadrática, sirve como ejemplo.

Definición 1.14.
- Un dominio D es un dominio de Dedekind si todo ideal propio de D se descompone de forma única salvo el orden en producto de ideales primos.
- Sea D un dominio entero y K su cuerpo cociente. Un ideal fraccionario de D es un D-submódulo no nulo M de K tal que existe $c \in D \setminus \{0\}$ de manera que $cM \subset D$. Además, si I es un ideal fraccionario no nulo de D, llamaremos $I^{-1} = \{x \in D \ : \ xI \subset D\}$. I^{-1} es un ideal fraccionario de D.

El anillo $\mathcal{O}_K$ no satisface el análogo del teorema fundamental de la aritmética, sin embargo, como propiedad análoga tenemos que $\mathcal{O}_K$ como anillo de enteros de un cuerpo cuadrático es Dedekind, lo que quiere decir que vamos a tener factorización a nivel de ideales como veremos a continuación.
Para probar esto, primero mostraremos un par de proposiciones útiles en el desarrollo de la demostración del teorema.

Proposición 1.15. *Sea I un ideal no nulo de $\mathcal{O}_K$, donde $\mathcal{O}_K$ es el anillo de enteros de un cuerpo de números algebraicos.*

a) $\mathcal{O}_K/I$ es finito.

b) $\mathcal{O}_K$ es noetheriano.

Demostración. a) Sabemos que existe $a \in I \cap \mathbb{Z}$, $a \neq 0$. Sea (a) el ideal principal generado por a en $\mathcal{O}_K$. Como una aplicación de $\mathcal{O}_K/(a)$ en $\mathcal{O}_K/I$ es sobreyectiva, basta probar que $\mathcal{O}_K/(a)$ es finito. De hecho mostraremos que $\mathcal{O}_K/(a)$ tiene exactamente a^n elementos donde n es el grado de la extensión.
Podemos escribir $\mathcal{O}_K = \mathbb{Z}w_1 + \mathbb{Z}w_2 + \ldots \mathbb{Z}w_n$. Sea $S = \{\sum \gamma_i w_i \ : \ 0 \leq \gamma_i < a\}$. Afirmamos que S es un conjunto de clases de representantes para $\mathcal{O}_K/(a)$.
Supongamos que $w = \sum m_i w_i \in \mathcal{O}_K$. Escribimos $m_i = q_i a + \gamma_i$ con $0 \leq \gamma_i < a$. Entonces $w = \sum \gamma_i w_i \mod (a)$. Así, toda clase de I contiene un elemento de S. Si $\sum \gamma_i w_i$ y $\sum \gamma_i' w_i$ están en S y en la misma clase módulo (a) entonces, por la independencia lineal de w_i vemos que $\gamma_i - \gamma_i'$ es divisible por a en $\mathbb{Z}$. Como $0 \leq \gamma_i, \gamma_i' < a$ se sigue que $\gamma_i = \gamma_i'$. Así S es un conjunto de representantes y $\mathcal{O}_K/(a)$ tiene a^n elementos.

b) Consideremos una cadena estrictamente ascendente de ideales de $\mathcal{O}_K$ (finita o infinita) de la forma $I_1 \subset I_2 \subset \cdots \subset \mathcal{O}_K$. Ahora, tomemos el cociente de todos los ideales de esta sucesión sobre I_1 para obtener

$$0 = I_1/I_1 \subset I_2/I_1 \subset \cdots \mathcal{O}_K/I_1.$$

Esta es una cadena estrictamente ascendente de subgrupos de $\mathcal{O}_K/I_1$. Por la parte (a), $\mathcal{O}_K/I_1$ es finito, luego solo tiene finitos grupos.

□

Teorema 1.16. *Sea $K = \mathbb{Q}(\sqrt{d})$ un cuerpo cuadrático y $\mathcal{O}_K$ su anillo de enteros. Para cualquier ideal I de $\mathcal{O}_K$, distinto de 0 y $\mathcal{O}_K$, existen ideales primos $P_1, P_2, \ldots, P_n$ de $\mathcal{O}_K$, no necesariamente distintos, tales que $I = P_1P_2\cdots P_n$. Esta factorización es única salvo por el orden.*

La prueba que haremos a continuación imita muchas de las ideas usadas para probar la factorización única con factores primos en $\mathbb{Z}$.

Demostración. **Existencia:** Sea S el conjunto de todos los ideales $0 \subset I \subset \mathcal{O}_K$ sin una factorización prima. Suponga que S es no vacío. Como D es noetheriano, S debe tener un elemento maximal, digamos $L \in S$. El ideal L no puede ser primo, ya que la factorización de un ideal primo es trivial. Entonces L es no maximal en $\mathcal{O}_K$, luego L está contenido propiamente en un ideal maximal P con $L \subset P \subset \mathcal{O}_K$.
La multiplicación de ideales fraccionarios preserva la inclusión estricta: si $J \subset K$ pero $IJ = IK$, cancelando I tenemos que $J = K$, lo cual es una contradicción. Multiplicando $L \subset P$ por P^{-1} obtenemos $LP^{-1} \subset \mathcal{O}_K$. De igual forma, $P \subset \mathcal{O}_K$ implica que $\mathcal{O}_K \subset P^{-1}$, lo cual a su vez implica que $L \subset LP^{-1}$.
Resumiendo, $LP^{-1} \subset \mathcal{O}_K$ es un ideal entero estrictamente mayor que L y por lo tanto no está en S. Así tenemos una factorización prima $LP^{-1} = P_1\cdots P_k$. Pero entonces $L = P_1\cdots P_kP$ es una factorización prima de L, lo cual contradice que $L \in S$. Así S debe ser vacío.
Para poder continuar con la unicidad, note que cualquier ideal de $\mathcal{O}_K$ es un ideal fraccionario, pues cumple la definición 1.14 trivialmente, y así tiene inverso multiplicativo puesto que el conjunto de los ideales fraccionarios de K forman un grupo bajo la multiplicación de ideales.
Unicidad: Sea $I = P_1\cdots P_k = Q_1\cdots Q_s$. Entonces $P_1 \mid Q_1\cdots Q_s$. Por la versión del lema de Euclides, tenemos que P_1 divide, digamos, a Q_1 ($P_1 \supseteq Q_1$). Pero todo ideal no nulo de $\mathcal{O}_K$ es maximal, luego $P_1 = Q_1$; cancelando obtenemos $P_2\cdots P_k = Q_2\cdots Q_s$. Procediendo inductivamente vemos que una factorización de I es la permutación de la otra. □

1.4. Índice de ramificación y grado de inercia.

Empezamos esta sección recordando que dado $I \subset \mathcal{O}_K$, donde $\mathcal{O}_K$ es el anillo de enteros de un cuerpo de números algebraicos K, tenemos que $I = \prod P^{a(P)}$ donde el producto es sobre los distintos ideales primos de $\mathcal{O}_K$ y los $a(P)$ son enteros no negativos donde casi todos son cero. Los enteros $a(P)$ son únicamente determinados por $a(P) = \mathrm{ord}_P I$.
Además, dado un ideal primo P de $\mathcal{O}_K$, tenemos que $P \cap \mathbb{Z} \neq 0$ ya que si $\alpha \in P$, tenemos que existen ciertos $a_i \in \mathbb{Z}$ tales que $\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_0 = 0$ y como podemos asumir que $a_0 \neq 0$ entonces $a_0 \in P \cap \mathbb{Z}$.

Definición 1.17. Sea P un ideal primo e I un ideal. Entonces el $\text{ord}_P I$ es definido como el único entero no negativo t tal que $P^t \supset I$ y $P^{t+1} \not\supset I$.

Como ya vimos en la proposición 1.15, dado un ideal $I \subset \mathcal{O}_K$ tenemos que $\mathcal{O}_K/I$ es finito, lo cual nos permite hacer la siguiente definición.

Definición 1.18. Sea p un entero primo. Consideremos (p) el ideal principal generado por $p \in \mathbb{Z}$ en $\mathcal{O}_K$.
El número $\text{ord}_P(p) = e$ es llamado el *índice de ramificación* de P. Como $\mathcal{O}_K/P$ es un cuerpo finito que contiene a $\mathbb{Z}/p\mathbb{Z}$ entonces el número de elementos en $\mathcal{O}_K/P$ es de la forma p^f para algún $f \geq 1$. El número f es llamado el *grado* de P.

Decimos que un ideal (p) de K ramifica si cualquiera de sus índices de ramificación e es mayor que 1.

Ahora enunciaremos y probaremos una proposición que nos dice cuál es el grado de P^e para P un ideal primo de $\mathcal{O}_K$ y $e \in \mathbb{Z}^+$.

Proposición 1.19. *Sea $P \subset \mathcal{O}_K$ un ideal primo y sea p^f el número de elementos en $\mathcal{O}_K/P$. El número de elementos en $\mathcal{O}_K/P^e$ es p^{ef}.*

Demostración. La afirmación es verdadera para $e = 1$. Si $e > 1$ entonces $\mathcal{O}_K/P^e$ tiene como subgrupo a P^{e-1}/P^e y su cociente es isomorfo a $\mathcal{O}_K/P^{e-1}$ por el segundo teorema de isomorfismos. Si podemos mostrar que P^{e-1}/P^e tiene p^f elementos entonces el resultado se tendrá por inducción.
Como $P^e \subset P^{e-1}$ propiamente, existe $\alpha \in P^{e-1}$ tal que $\alpha \notin P^e$. Afirmamos que $(\alpha) + P^e = P^{e-1}$: como $P^e \subset (\alpha) + P^e$, el ideal lateral debe ser una potencia de P. Como $(\alpha) + P^e \subset P^{e-1}$ debemos tener que $(\alpha) + P^e = P^{e-1}$.
Consideremos la aplicación $\mathcal{O}_K \longrightarrow P^{e-1}/P^e$ definida como $\gamma \to \gamma\alpha + P^e$. Fácilmente se puede ver que es un epimorfismo. Un elemento γ está en el núcleo si, y solo si, $\gamma\alpha \in P^e$, es decir, si y solo si, $\text{ord}_P(\gamma\alpha) \geq e$.
Ahora, $\text{ord}_P(\gamma\alpha) = \text{ord}_p(\gamma) + \text{ord}_P(\alpha) = \text{ord}_P(\gamma) + e - 1$. Así γ está en el núcleo si, y solo si, $\text{ord}_P(\gamma) \geq 1$ lo cual es equivalente a decir que $\gamma \in P$.
Así, $\mathcal{O}_K/P \cong P^{e-1}/P^e$ y así el grupo lateral tiene p^f elementos. □

Antes de continuar enunciaremos un teorema clásico en el desarrollo de la teoría de anillos.

Teorema 1.20 (Teorema chino de residuos.)**.** *Sea A un anillo y sean $I_1, ..., I_n$, $n \geq 2$, ideales biláteros de A tales que $I_i + I_j = A$, para cualesquiera índices $i \neq j$. Entonces, dada una familia finita de elementos $a_1, ..., a_n \in A$, existe un elemento $a \in A$, tal que $a - a_i \in I_i$ para cada $1 \leq i \leq n$.*

Presentamos ahora un teorema que relaciona el índice de ramificación, el grado de un ideal P con el grado de la extensión $n = [Q : F]$.

Teorema 1.21. *$\sum_{i=1}^{g} e_i f_i = n$, donde e_i es el índice de ramificación de (p) en P_i, f_i es el grado de (p) en P_i y n es el grado de la extensión.*

Demostración. Recuerde que $(p) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$ donde (p) es el ideal principal generado por p en $\mathcal{O}_K$.
Se puede ver que $P_i^{e_i} + P_j^{e_j} = \mathcal{O}_K$ para $i \neq j$.
Por el teorema chino de residuos tenemos que

$$\mathcal{O}_K/(p) \cong \mathcal{O}_K/P_1^{e_1} \oplus \mathcal{O}_K/P_2^{e_2} \oplus ... \oplus \mathcal{O}_K/P_g^{e_g}.$$

Sabemos que $|\mathcal{O}_K/(p)| = p^n$. Por otra parte también vimos que $|\mathcal{O}_K/P_i^{e_i}| = p^{e_i f_i}$. Luego

$$p^n = p^{e_1 f_1} p^{e_2 f_2} \cdots p^{e_g f_g}.$$

Por lo tanto $n = e_1 f_1 + e_2 f_2 + \ldots + e_g f_g$. □

1.4.1. Teoría de Galois.

Recordemos que dado un cuerpo K y un conjunto G de automorfismos de K, tenemos inmediatamente que el conjunto de todos los $x \in K$ tales que $\sigma(x) = x$, para todo $\sigma \in G$, es un subcuerpo de L, llamado el cuerpo fijo de G. Además, para una extensión L de K, $K \subset L$, el conjunto de K-automorfismos de L es un grupo bajo la composición de morfismos.

Teorema 1.22. *Sea L una extensión finita de grado n de un cuerpo K, donde K es finito o de característica cero. Las siguientes condiciones son equivalentes.*

(a) K es el cuerpo fijo del grupo G de K-automorfismos de L.

(b) Para todo $x \in L$, el polinomio minimal de x sobre K tiene todas sus raíces en L.

(c) L es generado por las raíces de un polinomio con coeficientes en K.

Bajo estas condiciones el grupo G de K-automorfismos de L es de orden n.

Demostración. $(a) \Rightarrow (b)$: Observe que, para $x \in L$, el polinomio $\prod_{\sigma \in G}(X - \sigma(x)) = P(X)$ es invariante bajo G. Esto se debe a que $\sigma\left(\prod_{\sigma \in G}(X - \sigma(x))\right) = \prod_{\sigma \in G}(X - \sigma^2(x))$ el cual lo que produce es una permutación de los factores ya que $\sigma^2(x) = \sigma'(x)$ para algún $\sigma' \in G$.
Por tanto los coeficientes de $P(X)$ pertenecen a K ya que por la parte (a), K es el cuerpo fijo de G.
Como x es raíz de $P(X)$, el polinomio minimal de x divide a $P(X)$ y así se tiene el resultado.
$(b) \Rightarrow (c)$: Tome un elemento primitivo x de L sobre K. Su polinomio minimal sobre K tiene todas sus raíces en L por (b).
Claramente, estas raíces generan a L sobre K ya que cualquiera de ellas lo hace.
$(c) \Rightarrow (a)$: Por hipótesis L es generado sobre K por un conjunto finito de elementos $(x^{(1)}, ..., x^{(q)})$ y por todos sus conjugados $x_j^{(i)}$.
Es claro que cualquier K-isomorfismo σ de L en una extensión de L, envía cada uno

de estos generadores en otro del mismo conjunto. Por lo tanto $\sigma(L) \subset L$. Además, por álgebra lineal tenemos que $\sigma(L) = L$, ya que σ es K-lineal e inyectiva.
En otras palabras, σ es un K-automorfismo de L. Se sigue entonces que deben haber exactamente $[L : K[x]]$ $K[x]$-isomorfismos de L en una extensión de L. Así, $n \leq [L : K[x]]$, por lo cual podemos concluir que $n = [L : K[x]]$ y $x \in K$.
Que el orden de G es n ha sido probado durante toda la demostración. □

Definición 1.23. Si las condiciones del teorema 1.22 se satisfacen, L es llamado una extensión de Galois de K y G es llamado el grupo de Galois de L sobre K. Si G es abeliano (respectivamente, cíclico), L es llamado una extensión abeliana (respectivamente, cíclica) de K.

Ahora enunciamos un corolario al teorema anterior el cual nos afirma que el grupo de Galois y la extensión de Galois de un cuerpo son únicos.

Corolario 1.24. *Sea K un cuerpo finito o un cuerpo de característica cero. Sea L una extensión de grado finito n de K, y sea H un grupo de automorfismos de L tal que K es el cuerpo fijo de H. Entonces L es una extensión de Galois de K y H es el grupo de Galois de L sobre K.*

Ejemplo 1.25 (Extensiones cuadráticas.)**.** Sea K un cuerpo cuadrático de característica cero, y sea L una extensión cuadrática de K. Sabemos que L es de la forma $K[x]$ donde x es raíz del polinomio $X^2 - d$ y $d \in K$ con d no cuadrado. Como la otra raíz es $-x$, existe un K-automorfismo no trivial σ definido por $\sigma(x) = -x$, es decir, $\sigma(a + bx) = a - bx$ donde $a, b \in K$.
Claramente $\sigma^2 = 1$ y K es el cuerpo fijo de σ. Así L es una extensión de Galois de K con grupo de Galois cíclico $\{1, \sigma\}$.

Veremos el un caso particular del teorema 1.21 en el caso en el que la extensión sea de Galois. Para empezar enunciamos la siguiente proposición.

Proposición 1.26. *Sea $p \in \mathbb{Z}$ un número primo. Suponga P_i y P_j ideales primos de $\mathcal{O}_K$ (anillo de enteros) que contienen a p. Entonces existe un $\sigma \in G$, donde G es el grupo de Galois de $K/\mathbb{Q}$, tal que $\sigma P_i = P_j$.*

Demostración. Suponga que existe un ideal primo P_0 que contiene a p y que no está en el conjunto de los $\{\sigma P_i | \sigma \in G\}$. Por el teorema chino de residuos, podemos encontrar $\alpha \in \mathcal{O}_K$ tal que $\alpha \equiv 0 \bmod P_0$ y $\alpha \equiv 1 \bmod \sigma P_i$ para todo $\sigma \in G$. Entonces $N(\alpha) = \prod_{\sigma \in G} \sigma\alpha \in P_0 \cap \mathbb{Z} = p\mathbb{Z}$. Se sigue que $N(\alpha) \in P_i$ y entonces $\sigma\alpha \in P_i$ para algún σ ya que P_i es primo. Pero entonces $\alpha \in \sigma^{-1} P_i$, contradiciendo que $\alpha \equiv 1 \bmod \sigma^{-1} P_i$. □

Ahora enunciaremos la versión del teorema 1.21 en el caso de que K sea una extensión de Galois.

Teorema 1.27. *Suponga que $K/\mathbb{Q}$ una extensión de Galois. Sea $p \in \mathbb{Z}$ un número primo y escriba $(p) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$. Entonces $e_1 = e_2 = \cdots = e_g$ y $f_1 = f_2 = \cdots = f_g$. Si e y f denotan los valores comunes, entonces $efg = n$.*

Demostración. Para un índice i existe $\sigma \in G$ tal que $\sigma P_1 = P_i$. Como $\mathcal{O}_K/P_1 \cong \mathcal{O}_K/\sigma P_1 \cong \mathcal{O}_K/P_i$ encontramos que $f_1 = f_i = f$. Así todos los f_i son iguales.
Aplicando σ a ambos lados de $(p) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$ tenemos que $\sigma(p) = (p)$ ya que $p \in \mathbb{Z}$. Así

$$(p) = (\sigma P_1)^{e_1} (\sigma P_2)^{e_2} \cdots (\sigma P_g)^{e_g}.$$

En este producto vemos que el exponente de $P_i = \sigma P_1$ es e_1. En la primera expresión el exponente de P_i es e_i. Por la unicidad de la factorización debemos tener que $e_i = e_1 = e$ y entonces todos los e_i son iguales.
Finalmente, como $\sum_{i=1}^{g} e_i f_i = n$ entonces $efg = n$. □

1.4.2. Descomposición de un número primo en un cuerpo cuadrático.

Sean $d \in \mathbb{Z}$ libre de cuadrados, K el cuerpo cuadrático $\mathbb{Q}[\sqrt{d}]$, $\mathcal{O}_K$ el anillo de enteros de K y p un número primo. Vamos a estudiar la factorización del ideal $p\mathcal{O}_K$ como un producto de ideales primos de $\mathcal{O}_K$.
La fórmula $\sum_{i=1}^{g} e_i f_i = 2$ conlleva a que $g \leq 2$ y se tengan las siguientes tres posibilidades:

(a) $g = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$; en este caso diremos que p se descompone en K.

(b) $g = 1$, $e_1 = 1$ y $f_1 = 2$; en este caso diremos que p sigue siendo primo en K.

(c) $g = 1$, $e_1 = 2$, $f_1 = 1$; en este caso diremos que p ramifica en K.

Consideremos entonces el caso cuando p es primo impar. Por la proposición 1.12 sabemos que $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ o $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ dependiendo de d. Pero si pasamos a las clases residuales de $\mathcal{O}_K$ módulo $p\mathcal{O}_K$, vemos que que en segundo caso $a + b\left[\frac{1+\sqrt{d}}{2}\right]$ es congruente a $a + (b+p)\left[\frac{1+\sqrt{d}}{2}\right]$ y este último pertenece a $\mathbb{Z} + \mathbb{Z}\sqrt{d}$.
Así para cualquier d tenemos que $\mathcal{O}_K/p\mathcal{O}_K \cong (\mathbb{Z} + \mathbb{Z}\sqrt{d})/(p)$.

Considere ahora $\varphi : \mathbb{Z}[X] \to \mathbb{Z} + \mathbb{Z}\sqrt{d}$ un morfismo tal que $\varphi(X) = \sqrt{d}$ y $\varphi(a_i) = a_i$. Note que φ en realidad es un epimorfismo. Sea $P(X) \in \mathbb{Z}[X]$ tal que $P(X) \in \ker(\varphi)$. Luego si $P(X) = a_0 + a_1 X + ... + a_n X^n$ tenemos que $\varphi(P(X)) = 0$ si, y solo si, $a_0 + a_1\sqrt{d} + ... + a_n(\sqrt{d})^n = 0$. Luego $\sqrt{d}$ es raíz de $P(X)$ y como $X^2 - d \in \mathbb{Z}[X]$ es el polinomio minimal de $\sqrt{d}$, concluimos que $X^2 - d$ debe dividir a $P(X)$. Así $\ker(\varphi) \subseteq \langle X^2 - d \rangle$. La otra contenencia es trivial por el hecho de φ ser un homomorfismo. Hemos probado que $\mathbb{Z}[X]/\langle X^2 - d \rangle \cong \mathbb{Z} + \mathbb{Z}\sqrt{d}$.
Por lo tanto tenemos que

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{Z}[X]/\left\langle p, X^2 - d \right\rangle \cong (\mathbb{Z}[X]/(p))/\left\langle X^2 - d \right\rangle \cong \mathbb{K}_p[X]/\left\langle X^2 - d \right\rangle$$

donde d denota la clase residual de d módulo p.
Ahora la afirmación p se descompone (respectivamente, permanece primo, ramifica) en $\mathcal{O}_K$ tiene la interpretación: $\mathcal{O}_K/p\mathcal{O}_K$ es el producto de dos cuerpos (respectivamente, es un cuerpo, contiene elementos nilpotentes). En otras palabras, el polinomio $X^2 - d \in \mathbb{K}_p[X]$ es el producto de dos polinomios lineales (respectivamente, es irreducible, es un cuadrado). Esto pasa si $d \neq 0$ y d es un cuadrado en $\mathbb{K}_p$ (respectivamente, no es un cuadrado en $\mathbb{K}_p$, es cero en $\mathbb{K}_p$).
Cuando $d \neq 0$ y sea un cuadrado en $\mathbb{K}_p$ (respectivamente, no es un cuadrado en $\mathbb{K}_p$) diremos que d es un residuo cuadrático (respectivamente, no es un residuo cuadrático) módulo p.

Resumiendo todo lo anterior tenemos la siguiente proposición.

Proposición 1.28. *Sea $L = \mathbb{Q}[\sqrt{d}]$.*

(a) Si $\left(\frac{d}{p}\right) = 1$ para p primo impar, p se descompone en K.

(b) Si $\left(\frac{d}{p}\right) = -1$ para p primo impar, p sigue siendo primo en K.

(c) Los primos divisores de d ramifican en K.

Existe un resultado análogo para el caso en el que $p = 2$.

Ejemplo 1.29. Sea $K = \mathbb{Q}[\sqrt{-14}]$, luego $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$. Los únicos primos que ramifican son 2 y 7, ya que son los divisores de -14.
Veamos que sucede con los primos 11 y 23. Por reciprocidad cuadrática tenemos que

$$\begin{aligned}\left(\frac{-14}{11}\right) &= \left(\frac{-3}{11}\right) = (-1)^{(11-1)/2}\left(\frac{3}{11}\right) = -\left(\frac{3}{11}\right) = -1.\\ \left(\frac{-14}{23}\right) &= \left(\frac{9}{23}\right) = \left(\frac{3}{11}\right)^2 = 1.\end{aligned}$$

Por lo tanto, 11 sigue siendo primo (sigue inerte), y 23 se descompone.

Terminamos esta sección dando la siguiente proposición la cual nos ayudará a decidir cuando un primo no ramifica o se descompone completamente en una extensión de Galois.

Proposición 1.30. *Sea $K \subset L$ una extensión de Galois, donde $L = K(\alpha)$ para algún $\alpha \in \mathcal{O}_L$. Sea $f(x)$ el polinomio mónico minimal de α sobre K, es decir, $f(x) \in \mathcal{O}_K[x]$. Si $\mathfrak{p}$ es primo en $\mathcal{O}_K$ y $f(x)$ es separable módulo $\mathfrak{p}$, entonces*

(i) $\mathfrak{p}$ no ramifica en L.

(ii) *Si* $f(x) \equiv f_1(x) \cdots f_g(x)$ *mod* $\mathfrak{p}$*, donde los* $f_i(x)$ *son distintos e irreducibles, entonces* $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L$ *es un ideal primo de* $\mathcal{O}_L$*,* $\mathfrak{P}_i \neq \mathfrak{P}_j$ *para* $j \neq i$*, y*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g.$$

Además, los $f_i(x)$ *tienen todos el mismo grado, el cual es igual al grado de inercia* f*.*

(iii) $\mathfrak{p}$ *se descompone completamente en* L *si, y solo si,* $f(x) \equiv 0$ *mod* $\mathfrak{p}$ *tiene una solución en* $\mathcal{O}_K$*.*

CAPÍTULO 2

Órdenes en cuerpos cuadráticos.

Definición 2.1. Un orden $\mathcal{O}$ en un cuerpo cuadrático K es un subconjunto $\mathcal{O} \subset K$ tal que:

(i) $\mathcal{O}$ es un subanillo de K que contiene al 1.

(ii) $\mathcal{O}$ es un $\mathbb{Z}$-módulo finitamente generado.

(iii) $\mathcal{O}$ contiene una $\mathbb{Q}$-base de K.

$\mathcal{O}$ es libre de torsión ya que de lo contrario, el subgrupo de torsión de $\mathcal{O}$ sería un subanillo de $\mathcal{O}$ y el 1 sería un elemento de este subgrupo lo cual implicaría que 1 tendría orden finito, es decir, que $\mathbb{Z} \subset \mathcal{O}$ tendría orden finito, lo cual es absurdo. Como $\mathcal{O}$ contiene una $\mathbb{Q}$-base de K y $[K : \mathbb{Q}] = 2$ entonces existen $\alpha_1, \alpha_2 \in \mathcal{O}$ tales que $\langle \alpha_1, \alpha_2 \rangle_{\mathbb{Q}} = K$. En particular

$$a_1\alpha_1 + a_2\alpha_2 = 0 \text{ con } a_1, a_2 \in \mathbb{Z} \Longleftrightarrow a_1 = 0 = a_2 \text{ ya que } \mathbb{Z} \subset \mathbb{Q}.$$

Entonces $\mathcal{O}$ es libre ya que contiene un subconjunto linealmente independiente. Como $\mathcal{O}$ es finitamente generado como $\mathbb{Z}$-módulo, $\mathcal{O} = \langle \gamma_1, \gamma_2, ..., \gamma_n \rangle_{\mathbb{Z}}$, luego

$$\begin{aligned} \alpha_1 = &\quad a_1\gamma_1 + a_2\gamma_2 + ... + a_n\gamma_n \ ; a_i \in \mathbb{Z}. \\ \alpha_2 = &\quad b_1\gamma_1 + b_2\gamma_2 + ... + b_n\gamma_n \ ; b_i \in \mathbb{Z}. \end{aligned}$$

Luego $\langle \gamma_1, ..., \gamma_n \rangle_{\mathbb{Q}} = K$ pero $[K : \mathbb{Q}] = 2$, luego en realidad se tiene que $\langle \gamma_1, \gamma_2 \rangle_{\mathbb{Q}} = K$ y así $\mathcal{O} = \langle \gamma_1, \gamma_2 \rangle_{\mathbb{Z}}$.
Como $\mathcal{O}$ contiene una $\mathbb{Q}$-base de K, resulta que K es el cuerpo de fracciones de $\mathcal{O}$ ya que

$$K = \frac{\langle \alpha_1, \alpha_2 \rangle_{\mathbb{Q}}}{\langle \alpha_1, \alpha_2 \rangle_{\mathbb{Q}} \setminus \{0\}}$$

$\mathcal{O} = \langle \alpha_1, \alpha_2 \rangle_{\mathbb{Q}}$. El anillo de enteros $\mathcal{O}_K$ en K es un orden en K debido a que

$$\mathcal{O}_K = [1, w_K], \text{ donde } w_K = \frac{d_K + \sqrt{d_K}}{2}$$

y d_K es el discriminante de $K = \mathbb{Q}(\sqrt{d})$ definido como

$$d_K = \begin{cases} d & \text{si } d \equiv 1 \bmod 4 \\ 4d & \text{de otro modo.} \end{cases} \tag{2.1}$$

Proposición 2.2. *Para cualquier orden $\mathcal{O}$ de K tenemos que $\mathcal{O} \subset \mathcal{O}_K$.*

Demostración. Recordemos el teorema de Caley-Hamilton: Sea R un anillo, $I \subset R$ un ideal y M un R-módulo que puede ser generado por n elementos. Sea φ un endomorfismo de M. Si $\varphi(M) \subset I(M)$ entonces existe un polinomio mónico $p(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$ con $a_i \in I^i$ para cada i, tal que $p(\varphi) = 0$ como endomorfismo.

Note que $\mathcal{O}$ es finitamente generado, $\mathbb{Z}$ es un anillo, $\mathcal{O}$ es un $\mathbb{Z}$-módulo y sea $s \in \mathcal{O}$, luego como $\mathcal{O}$ es un subanillo, la multiplicación por s es un endomorfismo tal que $\varphi(\mathcal{O}) \subset \mathcal{O}$.
Luego, por el teorema de Caley-Hamilton, existe un polinomio mónico tal que $p(\varphi) = 0$, en particular cuando $\varphi(1) = s$. Es decir, $s^n + a_{n-1}s^{n-1} + ... + a_0 = 0$ y así $s \in \mathcal{O}_K$. Luego $\mathcal{O} \subset \mathcal{O}_K$. □

Al ser $\mathcal{O}$ y $\mathcal{O}_K$ órdenes, se tendrá el siguiente resultado.

Lema 2.3. *Si $\mathcal{O}$ y $\mathcal{O}_K$ son $\mathbb{Z}$-módulos libres de rango 2, entonces $|\mathcal{O}_K/\mathcal{O}| = [\mathcal{O}_K : \mathcal{O}] < \infty$.*

Demostración. Sean A y B $\mathbb{Z}$-módulos libres de rango 2, $A \subseteq B$, luego $A = f_1\mathbb{Z} \oplus f_2\mathbb{Z}$ y $B = e_1\mathbb{Z} \oplus e_2\mathbb{Z}$. Sea $\overline{x + A} \in B/A$, como $B = \langle e_1, e_2 \rangle_{\mathbb{Z}}$, $x = n_1e_1 + n_2e_2$, $n_1, n_2 \in \mathbb{Z}$, y sea $\overline{y + A} \in B/A$, luego $y = m_1e_1 + m_2e_2$, tal que $\overline{x + A} = \overline{y + A}$. Entonces

$$\begin{aligned} \overline{x + A} = \overline{y + A} &\iff \overline{n_1e_1 + n_2e_2} + A = \overline{m_1e_1 + m_2e_2} + A \\ &\iff (n_1 - m_1)e_1 + (n_2 - m_2)e_2 \in A \\ &\iff (n_1 - m_1)e_1 + (n_2 - m_2)e_2 = l_1f_1 + l_2f_2 \text{ con } l_1, l_2 \in \mathbb{Z} \end{aligned}$$

Pero $f_1, f_2 \in A \subseteq B$, luego

$$\begin{aligned} f_1 &= s_1e_1 + s_2e_2 \\ f_2 &= p_1e_1 + p_2e_2 \end{aligned}$$

Así $(n_1 - m_1)e_1 + (n_2 - m_2)e_2 = l_1(s_1e_1 + s_2e_2) + l_2(p_1e_1 + p_2e_2)$.
Como e_1, e_2 son linealmente independientes,

$$\begin{aligned} n_1 - m_1 &= l_1s_1 + l_2p_1 \\ n_2 - m_2 &= l_1s_2 + l_2p_2 \end{aligned}$$

Por lo tanto tenemos que

$$\begin{aligned} n_1 &\equiv m_1 \bmod (\mathrm{mcd}(s_1, p_1)) \\ n_2 &\equiv m_2 \bmod (\mathrm{mcd}(s_2, p_2)). \end{aligned}$$

Lo cual prueba que $|\mathcal{O}_K/\mathcal{O}| = [\mathcal{O}_K : \mathcal{O}] < \infty$. □

A continuación enunciamos un lema que nos proporciona una base para cada orden.

Lema 2.4. *Sea $\mathcal{O}$ un orden en un cuerpo cuadrático K de discriminante d_K. Entonces $\mathcal{O}$ tiene índice finito en O_K y si $f = [\mathcal{O}_K : \mathcal{O}]$ entonces $\mathcal{O} = \mathbb{Z} \oplus fw_K\mathbb{Z}$ donde $w_K = \dfrac{d_K + \sqrt{d_K}}{2}$.*

Demostración. Como $\mathcal{O}$ y $\mathcal{O}_K$ son $\mathbb{Z}$-módulos libres de rango 2, se sigue del lema 2.3 que $[\mathcal{O}_K : \mathcal{O}] < \infty$. Tomando $f = [\mathcal{O}_K : \mathcal{O}]$ tenemos que $f\mathcal{O}_K \subset \mathcal{O}$ ya que $f\mathcal{O}_K \subset \mathcal{O} = |\mathcal{O}_K/\mathcal{O}|$ significa que $f(a + \mathcal{O}) = fa + \mathcal{O}$ lo cual implica que $fa \in \mathcal{O}$. Entonces $\mathbb{Z} + f\mathcal{O}_K \subset \mathcal{O}$.
Sin embargo, como $\mathcal{O}_K = [1, w_K]$ tenemos que $\mathbb{Z} + f\mathcal{O}_K = [1, fw_K]$.
Resta ver que $[1, fw_K]$ tiene índice f en $\mathcal{O}_K = [1, w_K]$, pero esto es obvio. □

Dado un orden $\mathcal{O}$ en un cuerpo cuadrático K, el índice $f = [\mathcal{O}_K : \mathcal{O}]$ es llamado el conductor del orden.

Otro invariante importante de $\mathcal{O}$ es su discriminante, el cual está definido como sigue.
Sea $\alpha \mapsto \alpha'$ el automorfismo no trivial de K, y suponga que $\mathcal{O} = [\alpha, \beta]$. Entonces el discriminante de $\mathcal{O}$ es el número

$$D = \left(\det \begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix}\right)^2.$$

Proposición 2.5. *(i) El discriminante de un orden en un cuerpo cuadrático es independiente de la base usada y así solo depende de $\mathcal{O}$.*

(ii) Si $\mathcal{O} = [1, fw_K]$ entonces $D = f^2d_K$.

(iii) Cualquier orden está unívocamente determinado por su discriminante.

(iv) Si $D \equiv 0, 1 \bmod 4$ no es un cuadrado, muestre que hay un orden cuadrático cuyo discriminante es D.

Demostración. (i) Sea $\mathcal{O} = [\alpha, \beta] = [1, fw_K]$, luego

$$\begin{aligned} \alpha &= a + b\frac{f}{2}(d_K + \sqrt{d_K}) \\ \alpha' &= a + b\frac{f}{2}(d_K - \sqrt{d_K}) \\ \beta &= c + d\frac{f}{2}(d_K + \sqrt{d_K}) \\ \beta' &= c + d\frac{f}{2}(d_K - \sqrt{d_K}) \end{aligned}$$

Por lo tanto:

$$\begin{aligned} D &= \left(\det\begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix}\right)^2 = (\alpha\beta' - \alpha'\beta)^2 \\ &= \Big[((a + b\frac{f}{2}(d_K + \sqrt{d_K}))(c + d\frac{f}{2}(d_K - \sqrt{d_K})) \\ &\quad -(a + b\frac{f}{2}(d_K - \sqrt{d_K}))(c + d\frac{f}{2}(d_K + \sqrt{d_K}))\Big]^2 \\ &= f^2 d_K (ad - bc)^2 \end{aligned}$$

Note que $(ad - bc)^2$ es el determinante de la matriz de cambio de base, luego $(ad - bc)^2 = 1$, lo cual prueba la afirmación deseada.

(ii) Note que

$$\begin{aligned} D &= \left(\det\begin{pmatrix} 1 & fw_K \\ 1 & fw_K \end{pmatrix}\right)^2 \\ &= (\frac{f}{2}(d_K - \sqrt{d_K}) - \frac{f}{2}(d_K + \sqrt{d_K}))^2 \\ &= (-f\sqrt{d_K})^2 = f^2 d_K \end{aligned}$$

(iii) Sea $\mathcal{O} = [1, fw_K]$ y $\mathcal{O}' = [\alpha, \beta]$ dos órdenes distintos tales que sus discriminantes coincides, es decir, $D(\mathcal{O}) = D(\mathcal{O}') = f^2 d_K$. Luego $[\mathcal{O}_K : \mathcal{O}] = f = [\mathcal{O}_K : \mathcal{O}']$. Como tienen el mismo conductor, por el lema 2.4, $\mathcal{O}' = [1, fw_K] = \mathcal{O}$.

(iv) D debe tener la forma $D = f^2 d_K$, entonces el orden deseado es $\mathcal{O} = [1, fw_K]$.

□

Así el discriminante satisface que $D \equiv 0, 1 \bmod 4$ ya que $d_K \equiv 0, 1 \bmod 4$ y $f^2 \equiv 0, 1 \bmod 4$. Además note también que $K = \mathbb{Q}(\sqrt{D})$, luego K es real o imaginario dependiendo de si $D > 0$ o $D < 0$.

Ejemplo 2.6. Considere $\mathbb{Z}[\sqrt{-n}] \subset K = \mathbb{Q}(\sqrt{-n})$. El discriminante de $\mathbb{Z}[\sqrt{-n}]$ es

$$D = \left(\det \begin{pmatrix} 1 & \sqrt{-n} \\ 1 & -\sqrt{-n} \end{pmatrix}\right)^2 = (-2\sqrt{-n})^2 = -4n.$$

Entonces $-4n = f^2 d_K$ lo cual facilita el cálculo del conductor de $\mathbb{Z}[\sqrt{-n}]$.

Proposición 2.7. *Sea $\mathcal{O}$ un orden en un cuerpo cuadrático K.*

(i) Sea $\mathfrak{a}$ un ideal no nulo de $\mathcal{O}$, entonces $\mathfrak{a}$ contiene un entero no nulo m.

(ii) Si $\mathfrak{a}$ es un ideal no nulo de $\mathcal{O}$, $\mathcal{O}/\mathfrak{a}$ es finito.

(iii) Todo ideal primo de $\mathcal{O}$ es maximal.

(iv) $\mathcal{O}$ es noetheriano.

Demostración. Para la demostración de esta proposición, imitaremos la prueba hecha en la proposición 1.15.

(i) Sea $\alpha \in \mathfrak{a}$. Luego $\overline{\alpha} \in \mathcal{O}$ ya que si $\alpha = a + bfw_K$, note que $\overline{\alpha} = a + bf\overline{w_K} \in \mathbb{Z} + f\mathcal{O}_K$ debido al lema 2.4. Como $\mathfrak{a}$ es un ideal, tenemos que $N(\alpha) = \alpha\overline{\alpha} \in \mathfrak{a}$, con $N(\alpha) \in \mathbb{Z}$. Luego $m = N(\alpha) \in \mathcal{O}$.

(ii) Note que $\mathcal{O}/m\mathcal{O} \to \mathcal{O}/\mathfrak{a}$ es sobreyectiva. Basta probar entonces que $\mathcal{O}/m\mathcal{O}$ es finito.
Podemos escribir $\mathcal{O} = \mathbb{Z} + fw_K\mathbb{Z}$. Sea $S = \{a_i + b_i f w_K |\ 0 \leq a_i, b_i < m\}$.
Afirmamos que S es el conjunto de clases representativas para $\mathcal{O}/m\mathcal{O}$.
Suponga que $w = m_1 + m_2 f w_K \in \mathcal{O}$. Escribamos $m_i = q_i m + \gamma_i$ con $0 \leq \gamma_i < 0$. Entonces claramente $w \equiv \gamma_1 + \gamma_2 f w_K \mod m\mathcal{O}$. Así, toda clase de $m\mathcal{O}$ contiene un elemento de S. Si $\gamma_1 + \gamma_2 f w_K$ y $\gamma_1' + \gamma_2' f w_K$ están en S y en la misma de clase mod $m\mathcal{O}$, usando la independencia lineal de la base vemos que $\gamma_i - \gamma_i'$ es divisible por m en $\mathbb{Z}$. Por lo tanto, $0 \leq \gamma_i, \gamma_i' < m$ y se sigue que $\gamma_i = \gamma_i'$. Lo que hemos probado es que S es el conjunto de clases representativas y $\mathcal{O}/m\mathcal{O}$ tiene m^2 elementos.

(iii) Sea P un ideal primo de $\mathcal{O}$, entonces $\mathcal{O}/P$ es un dominio entero finito. Tales anillos son un cuerpo. Así $\mathcal{O}/P$ es un cuerpo y por lo tanto P es maximal.

(iv) Sea $A_1 \subset A_2 \subset ...$ una cadena ascendente de ideales de $\mathcal{O}$. Como $\mathcal{O}/A_1$ es finito, existen finitos ideales que contiene a A_1.

□

Gracias a la anterior proposición podemos definir la norma de $\mathfrak{a}$ como $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$. Sin embargo, es obvio que si el conductor f de $\mathcal{O}$ es mayor que 1, entonces $\mathcal{O}$ no es integralmente cerrado en K, y así $\mathcal{O}$ no es un dominio de Dedekind cuando $f > 1$. Por lo tanto no podemos asumir que los ideales de $\mathcal{O}$ tengan factorización única.

Ejemplo 2.8. Sea $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$, el cual es un orden de conductor 2 en el cuerpo imaginario $K = \mathbb{Q}(\sqrt{-3})$.
Recuerde que α no unidad en un anillo R, es irreducible si $\alpha = \beta\gamma$ en R implica que β o γ es una unidad.

(a) Como $\mathcal{O}$ tiene conductor $f = 2$ y $d_K = -3$, ya que $d_K \equiv 1 \bmod 4$, el discriminante de $\mathcal{O}$ es $D = 4(-3) = -12$.
Por el teorema 2.13, $C(\mathcal{O}) \cong C(D)$ y se puede ver que solo hay una forma cuadrática primitiva reducida con discriminante $D = -12$, la cual es $f(x, y) = x^2 + 3y^2$. Así, $C(D) \cong \{1\} \cong C(\mathcal{O})$.

(b) Note que si un ideal $\mathfrak{a}$ es propio en $\mathcal{O}$, se tiene que $\mathfrak{a}$ no es ideal de $\mathcal{O}_K$. De igual forma, si un $\mathcal{O}$-ideal $\mathfrak{a}$ no es propio, implica que $\mathfrak{a}$ sigue siendo ideal si lo vemos como ideal de $\mathcal{O}_K$. Por tanto si suponemos que los ideales propios de $\mathcal{O}$ tienen factorización única, restaria ver si los ideales no propios también la tienen. Pero los ideales de $\mathcal{O}$ que no son propios también son ideales de $\mathcal{O}_K$ y este último anillo es un dominio de Dedekind. Por lo tanto todo $\mathcal{O}$ es un dominio de factorización única en este caso.

(c) Sea $\alpha, \beta \in \mathcal{O}$ tal que $2 = \alpha\beta$. Note que $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-3}$, luego $\alpha = a + b\sqrt{-3}$ y $\beta = c + d\sqrt{-3}$ con $a, b, c, d \in \mathbb{Z}$.
Como $N(2) = N(\alpha\beta) = N(\alpha)N(\beta)$ tenemos que $4 = N(\alpha)N(\beta)$ y de aquí los siguientes casos:

- Si $N(\alpha) = 4$ y $N(\beta) = 1$ implica que β es una unidad.
- Si $N(\alpha) = 1$ y $N(\beta) = 4$ implica que α es una unidad.
- Si $N(\alpha) = 2 = N(\beta)$ entonces $N(\alpha) = a^2 + 3b^2 = 2$ y esto significa que $b = 0$ y $a^2 = 2$ lo cual es una contradicción puesto que $a \in \mathbb{Z}$.

Por lo tanto 2 es irreducible en $\mathcal{O}$.
Consideremos ahora $1+\sqrt{-3}$. Note que $N(1+\sqrt{-3}) = 4$ y por el razonamiento anterior se tiene que $1 + \sqrt{-3}$ es también irreducible.

Como $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ se tiene que $\mathcal{O}$ no es un dominio de factorización única.

Para solucionar esto, introducimos el concepto de un ideal primo de un orden. Dado un ideal $\mathfrak{a}$ de $\mathcal{O}$, note que $\mathcal{O} \subset \{\beta \in K | \beta\mathfrak{a} \subset \mathfrak{a}\}$ ya que $\mathfrak{a}$ es un ideal de $\mathcal{O}$. Pero la igualdad no siempre se da.

Ejemplo 2.9. Considere el orden $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$ en $K = \mathbb{Q}[\sqrt{-3}]$. Entonces el $\mathcal{O}$-ideal $\mathfrak{a}$ generado por 2 y $1 + \sqrt{-3}$ cumple que

$$\{\beta \in K | \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}_K \tag{2.2}$$

pero $\mathcal{O} \neq \mathcal{O}_K$.

Note que $-3 \equiv 1 \bmod 4$, luego $d_K = -3$, $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}w_K$, con $w_K = \dfrac{-3+\sqrt{-3}}{2}$, y $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-3}$. Es claro que $\dfrac{-3+\sqrt{-3}}{2} \notin \mathcal{O}$.

Veamos por qué se tiene la igualdad en 2.2.

Sea $\beta \in K$ tal que $\beta\mathfrak{a} \subset \mathfrak{a}$, es decir, $\langle 2\beta, \beta(1+\sqrt{-3})\rangle \subset \langle 2, 1+\sqrt{-3}\rangle$. Luego

$$\begin{aligned} 2\beta &= 2x + (1+\sqrt{-3})y \text{ para algunos } x, y \in \mathbb{Z} \\ \beta &= x + (\frac{1+\sqrt{-3}}{2})y. \end{aligned}$$

Luego $\beta \in \mathcal{O}_K$. Por otra parte note que $1 \in \{\beta \in K | \beta\mathfrak{a} \subset \mathfrak{a}\}$ trivialmente. Como $\mathcal{O}_K = [1, w_K]$, restaría probar que w_K también pertenece a dicho conjunto. Note que

$$\begin{aligned} w_K\mathfrak{a} &= \langle 2wK, (1+\sqrt{-3})w_K\rangle \\ &= \langle -3+\sqrt{-3}, -3-\sqrt{-3}\rangle \end{aligned}$$

pero $-3+\sqrt{-3} = 2(-2) + (1+\sqrt{-3})$ y $-3-\sqrt{-3} = 2(-1) + (-1)(1+\sqrt{-3})$. Así $\mathcal{O}_K \subseteq \{\beta \in K | \beta\mathfrak{a} \subset \mathfrak{a}\}$.

En general decimos que un ideal $\mathfrak{a}$ de $\mathcal{O}$ es propio siempre que la igualdad se tenga, es decir, cuando

$$\mathcal{O} = \{\beta \in K | \beta\mathfrak{a} \subset \mathfrak{a}\}.$$

Proposición 2.10. *Sea K un cuerpo cuadrático.*

(i) Para cualquier orden de K, los ideales principales son propios siempre.

(ii) Para el orden maximal $\mathcal{O}_K$, todos los ideales son propios.

Demostración. (i) Sea $\mathcal{O}$ un orden y $\alpha \in \mathcal{O}$. Veamos que $\mathcal{O} = \{\beta \in K | \beta(\alpha\mathcal{O}) \subset \alpha\mathcal{O}\}$. Sabemos que $\mathcal{O} \subseteq \{\beta \in K | \beta(\alpha\mathcal{O}) \subset \alpha\mathcal{O}\}$ ya que $\alpha\mathcal{O}$ es $\mathcal{O}$-ideal. Sea $\beta \in K$ tal que $\beta(\alpha\mathcal{O}) \subset \alpha\mathcal{O}$. Por definición $1 \in \mathcal{O}$, luego $\beta\alpha \in \alpha\mathcal{O}$ y $\beta \in \mathcal{O}$.

(ii) Sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$. Consideremos el ideal principal generado por β sobre $\mathcal{O}_K$, luego $\langle\beta\rangle\,\mathfrak{a} = \beta\mathcal{O}_K\mathfrak{a}$ pero como $\mathfrak{a}$ es un ideal de $\mathcal{O}_K$, $\beta\mathcal{O}_K\mathfrak{a} \subset \beta\mathfrak{a} \subset \mathfrak{a}$, luego $\mathfrak{a}$ divide a $\langle\beta\rangle\,\mathfrak{a}$. Por lo tanto, existe C ideal de $\mathcal{O}_K$ (ya que $\mathcal{O}_K$ es un dominio de Dedekind) tal que $\langle\beta\rangle\,\mathfrak{a} = \mathfrak{a}C$, y como tenemos cancelación de ideales, $\langle\beta\rangle = C$, lo cual prueba que $\beta \in C \subset \mathcal{O}_K$.

□

También podemos extender esta terminología a ideales fraccionarios.

Un $\mathcal{O}$-ideal fraccionario $\mathfrak{b}$ es propio siempre que

$$\mathcal{O} = \{\beta \in K | \beta\mathfrak{b} \subset \mathfrak{b}\}. \tag{2.3}$$

Otra definición que podemos dar es que un $\mathcal{O}$-ideal fraccionario $\mathfrak{a}$ es invertible si existe otro $\mathcal{O}$-ideal fraccionario $\mathfrak{b}$ tal que $\mathfrak{ab} = \mathcal{O}$.
Note que los ideales fraccionarios principales (aquellos de la forma $\alpha\mathcal{O}$, $\alpha \in K^*$) son invertibles.

La noción de ser propio e invertible coinciden.

Proposición 2.11. *Sea $\mathcal{O}$ un orden en un cuerpo cuadrático K, y sea $\mathfrak{a}$ un $\mathcal{O}$-ideal fraccionario. Entonces $\mathfrak{a}$ es propio si, y solo si, $\mathfrak{a}$ es invertible.*

Demostración. Si $\mathfrak{a}$ es invertible, entonces $\mathfrak{ab} = \mathcal{O}$ para algún $\mathcal{O}$-ideal fraccionario $\mathfrak{b}$. Si $\beta \in K$ y $\beta\mathfrak{a} \subset \mathfrak{a}$ entonces

$$\beta\mathcal{O} = \beta(\mathfrak{ab}) = (\beta\mathfrak{a})\mathfrak{b} \subset \mathfrak{ab} = \mathcal{O}$$

y así $\beta \in \mathcal{O}$ lo cual prueba que $\mathfrak{a}$ es propio.
Para argumentar en el otro sentido necesitamos el siguiente lema.

Lema 2.12. *Sea $K = \mathbb{Q}(\tau)$ un cuerpo cuadrático, y sea $ax^2 + bx + c$ el polinomio minimal de τ, donde a, b y c son primos relativos. Entonces $[1, \tau]$ es un ideal fraccionario propio del orden $[1, a\tau]$ de K.*

Demostración. Primero, $[1, a\tau]$ es un orden ya que $a\tau$ es un entero algebraico. Entonces, dado $\beta \in K$, note que $\beta[1, \tau] \subset [1, \tau]$ es equivalente a:

$$\begin{aligned} \beta \cdot 1 &\in [1, \tau]. \\ \beta\tau &\in [1, \tau]. \end{aligned}$$

La primera línea dice que $\beta = m + n\tau$, $m, n \in \mathbb{Z}$. Para entender la segunda, note que:

$$\beta\tau = m\tau + n\tau^2 = m\tau + \frac{n}{a}(-b\tau + c)$$

ya que $a\tau^2 + b\tau + c = 0$ implica que $\tau^2 = \dfrac{-b\tau - c}{a}$. Luego

$$\beta\tau = \frac{-cn}{a} + \left(\frac{-bn}{a} + m\right)\tau.$$

Como $\mathrm{mcd}(a, b, c) = 1$, vemos que $\beta\tau \in [1, \tau]$ si, y solo si, $a|n$. Se sigue entonces que $\{\beta \in K | \beta[1, \tau] \subset [1, \tau]\} = [1, a\tau]$.

□

Continuando con la demostración de la proposición 2.11, note que $\mathfrak{a}$ es un $\mathbb{Z}$-módulo libre de rango 2, por lo tanto $\mathfrak{a} = [\alpha, \beta]$ para algunos $\alpha, \beta \in K$. Entonces $\mathfrak{a} = \alpha[1, \tau]$ donde $\tau = \beta/\alpha$. Si $ax^2 + bx + c$, con $\mathrm{mcd}(a, b, c) = 1$, es el polinomio minimal de τ, entonces el lema 2.12 implica que $\mathcal{O} = [1, a\tau]$.
Sea $\beta \to \beta'$ el automorfismo no trivial de K. Como τ' es la otra raíz de $ax^2 + bx + c$,

aplicando el lema 2.12 de nuevo, mostramos que $\mathfrak{a}' = \alpha'[1, \tau']$ es un ideal fraccionario para $[1, a\tau] = [1, a\tau'] = \mathcal{O}$.
Afirmamos que $\mathfrak{a}\mathfrak{a}' = \dfrac{N(\alpha}{a}\mathcal{O}$.
Para ver por qué, note que

$$a\mathfrak{a}\mathfrak{a}' = a\alpha\alpha'[1, \tau][1, \tau'] = N(\alpha)[a, a\tau, a\tau', a\tau\tau']$$

Como $\tau + \tau' = \dfrac{-b}{a}$, $\tau\tau' = \dfrac{c}{a}$ y $\text{mcd}(a, b, c) = 1$ entonces

$$a\mathfrak{a}\mathfrak{a}' = N(\alpha)[a, a\tau, -b, c] = N(\alpha)[1, a\tau] = N(\alpha)\mathcal{O}.$$

Lo cual prueba que $\mathfrak{a}$ es invertible. □

Dado un orden $\mathcal{O}$, $I(\mathcal{O})$ denota el conjunto de $\mathcal{O}$-ideales fraccionarios propios. Por la proposición 2.11, $I(\mathcal{O})$ es un grupo bajo la multiplicación. Los $\mathcal{O}$-ideales principales forman un subgrupo $P(\mathcal{O}) \subset I(\mathcal{O})$ y así podemos formar el cociente $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$ el cual es el grupo de clases de ideales del orden $\mathcal{O}$. Cuando $\mathcal{O}$ es el orden maximal $\mathcal{O}_K$, $I(\mathcal{O}_K)$ y $P(\mathcal{O}_K)$ se denotarán I_K y P_K respectivamente.

Teorema 2.13. *Sea $\mathcal{O}$ el orden de discriminante D en un cuerpo cuadrático imaginario K. Entonces:*

(i) Si $f(x, y) = ax^2 + bxy + cy^2$ es una forma cuadrática definida positiva de discriminante D, entonces $\left[a, (-b + \sqrt{D})/2\right]$ es un ideal propio de $\mathcal{O}$.

(ii) La aplicación que envía $f(x, y)$ en $\left[a, (-b + \sqrt{D})/2\right]$ induce un isomorfismo entre el grupo de clases de formas $C(D)$ y el grupo de clases de ideales $C(\mathcal{O})$. Así el orden de $C(\mathcal{O})$ es el número de clases $h(D)$.

(iii) Un entero positivo m es representado por una forma $f(x, y)$ si, y solo si, m es la norma $N(\mathfrak{a})$ para algún ideal $\mathfrak{a}$ en la correspondiente clase de ideales en $C(\mathcal{O})$.

Demostración. Sea $f(x, y) = ax^2 + bxy + cy^2$ una forma primitiva definida positiva con discriminante $D < 0$. Las raíces de $f(x, 1) = ax^2 + bx + c$ son complejas (ya que $D < 0$), entonces existe un único $\tau \in \mathcal{H}$ ($\mathcal{H}$ es la mitad superior del plano) tal que $f(\tau, 1) = 0$. Llamamos τ la raíz de $f(x, y)$. Como $a > 0$, se tiene que $\tau = \dfrac{-b + \sqrt{D}}{2a}$.
Así, $\left[a, \dfrac{-b + \sqrt{D}}{2}\right] = [a, a\tau] = a[1, \tau]$. Note que $\tau \in K = \mathbb{Q}[\sqrt{D}]$.

(i) Por el lema 2.12, $a[1, \tau]$ es un ideal propio del orden $[1, a\tau]$. Resta ver entonces que $[1, a\tau] = \mathcal{O}$.

Si f es el conductor de $\mathcal{O}$, entonces $D = f^2 d_K$ y así

$$\begin{aligned} a\tau &= \frac{-b+\sqrt{D}}{2} = \frac{-b+f\sqrt{d_K}}{2} \\ &= -\left(\frac{+fd_K}{2}\right) + f\left(\frac{d_K+\sqrt{d_K}}{2}\right) = -\left(\frac{b+fd_K}{2}\right) + fw_K \end{aligned}$$

Como $D = b^2 - 4ac = f^2 d_K$, entonces b y fd_K deben tener la misma paridad. Luego $\dfrac{b+fd_K}{2} \in \mathbb{Z}$ y $[1, a\tau] \subseteq [1, fw_K]$.

Note además que $fw_K = a\tau + \dfrac{b+fd_K}{2}$ y $\dfrac{b+fd_K}{2} \in \mathbb{Z}$ implica que $[1, fw_K] \subseteq [1, a\tau]$.

Por lo tanto, $[1, a\tau] = [1, fw_K] = \mathcal{O}$. Esto prueba que $\left[a, \dfrac{-b+\sqrt{D}}{2}\right] = a[1, \tau]$ es un $\mathcal{O}$-ideal propio.

(ii) Sea $f(x,y)$ y $g(x,y)$ formas de discriminante D, y sean τ y τ' sus respectivas raíces. Probaremos las siguientes equivalencias:

$$\begin{aligned} f(x,y), g(x,y) \text{ son propiamente equivalentes} &\iff \tau' = \frac{p\tau+q}{r\tau+s},\ \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}(2\mathbb{Z}) \\ &\iff [1,\tau] = \lambda[1,\tau'],\ \lambda \in K^*. \end{aligned}$$

Asuma que $f(x,y) = g(px+qy, rx+sy)$ donde $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}(2\mathbb{Z})$. Entonces

$$0 = f(\tau,1) = g(p\tau+q, r\tau+s) = (r\tau+s)^2 g\left(\frac{p\tau+q}{r\tau+s}, 1\right)$$

entonces $g\left(\dfrac{p\tau+q}{r\tau+s}, 1\right) = 0$ ya que si $(r\tau+s)^2 = 0$ tendremos que $\tau = -s/r \in \mathbb{Q}$ lo cual es contradictorio.

Por un cálculo sencillo se puede ver que $\mathrm{Im}\left(\dfrac{p\tau+q}{r\tau+s}\right) = \det\begin{pmatrix} p & q \\ r & s \end{pmatrix} |r\tau+s|^2 \mathrm{Im}(\tau)$.

Esto implica que $\left(\dfrac{p\tau+q}{r\tau+s}\right) \in \mathcal{H}$ y así $\tau' = \dfrac{p\tau+q}{r\tau+s}$, por la unicidad de las raíces.

Recíprocamente, si $\tau' = \dfrac{p\tau+q}{r\tau+s}$, entonces

$$0 = f(\tau,1) = g(p\tau+q, r\tau+s) = (r\tau+s)^2 g\left(\frac{p\tau+q}{r\tau+s}, 1\right).$$

Esto muestra que $f(x,y)$ y $g(x,y)$ son iguales ya que tienen la misma raíz. Por lo tanto $f(x,y) = g(px+qy, rx+sy)$ y así tenemos la primera equivalencia.

Para la segunda equivalencia, si $\tau' = \dfrac{p\tau+q}{r\tau+s}$, sea $\lambda = r\tau+s \in K^*$. Entonces

$$\lambda[1,\tau'] = (r\tau+s)\left[1, \frac{p\tau+q}{r\tau+s}\right] = [r\tau+s, p\tau+q] = [1,\tau]$$

ya que $[r\tau+s, p\tau+q] \subseteq [1,\tau]$ y

$$\begin{aligned} \tau &= -rq\tau - sq + ps\tau + qs = (ps-rq)\tau \\ 1 &= rp\tau + ps - rp\tau - rq = ps - rq = 1. \end{aligned}$$

Luego $[1,\tau] \subseteq [r\tau+s, p\tau+q]$.
Recíprocamente, si $[1,\tau] = \lambda[1,\tau']$ para algún $\lambda \in K^*$, entonces $[1,\tau] = [\lambda, \lambda\tau]$ lo cual implica que

$$\lambda\tau = p\tau + q \tag{2.4}$$
$$\lambda = r\tau + s \tag{2.5}$$

para algún $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z})$. Esto nos dices que $\tau' = \dfrac{p\tau+q}{r\tau+s}$ y por el hecho que $\mathrm{Im}\left(\dfrac{p\tau+q}{r\tau+s}\right) = \det\begin{pmatrix} p & q \\ r & s \end{pmatrix} |r\tau+s|^{-2}\mathrm{Im}(\tau)$ muestra que $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ ya que τ y τ' están en $\mathcal{H}$.
Esto completa la prueba de las equivalencias.
Usando las equivalencias anteriores se puede ver que la aplicación que envía $f(x,y)$ en $a[1,\tau]$ está bien definida y además induce una inyección.
Para mostrar que la aplicación es sobreyectiva, sea $\mathfrak{a}$ un $\mathcal{O}$-ideal fraccionario. Podemos escribir $\mathfrak{a} = [\alpha,\beta]$ para algunos $\alpha, \beta \in K$ ya que $\mathfrak{a}$ es de rango 2.
Cambiando α y β, si fuera necesario, podemos asumir que $\tau = \beta/\alpha$ está en $\mathcal{H}$.
Sea ax^2+bx+c el polinomio minimal de τ. Podemos asumir que $\mathrm{mcd}(a,b,c) = 1$ y $a > 0$. Entonces $f(x,y) = ax^2 + bxy + cy^2$ es definida positiva con discriminante $D = b^2 - 4ac$ y es enviada en $a[1,\tau]$ que tiene discriminante

$$\left(a \cdot \det\begin{pmatrix} 1 & \tau \\ 1 & \overline{\tau} \end{pmatrix}\right)^2 = (a(\overline{\tau}-\tau))^2 = D.$$

Este ideal está en la clase de $\mathfrak{a} = [\alpha,\beta] = \alpha[1,\tau]$ en $C(\mathcal{O})$, ya que $\alpha[1,\tau] = \left(\dfrac{a}{\alpha}\right)\alpha[1,\tau]$ y $\dfrac{a}{\tau} \in K^*$.
Esto prueba la sobreyectividad y consecuentemente se tiene la biyectividad entre $C(D)$ y $C(\mathcal{O})$.
La prueba de que es un isormofismo es bastante extensa y la omitimos en este documento.

(iii) Si m es representado por $f(x,y)$, $m = d^2a$, donde a está propiamente representado por $f(x,y)$. Podemos asumir que $f(x,y) = ax^2 + bxy + cy^2$. Entonces $f(x,y)$ es enviado en $\mathfrak{a} = a[1,\tau]$ y $N(\mathfrak{a}) = a$. De aquí que $N(d\mathfrak{a}) = d^2a = m$ y entonces m es la norma de un ideal en la clase de $\mathfrak{a}$.
Recíprocamente, asuma $N(\mathfrak{a}) = m$. Sabemos que $\mathfrak{a} = \alpha[1,\tau]$, donde $\mathrm{Im}(\tau) > 0$, $a\tau^2 + b\tau + c = 0$, $\mathrm{mcd}(a,b,c) = 1$ y $a > 0$. Entonces $f(x,y) = ax^2 + bxy + cy^2$ es enviado en la clase de $\mathfrak{a}$, luego solo tenemos que mostrar que $f(x,y)$ representado a m.
Sabemos que $m = N(\mathfrak{a}) = \dfrac{N(\alpha)}{a}$, sin embargo, $\alpha[1,\tau] = \mathfrak{a} \subset \mathcal{O} = [1, a\tau]$, luego $\alpha = p + qa\tau$ y $\alpha\tau = r + sa\tau$ para algunos enteros p, q, r, s.
Así $(p + qa\tau)\tau = r + sa\tau$ y como $a\tau^2 = -b\tau - c$, luego

$$\begin{aligned} (p + qa\tau)\tau = p\tau + qa\tau^2 &= r + sa\tau \\ p\tau + q(-b\tau - c) &= r + sa\tau \\ p\tau - bq\tau - qc &= r + sa\tau \\ p\tau &= (r + qc) + (sa + bq)\tau. \end{aligned}$$

Comparando coeficientes tenemos que $p = as + bq$. Así

$$\begin{aligned} m = \frac{N(\alpha)}{a} &= \frac{1}{a}(p^2 - bpq + acq^2) \\ &= \frac{1}{a}((as + bq)^2 - b(as + bq)q + acq^2) \\ &= \frac{1}{a}(a^2s^2 + absq + acq^2) \\ &= as^2 + bsq + cq^2 = f(s,q). \end{aligned}$$

Esto finaliza la prueba de *(iii)*.

□

Ahora daremos unas propiedades de la norma de ideales.

Lema 2.14. *Sea $\mathcal{O}$ un orden en un cuerpo cuadrático imaginario. Entonces:*

(i) $N(\alpha\mathcal{O}) = N(\alpha)$ *para* $\alpha \in \mathcal{O}$, $\alpha \neq 0$.

(ii) $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ *para $\mathcal{O}$-ideales propios de* $\mathfrak{a}$ *y* $\mathfrak{b}$.

(iii) $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}$ *para un $\mathcal{O}$-ideal propio* $\mathfrak{a}$.

Los cuerpo cuadráticos se dividen en dos tipos, real ($d_K > 0$) e imaginario ($d_K < 0$), y las unidades $\mathcal{O}_K^*$ son distintas en ambos casos.
En el caso imaginario, solo hay finitas unidades, mientras que en los cuerpo cuadráticos reales, hay infinitas unidades y determinarlas está relacionado con la ecuación de Pell y fracciones continuas.

Definimos ahora lo que sería el análogo al símbolo de Legendre pero en el caso en el que $p = 2$.
Si $D \equiv 0, 1 \bmod 4$ entonces el símbolo de Kronecker $(D/2)$ es

$$(D/2) = \begin{cases} 0 & \text{si } D \equiv 0 \bmod 4 \\ 1 & \text{si } D \equiv 1 \bmod 8 \\ -1 & \text{si } D \equiv 5 \bmod 8. \end{cases}$$

Aplicaremos este símbolo usualmente en el caso que $D = d_K$ sea el discriminante de un cuerpo cuadrático K. La siguiente proposición muestra el comportamiento de los primos de un cuerpo cuadrático.

Proposición 2.15. *Sea K un cuerpo cuadrático de discriminante d_K, y sea el automorfismo no trivial de K denotado $\alpha \mapsto \alpha'$. Sea $p \in \mathbb{Z}$ un primo.*

(i) Si $(d_K/p) = 0$, entonces $p\mathcal{O}_K = \mathfrak{p}^2$ para algún ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$.

(ii) Si $(d_K/p) = 1$, entonces $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ donde $\mathfrak{p} \neq \mathfrak{p}'$ son primos de $\mathcal{O}_K$.

(iii) Si $(d_K/p) = -1$ entonces $p\mathcal{O}_K$ es primo en $\mathcal{O}_K$.

Además, los primos en (i)-(iii) son todos los primos de $\mathcal{O}_K$.

Demostración. (i) Suponga que p es un primo impar que divide a d_K, y sea $\mathfrak{p}$ el ideal $\mathfrak{p} = p\mathcal{O}_K + \sqrt{d_K}\mathcal{O}_K$.
Elevando al cuadrado, $\mathfrak{p}^2 = p^2\mathcal{O}_K + p\sqrt{d_K}\mathcal{O}_K + d_K\mathcal{O}_K$.
Como d_K es libre de cuadrados (excepto por un fator de 4) y p es un divisor impar, $\mathrm{mcd}(p^2, d_K) = p$. Se sigue que $\mathfrak{p}^2 = p\mathcal{O}_K$, y entonces la relación $efg = [K : \mathbb{Q}] = 2$ del teorema 1.27 implica que $\mathfrak{p}$ es un ideal primo. El caso $p = 2$ es similar.
Vamos a probar (ii) y (iii) para un primo impar $p \not| d_K$. La clave será la proposición 1.30. Note que $f(x) = x^2 - d_K$ es el polinomio minimal del elemento primitivo $\sqrt{d_K}$ de K sobre $\mathbb{Q}$, y como $p \not| d_K$, $f(x)$ es separable módulo p. La proposición 1.30 muestra que p es no ramificado en K.
Si $(d_K/p) = 1$, entonces la congruencia $x^2 \equiv d_K \bmod p$ tiene solución, y como consecuencia p se descompone completamente en K por la parte (iii) de la proposición 1.30, es decir, $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ con $\mathfrak{p}_1 \neq \mathfrak{p}_2$ primos de $\mathcal{O}_K$.
Como $\mathrm{Gal}(K/\mathbb{Q})$ actúa transitivamente sobre los primos de K conteniendo a p, debemos tener que $\mathfrak{p}_1' = \mathfrak{p}_2$ y entonces $p\mathcal{O}_K$ se factoriza como se afirma.
Si $(d_K/p) = -1$ entonces $f(x) = x^2 - d_K$ es irreducible módulo p y así la parte (ii) de la proposición 1.30 afirma que $p\mathcal{O}_K$ es primo en K. La prueba de $p = 2$ es similar a la anterior.

□

El colorario que se tiene inmediatamente de la anterior proposición nos dice el comportamiento de los primos de $\mathbb{Z}$ cuando suben a la extensión cuadrática.

Corolario 2.16. *Sea K un cuerpo cuadrático con discriminante d_K, y sea p un primo entero. Entonces:*

(i) p ramifica en K si, y solo si, p divide a d_K.

(ii) p se descompone completamente en K si, y solo si, $(d_K/p) = 1$.

CAPÍTULO 3

El cuerpo de clases de Hilbert.

Nuestro objetivo es probar el siguiente teorema:

Teorema 3.1. *Sea $n > 0$ un entero que satisface la siguiente condición:*

$$n \text{ es libre de cuadrados, } n \not\equiv 3 \bmod 4. \tag{3.1}$$

Entonces existe un polinomio mónico irreducible $f_n(x) \in \mathbb{Z}[x]$ de grado $h(-4n)$ tal que si un primo impar p no divide a n ni al discriminante de $f_n(x)$, entonces

$$p = x^2 + ny^2 \Longleftrightarrow \begin{cases} (-n/p) = 1 \text{ y } f_n(x) \equiv 0 \bmod p \\ \text{tiene una solución en los enteros.} \end{cases}$$

Además, $f_n(x)$ puede ser tomado como el polinomio minimal de un entero algebraico real α para el cual $L = K(\alpha)$ es el cuerpo de clases de Hilbert de $K = \mathbb{Q}(\sqrt{-n})$.

Dado $n > 0$, sea K el cuerpo cuadrático imaginario $\mathbb{Q}(\sqrt{-n})$, entonces (2.1) y la proposición 1.12 implican que

$$d_K = -4n \Longleftrightarrow \mathcal{O}_K = \mathbb{Z}[\sqrt{-n}] \Longleftrightarrow n \text{ satisface (3.1).}$$

Así la condición (3.1) sobre n es equivalente a que $\mathbb{Z}[\sqrt{-n}]$ sea todo el anillo de enteros en K. Para los otros n vimos que $\mathbb{Z}[\sqrt{-n}]$ no es un dominio de Dedekind pero sí un orden.

El cuerpo de clases de Hilbert de un cuerpo de números K es definido en términos de las extensiones abelianas no ramificadas de K. Para ver esto qué significa empezamos viendo qué significa que sea abeliana. Una extensión $K \subset L$ es abeliana si es de Galois y si $\mathrm{Gal}(L/K)$ es un grupo abeliano. Antes de definir qué quiere decir con ser no ramificado, debemos discutir sobre la ramificación de los primos infinitos. Los ideales primos de $\mathcal{O}_K$ son llamados usualmente primos finitos para distinguirlos de los primos infinitos, los cuales son determinados por los embebimientos de K en

$\mathbb{C}$. Un primo real infinito es una aplicación $\sigma : K \to \mathbb{R}$. Un primo complejo infinito es una pareja de apliaciones conjugadas complejas $\sigma, \overline{\sigma} : K \to \mathbb{C}$, $\sigma \neq \overline{\sigma}$.
Dada una extensión $K \subset L$, primo infinito σ de K ramifica en L si este es un primo real infinito pero existe una extensión a L en la cual es un primo complejo infinito.

Ejemplo 3.2. Los primos infinitos de $\mathbb{Q}$ son no ramificado en $\mathbb{Q}(\sqrt{2})$ pero ramifican en $\mathbb{Q}(\sqrt{-2})$

Una extensión $K \subset L$ es no ramificada si esta es no ramificada para todos los primos, finitos o infinitos. Aunque es una restricción bastante fuerte, puede suceder que dado un cuerpo este tenga una extensión no ramificada de grado arbitrariamente alto. Pero si nos preguntamos por una extensión abeliana no ramificada, un mejor resultado se obtiene.

Teorema 3.3. *Dado un cuerpo de números K, existe una extensión de Galois finita L de K tal que:*

(i) L es una extensión abeliana no ramificada.

(ii) Cualquier otra extensión abeliana no ramificada de K está contenida en L.

El cuerpo L del teorema anterior es llamado el cuerpo de clases de Hilbert de K. Esta es la extensión abeliana no ramificada maximal de K y es única, claramente.
Para mostrar el gran poder que tiene el cuerpo de clases de Hilbert, necesitamos empezar a trabajar con el símbolo de Artin. Para definirlo necesitamos el siguiente lema.

Lema 3.4. *Sea $K \subset L$ una extensión de Galois, y sea $\mathfrak{p}$ un primo de $\mathcal{O}_K$ el cual no ramifica en L. Si $\mathfrak{P}$ es un primo de $\mathcal{O}_L$ que contiene a $\mathfrak{p}$, entonces existe $\sigma \in Gal(L/K)$ tal que para todo $\alpha \in \mathcal{O}_L$*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \ mod \ \mathfrak{P}$$

donde $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ es la norma de $\mathfrak{p}$.

Antes de hacer la demostración de este lema debemos definir un par de conjuntos y hacer algunas apreciaciones sobre ellos.
Sea $K \subset L$ una extensión de Galois, y sea $\mathfrak{P}$ un primo de L. Entonces el grupo de descomposición y el grupo de inercia de $\mathfrak{P}$ son definidos como:

$$D_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\} \tag{3.2}$$

$$I_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P} \text{ para todo } \alpha \in \mathcal{O}_L\} \tag{3.3}$$

Se puede mostrar fácilmente que $I_{\mathfrak{P}} \subset D_{\mathfrak{P}}$ y que un elemento $\sigma \in D_{\mathfrak{P}}$ induce un automorfismo σ' de $\mathcal{O}_L/\mathfrak{P}$ el cual es la identidad sobre $\mathcal{O}_K/\mathfrak{p}$, $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$.
Si G' denota el grupo de Galois de $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}$, se sigue que $\sigma' \in G'$. Así la aplicación $\sigma \mapsto \sigma'$ define un homomorfismo $D_{\mathfrak{P}} \to G'$ cuyo núcleo es exactamente el grupo de inercia $I_{\mathfrak{P}}$.
Resumimos esto en la siguiente proposición.

Proposición 3.5. *Sean $D_{\mathfrak{P}}$, $I_{\mathfrak{P}}$ y G' como antes.*

(i) El homomorfismo $D_{\mathfrak{P}} \to G'$ es sobreyectivo. Así $D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong G'$.

(ii) $|I_{\mathfrak{P}}| = e_{\mathfrak{P}|\mathfrak{p}}$ y $|D_{\mathfrak{P}}| = e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}}$.

Procedemos ahora a hacer la demostración del lema 3.4.

Demostración. (Lema 3.4.) Como en la proposición 3.5, sean $D_{\mathfrak{P}}$ y $I_{\mathfrak{P}}$ los grupos de descomposición e inercia de $\mathfrak{P}$. Recuerde que $\sigma \in D_{\mathfrak{P}}$ induce un elemento $\sigma' \in G'$, donde G' es el grupo de Galois de $\mathcal{O}_L/\mathfrak{P}$ sobre $\mathcal{O}_K/\mathfrak{p}$.
Como $\mathfrak{p}$ no ramifica en L, la parte (ii) de la proposición 3.5 nos dices que $|I_{\mathfrak{P}}| = e_{\mathfrak{P}|\mathfrak{p}} = 1$, y entonces la primera parte de la proposición implica que $\sigma \mapsto \sigma'$ define un isomorfismo

$$D_{\mathfrak{P}} \longrightarrow G'.$$

La estructura de grupo de Galois de G' es bien conocida: si $\mathcal{O}_K/\mathfrak{p}$ tiene q elementos, entonces G' es un grupo cíclico cuyo generador canónico está dado por el automorfismo de Frobenius $x \mapsto x^q$. Así existe un único $\sigma \in D_{\mathfrak{P}}$ el cual es enviado en el automorfismo de Frobenius. Como $q = N(\mathfrak{p})$ por definición, σ satisface nuestra afirmación

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}$$

para todo $\alpha \in \mathcal{O}_L$.
Para ver la unicidad, note que cualquier otro σ que satisfaga la condición debe pertenecer a $D_{\mathfrak{P}}$ y como es un isomorfismo, debe ser único. □

El símbolo único σ del lema 3.4 es llamado el símbolo de Artin y es denotado $((L/K)/\mathfrak{P})$ ya que este depende del primo $\mathfrak{P}$ de L.
Su propiedad crucial es que para cualquier $\alpha \in \mathcal{O}_L$ tenemos

$$\left((L/K)/\mathfrak{P}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}$$

donde $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. El símbolo de Artin tiene las siguientes propiedades.

Corolario 3.6. *Sea $K \subset L$ una extensión de Galois, y sea $\mathfrak{p}$ un primo no ramificado de K. Dado un primo $\mathfrak{P}$ de L que contiene a $\mathfrak{p}$, tenemos:*

(i) Si $\sigma \in Gal(L/K)$, entonces

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}.$$

(ii) El orden de $((L/K)/\mathfrak{P})$ es el grado de inercia $f = f_{\mathfrak{P}|\mathfrak{p}}$.

(iii) $\mathfrak{p}$ se descompone completamente en L si, y solo si, $((L/K)/\mathfrak{P}) = 1$.

Demostración. (i) Sea $\alpha \in \mathcal{O}_L$. Note que $\left(\frac{L/K}{\sigma(\mathfrak{P})}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \sigma(\mathfrak{P})$.

Por otra parte:

$$\begin{aligned}\left[\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}\right](\alpha) &\equiv \left[\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\right](\sigma^{-1}(\alpha)) \\ &\equiv \sigma(\sigma^{-1}(\alpha))^{N(\mathfrak{p})} \\ &\equiv \alpha^{N(\mathfrak{p})} \bmod \sigma(\mathfrak{P}).\end{aligned}$$

Como el símbolo de Artin es único, $\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}$.

(ii) Para probar esto, recuerde de la prueba del lema 3.4 que, como $\mathfrak{p}$ es no ramificado, el grupo de descomposición

$$D_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

es isomorfo al grupo de Galois de la extensión finita $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}$, cuyo grado es el grado de inercia f.
Por definición del símbolo de Artin, es enviado en un generador de $G' = \mathrm{Gal}\left(\frac{\mathcal{O}_L/\mathfrak{P}}{\mathcal{O}_K/\mathfrak{p}}\right)$ y así el símbolo de Artin tiene orden $f = f_{\mathfrak{P}|\mathfrak{p}}$.

(iii) Recuerde que $\mathfrak{p}$ se descompone completamente en L si, y solo si, $e = f = 1$. Como ya sabemos que $e = 1$, pues $\mathfrak{p}$ es no ramificado, entonces por (ii), $\mathrm{Ord}\left((L/K)/\mathfrak{P}\right) = f = f_{\mathfrak{P}|\mathfrak{p}} = 1$.

□

Cuando $K \subset L$ es una extensión Abeliana, el símbolo de Artin $((L/K)/\mathfrak{P})$ depende solo del primo $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Para ver esto, sea $\mathfrak{P}'$ otro primos que contiene a $\mathfrak{p}$. Hemos visto que $\mathfrak{P}' = \sigma(\mathfrak{P})$ para algún $\sigma \in \mathrm{Gal}(L/K)$. Entonces el corolario 3.6 implica que

$$\left(\frac{L/K}{\mathfrak{P}'}\right) = \left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1} = \left(\frac{L/K}{\mathfrak{P}}\right)$$

ya que $\mathrm{Gal}(L/K)$ es Abeliano. Se sigue entonces que siempre que $K \subset L$ es Abeliando, el símbolo de Artin puede ser escrito como $((L/K)/\mathfrak{p})$.
Para ver la importancia del símbolo de Artin veamos un ejemplo en el cual generaliza al símbolo de Legendre.

Ejemplo 3.7. Consideremos el polinomio $x^2 - 1 = 0$. Luego $K = \mathbb{Q}$ y $\mathcal{O}_K = \mathbb{Z}$. Sea $\mathfrak{p} = (p)$ un ideal primo de $\mathcal{O}_K$ con p primo impar. Sea $a \in \mathcal{O}_K$ tal que $na \notin \mathfrak{p}$, donde $n = 2$ es el grado del polinomio que estamos considerando.

- Es claro que $1 \neq -1$ módulo $\mathfrak{p}$ ya que $p \neq 2$, es decir, las raíces del polinomio son distintas.

- Note que n divide a $N(\mathfrak{p})-1$ puesto que $N(\mathfrak{p}) = |\mathbb{Z}/(p)| = p$.
- Usando el símbolo de Legendre sabemos que

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

Sea ahora $L = K(\sqrt{a})$. Note que L es una extensión abeliana de K. Relacionaremos el símbolo de Legendre (a/p) con el símbolo de Artin $((L/K)/\mathfrak{p})$.

- Note que $\mathfrak{p}$ es no ramificado en $L = \mathbb{Q}(\sqrt{a})$:
  Recuerde que $d_L = a$ si $a \equiv 1 \mod 4$ o $d_L = 4a$ si $a \not\equiv 1 \mod 4$.
  Como $2a \notin \mathfrak{p}$, entonces $p \not| \ d_L$ en ningún caso. Por el corolario 2.16, $\mathfrak{p}$ no ramifica en L.
- Sea $\mathfrak{P}$ un primo de $\mathcal{O}_L$ que contiene a p. Entonces

$$\begin{aligned}\left(\frac{L/K}{p}\right)(\sqrt{a}) &\equiv \sqrt{a}^{N(p)} \mod \mathfrak{P} \\ &\equiv a^{\frac{N(p)-1}{2}}\sqrt{a} \mod \mathfrak{P}.\end{aligned}$$

  Pero como vimos antes,

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

  Y como $p \in \mathfrak{P}$ entonces

$$\left(\frac{L/K}{p}\right)(\sqrt{a}) \equiv \left(\frac{a}{p}\right)\sqrt{a} \mod \mathfrak{P}.$$

Lo cual muestra que el símbolo de Artin y el símbolo de Legendre coinciden.

Cuando $K \subset L$ es una extensión abeliana no ramificada, las cosas son interesantes ya que $((L/K)/\mathfrak{p})$ está definido para todos los primos $\mathfrak{p}$ de $\mathcal{O}_K$. Como $\mathcal{O}_K$ es un dominio de Dedekind, cualquier ideal fraccionario $\mathfrak{a} \in I_K$ tiene una factorización prima

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i}, \quad r_i \in \mathbb{Z},$$

y entonces definimos el símbolo de Artin para $((L/K)/\mathfrak{a})$ como el producto

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{i=1}^{r}\left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}.$$

El símbolo de Artin define entonces un homomorfismo, llamado la aplicación de Artin,

$$\left(\frac{L/K}{\cdot}\right) : I_K \longrightarrow \mathrm{Gal}(L/K).$$

Note que cuando $K \subset L$ es ramificada, la aplicación de Artin no está definido en todo I_K.
El teorema de reciprocidad de Artin para el cuerpo de clases de Hilbert relaciona el cuerpo de clases de Hilbert con el grupo de clase de ideales $C(\mathcal{O}_K)$ como se ve a continuación.

Teorema 3.8. *Si L es el cuerpo de clases de Hilbert de un cuerpo de números de K, entonces la apliación de Artin*

$$\left(\frac{L/K}{\cdot}\right) : I_K \longrightarrow Gal(L/K)$$

es sobreyectiva, y su núcleo es exactamente el subgrupo P_K de ideales fraccionarios principales.
Así la aplicación de Artin induce un isomorfismo

$$C(\mathcal{O}_K) \cong Gal(L/K).$$

Si aplicamos la teoría de Galois a los teoremas 3.3 y 3.8, obtenemos la siguiente clasificación de las extensiones abelianas no ramificadas de K.

Corolario 3.9. *Dado un cuerpo de números K, existe una correspondencia uno a uno entre las extensiones abelianas no ramificadas M de K y subgrupos H del grupo de clase de ideales $C(\mathcal{O}_K)$. Además, si la extensión $K \subset M$ corresponde al subgrupo $H \subset C(\mathcal{O}_K)$, entonces la aplicación de Artin induce un isomorfismo*

$$C(\mathcal{O}_K)/H \cong Gal(M/K).$$

La importancia del corolario 3.9 es que nos permite encontrar todas las extensiones abelianas no ramificadas de K a partir del cálculo de los subgrupos del grupo de clase de ideales $C(\mathcal{O}_K)$. Esto es, que la información de K está intrínseca en la estructura de grupo de $C(\mathcal{O}_K)$.
El teorema 3.8 también nos da una caracterización de los primos de K que se descomponen completamente en el cuerpo de clases de Hilbert.

Corolario 3.10. *Sea L el cuerpo de clases de Hilbert de un cuerpo de números de K, y sea $\mathfrak{p}$ un ideal primo de K. Entonces*

$$\mathfrak{p} \textit{ se descompone completamente en } L \iff \mathfrak{p} \textit{ es un ideal principal.}$$

Demostración. El corolario 3.6 implica que el primo $\mathfrak{p}$ se descompone completamente en L si, y solo si $((L/K)/\mathfrak{p}) = 1$. Como la aplicación de Artin induce un isomorfismo $C(\mathcal{O}_K) \cong \mathrm{Gal}(L/K)$, vemos que $((L/K)/\mathfrak{p}) = 1$ si, y solo si, $\mathfrak{p}$ determina la clase

trivial de $C(\mathcal{O}_K)$. Por definición del grupo de clase de ideales, esto significa que $\mathfrak{p}$ es principal, y el corolario queda probado. □

3.1. Solución de $p = x^2 + ny^2$ para infinitos n.

Ahora que hemos desarrollado la teoría de cuerpo de clases de Hilbert, podemos hacer la prueba del teorema 3.1.

Demostración. (Teorema 3.1.) El primer paso es relacionar $p = x^2 + ny^2$ al comportamiento de p en el cuerpo de clases de Hilbert L. Este resultado es interesante y por eso lo enunciamos como un teorema.

Teorema 3.11. *Sea L el cuerpo de clases de Hilbert de $K = \mathbb{Q}(\sqrt{-n})$. Asuma que n satisface (3.1), luego $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$. Si p es un primo impar que no divide a n, entonces*

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

Demostración. Como n satisface (3.1), tenemos entonces que $d_K = -4n$ y $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$. Sea p un primo impar que no divide a n. Entonces $p \nmid d_K$, y por el corolario 2.16 tenemos que p no ramifica en K. Probaremos las siguientes equivalencias:

$$\begin{aligned} p = x^2 + ny^2 &\iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \neq \overline{\mathfrak{p}} \text{ y } \mathfrak{p} \text{ es principal en } \mathcal{O}_K \\ &\iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \neq \overline{\mathfrak{p}},\ \text{y } \mathfrak{p} \text{ se descompone completamente en } L \\ &\iff p \text{ se descompone completamente en } L. \end{aligned} \tag{3.4}$$

y el teorema 3.11 se tendrá.
Para la primera equivalencia, suponga que $p = x^2 + ny^2 = (x + \sqrt{-n}y)(x - \sqrt{-n}y)$. Tomando $\mathfrak{p} = (x + \sqrt{-n}y)\mathcal{O}_K$, entonces $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ debe ser la factorización prima de $p\mathcal{O}_K$ en $\mathcal{O}_K$. Note que $\mathfrak{p} \neq \overline{\mathfrak{p}}$ ya que p es no ramificado en K. Recíprocamente, suponga que $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$, donde $\mathfrak{p}$ es principal. Como $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$, podemos escribir $\mathfrak{p} = (x + \sqrt{-n}y)\mathcal{O}_K$. Esto implica que $p\mathcal{O}_K = (x^2 + ny^2)\mathcal{O}_K$, y se tiene entonces que $p = x^2 + ny^2$.
La segunda equivalencia de 3.4 se sigue inmediatamente del corolario 3.10. Para probar la última equivalencia, usaremos los siguientes lemas:

Lema 3.12. *Si $K \subset M \subset L$, donde L y M son Galois sobre K, entonces un primo $\mathfrak{p}$ de $\mathcal{O}_K$ se descompone completamente en L si, y solo si, este se descompone completamente en M y algún primo de $\mathcal{O}_M$ conteniendo a $\mathfrak{p}$ se descompone completamente en L.*

Lema 3.13. *Sea K un cuerpo cuadrático imaginario, y sea $K \subset L$ una extensión de Galois. Como es usual, τ denotará la conjugación compleja.*

(a) L es Galois sobre $\mathbb{Q}$ si, y solo si, $\tau(L) = L$.

(b) Si L es Galois sobre $\mathbb{Q}$, entonces

(i) $[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$.

(ii) *Para* $\alpha \in L \cap \mathbb{R}$, $L \cap \mathbb{R} = \mathbb{Q}(\alpha) \Leftrightarrow L = K(\alpha)$.

Lema 3.14. *Sea L el cuerpo de clases de Hilbert de un cuerpo cuadrático imaginario K, y sea τ la conjugación compleja. Entonces $\tau(L) = L$, y así L es Galois sobre $\mathbb{Q}$.*

Demostración. Es fácil ver que $\tau(L)$ es una extensión abeliana no ramificada de $\tau(K) = K$. Como L es la extensión maximal de estas, tenemos que $\tau(L) \subset L$, y entonces $\tau(L) = L$ ya que ellas tiene el mismo grado sobre K. Así $\tau \in \mathrm{Gal}(L/\mathbb{Q})$, lo cual implica que L es Galois sobre $\mathbb{Q}$.

□

Para terminar la prueba de (3.4), note que la condición

$$p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \neq \overline{\mathfrak{p}},\ \text{y } \mathfrak{p} \text{ se descompone completamente en } L$$

dice que p se descompone completamente en K y que algún primo de K que contiene a p se descompone completamente en L. Como L es Galois sobre $\mathbb{Q}$, es fácil ver que es equivalente a que p se descomponga completamente en L y así el teorema 3.11 queda probado. □

El siguiente paso para la prueba del teorema 3.1 es dar una forma más sencilla de decir que p se descompone completamente en L. Tenemos el siguiente criterio:

Proposición 3.15. *Sea K un cuerpo cuadrático imaginario, y sea L una extensión finita de K la cual es Galois sobre $\mathbb{Q}$. Entonces:*

(i) *Hay un entero algebraico real α tal que $L = K(\alpha)$.*

(ii) *Dado α como en (i), sea $f(x) \in \mathbb{Z}[x]$ el polinomio mónico de α. Si p es un primo que no divide al discriminante de $f(x)$, entonces*

$$p \text{ se descompone completamente en } L \iff \begin{cases} (d_K/p) = 1 \text{ y } f(x) \equiv 0 \bmod p \\ \text{tiene una solución entera.} \end{cases}$$

Demostración. Por hipótesis, L es Galois sobre $\mathbb{Q}$, y así $[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$ ya que $L \cap \mathbb{R}$ es el cuerpo fijo bajo la conjugación compleja. Esto implica que para $\alpha \in L \cap \mathbb{R}$,

$$L \cap \mathbb{R} \Longleftrightarrow L = K(\alpha).$$

Así, si $\alpha \in \mathcal{O}_L \cap \mathbb{R}$ satisface $L \cap \mathbb{R} = \mathbb{Q}(\alpha)$, entonces α es un elemento real integral primitivo de L sobre K, y (i) está probada. Además, dado un α, sea $f(x)$ su polinomio minimal sobre $\mathbb{Q}$. Entonces $f(x) \in \mathbb{Z}[x]$, y como $[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$, $f(x)$ es también el polinomio minimal de α sobre K.
Para probar la parte final de (ii), sea p un primo que no divide al discriminante de $f(x)$. Esto nos indica que $f(x)$ es separable módulo p. Por el corolario 2.16 tenemos que

$$p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \neq \overline{\mathfrak{p}} \Longleftrightarrow \left(\frac{d_K}{p}\right) = 1.$$

Suponemos que p se descompone completamente en K, entonces $\mathbb{Z}/p\mathbb{Z} \cong \mathcal{O}_K/\mathfrak{p}$. Como $f(x)$ es separable sobre $\mathbb{Z}/p\mathbb{Z}$, es separable sobre $\mathcal{O}_K/\mathfrak{p}$, y entonces la proposición 1.30 muestra que

$$\begin{aligned} p \text{ se descompone completamente en } L &\iff f(x) \equiv 0 \bmod \mathfrak{p} \text{ tiene solución en } \mathcal{O}_K \\ &\iff f(x) \equiv 0 \bmod p \text{ tiene solución en } \mathbb{Z}, \end{aligned}$$

donde la última equivalencia de nuevo usa que $\mathbb{Z}/p\mathbb{Z} \cong \mathcal{O}_K/\mathfrak{p}$. La proposición se sigue ahora de la última equivalencia de (3.4). □

Podemos ahora probar la principal equivalencia del teorema 3.1. Como el cuerpo de clases de Hilbert L de $K = \mathbb{Q}(\sqrt{-n})$ es Galois sobre $\mathbb{Q}$, la proposición 3.15 implica que existe un entero algebraico real α el cual es un elemento primitivo de L sobre K. Sea $f_n(x)$ el polinomio mónico minimal de α, y sea p un primo impar que no divide a n ni al discriminante de $f_n(x)$. Entonces el teorema 3.11 y la proposición 3.15 implican que

$$\begin{aligned} p = x^2 + ny^2 &\iff p \text{ se descompone completamente en } L \\ &\iff \begin{cases} (-n/p) = 1 \text{ y } f_n(x) \equiv 0 \bmod p \\ \text{tiene una solución en los enteros.} \end{cases} \end{aligned}$$

En la segunda equivalencia, recuerde que n satisface (3.1), luego $d_K = -4n$, y así $(d_K/p) = (-n/p)$.
Resta mostrar que el grado de $f_n(x)$ es el número de clases $h(-4n)$. Usando la teoría de Galois y el teorema 3.8, tenemos que $f_n(x)$ tiene grado

$$[L : K] = |\mathrm{Gal}(L/K)| = |C(\mathcal{O}_K)|.$$

Por el teorema 2.13 tenemos que, como $d_K < 0$, existe un isomorfismo natural

$$C(\mathcal{O}_K) \cong C(d_K)$$

entre el grupo de clase de ideales $C(\mathcal{O}_K)$ y el grupo de clases de formas $C(d_K)$. Como $d_K = -4n$, tenemos que $|C(\mathcal{O}_K)| = |C(-4n)| = h(-4n)$, lo cual completa la demostración del teorema 3.1. □

Ahora damos un ejemplo del teorema 3.1.

Ejemplo 3.16. Consideremos el caso $p = x^2 + 14y^2$. Por el teorema 3.1 sabemos que existe un polinomio $f_{14}(x)$ tal que

$$p = x^2 + 14y^2 \iff \begin{cases} (-14/p) = 1 \text{ y } f_{14}(x) \equiv 0 \bmod p \\ \text{tiene solución entera,} \end{cases}$$

pero todo lo que sabemos es que $f_{14}(x)$ tiene grado 4 ya que $h(-56) = 4$.
Esta es una debilidad del teorema 3.1: nos dice que existe un polinomio pero no sabemos cómo hallarlo.

Para determinar $f_{14}(x)$ necesitamos conocer el cuerpo de clases de Hilbert de $\mathbb{Q}(\sqrt{-14})$.

Proposición 3.17. *El cuerpo de clases de Hilbert de $K = \mathbb{Q}(\sqrt{-14})$ es $L = K(\alpha)$, donde $\alpha = \sqrt{2\sqrt{2}-1}$.*

Demostración. Como $h(-56) = 4$, el cuerpo de clases de Hilbert tiene grado 4 sobre K. Entonces $L = K(\alpha)$ será el cuerpo de clases una vez se muestre que $K \subset L$ es una extensión abeliana no ramificada de grado 4.
Para ver que es abeliana, note que existen cuatro automorfismo de L, los cuales forman un grupo bajo la composición. Por el teorema de estructura para grupos finitos, este grupo será isomorfo a $\mathbb{Z}_4$ o $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ los cuales son abelianos.
Además, como K es una extensión imaginaria cuadrática, los primos infinitos son automáticamente no ramificados.
Note que $\alpha^2 = 2\sqrt{2} - 1$, luego $\sqrt{2} \in L$. Si tomamos $K_1 = K(\sqrt{2})$ tenemos la extensión $K \subset K_1 \subset L$, y es suficiente mostrar que $K \subset K_1$ y $K_1 \subset L$ son no ramificados.
Como cada una de estas extensiones es obtenida adjuntando una raíz cuadrada ($K_1 = K(\sqrt{2})$ y $L = K_1(\sqrt{\mu})$, $\mu = 2\sqrt{2} - 1$), probemos primero un lema general sobre esta situación.

Lema 3.18. *Sea $L = K(\sqrt{\mu})$ una extensión cuadrática con $\mu \in \mathcal{O}_K$, y sea $\mathfrak{p}$ un primo de $\mathcal{O}_K$.*

(i) Si $2\mu \notin \mathfrak{p}$, entonces $\mathfrak{p}$ no ramifica en L.

(ii) Si $2 \in \mathfrak{p}$, $\mu \notin \mathfrak{p}$ y $\mu = b^2 - 4c$ para algunos $b, c \in \mathcal{O}_K$ entonces $\mathfrak{p}$ es no ramificado en L.

Demostración. (i) Como el discriminante de $x^2 - \mu$ es $4\mu \notin \mathfrak{p}$, $x^2 - \mu$ es separable módulo $\mathfrak{p}$. Así $\mathfrak{p}$ es no ramificado por la proposicion 1.30.

(ii) Note que $L = K(\beta)$ donde $\beta = (-b + \sqrt{\mu})/2$ es una raíz de $x^2 + bx + c$. El discriminante es $b^2 - 4c = \mu \notin \mathfrak{p}$, de nuevo $\mathfrak{p}$ es no ramificado por la proposición 1.30.

□

Ahora podemos probar la proposición 3.17. Para estudiar $K \subset K_1$, sea $\mathfrak{p}$ primo en $\mathcal{O}_K$. Como $K_1 = K(\sqrt{2})$, la parte (i) del lema 3.18 implica que $\mathfrak{p}$ es ramificado siempre que $2 \notin \mathfrak{p}$. Falta estudiar el caso que $2 \in \mathfrak{p}$. Como $\sqrt{-14} \in K$ y $\sqrt{2} \in K_1$, tenemos que $\sqrt{-7} \in K_1$, es decir, $K_1 = K(\sqrt{-7})$. Como $-7 \notin \mathfrak{p}$ y $-7 = 1^2 - 4 \cdot 2$, $\mathfrak{p}$ es no ramificado por la parte (ii) del lema 3.18.
La extensión $K_1 \subset L$ es más sencilla. Sabemos que $L = K_1(\sqrt{\mu})$, $\mu = 2\sqrt{2} - 1$. Sea $\mu' = -2\sqrt{2} - 1$. Como $\sqrt{\mu\mu'} = \sqrt{-7} \in K_1$, se sigue que $\sqrt{\mu'} \in L$ y de hecho

$$L = K_1(\sqrt{\mu}) = K_1(\sqrt{\mu'}).$$

Sea $\mathfrak{p}$ un primo de K_1. Si $2 \notin \mathfrak{p}$, entonces $\mu + \mu' = -2$ muestra que $\mu \notin \mathfrak{p}$ o $\mu' \notin \mathfrak{p}$ y $\mathfrak{p}$ es no ramificado por la parte (i) del lema 3.18.
Si $2 \in \mathfrak{p}$, entonces $\mu \notin \mathfrak{p}$ ya que $\mu = 2\sqrt{2} - 1$ puesto que de lo contrario tendría que $1 \in \mathfrak{p}$.
Además se tiene que $\mu = (1+\sqrt{2})^2 - 4$, y entonces la parte (ii) del lema 3.18 muestra que $\mathfrak{p}$ es no ramificado. □

Ahora podemos caracterizar cuándo un primo p es representado por $x^2 + 14y^2$.

Teorema 3.19. *Si $p \neq 7$ es un primo impar, entonces*

$$p = x^2 + 14y^2 \Longleftrightarrow \begin{cases} (-14/p) = 1 \text{ y } f_{14}(x) \equiv 0 \text{ mod } p \\ \text{tiene solución entera.} \end{cases}$$

Demostración. Como $\alpha = \sqrt{2\sqrt{2} - 1}$ es un elemento primitivo del cuerpo de clases de Hilbert de $K = \mathbb{Q}(\sqrt{-14})$, su polinomio minimal $x^4 + 2x^2 - 7 = (x^2 + 1)^2 - 8$ puede ser escogido como el polinomio $f_{14}(x)$. Su discriminante es $-2^{14} \cdot 7$, luego solo excluimos los primos 2 y 7. Así el teorema se sigue del teorema 3.1. □

Bibliografía

[1] **Cox, David A.** , *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication.* Second Edition. John Wiley & Sons New Jersey, Inc., New Jersey, 2013. ISBN: 978-1-118-39018-4.

[2] **K. Ireland and M. Rosen** , *A Classical Introduction to Modern Number Theory.* Springer-Verlag Berlin, Ltd., Berlin, 1982. ISBN: 978-1-4757-1781-5.