Trabajo Monográfico

Primos de la forma $x^2 + ny^2$

Autor: Felipe Negreira

Orientador: Gonzalo Tornaría.

Licenciatura en Matemática
Facultad de Ciencias
Universidad de la República
Uruguay

31 de Octubre de 2013

Resumen

El objetivo de esta monografía es la resolución de un problema concreto de la teoría de números:

Fijado un entero positivo n, ¿qué primos p pueden escribirse de la forma $p = x^2 + ny^2$ con x e y enteros?

El problema va a ser teóricamente resuelto varias veces en el texto, pero de forma parcial, para llegar finalmente a una resolución completa. Al mismo tiempo se ofrecerán varios ejemplos de soluciones en casos particulares de la práctica.

Las herramientas que serán implementadas vienen desde las más primitivas y elementales áreas de la teoría de números como la reciprocidad cuadrática y las formas cuadráticas, hasta otras más nuevas y sofisticadas como la teoría de números algebraicos y la teoría de cuerpos de clases.

El trabajo esta basado en el libro de Cox [2].

Palabras claves: reciprocidad cuadrática, teoría de cuerpos de clases.

Abstract

The aim of this monograph is to solve a particular problem in number theory:

Given a positive integer n, which primes p can be written as $p = x^2 + ny^2$ where x and y are integers?

The problem will be partially solved several times in the text, ending with a complete theoretical resolution. At the same time several examples of solutions in particular cases will be offered.

The tools that will be applied come from the most basic and elementary areas of number theory as quadratic reciprocity and quadratic forms, to more modern and sophisticated areas as algebraic number theory and class field theory.

The work is based on the book of Cox [2].

Key words: quadratic reciprocity, class field theory.

Índice general

Capítulo 0

Introducción

Lo que más llama la atención del problema $p = x^2+ny^2$ es su formulación elemental; alcanza conocer los conceptos básicos de la aritmética para poder entenderlo. El motivo de esta sencillez se debe a la antigüedad que tiene el problema: si bien su primera aparición formal fue en las cartas de Fermat de 1640 (que pueden leerse en [5], volumen II, páginas 212, 310-314) hay que tener en cuenta que el mismo fue inspirado por los textos escritos por Diophantus alrededor de 250 D.C. Y en esa época los problemas con números, que eran entendidos siempre como racionales, estaban centrados en la factorización en primos y las ecuaciones con enteros (hoy llamadas *Diofánticas*), preferentemente cercanas a la de Pitágoras $z^2 = x^2 + y^2$. Una recopilación de los trabajos de Diophantus pueden leerse en el libro *Arithmetica* escrito por Heath [7].

Reviendo estos trabajos a Fermat le resultó natural formularse las siguientes conjeturas:

Para todo primo p se cumple que

$$\begin{array}{rcl} p = x^2 + y^2 & \iff & p = 2 \text{ o } p \equiv 1 \text{ mód } 4 \\ p = x^2 + 2y^2 & \iff & p = 2 \text{ o } p \equiv 1, 3 \text{ mód } 8 \\ p = x^2 + 3y^2 & \iff & p = 3 \text{ o } p \equiv 1 \text{ mód } 3 \end{array} \tag{0.0.1}$$

Casi un siglo después, en 1729, Euler se encontró con estos resultados y consideró que merecían una prueba seria. Y aunque tuvo muchos problemas para demostrar los resultados y no pudo obtener formulaciones más generales, introdujo una idea que resultaría clave en el futuro para la resolución del problema $p = x^2 + ny^2$: la *reciprocidad*. De forma intuitiva Euler se dio cuenta que la condición necesaria $p \mid x^2 + ny^2$, implica que p tiene que cumplir con ciertas condiciones respecto de n, a saber: p debe estar entre un conjunto fijo de restos en la división por $4n$. Esto le llevó a también conjeturar

$$p = x^2 + 7y^2 \iff p = 7 \text{ o } p \equiv 1, 9, 11, 15, 23, 25 \text{ mód } 28.$$

Una recopilación de estos resultados y estas ideas pueden leerse la *Opera Omnia* de Euler [4].

El problema, y la teoría de números toda, adquirió una nueva dimensión con la introducción de las *formas cuadráticas* por parte de Lagrange en su *Recherches d'Arithmétique* [12] alrededor de 1775. Bajo este enfoque, el problema $p = x^2 + ny^2$ es visto como uno general de representación de formas:

Dada una forma cuadrática entera $Q(x, y)$ y un primo p, ¿representa $Q(x, y)$ a p?

Lagrange se dio cuenta que las formas de igual discriminante no pueden distinguirse en términos de representación, y que en particular $p \mid x^2 + ny^2$ no siempre implica $p = x^2 + ny^2$. Lo que hizo Lagrange fue utilizar su teoría para demostrar que en efecto esto último sucede en los teoremas enunciados por Fermat. Sin embargo se encontró con inconvenientes cuando quiso generalizar sus métodos en el resto de los casos de $p = x^2 + ny^2$, porque no conocía las propiedades de la reciprocidad cuadrática en general que son decisivas en los resultados de representación. Esto fue notado por su estudiante Legendre que una década más tarde en 1785 probó, aunque con algunos errores, cómo los estudios de su maestro se combinaban con la reciprocidad cuadrática para dar formulaciones más generales sobre representaciones de formas cuadráticas. A Legendre también se le atribuyen la notación (a/p) que indica cuándo un entero a es un cuadrado módulo p (que en el caso $x^2 + ny^2$, $(-n/p)$ viene a ser la condición $p \mid x^2 + ny^2$), y desde luego el enunciado de la *ley de reciprocidad cuadrática* que dice precisamente cómo se da vuelta la condición $(-n/p)$ a una de p según n (como sospechaba Euler). Las "pruebas" de Legendre están en su *Essai sur la Théorie des Nombres* [13].

Pero no fue hasta la aparición de Gauss que esta teoría adquirió la madurez suficiente. Con su libro *Disquisitiones Arithmeticae* en 1801 [6] Gauss no sólo formalizó toda la teoría desarrollada por Lagrange y Legendre, coronándose con resultados del tipo

$$p = \begin{cases} Q_1(x, y) \\ \quad \vdots \\ Q_G(x, y) \end{cases} \iff p \equiv r_1, \ldots, r_t \text{ mód } D$$

(donde D es el discriminante de las formas $Q_1(x, y), \ldots, Q_G(x, y)$), sino que también redujo esa misma lista de formas cuadráticas con su *teoría de géneros* y así conseguir una descripción más exacta de la *forma principal* $x^2 + ny^2$. Esto resolvió por ejemplo el caso de $n = 5$ contestando afirmativamente la conjetura de Euler

$$p = x^2 + 5y^2 \iff p \equiv 1, 9 \text{ mód } 20.$$

Pero a pesar de que estos aportes permitieron resolver otra nueva gran cantidad de casos de $p = x^2 + ny^2$, aún seguían habiendo casos en los que la forma $x^2 + ny^2$ no se podía separar exclusivamente. Por ejemplo en $n = 14$ la teoría hecha hasta entonces sólo permitía afirmar que

$$p = \begin{cases} x^2 + 14y^2 \\ \text{o} \\ 2x^2 + 7y^2 \end{cases} \iff p \equiv 1, 9, 15, 23, 25, 39 \text{ mód } 56.$$

Esto estaba evidenciando que la reciprocidad inducida por Euler no era suficiente para resolver los problemas de representación de formas, que alguna reciprocidad mayor no conocida estaba participando. Los matemáticos de la teoría de números se vieron entonces motivados a encontrar alguna ley de reciprocidad que se pudiera usar en los casos irresolutos. Gauss fue todavía capaz de descubrir dos reciprocidades más entre 1805 y 1814, la reciprocidad cúbica y la bicuadrática, con lo que pudo demostrar que

$$p = x^2 + 27y^2 \iff \begin{cases} p \equiv 1 \text{ mód } 3 \\ x^3 \equiv 2 \text{ mód } p \text{ tiene solución entera} \end{cases}$$

y

$$p = x^2 + 64y^2 \iff \begin{cases} p \equiv 1, 3 \text{ mód } 8 \\ x^4 \equiv 2 \text{ mód } p \text{ tiene solución entera} \end{cases}$$

Más tarde, alrededor de 1850, Eisentein y Jacobi elaboraron reciprocidades para potencias quintas, octavas y hasta duodécimas. También Kummer dio su propia versión de la reciprocidad. (Un buen sumario de esto puede leerse en el libro de Lemmermeyer *Reciprocity Laws: From Euler to Eisenstein* [14]). Pero ahora los elementos con los que se trabajaba habían dejado de ser enteros e incluso en muchos casos ni siquiera tenían la propiedad de factorización única. Fue recién a partir de 1871 que, gracias Dedekind, se empezó a comprender estas nuevas estructuras (hoy llamadas *dominios de Dedekind*) trasladando los conceptos de factorización en los elementos para los ideales donde ahora sí se podía sostener la unicidad de la factorización (una buena lectura al respecto es el libro de Dedekind *Sur la Théorie des nombres entiers algébriques* [3]). Sin dudas que todo esto le dio un nuevo enfoque al problema, dando origen al mismo tiempo a una nueva rama de la teoría de números: la *teoría de números algebraicos*. Desde entonces el problema $p = x^2 + ny^2$ ya no fue más visto como un problema de representación de formas y paso a ser un problema de factorización en el cuerpo de números $\mathbb{Q}(\sqrt{-n})$:

¿Cuándo un primo entero p (visto como ideal de $\mathbb{Q}(\sqrt{-n})$) se puede factorizar en términos (ideales principales) de la forma $x \pm \sqrt{-n}y$?

Por esto Hilbert, al igual que otros, estuvo tan interesado en, dado un cuerpo de números K, conseguir un cuerpo L por encima de K donde todos los ideales de K puedan ser entendidos como principales en L. A este cuerpo

luego se le llamó luego el *cuerpo de clases de Hilbert*. Pero para probar la existencia de semejante cuerpo necesariamente hay que pasar por los argumentos de la reciprocidad. Fue así que el mismo Hilbert propuso como noveno problema de su famosa lista de 23 problemas de 1900 [9] la búsqueda de una ley de reciprocidad unificara todas las anteriores y se pudiera aplicar en todos los cuerpos de números.

La solución, o al menos la que sirve para el problema $p = x^2 + ny^2$, vino 25 años más tarde en un conjunto de trabajos publicados por Artin en 1924, 1927 y 1929 (el concluyente articulo es *Idealklassen in oberkörpern und allgemeines reziprozitätsgesetz* [1]). Esto significó además el comienzo de una nueva rama de la teoría de números surgida como la continuación de la teoría de números algebraicos: la *teoría de cuerpos de clases*. En estos trabajos Artin demuestra la existencia del cuerpo de clases de Hilbert L sobre cualquier cuerpo de números K y lo hace precisamente a través de un nuevo mapa de reciprocidad hoy llamado *mapa de Artin*.

La reciprocidad viene del hecho que además este mapa permite decir que los ideales principales de K son exactamente aquellos que descomponen completamente en L. Lo cual en particular para el problema $p = x^2 + ny^2$ resulta definitorio: los primos p de la forma $p = x^2 + ny^2$ son exactamente los que descomponen completamente en L. Y esto se puede resumir en el siguiente teorema:

Teorema 1. *Sea n un entero positivo cualquiera. Entonces existe un polinomio entero mónico irreducible $f_n(x)$ tal que si p es un primo que no divide ni a $4n$ ni al discriminante de $f_n(x)$ se cumple que*

$$p = x^2 + ny^2 \iff \begin{cases} \left(\frac{-n}{p}\right) = 1 \ y \\ f_n(x) \equiv 0 \text{ mód } p \text{ tiene solución entera.} \end{cases}$$

De modo que en efecto este teorema no sólo generaliza a todos los resultados anteriores y sino que además resuelve el problema $p = x^2 + ny^2$ completamente. Una muestra de ello es la resolución del caso pendiente $p = x^2 + 14y^2$:

$$p = x^2 + 14y^2 \iff \begin{cases} \left(\frac{-14}{p}\right) = 1 \text{ y} \\ (x^2+1)^2 \equiv 8 \text{ mód } p \text{ tiene solución entera} \end{cases}$$

Por todo esto el teorema anterior es sin dudas el resultado más importante de todo este trabajo.

En esta monografía se procederá según el mismo recorrido histórico antes redactado, quedando así dividida en dos partes: una correspondiente a la época comprendida desde Fermat hasta Gauss donde se abordan los temas de la reciprocidad cuadrática y formas cuadráticas, y la otra con la teoría desarrollada a partir de 1900, es decir la teoría de números algebraicos y la teoría de cuerpos clases. Al final del último capítulo estos dos enfoques se relacionan a través de una correspondencia explícita.

Parte I

Reciprocidad cuadrática y formas cuadráticas

"Entonces, cuando tuve que probar que todo número primo que excede a un múltiplo de 4 por 1 está compuesto por la suma de dos cuadrados, me encontré a mi mismo en una tormenta". Pierre de Fermat.

En esta primera parte el problema $p = x^2 + ny^2$ se ataca con métodos elementales de teoría de números como lo son la *reciprocidad cuadrática* y la *teoría elemental de formas cuadráticas enteras.*

Los tres teoremas enunciados por Fermat en la introducción van a ser el punto de partida y al mismo la guía a lo largo de toda esta parte:

Teorema. *Un primo impar p puede ser escrito como $x^2 + y^2$ si y sólo si $p \equiv 1$ mód 4.*

Demostración. El directo es inmediato, ya que si $p = x^2 + y^2$ y p es impar entonces las congruencias módulo 4 (dónde los cuadrados sólo pueden ser 0 o 1) implican que $p \equiv 1$ mód 4.

La idea de la prueba del recíproco es que si un número N es la suma de dos cuadrados y tiene un divisor q que también lo es, entonces el cociente N/q puede ser escrito como la suma de dos cuadrados. Y de esta forma si $p \mid N = x^2 + y^2$, se puede ir descendiendo por cocientes de N por los divisores que son sumas de cuadrados, hasta llegar al mismo p. Esto es lo que se llama el *paso de descenso* de la prueba:

Si $p \mid x^2 + y^2$ con $mcd(x, y) = 1$ entonces p puede escribirse como $x^2 + y^2$.

Antes, hay que probar el siguiente lema:

Lema. *Supóngase que N es la suma de dos cuadrados relativamente primos y que $q = x^2 + y^2$ es un divisor primo de N. Entonces también N/q es la suma de dos cuadrados coprimos.*

Demostración. La clave del lema es la clásica igualdad

$$(x^2 + y^2)(z^2 + w^2) = (xz \pm yw)^2 + (xw \mp yz)^2, \tag{0.0.2}$$

de modo que si N y q son suma de cuadrados tiene sentido pensar que también lo será N/q, lo cual se verá con cuentas.

Sean $N = a^2 + b^2$ con a y b relativamente primos y $q = x^2 + y^2$. Luego usando la ecuación (0.0.2)

$$Nq = (xa + yb)^2 + (xb - ya)^2.$$

Y los dos sumandos de la izquierda son divisibles por q ya que q es un primo que divide a

$$x^2N - b^2q = x^2(a^2 + b^2) - b^2(x^2 + y^2) = x^2a^2 - b^2y^2 = (xa - by)(xa + by)$$
$$x^2N - a^2q = x^2(a^2 + b^2) - a^2(x^2 + y^2) = x^2b^2 - a^2y^2 = (xb - ay)(xb + ay)$$

por lo cual eventualmente cambiando el signo de x, se puede suponer que $q \mid xa + by, xb - ay$. Así

$$\frac{N}{q} = \left(\frac{xa + yb}{q}\right)^2 + \left(\frac{xb - ya}{q}\right)^2$$

puede ser visto como la suma de dos cuadrados. □

Ahora si p divide a $N = a^2 + b^2$ con a y b relativamente primos, lo único que impediría descender por el lema sería que alguno de los otros divisores primos q de N no se pueda escribir como suma de cuadrados. Pero esto conduciría a un absurdo: se pueden cambiar a y b para que todos los divisores primos de N diferentes de p sean menores que él, y en ese caso se vuelve a aplicar el mismo razonamiento obteniéndose primos cada vez más pequeños. Para esto muévanse a y b por múltiplos de p de modo que $|a|, |b| < p/2$ y se siga teniendo $p \mid a^2 + b^2$. Si ahora $d = mcd(a, b)$ entonces d no puede ser divisible por p dado que $|d| < p/2$; y entonces p divide a $(a/d)^2 + (b/d)^2$. En suma se puede reconstruir $N = a^2 + b^2$ para que p siga dividiéndolo, a y b sigan siendo coprimos pero además para que $N < p^2/2$ y en consecuencia todos sus otros divisores primos sean menores a p.

Para terminar la prueba del recíproco falta ver que, en efecto, $p \mid x^2 + y^2$. Esto se debe a la hipótesis $p \equiv 1$ mód 4 y se llama el *paso de reciprocidad*:

Si $p \equiv 1$ mód 4 *entonces* $p \mid x^2 + y^2$ *para ciertos* x, y *con* $mcd(x, y) = 1$.

De cualquier forma, si $p \equiv 1$ mód 4, entonces $p = 4k + 1$ y el *pequeño teorema de Fermat* implica que

$$(x^{2k} - 1)(x^{2k} + 1) = x^{4k} - 1 \equiv 0 \text{ mód } p$$

para todo $x \not\equiv 0$ mód p. Si para alguno de esos $x's$, $x^{2k} - 1 \not\equiv 0$ mód p, entonces $p \mid x^{2k} + 1$ y p divide a la suma de dos cuadrados relativamente primos. Pero como $x^{2k} - 1$ es un polinomio sobre el cuerpo $\mathbb{Z}/p\mathbb{Z}$, entonces tiene a lo sumo $2k < p - 1$ raíces y por lo tanto existen $x's$ tales que $x^{2k} - 1 \not\equiv 0$ mód p. □

En realidad, la igualdad (0.0.2) se puede generalizar para $n > 1$ de la siguente forma

$$(x^2 + ny^2)(z^2 + nw^2) = (xz \pm nyw)^2 + n(xy \mp zw)^2. \tag{0.0.3}$$

Esto permite también establecer un resultado análogo al lema del teorema con $n > 1$. Luego se podría pensar que todo el paso de descenso se puede repetir en general, pero esto podría no funcionar cuando $n > 3$ ya que en ese caso $(1 + n)p^2/2 > 2p^2$ y entonces cabe la posibilidad de que $x^2 + ny^2$

tenga divisores primos mayores que p aún teniéndose que $|x|, |y| \leq p/2$. De hecho cuando $n = 5$ se halla que $3 \mid 21 = 1^2 + 5 \cdot 2^2$ pero $3 \neq x^2 + 5y^2$.

De cualquier manera, para rehacer la misma prueba cuando $n > 1$ también hay que volver a enunciar el paso de reciprocidad. Con las mismas herramientas elementales usadas en el teorema se encuentra que

Si $p \equiv 1, 3$ mód 8 entonces existen x e y coprimos tales que $p \mid x^2 + 2y^2$

Si $p \equiv 1$ mód 3 entonces existen x e y coprimos tales que $p \mid x^2 + 3y^2$.

Luego los otros dos teoremas de Fermat

$$\begin{array}{lll} p = x^2 + 2y^2 & \iff & p = 2 \text{ o } p \equiv 1, 3 \text{ mód } 8 \\ p = x^2 + 3y^2 & \iff & p = 3 \text{ o } p \equiv 1 \text{ mód } 3 \end{array}$$

se siguen con los mismo métodos de la demostración anterior.

La motivación de toda esta primera parte será generalizar estos argumentos para cualquier valor de n. En el *paso de reciprocidad* se buscará, a través de la *reciprocidad cuadrática*, condiciones para p según n que aseguren $p \mid x^2 + ny^2$. Mientras que el *paso de descenso* tratará de clasificar los divisores de $x^2 + ny^2$ usando *teoría elemental de formas cuadráticas*.

Capítulo 1

Reciprocidad cuadrática

Aunque todavía no se pueda decir nada en el paso de descenso cuando $n > 1$, es productivo pensar que condiciones hacen falta para qué se cumpla el paso de reciprocidad, es decir para que $p \mid x^2 + ny^2$. Después de todo cuando $p = x^2 + ny^2$, p es un divisor de $x^2 + ny^2$.

Lo mejor sería obtener un resultado del tipo

$$p \mid x^2 + ny^2 \quad \text{si } p \equiv r_1, \ldots, r_s \text{ mód } m \tag{1.0.1}$$

para cierto entero m y ciertos restos $r_1, \ldots, r_s$. Mirando los casos ya resueltos, es esperable que el módulo m sea $4n$. Luego, hay que buscar congruencias de la forma $p \equiv r_1, \ldots, r_l$ mód $4n$ que impliquen $p \mid x^2 + ny^2$, con $mcd(x, y) = 1$.

Trabajando módulo p, $p \mid x^2 + ny^2$ quiere decir $x^2 + ny^2 \equiv 0$ mód p. Pero entonces y no puede ser divisible por p ya que en caso de serlo también lo sería x, lo cual contradice $mcd(x, y) = 1$. Luego, se puede pasar dividiendo por y^2 módulo p, y llegar a

$$\left(\frac{x}{y}\right)^2 \equiv -n \text{ mód } p.$$

De modo que el problema de $p \mid x^2 + ny^2$ es el mismo que si $-n$ es o no un cuadrado módulo p. Para dar una formulación más concreta de este hecho se define el *símbolo de Legendre* para primos impares p: dado un entero a el símbolo de Legendre de a módulo p es

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

Reformulando:

Lema 1.0.1. *Sea n un entero no nulo, y sea p un primo impar que no divide a n. Entonces*

$$p \mid x^2 + ny^2, mcd(x, y) = 1 \Longleftrightarrow \left(\frac{-n}{p}\right) = 1.$$

Sin embargo, con este lema no se puede dar por concluida la búsqueda de una relación que emparente a p y a n. Ya que aunque este lema establece una relación entre ambos, la misma es de n respecto a p y lo que se busca es una relación recíproca a esa, es decir de p respecto a n. Aquí es donde aparece la *reciprocidad cuadrática*, dando una formulación precisa de cómo se "da vuelta" el símbolo de Legendre:

Ley de reciprocidad cuadrática. *Si p y q son primos impares, entonces*

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right).$$

La demostración de esta ley se hará en la segunda parte como corolario de una formulación más general, aunque también es cierto que puede probarse de forma elemental y aparece en muchos textos introductorios de teoría de números (por ejemplo en el libro de Stein [18], Capítulo 6, Sección 6.3 de la versión libre).

De todas formas, así como está escrita la ley de reciprocidad cuadrática no se puede utilizar para dar vuelta $(-n/p)$ cuando n es compuesto.

Para resolver este inconveniente se utiliza la *propiedad multiplicativa* del símbolo de Legendre $(\cdot/p)$ (para ver una prueba de esto mirar en el mismo [18], Capítulo 6, página 58). Es decir, si $n = q_1 \dots q_l$ es la descomposición en primos de n (donde es posible que haya factores repetidos), entonces

$$\left(\frac{n}{p}\right) = \left(\frac{q_1}{p}\right)\dots\left(\frac{q_l}{p}\right).$$

Si todos los $q_i's$ fueran impares, se puede utilizar la ley de reciprocidad cuadrática en cada uno de los factores de la derecha y cambiar su producto por algo de la forma

$$(-1)^{(q_1-1)(p-1)/4}\left(\frac{p}{q_1}\right)\dots(-1)^{(q_l-1)(p-1)/4}\left(\frac{p}{q_l}\right).$$

Agrupando términos

$$\prod_{i=1}^{l}(-1)^{(q_i-1)(p-1)/4}\cdot\prod_{i=1}^{l}\left(\frac{p}{q_i}\right).$$

Así, surge naturalmente la necesidad de extender la definición del símbolo de Legendre al *símbolo de Jacobi* para números positivos compuestos impares, de modo que

$$\prod_{i=1}^{l}\left(\frac{p}{q_i}\right) = \left(\frac{p}{n}\right).$$

Es decir, el símbolo de Jacobi se define (de forma inequívoca) para que la operación $(p/\cdot)$ también sea multiplicativa.

Por otra parte, es una cuenta ver que

$$\prod_{i=1}^{l}(-1)^{(q_i-1)(p-1)/4} = (-1)^{(n-1)(p-1)/4}$$

y en conclusión

$$\left(\frac{n}{p}\right) = (-1)^{(n-1)(p-1)/4}\left(\frac{p}{n}\right). \tag{1.0.2}$$

Resta ver qué pasa cuando n tiene factores pares y luego para "dar vuelta" el $-n$ también hay que saber cómo se comporta el -1 módulo p. Para esto se utilizan las *leyes suplementarias* a la ley de reciprocidad cuadrática, que afirman

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

(la demostración de estas leyes suplementarias se hacen en el libro de Stein [18] conjuntamente con la ley de reciprocidad cuadrática).

De este modo, la reciprocidad cuadrática se puede enunciar de manera uniforme con la siguiente expresión: si $p \equiv q$ mód $4n$ son primos impares entonces

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

y lo mismo se podría decir para $-n$. El factor impar de n se resuelve usando (1.0.2), los factores pares con la ley suplementaria para 2 (y el -1 con la otra ley suplementaria en el caso de $-n$); la multiplicatividad junta las partes.

O sea que lo que, afirma la reciprocidad cuadrática, en definitiva, es que el símbolo (n/p) (o $(-n/p)$) no sólo es un homomorfismo módulo p sino que también lo es módulo n o mejor dicho $4n$. En particular, la reciprocidad cuadrática traduce el problema $(-n/p) = 1$ a congruencias en el sentido de (1.0.1): donde los restos $r_1, \ldots, r_s$ buscados quedan definidos por el núcleo del homomorfismo $(-n/\cdot)$.

Formalizando:

Teorema 1.0.2. *Si n es un entero positivo, entonces hay un único homomorfismo $\chi : (\mathbb{Z}/4n\mathbb{Z})^\times \to \{\pm 1\}$ tal que $\chi([p]) = (-n/p)$ para todo primo p que no divide a $4n$.*

Demostración. La idea es definir $\chi([m]) = (-n/m)$ siendo $(-n/m)$ el símbolo de Jacobi. Si esta definición puede hacerse para todas las clases del cociente $(\mathbb{Z}/4n\mathbb{Z})^\times$, la discusión anterior mostraría que χ es en efecto un homomorfismo y por la propia construcción del símbolo de Jacobi, sería además el único que cumple $\chi([p]) = (-n/p)$ para todo primo p que no divide a $4n$. De modo que sólo queda ver que toda clase de $(\mathbb{Z}/4n\mathbb{Z})^\times$ tiene un representante para el cual se pueda definir el símbolo de Jacobi, es decir un representante positivo impar. Pero esto es inmediato a partir de que todo elemento coprimo con $4n$ es impar. □

En suma, el teorema anterior puede entenderse como la ley de reciprocidad cuadrática en su contexto más general y de hecho es equivalente a dicha ley y sus leyes complementarias (una prueba guiada de esto puede hacerse con el Ejercicio 1.13 del libro de Cox [2]). Además tiene como agregado la formulación que se buscaba al principio de esta sección:

Corolario 1.0.3. *Sea n un entero no nulo, y sea $\chi : (\mathbb{Z}/4n\mathbb{Z})^\times \to \{\pm 1\}$ el homomorfismo del teorema anterior. Si p es un primo que no divide a $4n$, entonces son equivalentes:*

I. $p \mid x^2 + ny^2, mcd(x, y) = 1.$

II. $\left(\frac{-n}{p}\right) = 1.$

III. $[p] \in \ker(\chi).$

Capítulo 2

Formas cuadráticas

La teoría de formas cuadráticas se usa en este problema para clasificar los divisores de $x^2 + ny^2$. Esto significa un enfoque nuevo del *paso de descenso*.

De cualquier manera, el problema $p = x^2 + ny^2$, puede ser visto como un problema intrínseco a las formas cuadráticas cuando se lo mira como un problema de representación. Es decir en este contexto, el problema tiene una formulación propia

Fijado un entero positivo n, ¿qué primos puede representar la forma cuadrática $x^2 + ny^2$?

2.1. Formas cuadráticas enteras

Una *forma cuadrática entera* es una función

$$f(x, y) = ax^2 + bxy + cy^2$$

donde los coeficientes a, b, c y las variables x, y son enteros. Se dice además que la forma es *primitiva* si dichos coeficientes son coprimos.

En el contexto en el que se está trabajando lo que más va interesar de una forma cuadrática son los valores que representa: se dice que un número entero m *es representado* por la forma $f(x, y)$ si existen x e y enteros tales que $f(x, y) = m$. Si además esos x e y son relativamente primos, entonces se dice que m es *propiamente representado* $f(x, y)$. Una cuenta rápida muestra que los números primos sólo se pueden representar propiamente.

El otro elemento importante de una forma cuadrática es el *discriminante*, que está definido por $D := b^2 - 4ac$ si la forma es $f(x, y) = ax^2 + bxy + cy^2$. Un hecho notable es que los discriminantes D son cuadrados módulo 4 y por tanto $D \equiv 0, 1 \text{ mód } 4$.

En esencia, el discriminante es el que define la representación de una forma:

Lema 2.1.1. *Sea $D \equiv 0, 1 \bmod 4$ y sea m un entero impar coprimo con D. Entonces m es representado propiamente por alguna forma primitiva de discriminante D si y sólo si D es un cuadrado módulo m.*

La vaguedad de este resultado cuando no dice nada sobre la forma que representaría a m se debe, en parte, a que la representación de formas sólo se puede describir en términos de *equivalencias*. Una forma $f(x, y)$ es *equivalente* a otra $g(x, y)$ si existe una matriz $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in GL_2(\mathbb{Z})$ tal que

$$f\left(\begin{pmatrix} p & q \\ r & s \end{pmatrix}(x, y)^t\right) = f(px + qy, rx + sy) = g(x, y),$$

y es *propiamente equivalente* si $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$. Los nombres de "equivalencia" están porque en efecto ambas relaciones son de equivalencia.

Pero lo más importante de estas relaciones es que preservan los enteros representados y los discriminantes. También hay una suerte de recíproco de este hecho:

Lema 2.1.2. *Una forma $f(x, y)$ representa propiamente a un entero m si y sólo si es propiamente equivalente a una forma del tipo $mx^2 + bxy + cy^2$ con b y c enteros.*

Demostración. Primero supóngase que $f(p, q) = m$ con p y q coprimos. Luego existen enteros r y s tales que $ps - qr = 1$. Así $f(x, y)$ es equivalente a

$$f(px + ry, qx + sy) = f(p, q)x^2 + bxy + cy^2 = mx^2 + bxy + cy^2.$$

El recíproco es directo a partir de la igualdad anterior tomando $(x, y) = (1, 0)$. □

Y esto a su vez permite demostrar el lema que había quedado pendiente:

Demostración del Lema 2.1.1. Por el lema anterior si $f(x, y)$ es una forma de discriminante D que representa propiamente a m entonces puede considerarse que $f(x, y) = mx^2 + bxy + y^2$ pues formas equivalentes tienen el mismo discriminante. Luego $D = b^2 - 4mc$ y el resultado se sigue inmediatamente.

Recíprocamente si $D \equiv b^2 \bmod m$, entonces se puede considerar que D y b tienen la misma paridad dado que m es impar (y entonces eventualmente b se puede cambiar por $b + m$ que tiene otra paridad). Más aún como $D \equiv 0, 1 \bmod 4$ entonces $D \equiv b^2 \bmod 4m$. Luego $D = b^2 - 4mc$ y así la forma $f(x, y) = mx^2 + bxy + cy^2$ tiene discriminante D y representa propiamente a m. □

La condición "D es un cuadrado módulo m" hace recordar a los resultados de la reciprocidad cuadrática, el Corolario 1.0.3 y el Teorema 1.0.2. De hecho, el homomorfismo χ de ese teorema también se puede definir para enteros $D \equiv 1$ mód 4 de igual manera. Es decir, para cada discriminante D existe un único homomorfismo $\chi : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ tal que $\chi([p]) = (D/p)$ para todo primo p que divide a D (la prueba de esto es igual a la hecha en el capítulo anterior). Así, combinando con el Lema 2.1.1 con los resultados de reciprocidad cuadrática, se ha demostrado el siguiente teorema:

Teorema 2.1.3. *Sea $D \equiv 0, 1$ mód 4 y sea $\chi : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ el homomorfismo del Teorema 1.0.2. Si p es un primo que no divide a D, entonces p es representado por una forma cuadrática primitiva de discriminante D si y sólo si $[p] \in \ker(\chi)$.*

Visto de este modo el problema $p = x^2 + ny^2$ no es otra cosa que un problema de representación de formas para un discriminante dado. Es decir, la misma pregunta se puede formular para formas con otros discriminantes, porque la teoría desarrollada hasta ahora (y la que se desarrollará después) no hace una distinción especial entre los discriminantes pares o impares.

De cualquier manera, volviendo al caso $D = -4n$ el teorema anterior ofrece el siguiente corolario:

Corolario 2.1.4. *Sea n un entero y sea p un primo que no divide a $4n$. Entonces p es representado por una forma primitiva de discriminante $-4n$ si y sólo si $p \mid x^2 + ny^2$.*

Demostración. Se sigue inmediatamente del teorema anterior y del Corolario 1.0.3. □

Así que la condición $p \mid x^2 + ny^2$ del paso de descenso implica que p es representado una forma de discriminante $-4n$. Pero, en principio, podría haber otras formas cuadráticas de discriminante $-4n$ distintas de $x^2 + ny^2$, por ejemplo cuando $n = 3$ se ve que $(-3/13) = 1$ y que $13x^2 + 12xy + 3y^2$ es una forma que representa a 13. Por esto, es necesario reducir la cantidad de formas cuadráticas, mostrando que cada una de ellas es equivalente a una especialmente simple.

Sin embargo para poder hacer esta reducción hay que restringirse a las formas cuadráticas que son definidas y en particular las que son definidas positivas, dado que hay que incluir a la forma $x^2 + ny^2$. Dentro de estas formas, las reducidas serán aquellas primitivas $ax^2 + bxy + cy^2$ tales que

$$|b| \leq a \leq c \text{ y además } b \geq 0 \text{ en los casos que } |b| = a \text{ o } a = c.$$

Es importante observar que la forma $x^2 + ny^2$ es en efecto una forma reducida.

Lo notable de las formas reducidas es que son suficientes para describir todas las formas (definidas positivas) a menos de equivalencias propias:

Teorema 2.1.5. *Toda forma definida positiva es propiamente equivalente a una única forma reducida.*

Demostración. Una prueba de esto puede leerse en [18], Capítulo 9, Sección 9.3. □

Las restricciones de las formas reducidas fuerzan a que sólo haya una cantidad finita de ellas: si $ax^2+bxy+cy^2$ es una forma reducida de discriminante D, entonces $b^2 \leq a^2$ y $a \leq c$ y por tanto

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

por lo que

$$a \leq \sqrt{-D/3}.$$

Luego sólo hay finitos valores posibles para a y como $|b| \leq a$ también para b, y como $D = b^2 - 4ac$ es fijo también para c.

La cantidad de clases de formas primitivas definidas positivas de discriminante D es denotada por $h(D)$. En suma:

Corolario 2.1.6. *Sea $D < 0$ un discriminante fijo. Entonces el número $h(D)$ es finito, y más aún es igual al número de formas reducidas de discriminante D.*

El algoritmo anterior permite construir una tabla de formas para distintos discriminantes. En particular es útil para saber cuántas y qué formas hay de discriminante $-4n$ para distintos valores de n:

n	$h(-4n)$	Formas primitivas reducidas de discriminante $-4n$
1	1	x^2+y^2
2	1	x^2+2y^2
3	1	x^2+3y^2
4	1	x^2+4y^2
5	2	$x^2+5y^2, 2x^2+2xy+3y^2$
6	2	$x^2+6y^2, 2x^2+3y^2$
7	1	x^2+7y^2
14	4	$x^2+14y^2, 2x^2+7y^2, 3x^2 \pm 2xy+5y^2$
26	6	$x^2+26y^2, 2x^2+13y^2, 3x^2 \pm 2xy+9y^2, 5x^2 \pm 4xy+6y^2$
27	3	$x^2+27y^2, 4x^2 \pm 2xy+7y^2$

O sea que, aunque se reduzcan las posibilidades a un número finito de formas que pueden tener discriminante como el de x^2+ny^2, no necesariamente esta cantidad tiene que ser 1. Y de hecho, los n de la tabla para los cuales $h(-4n)=1$ son los únicos que cumplen con eso:

Teorema 2.1.7. *Sea n un entero positivo. Entonces*

$$h(-4n) = 1 \iff n = 1, 2, 3, 4 \text{ o } 7.$$

Demostración. La idea de la prueba es mostrar que cuando $n \notin \{1, 2, 3, 4, 7\}$ entonces se puede construir una forma reducida distinta de $x^2 + ny^2$ pero con el mismo discriminante, por lo que $h(-4n) > 1$.

Primero supóngase que n no es una potencia de un primo, es decir que puede escribirse de la forma $n = ac$ donde $1 < a < c$ y a y c son coprimos. Luego la forma

$$ax^2 + cy^2$$

tiene discriminante $-4ac = -4n$ y es reducida.

Si n es potencia de un primo, pueden pasar dos cosas, que n sea una potencia de 2 o que sea la potencia de un primo impar. Si $n = 2^r$ con $r \geq 4$ entonces la forma

$$4x^2 + 4xy + (2^{r-2} + 1)y^2$$

tiene discriminante $4^2 - 4(4(2^{r-2} + 1)) = 4^2 - 4 \cdot 2^r - 4^2 = -4 \cdot 2^r = -4n$. Pero además esta forma es reducida ya que $4 \leq 2^{r-2} + 1$. Para $n = 8$ está la forma

$$3x^2 + 2xy + 3y^2$$

que es reducida con discriminante $-32 = -4 \cdot 8$.

Cuando $n = p^r$ con p primo impar y $n + 1$ puede ser escrito de la forma $n + 1 = ac$ con $2 \leq a < c$ y a y c coprimos, entonces la forma

$$ax^2 + 2xy + c^2$$

tiene discriminante $2^2 - 4(n + 1) = -4n$ y es reducida.

Por lo que sólo queda el caso en el que $n = p^r$ y $n+1$ es una potencia de un primo. Pero como p es impar sólo puede ser $n+1 = 2^s$. Si $s \geq 6$ entonces

$$8x^2 + 6xy + (2^{s-3} + 1)y^2$$

es una forma reducida ya que $8 \leq 2^{s-3} + 1$. Y más aún tiene discriminante $6^2 - 4 \cdot 8(2^{s-3} + 1) = 4 - 4 \cdot 2^s = 4 - 4(n + 1) = -4n$. Los casos para $s = 1, 2, 3, 4$ y 5 corresponden a $n = 1, 3, 7, 15$ y 31 respectivamente. Ahora $n = 15$ no es posible porque ni siquiera es una potencia de un primo, y para $n = 31$ está la forma primitiva y reducida

$$5x^2 + 4xy + 7y^2$$

con discriminante $16 - 4 \cdot 5 \cdot 7 = -124 = -4 \cdot 31$. □

Luego con el Corolario 2.1.4 sólo se puede añadir un teorema más a los tres probados en el principio de esta parte, y es para $n = 7$. (El caso de $p = x^2 + 4y^2$ se omitió porque es el mismo que $p = x^2 + y^2$: si p es impar se puede considerar y par y luego factorizando queda $p = x^2 + 4y'^2$).

2.1.1. Ejemplo $p = x^2 + 7y^2$

Por el Corolario 2.1.4 y como $h(-4 \cdot 7) = 1$, los primos p no divisores de 28 que se pueden escribir de la forma $p = x^2 + 7y^2$ son exactamente aquellos tales que $(-7/p) = 1$. Usando la reciprocidad cuadrática

$$\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = (-1)^{p-1/2}(-1)^{(p-1)(7-1)/4}\left(\frac{p}{7}\right) = \left(\frac{p}{7}\right).$$

Los restos módulo 7 que caraterizan la condición $(p/7) = 1$ son $1, 2$ y 4. Al pasar módulo 28, los candidatos a elementos del núcleo del homomorfismo de reciprocidad χ del Teorema 1.0.2 son

$$1, 2, 4, 1 + 7 = 8, 2 + 7 = 9, 4 + 7 = 11, 1 + 7 \cdot 2 = 15, 2 + 7 \cdot 2 = 16,$$
$$4 + 7 \cdot 2 = 18, 1 + 7 \cdot 3 = 22, 2 + 7 \cdot 3 = 23, 4 + 7 \cdot 3 = 25.$$

Pero χ se restringe a los invertibles módulo 28, o sea que de la lista anterior sólo quedan

$$1, 9, 11, 15, 23, 25.$$

En consecuencia si p es un primo que no divide a 28 (estos son 2 y 7) se tiene que

$$p = x^2 + 7y^2 \iff p \equiv 1, 9, 11, 15, 23, 25 \text{ mód } 28.$$

Sobre los primos divisores de 28, el 2 no es de la forma $x^2 + 7y^2$ mientras que el 7 obviamente sí.

2.1.2. Consideraciones sobre discriminantes impares

Por otra parte, mirando de nuevo el problema como un problema de representación de formas, también tiene sentido preguntarse a partir del resultado anterior, si es posible decir lo mismo sobre discriminantes negativos pero impares, es decir si los discriminantes negativos impares para los cuales hay una sola forma reducida, no son más que una cantidad finita. La respuesta es también afirmativa y de hecho se sabe cuáles son todos ellos: -3, -7, -11, -19, -27, -43, -67, -163 (una prueba de esto puede encontrarse en [2], Sección 12, página 271). A partir de esto también se pueden enunciar resultados del tipo

$$\begin{aligned} p \equiv 1 \text{ mód } 3 &\iff p = x^2 + xy + y^2 \\ p \equiv 1, 2, 4 \text{ mód } 7 &\iff p = x^2 + xy + 2y^2 \\ p \equiv 1, 3, 4, 5, 7 \text{ mód } 11 &\iff p = x^2 + xy + 3y^2 \\ p \equiv 1, 4, 5, 6, 7, 9, 11, 16, 17 \text{ mód } 19 &\iff p = x^2 + xy + 5y^2. \end{aligned}$$

2.2. Teoría elemental de géneros

Una consecuencia inmediata del Teorema 2.1.7 es que no se puede seguir avanzado sólo con resultados como el Teorema 2.1.3. Por ejemplo cuando $n = 5$ la teoría desarrollada hasta ahora apenas dice que

$$p \equiv 1, 3, 7, 9 \text{ mód } 20 \iff \left(\frac{-5}{p}\right) = 1 \iff p = \begin{cases} x^2 + 5y^2 \\ \text{o} \\ 2x^2 + 2xy + 3y^2 \end{cases}$$

lo cual no decide cuando $p = x^2 + 5y^2$.

De modo que es preciso encontrar una manera de distinguir las formas de discriminante $-4n$ y poder separar así la forma $x^2 + ny^2$ de las demás. Para esto se utiliza la *teoría de géneros*.

Se dice que dos formas primitivas definidas positivas de discriminante D *están en el mismo género* si representan el mismo conjunto de valores invertibles módulo D. En particular como dos formas equivalentes representan los mismos enteros, entonces también son del mismo género. Y como hay un número finito de clases, cada *género* tiene una cantidad finita de clases. Por ejemplo, cuando $D = -4 \cdot 5 = -20$ hay dos géneros, cada uno de ellos con una clase:

$$\begin{array}{cc} x^2 + 5y^2 & \text{representa } 1, 9 \text{ en } (\mathbb{Z}/20\mathbb{Z})^\times \\ 2x^2 + 2xy + 3y^2 & \text{representa } 3, 7 \text{ en } (\mathbb{Z}/20\mathbb{Z})^\times. \end{array}$$

Una observación interesante en este caso es que los conjuntos representados por cada uno de los géneros son disjuntos. En realidad, como se verá más adelante, este no es un hecho aislado sino que responde a una regla general: a géneros distintos corresponden conjuntos disjuntos de valores representados (módulo D).

Pero para ver el verdadero aporte que hace esta teoría al problema $p = x^2 + ny^2$ hay que combinarla con el Teorema 2.1.3. Este acoplamiento permite refinar las congruencias para cuando hay más de una forma por discriminante. Concretamente, en el caso tomado como referencia de $D = -20$ se obtiene que

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

O sea que la idea es encontrar congruencias que caractericen al género donde se encuentra la forma $x^2 + ny^2$. Este género es llamado el *género principal* por ser el género de la forma

$$x^2 + ny^2 = x^2 - \frac{D}{n}y^2$$

que es la *forma principal* de discriminante $D = -4n$.

Y se aclara el discriminante, porque como antes esta teoría también puede hacerse del mismo modo en discriminantes D impares. Aquí la forma principal es

$$x^2 + xy + \frac{1-D}{4}y^2.$$

La caracterización del género principal se hace con la siguiente extensión del Teorema 2.1.3:

Teorema 2.2.1. *Dado un entero negativo $D \equiv 0, 1 \bmod 4$, sea el núcleo $\ker(\chi) \subset (\mathbb{Z}/D\mathbb{Z})^\times$ como en el Teorema 1.0.2, y sea H el conjunto de los valores que representa la forma principal de discriminante D. Si p es un primo impar que no divide a D, entonces p es representado por una forma reducida de discriminante D del género principal si y sólo si $[p] \in H$.*

Antes hay que demostrar el siguiente lema:

Lema 2.2.2. *Sea un entero negativo $D \equiv 0, 1 \bmod 4$, y sea $H \subset \ker(\chi)$ como en el Teorema 2.2.1. Sea además $f(x, y)$ una forma de discriminante D. Entonces:*

I. *los valores en $(\mathbb{Z}/D\mathbb{Z})^\times$ representados por la forma principal de discriminante D forman un subgrupo $H \subset \ker(\chi)$,*

II. *los valores en $(\mathbb{Z}/D\mathbb{Z})^\times$ representados por $f(x, y)$ forman una coclase de H en $\ker(\chi)$.*

Demostración. En realidad, en general, todo valor representado por una forma de discriminante D está en el núcleo de χ. Esto es debido al Teorema 2.1.3 que asegura el caso para los que son propiamente representados y a que todo valor m coprimo a D que es representado por una forma de ese discriminante puede ser escrito como d^2m' donde m' es propiamente representado. En suma como χ es un homomorfismo

$$\chi([m]) = \chi([d^2])\chi([m']) = \chi([d])^2 = 1.$$

Luego, en particular, H es un subconjunto de $\ker(\chi)$. Más aún es un subgrupo. Cuando $D = -4n$ esto se ve con la identidad de (0.0.3). Y cuando $D \equiv 1 \bmod 4$ la congruencia

$$4\left(x^2 + xy + \frac{1-D}{4}y^2\right) \equiv (2x + y)^2 \bmod D,$$

muestra que H es el subgrupo de los cuadrados módulo D.

Para probar el segundo se usa la siguiente igualdad: si la forma es $f(x, y) = ax^2 + bxy + cy^2$ entonces

$$4af(x, y) = (2ax + by)^2 - Dy^2. \tag{2.2.1}$$

Luego la idea es "invertir" de alguna manera el factor $4a$ módulo D para concluir que los valores tomados por $f(x, y)$ módulo D están en una coclase de H.

Cuando $D = -4n$ se puede dividir entre 4 a ambos lados de (2.2.1), dado que además b tiene que ser par o sea de la forma $2b'$, y obtener

$$af(x, y) = (ax + b'y)^2 + ny^2.$$

Y cuando $D \equiv 1$ mód 4 el 4 es invertible módulo D. Resta ver qué pasa con a, para esto se usa la siguiente observación:

Lema 2.2.3. *Dada una forma primitiva $f(x, y)$ y un entero M, entonces $f(x, y)$ representa números relativamente primos a M.*

Con ese resultado tomando $M = D$ se puede considerar, gracias al Lema 2.1.2, que a es coprimo con D y por eso se puede invertir módulo D. Luego si $D = -4n$ la cuenta hecha antes muestra que los valores de $f(x, y)$ caen en $[a]^{-1}H$. Recíprocamente si $[c] \in [a]^{-1}H$ entonces $ac \equiv z^2 + nw^2$ mód $4n$ para ciertos enteros z, w. Usando (2.2.1) dividida por 4 y recordando la igualdad (0.0.3) se consigue una solución a $f(x, y) \equiv c$ mód $4n$. Así $[a]^{-1}H$ consiste exactamente de los valores representados en $(\mathbb{Z}/D\mathbb{Z})^\times$ por $f(x, y)$.

En el caso $D \equiv 1$ mód 4, multiplicando a izquierda por el inverso de $4a$ en (2.2.1) se obtiene

$$f(x, y) \equiv (4a)^{-1}(2ax + by)^2 \text{ mód } D$$

que está en $[4a]^{-1}H$ por lo antes visto. Si $[c] \in [4a]^{-1}H$ entonces

$$c \equiv (4a)^{-1}\left(x^2 + xy + \frac{1 - D}{4}y^2\right) \equiv (4a)^{-1}(2x + y)^2 \text{ mód } D$$

y $f(x, y) \equiv c$ mód D tiene solución. Por lo que $[4a]^{-1}H$ es el conjunto de valores representado por $f(x, y)$ módulo D. □

Demostración del Lema 2.2.3. Dado un primo p, alguno de los tres valores de $f(1, 0)$, $f(1, 1)$ y $f(0, 1)$ tiene que ser coprimo con p porque la forma $f(x, y) = ax^2 + bxy + cy^2$ es primitiva y entonces $mcd(a, a + b + c, c) = 1$.

Luego si $p_1, \ldots, p_r$ son los primos que dividen a M y $v_1, \ldots, v_r$ son los respectivos vectores que hacen a $f(v_i)$ coprimo con p_i, por el Teorema Chino de los restos (para una demostración del Teorema mirar la Sección 3.4 del Capítulo 3 del libro de Stein [18]) se puede encontrar un vector de coordenadas enteras v tal que $f(v)$ sea relativamente primo con M. □

A la vista de que los valores de $\ker(\chi)$ son exactamente los representados por las formas de discriminante D y usando el segundo punto del lema, se puede reformular el mismo segundo punto de la siguiente manera: *"las coclases de H en $\ker(\chi)$ son los valores en $(\mathbb{Z}/D\mathbb{Z})^\times$ representados por*

una forma $f(x, y)$ de discriminante D". Y como las coclases particionan el núcleo, si $[p] \in \ker(\chi)$ entonces $[p]$ tiene que estar en una y sólo una coclase. En particular si $[p] \in H$ entonces necesariamente p es representado por una forma del género principal, y el Teorema 2.2.1 se sigue inmediatamente. Más aún dada una coclase cualquiera H', definiendo *género* de H' como todas las formas de discriminante D que representan valores de H' módulo D, se puede extender el Teorema 2.2.1 a otras coclases de la siguiente forma *"si p es un primo impar que no divide a D, entonces p es representado por una forma reducida de discriminante D en el género de H' si y sólo si $[p] \in H'$"*.

Volviendo al género principal y al caso $x^2 + ny^2$, donde $D = -4n$, el Teorema 2.2.1 ofrece congruencias explícitas:

Corolario 2.2.4. *Sea n un entero positivo y sea p un primo impar que no divide a n. Entonces p es representado por una forma de discriminante $-4n$ en el género de la forma principal si y sólo si para cierto entero β*

$$p \equiv \beta^2 \ \ o \ \beta^2 + n \text{ mód } 4n.$$

Demostración. Los valores que representa la forma principal x^2+ny^2 son por un lado cuadrados módulo $4n$ (cuando y es par), y por otro los cuadrados más n módulo $4n$ (cuando y es impar). El resto se sigue del Teorema 2.2.1. □

Y en el mejor de los casos, cuando el género principal consta solamente de la forma principal, el corolario anterior da congruencias que resuelven $p = x^2 + ny^2$. Esto sucede para $n = 5$, pero también por ejemplo para $n = 6$.

2.2.1. Ejemplo $p = x^2 + 6y^2$

Para empezar hay que ver cuáles son las congruencias que caracterizan a las formas de discrimintante -24. Esto, como antes gracias al Corolario 2.1.4, se hace con el núcleo del homomorfismo χ del Teorema 1.0.2: es decir los primos p que no dividen a 24 y son representados por una forma reducida de discriminante -24 están caracterizados por la condición $(-6/p) = 1$. Usando la reciprocidad cuadrática

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{p-1/2}(-1)^{p^2-1/8}(-1)^{(p-1)(3-1)/4}\left(\frac{p}{3}\right)$$
$$= (-1)^{p^2-1/8}\left(\frac{p}{3}\right).$$

De este modo los p que cumplen $(-6/p) = 1$ tienen que verificar

$$\begin{cases} p \equiv 1, 7 \text{ mód } 8 \\ p \equiv 1 \text{ mód } 3 \end{cases}$$

en el caso que ambos factores sean 1, o

$$\begin{cases} p \equiv 3, 5 \text{ mód } 8 \\ p \equiv 2 \text{ mód } 3 \end{cases}$$

si ambos son -1. Usando el Teorema chino de los restos esto es equivalente a

$$\begin{array}{ll} p \equiv 1, 7 \text{ mód } 24 & \text{en el primer caso} \\ p \equiv 5, 11 \text{ mód } 24 & \text{en el segundo.} \end{array}$$

O sea que los primos no divisores de 24 que son representados por una forma de discriminante -24 tienen que cumplir $p \equiv 1, 5, 7, 11$ mód 24.

Ahora, hay sólo $h(-4 \cdot 6) = 2$ formas reducidas de discriminante -24:

$$\begin{array}{c} x^2 + 6y^2 \\ 2x^2 + 3y^2. \end{array}$$

La forma principal $x^2 + 6y^2$ es la que representa al 1 y al 7 módulo 24. Por otra parte el conjunto de valores invertibles módulo 24 representados por la forma principal tiene que tener tamaño 2 porque particiona en 2 coclases (correspondientes a las dos formas) al grupo $(\mathbb{Z}/24\mathbb{Z})^\times$ (Lema 2.2.3) que tiene orden 4. O sea que el conjunto los valores 1 y 13 son todos los invertibles módulo 24 que representa la forma $x^2 + 6y^2$.

Sobre los divisores primos de 24, 2 y 3, está claro que no pueden ser representados por $x^2 + 6y^2$. En suma

$$p = x^2 + 6y^2 \iff p \equiv 1, 7 \text{ mód } 24$$

para todo primo p.

Pero bien, ¿cuántos teoremas más de este tipo se pueden obtener con esta teoría?, es decir ¿para cuántos n el género principal de las formas de discriminante $-4n$ tiene una sola forma? Desde luego no funciona para todos los casos: cuando $n = 14$, el género principal tiene dos formas y entonces la teoría de géneros sólo dice que

$$p = \begin{cases} x^2 + 14y^2 \\ \text{o} \\ 2x^2 + 7y^2 \end{cases} \iff p \equiv 1, 9, 15, 23, 25, 39 \text{ mód } 56.$$

Mas tampoco es cierto para infinitos casos. De hecho se sabe que sólo es cierto para: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848 y eventualmente un número más (secuencia A000926 en OEIS [17]).

Se necesita algo más para resolver el problema $p = x^2 + ny^2$. Nuevas teorías. Nuevas formas de entender la reciprocidad cuadrática y las formas cuadráticas.

Parte II

Teoría de números algebraicos y teoría de cuerpos de clases

"Esencialmente, el álgebra y el dinero determinan las clases, la primera a nivel intelectual, el segundo a nivel práctico". Simone Weil.

La idea madre de esta parte es la siguiente: supóngase que $p = x^2 + ny^2$. Luego, en cierto contexto, p se podría factorizar como

$$(x + \sqrt{-n}y)(x - \sqrt{-n}y).$$

Ahora, este entorno obviamente se sale de los enteros, y a veces ni siquiera se puede inscribir en un dominio factorial. Esto requiere definir nuevas estructuras como lo son los *dominios de Dedekind*, donde también se habla de factorización pero al nivel de ideales.

Sin embargo, aún habiendo comprendido estos nuevos dominios, a priori nada asegura que un primo p descomponga en ellos. Y aunque lo haga, tampoco se puede afirmar $p = x^2 + ny^2$ porque en los dominios de Dedekind la factorización es con ideales y en principio estos no tienen por qué ser todos principales. Para responder estas preguntas se trabaja con los cuerpos de la forma $\mathbb{Q}(\sqrt{-n})$, utilizando esencialmente *teoría de Galois* a través, primero de la *teoría de números algebraicos* y después de la *teoría de cuerpos de clases*.

Como primera conclusión de esta parte se prueba la siguiente versión del Teorema principal 1:

Teorema 2. *Sea $n \not\equiv 3 \bmod 4$ libre de cuadrados. Entonces existe un polinomio entero mónico irreducible $f_n(x)$ tal que si p es un primo que no divide ni a $4n$ ni al discriminante de $f_n(x)$ se cumple que*

$$p = x^2 + ny^2 \iff \begin{cases} \left(\frac{-n}{p}\right) = 1 \ y \\ f_n(x) \equiv 0 \bmod p \text{ tiene solución entera.} \end{cases}$$

Pero este teorema no puede considerarse del todo satisfactorio para responder la pregunta $p = x^2 + ny^2$, ya que las condiciones de ser libres de cuadrados y $n \not\equiv 3 \bmod 4$ dejan muchos casos de n sin contestar. Esto en realidad no presenta una dificultad una vez probado el Teorema 2, y haciendo las adaptaciones correspondientes, se puede probar el Teorema 1 para cualquier n.

Por otra parte, este teorema generaliza los resultados probados en la primera parte en el sentido que a la condición $(-n/p) = 1$, que en la primera parte quiere decir que p es representado por alguna de forma de discriminante $-4n$, se la refina por otra congruencia módulo p, $f_n(x) \equiv 0 \bmod p$ que de alguna manera distingue exactamente a la forma $x^2 + ny^2$ de las demás cuando esta última congruencia tiene solución. Y esta "generalización conceptual" se traduce de manera explícita a una correspondencia entre ideales de cuerpos cuadráticos y formas cuadráticas como se ve en el último capítulo.

Capítulo 3

Teoría de números algebraicos

Antes de trabajar directamente con los cuerpos $\mathbb{Q}(\sqrt{-n})$, es necesario entender las generalidades de los cuerpos que tienen grado finito sobre $\mathbb{Q}$ y luego ver cómo se aplican estos resultados sobre los cuerpos que tiene grado 2. Este estudio se hace con la *teoría de números algebraicos*.

Los resultados de este capítulo son a su vez básicos e imprescindibles en el desarrollo de esta teoría, pero sin embargo muchos de ellos no guardan una relación directa en la solución del problema $p = x^2 + ny^2$ y demostrarlos supondría desviar el foco del objetivo. Por este motivo la mayoría de las pruebas son omitidas con su respectiva referencia (una buena lectura sobre estos temas se puede hacer con el libro *Number Fields* [15] de Marcus).

3.1. Cuerpos de números

Un *cuerpo de números* K es un subcuerpo de los complejos $\mathbb{C}$ que tiene grado finito sobre $\mathbb{Q}$. Luego la forma de estos cuerpos K viene dada por el Teorema del elemento primitivo, que implica $K = \mathbb{Q}(\zeta)$ donde ζ es algún complejo algebraico (ver el Teorema 2 del segundo Apéndice [15]).

En estos cuerpos, $\mathcal{O}_K$ denota el conjunto de los *enteros algebraicos*, es decir todos los $\alpha \in K$ que son raíces de un polinomio mónico entero. Obsérvese que cuando $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$. Pero no siempre $\mathcal{O}_K$ es "como $\mathbb{Z}$". Y tampoco siempre pasa que si $K = \mathbb{Q}(\zeta)$ entonces $\mathcal{O}_K = \mathbb{Z}[\zeta]$, aunque sí se van poder establecer resultados similares para cuando $\zeta = \sqrt{N}$ que son las situaciones que se van a estudiar. En cualquier caso, siempre se puede decir que $\mathcal{O}_K$ es un anillo (de hecho es un dominio con cuerpo de fracciones K), y también que es un $\mathbb{Z}$-módulo libre de rango finito (específicamente se prueba que el rango es $[K : \mathbb{Q}]$). (Las referencias del libro de Marcus [15] para las pruebas de estos hechos están en los corolarios de los Teoremas 2 y 9).

Esto último implica que todos los ideales de $\mathcal{O}_K$ son finitamente generados, y más aún que los cocientes $\mathcal{O}_K/\mathfrak{a}$ por ideales no nulos $\mathfrak{a}$, son finitos. Luego, se puede definir la *norma* de un ideal no nulo $\mathfrak{a}$ de $\mathcal{O}_K$ como siendo

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

Y si bien estas condiciones no alcanzan para que $\mathcal{O}_K$ sea un dominio factorial, son suficientes para que sea otro tipo de dominio muy parecido:

Teorema 3.1.1. *Sea K un cuerpo de números. Entonces $\mathcal{O}_K$ es un dominio de Dedekind, es decir:*

I. *$\mathcal{O}_K$ es integralmente cerrado en K, i.e., si $\alpha \in K$ es raíz de un polinomio mónico con coeficientes en $\mathcal{O}_K$ entonces $\alpha \in \mathcal{O}_K$.*

II. *$\mathcal{O}_K$ es Noetheriano, i.e., todo ideal es finitamente generado.*

III. *Todo ideal primo en $\mathcal{O}_K$ es maximal.*

Demostración. Ver Teorema 14 del libro de Marcus [15]. □

Aunque no se pueda hablar de factorización a nivel de los elementos en los dominios de Dedekind, sí se puede hacer al nivel de los ideales:

Corolario 3.1.2. *Todo ideal no nulo $\mathfrak{a}$ de $\mathcal{O}_K$ puede escribirse como producto*

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$$

de ideales primos, y esta factorización es única a menos de reordenaciones.

Demostración. Ver Teorema 16 del libro de Marcus [15]. □

La multiplicación de ideales (no nulos) les da una estructura natural de monoide, pero también va interesar extender la noción de ideal para que estos formen un grupo con la misma operación. Para esto se agregan los *ideales fraccionales* de $\mathcal{O}_K$ que son todos los $\mathcal{O}_K$-submódulos de K finitamente generados.

Así se puede probar que todo ideal fraccional no nulo $\mathfrak{a}$ es invertible, es decir existe otro ideal fraccional $\mathfrak{b}$ tal que $\mathfrak{ab} = \mathcal{O}_K$ (en el Marcus [15] esto está probado en el Teorema 15). Este ideal $\mathfrak{b}$ se denotará $\mathfrak{a}^{-1}$. Con esta notación y usando el Corolario 3.1.2, también se puede hacer factorización para ideales fraccionales:

Corolario 3.1.3. *Todo ideal fraccional no nulo $\mathfrak{a}$ puede escribirse de forma única como producto $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i}$ con $\mathfrak{p}_i$ distintos ideales primos de $\mathcal{O}_K$ y r_i exponentes enteros.*

Demostración. Es inmediato a partir del corolario anterior. □

Este grupo de ideales fraccionales (no nulos) se denota por I_K. El subgrupo más importante de I_K es el de ideales fraccionales *principales* de K, es decir ideales de la forma $\alpha\mathcal{O}_K$ con $\alpha \in K^\times$. Este subgrupo se denota por P_K. El cociente de estos grupos va a tener gran relevancia en la solución del Teorema 2 y se llama el *grupo de clases ideales*, $C(\mathcal{O}_K)$.

La siguiente cuestión a explorar es qué pasa con los primos en las extensiones, un fenómeno que se conoce por *descomposición*. Dada L/K una extensión de cuerpos de números, si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_K$ entonces $\mathfrak{p}\mathcal{O}_L$ será un ideal en $\mathcal{O}_L$ y por tanto tiene que tener una factorización

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$$

en primos de $\mathcal{O}_L$. Se dice que los primos $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ *caen* sobre $\mathfrak{p}$ porque $\mathfrak{P}_\mathfrak{i} \cap \mathcal{O}_K = \mathfrak{p}$, o también debido a que $\mathfrak{p}\mathcal{O}_L \subset \mathfrak{P}_i$ se dice que *contienen* a $\mathfrak{p}$. Los exponentes e_i son llamados los *índices de ramificación* de $\mathfrak{P}_i$ sobre $\mathfrak{p}$, y se denotan $e_{\mathfrak{P}_i|\mathfrak{p}}$. Además cada primo $\mathfrak{P}_i$ da una extensión del cuerpo $\mathcal{O}_K/\mathfrak{p}$, a saber $\mathcal{O}_L/\mathfrak{P}_i$. El grado de esta extensión se llama el *grado de inercia* de $\mathfrak{P}_i$ sobre $\mathfrak{p}$, y se denota $f_{\mathfrak{P}_i|\mathfrak{p}}$.

La relación básica que guardan estos números e_i y f_i con la extensión L/K es la siguiente:

Teorema 3.1.4. *Sean $K \subset L$ cuerpos de números, y sea $\mathfrak{p}$ un primo de K. Si e_i, f_i son los respectivos índices de ramificación y grados internos, entonces*

$$\sum e_i f_i = [L : K].$$

Demostración. Ver Teorema 21 del libro de Marcus [15]. □

En particular, las cosas son mucho más sencillas cuando la extensión es de Galois (como pasará en muchos de los casos estudiados a posteriori) porque todos los primos que caen sobre un primo dado tienen el mismo comportamiento. Lo cual tiene sentido ya que el grupo de Galois actúa transitivamente. Formalizando:

Teorema 3.1.5. *Sea L/K una extensión de Galois entre cuerpos de números, y sea $\mathfrak{p}$ un primo en K.*

I. *El grupo de Galois $Gal(L/K)$ actúa transitivamente sobre los primos de L que contienen a $\mathfrak{p}$, es decir si $\mathfrak{P}$ y $\mathfrak{P}'$ son dos primos de L que contienen a $\mathfrak{p}\mathcal{O}_L$ entonces existe un $\sigma \in Gal(L/K)$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$.*

II. *Todos los primos que contienen a $\mathfrak{p}$, $\mathfrak{P}_1, \dots, \mathfrak{P}_g$, tienen un mismo índice de ramificación e y un mismo grado de inercia f. Por lo que*

$$efg = [L : K].$$

Demostración. Teorema 23 del libro de Marcus [15]. □

A grandes rasgos las descomposiciones de un primo $\mathfrak{p}$ en una extensión de Galois L/K pueden dividirse en dos tipos: *ramificada* cuando $e > 1$ y *no ramificada* si $e = 1$. También si $e = f = 1$ se dice que $\mathfrak{p}$ *descompone completamente* y cuando $e = g = 1$ se dice que el primo permanece *inerte*.

Pero la relación de los primos con el grupo de Galois no termina con este Teorema 3.1.5. Una forma de profundizar este vínculo es entendiendo mejor la acción del grupo de Galois sobre los primos. En este sentido los subgrupos estabilizadores de los primos tienen un rol fundamental.

Si $\mathfrak{P}$ es un primo de L en la extensión L/K, se define el *grupo de descomposición* de $\mathfrak{P}$ como siendo

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

Y este grupo de descomposición se mapea naturalmente en el grupo de Galois de $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$ (una extensión de cuerpos finitos siempre es Galois, como se muestra en el primer Apéndice del libro de Marcus [15]), siendo $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Es decir $\sigma \in D_{\mathfrak{P}}$ induce un automorfismo de $\mathcal{O}_L/\mathfrak{P}$ que es la identidad en $\mathcal{O}_K/\mathfrak{p}$. Este mapa resulta ser un homomorfismo cuyo núcleo es

$$I_{\mathfrak{P}} := \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\alpha) \equiv \alpha \text{ mód } \mathfrak{P}\}$$

que se llama el *grupo de inercia* de $\mathfrak{P}$.

La importancia de esta correspondencia está dada por el siguiente resultado:

Proposición 3.1.6. *Sea L/K una extensión de Galois y sea $\mathfrak{P}$ un primo en L. Sea $\tilde{G} = Gal((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$.*

I. *El homomorfismo $D_{\mathfrak{P}} \to \tilde{G}$ es sobreyectivo. Luego $D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \tilde{G}$.*

II. *$|I_{\mathfrak{P}}| = e_{\mathfrak{P}|\mathfrak{p}}$ y $|D_{\mathfrak{P}}| = e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}}$.*

Demostración. Ver Teorema 28 de Marcus [15]. □

Casi siempre las extensiones que se van a trabajar son sobre $\mathbb{Q}$ y por tanto los primos "de abajo" van a ser los primos enteros. En particular va a interesar cuándo los primos enteros descomponen completamente en estas extensiones. Para poder decidir cuándo pasa esto se utiliza fuertemente el siguiente resultado:

Proposición 3.1.7. *Sea L/K una extensión de Galois, donde $L = K(\alpha)$ para cierto $\alpha \in \mathcal{O}_L$. Sea $f(x)$ el polinomio minimal de α sobre K, luego $f(x) \in \mathcal{O}_K[x]$. Si $\mathfrak{p}$ es un primo en $\mathcal{O}_K$ y $f(x)$ es separable módulo $\mathfrak{p}$, entonces*

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

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

Más aún todos los $f_i(x)$ *tienen el mismo grado, que es el grado de inercia* f.

II. $\mathfrak{p}$ *descompone completamente en* L *si y sólo si* $f(x) \equiv 0 \bmod \mathfrak{p}$ *tiene solución en* $\mathcal{O}_K$.

Demostración. La idea de la prueba es la siguiente: si $\mathfrak{p}\mathcal{O}_L = \mathfrak{Q}_1^e \dots \mathfrak{Q}_s^e$ es la descomposición de $\mathfrak{p}\mathcal{O}_L$, la congruencia $f(x) \equiv f_1(x)\dots f_g(x) \bmod \mathfrak{p}$ y el hecho de que $f(\alpha) = 0$ muestra que cada uno de los $f_i(\alpha)$ tiene que estar en algún $\mathfrak{Q}_j$. Además cada $f_i(\alpha)$ tiene que estar en un primo distinto pues los $f_i(x)$ son coprimos módulo $\mathfrak{p}$ y por tanto módulo cualquier $\mathfrak{Q}_j$ que caiga sobre $\mathfrak{p}$ (esto está dado por el algoritmo de Euclides).

Así cada uno de los $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L$ está contenido en un único $\mathfrak{Q}_j$ y esta correspondencia es inyectiva. O sea que lo hay que probar es que en realidad los $\mathfrak{P}_i$ son los mismos que los $\mathfrak{Q}_j$, es decir que son la misma cantidad ($s = g$) y que estas inclusiones son de hecho igualdades. Por otra parte para ver que los $\mathfrak{P}_i$ son primos y que en efecto $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \dots \mathfrak{P}_g$, también hay que ver que $e = 1$.

Pero en vez de probar las cosas por pasos se prueba todo junto, es decir una vez visto que $e = 1$ y que f es el grado de cualquiera de los $f_i(x)$, el resto se sigue de las igualdades

$$efs = [L : K] = gr(irr_K(\alpha)) = gr(f(x)) = \sum_{i=1}^{g} gr(f_i(x))$$

dadas por el Teorema 3.1.5 y el hecho de que $f(x) \equiv f_1(x)\dots f_g(x) \bmod \mathfrak{p}$. Es decir bajo estos supuestos, se tendría que $efs = fs = \sum_{i=1}^{g} f = fg$ de modo que $s = g$ y como además $e = 1$, entonces $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \dots \mathfrak{P}_g$ donde el grado de inercia f es el grado de cualquiera de los $f_i(x)$.

Luego sólo hay que probar que $e = 1$ y que $gr(f_i(x)) = f$ para todo i. Ahora dado un i fijo, la forma para probar que $gr(f_i(x)) = f$ es siempre la misma: por un lado ver que $f \geq gr(f_i(x))$ y por otro que $gr(f_i(x)) \geq ef$. Aquí se desprende además que $e = 1$.

Para facilitar la notación y evitar confusiones, las cuentas se van a hacer con $f_1(x)$. Antes de empezar hay que recordar que $f_1(x) \in \mathfrak{Q}$ para algún primo $\mathfrak{Q}$ que cae sobre $\mathfrak{p}$.

Afirmación. $f \geq gr(f_1(x))$.

$$f = f_{\mathfrak{Q}|\mathfrak{p}} = [\mathcal{O}_L/\mathfrak{Q} : \mathcal{O}_K/\mathfrak{p}] = [\mathcal{O}_L/\mathfrak{Q} : (\mathcal{O}_K/\mathfrak{p})[\alpha]]\,[(\mathcal{O}_K/\mathfrak{p})[\alpha] : \mathcal{O}_K/\mathfrak{p}]\,.$$

Como $f_1(x)$ es irreducible módulo $\mathfrak{p}$ y $f_1(\alpha) \in \mathfrak{Q}$, entonces $f_1(x)$ es el polinomio minimal de la clase de α módulo $\mathfrak{p}$. Luego

$$gr(f_1(x)) = [(\mathcal{O}_K/\mathfrak{p})[\alpha] : \mathcal{O}_K/\mathfrak{p}]\,.$$

En suma $f \geq gr(f_1(x))$.

Afirmación. $gr(f_1(x)) \geq |D_{\mathfrak{Q}}|$.

Como $f_1(x) \in \mathcal{O}_K$ entonces $\sigma(f_1(\alpha)) = f_1(\sigma(\alpha))$ para todo $\sigma \in \mathrm{Gal}(L/K)$. Como $f_1(\alpha) \in \mathfrak{Q}$ entonces $\sigma(f_1(\alpha)) \in \mathfrak{Q}$ para todo $\sigma \in D_{\mathfrak{Q}}$. En suma $f_1(\sigma(\alpha)) \in \mathfrak{Q}$ para todo $\sigma \in D_{\mathfrak{Q}}$ y se puede definir

$$\begin{array}{ccc} D_{\mathfrak{Q}} & \longrightarrow & \{\text{raíces de } f_1(x) \text{ módulo } \mathfrak{Q}\} \\ \sigma & \mapsto & \overline{\overline{\sigma(\alpha)}} \end{array}$$

Además este mapa es inyectivo: sean $\alpha_1, \ldots, \alpha_n$ las raíces de $f(x)$ en $\mathcal{O}_L$, que son obviamente todas distintas por estar en característica cero. Sean $\overline{\overline{\sigma(\alpha_1)}}, \ldots, \overline{\overline{\sigma(\alpha_n)}}$ las clases las respectivas raíces módulo $\mathfrak{Q}$. Como $f(x)$ es separable módulo $\mathfrak{p}$ y $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{Q}$, entonces también las raíces de $f(x)$ son todas diferentes módulo $\mathfrak{Q}$. Si $\sigma \in D_{\mathfrak{Q}}$ entonces $\sigma(\alpha)$ es una raíz de $f(x)$ y $\overline{\overline{\sigma(\alpha)}}$ es una raíz de $f(x)$ módulo $\mathfrak{Q}$. O sea que $\sigma(\alpha) = \alpha_i$ si y sólo si $\overline{\overline{\sigma(\alpha)}} = \overline{\overline{\sigma(\alpha_i)}}$. Luego, dados $\sigma, \tau \in D_{\mathfrak{Q}}$, $\overline{\overline{\sigma(\alpha)}} = \overline{\overline{\tau(\alpha)}}$ si y sólo si $\sigma(\alpha) = \tau(\alpha)$ o equivalentemente $\sigma = \tau$ ya que $L = K(\alpha)$.

En suma

$$f \geq gr(f_1(x)) \geq |D_{\mathfrak{Q}}| = fe$$

y por tanto $e = 1$ y $f = gr(f_1(x))$.

Por último obsérvese que $\mathfrak{p}$ descompone completamente en L si y sólo si $f = 1$, lo que es lo mismo a que $gr(f_i(x)) = 1$ para algún i. Pero la congruencia $f(x) \equiv 0$ mód $\mathfrak{p}$ tiene solución si y sólo si $f_i(x) \equiv 0$ mód $\mathfrak{p}$ tiene solución para algún i, y como $f_i(x)$ es irreducible módulo $\mathfrak{p}$ para todo i, entonces esto último es equivalente a que $gr(f_i(x)) = 1$. En suma $\mathfrak{p}$ descompone completamente en L si y sólo si $f(x) \equiv 0$ mód $\mathfrak{p}$ tiene solución. □

Antes de pasar a la siguiente sección es preciso, en vista de los intereses futuros, ver cómo cambia la descomposición de un primo al bajar o subir por una torre de extensiones.

Proposición 3.1.8. *Sea $L/M/K$ una torre de extensiones de cuerpos de números tal que L/M y M/K son Galois. Sean además $\mathfrak{p}$ un primo de $\mathcal{O}_K$, $\mathfrak{P}$ un primo de M y $\mathfrak{Q}$ un primo de L, tales que $\mathfrak{Q}$ cae sobre $\mathfrak{P}$ y $\mathfrak{P}$ cae sobre $\mathfrak{p}$. Entonces*

$$\begin{aligned} e_{\mathfrak{Q}|\mathfrak{p}} &= e_{\mathfrak{Q}|\mathfrak{P}} e_{\mathfrak{P}|\mathfrak{p}} \\ f_{\mathfrak{Q}|\mathfrak{p}} &= f_{\mathfrak{Q}|\mathfrak{P}} f_{\mathfrak{P}|\mathfrak{p}}. \end{aligned}$$

Demostración. Ver observaciones de la página 65 del Marcus [15]. □

En particular va interesar los casos de descomposición completa:

Corolario 3.1.9. *Sea $L/M/K$ como en la parte anterior. Luego un primo $\mathfrak{p}$ de $\mathcal{O}_K$ descompone completamente sobre L si y sólo si lo hace sobre M y los primos de M que lo descomponen, descomponen completamente sobre L.*

3.2. Cuerpos cuadráticos

Un *cuerpo cuadrático* es un cuerpo de números que tiene grado 2 sobre $\mathbb{Q}$, es decir un cuerpo de la forma $K = \mathbb{Q}(\sqrt{N})$. Como no cambia nada se puede considerar $N \neq 0, 1$ y libre de cuadrados.

La razón de trabajar con estos cuerpos es que la descomposición de los primos enteros en estas extensiones de $\mathbb{Q}$ resulta especialmente útil para resolver el problema $p = x^2 + ny^2$. Porque si un primo $p \in \mathbb{Z}$ descompone completamente en $K = \mathbb{Q}(\sqrt{-n})$ entonces, visto que el grado de la extensión es 2, se tiene que $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ con $\mathfrak{p} \neq \mathfrak{p}'$ primos de $\mathcal{O}_K$. Y en ese caso si $\mathfrak{p} = (x + \sqrt{-n}y)\mathcal{O}_K$ es un ideal principal, entonces la acción del grupo de Galois implica que $\mathfrak{p}' = (x - \sqrt{-n}y)\mathcal{O}_K$, por lo que $p = x^2 + ny^2$. Pero además hay que exigir que x e y sean ambos enteros, ya que esto no necesariamente se cumple. En suma para que $p = x^2 + ny^2$ con x, y enteros, hace falta que p descomponga completamente, que los ideales $\mathfrak{p}, \mathfrak{p}'$ en que lo haga sean principales, y que los enteros algebraicos de $\mathbb{Q}(\sqrt{-n})$ sean exactamente $\mathbb{Z}[\sqrt{-n}]$.

En esta sección se van a aplicar los resultados generales de cuerpos de números para decidir cuándo un primo p descompone completamente en $\mathbb{Q}(\sqrt{N})$ y también para ver cuándo los enteros algebraicos de este cuerpo son $\mathbb{Z}[\sqrt{N}]$. La cuestión de cuándo los ideales en los que descompone p son principales es bastante más difícil y requiere de herramientas de teoría de cuerpos de clases.

Siguiendo el orden del Teorema 2 primero hay que demostrar el resultado sobre los enteros algebraicos ya que este resultado depende del resto que deje N módulo 4.

Proposición 3.2.1. *Sea $K = \mathbb{Q}(\sqrt{N})$ un cuerpo cuadrático. Entonces*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{N}] & \text{si } N \not\equiv 1 \text{ mód } 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right] & \text{si } N \equiv 1 \text{ mód } 4. \end{cases}$$

Demostración. Sea $x = a + b\sqrt{N} \in \mathcal{O}_K$. Luego $T(x) = 2a$ y $N(x) = a^2 - b^2N$ son enteros por ser los coeficientes del polinomio minimal de x en $\mathbb{Z}$.

Luego $4Nb^2 = 4a^2 - 4N(x)$ es entero. Como b es racional, entonces existen dos enteros coprimos p y q tales que $b = \frac{p}{q}$. En suma $4N\frac{p^2}{q^2}$ es entero

y como N es libre de cuadrados, entonces $q^2 \mid 4$. O sea que $q = 1$ o 2. Luego $4Nb^2 = 4Np^2$ o $4Nb^2 = Np^2$ según $q = 1$ o 2.

Si $N \equiv 2$ mód 4 entonces usando la igualdad $4Nb^2 = 4a^2 - 4N(x)$ se tiene que $4a^2 \equiv 8p^2$ o $2p^2$ mód 4. Y como $2a$ es entero, entonces mirando los cuadrados módulo 4 se tiene que $4a^2 \equiv 8p^2 \equiv 0$ mód 4 en cuyo caso $q = 1$, pues si $4a^2 \equiv 2p^2$ mód 4 entonces $q = 2$ y p debería ser par pero en ese caso no serían coprimos.

Los mismos argumentos de los cuadrados muestran que si $N \equiv 3$ mód 4 entonces $4a^2 \equiv 12p^2$ o $3p^2$ mód 4 y por eso necesariamente $q = 1$.

En cualquier caso, si $N \not\equiv 1$ mód 4, entonces b es entero y así $4a^2 - 4N(x) = 4Nb^2 \equiv 0$ mód 4 por lo que $2a$ es par o lo que es lo mismo que a es entero. Entonces $\mathcal{O}_K \subset \mathbb{Z}[\sqrt{N}]$; pero más aún esos conjuntos son iguales porque

$$x^2 + 2ax + b^2N - a^2$$

es un polinomio entero para todo $a + b\sqrt{N} \in \mathbb{Z}[\sqrt{N}]$.

Si $N \equiv 1$ mód 4 entonces $4a^2 \equiv 4Nb^2 \equiv 4b^2$ mód 4. O sea que $2a \equiv 2b$ mód 2 y por tanto $a + b\sqrt{N} = \frac{2a-2b}{2} + 2b\frac{1+\sqrt{N}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right]$ y por eso $\mathcal{O}_K \subset \mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right]$. Y también en este caso los conjuntos son iguales porque el polinomio

$$x^2 + 2ax + \frac{b^2N - 4a^2 - b^2}{4}$$

tiene coeficientes enteros para todo $a + b\frac{1+\sqrt{N}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right]$. □

Volviendo a la discusión anterior:

Corolario 3.2.2. *Sea $K = \mathbb{Q}(\sqrt{-n})$ con $n \not\equiv 3$ mód 4 libre de cuadrados. Si p es un primo entero tal que $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ con $\mathfrak{p}$ principal entonces $p = x^2+ny^2$ con x e y enteros.*

Ahora se pasa a clasificar la descomposición de un primo p en cuerpos cuadráticos. A partir de la Proposición general 3.1.7, la decisión en este caso es bastante directa, ya que si en esa proposición se toma $L = \mathbb{Q}(\sqrt{N})$ y $K = \mathbb{Q}$, el polinomio $f(x)$ en este caso es $x^2 - N$. Y saber si dicho polinomio descompone o no módulo p, es equivalente a saber si N es un cuadrado o no módulo p. Así:

Proposición 3.2.3. *Sea $K = \mathbb{Q}(\sqrt{N})$ un cuerpo cuadrático, y sea p un primo impar de $\mathbb{Z}$.*

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

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

III. *Si $(N/p) = -1$, entonces $p\mathcal{O}_K$ es primo en $\mathcal{O}_K$.*

Demostración. i. Sea

$$\mathfrak{p} = p\mathcal{O}_K + \sqrt{N}\mathcal{O}_K.$$

Elevando al cuadrado se obtiene

$$\mathfrak{p}^2 = p^2\mathcal{O}_K + p\sqrt{N}\mathcal{O}_K + N\mathcal{O}_K.$$

Como N es libre de cuadrados y p es un divisor de N, entonces debe ser $mcd(p^2, N) = p$. Como además $\sqrt{N} \in \mathcal{O}_K$, se sigue que $\mathfrak{p}^2 = p\mathcal{O}_K$.

ii. y iii. Considérese el polinomio $x^2 - N$ minimal que anula a $\sqrt{N}$. Si p un primo impar, entonces

$$x^2 - N \text{ tiene dos raíces distintas módulo } p \iff \left(\frac{N}{p}\right) = \left(\frac{N}{p}\right) = 1$$
$$\text{y el polinomio es irreducible módulo } p \iff \left(\frac{N}{p}\right) = \left(\frac{N}{p}\right) = -1.$$

Luego la Proposición 3.1.7 muestra que p descompone completamente en el primer caso y permanece inerte en el segundo. □

Luego la descomposición de los primos enteros en $\mathbb{Q}(\sqrt{-n})$ queda clasificada por:

Corolario 3.2.4. *Sea $K = \mathbb{Q}(\sqrt{-n})$ un cuerpo cuadrático y sea p un primo entero impar. Entonces*

I. *p ramifica si y sólo si $(-n/p) = 0$.*

II. *p descompone completamente si y sólo si $(-n/p) = 1$.*

Capítulo 4

Teoría de cuerpos de clases

Con lo hecho en el capítulo anterior se puede saber cuando un primo entero p descompone completamente en $\mathbb{Q}(\sqrt{-n})$ y cómo tiene que ser n para que si p descompone en ideales principales de $\mathbb{Q}(\sqrt{-n})$, entonces se pueda afirmar $p = x^2 + ny^2$ con x e y enteros. Pero nada se sabe de cuándo es que los ideales que descomponen a p en $\mathbb{Q}(\sqrt{-n})$ son principales. Aquí es donde se usa la *teoría de cuerpos de clases*.

A grandes rasgos lo que se hace es construir un cuerpo de números L por encima de $K = \mathbb{Q}(\sqrt{-n})$ de modo que la descomposición completa de cualquier primo entero p en este cuerpo L baje en K a una descomposición completa en ideales principales. Luego alcanza con ver cuáles son los primos enteros que descomponen completamente en esta extensión L. La idea de fondo y lo que hace que todo funcione, es una generalización de la reciprocidad cuadrática, llamada la *reciprocidad de Artin*. Esta nueva reciprocidad entiende *las clases de ideales* de K como elementos del grupo de Galois de L/K, lo cual permite decidir mucho más fácilmente cuando un ideal es principal o no.

4.1. El cuerpo de clases de Hilbert

El cuerpo de clases de Hilbert de un cuerpo de números K se define en términos de extensiones *abelianas* y *no ramificadas*. Estas expresiones, aunque sean hasta ahora desconocidas, resultan fáciles de suponer.

Una extensión de Galois L/K es *abeliana* si lo es su grupo de Galois. Con la expresión "no ramificada" es esperable que implique que todos los primos de K no ramifiquen en la extensión correspondiente. Sin embargo para adaptar la teoría a cualquier caso es preciso extender la noción de lo que es un primo: por un lado están los *primos finitos* de K que son los que ya se han definido, es decir los ideales primos de $\mathcal{O}_K$; pero además se agregan los *primos infinitos*, que son los monomorfismos $\sigma : K \to \mathbb{R}$ o $\mathbb{C}$ según sean *reales* o *complejos*. La ramificación de estos nuevos primos en una extensión

L/K se da cuando son reales en K pero admiten una extensión compleja en L. Es importante observar que en los cuerpos imaginarios los primos infinitos tienen que ser necesariamente complejos y por eso la ramificación de los primos de estos cuerpos sólo se puede dar cuando son finitos. En particular esto se aplica para los cuerpos los de la forma $\mathbb{Q}(\sqrt{-n})$. En cualquier caso, una extensión arbitraria de cuerpos de números L/K se dice *no ramificada* si *todos* los primos de K no ramifican en L.

Finalmente el *cuerpo de clases de Hilbert* de un cuerpo de números K es la mayor de todas las extensiones abelianas no ramificadas. Su existencia está garantizada por los teoremas de cuerpos de clases que se verán en la última sección de este capítulo.

El mayor aporte de este nuevo cuerpo al problema $p = x^2 + ny^2$ es la siguiente equivalencia:

Proposición 4.1.1. *Sea L el cuerpo de clases de Hilbert de K, y sea $\mathfrak{p}$ un primo de K. Entonces*

$$\mathfrak{p} \text{ descompone completamente en } L \iff \mathfrak{p} \text{ es principal en } K.$$

Esto resuelve cuando un ideal es principal sobre cualquier cuerpo de números y en particular sobre $\mathbb{Q}(\sqrt{-n})$, que es exactamente lo que falta para decidir cuándo p se puede escribir como $x^2 + ny^2$.

Ahora bien, para llegar a este resultado antes que hay atravesar la correspondencia que tienen los ideales de K con el grupo de Galois de L/K, que es lo que está en el fondo de la esencia del cuerpo de clases de Hilbert.

Lema 4.1.2. *Sea $K \subset L$ una extensión de Galois, y sea $\mathfrak{p}$ un primo de $\mathcal{O}_K$ que es no ramificado en L. Si $\mathfrak{P}$ es un primo de $\mathcal{O}_L$ conteniendo a $\mathfrak{p}$, entonces hay un único elemento $\sigma \in Gal(L/K)$ tal que para todo $\alpha \in \mathcal{O}_L$*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \text{ mód } \mathfrak{P}.$$

Demostración. La clave está en la relación dada en el capítulo anterior por la Proposición 3.1.6, vinculando los grupos de descomposición $D_{\mathfrak{P}}$ e inercia $I_{\mathfrak{P}}$ de $\mathfrak{P}$, con el grupo de Galois $\tilde{G}$ de $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$. Específicamente, $\sigma \in D_{\mathfrak{P}}$ induce naturalmente un automorfismo de $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$. Y este mapeo era en realidad un homomorfismo de grupos sobreyectivo cuyo núcleo era $I_{\mathfrak{P}}$.

La Proposición 3.1.6 también dice que $|I_{\mathfrak{P}}| = e_{\mathfrak{P}|\mathfrak{p}}$, y como ahora $e_{\mathfrak{P}|\mathfrak{p}} = 1$, entonces este epimorfismo de grupos es de hecho un isomorfismo. Y esto da la existencia del σ buscado en el lema, ya que $\tilde{G}$ es un grupo cíclico generado por el automorfismo de Frobenius $x \mapsto x^q$ siendo $q = |\mathcal{O}_K/\mathfrak{p}| = N(\mathfrak{p})$ (ver Apéndice 1 de Marcus [15]). Luego, volviendo por el isomorfismo, existe un único $\sigma \in D_{\mathfrak{P}}$ tal que se mapea en el automorfismo de Frobenius. Pero entonces

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \text{ mód } \mathfrak{P}.$$

Para terminar es importante notar que cualquier σ que cumpla esta condición debe estar en $D_{\mathfrak{P}}$, así que la unicidad local implica la unicidad global en $\mathrm{Gal}(L/K)$. □

A este único elemento se conoce como el *símbolo de Artin* de $\mathfrak{P}$, y se denota como

$$\left(\frac{L/K}{\mathfrak{P}}\right).$$

De este modo el símbolo de Artin es un vehículo que lleva ideales primos en elementos del grupo de Galois de L/K. Pero el problema es que estos ideales son por el momento ideales de L y no de K. O sea a priori, $((L/K)/\mathfrak{P})$ depende de $\mathfrak{P}$ y podría cambiar con otro primo $\mathfrak{P}'$ que caiga sobre el mismo primo en K. En concreto, el comportamiento del símbolo de Artin es el siguiente:

Corolario 4.1.3. *Sea $K \subset L$ una extensión de Galois, y sea $\mathfrak{p}$ un primo no ramificado de K. Dado $\mathfrak{P}$ un primo de L que contiene a $\mathfrak{p}$, se tiene que:*

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. *$\mathfrak{p}$ descompone completamente si y sólo si $((L/K)/\mathfrak{P}) = 1$.*

Demostración. Por definición para todo $\alpha \in \mathcal{O}_L$

$$\left(\frac{L/K}{\mathfrak{P}}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \text{ mód } \mathfrak{P}.$$

Luego

$$\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}(\alpha) \equiv \sigma(\sigma^{-1}(\alpha)^{N(\mathfrak{p})}) = \alpha^{N(\mathfrak{p})} \text{ mód } \sigma(\mathfrak{P}),$$

y por unicidad

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

Por otra parte, como $\mathfrak{p}$ no ramifica, entonces $D_{\mathfrak{P}}$ es isomorfo al grupo de Galois de $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$ y entonces el orden de $((L/K)/\mathfrak{P})$ es el orden del automorfismo de Frobenius que es $[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = f$.

En tanto $\mathfrak{p}$ descompone completamente si y sólo si $f = 1$ o lo que es lo mismo $((L/K)/\mathfrak{P}) = 1$. □

Así cuando la extensión L/K es abeliana, el símbolo de Artin de un primo $\mathfrak{P}$ de L depende sólo del primo sobre el que cae $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, ya que por la propiedad básica del Teorema 3.1.5 todos los primos que caen sobre $\mathfrak{p}$ son conjugados por el grupo de Galois. Esto permite escribir el símbolo de Artin de los primos que caen sobre $\mathfrak{p}$ simplemente como $((L/K)/\mathfrak{p})$. Claro que para que todo tenga sentido $\mathfrak{p}$ tiene que ser no ramificado.

De todas formas, cuando la extensión L/K es no ramificada además de abeliana, la definición del símbolo de Artin se puede extender de forma natural a cualquier ideal fraccional de K. Es decir si $\mathfrak{a} \in I_K$, entonces haciendo la factorización dada por el Corolario 3.1.3, puede escribirse

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i}$$

con los $\mathfrak{p}_i$ primos de $\mathcal{O}_K$ y los r_i enteros. Así se define el símbolo de Artin $((L/K)/\mathfrak{a})$ como siendo el producto

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

Y se dice que esta definición es natural, porque es la única que hace que el mapa

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

sea un homomorfismo de grupos. Su nombre es el *mapa de Artin*.

La relación que tiene el mapa de Artin con el cuerpo de clases de Hilbert, es que la correspondencia de este mapa es especialmente útil cuando L es el cuerpo de clases de Hilbert de K:

Teorema 4.1.4. *Si L es el cuerpo de clases de Hilbert de un cuerpo de números K, entonces el mapa de Artin*

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

es sobreyectivo, y su núcleo es exactamente el subgrupo P_K de ideales fraccionales principales. Así el mapa de Artin induce un isomorfismo

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

La aparición de el grupo $C(\mathcal{O}_K)$ explica por qué L es llamado un "cuerpo de clases". Este resultado es la versión para el cuerpo de clases de Hilbert de una correspondencia más general llamada *reciprocidad de Artin*. Al igual que los otros teoremas de cuerpos de clases, la reciprocidad de Artin se verá con más detalle en la última sección de este capítulo. De todas formas a los efectos de probar la Proposición 4.1.1, ya está todo pronto:

Demostración de la Proposición 4.1.1. Por el Corolario 4.1.3 que $\mathfrak{p}$ descomponga completamente es equivalente a que $((L/K)/(\mathfrak{p})) = 1$. Pero esto, por la reciprocidad de Artin, es lo mismo a decir que $\mathfrak{p}$ es principal. □

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

Hasta ahora se vieron que condiciones tienen que cumplir los primos de un cuerpo de números K para ser principales. Pero para resolver $p = x^2+ny^2$ resta ver cómo se relacionan los primos enteros p con estas condiciones. Es decir de qué forma tiene que ser p para que los primos que lo descompongan en $K = \mathbb{Q}(\sqrt{-n})$ sean principales. Sin embargo esta pregunta se vuelve sencilla al ver como es la extensión del cuerpo de clases de Hilbert de K sobre $\mathbb{Q}$:

Lema 4.2.1. *Sea L el cuerpo de clases de Hilbert de un cuerpo cuadrático imaginario K, y sea τ la conjugación compleja. Luego $\tau(L) = L$ y consecuentemente L es Galois sobre $\mathbb{Q}$.*

Demostración. Trasladando, $\tau(L)$ es un extensión abeliana no ramificada de $\tau(K) = K$. Como L es la más grande de esas extensiones, entonces $\tau(L) = L$ pues ambos tienen el mismo grado sobre K. Así σ y $\tau\sigma$ son automorfismos de $L/\mathbb{Q}$ para cualquier $\sigma \in \mathrm{Gal}(L/K)$; y son distintos ya que K es imaginario. En consecuencia $|\mathrm{Aut}(L/\mathbb{Q})| \geq |\mathrm{Gal}(L/K)| \cdot 2 = [L : K] \cdot 2 = [L : \mathbb{Q}]$, y $L/\mathbb{Q}$ es Galois. □

Recordando la Proposición 4.1.1, la condición necesaria para que los primos de K sean principales es que deben descomponer completamente en el cuerpo de clases de Hilbert L. Ahora al mirar la torre de extensiones $L/K/\mathbb{Q}$ con la propiedad dada por el Corolario 3.1.9, si p es un primo entero y $\mathfrak{p}$ es un primo de K que cae sobre p, para que $\mathfrak{p}$ sea principal alcanza con que p descomponga completamente en L. Y, más aún, esta condición también implica que p descompone completamente en K. De hecho el mismo Corolario 3.1.9 dice que también es cierto el recíproco, es decir si p descompone completamente en K y cualquier primo $\mathfrak{p}$ de K que cae sobre p descompone completamente en L entonces p descompone completamente en L.

Sumando todo lo hecho:

Teorema 4.2.2. *Sea L el cuerpo de clases de Hilbert de $K = \mathbb{Q}(\sqrt{-n})$ con $n \not\equiv 3 \bmod 4$ libre de cuadrados. Si p es un primo que no divide a $4n$, entonces*

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

Demostración. En realidad ya está todo probado, para formalizar tan sólo hay que notar que el teorema se sigue de las siguientes equivalencias

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

Para la primera equivalencia hay que recordar el Corolario 3.2.2, que se basaba en el hecho de que la condición $n \not\equiv 3$ mód 4 implica $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$. Esto es para el recíproco; el directo se sigue inmediatamente (aunque es importante usar que p no divide a n para que $\mathfrak{p} \neq \mathfrak{p}'$, ya que en ese caso p no ramifica en K por lo visto en el Corolario 3.2.4).

Las otras dos equivalencias, se siguen de la discusión anterior, es decir la segunda sale de la Proposición 4.1.1, mientras que la tercera deviene de que L es Galois sobre $\mathbb{Q}$ y del Corolario 3.1.9. □

A esta altura, lo único que queda para llegar al Teorema 2, es ver cómo se traduce la condición de que p descomponga en L a que un polinomio factorice módulo p. Pero esto ya está hecho al principio de esta segunda parte en la Proposición 3.1.7, de modo que sólo hay que adaptar ese resultado a este caso para obtener exactamente el Teorema 2:

Proposición 4.2.3. *Sea $K = \mathbb{Q}(\sqrt{-n})$ un cuerpo cuadrático imaginario y sea L una extensión finita y Galois de K que queda invariante por la conjugación compleja. Entonces:*

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

II. *Dado α como en la parte anterior, sea $f(x) \in \mathbb{Z}[x]$ su polinomio minimal. Si p es un primo que no divide al discriminante de $f(x)$, entonces p descompone completamente en L si y sólo si*

$$\begin{cases} (-n/p) = 1 \text{ y} \\ f(x) \equiv 0 \text{ mód } p \text{ tiene solución entera.} \end{cases}$$

Demostración. Por el Teorema del elemento primitivo existe $\alpha \in \mathbb{R}$ tal que $L \cap \mathbb{R} = \mathbb{Q}(\alpha)$. Incluso se puede considerar α entero algebraico.

Como K es imaginario entonces $[K(\alpha) : \mathbb{Q}(\alpha)] = 2$ (de lo contrario $K \subset \mathbb{R}$).

Como $L \cap \mathbb{R}$ es el subcuerpo de L que queda fijo por la conjugación compleja del grupo de Galois $\mathrm{Gal}(L/\mathbb{Q})$ entonces $[L : L \cap \mathbb{R}] = 2$.

En suma

$$\begin{cases} [L : L \cap \mathbb{R}] = [K(\alpha) : \mathbb{Q}(\alpha)] \\ L \cap \mathbb{R} = \mathbb{Q}(\alpha) \end{cases}$$

de donde se sigue $K(\alpha) = L$, lo cual prueba la primera parte. Más aún si $f(x) \in \mathbb{Z}[x]$ es el polinomio minimal de α sobre $\mathbb{Q}$ entonces se cumple que

$gr(f(x)) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [L \cap \mathbb{R} : \mathbb{Q}]$. Y como

$$[L : \mathbb{Q}] = \begin{cases} [L : K][K : \mathbb{Q}] = [L : K] \cdot 2 \\ [K(\alpha) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \end{cases}$$

entonces $[L : K] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = gr(f(x))$ y en consecuencia $f(x)$ también es el polinomio minimal de α sobre K.

Respecto a la segunda parte hay que notar que un primo entero p descompone completamente en L si y sólo si

$$\begin{cases} p \text{ descompone completamente en } K \text{ y} \\ \text{todo primo } \mathfrak{p} \text{ de } K \text{ que cae sobre a } p, \text{ descompone completamente en } L. \end{cases}$$

De la sección de cuerpos cuadráticos del tercer capítulo (Corolario 3.2.4), se sabe que la condición necesaria y suficiente para que p descomponga completamente en $K = \mathbb{Q}(\sqrt{-n})$ es que $(-n/p) = 1$.

De todas formas si p descompone completamente en K y $\mathfrak{p}$ es un primo de K que cae sobre p, entonces $\mathbb{Z}/p\mathbb{Z} \simeq \mathcal{O}_K/\mathfrak{p}$ pues $f_{\mathfrak{p}|p} = 1$. Ahora si además p no divide al discriminante de $f(x)$ entonces este polinomio tiene que ser separable sobre $\mathcal{O}_K/\mathfrak{p}$, y luego la Proposición 3.1.7 muestra que $\mathfrak{p}$ descompone completamente en L si y sólo si

$$f(x) \equiv 0 \text{ mód } \mathfrak{p} \text{ tiene solución en } \mathcal{O}_K,$$

lo cual volviendo por el isomorfismo $\mathbb{Z}/p\mathbb{Z} \simeq \mathcal{O}_K/\mathfrak{p}$, es equivalente a que $f(x) \equiv 0$ mód p tenga solución entera.

En suma p descompone completamente en L si y sólo si

$$\begin{cases} (-n/p) = 1 \text{ y} \\ f(x) \equiv 0 \text{ mód } p \text{ tiene solución entera.} \end{cases}$$

□

Así, concluye la demostración del Teorema 2. Aunque en la práctica esto no significó un gran avance, ya que no se obtuvieron resultados para resolver casos concretos del problema $p = x^2 + ny^2$ como se había hecho en la primera parte. Es decir este teorema depende del polinomio $f_n(x)$ del cual hasta lo hecho ahora no se conoce nada. De hecho lo que se puede deducir a partir de la proposición anterior, es que para conocer este polinomio $f_n(x)$ hay que conocer el cuerpo de clases de Hilbert de $\mathbb{Q}(\sqrt{-n})$. Y en realidad, como se va a ver más adelante, el problema de encontrar el polinomio que satisfaga las equivalencias del Teorema 2 es el mismo problema que encontrar el cuerpo de clases de Hilbert.

A pesar de todo es posible conocer el grado de $f_n(x)$. Esto se va hacer en el siguiente capítulo. Concretamente se prueba que el cardinal de $C(\mathcal{O}_K)$

es $h(-4n)$ cuando $K = \mathbb{Q}(\sqrt{-n})$ y el resto se sigue de la reciprocidad de Artin y la proposición anterior puesto que

$$gr(f_n(x)) = [L : K] = |C(\mathcal{O}_K)|.$$

De todas formas, conociendo este resultado vuelve más fácil conjeturar cuáles van a ser estos polinomios $f_n(x)$ cuando la cantidad de clases $h(-4n)$ no es muy grande. Este es el caso por ejemplo de $n = 14$ que había quedado irresoluto con las herramientas de la primera parte.

4.2.1. Ejemplo $p = x^2 + 14y^2$

Por lo antes computado se sabe que $h(-4 \cdot 14) = 4$ y por lo tanto $f_{14}(x)$ es de grado 4. Específicamente $f_{14}(x) = (x^2 + 1)^2 - 8$. O sea

Teorema 4.2.4. *Si p es un primo impar distinto de 7 entonces*

$$p = x^2 + 14y^2 \iff \begin{cases} (-14/p) = 1 \\ (x^2+1)^2 \equiv 8 \text{ mód } p \text{ tiene solución entera.} \end{cases}$$

O como $\sqrt{2\sqrt{2}-1}$ es raíz de $(x^2 + 1) - 8$, esto también es lo mismo a decir que

Proposición 4.2.5. *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 el cuerpo de clases de Hilbert tiene grado 4 sobre K, entonces para mostrar que $L = K(\alpha)$ es dicho cuerpo alcanza con mostrar que L es una extensión abeliana no ramificada de grado 4 sobre K.

Antes que nada, ver L/K es de Galois es inmediato a partir de la cuenta que muestra que las raíces de $(x^2 + 1)^2 - 8$ son $\alpha, -\alpha, \frac{2\sqrt{-14}}{\alpha^3+\alpha}, -\frac{2\sqrt{-14}}{\alpha^3+\alpha}$ que están todas en L. Esto también muestra que L/K tiene grado cuatro, pues ninguna de estas raíces está en K. Finalmente, como los grupos de orden 4 son todos abelianos, entonces también lo es el grupo de Galois de la extensión L/K.

Ahora resta ver que L es no ramificada sobre K. Sobre los primos infinitos no hay nada que decir pues K es imaginario y por tanto estos primos son no ramificados en cualquier extensión. Con los primos finitos, se procede de la siguiente manera: se construye una cuerpo intermedio M tal que la torre de extensiones $K \subset M \subset L$ cumpla que M/K y L/M son no ramificadas, y el resto se sigue de la Proposición 3.1.8. Para esto sea $M = K(\sqrt{2})$. Obsérvese que $L = M(\sqrt{\mu})$ donde $\mu = 2\sqrt{2} - 1$, por lo que, tanto M/K como L/M son extensiones cuadráticas por enteros algebraicos. Esto facilita la prueba de que ambas son no ramificadas, gracias al siguiente resultado general:

Lema 4.2.6. *Sea $L = K(\sqrt{u})$ una extensión cuadrática de un cuerpo de números, donde $u \in \mathcal{O}_K$, y sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$. Entonces*

I. *Si* $2u \notin \mathfrak{p}$, *entonces* $\mathfrak{p}$ *no ramifica en* L.

II. *Si* $2 \in \mathfrak{p}$, $u \notin \mathfrak{p}$ *y* $u = b^2 - 4c$ *para ciertos* $b, c \in \mathcal{O}_K$, *entonces* $\mathfrak{p}$ *no ramifica en* L.

Demostración. La clave es usar una vez más la Proposición 3.1.7. Para el primer caso basta ver que $x^2 - u$ es el polinomio minimal de u sobre K y que tiene discriminante $4u \notin \mathfrak{p}$. Y para el segundo hay que observar que $L = K(\beta)$ donde $\beta = (-b + \sqrt{u})/2$ es una raíz de $x^2 + bx + c$ que es un polinomio de discriminante $b^2 - 4c = u \notin \mathfrak{p}$. □

Con estas herramientas se dirime la descomposición. Para M/K sea $\mathfrak{p}$ un primo en K. Como $M = K(\sqrt{2})$, entonces el lema anterior implica que $\mathfrak{p}$ es no ramificado en M cuando $2 \notin \mathfrak{p}$. Si $2 \in \mathfrak{p}$ alcanza con observar que como $K = \mathbb{Q}(\sqrt{-14})$ entonces M también se puede escribir como $K(\sqrt{-7})$ y luego $-7 = 1^2 - 4 \cdot 2 \notin \mathfrak{p}$, que por el segundo caso del lema implica que $\mathfrak{p}$ no ramifica.

Para trabajar con la extensión L/M hay que recordar que $L = M(\sqrt{\mu})$ con $\mu = 2\sqrt{2} - 1$. Sea $\mathfrak{p}$ un primo de M. La diferencia aquí es que el caso fácil es $2 \in \mathfrak{p}$: bajo este supuesto $\mu \notin \mathfrak{p}$ y $\mu = (1 + \sqrt{2})^2 - 4$. Para el caso $2 \notin \mathfrak{p}$ sea $\mu' = -2\sqrt{2} - 1$ y nótese que $L = M(\sqrt{\mu'})$; luego como $\mu + \mu' = -2$ entonces alguno de μ o μ' no están en $\mathfrak{p}$. □

Demostración del Teorema 4.2.4. En vistas de que el Teorema 2 se basa en la Proposición 4.2.3, lo único que resta ver es que la condición de p primo distinto de 2 y 7 es equivalente a que p no divida al discriminante de $(x^2 + 1)^2 - 8$. Pero esto es cierto ya que dicho discriminante es $-2^{14} \cdot 7$. □

Estos métodos también pueden usarse para calcular otros cuerpos de clases de Hilbert. Así, por ejemplo, para $K = \mathbb{Q}(\sqrt{-17})$ se prueba que $L = K(\alpha)$ con $\alpha = \sqrt{(1 + \sqrt{17})/2}$ es su cuerpo de clases de Hilbert.

Sin embargo, todos estos ejemplos presentan un mismo aspecto insatisfactorio que impide extender la prueba para cualquier caso: no explican cómo se halla el elemento primitivo α del cuerpo de clases de Hilbert. Y el hecho es que calcular el cuerpo de clases de Hilbert es en general algo difícil de hacer explícitamente, aunque estas herramientas lo facilitan para cuerpos con números de clases manejables (ver el Capítulo VII de *Seminar on Complex Multiplication* [8] escrito por Herz).

4.3. Los teoremas de la teoría de cuerpos de clases

El principal objetivo de esta sección es demostrar los teoremas de cuerpos de clases citados en la sección anterior. En realidad lo que se va a hacer es mostrar cómo a partir de los grandes teoremas de cuerpos de clases se obtienen los resultados que se precisan para la resolución del Teorema 2,

como lo son la existencia del *cuerpo de clases de Hilbert* y la *reciprocidad de Artin*. Al mismo tiempo estos teoremas permiten probar otros resultados importantes de la teoría de números, como por ejemplo las reciprocidades de cualquier orden, y en particular la cuadrática que había quedado pendiente en la primera parte. No obstante en esta sección tampoco se verán las demostraciones de los teoremas fundamentales, no porque no sean importantes sino porque su demostración llevaría demasiado tiempo y no aportaría mucho a la resolución del problema $p = x^2 + ny^2$. La referencia será el libro de Janusz *Algebraic Number Fields* [10].

Como se dijo al comienzo del capítulo, el resultado central de esta teoría y lo que da sentido a todo es la reciprocidad de Artin. En particular como se vio antes, la reciprocidad de Artin es la que muestra la utilidad al cuerpo de clases de Hilbert. Por eso es lo primero a ver.

Recuérdese que para definir el símbolo de Artin de un primo $\mathfrak{p}$ en una extensión abeliana L/K es necesario que éste no ramifique. Cuando L es el cuerpo de clases de Hilbert de K esto pasa siempre, pero en general no tendría por qué ser así. En cualquier caso la definición del símbolo de Artin puede hacerse para todo ideal fraccional $\mathfrak{a}$ de K que descomponga en primos no ramificados. Luego, este conjunto de ideales se identifica por el mismo *mapa de Artin* con el grupo de Galois de L/K.

Para caracterizar a estos ideales se define una nueva estructura: los módulos. Un *módulo* en un cuerpo de números K es un producto formal

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

sobre todos los primos $\mathfrak{p}$, finitos o infinitos, de K, donde los exponentes deben satisfacer:

I. $n_{\mathfrak{p}} \geq 0$, y a lo sumo una cantidad finita es no nula.

II. $n_{\mathfrak{p}} = 0$ cuando $\mathfrak{p}$ es un primo complejo infinito.

III. $n_{\mathfrak{p}} \leq 1$ cuando $\mathfrak{p}$ es un primo real infinito.

O sea, dicho de otra forma un módulo $\mathfrak{m}$ es el producto formal de una cantidad finita de potencias enteras de primos finitos con una cantidad finita de primos reales infinitos. Así $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, donde $\mathfrak{m}_0$ es un ideal fraccional y $\mathfrak{m}_\infty$ es el producto de distintos primos reales infinitos. Cuando $n_{\mathfrak{p}} = 0$ para todo primo $\mathfrak{p}$, se escribe $\mathfrak{m} = 1$.

Si bien es cierto que cuando K es un cuerpo imaginario (como pasa en la mayoría de los casos que se están viendo) no hay primos reales infinitos, la inclusión de los primos infinitos se hace para formar una teoría completa que abarque todos los cuerpos de números.

Ahora bien, ¿cómo ayuda esto a describir los ideales primos que no ramifican en una extensión L/K? La idea es la siguiente: se toma $\mathfrak{m}$ como siendo

el módulo producto de todos los primos ramificados de la extensión (que siempre son una cantidad finita, ver Corolario 2 del Teorema 24 en el libro de Marcus [15]) y luego los ideales primos que no ramifican pueden ser vistos como ideales módulos coprimos a este módulo $\mathfrak{m}$. Más específicamente, los ideales fraccionales de K que descomponen en primos que no están en $\mathfrak{m}$ son todos los módulos coprimos a $\mathfrak{m}$.

En general, dado un módulo $\mathfrak{m}$, se define $I_K(\mathfrak{m})$ como siendo el conjunto de todos los ideales fraccionales de K relativamente primos a $\mathfrak{m}$ (o mejor dicho a $\mathfrak{m}_0$). Lo interesante de este conjunto es que mantiene una estructura de grupo. Además, siguiendo la discusión anterior, si $\mathfrak{m}$ es un módulo divisible por todos primos ramificados de una extensión abeliana L/K entonces $I_K(\mathfrak{m})$ se mapea por el símbolo de Artin a $\mathrm{Gal}(L/K)$. Esto da un homomorfismo

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K)$$

que es llamado el *mapa de Artin* para la extensión L/K y el módulo $\mathfrak{m}$.

El siguiente paso es describir el núcleo de este homomorfismo. En este sentido el subgrupo más importante de $I_K(\mathfrak{m})$ es $P_{K,1}(\mathfrak{m})$ generado por los ideales principales $\alpha\mathcal{O}_K$, donde $\alpha \in \mathcal{O}_K$ satisface

$\alpha \equiv 1$ mód $\mathfrak{m}_0$ y $\sigma(\alpha) > 0$ para todo primo real infinito σ que divida a $\mathfrak{m}_\infty$.

Un subgrupo H de $I_K(\mathfrak{m})$ es llamado *grupo de congruencia* para $\mathfrak{p}$ si

$$P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$$

y el cociente

$$I_K(\mathfrak{m})/H$$

se dice que es un *grupo generalizado de clases de ideales*. La razón de este nombre viene dada por el caso $\mathfrak{m} = 1$. Aquí $P_K = P_{K,1}(1)$ es un grupo de congruencia, y su correspondiente grupo generalizado de clases ideales no es otra cosa que el *grupo de clases de ideales* $C(\mathcal{O}_K) = I_K/P_K$.

La idea básica de teoría de cuerpos de clases es que estos grupos generalizados de clases de ideales son los grupos de todas las extensiones abelianas de K, y esta identificación está dada por el mapa de Artin.

Ley de reciprocidad de Artin. *Sea L/K una extensión abeliana, y sea $\mathfrak{m}$ un módulo divisible por todos los primos de K, finitos o infinitos, que ramifican en L. Entonces:*

I. *El mapa de Artin $\Phi_{\mathfrak{m}}$ es sobreyectivo.*

II. *Si los exponentes de los primos finitos que dividen a $\mathfrak{m}$ son suficientemente grandes, entonces $\ker(\Phi_{\mathfrak{m}})$ es un grupo de congruencia para $\mathfrak{m}$, es decir*

$$P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}}) \subset I_K(\mathfrak{m})$$

y consecuentemente el isomorfismo

$$I_K(\mathfrak{m})/\ker(\Phi_\mathfrak{m}) \xrightarrow{\sim} Gal(L/K)$$

muestra que $Gal(L/K)$ es un grupo generalizado de clases de ideales.

Demostración. Ver el Capítulo V del libro de Janusz [10], Teorema 5.7. □

Una imprecisión que presenta este teorema es que el módulo $\mathfrak{m}$ para el cual $\ker(\Phi_\mathfrak{m})$ es un grupo de congruencia, podría variar. De hecho si $P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_\mathfrak{m})$, y $\mathfrak{n}$ es divisible por $\mathfrak{m}$ entonces también se cumple que $P_{K,1}(\mathfrak{n}) \subset \ker(\Phi_\mathfrak{n})$. Luego $\mathrm{Gal}(L/K)$ es un grupo de clases generalizado para infinitos módulos. Sin embargo, puede construirse un módulo de modo tal que cualquier otro módulo que cumpla con esta propiedad es múltiplo de él. Esto es lo que prueba el siguiente teorema:

Teorema del conductor. *Sea L/K una extensión abeliana. Hay un módulo $\mathfrak{f} = \mathfrak{f}(L/K)$ tal que:*

I. *Cualquier primo de K, sea finito o infinito, que ramifique en L divide a $\mathfrak{f}$.*

II. *Si $\mathfrak{m}$ es un módulo de K divisible por todos los primos que ramifican en L, entonces $\ker(\Phi_\mathfrak{m})$ es un grupo de congruencia si y sólo si $\mathfrak{f}|\mathfrak{m}$.*

Demostración. Ver el Capítulo V del libro de Janusz [10], Teorema 12.7. □

El teorema lleva este nombre porque al módulo $\mathfrak{f}(L/K)$ se le llama *conductor*.

El ingrediente que falta para asegurar la existencia del cuerpo de clases de Hilbert (y cualquier otro cuerpo de clases generalizado) es precisamente el teorema de existencia:

Teorema de existencia. *Sea $\mathfrak{m}$ un módulo de K, y sea H un grupo de congruencia para $\mathfrak{m}$, es decir*

$$P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m}).$$

Entonces hay una única extensión abeliana L de K tal que todos los primos ramificados de ella dividen a $\mathfrak{m}$, y el núcleo del mapa de Artin

$$\Phi_\mathfrak{m} : I_K \longrightarrow Gal(L/K)$$

es exactamente H.

Demostración. Ver el Capítulo V del libro de Janusz [10], Teorema 9.16. □

La importancia de este teorema es que permite construir extensiones abelianas de K con un grupo de Galois específico y una ramificación restringida.

En particular asegura la existencia del cuerpo de clases de Hilbert. En efecto si $\mathfrak{m} = 1$ y $H = P_K = P_{K,1}$, entonces se puede construir una extensión L tal que $\mathrm{Gal}(L/K)$ sea isomorfo por el mapa de Artin al grupo de clases de ideales $C(\mathcal{O}_K) = I_K/P_K$. Aunque en realidad esta no fue la definición que se dio en la primera sección del capítulo sobre cuerpo de clases de Hilbert. En ese entonces el cuerpo de clases de Hilbert de K había sido presentado como la mayor extensión abeliana de K. De todos modos esta extensión L cuyo grupo de Galois sobre K es $C(\mathcal{O}_K)$ constituye, en efecto, la mayor extensión abeliana no ramificada de K.

Que es no ramificada es inmediato a partir del hecho que todos los primos ramificados de la extensión deben dividir a $\mathfrak{m} = 1$. Para probar la maximalidad se usa la propiedad minimal del conductor. Nótese que $\mathfrak{f}(L/K) = 1$. Pero esto también es cierto para cualquier otra extensión abeliana no ramificada de K. O sea que si M es otra extensión de estas entonces $\mathfrak{f}(M/K)|\mathfrak{f}(L/K)$, y por la segunda parte del teorema del conductor esto implica que

$$P_{K,1} \subset \ker(\Phi_{M/K,1}).$$

Y como $\ker(\Phi_{L/K,1}) = P_K = P_{K,1}$ por construcción, entonces

$$\ker(\Phi_{L/K,1}) \subset \ker(\Phi_{M/K,1}).$$

Ahora hay que ver como se traduce esta condición para que $M \subset L$. Lo cual se hace gracias a la unicidad del teorema de existencia:

Corolario 4.3.1. *Sean L y M dos extensiones de K. Luego $M \subset L$ si y sólo si hay un módulo $\mathfrak{m}$ divisible por todos los primos de K que ramifican en L o en M, para el cual*

$$P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{L/K,\mathfrak{m}}) \subset \ker(\Phi_{M/K,\mathfrak{m}}).$$

Demostración. Si $M \subset L$ entonces se puede considerar

$$r : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$$

la restricción. Por la reciprocidad de Artin se puede tomar un módulo $\mathfrak{m}$ de modo que tanto $\ker(\Phi_{L/K,\mathfrak{m}})$ como $\ker(\Phi_{M/K,\mathfrak{m}})$ sean grupos de congruencia para $\mathfrak{m}$. De hecho alcanza que sólo lo sea $\ker(\Phi_{L/K,\mathfrak{m}})$, puesto que la unicidad del símbolo de Artin implica que $r \circ \Phi_{L/K,\mathfrak{m}} = \Phi_{M/K,\mathfrak{m}}$ y por lo tanto

$$P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{L/K,\mathfrak{m}}) \subset \ker(\Phi_{M/K,\mathfrak{m}});$$

lo cual, por otra parte, termina la prueba del directo.

Ahora asúmase $P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{L/K,\mathfrak{m}}) \subset \ker(\Phi_{M/K,\mathfrak{m}})$. El mapa

$$\Phi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$$

manda $\ker(\Phi_{M/K,\mathfrak{m}})$ en un subgrupo H de $\mathrm{Gal}(L/K)$. A su vez por la correspondencia de Galois, H se corresponde a un cuerpo intermedio $K \subset M' \subset L$, es decir $H = \mathrm{Gal}(L/M')$. Razonando como en el antes, si r es la restricción $\mathrm{Gal}(L/K)$ a $\mathrm{Gal}(M'/K)$ entonces $r \circ \Phi_{L/K,\mathfrak{m}} = \Phi_{M'/K,\mathfrak{m}}$. Luego la sobreyectividad de los mapas muestra que

$$\ker(\Phi_{M'/K,\mathfrak{m}}) = \Phi^{-1}_{L/K,\mathfrak{m}}(\ker(r)) = \Phi^{-1}_{L/K,\mathfrak{m}}(\mathrm{Gal}(L/M')) = \Phi^{-1}_{L/K,\mathfrak{m}}(H).$$

En particular $\ker(\Phi_{L/K,\mathfrak{m}} \subset \ker(\Phi_{M/K,\mathfrak{m}}) \subset \ker(\Phi_{M'/K,\mathfrak{m}})$. Ahora, al bajar todo módulo $\ker(\Phi_{L/K,\mathfrak{m}})$, como $\Phi_{L/K,\mathfrak{m}}$ es un isomorfismo, las igualdades anteriores se convierten en $\frac{\ker(\Phi_{M/K,\mathfrak{m}})}{\ker(\Phi_{L/K,\mathfrak{m}})} = \frac{\ker(\Phi_{M'/K,\mathfrak{m}})}{\ker(\Phi_{L/K,\mathfrak{m}})}$, y subiendo $\ker(\Phi_{M/K,\mathfrak{m}}) = \ker(\Phi_{M'/K,\mathfrak{m}})$. Luego, la unicidad del teorema de existencia fuerza a que $M = M'$. En tanto $M \subset L$. □

Además de proveer estos cuerpos, la reciprocidad de Artin también generaliza a la reciprocidad cuadrática y a otras reciprocidades que se definen para órdenes más grandes.

De hecho, el símbolo de Legendre no es más que un caso particular del símbolo de Artin. Si $K = \mathbb{Q}$, $L = K(\sqrt{p})$ y q es un primo de $\mathbb{Z}$ que no ramifica en L (que, por otra parte, son todos los primos enteros distintos de p), entonces por definición

$$\left(\frac{L/K}{q}\right)(\sqrt{p}) \equiv \sqrt{p}^{N(q)} \text{ mód } \mathfrak{Q}$$

siendo $\mathfrak{Q}$ un primo de L que cae sobre q. Luego

$$\left(\frac{L/K}{q}\right)(\sqrt{p}) \equiv p^{q/2} = p^{(q-1)/2}\sqrt{p} \text{ mód } \mathfrak{Q}.$$

Por el criterio de Euler $p^{q-1/2} \equiv \left(\frac{p}{q}\right)$ mód q (una prueba de este criterio puede encontrarse en el libro de Stein [18], Capítulo 6, Sección 6.2).

En suma

$$\left(\frac{L/K}{q}\right)(\sqrt{p}) \equiv \left(\frac{p}{q}\right)\sqrt{p} \text{ mód } \mathfrak{Q}.$$

Y como $((L/K)/q)(\sqrt{p})$ es $\pm\sqrt{p}$, entonces los factores anteriores son iguales. Más aún $((L/K)/q)(\sqrt{p})$ queda determinado por el valor que tome $\sqrt{p}$; de modo que en cierto sentido el mapa $((L/K)/\cdot)$ es $(p/\cdot)$.

Lo que agrega la reciprocidad de Artin es que este mapa sólo depende módulo p. Lo que es en definitiva, la reciprocidad cuadrática. Formalizando:

Ley de reciprocidad cuadrática. *Si p y q son primos impares, entonces*

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right).$$

Demostración. La reciprocidad cuadrática puede ser reescrita de la siguiente manera

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$

donde $p^* = (-1)^{p-1/2}p$ (para esta conversión hay que multiplicar a ambos lados por $(-1)^{p-1/2}$ y luego usar el criterio de Euler).

Ahora la idea de la demostración es probar que los símbolos $(p^*/\cdot)$ y $(\cdot/p)$ definen un mismo homomorfismo, a saber: el mapa de Artin de $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$.

Para entender esta última extensión se agranda a una extensión ciclotómica que resulta más manejable.

En concreto, es fácil ver que la extensión $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, donde ζ_p una raíz p-ésima de la unidad, es de Galois y su grupo de Galois es un grupo de clases de ideales generalizados para el módulo $p\infty$ (el ideal generado por p y todos los primos infinitos reales). De hecho se tiene $\ker(\Phi_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}, p\infty) = P_{\mathbb{Q},1}(p\infty)$ (ver la discusión siguiente al Teorema 8.2, en la Sección 8 del Cox [2]). Luego cualquier subcuerpo de números de $\mathbb{Q}(\zeta_p)$ también tendrá como grupo de Galois un grupo de clases de ideales para el módulo $p\infty$. Como la extensión $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es cíclica de orden $p-1$, entonces sólo hay un subcuerpo cuadrático $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_p)$. Aquí es donde entra $\mathbb{Q}(\sqrt{p^*})$, porque si $K = \mathbb{Q}(\sqrt{m})$ y el único primo entero que no ramifica en K es p (debido a que $\mathrm{Gal}(K/\mathbb{Q})$ es un grupo de clases de ideales para $p\infty$) entonces por lo visto en la Proposición 3.2.3 necesariamente $m = p$ o $-p$, y de hecho como $K \subset \mathbb{Q}(\zeta_p)$, el signo viene dado por $(-1)^{p-1/2}$.

Así $\ker(\Phi_{\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}}, p\infty)$ es un grupo de congruencias para el módulo $p\infty$. Por la discusión anterior el mapa de Artin de $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$ no es otra cosa que $(p^*/\cdot)$, y como $P_{\mathbb{Q},1}(p\infty) \subset \ker(\Phi_{\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}}, p\infty)$ este mapa se puede bajar al cociente por $P_{\mathbb{Q},1}(p\infty)$. Formalmente, $\Phi_{\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}}, p\infty$ induce un homomorfismo

$$I_{\mathbb{Q}}(p\infty)/P_{\mathbb{Q},1}(p\infty) \to \{\pm 1\}.$$

Además la reciprocidad de Artin también dice que este mapa es sobreyectivo.

Y como $I_{\mathbb{Q}}(p\infty)/P_{\mathbb{Q},1}$ es naturalmente isomorfo a $(\mathbb{Z}/p\mathbb{Z})^\times$ vía $[a] \in (\mathbb{Z}/p\mathbb{Z})^\times \mapsto [a\mathbb{Z}] \in I_{\mathbb{Q}}(p\infty)/P_{\mathbb{Q},1}$, entonces $(p^*/\cdot)$ define un homomorfismo sobreyectivo de $(\mathbb{Z}/p\mathbb{Z})^\times$ a $\{\pm 1\}$. Pero el símbolo de Legendre $(\cdot/p)$ también es un homomorfismo sobreyectivo entre estos grupos. Luego, el hecho de que $(\mathbb{Z}/p\mathbb{Z})^\times$ sea cíclica implica que

$$(p^*/\cdot) = (\cdot/p)$$

ya que sólo puede haber un homomorfismo de este tipo.

En particular

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

□

Capítulo 5

Órdenes en cuerpos cuadráticos

En este último capítulo se harán las adaptaciones correspondientes para generalizar el Teorema 2 a cualquier valor de n.

Lo único que impide usar la prueba hecha hasta ahora para solucionar $p = x^2 + ny^2$ es que los enteros algebraicos de $K = \mathbb{Q}(\sqrt{-n})$ no sean exactamente $\mathbb{Z}[\sqrt{-n}]$, que como se vio está vinculado con las condiciones de libertad de cuadrados y $n \not\equiv 3$ mód 4 del Teorema 2.

Pero para poder usar este teorema hay que verificar que los ideales principales de $\mathbb{Z}[\sqrt{-n}]$ son un grupo de clases de ideales generalizado. Por eso, antes que nada, es preciso estudiar los anillos $\mathbb{Z}[\sqrt{-n}]$ dentro de los enteros algebraicos de $\mathbb{Q}(\sqrt{-n})$. Dichos anillos son un caso particular de lo que es un *orden* en un cuerpo cuadráticos.

Por otra parte, los ideales de los órdenes cuadráticos guardan una relación biunívoca con las formas cuadráticas. Lo cual cierra el nexo entre el enfoque de la primera parte con el de la segunda de este trabajo. Porque a fin de cuentas, la teoría de cuerpos de clases usada en los cuerpos cuadráticos no es más que una generalización de teoría de formas cuadráticas.

5.1. Órdenes en cuerpos cuadráticos

Un *orden* en un cuerpo cuadrático K es un subconjunto $\mathcal{O} \subset K$ tal que

I. $\mathcal{O}$ es un subanillo de K que tiene al 1,

II. $\mathcal{O}$ es un $\mathbb{Z}$-módulo finitamente generado,

III. $\mathcal{O}$ contiene una $\mathbb{Q}$-base de K.

Es fácil ver a partir de estas condiciones que los órdenes son $\mathbb{Z}$-álgebras libres de rango 2 con cuerpo de fracciones K.

Luego los enteros algebraicos $\mathcal{O}_K$ son siempre un orden en K. De hecho, la condición de ser finitamente generado fuerza a un orden cualquiera $\mathcal{O}$ a que esté contenido en $\mathcal{O}_K$. O sea que $\mathcal{O}_K$ es el *orden máximo* de K.

Pero no siempre $\mathcal{O}_K$ va a ser el orden a trabajar. En el problema $p = x^2 + ny^2$ el orden que va interesar es $\mathbb{Z}[\sqrt{-n}]$ y éste, como se vio antes en la sección de cuerpos cuadráticos, no tiene por qué contener a todos los enteros algebraicos de $\mathbb{Q}(\sqrt{-n})$.

De hecho, por la Proposición 3.2.1, se sabe que si $K = \mathbb{Q}(\sqrt{N})$ (con $N \neq 0, 1$ libre de cuadrados) entonces $\mathcal{O}_K = \mathbb{Z}[\sqrt{N}]$ o $\mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right]$ según $N \not\equiv 1$ mód 4 o $N \equiv 1$ mód 4 respectivamente.

De todas formas, la base de un orden cualquiera se puede describir en un función de una base de $\mathcal{O}_K$:

Proposición 5.1.1. *Sea $\mathcal{O}$ un orden en un cuerpo cuadrático K. Entonces $\mathcal{O}$ tiene índice finito en $\mathcal{O}_K$, y más aún si $f = [\mathcal{O}_K : \mathcal{O}]$ entonces*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K.$$

Demostración. Que $\mathcal{O}$ tiene índice finito en $\mathcal{O}_K$ es inmediato a partir de que $\mathcal{O} \subset \mathcal{O}_K$ y que ambos son $\mathbb{Z}$-módulos libres de rango 2. Ahora si $f = [\mathcal{O}_K : \mathcal{O}]$, se sigue que $\mathbb{Z} + f\mathcal{O}_K \subset \mathcal{O}$. Pero, a causa de la estructura de $\mathcal{O}_K$ vista en la discusión anterior, $\mathbb{Z} + f\mathcal{O}_K$ tiene exactamente índice f. Luego $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$. □

El índice $f = [\mathcal{O}_K : \mathcal{O}]$ es llamado el *conductor* de $\mathcal{O}$. El orden $\mathbb{Z}[\sqrt{-n}]$ por ejemplo, cuando n es libre de cuadrados, tiene conductor 1 o 2 según sea o no el orden máximo.

Ahora, para calcular una base de $\mathcal{O}_K$ no hay más que mirar los resultados de la Proposición 3.2.1, que pueden expresarse de manera uniforme: si $K = \mathbb{Q}(\sqrt{N})$, entonces llamando

$$d_K := \begin{cases} 4N & \text{si } N \not\equiv 1 \text{ mód } 4 \\ N & \text{si } N \equiv 1 \text{ mód } 4 \end{cases} \quad \text{y } w_K := \frac{d_K + \sqrt{d_K}}{2},$$

se obtiene que $\{1, w_K\}$ es una base para $\mathcal{O}_K$.

Y con la proposición anterior se consigue la base $\{1, fw_K\}$ para $\mathcal{O}$.

El otro invariante, además del índice, de $\mathcal{O}$ es su *discriminante*, definido la siguiente manera: sea $\alpha \mapsto \alpha'$ el automorfismo no trivial de K; si $\{\alpha, \beta\}$ es una base de entonces el discriminante de $\mathcal{O}$ es el número

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

Y como las matrices de cambio de base tienen determinante 1, entonces se sigue que este número no depende de la base elegida. Por ejemplo con $\{1, fw_K\}$ se obtiene que el discriminante de $\mathcal{O}$ es

$$D = f^2 d_K.$$

Así, no es difícil ver que el discriminante D caracteriza de forma única al orden $\mathcal{O}$ en K. En particular $\mathbb{Z}[\sqrt{-n}]$ es el único orden de discriminante $-4n$ en $\mathbb{Q}(\sqrt{-n})$.

El siguiente asunto a explorar es que sucede con los ideales en un orden arbitrario $\mathcal{O}$. La realidad no es muy distinta que en $\mathcal{O}_K$, dado que todo orden tiene dos de las tres propiedades de un dominio de Dedekind. Es decir $\mathcal{O}$ sigue siendo un $\mathbb{Z}$-módulo libre de rango finito y en consecuencia todos los ideales $\mathfrak{a}$ son finitamente generados y sus cocientes $\mathcal{O}/\mathfrak{a}$ son finitos (aquí también se define la norma como siendo $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$). La diferencia se puede presentar en la integridad sobre K, pues cuando el conductor f de $\mathcal{O}$ es mayor a 1 entonces por ejemplo el polinomio $x^2 - d_K$ no tiene raíces en $\mathcal{O}$ por lo que dicho orden no es integralmente cerrado. Esta última variación impide asumir la factorización en primos sobre los ideales de $\mathcal{O}$; lo cual genera un problema cuando se quiere usar el símbolo de Artin con estos ideales. Y visto que la reciprocidad de la teoría de cuerpos de clases es imprescindible para resolver el problema $p = x^2 + ny^2$, resulta imperioso encontrar una solución a este inconveniente.

Lo que se hace para esto es, primeramente, restringirse a los ideales *propios* de $\mathcal{O}$. Por definición, para cualquier ideal $\mathfrak{a}$ se cumple que

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

Pero no siempre estos conjuntos son iguales. Por ejemplo, para el orden $\mathbb{Z}[\sqrt{-3}]$ del cuerpo $\mathbb{Q}(\sqrt{-3})$, se puede ver que el ideal $\mathfrak{a}$ generado por 2 y $1 + \sqrt{-3}$ cumple que el conjunto $\{\beta \in \mathbb{Q}(\sqrt{-3}) : \beta\mathfrak{a} \subset \mathfrak{a}\}$ es de hecho el orden máximo (que es mayor a $\mathbb{Z}[\sqrt{-3}]$).

En general un ideal $\mathfrak{a}$ se dice *propio* cuando se cumple la igualdad, es decir cuando

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

Los ideales propios son especialmente buenos porque son los únicos que se pueden invertir y así formar un grupo. Aunque que claro que para esto hay volver a trabajar con los *ideales fraccionales* pero ahora de $\mathcal{O}$, que como antes son los $\mathcal{O}$-submódulos de K finitamente generados. Al igual que antes, se puede ver que estos ideales fraccionales son de la forma $\alpha\mathfrak{a}$ donde $\mathfrak{a}$ es un ideal de $\mathcal{O}$ y $\alpha \in K^\times$. El concepto de ser propio es el mismo para un ideal fraccional $\mathfrak{b}$, es decir es propio si

$$\mathcal{O} = \{\beta \in K : \beta\mathfrak{b} \subset \mathfrak{b}\}.$$

Por último un ideal fraccional $\mathfrak{a}$ es *invertible* si existe otro $\mathfrak{b}$ tal que $\mathfrak{ab} = \mathcal{O}$.

Proposición 5.1.2. *En un orden $\mathcal{O}$ de un cuerpo cuadrático K, los ideales (fraccionales) propios y los invertibles son los mismos.*

Demostración. Si es $\mathfrak{a}$ es un ideal invertible, entonces por definición existe un ideal $\mathfrak{b}$ tal que $\mathfrak{ab} = \mathcal{O}$. Luego si $\beta \in K$ es tal que $\beta\mathfrak{a} \subset \mathfrak{a}$ entonces

$$\beta\mathcal{O} = \beta\mathfrak{ab} \subset \mathfrak{ab} = \mathcal{O},$$

y se sigue que $\beta \in \mathcal{O}$. Así, $\mathfrak{a}$ es propio.

Para ver que los ideales propios son invertibles antes hay que probar el siguiente lema:

Lema 5.1.3. *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 enteros relativamente primos. Luego $[1, \tau]_{\mathbb{Z}}$ es un ideal propio del orden $[1, a\tau]_{\mathbb{Z}}$ de K.*

Demostración. Dado $\beta \in K$, $\beta[1, \tau] \subset [1, \tau]$ es equivalente a

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

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

$$\beta\tau = m\tau + n\tau^2 = m\tau + \frac{n}{a}(-b\tau - c) = \frac{-cn}{a} + \left(\frac{-bn}{a} + m\right)\tau.$$

Y como a, b y c son coprimos entonces $\beta \cdot \tau \subset [1, \tau]$ si y sólo si $n \mid a$ o mejor dicho

$$\left\{\beta \in K : \beta[1, \tau] \subset [1, \tau]\right\} = [1, a\tau].$$

□

Sea ahora $\mathfrak{a}$ un ideal propio de $\mathcal{O}$. La idea es escribir a $\mathfrak{a}$ de la forma $[1, \tau]$ como en el lema y luego usar el mismo lema para afirmar que el conjugado $[1, \tau']$ es su inverso. Porque si τ y τ' son las raíces de $ax^2 + bx + c$ entonces usando la relación entre coeficientes y raíces y suponiendo $mcd(a, b, c) = 1$ se tiene que

$$a[1, \tau][1, \tau'] = a[1, \tau, \tau', \tau\tau'] = [a, a\tau, -b, c] = [1, a\tau].$$

Ahora para empezar, es fácil ver que $\mathfrak{a}$ es un $\mathbb{Z}$-módulo libre de rango 2; luego existen $\alpha, \beta \in K$ tales que $\{\alpha, \beta\}$ es una $\mathbb{Z}$-base de $\mathfrak{a}$. Así $\tau = \beta/\alpha$ no puede ser racional, y su polinomio racional sobre $\mathbb{Z}$ tiene que ser de la forma $ax^2 + bx + c$. Sin perder generalidad se puede suponer que a, b y c son coprimos. Por otra parte $\mathfrak{a} = [\alpha, \beta] = \alpha[1, \tau]$. En suma, por el lema anterior, $\mathfrak{a}$ es un ideal propio de $[1, a\tau]$. Así $\mathcal{O} = [1, a\tau]$. Luego tomando τ' como antes y α' el conjugado de α (todo por el automorfismo no trivial de K) se tiene que $\mathfrak{a}' = \alpha'[1, \tau']$ cumple que

$$a\mathfrak{a}\mathfrak{a}' = \alpha\alpha'\mathcal{O}$$

por las cuentas anteriores. Así, $\mathfrak{a}$ es invertible. □

Ahora, se puede volver a definir un grupo para los ideales de un orden $\mathcal{O}$, a saber: el de los ideales propios, que se denota por $I(\mathcal{O})$. El subgrupo que más va interesar es $P(\mathcal{O})$ de los ideales principales (que son siempre propios), es decir los de la forma $\alpha\mathcal{O}$ con $\alpha \in K^\times$. Así, el *grupo de clases de ideales* de $\mathcal{O}$ queda definido por

$$C(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O}).$$

Es fácil ver que cuando $\mathcal{O}$ es el orden máximo $\mathcal{O}_K$, todos los ideales son propios y por eso las definiciones de estos grupos coinciden con las dadas en el capítulo 3. Es decir $I(\mathcal{O}_K) = I_K$ y $P(\mathcal{O}_K) = P_K$. Y de hecho las razones de trabajar con estos grupos son las mismas que antes: recuérdese que en el orden $\mathbb{Z}[\sqrt{-n}]$ los ideales principales son exactamente los que se precisan para resolver el problema $p = x^2 + ny^2$.

5.2. Ideales coprimos al conductor

Lo que aún no sucede en general para los ideales de $I(\mathcal{O})$ de un orden cualquiera, es la factorización única en primos. A modo de ejemplo en $\mathbb{Z}[\sqrt{-3}]$, el ideal generado por 4 cumple que

$$(4) = (2)(2) = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

y no hay forma de convertir los factores de una descomposición a otra. De hecho por esto, ni siquiera se puede decir de ninguno de esos factores que sean primos.

A modo general el problema que presenta un orden $\mathcal{O}$ (distinto del máximo) son los ideales que tienen como factor al conductor f, ya que estos no admiten factorización única en primos y por tanto no pueden adaptarse como ideales de $\mathcal{O}_K$.

Para poder hacer factorización es preciso restringirse a un conjunto más pequeño de ideales. Con este fin se definen los ideales coprimos al conductor: se dice que un $\mathcal{O}$-ideal $\mathfrak{a}$ es *coprimo al conductor* f si

$$\mathfrak{a} + f\mathcal{O} = \mathcal{O}.$$

Otra forma de caracterizar a los ideales coprimos al conductor f es por su norma:

Proposición 5.2.1. *Un ideal de $\mathcal{O}$ es coprimo a f si y sólo si lo es su norma.*

Demostración. Dado un ideal $\mathfrak{a}$, la multiplicación por f, $m_f : \mathcal{O}/\mathfrak{a} \to \mathcal{O}/\mathfrak{a}$, es un homomorfismo de grupos finitos. Pero más interesante aún

$$m_f \text{ es un isomorfismo} \iff \mathfrak{a} \text{ es propio},$$

pues

$$\begin{array}{rcl} m_f \text{ es un isomorfismo} & \iff & m_f \text{ es sobreyectivo y} \\ m_f \text{ es sobreyectivo} & \iff & \mathfrak{a} + f\mathcal{O} = \mathcal{O}. \end{array}$$

Y por el teorema de estructura para grupos abelianos finitos se sabe que la multiplicación por f es un isomorfismo si y sólo si f es relativamente primo al orden del grupo, es decir en este caso a $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$. □

Luego los ideales coprimos al conductor son cerrados bajo multiplicación (porque la norma es multiplicativa). Esto permite encerrarlos en un monoide. Pero para darle una estructura de grupo hay que verificar que estos ideales sean en efecto invertibles, o en otras palabras propios.

Lema 5.2.2. *Todos los $\mathcal{O}$-ideales coprimos al conductor f son propios.*

Demostración. Sea $\mathfrak{a}$ un ideal de $\mathcal{O}$ coprimo con f y sea $\beta \in K$ tal que $\beta\mathfrak{a} \subset \mathfrak{a}$. Luego β tiene que ser entero algebraico de K, es decir $\beta \in \mathcal{O}_K$; y así

$$\beta\mathcal{O} = \beta(\mathfrak{a} + f\mathcal{O}) = \beta\mathfrak{a} + \beta f\mathcal{O} \subset \mathfrak{a} + f\mathcal{O}_K.$$

Y como $f\mathcal{O}_K \subset \mathcal{O}$, entonces $\beta\mathcal{O} \subset \mathcal{O}$. Luego $\beta \in \mathcal{O}$, lo que prueba que $\mathfrak{a}$ es propio. □

Así se define el subgrupo $I(\mathcal{O}, f)$ de $I(\mathcal{O})$ generado por los ideales coprimos al conductor. De forma intuitiva se puede pensar a los ideales fraccionales de $I(\mathcal{O}, f)$ como los ideales que no tienen ninguna potencia, positiva o negativa, de f. Por ejemplo en $\mathbb{Z}[\sqrt{-3}]$ se sacan todos los ideales múltiplos de (2). Esto a su vez hace desaparecer el inconveniente que había con (20) porque el ideal deja de ser considerado. Más aún, cómo se verá en la siguiente sección, al quitar estos ideales se puede hacer factorización sin problemas.

Y lo bueno es que $I(\mathcal{O}, f)$ es lo suficientemente grande como para que cualquier ideal de $I(\mathcal{O})$ se vea representado allí. O sea que a menos de una multiplicación por un escalar, cualquier ideal propio de $\mathcal{O}$ puede ser visto como un ideal coprimo con el conductor. Formalizando:

Proposición 5.2.3. *La inclusión $I(\mathcal{O}, f) \subset I(\mathcal{O})$ induce un isomorfismo*

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \backsimeq I(\mathcal{O})/P(\mathcal{O}) = C(\mathcal{O}),$$

donde el grupo $P(\mathcal{O}, f)$ es el generado por los ideales principales $\alpha\mathcal{O}$, $\alpha \in \mathcal{O}$, coprimos con f.

Demostración. Eventualmente multiplicando por una potencia de f, todo ideal fraccional de $\mathcal{O}$ es equivalente a uno propio. Es decir el mapa $I(\mathcal{O}, f) \to C(\mathcal{O})$, inducido por la inclusión, es sobreyectivo.

Además es un homomorfismo con núcleo $I(\mathcal{O}, f) \cap P(\mathcal{O})$. Es fácil ver que $P(\mathcal{O}, f) \subset I(\mathcal{O}, f) \cap P(\mathcal{O})$. Para probar la otra inclusión, sea $\alpha\mathcal{O} = \mathfrak{a}\mathfrak{b}^{-1}$ un elemento de $I(\mathcal{O}, f) \cap P(\mathcal{O})$ donde $\alpha \in K^\times$ y $\mathfrak{a}, \mathfrak{b}$ son coprimos a f. Sea

$m = N(\mathfrak{b})$. Luego $m\mathcal{O} = N(\mathfrak{b})\mathcal{O} = \mathfrak{b}\mathfrak{b}'$, siendo $\mathfrak{b}'$ el conjugado de $\mathfrak{b}$ por el automorfismo no trivial de K. Así $m\mathfrak{b}^{-1} = \mathfrak{b}'$. Pero entonces

$$m\alpha\mathcal{O} = m\mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{a}\mathfrak{b}'$$

que es un $\mathcal{O}$-ideal con norma coprima a f. O sea $m\alpha\mathcal{O} \in P(\mathcal{O}, f)$ y en consecuencia también $\alpha\mathcal{O} = m\alpha\mathcal{O}(m\mathcal{O})^{-1} \in P(\mathcal{O}, f)$. □

5.3. El cuerpo de clases de anillo

Lo que queda por hacer para reformular el Teorema 2 en el caso general, es convertir el grupo de clases de ideales de un orden arbitrario $\mathcal{O}$ en un grupo de clases de ideales generalizado (en el sentido de la teoría de cuerpos de clases). O sea que lo que hay que hacer es trasladar los ideales propios de $\mathcal{O}$ en términos de ideales del orden máximo $\mathcal{O}_K$. Y son precisamente los ideales coprimos al conductor los encargados de hacer este pasaje.

Proposición 5.3.1. *Sea $\mathcal{O}$ un orden con conductor f en un cuerpo cuadrático K.*

I. *Si $\mathfrak{a}$ es un ideal de $\mathcal{O}_K$ coprimo a f entonces $\mathfrak{a} \cap \mathcal{O}$ es un ideal de $\mathcal{O}$ coprimo a f y más aún de la misma norma.*

II. *Si $\mathfrak{a}$ es un ideal de $\mathcal{O}$ coprimo a f entonces $\mathfrak{a}\mathcal{O}_K$ es un ideal de $\mathcal{O}_K$ coprimo a f y más aún de la misma norma.*

III. *El mapa $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ define un isomorfismo de grupos $I(\mathcal{O}, f) \backsimeq I_K(f)$ con inverso $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$.*

Demostración. i. Si $\mathfrak{a}$ es un ideal de $\mathcal{O}_K$ es inmediato que $\mathfrak{a} \cap \mathcal{O}$ es un ideal de $\mathcal{O}$. Para ver que $\mathfrak{a} \cap \mathcal{O}$ es coprimo a f, siendo que $\mathfrak{a}$ lo es, basta ver que el cociente $\mathcal{O}/\mathfrak{a} \cap \mathcal{O}$ se inyecta por la inclusión en $\mathcal{O}_K/\mathfrak{a}$ y por tanto $N(\mathfrak{a} \cap \mathcal{O})$ es coprimo a f. Para las normas, considérese la multiplicación por f

$$\mathcal{O}/\mathfrak{a} \cap \mathcal{O} \longrightarrow \mathcal{O}_K/\mathfrak{a}$$

define un mapa inyectivo. Más aún como $f\mathcal{O}_K \subset \mathcal{O}$ entonces el mapa también es sobreyectivo y en suma las normas de $\mathfrak{a}$ y $\mathfrak{a} \cap \mathcal{O}$ son iguales.

ii. Si $\mathfrak{a}$ es un ideal de $\mathcal{O}$ coprimo a f entonces $\mathfrak{a}\mathcal{O}_K$ es un ideal de $\mathcal{O}_K$ tal que

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

es decir que es coprimo a f. La igualdad de normas se sigue de la misma cuenta de la parte anterior.

iii. Visto las partes anteriores, lo que resta probar es que

$$\begin{aligned} \mathfrak{a}\mathcal{O}_K \cap \mathcal{O} &= \mathfrak{a} \quad \text{para todo ideal } \mathfrak{a} \text{ de } \mathcal{O} \\ (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K &= \mathfrak{a} \quad \text{para todo ideal } \mathfrak{a} \text{ de } \mathcal{O}_K. \end{aligned}$$

Para la primera igualdad, si $\mathfrak{a}$ es un ideal de $I(\mathcal{O}, f)$, nótese primero que la inclusión $\mathfrak{a} \subset \mathfrak{a}\mathcal{O}_K \cap \mathcal{O}$ es obvia. En la otra dirección

$$\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} = (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})\mathcal{O} = (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})(\mathfrak{a} + f\mathcal{O}) \subset \mathfrak{a} + f(\mathfrak{a}\mathcal{O}_K \cap \mathcal{O}) \subset \mathfrak{a} + \mathfrak{a}f\mathcal{O}_K$$

y esto último está contenido en $\mathfrak{a}$ ya que $f\mathcal{O}_K \subset \mathcal{O}$.

Para la segunda igualdad, si $\mathfrak{a}$ es un ideal de $I_K(f)$, la inclusión obvia es $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K \subset \mathfrak{a}$. En la otra dirección

$$\mathfrak{a} = \mathfrak{a}\mathcal{O} = \mathfrak{a}(\mathfrak{a} \cap \mathcal{O} + f\mathcal{O}) \subset (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K + f\mathfrak{a}.$$

Y luego como $f\mathfrak{a} \subset f\mathcal{O}_K \subset \mathcal{O}$, entonces $f\mathfrak{a} \subset \mathfrak{a} \cap \mathcal{O} \subset (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K$ y en suma $\mathfrak{a} \subset (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K$.

Por último, para ver que $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ es un homomorfismo de grupos alcanza con ver que

$$(\mathfrak{a}\mathfrak{b}) = \mathfrak{a}\mathcal{O}_K \cdot \mathfrak{b}\mathcal{O}_K.$$

□

En particular, este resultado permite hacer factorización en los ideales coprimos al conductor y por consiguiente habilita el uso del símbolo de Artin sobre todos estos ideales. De todas formas, para completar el vínculo entre el grupo de clases de ideales $C(\mathcal{O})$ y los grupos de clases generalizados, hay que ver que esta correspondencia entre $I(\mathcal{O}, f)$ y $I_K(f)$ es lo suficientemente buena como para que al pasar al cociente $I(\mathcal{O}, f)/P(\mathcal{O}, f)$ quede isomorfo a un grupo de clases generalizado. O dicho de otro modo lo que hay que verificar es que el subgrupo $P(\mathcal{O}, f)$ va a parar a un grupo de congruencias.

Proposición 5.3.2. *La imagen de $P(\mathcal{O}, f)$ por el isomorfismo de la proposición anterior, es $P_{K,\mathbb{Z}}(f)$ el grupo generado por los ideales principales $\alpha\mathcal{O}_K$ donde $\alpha \in \mathcal{O}_K$ y $\alpha \equiv a \bmod f\mathcal{O}_K$ para algún $a \in \mathbb{Z}$ coprimo con f. Así*

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \backsimeq I_K(f)/P_{K,\mathbb{Z}}(f).$$

Demostración. El isomorfismo de la proposición anterior lleva ideales de $I(\mathcal{O}, f)$ en ideales de $I_K(f)$ mediante $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$. Luego mirando los generadores $P(\mathcal{O}, f)$ y $P_{K,\mathbb{Z}}(f)$, se ve que el teorema se sigue de las siguientes equivalencias: si $\alpha \in \mathcal{O}_K$ entonces

$$\alpha \equiv a \bmod f\mathcal{O}_K, a \in \mathbb{Z}, mcd(a, f) = 1 \iff \alpha \in \mathcal{O}, mcd(N(\alpha), f) = 1,$$

siendo $N(\alpha)$ el producto $\alpha\alpha'$ donde α' es el conjugado de α por el automorfismo no trivial. De hecho puede probarse que $N(\alpha)$ es la norma del ideal $\alpha\mathcal{O}$.

Ahora, para probar el directo, supóngase que $\alpha \equiv a \bmod f\mathcal{O}_K$ donde a es un entero relativamente primo a f. Haciendo cuentas se sigue que $N(\alpha) \equiv a^2 \bmod f\mathcal{O}_K$ y por tanto $N(\alpha)$ también es coprimo con f. En la otra dirección, nótese que si $\alpha \in \mathcal{O} = [1, fw_K]$ cumple que $mcd(N(\alpha), f) = 1$ entonces necesariamente $\alpha \equiv a \bmod f\mathcal{O}_K$ con $a \in \mathbb{Z}$ y $mcd(a, f) = 1$. □

Corolario 5.3.3. *Sea $\mathcal{O}$ un orden con conductor f en un cuerpo cuadrático K. Entonces $C(\mathcal{O})$ es (naturalmente) isomorfo a $I_K(f)/P_{K,\mathbb{Z}}(f)$.*

Demostración. Es inmediato a partir del isomorfismo de la sección anterior $C(\mathcal{O}) \backsimeq I(\mathcal{O}, f)/P(\mathcal{O}, f)$ de la sección anterior dado por la Proposición 5.2.3, y el isomorfismo $I(\mathcal{O}, f)/P(\mathcal{O}, f) \backsimeq I_K(f)/P_{K,\mathbb{Z}}(f)$ de la proposición anterior. □

Volviendo a las definiciones en el capítulo de la teoría de cuerpos de clases, es claro que

$$P_K(f) \subset P_{K,\mathbb{Z}}(f) \subset I_K(f)$$

y que por lo tanto $I_K(f)/P_{K,\mathbb{Z}}(f)$ es un grupo de clases generalizado (en este caso para el módulo $f\mathcal{O}_K$). O sea que en efecto los grupos de clases de ideales de ordenes arbitrarios pueden verse como un grupo de clases de ideales generalizado.

De este modo, dado un orden $\mathcal{O}$ de K, el teorema de existencia da una extensión L correspondiente al grupo $C(\mathcal{O})$, en el sentido de que el grupo de Galois $\mathrm{Gal}(L/K)$ es isomorfo por el mapa Artin a $C(\mathcal{O})$. Este cuerpo L se llama el *cuerpo de clases de ideales* del orden $\mathcal{O}$. La reciprocidad de Artin le da las propiedades deseadas a este nuevo cuerpo, porque ahora los primos de K que descomponen completamente en L son exactamente aquellos que pueden escribirse como un ideal principal de $\mathcal{O}$. Por otra parte, los primos que ramifican deben dividir al conductor $\mathfrak{f}(L|K)$ que es exactamente el conductor $f = [\mathcal{O}_K : \mathcal{O}]$ ya que el grupo de clases asociado a $\mathcal{O}$ es $I_K(f)/P_{K,\mathbb{Z}}(f)$.

5.4. Solución de $p = x^2 + ny^2$ para todo n

Hechas todas las consideraciones correspondientes, sólo resta adaptar las pruebas del capítulo anterior al caso general de $p = x^2 + ny^2$.

Teorema 5.4.1. *Sea n un entero positivo cualquiera, y sea L el cuerpo de clases de ideales del orden $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ en el cuerpo cuadrático $K = \mathbb{Q}(\sqrt{-n})$. Si p es un primo que no divide a $4n$, entonces*

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

Al igual que antes, hay que verificar primero que L es una extensión de Galois sobre $\mathbb{Q}$.

Lema 5.4.2. *Sea L el cuerpo de clases de ideales de un orden $\mathcal{O}$ en un cuerpo cuadrático imaginario K, y sea τ la conjugación compleja. Luego $\tau(L) = L$ y, al igual que en el Lema 4.2.1, L es Galois sobre $\mathbb{Q}$.*

Demostración. La igualdad $\tau(L) = L$ se sigue de que L y $\tau(L)$ son el cuerpo dado por el Teorema de existencia para un mismo grupo de congruencia del módulo $f\mathcal{O}_K$ (siendo f el conductor de $\mathcal{O}$).

La clave está en que el conjunto de los ideales coprimos al conductor $I_K(f)$ es cerrado por la conjugación compleja τ. En particular esto implica que los primos de K que ramifican en $\tau(L)$ son los mismos que los que lo hacen en L. Luego es casi inmediato a partir de la unicidad del símbolo de Artin que

$$\Phi_{\tau(L)/K}(\tau(\mathfrak{a})) = \tau\Phi_{L/K}(\mathfrak{a})\tau^{-1}$$

para todo ideal $\mathfrak{a}$ de $I_K(f)$. Y entonces

$$\ker(\Phi_{\tau(L)/K}) = \tau(\ker(\Phi_{L/K})) = \tau(P_K(f)) = P_K(f) = \ker(\Phi_{L/K}).$$

□

Demostración del Teorema 5.4.1. De nuevo, el teorema se sigue de las equivalencias

$$\begin{aligned} p = x^2 + ny^2 &\iff p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}', \text{ y } \mathfrak{p} = \alpha\mathcal{O}_K \text{ con } \alpha \in \mathcal{O} \\ &\iff p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}', \text{ y } \mathfrak{p} \text{ descompone completamente en } L \\ &\iff p \text{ descompone completamente en } L. \end{aligned}$$

La única novedad se presenta en la condición $\mathfrak{p} = \alpha\mathcal{O}_K$ con $\alpha \in \mathcal{O}$, y la misma se debe a la correspondencia entre $C(\mathcal{O})$ e $I_K(f)/P_K(f)$ de la sección anterior (f es el conductor de $\mathcal{O}$). O sea esta hipótesis es equivalente a $\mathfrak{p} \in P_K(f)$ (aquí también hay que usar que $p = N(\mathfrak{p})$ no divide a f, dado que no divide a $-4n = fd_K$), lo cual es obviamente equivalente a que $\mathfrak{p}$ descomponga completamente en L. □

Ahora volviendo a usar la Proposición 4.2.3 se obtiene el teorema final de la introducción 1 en toda su generalidad.

Teorema 1. *Sea n un entero positivo cualquiera. Entonces existe un polinomio entero mónico irreducible $f_n(x)$ tal que si p es un primo que no divide ni a $4n$ ni al discriminante de $f_n(x)$ se cumple que*

$$p = x^2 + ny^2 \iff \begin{cases} \left(\frac{-n}{p}\right) = 1 \text{ y} \\ f_n(x) \equiv 0 \text{ mód } p \text{ tiene solución entera.} \end{cases}$$

Esto libera las soluciones en los casos $p = x^2 + ny^2$ que quedaron sin resolver, es decir cuando $n \equiv 3$ mód 4 o cuando n no es libre de cuadrados. Ahora para buscar los respectivos cuerpos de clases es necesario conocer algo acerca de ellos.

Al igual que antes a partir del Teorema 5.5.1, se obtiene que el tamaño de la extensión del cuerpo de clases para el orden $\mathbb{Z}[\sqrt{-n}]$ en $\mathbb{Q}(\sqrt{-n})$ es igual a $h(-4n)$. También es posible conocer la forma del grupo de Galois

del cuerpo de clases sobre $\mathbb{Q}$. En concreto, la construcción del Lema 4.2.1 muestra que el grupo de Galois de un cuerpo de clases L sobre $\mathbb{Q}$ es un producto semidirecto

$$\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Gal}(L/K) \rtimes \mathrm{Gal}(K/\mathbb{Q})$$

donde K es el cuerpo cuadrático imaginario que extiende L.

Para ver la utilidad de esto en la práctica considérese el ejemplo de Gauss $p = x^2 + 27y^2$.

5.4.1. Ejemplo $p = x^2 + 27y^2$

De lo anterior si L es el correspondiente cuerpo de clases para el orden $\mathbb{Z}[\sqrt{-27}]$, entonces como $h(-4 \cdot 27) = 3$, el grupo de Galois de L sobre $\mathbb{Q}$ tiene que ser $C_3 \rtimes C_2 \simeq S_3$.

Por otra parte y antes que esto, se puede decir que como la extensión L/K es cíclica de grado 3, L tiene que ser la forma $K(\sqrt[3]{\alpha})$ para cierto α libre de cubos en K (esto es un corolario del Teorema de la base normal, que puede leerse en el libro de Milne [16], Capítulo 5, página 63). Ahora que el grupo de Galois de L sobre $\mathbb{Q}$) sea S_3 muestra que α puede ser visto como un entero libre de cubos m (ver Cox [2], Sección 9, Lema 9.6).

Lo que puede ser distinto en este y todos los casos nuevos considerados de $p = x^2 + ny^2$ es la ramificación: cuando el conductor f del orden $\mathbb{Z}[\sqrt{-n}]$ en el cuerpo $K = \mathbb{Q}(\sqrt{-n})$ es mayor a 1, los divisores primos de $f\mathcal{O}_K$ podrían ramificar en el correspondiente cuerpo de clases L, pero son los únicos con esa chance (recordar la construcción del cuerpo de clases luego del Corolario 5.3.3).

Luego como para el orden $\mathbb{Z}[\sqrt{-27}]$ el conductor es 6, las posibilidades del cuerpo de clases $L = K(\sqrt[3]{m})$ se reducen a sólo cuatro:

$$K(\sqrt[3]{2}), K(\sqrt[3]{3}), K(\sqrt[3]{6}), K(\sqrt[3]{12}).$$

Esto quiere decir que el polinomio $f_{27}(x)$ asociado a L tiene que ser uno de la lista

$$x^3 - 2, x^3 - 3, x^3 - 6, x^3 - 12.$$

Ahora para saber cuáles de estos polinomios pueden ser se utiliza que el hecho de que si lo fuesen entonces cumplirían con las equivalencias del Teorema 5.5.1. En este caso, por ejemplo $x^3 - 3$ no puede ser dicho polinomio ya que $31 = 2^2 + 27 \cdot 1^2$ pero $x^3 - 3$ no tiene raíces enteras módulo 31. De la misma manera se descartan $x^3 - 6$ y $x^3 - 12$, por lo que $f_{27}(x) = x^3 - 2$. Es decir

$$p = x^2 + 27y^2 \iff \begin{cases} \left(\frac{-27}{p}\right) = 1 \\ x^3 - 2 \equiv 0 \text{ mód } p \quad \text{tiene solución entera.} \end{cases}$$

Con este tipo de herramientas se puede reducir los candidatos de cuerpos de clases para un orden a una cantidad finita. Luego se constata cuál de los correspondientes polinomios cumple la equivalencia del Teorema 5.5.1 y así se obtienen resultados concretos para la solución de $p = x^2 + ny^2$.

5.5. Órdenes y formas cuadráticas

Hay algo subyacente, hasta ahora no mencionado, en la construcción de todos los cuerpos de clases construidos como ejemplos, y es la estructura del grupo de ideales correspondiente. Algo parecido pasaba en la primera parte cuando, en el fondo, todo se reducía a la estructura de las formas cuadráticas. Esta coincidencia no es una casualidad. Se debe a que estas estructuras están estrechamente relacionadas. De hecho son la misma:

Teorema 5.5.1. *Sea $\mathcal{O}$ un orden de discriminante D en un cuerpo cuadrático imaginario K.*

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

II. *El mapa que manda $f(x,y)$ en $[a, (-b+\sqrt{D})/2]$ define una biyección entre las clases de las formas primitivas y definidas positivas de discriminante D y el grupo de clases de ideales de $\mathcal{O}$.*

III. *Un entero positivo m es representado por una forma $f(x,y)$ si y sólo si m es la norma $N(\mathfrak{a})$ de un ideal $\mathfrak{a}$ de $\mathcal{O}$ en la clase de ideales correspondiente a $f(x,y)$.*

Demostración. Sea $f(x,y) = ax^2 + bxy + cy^2$ una forma primitiva definida positiva de discriminante D.

De que $f(x,y)$ sea definida positiva se sigue que las raíces de $f(x,1) = ax^2 + bx + c$ son complejas, y por tanto hay un único $\tau \in \mathbb{H}$ (el semiplano superior complejo) tal que $f(\tau, 1) = 0$. Se dice que τ es la "raíz"de $f(x,y)$. A causa de que $f(x,y)$ es discriminante D, se tiene que $D = b^2 - 4ac$ y por consiguiente $\tau = \frac{-b+\sqrt{D}}{2a}$. Luego

$$[a, (-b+\sqrt{D})/2] = [a, a\tau] = a[1, \tau].$$

Por el Lema 5.1.3, esto implica que $[a, (-b+\sqrt{D})/2]$ es un ideal de $[1, a\tau]$. De cualquier forma, considerando que $D = f^2 d_K$ con f el conductor de $\mathcal{O}$, se tiene que

$$a\tau = \frac{-b+\sqrt{D}}{2} = \frac{-b+f\sqrt{d_K}}{2} = -\frac{b+D}{2} + \frac{fd_K + f\sqrt{d_K}}{2} = -\frac{b+D}{2} + fw_K.$$

Y como $D = b^2 - 4ac$ y b tienen la misma paridad, entonces $\frac{b+D}{2} \in \mathbb{Z}$ y por lo tanto $[1, a\tau] = [1, fw_K] = \mathcal{O}$. Lo cual prueba el primer punto.

Para probar que esta correspondencia es inyectiva, por la cuenta anterior, alcanza con probar que si $f(x, y)$ y $g(x, y)$ dos formas definidas positivas de determinante D y con raíces τ y τ' entonces

$$f(x, y) \text{ y } g(x, y) \text{ son propiamente equivalentes} \iff [1, \tau] = \lambda[1, \tau'], \lambda \in K^\times.$$

Esto es fácil ver a través de una tercera afirmación equivalente:

$$\tau' = \frac{p\tau + q}{r\tau + s}, \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Es decir si $f(x, y)$ y $g(x, y)$ son propiamente equivalentes entonces por definición $f(x, y) = (px + qy, rx + sy)$, donde $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$; así

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

por lo que $\frac{p\tau+q}{r\tau+s}$ es raíz de $g(x, 1)$ y como además está en $\mathbb{H}$ entonces $\tau' = \frac{p\tau+q}{r\tau+s}$. Recíprocamente y por la misma cuenta, si $\tau' = \frac{p\tau+q}{r\tau+s}$ entonces $f(x, y)$ y $g(px + qy, rx + sy)$ tienen la misma raíz τ y por tanto son iguales, o sea $f(x, y)$ y $g(x, y)$ son propiamente equivalentes.

También si $\tau' = \frac{p\tau+q}{r\tau+s}$ entonces definiendo $\lambda := r\tau + s$ se cumple que

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

ya que $ps - qr = 1$. Al revés, la condición $[1, \tau] = \lambda[1, \tau']$ implica que

$$\lambda\tau' = p + q\tau$$
$$\lambda = r\tau + s.$$

Si además $\lambda \in K^\times$, entonces la matriz $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ tiene que ser una de cambio de base. Más aún como $\tau' = \frac{p\tau+q}{r\tau+s}$, y ambas τ y τ' están en el semiplano superior $\mathbb{H}$ entonces $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$. Esto completa la prueba de las equivalencias.

Para mostrar que el mapa es sobreyectivo se usa la misma idea que en la Proposición 5.1.2: si $\mathfrak{a}$ es un ideal fraccional de $\mathcal{O}$ entonces se puede escribir de la forma $\alpha[1, \tau]$ donde τ es una raíz de un polinomio irreducible entero $ax^2 + bx + c$. El discriminante de este polinomio viene dado por la misma cuenta del Lema 5.1.3. Es decir, suponiendo sin pérdida de generalidad que $mcd(a, b, c) = 1$, se tiene que $\mathcal{O} = [1, a\tau]$ y luego el discriminante D de $\mathcal{O}$ es

$a^2(\tau-\tau')^2$ donde τ' es el conjugado de τ. Por otro lado usando las relaciones entre coeficientes y raíces se obtiene que

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

O sea que ax^2+bx+c tiene discriminante D. Para la correspondencia esto significa que hay una forma cuadrática $f(x,y) = ax^2+bxy+cy^2$ con discriminante D, que además se puede tomar primitiva y definida positiva (imponiendo $a>0$). Y lo más interesante es que, como se vio al principio de este teorema, $f(x,y)$ se corresponde al ideal $a[1,\tau]$ (se puede suponer sin pérdida de generalidad que $\tau \in \mathbb{H}$), que está en la misma clase que $\alpha[1,\tau] = \mathfrak{a}$.

Resta probar la tercera parte. Si m es un entero representado por $f(x,y)$, entonces factorizando $m = d^2a$ se tiene que a debe ser propiamente representado por la misma forma $f(x,y)$. Luego por lo visto antes en el capítulo de formas cuadráticas, eventualmente cambiando $f(x,y)$ por una forma equivalente se puede suponer que $f(x,y) = ax^2+bxy+cy^2$. Más aún incluso se puede considerar que $mcd(a,b,c) = 1$. Luego $f(x,y)$ se mapea a $\mathfrak{a} = a[1,\tau]$ siendo τ una raíz de $f(x,y)$. Es fácil ver que $a[1,\tau]$ tiene índice a en $[1,a\tau] = \mathcal{O}$ y por lo tanto $N(\mathfrak{a}) = a$. Ahora usando la multiplicatividad de la norma $N(d\mathfrak{a}) = N(d\mathcal{O})N(\mathfrak{a}) = d^2a = m$ (recordar que $N(d\mathcal{O}) = N(d) = dd' = d^2$ siendo $d' = d$ el conjugado de d).

En la otra dirección, si m es la norma $N(\mathfrak{a})$ de algún ideal $\mathfrak{a} = \alpha[1,\tau]$, entonces la forma a considerar es $f(x,y) = ax^2+bxy+cy^2$ donde ax^2+bx+c es el polinomio minimal de τ (con $a>0$ y $mcd(a,b,c)=1$). Al igual que antes

$$a^2N(\mathfrak{a}) = N(a\mathfrak{a}) = N(a\alpha[1,\tau]) = N(\alpha a[1,\tau]) = N(\alpha)a$$

por lo que $m = N(\mathfrak{a}) = N(\alpha)/a$. Ahora para calcular $N(\alpha) = \alpha\alpha'$ hay que tener en cuenta que como $\mathfrak{a} = \alpha[1,\tau] \subset [1,a\tau]$ entonces $\alpha = p+aq\tau$ y por lo tanto $\alpha' = p+aq\tau'$. Como τ y τ' son las raíces de ax^2+bx+c se obtiene que

$$N(\alpha) = p^2 - bpq + acq^2.$$

Por otra parte, la inclusión $\alpha[1,\tau] \subset [1,a\tau]$ también dice que $\alpha\tau = r+sa\tau$. Además el hecho de que τ sea raíz de ax^2+bx+c implica $a\tau^2 = -b\tau - c$. Luego comparando coeficientes se llega a que $p = as+bq$. Así

$$p^2 - bpq + acq^2 = (as+bq)^2 - b(as+bq)q + caq^2 = a^2s^2 + absq + caq^2$$

y por consiguiente $m = N(\alpha)/a = as^2+bsq+cq^2 = f(s,q)$. □

La importancia de esta relación en el desarrollo de todo este trabajo es que establece una conexión entre los métodos usados para solucionar el problema $p = x^2+ny^2$ de la primera parte con los usados en la segunda parte. Para empezar, la condición $(-n/p) = 1$ implica por el lado de las formas

cuadráticas, que p tiene que ser representado por una forma cuadrática de discriminante $-4n$ (Corolarios 2.1.4 y 1.0.3), y yendo por la correspondencia significa que p tiene que ser la norma de algún ideal de $\mathbb{Z}[\sqrt{-n}]$. O también, la condición $(-n/p) = 1$ puede entenderse como que p descompone en dos ideales de $\mathbb{Z}[\sqrt{-n}]$ (Proposición 3.2.3), y por lo tanto tiene que ser la norma de cualquiera de ellos, y así, volviendo por la correspondencia se tiene que p debe ser representado por una forma de discriminante $-4n$. Pero dentro de estas formas, que $p = x^2 + ny^2$ quiere decir que p tiene que ser la norma de algún ideal en la clase de $[1, \sqrt{-n}]$, es decir p tiene que ser la norma de un ideal principal de $\mathbb{Z}[\sqrt{-n}]$. Y recíprocamente si p es la norma de un ideal principal de $\mathbb{Z}[\sqrt{-n}]$ entonces p debe ser representado por la forma x^2+ny^2.

Asimismo, este teorema le da una estructura de grupo al conjunto de las formas cuadráticas primitivas y definidas positivas de un discriminante D, que se llama el *grupo de clases de formas* y se denota por $C(D)$. En realidad la operación de grupo y su respectiva identidad, se pueden definir de forma explícita y sin necesidad de esta correspondencia (esto esta hecho en la Sección 3 del libro de Cox [2]). Lo cual permite, ahora sí gracias a la correspondencia, entender mucho mejor como operan los ideales de un orden en un cuerpo cuadrático.

Por si esto no fuera poco, en este intercambio además está participando una tercera pieza que es el cuerpo de clases. Es decir a través de la correspondencia de Artin se prueba que el cuerpo de clases para un orden $\mathcal{O}$ en un cuerpo cuadrático, tiene como grupo de Galois a $C(\mathcal{O})$. De este modo, usando la nueva correspondencia, el grupo de Galois del cuerpo de clases asociado a $\mathcal{O}$ puede pensarse como $C(D)$ donde D es el discriminante de $\mathcal{O}$. Y es esta interacción entre las tres estructuras la que hizo y hace posible la construcción de varios cuerpos ejemplos de cuerpos clases.

Permite también, traducir la teoría de géneros hecha en la primera parte a una estructura de la segunda parte. Concretamente como el género principal conforma un subgrupo de las formas cuadráticas se le puede asociar un cuerpo intermedio, a través primero del mapa de Artin y después de la correspondencia de Galois. Formalizando, si L es el cuerpo de clases para el orden $\mathbb{Z}[\sqrt{-n}]$ en el cuerpo cuadrático $K = \mathbb{Q}(\sqrt{-n})$, entonces existe un cuerpo intermedio $K \subset M \subset L$ tal que $\mathrm{Gal}(L/M)$ es isomorfo al subgrupo conformado por el género principal. M es llamado por esto el *cuerpo de géneros*. Se puede probar que el cuerpo de géneros M es de la forma

$$M = K(\sqrt{p_1^*}, \ldots, \sqrt{p_s^*})$$

donde $p_i^* = (-1)^{p_i - 1/2} p_i$ y $p_1, \ldots, p_s$ son los divisores primos impares de n (esta construcción esta hecha en la Sección 6 del libro de Cox [2]). En la práctica este cuerpo resulta útil para calcular cuerpos de clases, visto que el grado de la extensión de L/M eventualmente disminuye al de L/K.

5.5.1. Ejemplo $p = x^2 + 26y^2$

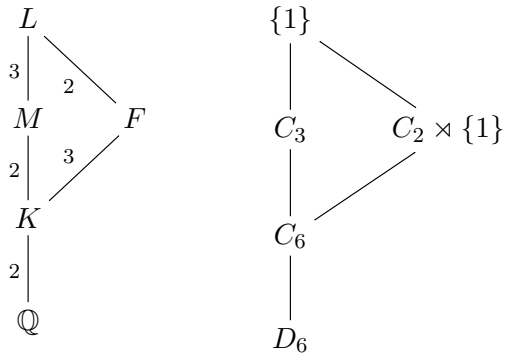
Para ver como ayuda el cuerpo de géneros en un computo particular y al mismo tiempo para rever los métodos antes usados, considérese el caso $p = x^2 + 26y^2$. Los cuerpos asociados a este problema son en principio $\mathbb{Q}$, $K = \mathbb{Q}(\sqrt{-26})$ y L el cuerpo de clases para el orden $\mathbb{Z}[\sqrt{-26}]$. Aquí el cuerpo de géneros es $M = K(\sqrt{13})$. De momento, el diagrama de cuerpos es el siguiente

Para entender cómo es el cuerpo de clases se estudia la estructura de grupos asociado por la correspondencia de Galois. Pero a su vez esta estructura viene dada por la relación con las formas cuadráticas. Es decir la forma de $\mathrm{Gal}(L/K)$ es la misma que la del grupo $C(-4 \cdot 26)$. Con la teoría de formas cuadráticas se puede calcular que $h(-4 \cdot 26) = |C(-4 \cdot 26)| = 6$. Ahora para definir la estructura se usa la forma que tiene el género principal, a saber: las formas de este subgrupo son los cuadrados (en cualquier caso). Por otra parte en el caso $x^2 + 26y^2$ el cuerpo de géneros M tiene grado dos sobre K y por tanto el correspondiente subgrupo de géneros $\mathrm{Gal}(L/M)$ tiene tres elementos. En suma, no hay otra alternativa a que $\mathrm{Gal}(L/K) \simeq C_6$.

Luego, y debido a que $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Gal}(L/K) \rtimes \mathrm{Gal}(K/\mathbb{Q})$, el grupo de Galois de $L/\mathbb{Q}$ tiene que ser $D_6 = C_6 \rtimes C_2$. Trasladando el diagrama de cuerpos a subgrupos de $\mathrm{Gal}(L/\mathbb{Q})$ queda

De modo que si F es un cuerpo que se corresponde con un 2-subgrupo de D_6, la composición de F con el cuerpo de géneros M tiene que ser el cuerpo

de clases L, dado que el grupo asociado a M tiene orden 3. Ahora, los 2-subgrupos de D_6 que no son normales no sirven de mucho para reducir el problema porque para calcularlos a través de su grupo de Galois (sobre el cuerpo base $\mathbb{Q}$) hay que irse a cuerpos más grandes que en definitiva van a corresponder 2-grupos normales. Y como el único 2-subgrupo normal de D_6 es $C_2 \rtimes \{1\}$, la única posibilidad es que F sea el cuerpo fijo por $C_2 \rtimes \{1\}$. Nótese que en ese caso el grupo de Galois de $F/\mathbb{Q}$ es $D_6/C_2 \rtimes \{1\} = S_3$.



Ahora para calcular F se usa la información proporcionada por la ramificación de ideales. Es decir, gracias al teorema de existencia se sabe que los primos de K que pueden ramificar en el cuerpo de clases L de $\mathbb{Z}[\sqrt{-26}]$, son los divisores de $2\mathcal{O}_K$. En total mirando la extensión $L/\mathbb{Q}$, los únicos primos enteros que pueden ramificar en L son el 2 y el 13. Y como la ramificación es multiplicativa en torres (Proposición 3.1.8), lo mismo se aplica para F, es decir: sólo el 2 y el 13 pueden ramificar en F. Luego utilizando la tabla de cuerpos de números de Jones [11], la cantidad de candidatos para F queda en tan sólo dos, definidos por los polinomios:

$$x^6 + 8x^4 + 29x^2 + 26 \quad \text{y} \quad x^6 - 2x^5 + 2x^4 - 6x^3 + 25x^2 - 20x + 8.$$

Para terminar la clasificación se vuelve a usar la correspondencia de Galois: como F se corresponde con el grupo $C_2 \rtimes \{1\}$ en D_6 entonces el cuerpo cuadrático $K = \mathbb{Q}(\sqrt{-26})$ tiene que estar incluido en F; luego F sólo puede ser el cuerpo definido por el polinomio $x^6 + 8x^4 + 29x^2 + 26$ ya que el otro no contiene a las raíces $x^2 + 26$ (cuentas realizadas con *Sage* [19]).

Ahora componiendo F con M el cuerpo compuesto L debe quedar definido por el polinomio

$$x^{12} + 8x^{10} + 23x^8 + 32x^6 + 25x^4 + 14x^2 + 4.$$

El último paso para encontrar el polinomio $f_{26}(x)$ viene dado por la Proposición 4.2.3 del capítulo anterior: dicho polinomio debe ser un minimal de L sobre $L \cap \mathbb{R}$. Luego

$$f_{26}(x) = x^6 - x^5 + 2x^4 + x^3 - 2x^2 - x - 1.$$

De nuevo todas las cuentas fueron realizadas con Sage [19].

El teorema para $n = 26$ quedaría

$$p = x^2 + 26y^2 \iff \begin{cases} \left(\frac{-26}{p}\right) = 1 \text{ y} \\ x^6 - x^5 + 2x^4 + x^3 - 2x^2 - x - 1 \equiv 0 \text{ mód } p \\ \text{tiene solución entera.} \end{cases}$$

La novedad que además tiene este ejemplo es la utilización de tablas de cuerpos de números y cuentas con programas de computación (tablas de Jones [11] y computos con Sage [19]). Si bien quizá esto no represente un verdadero avance teórico, puesto que muchas de las cuentas que se hacen son hechas a partir de una base de datos con el mismo tipo de argumentos esbozados antes e incluso matemática más compleja (en particular la multiplicación compleja, ver Capítulo 3 del libro de Cox [2]), es sin dudas una herramienta muy útil para realizar los cálculos en la práctica.

5.5.2. Consideraciones sobre discriminantes impares

Al igual que en la primera parte, corresponde preguntarse si es posible hacer estas construcciones también para discriminantes impares. En realidad como muestra todo este último capítulo, no hay nada que impida hacerlo. Para empezar siempre que D sea 0 o 1 módulo 4 se puede construir un cuerpo cuadrático con discriminante D, a saber: $K = \mathbb{Q}(\sqrt{D})$. Luego manteniendo $D < 0$, los mismos teoremas de cuerpos de clases se pueden repetir para construir cuerpos de órdenes con discriminante impar D. Y todo funciona exactamente igual que en la primera parte porque en el fondo la correspondencia con las formas cuadráticas sigue siendo la misma del Teorema 5.5.1. Cuando D es impar tomando por ejemplo el orden maximal de $\mathbb{Q}(\sqrt{D})$ es que se obtiene la estructura de grupo $C(D)$ para las formas cuadráticas de discriminante D. Recuérdese que aquí la forma principal es $x^2 + xy + \frac{1-D}{4}y^2$, por lo que todos los resultados de representación que se pueden obtener con la teoría de cuerpos de clases se referirán a dicha forma. De hecho el Teorema 5.5.1 se rehace idénticamente con la forma $x^2 + xy + \frac{1-D}{4}y^2$.

Por ejemplo, cuando $D = -23$ se puede probar que

$$p = x^2 + xy + 6y^2 \iff \begin{cases} \left(\frac{-23}{p}\right) = 1 \text{ y} \\ x^3 - x^2 + 1 \equiv 0 \text{ mód } p \text{ tiene solución entera.} \end{cases}$$

Y el proceder es con las mismas herramientas que antes. En este caso, a partir de que la estructura de $C(-23)$ es un C_3, se prueba que cualquier subextensión del cuerpo de clases L que tenga grado 3 sobre $\mathbb{Q}$ tiene como clasura de Galois necesariamente al mismo L, o sea que su grupo de Galois es S_3; luego con la ramificación restringida a 23 sólo hay una chance posible para el polinomio $f_{23}(x)$.

Bibliografía

[1] E. Artin, *Idealklassen in oberkörpern und allgemeines reziprozitätsgesetz*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 7 no. 1 (46-51), Hamburgo, 1929.

[2] D.A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, Wiley, Nueva York, Chichester, Weinheim, Brisbane, Singapore y Toronto, 1989.

[3] J.W.R. Dedekind, *Sur la Théorie des nombres entiers algébriques*, Francia, 1877. Traducción al inglés por Cambridge University Press, 1996.

[4] L. Euler, *Opera Omnia*, Serie prima, Vols. I-V, Teubner, Leipzig y Berlin, 1911-1944.

[5] P. de Fermat, *Oeuvres*, Gauthier-Villars, Paris, 1891-1896.

[6] C.F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, 1801. Reimpreso por Springer-Verlag, Berlin, Heidelberg y Nueva York, 1986.

[7] T.L. Heath, *Arithmetica*, 1910. Pueden leerse libremente desde la Califonia Digital Library en https://archive.org/details/diophantusofalex00heatiala.

[8] C.S. Herz, *Construction of class fields* en *Seminar on Complex Multiplication*, Springer-Verlag, Berlin, Heidelberg y Nueva York, 1966.

[9] D. Hilbert, *Mathematical problems*, Bulletin of the American Mathematical Society 8 no. 10 (437–479), 1902.

[10] G.J. Janusz, *Algebraic Number Fields*, Academic Press, Nueva York, 1973.

[11] J. Jones, *Number Fields for small degrees*, http://hobbes.la.asu.edu/NFDB/.

[12] J.L. Lagrange, *Oeuvres*, Vol. 3, Gauthier-Villars, Paris, 1869.

[13] A.M. Legendre, *Essai sur la Théorie des Nombres*, Paris, 1798. Tercera edición republicada como *Théorie des Nombres*, Paris, 1830. Reimpreso por Blanchard, Paris, 1955.

[14] F. Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*, Springer-Verlag, Berlin, Heidelberg y Nueva York, 2005.

[15] D.A. Marcus, *Number Fields*, Springer-Verlag, Berlin, Heidelberg y Nueva York, 1977.

[16] J.S. Milne, *Field and Galois Theory*, versión legal libre en http://www.jmilne.org/math/CourseNotes/ft.html/.

[17] The On-Line Encyclopedia of Integer Sequences, OEIS, http://oeis.org/.

[18] W.A. Stein, *Elementary number theory: Primes, Congruences and Secrets*, Springer-Verlag, Berlin, Heidelberg y Nueva York, 2003. Copia legal libre disponible en http://modular.math.washington.edu/edu/Fall2002/124/stein/.

[19] Sage, http://www.sagemath.org/, The Sage Notebook http://nb.sagemath.org/.