Departamento de Matemáticas, Facultad de Ciencias
Universidad Autónoma de Madrid

Disquisitiones Arithmeticae: Formas binarias cuadráticas y la Teoría Algebraica de Números

Trabajo de fin de grado

Grado en Matemáticas

Autora: Andrea Infantes Serrano
Tutor: Enrique González Jiménez

Curso 2021-2022

Resumen

Disquisitiones Arithmeticae es la obra más significativa del matemático, físico y astrónomo alemán Carl Friedrich Gauss. En ella reúne los resultados más importantes que se conocían hasta el momento sobre la Teoría de Números, dotándoles de una conexión y dejando de ser un mero conjunto de teoremas y conjeturas sin ninguna convergencia. A su vez, Gauss expuso nuevas investigaciones sobre esta teoría que dieron lugar al libro de mayor trascendencia para todos los grandes matemáticos de la época.

En dicho trabajo se encuentran resultados de extraordinaria relevancia para la matemática posterior al siglo XVIII, como la primera demostración completa y sin error de la *Ley de Reciprocidad Cuadrática* y la construcción geométrica formal del polígono regular de 17 lados.

El objetivo fundamental de este trabajo se centrará en la sección de mayor envergadura de *Disquisitiones Arithmeticae*, las *formas binarias cuadráticas*, resumiendo sus aspectos más característicos según el tratamiento de Gauss y mostrando la equivalencia entre su método y los procedimientos de la matemática actual. Se estudiará en profundidad el concepto de la *composición* mediante la *composición de Dirichlet*, que convierte el grupo de clases en un grupo finito abeliano, así como la relación de las formas con los ideales de los cuerpos cuadráticos imaginarios a través de los *órdenes*. Asimismo, se expondrán conceptos más profundos de dicha teoría y los otros resultados más emblemáticos de la obra gaussiana mencionados en el párrafo anterior.

Abstract

Disquisitiones Arithmeticae is the most prestigious work of the German mathematician, physicist and astronomer Carl Friedrich Gauss. He gathered the most important findings that had been known until that moment on the Number Theory, connecting them and thus ceasing to be a mere set of theorems and speculations without any convergence. Gauss also presented new investigations on this theory that gave shape to the most important book for all the great mathematicians of the time.

This work contains results of extraordinary relevance for mathematics after the XVIII century, such as the first complete and error-free proof of the *Law of Quadratic Reciprocity* and the formal geometrical construction of the 17-sided regular polygon.

The main objective of this paper will focus on the largest section of *Disquisitiones Arithmeticae*: the *binary quadratic forms*. I will outline the most characteristic aspects of these according to Gauss's treatment and show the equivalence between his method and the procedures of present-day mathematics. I will study the concept of *composition* via the *Dirichlet composition*, which converts the group of classes into a finite abelian group, as well as the relation between these forms with the ideals of quadratic imaginary fields through *orders*. I will also present deeper concepts of this theory and additional outcomes of the gaussian work mentioned in the previous paragraph.

Índice general

Introducción

Toda persona que haya tenido la más mínima relación con las ciencias ha estudiado alguna vez un "Teorema de Gauss". De hecho, lo más probable es que, si se le preguntara a distintas personas sobre el contenido de dicho teorema, sus respuestas serían diferentes. Esto es entendible, ya que este matemático, científico y astrónomo demostró tantos resultados a lo largo de su vida que abarcó la mayoría de los campos. Por si fuera poco, su portento se desarrolló desde tan temprana edad que apenas al alcanzar la mayoría de edad ya había probado teoremas como el *Teorema Fundamental del Álgebra* o la *Ley de los Mínimos Cuadrados*.

Carl Friedrich Gauss es uno de los matemáticos más importantes de la Historia de las Matemáticas. Toda la teoría que conocemos en la mayoría de las ramas de esta materia dependen directa o indirectamente de los resultados que él desarrolló en vida. Se especializó en temas como el Análisis Matemático, la Geometría Diferencial, la Estadística, la Geodesia, el Magnetismo, la Óptica y hasta la Teoría de Números. En particular, destaca su trabajo en ésta última ya que, para Gauss, si bien las Matemáticas eran la reina de las ciencias, la Teoría de Números resulta la reina de las Matemáticas. Fue el primero en unificar todo el conocimiento que existía hasta la fecha sobre este campo, dotándolo de un sentido, conexión y convergencia, así como aportó aún más teoremas de cuantiosa relevancia. La obra en la que desarrolló todo esto es, precisamente, *Disquisitiones Arithmeticae*.

Disquisitiones Arithmeticae es un compendio de la Teoría de Números desarrollada desde la Antigua Grecia hasta la matemática del siglo XVIII de Fermat, Euler, Lagrange o Legendre, así como una recopilación de los resultados que Gauss realizó sobre esta disciplina. Entre estos, se encuentran la *Ley de Reciprocidad Cuadrática* y la prueba de qué polígonos regulares son capaces de construirse con regla y compás según su número de lados, cuestión que llevaba sin resolverse desde tiempos de Euclides. En particular lo prueba para el heptadecágono, suponiendo el final de su obra y uno de los resultados de mayor orgullo para el matemático.

Por otro lado, destaca el contenido de mayor extensión de la obra, el estudio de las *formas binarias cuadráticas*. Dichas formas son aquellas de expresión

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

Aunque a priori parezcan una simple ecuación, las formas binarias cuadráticas encierran una teoría sorprendente que Gauss pudo apreciar desde el principio y le llevó a establecer, con ello, resultados que han derivado en importantes teoremas en la Teo-

ría de Números Algebraica. Dicho estudio será el que expondremos en este trabajo, explicando las ideas fundamentales del trabajo y relacionándolos con la matemática actual, para posteriormente concluir en dos resultados de especial interés.

Gauss partió del concepto de *determinante* de una forma binaria cuadrática para poder clasificar dichas formas según su determinante. Posteriormente, definió el concepto de formas *equivalentes* como aquellas que podían transformarse una en otra mediante un cambio de variables particular. Dadas dos formas binarias cuadráticas $f(x, y)$ y $g(x, y)$, estas son equivalentes si

$$f(x, y) = g(px' + qy', rx' + sy'), \text{ con } p, q, r, s \in \mathbb{Z} \text{ y } ps - qr = \pm 1.$$

Esto posibilita establecer la equivalencia como una relación de equivalencia que nos permite clasificar las formas binarias cuadráticas fácilmente. Para ello, Gauss definió las formas *reducidas* como los representantes de las clases formadas por dicha relación ya que, como se probará en el trabajo, cada clase consta de una única forma reducida. Una forma binaria cuadrática $f(x, y) = ax^2 + bxy + cy^2$ de determinante negativo es reducida si $-a < b \leq a < c$ o $0 \leq b \leq a = c$. Gracias a esto se puede definir $C(D)$, el grupo de clases de formas binarias cuadráticas de determinante D, donde el número de las distintas formas reducidas de un determinante dado resulta su cardinal.

La primera cuestión de importancia que Gauss expuso en *Disquisitiones Arithmeticae* y que se tratará en este trabajo emplea el concepto de *composición*. Dicha operación multiplica formas binarias cuadráticas y, mediante un cambio de variables, las convierte en otra forma binaria cuadrática. Dadas dos formas $f(x, y)$ y $g(x, y)$, su composición es

$$f(x, y)g(z, w) = \mathfrak{F}(B_1(x, y; z, w), B_2(x, y; z, w)),$$

donde $B_i(x, y; z, w) = a_i xz + b_i xw + c_i yz + d_i yw$ para $i = 1, 2$ son formas bilineales con coeficientes enteros.

El principal resultado sobre la composición es que dicha operación convierte a $C(D)$ en un grupo abeliano finito. Esto resulta verdaderamente sorprendente ya que, en la época de Gauss, ni siquiera se había definido el concepto de grupo, pero él probó que dicha operación cumple las propiedades que los definen. En este trabajo se estudiará la composición a través de la *composición de Dirichlet*. Dadas dos formas $f(x, y)$ y $g(x, y)$ que cumplen una serie de requisitos, su composición de Dirichlet es $f \circ g$:

$$(f \circ g)(x, y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2$$

donde B es un entero que cumple unas determinadas condiciones de congruencia con los coeficientes de las formas $f(x, y)$ y $g(x, y)$. Esta expresión resulta el método actual de mayor similitud al gaussiano pero con una notación y tratamiento más simple y teórico.

Todo el contenido expuesto hasta ahora se tratará en el primer capítulo del trabajo, profundizando en la materia y trasladándolo a la notación de hoy en día. Para ello, se utilizará el *discriminante* de una forma binaria cuadrática en vez del determinante gaussiano, el cual resulta cuatro veces el valor de éste último debido a la notación

que empleaba Gauss. También se encontrará una sección dedicada a otros aspectos de importancia de *Disquisitiones Arithmeticae* como la *Ley de Reciprocidad Cuadrática* y la construcción geométrica formal del heptadecágono. Asimismo, se exhibirán otros conceptos estudiados en la obra de mayor profundidad sobre la composición como los *géneros*, así como de las conjeturas de Gauss derivadas de dicha teoría que han sido objeto de estudio durante los últimos siglos.

Toda la información sobre la teoría expuesta en *Disquisitiones Arithmeticae* se recoge en la obra [10], una traducción al castellano de la obra de Gauss realizada por Hugo Barrantes Campos, Michael Josephy y Ángel Ruiz Zúñiga y que ha sido el libro de consulta para la elaboración de este trabajo. Además, en [2] se encuentra información de especial interés sobre la composición que prueba que $C(D)$ es un grupo abeliano finito.

Para explicar la otra finalidad del trabajo, se estudiarán detalladamente los *órdenes* de los cuerpos cuadráticos imaginarios. Esto se debe a que, dado un orden $\mathcal{O}$, el grupo de clases $C(\mathcal{O})$ en un cuerpo cuadrático imaginario es isomorfo al grupo de clases de formas binarias cuadráticas de determinante $D < 0$ mencionado anteriormente. Por ello, podemos tratar indistintamente con formas binarias cuadráticas o con ideales de órdenes de cuerpos cuadráticos imaginarios. Este será el otro objeto de estudio del trabajo y que se explicará con detalle en el segundo capítulo. Además, se trabajará con el *anillo de enteros* $\mathcal{O}_K$ de los cuerpos cuadráticos imaginarios y los *discriminantes* de $\mathcal{O}$ y $\mathcal{O}_K$ para ello. Por último, se presentarán los ideales *fraccionarios* y los ideales *propios* para establecer la relación que se pretende en este capítulo.

En [5] se profundiza sobre estos aspectos, así como se expone la teoría sobre formas binarias cuadráticas con las herramientas matemáticas actuales para poder establecer la relación con el grupo de clases de los órdenes anteriormente mencionados. Otra explicación detallada de esto último se puede encontrar en [18]. Asimismo, en [13] se expone de otra manera la teoría relacionada con los órdenes de los cuerpos cuadráticos imaginarios desde el punto de vista de los *módulos* de los cuerpos de números. En dicho libro también se estudian las formas binarias cuadráticas y se analizan los conceptos de equivalencia y género, así como en [21].

Por otro lado, en el Apéndice A se podrá encontrar una breve bibliografía de Gauss donde se expondrán su vida y principales resultados, mostrando su forma de trabajo y la trascendencia de éste en las ciencias, especialmente en las Matemáticas. Posteriormente, en el Apéndice B aparecerán demostraciones de nivel más elemental de algunos resultados del trabajo. En el Apéndice C se ubica un método curioso explicado en [3] para encontrar formas binarias cuadráticas reducidas de discriminante negativo utilizando números complejos. Después, en el Apéndice D, se incluyen definiciones y resultados relacionados con los módulos de un cuerpo de números y la Teoría Algebraica de Números, que podrán servir como consulta para comprender mejor el contenido del trabajo. Finalmente, en el Apéndice E se podrán encontrar ciertas conjeturas que realizó Gauss sobre el cardinal del grupo de clases y que han supuesto un profundo estudio en la Teoría Algebraica de Números de los últimos siglos.

CAPÍTULO 1
Disquisitiones Arithmeticae

1.1. Las matemáticas de la época y *Disquisitiones*

Hasta principios del siglo XIX, la Teoría de Números constaba únicamente de una colección inconexa de resultados que los prestigiosos matemáticos de la Historia de las Matemáticas habían enunciado y demostrado. Gracias a la célebre obra de Gauss, dichos teoremas pudieron unificarse, tomar una dirección y converger en una teoría completa y coherente que dominaría durante dicho siglo y hasta gran parte del siguiente. Asimismo, también supuso la pieza necesaria para originar lo que actualmente se conoce como la Teoría Algebraica de Números y, con ello, culminar en la demostración de teoremas sin respuesta, como el Último Teorema de Fermat o el Teorema de Galois.

Poco antes de la publicación de *Disquisitiones* los ilustres Fermat, Euler, Lagrange y Legendre habían realizado numerosos avances en este campo. Muchos habían probado (con un enfoque distinto) los mismos lemas que Gauss demuestra en las tres primeras secciones de *Disquisitiones*. Sin embargo, otros resultados como la *Ley de Reciprocidad Cuadrática* o algunas propiedades sobre las formas binarias cuadráticas habían sido enunciados por éstos sin una demostración válida, puesto que dichas pruebas omitían pasos no triviales o cometían ciertos errores. Por otro lado, es importante el enfoque conceptual de aquellos matemáticos comparado con el que Gauss brindaba a su teoría: además de sus propios aportes, empleó métodos generales que englobaban la mayoría de los resultados. Era el único matemático de la época que poseía un tratamiento abstracto de las matemáticas, por lo que encaminó la matemática moderna que surgiría a partir de él, suponiendo un punto de inflexión en el tratamiento de dicha teoría.

Hasta finales del siglo XVIII, los conocimientos sobre Álgebra se fundamentaban en tratamientos simples de congruencias y resultados derivados de estas como su *Pequeño Teorema de Fermat*[1] o el *Teorema de Wilson*[2]. De hecho, fue Gauss quien introdujo en *Disquisitiones* por primera vez la notación $\equiv$ para el símbolo de la congruencia[3]. Se había definido el concepto de residuo y módulo, a lo que Gauss añadió los conceptos de

[1] [10], #50, pág. 41.
[2] [10], #78, pág. 61.
[3] En [10], #4, pág. 8, lo enuncia de la siguiente forma: "Adoptamos este símbolo por la gran analogía que se encuentra entre la igualdad y la congruencia. Por la misma razón, el ilustre Legendre,

residuos mínimos y probó con validez importantes teoremas como el "Teorema de Oro". Por otra parte, también se conocían otros resultados como el *Teorema Fundamental del Álgebra*, la existencia de las raíces primitivas de la unidad o las sumas geométricas. Es por ello por lo que, gracias a la perspectiva tan avanzada de Gauss con respecto a su época, pudo enfocar dicha teoría, todavía muy elemental, para dar lugar a resultados como la construcción geométrica del heptadecágono.

Sin duda alguna, *Disquisitiones* fue un antes y un después en las matemáticas. Se convirtió en una notoria referencia para todos los matemáticos de entonces; incluso se dice que el gran Dirichlet lo tenía en su escritorio y lo estudiaba religiosamente. Y no es para menos pues, si no fuera por esta conspicua obra, no gozaríamos de los conocimientos relativos al Álgebra que poseemos en la actualidad.

Gauss escribió todas las ideas que recogió en esta obra durante los tres años que estudió en la Universidad de Göttingen, la cual supuso el auge de su formación y el período de mayor esplendor intelectual del matemático debido a la exorbitante cantidad de resultados que planteó y probó en aquella época a tan corta edad.

Originalmente, *Disquisitiones* iba a ser una simple obra que trabajara la Aritmética Superior para divulgar sus hallazgos en este campo. Para Gauss, si bien las Matemáticas eran la reina de las ciencias, la Teoría de Números resulta la reina de las Matemáticas. La curiosidad que éstas le generaban le llevó a plantearse ciertos problemas que, tras resolver, le llevaban a otras cuestiones relacionadas, completando con ello las cuatro primeras secciones de *Disquisitiones*, tal y como él relata en la introducción del libro[4]. Tras escribirlas, su interés le hizo expandirse más allá de la Aritmética, obteniendo los resultados que figuran en las secciones V, VI y VII. Se preveía una octava sección, pero debido a los costes de publicación ésta quedó excluida.

Las secciones I, II y III conforman un resumen de los avances en la Teoría de Números que se habían realizado hasta la época. En ella figuran resultados de los eminentes matemáticos del siglo XVIII, así como pruebas adicionales dadas por Gauss con un enfoque diferente a los suyos. La primera sección tan solo abarca la noción de congruencia entre dos enteros racionales, mientras que la segunda trata las congruencias de primer grado y la tercera corresponde al estudio de las progresiones geométricas módulo un primo p. Estas dos últimas secciones muestran importantes resultados como la unicidad de la factorización de enteros en primos y las definiciones de máximo común divisor y mínimo común múltiplo, así como la investigación de los residuos de una potencia de un número dado un módulo primo.

La sección IV muestra el estudio que desembocó en la *Ley de Reciprocidad Cuadrática*, la cual se explicará con mayor detalle en la sección 1.4.1. Posteriormete, en la sección V, se muestra toda la teoría que el matemático desarrolló sobre las formas binarias cuadráticas, siendo este el capítulo de mayor envergadura de su trabajo y que se encuentra en la sección 1.2. Por otro lado, la sección VI resulta un anexo de

en su tratado, usó el mismo símbolo para la igualdad y la congruencia, lo que nosotros dudamos en imitar para que no se originara ninguna ambigüedad".

[4] [10], pág. 4.

lo anterior, pues recolecta aplicaciones obtenidas con los resultados probados en las secciones anteriores.

La sección VII contiene uno de los resultados de mayor orgullo del matemático: la construcción con regla y compás del heptadecágono. Aunque se trate de un resultado geométrico, la metodología empleada para su desarrollo parte del estudio de las raíces primitivas de la unidad, rompiendo con la intuición que se tenía para ello. Podrá verse este tema con mayor profundidad en la sección 1.4.2.

Disquisitiones fue publicado en el verano de 1801 en Leizpig, aproximadamente tres años después de la vuelta de Gauss de Göttingen a Braunschweig, su ciudad natal. Las cuatro primeras secciones las escribió como borrador en 1796 y editó de forma definitiva en febrero de 1797; la sección V se elaboró por primera vez también en 1796, pero las diversas modificaciones atrasaron su finalización hasta 1800. Además, la sección VI fue confeccionada paralelamente a las secciones IV y V al tratarse de una consecuencia de estas. Por último, la sección VII fue realizada tras la reciente demostración de su principal resultado el 30 de marzo de 1796, finalizando con ello el contenido de una de las más ilustres publicaciones de la Historia de las Matemáticas.

1.2. Formas binarias cuadráticas

Definición 1.1. Una **forma binaria cuadrática** es una expresión de la forma

$$f(x,y) = ax^2 + bxy + cy^2, \quad a,b,c \in \mathbb{Z}. \tag{1.1}$$

Se dice que $f(x,y)$ es **primitiva** si a, b y c son coprimos.

Nota 1.2. A partir de ahora, se llamarán formas a las formas binarias cuadráticas.

Observación 1.3. Toda forma es un múltiplo entero de alguna forma primitiva.

Sea $f(x,y) = ax^2 + bxy + cy^2$ una forma. Definimos:

$$F = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}, \quad X = \begin{pmatrix} x \\ y \end{pmatrix}, \quad X^T = \begin{pmatrix} x & y \end{pmatrix}.$$

Así, la expresión matricial de $f(x,y)$ es X^TFX:

$$X^TFX = (x,y)\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = (ax + \frac{b}{2}y, \frac{b}{2}x + cy)\begin{pmatrix} x \\ y \end{pmatrix} = ax^2 + bxy + cy^2.$$

Notación. A partir de ahora se usará F como la matriz asociada a la forma f, y de manera análoga se establecerán las matrices para formas de distinto nombre (g y G, h y H, etc.).

Definición 1.4. Un entero m se representa mediante la forma $f(x,y)$ si la ecuación $m = f(x,y) = ax^2 + bxy + cy^2$ tiene solución entera para x e y. Además, decimos que m se **representa propiamente** por $f(x,y)$ si x e y son coprimos.

Definición 1.5. Sea $f(x,y) = ax^2 + bxy + cy^2$ una forma. El **discriminante** de $f(x,y)$ se define como $D = b^2 - 4ac$.

Definición 1.6. Decimos que dos formas $f(x,y)$ y $g(x,y)$ son **equivalentes** si una puede transformarse en la otra mediante sustituciones de la forma $x = px' + qy'$ e $y = rx' + sy'$, donde $p, q, r, s \in \mathbb{Z}$ y $ps - qr = 1$.

Dicha sustitución puede expresarse de forma matricial mediante $X = UX'$, donde

$$U = \begin{pmatrix} p & q \\ r & s \end{pmatrix}, \quad X' = \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

Por tanto, la condición necesaria para la equivalencia es que $\det U = 1$ para que f se transforme en $X'^T G X'$, donde $G = U^T F U$. Como $\det\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) = ps - qr = 1$, esto supone que $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in SL(2,\mathbb{Z})$, el grupo de *matrices unimodulares*, de lo que se sigue el siguiente corolario:

Corolario 1.7. *La equivalencia de formas es una relación de equivalencia. En consecuencia, se puede designar la equivalencia entre dos formas f y g como $f \sim g$.*

Demostración. Veamos que cumple las propiedades de las relaciones de equivalencia.

La reflexividad se sigue de que $U = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in SL(2,\mathbb{Z})$, por lo que $f \sim f$.

Para ver la simetría, si $f \sim g$, existe una matriz $U \in SL(2,\mathbb{Z})$ tal que $G = U^T F U$. Entonces, $F = (U^T)^{-1} G U^{-1} = (U^{-1})^T G U^{-1}$. Como $U^{-1} \in SL(2,\mathbb{Z})$, resulta $g \sim f$.

Veamos la transitividad. Si $f \sim g$ y $g \sim h$, entonces $G = U^T F U$, $H = V^T G V$ para algunas matrices $U, V \in SL(2,\mathbb{Z})$. En consecuencia, se tiene que $H = V^T U^T F U V = (UV)^T F (UV)$, y como $UV \in SL(2,\mathbb{Z})$ por ser un grupo, se concluye que $f \sim h$. □

Gauss escribe[5] las formas como $ax^2 + 2bxy + cy^2$ y trabaja con el *determinante* de una forma en lugar de con su discriminante. Por ello, dicho determinante, que él define como $b^2 - ac$, resulta 4 veces el discriminante que nosotros conocemos. Además, en su definición de formas equivalentes es indispensable que ambas tengan el mismo determinante. Ahora bien, ¿es la definición de formas equivalentes mencionada anteriormente análoga a la gaussiana?

En *Disquisitiones* lo introduce[6] de la siguiente manera: "Si la forma F, cuyas indeterminadas son x e y, puede transmutarse en otra F', cuyas indeterminadas son x' e y', por las transformaciones $x = \alpha x' + \beta y'$ e $y = \gamma x' + \delta y'$, $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$, diremos que la primera *implica* la segunda o que la segunda *está contenida en la primera*".

El matemático explica que, definiendo las formas $F = ax^2 + 2bxy + cy^2$ y $F' = a'x'^2 + 2b'x'y' + c'y'^2$, realizando la sustitución de las variables por las transformaciones

[5] De esta manera, al escribir la matriz asociada puede poner b en los términos correspondientes de esta, aunque solamente emplea matrices al estudiar las formas ternarias. Hacía no mucho que las matrices comenzaban a utilizarse en el lenguaje matemático, y se puede observar en *Disquisitiones* que son diferentes a las actuales, ya que Gauss ponía comas para separar los términos y nunca se refiere a ellas como matrices.

[6] [10], #157, pág. 125.

mencionadas anteriormente, obtenemos las siguientes igualdades[7]:

$$\begin{aligned} a' &= a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = F(\alpha,\gamma) \\ b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \\ c' &= a\beta^2 + 2b\beta\delta + c\delta^2 = F(\beta,\delta). \end{aligned} \tag{1.2}$$

Si se multiplica la segunda ecuación por ella misma y la primera por la tercera, para luego restar ambas soluciones y quitar las cancelaciones, se obtiene

$$b'^2 - a'c' = (b^2 - ac)(\alpha\delta - \beta\gamma)^2.$$

De aquí se deduce que el determinante de F' es divisible por el de F y que el cociente de ellos es un cuadrado, por lo que han de tener el mismo signo para que dicho cuadrado sea positivo. Si una estuviera contenida en la otra y viceversa tendrán el mismo determinante, por lo que $(\alpha\delta - \beta\gamma)^2 = 1$. Gauss define estas formas como *equivalentes*, aquellas donde $\det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \pm 1$.

Gauss distingue, además, entre transformaciones *propias* e *impropias* como aquellas donde $\alpha\delta - \beta\gamma$ es positivo o negativo respectivamente. En particular, define las formas *propiamente equivalentes* como aquellas en las que $\alpha\delta - \beta\gamma = 1$ y las *impropiamente equivalentes* en las que $\alpha\delta - \beta\gamma = -1$. No obstante, aunque Gauss definiera la equivalencia como aquellas transformaciones con determinante ± 1, en la matemática actual se restringe al caso $+1$ ya que es el único de verdadero interés, por lo que de aquí en adelante se contemplará de dicha manera.

De lo anteriormente mencionado podemos formular el siguiente lema:

Lema 1.8. *Formas equivalentes tienen el mismo discriminante.*

Demostración. Dada la Definición 1.6, consideremos $f(x,y)$ y $g(x,y)$ dos formas equivalentes con discriminantes D y D' respectivamente y U, F y G definidas como antes. Entonces, $D = -4\det F$ y $D' = -4\det G$, de modo que $\det G = \det U^T \cdot \det F \cdot \det U = \det F$ si y solo si $\det U^T = \det U = \pm 1$. De esta manera, las dos formas tendrán el mismo discriminante cuando $ps - qr = \pm 1$, que es justo lo que ocurre con las equivalencias en el sentido gaussiano. □

Las formas equivalentes poseen la siguiente propiedad:

Lema 1.9. *Sean $f(x,y)$ y $g(x,y)$ formas equivalentes y $n \in \mathbb{Z}$. Entonces f representa propiamente a n si y solo si g representa propiamente a n.*

Demostración. Sean las formas $f(x,y) = ax^2 + bxy + cy^2$ y $g(x,y) = a'x^2 + b'xy + c'y^2$, de modo que $G = U^T F U$ con la notación utilizada en la Definición 1.6. Definiendo $X_0 = \begin{pmatrix} x_0 & y_0 \end{pmatrix}^T$ y $X_1 = \begin{pmatrix} x_1 & y_1 \end{pmatrix}^T$, si $n = X_0^T F X_0$, entonces $n = X_0^T (U^{-1})^T G U^{-1} X_0$, por lo que $n = X_1^T G X_1$, donde $X_1 = U^{-1} X_0$. Además, si asumimos que $\mathrm{mcd}(x_0, y_0) = 1$, al ser $x_0 = px_1 + qy_1$ e $y_0 = rx_1 + sy_1$, se sigue que $\mathrm{mcd}(x_1, y_1) = 1$. Si x_1 e y_1 tuvieran un factor común, por la definición de x_0 e y_0 estos tendrían el mismo factor común, llegando a una contradicción al tener $\mathrm{mcd}(x_0, y_0) = 1$. □

[7] Con la notación actual, donde se escribe b en vez de $2b$, en la segunda ecuación se multiplicarían los términos $a\alpha\beta$ y $c\gamma\delta$ por 2 y no aparecería el 2 que acompaña a b en la primera y tercera ecuación.

Existe una relación entre las representaciones propias y las equivalencias:

Lema 1.10. *Una forma $f(x,y)$ representa propiamente al entero m si y solo si $f(x,y)$ es equivalente a la forma $mx^2+Bxy+Cy^2$ para ciertos B, C enteros.*

Demostración. Para la primera implicación supongamos que $f(p,q)=m$, donde p y q son coprimos. Por la identidad de Bezout, podemos encontrar enteros r y s tales que $ps-qr=1$. Si $f(x,y)=ax^2+bxy+cy^2$, entonces

$$f(px+ry,qx+sy)=f(p,q)x^2+(2apr+bps+brq+2cqs)xy+f(r,s)y^2=mx^2+Bxy+Cy^2$$

es la forma que buscábamos. Para probar el recíproco, observamos que $mx^2+Bxy+Cy^2$ representa m propiamente tomando $(x,y)=(1,0)$, como queríamos demostrar. □

El discriminante tiene gran influencia sobre ciertos aspectos de la forma. Uno es la paridad de sus coeficientes: como $D=b^2-4ac$, resulta $D\equiv b^2\,(\text{mód }4)$, de lo que se sigue que el coeficiente b será par (respectivamente impar) si y solo si $D\equiv 0\,(\text{mód }4)$ (respectivamente $D\equiv 1\,(\text{mód }4)$). Como los cuadrados solo pueden ser $0\,(\text{mód }4)$ o 1 (mód 4), esto implica que los discriminantes solo pueden tomar dichos valores.

Para saber cuándo un entero m puede ser representado por una forma de discriminante D tenemos el siguiente lema:

Lema 1.11. *Sea $D\equiv 0,1\,(\text{mód }4)$ un entero y m un entero impar coprimo con D. Entonces m se representa propiamente por una forma de discriminante D si y solo si D es un residuo cuadrático*[8] *módulo m.*

Demostración. Si $f(x,y)$ representa propiamente a m, por el Lema 1.10 podemos asumir que $f(x,y)=mx^2+bxy+cy^2$. Entonces, $D=b^2-4mc$, de modo que $D\equiv b^2$ (mód m). Recíprocamente, supongamos que $D\equiv b^2\,(\text{mód }m)$. Como m es impar y sabiendo que b y D poseen la misma paridad por ser $D\equiv b^2\,(\text{mód }4)$, el hecho de que $D\equiv 0,1\,(\text{mód }4)$ implica que $D\equiv b^2\,(\text{mód }4m)$. Esto significa que $D=b^2-4mc$ para algún $c\in\mathbb{Z}$. Por tanto, $mx^2+bxy+cy^2$ representa propiamente a m, tiene discriminante D y los coeficientes son coprimos entre sí debido a que m es coprimo con D. Si $\text{mcd}(m,b)=n$, entonces $D=(n\cdot b')^2-4n\cdot m'c$ para unos b', $m'\in\mathbb{Z}$ y $D=n\cdot[n(b')^2-4m'c]$, por lo que $\text{mcd}(m,D)=n$. □

Existe un lema de especial interés sobre formas primitivas:

Lema 1.12. *Dada una forma primitiva $f(x,y)$ y un entero M, entonces $f(x,y)$ representa propiamente al menos un número coprimo con M.*

Demostración. Sea $f(x,y)=ax^2+bxy+cy^2$ una forma primitiva y M un número entero. Podemos afirmar que, para todo p primo, al menos un valor de $f(1,0)$, $f(0,1)$ o $f(1,1)$ es coprimo con p. Si no fuera así, entonces existirían unos n_1, n_2, $n_3\in\mathbb{N}$

[8] Gauss demostró un teorema análogo ([10], #154, pág. 122), aunque solo demostró la implicación de izquierda a derecha, no especificó que m fuera impar ni tampoco que $D\equiv 0,1\ (\text{mód }4)$.

tales que $\text{mcd}(f(1,0),p) = n_1$, $\text{mcd}(f(0,1),p) = n_2$ y $\text{mcd}(f(1,1),p) = n_3$. Como p es primo y sus únicos divisores son 1 y p, esto implica que necesariamente $n_1 = n_2 = n_3 = p$. Sin embargo, al ser $f(1,0) = a$ y $f(0,1) = c$, entonces $\text{mcd}(a,c) = p$ y llegaríamos a una contradicción, puesto que la forma es primitiva.

Ahora, sea M descompuesto como $M = sig(m)p_1^{r_1} \cdot p_2^{r_2} \cdots p_s^{r_s}$, con p_i primo para todo $i = 1, \ldots, s$ y siendo $sig(m)$ el signo de m. Por lo anterior, sabemos que para todo $i \in \{1, \ldots, s\}$ existen $\alpha_i, \beta_i \in \{0,1\}$ tales que $\text{mcd}(\alpha_i, \beta_i) = 1$ y $f(\alpha_i, \beta_i) \not\equiv 0 \pmod{p_i}$. Por el Teorema Chino del Resto, existen $x_0, y_0 \in \mathbb{Z}$ tales que

$$\begin{aligned} x_0 &\equiv \alpha_1 \pmod{p_1}, & y_0 &\equiv \beta_1 \pmod{p_1}, \\ x_0 &\equiv \alpha_2 \pmod{p_2}, & y_0 &\equiv \beta_2 \pmod{p_2}, \\ &\vdots & &\vdots \\ x_0 &\equiv \alpha_s \pmod{p_s}, & y_0 &\equiv \beta_s \pmod{p_s}. \end{aligned}$$

De esta manera, para cualquier $i \in \{1, \ldots, s\}$, se tiene

$$f(x_0, y_0) = ax_0^2 + bx_0y_0 + cy_0^2 \equiv a\alpha_i^2 + b\alpha_i\beta_i + c\beta_i^2 = f(\alpha_i, \beta_i) \not\equiv 0 \pmod{p_i},$$

por lo que $\text{mcd}(f(x_0, y_0), M) = 1$.

Por último, basta ver que podemos escoger x_0 e y_0 coprimos. Por el Teorema Chino del Resto se había conseguido $x_0 \equiv \alpha \pmod{M}$ e $y_0 \equiv \beta \pmod{M}$ y, por el Teorema de Dirichlet de primos en progresiones aritméticas, al existir infinitos primos representando cada clase en $\mathbb{Z}/M\mathbb{Z}$, se pueden escoger x_0 e y_0 primos, resultando $\text{mcd}(x_0, y_0) = 1$. □

El signo del discriminante también causa un fuerte efecto en el comportamiento de la forma. Si $f(x,y) = ax^2 + bxy + cy^2$, se tiene

$$4af(x,y) = (2ax + by)^2 - Dy^2. \tag{1.3}$$

A partir del estudio de (1.3) obtenemos las siguientes definiciones:

Definición 1.13. Si $D > 0$, entonces $f(x,y)$ representa tanto valores positivos como valores negativos. A las formas de este tipo las denotamos formas **indefinidas**. Si $D < 0$, la forma representa o únicamente valores positivos o únicamente valores negativos, dependiendo del signo de a, denominándolas **definidas positivas** o **definidas negativas** respectivamente.

Observación 1.14. Todas las formas equivalentes serán ambas o bien definidas positivas, o bien definidas negativas, o bien indefinidas. Esto se deduce del Lema 1.9.

Gracias a la Definición 1.13 se puede introducir el siguiente concepto:

Definición 1.15. Una forma binaria cuadrática primitiva definida positiva $f(x,y) = ax^2 + bxy + cy^2$ es **reducida** si $-a < b \leq a < c$ o $0 \leq b \leq a = c$.

Nota 1.16. La noción de formas reducidas también se aplica a formas indefinidas y a formas definidas negativas pero con otras condiciones. No obstante, nos centraremos en el uso para formas definidas positivas, ya que la teoría para el resto es mucho más compleja y se escapa de nuestros intereses.

Lema 1.17. *Las formas reducidas satisfacen* $|b| \leq a \leq c$ *y, cuando* $|b| = a$ *o* $a = c$, *entonces* $b \geq 0$. *Cuando sea conveniente se usará esta definición equivalente.*

Demostración. Partiendo del caso (a): $-a < b \leq a < c$ o (b): $0 \leq b \leq a = c$, de (a) obtenemos que $|b| < a < c$, por lo que basta probar que en los extremos se consigue $b \geq 0$ para finalizar. Sea $|b| = a$ y supongamos que $b < 0$. Entonces $b = -a$, lo que es imposible por (a). Por último, si $a = c$, de (b) se sigue, de manera directa, que $b \geq 0$.

Para el recíproco, comenzamos con (A): $|b| \leq a \leq c$ o (B): si $|b| = a$ o $a = c$, entonces $b \geq 0$. De (A) obtenemos que $-a \leq b \leq a \leq c$, por lo que para conseguir (a) solamente se necesita probar que no es posible tener $b = -a < 0$ ni $a = c$. Lo primero se sigue de (B), ya que si $b = -a$, entonces $|b| = a$, caso en el que resulta $b \geq 0$, por lo que obtendríamos una contradicción. Por otro lado, si $a = c$, entonces $b \geq 0$ por (B), y por (A), finalmente, resulta $0 \leq b \leq a = c$. □

Gauss define[9] por primera vez las formas reducidas de la siguiente manera: "Partiendo de una forma cualquiera (a, b, a') cuyo determinante negativo sea $= -D$, donde D es un número positivo, se debe encontrar una forma (A, B, C) propiamente equivalente a esta, en la cual A no sea mayor que $\sqrt{\frac{4D}{3}}$, ni mayor que C, ni menor que $2B$. A las formas de este tipo las denotaremos como *formas reducidas*".

Para demostrar la analogía entre la definición de Gauss y la de 1.15, tomaremos los términos en minúscula y D como los de nuestra definición y los términos en mayúscula y $-\tilde{D}$ como la de Gauss. La comparación entre a y c con la de A y C se sigue al tener $A \leq C$ como hipótesis, y $A \geq 2B$ se obtiene al considerar $2B = b$ ya que, entonces, $a \geq b$ es otra de las hipótesis. Veamos por último qué ocurre con la cota $\sqrt{\frac{4\tilde{D}}{3}}$.

$$-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2 \Rightarrow a \leq \sqrt{\frac{-D}{3}}. \tag{1.4}$$

Como se tenía por la terminología de Gauss que $D = -4\tilde{D}$, obtenemos la cota deseada.

La motivación de Gauss para definir formas reducidas residía en poder buscar formas que pudieran ser, de algún modo, representantes del resto de formas y con los coeficientes más pequeños posibles, para poder tratar únicamente con estas sin tener que complicarse en los cálculos y propiedades. Esto se debe a que, como se probará más adelante, toda forma es equivalente a una única forma reducida.

Ejemplo 1.18. Vamos a ver cómo hallar, utilizando la cota de (1.4) y el Lema 1.17, formas reducidas de un discriminante dado. Sea $D = -68$, se tiene que $a \leq \sqrt{-(-68)/3} < \sqrt{25} = 5$. Por tanto, podemos partir de $|b| \leq a \leq 4$ para dividir en casos en función del valor de a y usando que $b^2 - 4ac = -68$.

Si $a = 0$, se tiene que $-68 = b^2$, lo cual es imposible. Si $a = 1$, entonces $|b| \leq 1$ y $b^2 - 4c = -68$, por lo que hemos de evaluar las diferentes posibilidades para b. Cuando $b = 0$ se obtiene $c = 17$, de lo que obtenemos la forma reducida $x^2 + 17y^2$. Por otro lado, si $|b| = 1$, se tiene $c = \frac{69}{4} \notin \mathbb{Z}$, de modo que no existe solución en este caso.

[9] [10], #171, pág. 148.

Para $a = 2$, tenemos que $|b| \leq 2$ y $b^2 - 8c = -68$. Sustituyendo b por las diferentes posibilidades, la única que da soluciones con $a, b, c \in \mathbb{Z}$ es $|b| = 2$ y $c = 9$. Como $|b| = a$, entonces $b \geq 0$, por lo que se obtiene la forma reducida $2x^2 + 2xy + 9y^2$.

De la misma manera, para $a = 3$, la única solución con coeficientes enteros es $|b| = 2$ y $c = 6$, lo que da lugar a las formas reducidas $3x^2 \pm 2xy + 6y^2$. Como para $a = 4$ no se satisface $b^2 - 16c = -68$ con valores enteros, las únicas formas reducidas de discriminante $D = -68$ son las mencionadas anteriormente.

Una propiedad muy importante sobre formas reducidas es la siguiente:

Lema 1.19. *Si f y g son dos formas reducidas equivalentes, entonces $f = g$.*

Demostración. Sean $f(x, y) = ax^2 + bxy + cy^2$ y $g(x, y) = a'x^2 + b'xy + c'y^2$ dos formas reducidas. Si $x, y \in \mathbb{Z}\backslash\{0\}$ y $|x| \geq |y|$, entonces

$$f(x, y) \geq |x|(a|x| - |by|) + c|y|^2 \geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Análogamente, si $|y| \geq |x|$, también se obtiene $f(x, y) \geq a - |b| + c$. Esta cota implica que los tres valores más pequeños que puede representar $f(x, y)$ con $\mathrm{mcd}(x, y) = 1$ son a, c y $a - |b| + c$, y precisamente en ese orden por la definición de forma reducida del Lema 1.17, obteniéndose mediante $(x, y) = (1, 0)$, $(x, y) = (0, 1)$ y $(x, y) = (1, \pm 1)$ respectivamente. Por el Lema 1.9, g representa los mismos valores que f cuando $\mathrm{mcd}(x, y) = 1$, y como g es también reducida, es necesario que $a = a'$, ya que son ambos el valor más pequeño que representan dichas formas.

Tras esto, hemos de distinguir los casos $a < c$ y $a = c$. Veamos lo que ocurre cuando $a < c$. En este caso, $a < c \leq a - |b| + c$. Si $a = c'$, entonces el entero a podría tener más representaciones mediante la forma g que mediante f. Por lo tanto, $a < c'$, lo que implica $c = c'$ al ser ambos los siguientes valores más pequeños después de $a = a'$ que se pueden representar por ambas formas. Definiendo D como el discriminante de f (y por tanto de g), de $b^2 = D + 4ac = (b')^2$ se sigue que $|b| = |b'|$, luego solamente queda demostrar que $b = -b'$ implica $b = 0$. Al ser g reducida, se tiene $-a < -b$, por lo que $a \neq b$ y podemos asumir que $-a < b < a < c$. De esta manera, se tiene que $f(x, y) \geq a - |b| + c > c > a$ para todos los $x, y \in \mathbb{Z}\backslash\{0\}$. Después, si consideramos $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$ la matriz de la transformación de f a g, se puede apreciar que

$$a' = f(p, r), \quad b' = 2apq + b(ps + qr) + 2crs, \quad c' = f(q, s). \tag{1.5}$$

En este caso, $a' = a = ap^2 + bpr + cr^2$, obteniéndose de $p = \pm 1$ y $r = 0$. Ahora, de $ps - qr = 1$ se sigue que $s = \pm 1$, y como $c = f(q, s)$ resulta $q = 0$. Sustituyendo en b' se sigue que $b = b'$, por lo que $b = 0$.

Por último, queda considerar el caso $a = c$. Aquí, el valor a tiene las 2 representaciones que ya tenía más las 2 de c, tanto por la forma f como por g, lo que implica que $c' = a = c$. Se obtiene de nuevo $|b| = |b'|$, pero en esta situación, al tener como hipótesis $b \geq 0$ y $b' \geq 0$ por la definición de forma reducida, se tiene $b = b'$. □

Uno de los resultados fundamentales sobre formas reducidas es el siguiente:

Teorema 1.20. *Toda forma primitiva definida positiva es equivalente a una única forma reducida.*[10]

Demostración. Sean U, V^+ y V^- las matrices

$$U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad V^+ = \begin{pmatrix} 1 & +1 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad V^- = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

Vamos a probar que, aplicando estas transformaciones, podemos conseguir en un número finito de pasos $|b| \leq a \leq c$. Computando, se tiene que $U^T F U = \begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix}$, lo que implica que U intercambia a y c, por lo que si teníamos $a > c$ en F, ahora tendremos $a < c$ en $U^T F U$. Además,

$$(V^\pm)^T F V^\pm = \begin{pmatrix} a & \pm a + b/2 \\ \pm a + b/2 & a \pm b + c \end{pmatrix},$$

por lo que $V^\pm$ sustituye b por $b \pm 2a$, mientras que a se mantiene. Por consiguiente, aplicando esta transformación en un número finito de ocasiones, podemos obtener $|b| \leq a$, ya que cada aplicación V^+ hace que a sea más pequeño en proporción.

Si $b = -a$, aplicando la matriz $V^\pm$, podemos conseguir $b = a$, mientras que c no varía. Si $a = c$, se puede obtener $b \geq 0$ aplicando la matriz U.

Por último, la unicidad de dicha forma reducida se sigue del Lema 1.19. □

Ejemplo 1.21. Como toda forma es equivalente a una forma reducida, vamos a utilizar la metodología empleada en el Teorema 1.20 para hallar formas reducidas asociadas a una forma binaria cuadrática.

Sea $f(x, y) = 73x^2 + 54xy + 10y^2$ cuya matriz asociada es $F = \begin{pmatrix} 73 & 27 \\ 27 & 10 \end{pmatrix}$. Aplicando las matrices U y $V^\pm$ como sigue, llegamos a

$$F \xrightarrow[U]{a>c} \begin{pmatrix} 10 & -27 \\ -27 & 73 \end{pmatrix} \xrightarrow[V^+]{|b|>a,\, b<0} \begin{pmatrix} 10 & -17 \\ -17 & 29 \end{pmatrix} \xrightarrow[V^+]{|b|>a,\, b<0} \begin{pmatrix} 10 & -7 \\ -7 & 5 \end{pmatrix} \xrightarrow[U]{a>c} \begin{pmatrix} 5 & 7 \\ 7 & 10 \end{pmatrix}$$
$$\xrightarrow[V^-]{|b|>a,\, b>0} \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} \xrightarrow[U]{a>c} \begin{pmatrix} 1 & -2 \\ -2 & 5 \end{pmatrix} \xrightarrow[V^+]{|b|>a,\, b<0} \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \xrightarrow[V^+]{|b|>a,\, b<0} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

siendo esta última la matriz deseada al cumplir las condiciones de la definición de forma reducida, por lo que la forma reducida asociada resulta $x^2 + y^2$.

Observación 1.22. Existe otro método para encontrar formas reducidas asociadas a una cierta forma utilizando números complejos. En el Apéndice C se podrá encontrar más información al respecto.

Como las formas reducidas $f(x, y) = ax^2 + bxy + cy^2$ cumplen la cota de (1.4) existe solamente un número finito de elecciones para a. En consecuencia, como se tiene que $|b| \leq a$, lo mismo ocurre para b en caso de que tengamos un D fijo y, al ser $D = b^2 - 4ac$, análogamente sucede con c. De aquí se sigue el siguiente corolario:

[10] Gauss probó este resultado en [10], #172, pág. 151.

Corolario 1.23. *Existe únicamente un número finito*[11] *de formas reducidas para un discriminante dado D.*

1.2.1. Clases

Antes de continuar se recuerda que en toda ocasión se está trabajando con formas binarias cuadráticas de $D < 0$.

Se dice que dos formas están en la misma **clase** si son equivalentes. Denotamos por $C(D)$ al conjunto de clases de formas primitivas definidas positivas de discriminante D y por $h(D)$ al número de clases de formas de este mismo tipo que, por el Teorema 1.20 es, precisamente, el número de formas reducidas.

Del hecho de que existan un número finito de formas reducidas y de que toda forma primitiva definida positiva sea equivalente a una forma reducida se sigue el siguiente teorema:

Teorema 1.24. *Sea $D < 0$. Entonces el número $h(D)$ de clases de formas primitivas definidas positivas de discriminante D es finito y, además, coincide con el número de formas reducidas de discriminante D.*

Ejemplo 1.25. Para discriminantes pequeños es fácil computar formas reducidas y números de clases.[12] En la siguiente tabla se muestran algunos ejemplos:

D	$h(D)$	**Formas reducidas de discriminante D**
-4	1	$x^2 + y^2$
-8	1	$x^2 + 2y^2$
-12	1	$x^2 + 3y^2$
-20	2	$x^2 + 5y^2$, $2x^2 + 2xy + 3y^2$
-56	4	$x^2 + 14y^2$, $2x^2 + 7y^2$, $3x^2 \pm 2xy + 5y^2$
-68	4	$x^2 + 17y^2$, $2x^2 + 2xy + 9y^2$, $3x^2 \pm 2xy + 6y^2$
-108	3	$x^2 + 27y^2$, $4x^2 \pm 2xy + 7y^2$
-256	4	$x^2 + 64y^2$, $4x^2 + 4xy + 17y^2$, $5x^2 \pm 2xy + 13y^2$

Observación 1.26. Nótese que $x^2 + ny^2$ siempre es una forma reducida. En efecto, como en este caso $a = 1$, $b = 0$ y $c = n \in \mathbb{N}$, se tiene que $0 < 1 \leq c$.

Para formas indefinidas también existe una teoría similar, pero es mucho más complicada. Además, existen conexiones entre este tipo de formas y las fracciones continuas o con la ecuación de Pell[13].

[11] Gauss también prueba esto en [10], #185, pág. 170, y encuentra dos métodos para encontrar dichas formas.

[12] Para la codificación de las formas reducidas, en `SageMath` existe el comando `BinaryQF_reduced_representatives(n)`, que proporciona las formas reducidas existentes de discriminante n.

[13] Es lo que Gauss trata en [10], #183–205, págs. 166–204, si bien no hace mención de que sean fracciones continuas ni la ecuación de Pell como tal.

1.2.2. Composición

Introducción

Uno de las conceptos más importantes y complejos de la teoría sobre formas binarias cuadráticas que desarrolló Gauss fue la *composición*, debido a todos los resultados que se derivaron de esta. Vamos a proceder a mostrar los resultados más importantes del matemático en este área. En primer lugar, veamos un par de ejemplos para comprender el sentido de la composición.

Ejemplo 1.27. Sea la forma $x^2 + y^2$ de discriminante $D = -4$. Multiplicándola consigo misma resulta $(x^2+y^2)(z^2+w^2) = (xz+yw)^2+(xw-yz)^2$, e intercambiando $xz + yw$ por x' y $xw - yz$ por y' nos vuelve a dar la forma $(x')^2 + (y')^2$.

Ejemplo 1.28. Sea la forma $2x^2 + 2xy + 3y^2$ de discriminante $D = -20$. Podemos apreciar que

$$(2x^2 + 2xy + 3y^2)(2z^2 + 2zw + 3w^2) = (2xz + xw + yz + 3yw)^2 + 5(xw - yz)^2.$$

Sustituyendo por $x' = 2xz+xw+yz+3yw$ e $y' = xw-yz$, resulta la forma $(x')^2+5(y')^2$, que es la única otra forma reducida de discriminante $D = -20$.

Esto indica que, multiplicando ciertas formas de discriminante D y realizando un cambio de variables, podemos encontrar otra con el mismo discriminante. Con esto Gauss dio lugar al concepto de *composición* de dos formas primitivas definidas positivas de discriminante D. De manera más formal, podemos escribir la composición entre $f(x, y)$ y $g(x, y)$, denotada como $\mathfrak{F}(x, y)$, de la siguiente manera:

$$f(x, y)g(z, w) = \mathfrak{F}(B_1(x, y; z, w), B_2(x, y; z, w)) \tag{1.6}$$

donde $B_i(x, y; z, w) = a_i xz + b_i xw + c_i yz + d_i yw$ para $i = 1, 2$ son formas bilineales con coeficientes enteros.

Gauss lo define[14] introduciendo el concepto de forma *transformable* para denotar a $\mathfrak{F}$ como la forma *transformable* de fg.

Tanto Legendre como Gauss trataron la composición de formas binarias cuadráticas. De hecho, Legendre lo hizo unos pocos años antes al presentarlo en *Essai Sur la Théorie des Nombres* [15] en 1798, pero Gauss no tenía constancia de ello hasta que *Disquisitiones* estaba en manos de la editorial. Gauss sabía que Legendre había trabajado otros aspectos como la *Ley de Reciprocidad Cuadrática* como él, pero respecto a este tema le era desconocido que alguien lo hubiera tratado anteriormente. Sin embargo, a pesar de que Gauss fuera un poco posterior, atacó la composición con una precisión, formalidad matemática y completitud que dejó la teoría de Legendre en un segundo plano. La diferencia fundamental entre ambos reside en que Legendre, si bien habló de equivalencias, no distinguió entre equivalencia propia e impropia, lo que hacía que su composición no tuviera un valor único.

[14] [10], #235, pág. 247.

Composición de Dirichlet

El resultado de la teoría de Gauss más importante sobre composición es que, para un discriminante fijo, la composición (tal y como él la definió) convierte el conjunto de clases de formas en un grupo abeliano finito[15]. Aunque no usara la terminología de grupos, su investigación anticipó esta teoría, ya que demostró precisamente lo que resultan las propiedades de los grupos de estas características.

Demostrar esto es largo y complicado ya que la composición gaussiana es un concepto difícil con el que trabajar, y la demostración del matemático es larga y engorrosa. Sin embargo, para solventar este problema, podemos utilizar la *composición de Dirichlet*. Antes de introducir este concepto, enunciaremos primero ciertos lemas:

Lema 1.29. *Sean $u_1, v_1, ..., u_r, v_r, m$ números con $\mathrm{mcd}(u_1, ..., u_r, m) = 1$ y B un entero. Entonces, las congruencias*

$$u_i B \equiv v_i \pmod{m}, \quad i = 1, ..., r,$$

tienen solución única módulo m si y solo si para todo $i, j = 1, ..., r$, se tiene

$$u_i v_j \equiv u_j v_i \pmod{m}. \tag{1.7}$$

Demostración. Para la primera implicación, sea $B \equiv \frac{v_j}{u_j} \pmod{m}$ para todo $i = 1, ..., r$. Sustituyendo el valor de B se obtiene $u_i \frac{v_j}{u_j} \equiv v_i \pmod{m}$, de lo que se sigue $u_i v_j \equiv u_j v_i \pmod{m}$. En la otra dirección, al tener $\mathrm{mcd}(u_1, \ldots, u_r, m) = 1$, por Bezóut existen a, $a_1, \ldots, a_r \in \mathbb{Z}$ tales que $am + \sum_{i=1}^{r} a_i u_i = 1$. Multiplicando todo por v_i, tomando módulo m y utilizando que $u_i v_j \equiv u_j v_i \pmod{m}$, se sigue que

$$v_i \sum_{j=1}^{r} a_j u_j \equiv v_i \pmod{m} \Longrightarrow v_i \sum_{j=1}^{r} a_j u_j \equiv u_i \sum_{j=1}^{r} a_j v_j \equiv v_i \pmod{m}.$$

Sustituyendo $\sum_{j=1}^{r} a_j v_j$ por B obtenemos la ecuación deseada.

Para demostrar la unidad, tomemos dos soluciones x y x'. Para todo $1 \leq i \leq r$ se tiene que $u_i x \equiv u_i x' \pmod{m}$. En particular, para todo primo p y entero $e \geq 1$ tal que $p^e \mid m$ se tiene $u_i x \equiv u_i x' \pmod{p^e}$. Como $\mathrm{mcd}(u_1, \ldots, u_r, m) = 1$, existe i_0 tal que $p \nmid u_{i_0}$. Entonces, de la anterior congruencia, escribiendo $i = i_0$, se deduce que $x \equiv x' \pmod{p^e}$. Como p^e es arbitrario entre las potencias de primo que dividen a m, se concluye que $x \equiv x' \pmod{m}$. □

Lema 1.30. *Sean $f(x, y) = ax^2 + bxy + cy^2$ y $g(x, y) = a'x^2 + b'xy, c'y^2$ dos formas de discriminante D que satisfacen*[16] $\mathrm{mcd}(a, a', (b + b')/2) = 1$. *Entonces, existe un único entero $B = B(f, g)$ módulo $2aa'$ de manera que*

$$\begin{aligned} B &\equiv b \pmod{2a}, \\ B &\equiv b' \pmod{2a'}, \\ B^2 &\equiv D \pmod{4aa'}. \end{aligned}$$

[15] [10], se puede encontrar en los artículos #236-240 y #245-249 de su obra, ya que los distintos resultados que prueba en estos definen las propiedades de un grupo de esta forma.

[16] Ya que, como b y b' tienen la misma paridad al tener la misma que D, $(b + b')/2$ es un entero.

Demostración. Para poder comenzar es necesario reescribir estas congruencias. Si B es un número que satisface las dos primeras, entonces $B^2 - (b+b')B + bb' \equiv (B-b)(B-b') \equiv 0 \pmod{4aa'}$, por lo que la tercera congruencia se puede escribir como $(b+b')B \equiv bb' + D \pmod{4aa'}$. Dividiendo entre 2, se convierte en

$$(b+b')/2 \cdot B \equiv (bb'+D)/2 \pmod{2aa'}. \tag{1.8}$$

Multiplicando las dos primeras congruencias del lema por a' y a respectivamente y combinándolas con (1.8), se puede ver que las tres congruencias iniciales equivalen a

$$\begin{aligned} a' \cdot B &\equiv a'b \pmod{2aa'} \\ a \cdot B &\equiv ab' \pmod{2aa'} \\ (b+b')/2 \cdot B &\equiv (bb'+D)/2 \pmod{2aa'}. \end{aligned} \tag{1.9}$$

Asumiendo que $\mcd(a, a', (b+b')/2) = 1$, las congruencias de (1.9) satisfacen la condición sobre el máximo común divisor del Lema 1.29.

Por último, hemos de comprobar que las condiciones de (1.7) se verifican para (1.9). Para ello, denotemos como (I), (II) y (III) las ecuaciones que forman (1.9) respectivamente. Tomando $u_1 = a'$, $u_2 = a$, $u_3 = \frac{b+b'}{2}$, $v_1 = a'b$, $v_2 = ab'$ y $v_3 = \frac{bb'+D}{2}$ y sustituyendo, obtenemos:

$$\begin{aligned} u_1v_2 = a' \cdot ab' &\overset{(II)}{\equiv} a' \cdot aB \overset{(I)}{\equiv} a \cdot a'b' \pmod{2aa'} = u_2v_1 \\ u_1v_3 = a' \cdot \frac{bb'+D}{2} &\overset{(III)}{\equiv} a' \cdot B\frac{b+b'}{2} \overset{(I)}{\equiv} a' \cdot b\frac{b+b'}{2} \pmod{2aa'} = u_3v_1 \\ u_2v_3 = a \cdot \frac{bb'+D}{2} &\overset{(III)}{\equiv} a \cdot B\frac{b+b'}{2} \overset{(II)}{\equiv} a \cdot b'\frac{b+b'}{2} \pmod{2aa'} = u_3v_2. \end{aligned}$$

La existencia y unicidad de la B deseada se sigue inmediatamente del Lema 1.29. □

Proposición 1.31. *Sean $f(x,y) = ax^2 + bxy + cy^2$ y $g(x,y) = a'x^2 + b'xy + c'y^2$ dos formas primitivas definidas positivas de discriminante $D < 0$ que satisfacen $\mcd(a, a', (b+b')/2) = 1$. Definimos la* ***composición de Dirichlet*** *de las formas $f(x,y)$ y $g(x,y)$ como la forma*

$$(f \circ g)(x,y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2, \tag{1.10}$$

donde $B = B(f,g)$ (véase Lema 1.30). Entonces, la composición de Dirichlet $(f \circ g)(x,y)$ es una forma primitiva definida positiva de discriminante D.

Demostración. La forma $(f \circ g)(x,y)$ tiene discriminante D pues $B^2 - 4aa'\frac{B^2-D}{4aa'} = B^2 - B^2 + D = D$. Además, como f y g son definidas positivas y, por tanto, satisfacen $a > 0$ y $a' > 0$, resulta $D < 0$ y $aa' > 0$, por lo que $(f \circ g)(x,y)$ es definida positiva.

El siguiente paso es probar que $(f \circ g)(x,y)$ es composición de $f(x,y)$ y $g(x,y)$. Sea $C = (B^2 - D)/4aa'$, de manera que $(f \circ g)(x,y) = aa'x^2 + Bxy + Cy^2$. Se puede probar que $f(x,y) \sim ax^2 + Bxy + a'Cy^2$ y $g(x,y) \sim a'x^2 + Bxy + aCy^2$. Sea $F = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ la

matriz asociada a f. Por las congruencias del Lema 1.30, buscamos un B que cumpla $B \equiv b \pmod{2a}$, por lo que será de la forma $B = b + 2an$ para algún $n \in \mathbb{Z}$. Si $B > 0$, aplicando la matriz V^+ de la prueba del Teorema 1.20 se obtiene

$$F \xrightarrow{V^+} \begin{pmatrix} a & \frac{2a+b}{2} \\ \frac{2a+b}{2} & a+b+c \end{pmatrix} \xrightarrow{V^+} \begin{pmatrix} a & \frac{4a+b}{2} \\ \frac{4a+b}{2} & c' \end{pmatrix} \xrightarrow{V^\pm} \cdots \xrightarrow{V^+} \begin{pmatrix} a & an+b/2 \\ an+b/2 & \tilde{C} \end{pmatrix},$$

de modo que aplicando n veces V^+ se incrementa b hasta $b+2an$, justo como la B que buscábamos. Análogamente se haría con V^- si $B < 0$. Para determinar $\tilde{C}$, sabemos que $D = B^2 - 4a\tilde{C}$, por lo que $\tilde{C} = \frac{B^2-D}{4a} = a'C$, como queríamos. De la misma manera, aplicando la matriz $V^\pm$ las veces que sea necesaria a g, obtenemos la forma $a'x^2 + Bxy + aCy^2$.

Para estas dos últimas formas mencionadas se tiene la igualdad:

$$(ax^2 + Bxy + a'Cy^2)(a'z^2 + Bzw + aCw^2) = (f \circ g)(X, Y),$$

donde $X = xz - Cyw$ e $Y = axw + a'yz + Byw$. De aquí se sigue que $(f \circ g)(x, y)$ es la composición de $f(x, y)$ y $g(x, y)$.

Para ver que $(f \circ g)(x, y)$ es primitiva, supongamos que cierto primo p divide a todos los coeficientes. Entonces, p divide a todos los valores representados por $(f \circ g)(x, y)$. Como $(f \circ g)(x, y)$ es la composición de $f(x, y)$ y $g(x, y)$, esto implica que p divide a todos los números de la forma $f(x, y)g(w, z)$. Pero $f(x, y)$ y $g(x, y)$ son primitivas por lo que, por el Lema 1.12, representan números coprimos con p. Por ello, $f(x, y)g(w, z)$ también representaría un número coprimo con p, lo que resulta una contradicción. □

Existe un tipo de formas binarias cuadráticas de especial interés:

Definición 1.32. Sea un entero negativo $D \equiv 0, 1 \pmod 4$, la **forma principal** se define como

$$\begin{aligned} x^2 - \frac{D}{4}y^2 &\quad \text{si } D \equiv 0 \pmod 4, \\ x^2 + xy + \frac{1-D}{4}y^2 &\quad \text{si } D \equiv 1 \pmod 4. \end{aligned}$$

Es fácil ver que la forma principal tiene discriminante D y que es reducida. En efecto, para el caso $D \equiv 0 \pmod 4$, el discriminante es igual a $-4 \cdot 1 \cdot \frac{-D}{4} = D$, y es reducida ya que $0 < 1 \leq -\frac{-D}{4} = \frac{4n}{4} = n$ para algún $n \in \mathbb{N}$; cuando tenemos $D \equiv 1 \pmod 4$, el discriminante resulta $1^2 - 4 \cdot 1 \cdot \frac{1-D}{4} = 1 - (1 - D) = D$, y es reducida al ser $1 = 1 \leq \frac{1-D}{4} = \frac{1+4n-1}{4} = n$ para algún $n \in \mathbb{N}$, ya que $D < 0$.

Nuestro principal interés es probar que la composición de Dirichlet convierte a $C(D)$ en un grupo abeliano finito, pero antes se han de introducir ciertos resultados:

Lema 1.33. *Sean $f(x, y) = a_1x^2 + b_1xy + c_1y^2$ y $g(x, y) = a_2x^2 + b_2xy + c_2y^2$ dos formas con el mismo discriminante y que satisfacen $a_1 = a_2$ y $b_1 \equiv b_2 \pmod{2a_1}$. Entonces, dichas formas son equivalentes.*

Demostración. Se podrá encontrar en el Apéndice B. □

Lema 1.34. *Sean* $f_1(x,y) = a_1x^2 + b_1xy + c_1y^2$ *y* $g_1(x,y) = a_2x^2 + b_2xy + c_2y^2$ *dos formas con el mismo discriminante y tales que* $\mathrm{mcd}(a_1, a_2, \frac{b_1+b_2}{2}) = 1$. *Entonces, existen dos enteros* B *y* C *para los que las formas* $f_2(x,y) = a_1x^2 + Bxy + a_2Cy^2$ *y* $g_2(x,y) = a_2x^2 + Bxy + a_1Cy^2$ *cumplen que* $f_1 \sim f_2$, $g_1 \sim g_2$, $\mathrm{mcd}(a_1, a_2, B) = 1$ *y tienen el mismo discriminante.*

Demostración. Se podrá encontrar en el Apéndice B. □

Lema 1.35. *Dos formas* $f(x,y) = a_1x^2 + b_1xy + c_1y^2$ *y* $g(x,y) = a_2x^2 + b_2xy + c_2y^2$ *del mismo discriminante son equivalentes si y solo si existen enteros* α *y* γ *tales que*

$$\begin{aligned} a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2 &= a_2 \\ 2a_1\alpha + (b_1 + b_2)\gamma &\equiv 0 \pmod{2a_2} \\ (b_1 - b_2)\alpha + 2c_1\gamma &\equiv 0 \pmod{2a_2}. \end{aligned}$$

Demostración. Se podrá encontrar en el Apéndice B. □

Teorema 1.36. *Sean las formas* $f_1(x,y) = a_1x^2 + Bxy + a_2Cy^2$ *y* $f_2(x,y) = a_2x^2 + Bxy + a_1Cy^2$ *de igual discriminante y* $f_3(x,y) = m_1x^2 + Nxy + m_2Ly^2$ *y* $f_4(x,y) = m_2x^2 + Nxy + m_1Ly^2$ *con la misma condición; además,* $\mathrm{mcd}(a_1, a_2, B) = \mathrm{mcd}(m_1, m_2, N) = 1$. *Entonces, si* $f_1 \sim f_3$ *y* $f_2 \sim f_4$, *se cumple que* $f_1 \circ f_2 \sim f_3 \circ f_4$.

Demostración. Como esta prueba consta únicamente de resoluciones de congruencias y ecuaciones, se podrá encontrar en el Apéndice B. □

Con estos resultados se puede demostrar el siguiente teorema:

Teorema 1.37. *Sea* $D \equiv 0, 1 \pmod 4$ *un entero negativo y* $C(D)$ *el conjunto de clases de formas primitivas definidas positivas de discriminante* D. *Entonces, la composición de Dirichlet induce una operación bien definida en* $C(D)$ *que convierte a* $C(D)$ *en un grupo abeliano finito cuyo orden es el número de clases* $h(D)$.

Además, la inversa de la clase que contiene a la forma $ax^2 + bxy + cy^2$ *es la clase que contiene a* $ax^2 - bxy + cy^2$, *la forma opuesta de* $ax^2 + bxy + cy^2$.

Demostración. El primer paso es comprobar que la composición de Dirichlet está definida para cualquier par de clases en $C(D)$. Esto se sigue de los Lemas 1.10 y 1.12, ya que nos permiten trabajar con una forma $f(x,y) = ax^2 + bxy + cy^2$ dada y otra forma g que sea equivalente a una cierta $g' = a'x^2 + b'xy + c'y^2$, de modo que $\mathrm{mcd}(a, a') = 1$ y, como todas tienen el mismo discriminante, se puede aplicar la composición de Dirichlet.

En segundo lugar, hemos de demostrar que la operación está bien definida en el nivel de clases. Sean f y g formas de mismo discriminante. Por lo comentado anteriormente, existen una $\tilde{g}$ tal que $g \sim \tilde{g}$ y f y $\tilde{g}$ cumplen la condición deseada del máximo común divisor. Mediante el Lema 1.34, podemos encontrar $\hat{f}(x,y) = a_1x^2 + Bxy + a_2Cy^2$ y $\hat{g}(x,y) = a_2x^2 + Bxy + a_1Cy^2$ que son equivalentes a f y $\tilde{g}$

respectivamente. Entonces, denotando por $[f]$ a la clase de la forma f y haciendo un abuso de notación denotando la composición de clases con $\circ$, resulta

$$[f] \circ [g] = [\hat{f}] \circ [\hat{g}] := [\hat{f} \circ \hat{g}],$$

la primera igualdad proviene de la definición de clase y la segunda del Teorema 1.36.

Para probar la asociatividad, sean las formas $f_i(x, y) = a_i x^2 + b_i xy + c_i y^2$ para $i = 1, 2, 3$ con el mismo discriminante. Por los Lemas 1.10 y 1.12, es posible encontrar una forma equivalente a f_2 de modo que $\text{mcd}(a_1, a_2, a_3) = 1$, de modo que todos los pares de formas que se van a escoger en la demostración posean la condición de coprimalidad necesaria. Para simplificar la notación, seguiremos denotando por f_2 a dicha forma equivalente, y consideramos la siguiente composición:

$$([f_1] \circ [f_2]) \circ [f_3] = [a_1 a_2 x^2 + Bxy + Cy^2] \circ [f_3] = [a_1 a_2 a_3 x^2 + B'xy + C'y^2].$$

Por el Lema 1.33 se deduce que, asumiendo la igualdad de discriminante, la condición necesaria y suficiente para que B' cumpla la última igualdad es $B' \equiv b_i \pmod{2a_i}$ para $i = 1, 2, 3$. Ahora, considerando la composición

$$[f_1] \circ ([f_2] \circ [f_3]) = [f_1] \circ [a_2 a_3 x^2 + \beta xy + \gamma y^2] = [a_1 a_2 a_3 x^2 + \beta' xy + \gamma' y^2]$$

se llega a las mismas congruencias para β', de lo que se sigue que $B' \equiv \beta' \pmod{2a_1 a_2 a_3}$ ya que $\text{mcd}(a_1, a_2, a_3) = 1$. Teniendo en cuenta que ambas formas tienen el mismo primer término $a_1 a_2 a_3$ y usando el Lema 1.33, podemos afirmar que son equivalentes, concluyendo la demostración de la asociatividad.

El siguiente paso será probar que la clase principal es el elemento identidad de $C(D)$. Para ello, vamos a probar que $x^2 + bxy + cy^2$ es equivalente a la forma principal. Si $D \equiv 0 \pmod 4$, entonces b es par, por lo que podemos escribirlo como $b = 2b'$ con $b' \in \mathbb{Z}$. Utilizando b' veces la matriz $V^{\pm}$ de la prueba del Teorema 1.20,

$$\begin{pmatrix} 1 & b' \\ b' & c \end{pmatrix} \xrightarrow{V^{\pm}} \cdots \xrightarrow{V^{\pm}} \begin{pmatrix} 1 & 0 \\ 0 & -D/4 \end{pmatrix},$$

obteniendo la forma principal $x^2 - \frac{D}{4} y^2$. Por otro lado, si $D \equiv 1 \pmod 4$, b es impar, por lo que lo podemos escribir como $b = 2n + 1$ con $n \in \mathbb{Z}$. Aplicando n veces $V^{\pm}$,

$$\begin{pmatrix} 1 & n + 1/2 \\ n + 1/2 & c \end{pmatrix} \xrightarrow{V^{\pm}} \cdots \xrightarrow{V^{\pm}} \begin{pmatrix} 1 & 1/2 \\ 1/2 & (1 - D)/4 \end{pmatrix}.$$

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

Sean $f(x, y) = a_1 x^2 + b_1 xy + c_1 y^2$ y $g(x, y) = a_2 x^2 + b_2 xy + c_2 y^2$ dos formas de discriminante D. Nótese que $x^2 + b_1 xy + c_1 y^2 \sim x^2 + b_2 xy + c_2 y^2$ por el Lema 1.33, ya que tienen el mismo discriminante, el mismo primer término y $b_1 \equiv b_2 \pmod 2$, por lo que se encuentran en la misma clase. Se tiene que

$$\begin{aligned}[x^2 + b_1 xy + c_1 y^2] \circ [a_2 x^2 + b_2 xy + c_2 y^2] &= [x^2 + Bxy + a_2 C y^2] \circ [a_2 x^2 + Bxy + Cy^2] \\ &= [a_2 x^2 + Bxy + Cy^2] = [a_2 x^2 + b_2 xy + c_2 y^2]\end{aligned}$$

donde la primera igualdad se sigue del Lema 1.34 y la última del hecho de que $B \equiv b_2 \pmod{2a_2}$, por lo que podemos usar el Lema 1.33.

Por último, dada $f(x,y) = ax^2+bxy+cy^2$, su opuesta es $\tilde{f}(x,y) = ax^2-bxy+cy^2$. Como $\mcd(a,a,(b+(-b))/2) = a$ y puede que sea mayor que 1, no se puede aplicar la composición de Dirichlet directamente. Pero si se utiliza la equivalencia $(x,y) \to (-y,x)$, entonces se puede utilizar la forma equivalente $g(x,y) = cx^2+bxy+ay^2$. Como $\mcd(a,c,(b+b)/2) = \mcd(a,c,b) = 1$, se pueden aplicar las fórmulas de Dirichlet de $f(x,y)$ a $g(x,y)$. Entonces,

$$[f] \circ [\tilde{f}] = [f] \circ [g] = [ax^2+bxy+cy^2] \circ [cx^2+bxy+ay^2] = [acx^2+bxy+y^2]$$

donde la última igualdad se sigue del hecho de que b es una de las soluciones a las congruencias $x \equiv b \pmod{2a}$ y $x \equiv b \pmod{2c}$ y que hace del discriminante un entero, como era necesario. Se tiene que $acx^2+bxy+y^2 \sim x^2-bxy+acy^2$ por el cambio mencionado anteriormente, y como $x^2-bxy+acy^2 \sim x^2+bxy+acy^2$ aplicando b veces la matriz $V^{\pm}$, obtenemos la equivalencia necesaria con la forma principal. Con esto queda demostrado que la inversa es la forma opuesta y, finalmente, que la composición de Dirichlet convierte a $C(D)$ en un grupo abeliano finito. □

Ejemplo 1.38. Vamos a aplicar toda la teoría vista anteriormente para determinar la estructura de $C(-68)$. Por el Ejemplo 1.18 sabemos que $h(-68) = 4$, por lo que solo puede ser o bien $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ o $\mathbb{Z}/4\mathbb{Z}$. Para determinar la estructura adecuada, basta componer sus elementos y ver lo que sucede, por lo que compondremos las formas reducidas que representan cada clase mediante la composicón de Dirichlet consigo mismas y analizaremos el resultado.

Al componer $3x^2+2xy+6y^2$ consigo misma necesitamos un $B \in \mathbb{Z}$ que cumpla $B \equiv 2 \pmod 6$ y $B^2 \equiv -68 \pmod{36}$, por lo que $B = 2$ sirve. En consecuencia, $C = 2$ y obtenemos $9x^2+2xy+2y^2$. Si a esta forma le aplicamos la matriz U resulta $2x^2-2xy+9y^2$ que, cambiando (x,y) por $(-x,y)$, resulta equivalente a la forma $2x^2+2xy+9y^2$. Si componemos esta forma con $3x^2+2xy+6y^2$ el B buscado debe satisfacer $B \equiv -2 \pmod 4$, $B \equiv 2 \pmod 6$ y $B^2 \equiv -68 \pmod{24} \equiv 4 \pmod{24}$, por lo que de nuevo funciona $B = 2$. Se sigue que $C = 3$ y se obtiene $6x^2+2xy+3y^2$. Como no puede haber elementos de orden 3, sabemos que tendremos que componer una vez más, por lo que componiendo esta última con $3x^2+2xy+6y^2$ las condiciones necesarias son, esta vez, $B \equiv 2 \pmod{12}$, $B \equiv 2 \pmod 6$ y $B^2 \equiv -68 \pmod{72} \equiv 4 \pmod{72}$, por lo que también nos vale $B = 2$. Aquí, $C = 1$, y obtenemos $18x^2+2xy+y^2$. Si a esta forma le aplicamos la matriz U y después V^+, obtenemos la forma x^2+17y^2, la forma principal, por lo que $[3x^2+2xy+6y^2]$ tiene orden 4.

Análogamente, la forma reducida $3x^2-2xy+6y^2$ tiene el mismo comportamiento pero empleando $B = -2$ y las formas obtenidas al componer resultan las opuestas de las anteriores. Esto es lógico, al ser la opuesta de una forma su propia inversa por el Teorema 1.37. Por tanto, $[3x^2-2xy+6y^2]$ tiene también orden 4.

Como x^2+17y^2 es la forma principal, sabemos que no existen dos elementos de orden 2 en $C(-68)$, de modo que ha de ser $C(-68) = \mathbb{Z}/4\mathbb{Z}$.

Nótese que en todas las formas utilizadas se cumplen las condiciones de coprimalidad necesarias para aplicar la composición de Dirichlet.

La teoría de Gauss sobre la composición siempre ha sido una de las partes más difíciles de *Disquisitiones* de leer. Parte de la razón reside en la complejidad de la presentación de Gauss ya que, por ejemplo, la prueba de que la composición es asociativa consta de 28 ecuaciones que han de satisfacerse. Por otro lado, también se trata de gran complejidad conceptual, pues requiere un gran nivel de abstracción. Sin embargo, es remarcable la importancia de los avances matemáticos que supuso dicha teoría, ya que consiguió demostrar que la composición formaba un grupo abeliano finito sin tan siquiera haberse definido por aquel entonces el concepto de grupo.

1.3. Más sobre formas binarias cuadráticas

Para poder clasificar formas reducidas de un mismo discriminante tenemos la teoría de *géneros*, cuya idea básica se debe a Lagrange. Dicha teoría es importante, ya que relaciona la congruencia de un primo p en un cierto módulo $(\mathbb{Z}/N\mathbb{Z})$ con las formas reducidas asociadas que pueden representar p.

La teoría de géneros ha sido objeto de cuidadoso estudio durante más de 200 años por la importancia y profundidad que alberga, aunque se trata de un concepto bastante denso al esconder teoría muy abstracta detrás. A pesar de ello, Gauss obtuvo resultados brillantes sobre géneros y en comparación con sus coetáneos, aunque estos no permitían satisfacer de manera concluyente cuestiones como qué formas binarias cuadráticas pueden representar un cierto primo p, solo "acotan" la respuesta.

Todos sus resultados aparecen en *Disquisitiones* entre los artículos #229 y #287. Sin embargo, la definición de géneros de Gauss requiere de muchos conocimientos previos y asignaciones de formas binarias cuadráticas en otros componentes de los géneros como son los *caracteres asignados*, resultando aún más complejo. Además, Gauss considera tanto formas definidas como indefinidas y, en particular, demuestra todos los resultados para cualesquiera discriminantes no cuadrados, positivos y negativos, lo que hace que sus demostraciones sean mucho más complicadas y extensas[17].

Al constar cada género de un número finito de clases, Gauss conjeturó[18] sobre qué discriminantes de la forma $-4n$ constan de una clase por género, obteniendo una lista de 65 discriminantes. Agrupándolos según el número de clases, resultan:

$h(-4n)$	n's con una clase por género
1	$1, 2, 3, 4, 7$
2	$5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58$
4	$21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85,$ $88, 93, 102, 112, 130, 133, 177, 190, 232, 253$
8	$105, 120, 165, 168, 210, 240, 273, 280, 312, 330,$ $345, 357, 385, 408, 462, 520, 760$
16	$840, 1320, 1365, 1848$

[17] [10], Gauss comentó tras exponer toda su teoría: "Estos teoremas se encuentran entre los más hermosos de la teoría de formas binarias, especialmente porque, a pesar de su extrema simplicidad, son tan profundos que una demostración rigurosa requiere la ayuda de otras muchas investigaciones".

[18] [10], #303, págs. 374–375.

Gauss siempre estuvo interesado en estas 65 n's porque habían sido descubiertos recientemente por Euler en un contexto diferente. Euler llamó a un número n un *número idóneo* si satisfacía la condición siguiente: "Sea m un número impar coprimo con n, el cual se representa propiamente por $x^2 + ny^2$. Si la ecuación $m = x^2 + ny^2$ tiene solución única con $x, y > 0$, entonces m es un número primo".

Euler estaba interesado en estos números porque le ayudaban a encontrar primos de gran tamaño. Por ejemplo, para $n = 1848$, podía probar que $18{,}518{,}809 = 197^2 + 1848 \cdot 100^2$ era un número primo, lo cual era una cifra muy grande para su época.

Gauss sugirió que no hay más n's que esas 65 dadas por Euler. En 1934 Sarvadaman Chowla demostró [4] que dicho número es finito, y en 1973, gracias a P. J. Weinberger [23], se supo que la lista de Euler era completa salvo por, posiblemente, un n más. Que este último n exista o no es una cuestión sin resolver a día de hoy.

Gauss no asumía que los coeficientes de las formas fueran primos entre sí, y organizó[19] las formas en *órdenes* de manera que dos formas $ax^2 + 2bxy + cy^2$ y $a'x^2 + 2b'xy + c'y^2$ se encuentran en el mismo *orden* si $\mathrm{mcd}(a, b, c) = \mathrm{mcd}(a', b', c')$ y $\mathrm{mcd}(a, 2b, c) = \mathrm{mcd}(a', 2b', c')$.

La clasificación de las formas binarias cuadráticas de Gauss consta de órdenes, que estaban hechos de géneros, que se convertían en clases. La terminología de Gauss proviene de la clasificación "linneana" en biología, donde las categorías eran clases, órdenes, familias, géneros y especies. También el término de equivalencia de clases tiene cierto parecido a la terminología de la biología en el siglo XVIII.

Con todos estos resultados, Gauss consiguió elaborar la sección V de *Disquisitiones Arithmeticae*, siendo esta la más extensa de su obra. Sin duda alguna, supuso el mayor avance de la época sobre las formas binarias cuadráticas, y abrieron un horizonte nuevo a lo que, posteriormente, nació como la Teoría de Números Algebraica.

1.4. Otros resultados de interés

Aunque las formas binarias cuadráticas abarquen una gran parte de *Disquisitiones Arithmeticae*, la obra consta de otros resultados de extraordinaria relevancia y trascendencia. En esta sección expondremos los más importantes y los contextualizaremos con los avances de otros matemáticos coetáneos a Gauss sobre dichos temas.

1.4.1. La Ley de Reciprocidad Cuadrática

La *Ley de Reciprocidad Cuadrática* designa al teorema que relaciona la solubilidad de dos congruencias de segundo grado relacionadas entre sí. Es reconocida como uno de los resultados más preciosos de la teoría de números; de hecho, el propio Gauss, al demostrarla, la denominó el "Teorema de oro".[20]

[19] [10], #226, pág. 233.

[20] Aunque en su obra lo nombra constantemente como el "Teorema fundamental".

Esta proposición fue formulada[21] por primera vez por el ilustre Leonhard Euler en una carta a Goldbach en 1742 y probada por primera vez por Legendre en 1798, aunque de forma fallida al emplear argumentos no demostrados. A su vez y sin constancia del trabajo de sus compañeros, Gauss realizó en 1796 la primera demostración válida y completa del teorema. No obstante, debido al carácter reservado del matemático para publicar sus descubrimientos, no salió a la luz hasta publicarse *Disquisitiones*.

La forma en la que Gauss lo enunció[22] fue la siguiente: "Si p es un número primo de la forma $4n+1$, $+p$ será un residuo o no residuo de cualquier número primo que, tomado positivamente, es un residuo o no residuo del mismo p. Si p es un número primo de la forma $4n+3$, $-p$ tendrá la misma propiedad."

El matemático empleó[23] la notación aRb para referirse a cuando un cierto número a es un residuo cuadrático módulo b y a aNb para el caso contrario. Sin embargo, actualmente se trabaja con la notación del símbolo de Legendre para trabajar de manera más simple con los residuos cuadráticos. Para consultar el enunciado con dicha notación consúltese el Teorema D.26.

Gauss trata dicho teorema en la sección IV de *Disquisitiones*, abarcando aproximadamente 60 artículos sobre este. En los primeros se puede encontrar una introducción, notación y ciertos resultados, algunos tratados por otros matemáticos como Euler o Fermat. Posteriormente, expone algunos ejemplos que muestran de manera práctica cómo funciona la ley para valores concretos, antes de centrarse en la generalización del teorema y su prueba, dividida en casos según las congruencias de los primos. Por último, aplica la ley para dos números cualesquiera no necesariamente primos y para la resolución de ecuaciones del tipo $x^2 - A$ en los casos en los que x es un residuo cuadrático módulo A, además de hablar del estudio de otros matemáticos sobre esta.

Si bien Gauss hizo dos pruebas de la ley en *Disquisitiones*, realizó 8 a lo largo de su vida, y actualmente se conocen al menos 196 demostraciones distintas[24].

La primera prueba de la obra utiliza los conocimientos que expone a lo largo de la sección IV y se basa en una recurrencia, distinguiendo 8 casos hasta completar la demostración y creando un algoritmo que determina cuándo un número es un residuo cuadrático para un módulo dado mediante la factorización en producto de primos. Una demostración de esta índole fue propuesta por Euler[25] pero fue en vano, ya que cometió un error al clasificar los residuos y no residuos en un cierto módulo al no especificar propiamente cuáles debían de ser cada uno. Gauss realizó la prueba, según las anotaciones al final de su obra, en abril de 1796.

La segunda prueba[26] se encuentra en la sección V sobre formas binarias cuadráticas para ciertos residuos, utilizando la terminología de los caracteres asignados. Gauss realizó dicha demostración el 27 de julio de 1796, aunque la refinó y redujo a la forma

[21] Toda esta información la expone Gauss en las anotaciones que realizó tras escribir la teroía de *Disquisitiones* y antes su publicación.
[22] [10], #131, pág. 99.
[23] [10], #131, pág. 100.
[24] Dichas demostraciones se pueden encontrar en [16].
[25] Dicha demostración aparece en [8], presentada a la Academia de San Petersburgo el 20 de noviembre de 1775.
[26] [10], #262, sección V, págs. 297–299.

expuesta en su trabajo en la primavera de 1800. Una idea parecida fue expuesta[27] también por Euler, aunque no fue capaz de exponer una demostración válida de ello. Otra demostración de este tipo fue propuesta por Legendre[28] de una manera muy ingeniosa, aunque del mismo modo inválida al suponer muchas sentencias sin su demostración pertinente, como él mismo confiesa en su obra.

Lagrange también realizó estudios sobre la ley[29], llegando al mismo enunciado que Gauss, aunque él tampoco pudo brindar una prueba correcta y completa.

Gauss demostró dicho teorema de manera independiente al resto de matemáticos de la época, pero el extenso periodo de publicación de *Disquisitiones* hizo que, tras haber realizado la prueba y recogido todo aquello en su obra, pudiera informarse de los avances de sus compañeros y agregar nuevos resultados, donde pudo mencionar el trabajo de estos sobre esta teoría y explicar la incompletitud de sus pruebas.

Además de la Ley de Reciprocidad Cuadrática, Gauss también trató con las leyes de reciprocidad cúbica y bicuadrática entre 1808 y 1817, además de estudiar el teorema de los residuos cuadráticos en artículos publicados en 1828 y 1832 respectivamente. Sin embargo, el resultado de mayor envergadura en este asunto surgió en 1825 cuando el matemático descubrió que los enteros complejos gaussianos, que habían sido introducidos anteriormente por Euler y Lagrange, se comportaban como los enteros racionales ordinarios. Posteriormente, en 1828, estableció le ley de reciprocidad cuadrática para enteros complejos sin demostración, y fue verdaderamente Jacobi quien la expuso al mundo por primera vez con su prueba correspondiente.

Todos estos resultados abrieron las puertas para desarrollar una de las más extraordinarias teorías de las matemáticas del siglo XIX: los números algebraicos. Aunque ni el propio Gauss fuera consciente de la trascendencia de aquello, todo ello supuso siglos de estudios de los más brillantes matemáticos del momento, como sus discípulos Lamé, Dirichlet, Dedekind o Kummer, y hasta discípulos de estos mismos como Kronecker. Todos ellos proporcionaron resultados de especial importancia para la resolución de teoremas tan emblemáticos como el último Teorema de Fermat o dar pasos agigantados en lo que actualmente se conoce como la Teoría de Números Algebraica.

1.4.2. La construcción geométrica del heptadecágono

Este resultado, demostrado por el joven Gauss el 30 de marzo de 1796 con tan solo 18 años de edad, supuso un hallazgo memorable en la Historia de las Matemáticas, además de un encuentro entre la Artimética, el Álgebra y la Geometría.

Durante más de 2000 años, desde la época de Euclides donde se conocía la teoría correspondiente a la división del círculo en 3 y 5 partes, no se había realizado ningún avance digno en este campo. Sin embargo, fue nuestro matemático quien, mediante una ingeniosa teoría, obtuvo este importante descubrimiento.

[27] De criteris aequationis $fxx + gyy = hzz$ utrumque resolutionem admittat necne, (donde f, g, h son dados, x, y, z indeterminados), fragmento de [9].

[28] [15], pág. 520.

[29] [14], pág. 465, y obras suyas posteriores.

Gauss se preocupó por estudiar matemáticamente qué polígonos regulares podrían dibujarse mediante regla y compás.

A pesar de tratarse de un resultado geométrico, Gauss aborda el asunto empleando el álgebra relacionada con las raíces de la unidad y los polinomios.

En aquella época ya se tenía una visión clara del modelo geométrico de representación de los números complejos y de su potencial revolucionario para atacar ecuaciones ciclotómicas. Además, cincuenta años atrás, Euler expuso [7] por primera vez la ecuación que definía la exponencial en el plano complejo, $e^{i\pi} = \cos\pi + i\,\mathrm{sen}\,\pi = -1$. Esto ayudó a que nuestro matemático, conociendo las raíces de la ecuación, de la forma $e^{i\frac{2k\pi}{p}}$, estableciera que dichas raíces definen los vértices de un polígono regular de p lados. Además, empleó la idea de relacionar las funciones de las raíces que permanecen invariantes o que toman un número pequeño de valores al permutar las raíces con las soluciones de la ecuación que había sido desarrollada ampliamente por Lagrange en una memoria de 1771.

Gauss expuso[30] toda la teoría pertinente a este problema en la sección VII de *Disquisitiones Arithmeticae*, finalizando con ello esta obra de renombre. Su método parte de las divisiones del círculo en un número primo de lados, pues es el caso más simple y del cual se derivan el resto de divisiones, para recordar que la ecuación que determina los vértices del polígono de N lados no es otra que $X^N - 1$, aquella cuyas soluciones son 1 y las raíces de la unidad. A partir de ahí, analiza la forma trigonométrica de las soluciones e intenta relacionar el grado del polinomio con sus factores primos para encontrar soluciones en polinomios de grado dichos factores que le ayuden a encontrar el valor de los vértices. Si los vértices se pueden expresar en términos de sumas, restas, multiplicaciones, divisiones y raíces cuadradas, entonces el polígono de dicho número de lados se puede construir, ya que dichas operaciones se pueden realizar geométricamente con regla y compás.

Ahora bien, ¿para qué valor de N se cumple precisamente dicha condición? Gauss declaró que se trataban, nada más y nada menos, de los valores de N primos que resultan una unidad mayor que una potencia de una potencia de 2, es decir, $N = 2^{2^\mu} - 1$. Es por ello por lo que lo prueba para $N = 17$, ya que $N - 1 = 16 = 2^4$.

Gauss no hizo una construcción explícita del polígono en su trabajo, pero escribió la fórmula[31] para el coseno del ángulo $\frac{2}{17}\pi$

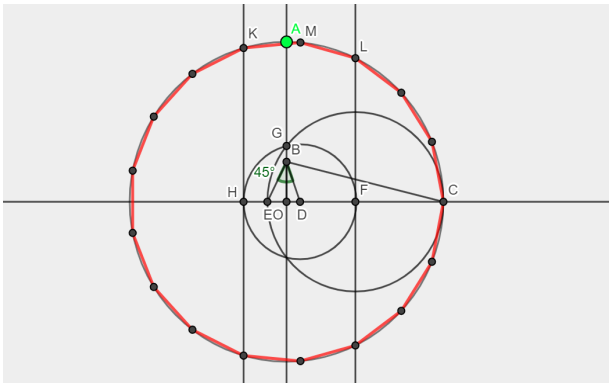
$$\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}$$

y probó que el heptadecágono puede construirse siempre que se pueda construir un segmento de esa longitud dado un segmento de longitud la unidad. Al solo aparecer las operaciones anteriormente mencionadas, es posible trasladar dicha fórmula a una construcción geométrica bastante complicada. Además, facilitó la lista de aquellos polígonos de menos de 300 lados que se podían construir de dicha manera.

[30] [10] pág. 420 en adelante.
[31] [10] #365, pág. 470.

En la actualidad existen métodos más eficientes para dicha construcción descubiertos al analizarse la prueba de Gauss. El matemático H. W. Richmond expuso [19] un método simplificado en 1893 de la forma siguiente:

1. Se dibujan los ejes perpendiculares que se cortan en O.
2. Se dibuja una circunferencia con centro en O y radio OA.
3. Se obtiene un punto B tal que el segmento OB es la cuarta parte del radio OA.
4. Se obtiene el punto D tal que el ángulo OBD es la cuarta parte del ángulo OBC.
5. Se obtiene el punto E tal que el ángulo EBD es de 45^{o}.
6. Se obtiene el punto medio F del segmento EC.
7. Se dibuja la circunferencia de centro F y radio FG que corta al eje vertical en G.
8. Se dibuja la circunferencia de centro D y radio DG que corta al eje horizontal también en H.
9. Se trazan dos rectas verticales por H y F que cortan a la circunferencia en los puntos K y L.
10. Se obtiene el punto medio M del arco KL.
11. El segmento KM es el lado del polígono regular de 17 lados.



Con este hallazgo el matemático finalizó una cuestión abierta durante más de dos milenios y encaminó su destino hacia el campo de las Matemáticas, abandonando las lenguas clásicas que estudiaba simultáneamente hasta ese momento.

CAPÍTULO 2
Formas binarias cuadráticas y cuerpos cuadráticos

Gracias a la teoría recogida en *Disquisitiones Arithmeticae* se desarrolló lo que actualmente se conoce como la Teoría de Números Algebraica. Gran parte de este área trabaja empleando ideales gracias a la simplicidad de operar con ellos comparado con la metodología de Gauss. Sin embargo, ambas maneras están íntimamente conectadas.

Las formas binarias cuadráticas resultan extremadamente útiles para aplicar en el álgebra moderno, ya que existe una analogía entre estas y los ideales de los *órdenes* de los cuerpos cuadráticos empleados en la matemática actual.

Se puede relacionar el grupo de clases de ideales con el grupo de clases de formas binarias cuadráticas $C(D)$ de la sección anterior como se verá próximamente, pero para ello se han de introducir ciertos conceptos y resultados previamente.

En el Apéndice D se recordarán propiedades y resultados sobre los cuerpos de números y módulos para facilitar la comprensión a la hora de definir los *órdenes*, que ayudarán a probar la relación entre las formas binarias cuadráticas y los ideales de los órdenes de los cuerpos cuadráticos.

2.1. Órdenes en cuerpos cuadráticos

Antes de definir los órdenes, se requiere de una breve introducción sobre *módulos*.

Definición 2.1. Sea K un cuerpo de números de grado n. Un **módulo** en K es un subgrupo M del grupo $(K, +)$ generado por un conjunto finito $\alpha_1, \ldots, \alpha_r$ de elementos de K:

$$M = \langle \alpha_1, \ldots \alpha_r \rangle_{\mathbb{Z}} = \{a_1\alpha_1 + \cdots + a_r\alpha_r \mid a_1, \ldots, a_r \in \mathbb{Z}\}.$$

Si K es un cuerpo de números de grado n y M un módulo de K, para todo $\alpha \in M$ y todo $m \in \mathbb{Z}$ se tiene que $m\alpha = 0$ si y solo si $m = 0$ o $\alpha = 0$, por lo que M es libre de torsión. Que sea libre implica que tiene base, y todas las bases poseen el mismo número de elementos. De aquí se siguen las siguientes definiciones:

Definición 2.2. Sea K un cuerpo de números de grado n y M un módulo en K. Al número de elementos de la base de M se le denomina el **rango** de M.

Definición 2.3. Sea K un cuerpo de números de grado n y M un módulo en K. Si M tiene rango n, entonces es un **módulo completo**.

Definición 2.4. Sea M un módulo completo de un cuerpo de números K. Se dice que $\alpha \in K$ es un **coeficiente** de M si $\alpha M \subset M$. Como el conjunto de todos los coeficientes de M es un subanillo de K, se le denomina el **anillo de coeficientes** de M y se denota como $\mathcal{O}_M$.

Teorema 2.5. *Si M es un módulo completo de K, $\mathcal{O}_M$ es un módulo completo.*

Demostración. Sea $\gamma \in M$ no nulo. Entonces $\gamma\mathcal{O}_M \subset M$ y se trata de un subgrupo abeliano de M, luego es un módulo. Por tanto, $\mathcal{O}_M = \gamma^{-1}(\gamma\mathcal{O}_M)$ es también un módulo, y solo queda comprobar que es de rango máximo.

Sea $m_1, \ldots, m_n$ una base de M. Si $\alpha \in K$ es no nulo, existen $a_{ij} \in \mathbb{Q}$ tales que $\alpha m_i = \sum_{j=1}^{n} a_{ij} m_j$. Dado esto, definiendo el producto de los denominadores de a_{ij} como c, éste resulta un entero racional no nulo y cada $ca_{ij} \in \mathbb{Z}$, luego $ca_{ij}m_j \in M$ y $c\alpha m_i \in M$. Como $m_1, \ldots, m_n$ es una base de M, se sigue que $c\alpha \in \mathcal{O}_M$. Sea $\alpha_1, \ldots, \alpha_n$ una $\mathbb{Q}$-base de K, aplicando lo anterior se pueden encontrar racionales no nulos $c_1, \ldots, c_n$ tales que $c_1\alpha_1, \ldots, c_n\alpha_n \in \mathcal{O}_M$, luego $\mathcal{O}_M$ contiene n elementos linealmente independientes. Esto implica que su rango es n, por lo que es completo. □

El teorema anterior permite definir el siguiente concepto:

Definición 2.6. Se dice que $\mathcal{O}$ es un **orden** de un cuerpo de números K si es un módulo completo de K que además es un anillo con unidad.

Todo orden $\mathcal{O}$ es el anillo de coeficientes de un módulo completo ya que, como $1 \in \mathcal{O}$, es su propio anillo de coeficientes. Cabe mencionar una importante característica de los ideales que los componen:

Teorema 2.7. *Sea $\mathcal{O}$ un orden de un cuerpo de números K. Los ideales no nulos de $\mathcal{O}$ son módulos completos (aunque su anillo de coeficientes no es necesariamente $\mathcal{O}$).*

Demostración. Sea I un ideal no nulo de $\mathcal{O}$. Por el Teorema D.5, I es un módulo finitamente generado. Sea $\alpha \in I$ no nulo, entonces $\alpha\mathcal{O} \subset I$ es un módulo completo, ya que $\mathcal{O}$ lo es. El rango de I ha de ser mayor o igual que el de $\alpha\mathcal{O}$, que es máximo, luego I es un módulo completo. □

Los elementos de los órdenes resultan de especial interés por el siguiente lema:

Lema 2.8. *Sea $\mathcal{O}$ un orden de un cuerpo numérico K. Si $\alpha \in \mathcal{O}$, entonces α es un entero algebraico.*

Demostración. Si $\alpha \in \mathcal{O}$, entonces $\mathbb{Z}[\alpha] \subset \mathcal{O}$ al ser $\mathcal{O}$ un anillo. Como $\mathcal{O}$ es finitamente generado y por el Teorema D.5, siendo $A = \mathbb{Z}$, $M = \mathcal{O}$ y $\mathbb{Z}[\alpha]$ su submódulo, éste es finitamente generado. Aplicando el Teorema D.11 se sigue que α es un entero. □

Gracias a esto se puede definir un concepto bastante familiar:

Definición 2.9. Sea K un cuerpo de números. El anillo de todos los enteros algebraicos de K es el **orden maximal** o **anillo de enteros** de K y se denota como $\mathcal{O}_K$.

Nos interesa conocer la relación de $\mathcal{O}_K$, del cual conocemos sus propiedades y características, con los órdenes que no son maximales, ya que queremos utilizarlos para establecer la relación entre los ideales de los órdenes de los cuerpos cuadráticos y las formas binarias cuadráticas. Para ello, introducimos el siguiente concepto:

Definición 2.10. Sea K un cuerpo cuadrático y $B = \{\alpha, \beta\}$ una base de K. Sea $\alpha \to \alpha'$ el automorfismo no trivial de K. Definimos el **discriminante** de B como

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

Si M es un módulo completo en K y $B = \{\alpha, \beta\}$ una base de M, definimos $\Delta[M] = \Delta[B]$. Además, $\Delta[M]$ es independiente de la base elegida.

Por (D.3), $\mathcal{O}_K$ se puede escribir de la siguiente manera:

$$\mathcal{O}_K = \langle 1, w_K \rangle, \quad w_k = \frac{\Delta_K + \sqrt{\Delta_K}}{2}, \tag{2.1}$$

donde $\Delta_K = \Delta[\mathcal{O}_K]$ es el discriminante de K (ver (D.1)).

Teorema 2.11. *Sea K un cuerpo cuadrático y B una base de K formada por enteros algebraicos. Entonces $\Delta[B] \in \mathbb{Z}$ y $\Delta[B] \equiv 0, 1 \,(\text{mód } 4)$.*

Demostración. Ver [12], Teorema 10.13. □

Teorema 2.12. *Sea K es un cuerpo cuadrático, B, C dos bases de K y M_C^B la matriz de cambio de base entre B y C. Entonces $\Delta[B] = |M_C^B|^2 \Delta[C]$.*

Demostración. Ver [12], Teorema 10.3. □

Definición 2.13. Sea M un módulo completo en un cuerpo cuadrático K y $\mathcal{O}$ su anillo de coeficientes. Sea B una base de M y C una base de $\mathcal{O}$. Sea D_B^C la matriz de cambio de base de B a C. Por el Teorema 2.12, definimos la **norma** de M como

$$N(M) = |\det D_B^C| = \sqrt{\frac{\Delta[M]}{\Delta[\mathcal{O}]}}.$$

De este modo, $N(M)$ es un número racional positivo tal que $\Delta[M] = N(M)^2 \Delta[\mathcal{O}]$.

Esto nos permite enunciar el siguiente teorema:

Teorema 2.14. *Sea M un módulo completo contenido en su anillo de coeficientes $\mathcal{O}$. Entonces, $N(M) = |\mathcal{O}/M|$.*

Demostración. Sabemos que existe una base $C = \{\alpha_1, \ldots, \alpha_n\}$ de $\mathcal{O}$ tal que para ciertos enteros racionales a_i se tiene que $B = \{a_1\alpha_1, \ldots, a_n\alpha_n\}$ es una base de M. La matriz D_B^C es una matriz diagonal, por lo que $N(M) = |a_1 \cdots a_n|$.

El isomorfismo entre $\mathcal{O}$ y $\mathbb{Z}^n$ que envía C a la base canónica $\{e_1, \ldots, e_n\}$ de $\mathbb{Z}^n$ manda la base B a la base $\{a_1e_1, \ldots, a_ne_n\}$, luego envía M al módulo $a_1\mathbb{Z} \times \cdots \times a_n\mathbb{Z}$, de modo que

$$\mathcal{O}/M \cong (\mathbb{Z} \times \cdots \times \mathbb{Z})/(a_1\mathbb{Z} \times \cdots \times a_n\mathbb{Z}) \cong (\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_n\mathbb{Z}).$$

En consecuencia, $|\mathcal{O}/M| = |(\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_n\mathbb{Z})| = |a_1| \cdots |a_n| = N(M)$. □

Teorema 2.15. *Sea K un cuerpo de números. Si $\mathcal{O} \subset \mathcal{O}'$ son dos órdenes de K, entonces $\Delta[\mathcal{O}] = m^2\Delta[\mathcal{O}']$ para cierto $m \in \mathbb{N}$. Además, $m = 1$ si y solo si $\mathcal{O} = \mathcal{O}'$.*

Demostración. Los elementos de la base de $\mathcal{O}$ se expresan como combinación lineal de los elementos de una base de $\mathcal{O}'$ con coeficientes enteros racionales. Por tanto, la matriz D de cambio de base tiene coeficientes enteros racionales también, de modo que su determinante es un entero racional. Por el Teorema 2.12 se tiene que $\Delta[\mathcal{O}] = |D|^2\Delta[\mathcal{O}']$. Además, los órdenes coincidirán si y solo si D es una matriz de cambio de base en $\mathcal{O}'$, lo que sucede si y solo si $|D| = \pm 1$. □

Sabemos que, en los cuerpo cuadráticos, $\mathcal{O}_K$ tiene la forma descrita en (D.2). Esto implica que, para cada $0 \neq m \in \mathbb{N}$, el conjunto $\mathcal{O}_m = \mathbb{Z}[m\alpha] = \{a + bm\alpha \mid a, b \in \mathbb{Z}\}$ es un orden de K. Se sigue que $\Delta[\mathcal{O}_m] = m^2\Delta_K$, pues la matriz de cambio de base entre $\{1, \alpha\}$ y $\{1, m\alpha\}$ tiene determinante m. Esto prueba, además, que los órdenes $\mathcal{O}_m$ son distintos dos a dos. Gracias al siguiente teorema veremos que son todos los órdenes de K.

Teorema 2.16. *Sea $K = \mathbb{Q}(\sqrt{D})$ un cuerpo cuadrático y $\alpha = w_K$ definido en (2.1). Entonces, los órdenes de K son de la forma $\mathcal{O}_m = \mathbb{Z}[m\alpha] = \{a + bm\alpha \mid a, b \in \mathbb{Z}\}$ y se tiene $\Delta[\mathcal{O}_m] = m^2\Delta_K$.*

Demostración. Sea $\mathcal{O}$ un orden de K y sea m el mínimo natural tal que existe un elemento en $\mathcal{O}$ de la forma $a + m\alpha$, con $a \in \mathbb{Z}$. Como $\mathbb{Z} \subset \mathcal{O}$ resulta $m\alpha \in \mathcal{O}$, luego $\mathcal{O}_m \subset \mathcal{O}$.

Si $a + b\alpha \in \mathcal{O}$, entonces existen enteros racionales c y r tales que $b = mc + r$ y $0 \leq r < m$. Se tiene que $(a + b\alpha) - (a + cm\alpha) = r\alpha \in \mathcal{O}$, luego por definición de m ha de ser $r = 0$, de modo que $a + b\alpha = a + mc\alpha \in \mathcal{O}_m$, obteniéndose la igualdad. □

El Teorema 2.16 induce la siguiente definición:

Definición 2.17. Sea K un cuerpo de números y sea $\mathcal{O}_K$ su anillo de enteros. Si $\mathcal{O}$ es cualquier orden de K, llamaremos **índice** de $\mathcal{O}$ al único número natural tal que $\mathcal{O} = \mathcal{O}_m$, y lo denotaremos como índ$(\mathcal{O})$.

Observación 2.18. En particular, índ$(\mathcal{O})$ es el valor absoluto del determinante de la matriz de cambio de base entre una base de $\mathcal{O}$ y una base entera de K. Empleando el argumento de la prueba del Teorema 2.14 se deduce que índ$(\mathcal{O}) = |\mathcal{O}_K/\mathcal{O}|$.

Los órdenes no maximales de los cuerpos de números comparten algunas propiedades con los anillos de enteros:

Teorema 2.19. *Sea $\mathcal{O}$ un orden de un cuerpo de números. Entonces:*

(i) $\mathcal{O}$ es un anillo noetheriano.

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

(iii) Si $\mathfrak{p} \subset \mathcal{O}$ es un ideal primo no nulo, entonces es maximal.

Demostración. Para probar (i), sabemos que $\mathcal{O}$ es un $\mathbb{Z}$-módulo libre finitamente generado. En particular, es de la forma $\mathbb{Z}[a_1, \ldots, a_d]$, con $d \in \mathbb{N}$, luego es noetheriano. Para probar (ii), por el Teorema 2.7, como $\mathfrak{a}$ es un ideal no nulo, entonces es un módulo completo, y todos los elementos de $\mathcal{O}$ son coeficientes de $\mathfrak{a}$, luego su anillo de coeficientes es un orden de $\mathcal{O}'$ tal que $\mathcal{O} \subset \mathcal{O}'$. Por el Teorema 2.14 sabemos que $\mathcal{O}'/\mathfrak{a}$ es finito, luego $\mathcal{O}/\mathfrak{a}$ también lo es. Por último, para demostrar (iii) basta recordar que como $\mathfrak{p}$ es primo, entonces $\mathcal{O}/\mathfrak{p}$ es un dominio de integridad finito, luego es un cuerpo, lo que implica que $\mathfrak{p}$ es maximal. □

Del teorema anterior obtenemos la siguiente definición:

Definición 2.20. Sea $\mathfrak{a}$ un ideal del orden $\mathcal{O}$. Llamamos **norma** de $\mathfrak{a}$ a $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$.

Se puede apreciar que todos los órdenes cumplen dos de las tres propiedades que cumplen los dominios de Dedekind, pero los que no son maximales carecen de la propiedad de ser íntegramente cerrados. En efecto, solamente $\mathcal{O}_K$ es íntegramente cerrado, ya que es el único orden que posee todos los enteros algebraicos de K. En consecuencia, los órdenes no maximales no pueden ser ni dominios de Dedekind ni dominios de factorización única. Sin embargo, la dificultad que nos supondría este hecho para nuestro propósito puede ser 'acotada'.

Para remediar esta situación nótese que, dado cualquier ideal $\mathfrak{a}$ de $\mathcal{O}$, se cumple

$$\mathcal{O} \subset \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\} \tag{2.2}$$

ya que $\mathfrak{a}$ es un ideal de $\mathcal{O}$. Sin embargo, la igualdad que necesitamos no ocurre. Por ejemplo, si $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$ es el orden de índice 2 en $K = \mathbb{Q}(\sqrt{-3})$, y $\mathfrak{a}$ es un ideal de $\mathcal{O}$ generado por 2 y por $1 + \sqrt{-3}$, entonces resulta

$$\mathcal{O} \neq \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$$

ya que $\frac{1+\sqrt{-3}}{2} \cdot 2 = 1 + \sqrt{-3} \in \mathfrak{a}$ y $\frac{1+\sqrt{-3}}{2} \cdot (1 + \sqrt{-3}) = (-1 + \sqrt{-3}) \in \mathfrak{a}$ pero $\frac{1+\sqrt{-3}}{2} \notin \mathcal{O}$. Esto da lugar a la siguiente definición:

Definición 2.21. Sea K un cuerpo cuadrático, $\mathcal{O}$ un orden de K y $\mathfrak{a}$ un ideal de $\mathcal{O}$. Se dice que $\mathfrak{a}$ es un ideal **propio** de $\mathcal{O}$ cuando (2.2) se convierte en una igualdad, es decir, cuando

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

Observación 2.22. Los ideales principales son siempre propios. Sea $\mathfrak{a} = \langle a \rangle \subset \mathcal{O}$, si $\beta\mathfrak{a} \subset \mathfrak{a}$ para algún $\beta \in K$, entonces $\beta a = ca$ para algún $c \in \mathcal{O}$. Como esto se cumple también en K al ser $\mathcal{O}$ un subanillo suyo, podemos multiplicar por $a^{-1} \in K$, resultando $\beta = c$, de modo que $\beta \in \mathcal{O}$. Además, para el orden maximal *todos* los ideales son propios, ya que si $\mathfrak{a}$ es un ideal de $\mathcal{O}_K$, entonces $\{\beta \in K \colon \beta\mathfrak{a} \subset \mathfrak{a}\}$ es un orden que contiene a $\mathcal{O}_K$. Como $\mathcal{O}_K$ es el orden maximal, se sigue que $\mathcal{O}_K = \{\beta \in K \colon \beta\mathfrak{a} \subset \mathfrak{a}\}$.

Esta terminología se puede extender a *ideales fraccionarios*.

Definición 2.23. Sea K un cuerpo cuadrático y $\mathcal{O}$ un orden de K. Se dice que $\mathfrak{a} \subset K$ es un **ideal fraccionario** de $\mathcal{O}$ si es un $\mathcal{O}$-submódulo no nulo finitamente generado. En otras palabras, $\mathfrak{a}$ es un $\mathcal{O}$-submódulo de K de manera que existe un $\alpha \in \mathcal{O}$, $\alpha \neq 0$ tal que $\alpha\mathfrak{a} \subseteq \mathcal{O}$.

Una vez definidos los ideales fraccionarios se puede hablar de ideales *invertibles*:

Definición 2.24. Un ideal fraccionario $\mathfrak{a}$ del orden $\mathcal{O}$ es **invertible** si existe otro ideal fraccionario $\mathfrak{b}$ de $\mathcal{O}$ de manera que $\mathfrak{ab} = \mathcal{O}$.

Nótese que los ideales fraccionarios principales (aquellos de la forma $\alpha\mathcal{O}$ para $\alpha \in K^*$) son invertibles, al ser su generador una unidad. El resultado más interesante es que, en cuerpos cuadráticos, los conceptos de propio e invertible coinciden. Para poder probar esto, enunciaremos primero el siguiente lema:

Lema 2.25. *Sea $K = \mathbb{Q}(\tau)$ un cuerpo cuadrático y sea $ax^2 + bx + c$ el polinomio mínimo de τ, donde a, b y c son enteros primos entre sí. Entonces $\langle 1, \tau \rangle$ es un ideal propio fraccionario del orden $\langle 1, a\tau \rangle$ de K.*

Demostración. En primer lugar, como $a\tau$ es un entero algebraico, $\langle 1, a\tau \rangle$ es un orden. Por tanto, dado $\beta \in K$, se tiene que $\beta\langle 1, \tau \rangle \subset \langle 1, \tau \rangle$ es equivalente a $\beta \cdot 1 \in \langle 1, \tau \rangle$ y $\beta \cdot \tau \in \langle 1, \tau \rangle$. De $\beta \cdot 1 \in \langle 1, \tau \rangle$ se obtiene que $\beta = m + n\tau, m, n \in \mathbb{Z}$. Para entender $\beta \cdot \tau \in \langle 1, \tau \rangle$, nótese que

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

Como $\mathrm{mcd}(a, b, c) = 1$, se puede apreciar que $\beta\tau \in \langle 1, \tau \rangle$ si y solo si $a \mid n$. De esto se sigue que $\{\beta \in K \colon \beta\langle 1, \tau \rangle \subset \langle 1, \tau \rangle\} = \langle 1, a\tau \rangle$, concluyendo la prueba. □

Con ello, podemos enunciar la siguiente proposición:

Proposición 2.26. *Sea $\mathcal{O}$ un orden en un cuerpo cuadrático K, y sea $\mathfrak{a}$ un ideal fraccionario de $\mathcal{O}$. Entonces $\mathfrak{a}$ es propio si y solo si $\mathfrak{a}$ es invertible.*

Demostración. Si $\mathfrak{a}$ es invertible, entonces $\mathfrak{ab} = \mathcal{O}$ para otro ideal fraccionario $\mathfrak{b}$ de $\mathcal{O}$. Si $\beta \in K$ y $\beta\mathfrak{a} \subset \mathfrak{a}$, entonces se tiene $\beta\mathcal{O} = \beta(\mathfrak{ab}) = (\beta\mathfrak{a})\mathfrak{b} \subset \mathfrak{ab} = \mathcal{O}$, de lo que se sigue que $\beta \in \mathcal{O}$, probando que $\mathfrak{a}$ es propio.

Supongamos ahora que $\mathfrak{a}$ es un ideal propio de $\mathcal{O}$. Por la definición de ideal propio, $\mathfrak{a}$ es un $\mathbb{Z}$-módulo de rango 2, por lo que $\mathfrak{a} = \langle \alpha, \beta \rangle$ para algunos $\alpha, \beta \in K$. Entonces, $\mathfrak{a} =$

$\alpha\langle 1,\tau\rangle$, donde $\tau = \beta/\alpha$. Si ax^2+bx+c, con $\mathrm{mcd}(a,b,c)=1$, es el polinomio mínimo de τ, entonces el Lema 2.25 implica que $\mathcal{O} = \langle 1, a\tau\rangle$. Sean $\beta \to \beta'$ el automorfismo no trivial de K y τ' la otra raíz de ax^2+bx+c. Por este mismo lema también obtenemos que $\mathfrak{a}' = \alpha'\langle 1,\tau'\rangle$ es un ideal fraccionario de $\langle 1, a\tau\rangle = \langle 1, a\tau'\rangle = \mathcal{O}$. Se puede afirmar que

$$\mathfrak{a}\mathfrak{a}' = \frac{N(\alpha)}{a}\mathcal{O}. \tag{2.3}$$

Para ver el porqué, nótese que $a\mathfrak{a}\mathfrak{a}' = a\alpha\alpha'\langle 1,\tau\rangle\langle 1,\tau'\rangle = N(\alpha)\langle a, a\tau, a\tau', a\tau\tau'\rangle$. Como $\tau+\tau' = -b/a$ y $\tau\tau' = c/a$ y $\mathrm{mcd}(a,b,c)=1$, entonces $a\mathfrak{a}\mathfrak{a}' = N(\alpha)\langle a, a\tau, -b, c\rangle = N(\alpha)\langle 1, a\tau\rangle = N(\alpha)\mathcal{O}$. Esto implica (2.3), lo que prueba que $\mathfrak{a}$ es invertible. □

Dado un orden $\mathcal{O}$, denotamos $I(\mathcal{O})$ como el conjunto de todos los ideales fraccionarios propios de $\mathcal{O}$ y $P(\mathcal{O})$ como el conjunto de todos los ideales fraccionarios principales. El resultado más importante sobre estos conjuntos es:

Teorema 2.27. *Sea $\mathcal{O}$ un orden. Entonces, $I(\mathcal{O})$ forma un grupo abeliano con la operación de multiplicación y $P(\mathcal{O})$ forma un subgrupo de $I(\mathcal{O})$.*

Demostración. La existencia de neutro e inverso se siguen de la Proposición 2.26. Además, las propiedades conmutativa y asociativa se cumplen dado que la multiplicación de ideales las satisface. Veamos que la multiplicación es cerrada en $I(\mathcal{O})$. Sean $\mathfrak{a},\mathfrak{b} \in I(\mathcal{O})$. Por la Proposición 2.26, existen $\mathfrak{a}^{-1},\mathfrak{b}^{-1} \in I(\mathcal{O})$ tales que $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{b}\mathfrak{b}^{-1} = \mathcal{O}$. Por tanto, $\mathfrak{a}\mathfrak{b}\mathfrak{b}^{-1}\mathfrak{a}^{-1} = \mathcal{O}$, lo que prueba que $\mathfrak{a}\mathfrak{b}$ es invertible y, por la Proposición 2.26, es propio, por lo que $\mathfrak{a}\mathfrak{b} \in I(\mathcal{O})$.

Como todo ideal fraccionario principal es propio por la Observación 2.22 y el producto de dos ideales fraccionarios principales es principal, $P(\mathcal{O}) \subset I(\mathcal{O})$ es un subgrupo de $I(\mathcal{O})$. □

A partir de estos conjuntos podemos definir $C(\mathcal{O})$, el grupo de clases de los ideales de un orden $\mathcal{O}$, como el cociente

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

mediante la misma relación de equivalencia que define a $C(\mathcal{O}_K)$, el grupo de clases del anillo de enteros (ver D.23).

2.2. Formas binarias cuadráticas e ideales

Tras estos resultados, por fin, se puede proceder a relacionar el grupo de clases de ideales $C(\mathcal{O})$ de un orden $\mathcal{O}$ de discriminante D en un cuerpo cuadrático con el grupo de clases de formas $C(D)$ de discriminante D (definido en el capítulo anterior):

Teorema 2.28. *Sea K un cuerpo cuadrático imaginario y $\mathcal{O}$ un orden de K de discriminante $D<0$. Entonces:*

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

(ii) La aplicación que envía $f(x,y)$ a $\langle a, (-b+\sqrt{D})/2\rangle$ induce un isomorfismo entre $C(D)$ y $C(\mathcal{O})$. Por tanto, el orden de $C(\mathcal{O})$ es el número de clases $h(D)$ mencionado en la sección 1.2.1.

Demostración. Sea $f(x,y) = ax^2 + bxy + cy^2$ una forma definida positiva primitiva de discriminante $D < 0$. Las raíces de $f(x,1) = ax^2 + bx + c$ son complejas, por lo que hay una única $\tau \in \mathbb{H}$ (el semiplano superior) de manera que $f(\tau, 1) = 0$. Como $a > 0$ por ser f definida positiva, se sigue que $\tau = (-b + \sqrt{D})/2a$. En consecuencia, $\langle a, (-b+\sqrt{D})/2\rangle = \langle a, a\tau\rangle = a\langle 1, \tau\rangle$.

Para probar (i) se tiene que $a\langle 1,\tau\rangle$ es un ideal propio del orden $\langle 1, a\tau\rangle$ por lo siguiente: si m es el índice de $\mathcal{O}$, sabemos que $D = m^2\Delta_K$, y resulta

$$a\tau = \frac{-b+\sqrt{D}}{2} = \frac{-b+m\sqrt{\Delta_K}}{2} = -\frac{b+m\Delta_K}{2} + m\Big(\frac{\Delta_K+\sqrt{\Delta_K}}{2}\Big) = -\frac{b+m\Delta_K}{2} + mw_K.$$

Como $D = b^2 - 4ac = m^2\Delta_K$, $m\Delta_K$ y b tienen la misma paridad, por lo que $(b + m\Delta_K)/2 \in \mathbb{Z}$. Se sigue que $\langle 1, a\tau\rangle = \langle 1, mw_K\rangle = \mathcal{O}$. Aplicando el Lema 2.25, se concluye que $a\langle 1,\tau\rangle$ es un ideal propio de $\mathcal{O}$.

Para probar (ii), sean $f(x,y)$ y $g(x,y)$ formas de discriminante D, y sean τ y τ' las raíces en el semiplano superior de $f(x,1)$ y $g(x,1)$ respectivamente. Se ha de probar:

$$\begin{aligned} & f(x,y), g(x,y) \text{ son equivalentes} \\ \iff & \tau' = \tfrac{p\tau+q}{r\tau+s}, \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL(2,\mathbb{Z}). \\ \iff & \langle 1,\tau\rangle = \lambda\langle 1,\tau'\rangle, \lambda \in K^*. \end{aligned} \tag{2.4}$$

Para comprobar que esto es verdad, asumimos que $f(x,y) = g(px+qy, rx+sy)$, donde $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in SL(2,\mathbb{Z})$. Entonces

$$0 = f(\tau,1) = g(p\tau+q, r\tau+s) = (r\tau+s)^2 g\Big(\frac{p\tau+q}{r\tau+s}, 1\Big), \tag{2.5}$$

lo que obliga que $g((p\tau+q)/(r\tau+s)) = 0$. Mediante algunas cuentas, se llega a

$$\mathrm{Im}\left(\frac{p\tau+q}{r\tau+s}\right) = \det\begin{pmatrix} p & q \\ r & s \end{pmatrix} |r\tau+s|^{-2}\mathrm{Im}(\tau). \tag{2.6}$$

Esto implica que $(p\tau+q)/(r\tau+s) \in \mathbb{H}$, de modo que $\tau' = (p\tau+q)/(r\tau+s)$ por la unicidad de la raíz τ'. En la otra dirección, si $\tau' = (p\tau+q)/(r\tau+s)$, entonces (2.5) prueba que $f(x,y)$ y $g(px+qy, rx+sy)$ tienen la misma raíz, por lo que deben ser iguales. Esto prueba la primera equivalencia de (2.4). Por otro lado, si $\tau' = (p\tau+q)/(r\tau+s)$, siendo $\lambda = r\tau+s \in K^*$. Entonces

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

ya que $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in SL(2,\mathbb{Z})$. En la otra dirección, si $\langle 1,\tau\rangle = \lambda\langle 1,\tau'\rangle$ para algún $\lambda \in K^*$, entonces $\langle 1,\tau\rangle = \langle \lambda, \lambda\tau'\rangle$, lo que implica que

$$\lambda\tau' = p\tau + q, \qquad \lambda = r\tau + s$$

para algunos $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in GL(2,\mathbb{Z})$. Despejando, se obtiene

$$\tau' = \frac{p\tau + q}{r\tau + s}$$

y, en consecuencia, (2.6) prueba que $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in SL(2,\mathbb{Z})$ ya que tanto τ como τ' se encuentran en $\mathbb{H}$. Esto termina la demostración de (2.4).

Ahora, usando el primer y tercer enunciado de (2.4), se puede ver que la aplicación que envía $f(x,y)$ a $a\langle 1,\tau\rangle$ induce una inyección $C(D) \longrightarrow C(\mathcal{O})$. Para ver que esta función es sobreyectiva, sea $\mathfrak{a}$ un ideal fraccionario de $\mathcal{O}$. Por la definición de ideal fraccionario, se puede escribir $\mathfrak{a} = \langle \alpha, \beta\rangle$ para algunos α, $\beta \in K$. Cambiando α y β si fuera necesario, se puede asumir que $\tau = \beta/\alpha \in \mathbb{H}$. Estableciendo $ax^2 + bx + c$ como el polinomio mínimo de τ sobre $\mathbb{Q}$, poniendo común denominador y cambiando signos, se puede asumir que $a, b, c \in \mathbb{Z}$, $\mathrm{mcd}(a,b,c) = 1$ y $a > 0$. Entonces, $f(x,y) = ax^2 + bxy + cy^2$ es una forma definida positiva de discriminante D y $f(x,y)$ va a $a\langle 1,\tau\rangle$. Como $[\mathfrak{a}] = [\langle 1, \beta/\alpha\rangle] = [\langle 1,\tau\rangle] = [a\langle 1,\tau\rangle]$ la sobreyectividad queda probada.

De esta manera, se tiene la biyección

$$C(D) \longrightarrow C(\mathcal{O}) \tag{2.7}$$

El siguiente paso es probar que dicha biyección se trata de un homomorfismo. Sean dos formas $f(x,y) = a_1x^2+b_1xy+c_1y^2$ y $g(x,y) = a_2x^2+b_2xy+c_2y^2$ de discriminante $D < 0$ y su composición de Dirichlet $f\circ g = a_1a_2x^2+Bxy+Cy^2$. Sus ideales asociados en $\mathcal{O}$ son $\langle a_1, (-b_1 + m\sqrt{\Delta_K})/2\rangle$, $\langle a_2, (-b_2 + m\sqrt{\Delta_K})/2\rangle$ y $\langle a_1a_2, (-B + m\sqrt{\Delta_K})/2\rangle$ respectivamente. Escribiendo $\Delta = (-B + m\sqrt{\Delta_K})/2$ y usando las dos primeras congruencias del Lema 1.30, dichos ideales se pueden reescribir como $\langle a_1, \Delta\rangle$, $\langle a_2, \Delta\rangle$ y $\langle a_1a_2, \Delta\rangle$. Esto se sigue del hecho de que $\langle a, z + na\rangle = \langle a, z\rangle$ para cualquier $z \in K$ y $n \in \mathbb{N}$. Por tanto, nuestro objetivo es probar que $[\langle a_1, \Delta\rangle][\langle a_2, \Delta\rangle] = [\langle a_1a_2, \Delta\rangle]$ en $C(\mathcal{O})$. Nótese que

$$\Delta^2 = \frac{B^2 - 2Bm\sqrt{\Delta_K} + m^2\Delta_K}{4} = \frac{B^2 + D - 2Bm\sqrt{\Delta_K}}{4} \equiv \frac{2B^2 - 2Bm\sqrt{\Delta_K}}{4} \equiv -B\Delta (\mathrm{mód} a_1a_2).$$

Por tanto, $\langle a_1, \Delta\rangle\langle a_2, \Delta\rangle = \langle a_1a_2, a_1\Delta, a_2\Delta, \Delta^2\rangle = \langle a_1a_2, a_1\Delta, a_2\Delta, -B\Delta\rangle$. Por otro lado, sabemos que si $z \in \mathbb{Z}$ divide simultáneamente a los enteros a_1, a_2 y B, entonces las dos congruencias del Lema 1.30 implican que z divide a b_1 y b_2. En consecuencia, z divide a $\mathrm{mcd}(a_1, a_2, (b_1 + b_2)/2) = 1$ por las condiciones dadas en la definición de la composición de Dirichlet, por lo que ha de ser $\mathrm{mcd}(a_1, a_2, B) = 1$. Por Bézout, existen $x, y, z \in \mathbb{Z}$ tales que $\Delta = xa_1\Delta + ya_2\Delta - zB\Delta$, y se sigue que $\langle a_1a_2, a_1\Delta, a_2\Delta, -B\Delta\rangle = \langle a_1a_2, \Delta\rangle$, finalizando la demostración.

El último paso sería probar que $C(D)$ es un grupo bajo la composición de Dirichlet. Como esto había sido probado en el Teorema 1.37, se concluye la prueba de (ii). □

Vamos a ver un ejemplo que ilustre de manera práctica el teorema.

Ejemplo 2.29. Sea $K = \mathbb{Q}(\sqrt{-17})$. En D.27 se ha explicado con detalle el proceso por el cual se obtienen los elementos de $C(\mathcal{O}_K)$, siendo $\mathcal{O}_K = \mathbb{Z}[\sqrt{-17}]$ al ser $-17 \equiv 3$ (mód 4). Se habían obtenido 4 clases distintas en $C(\mathcal{O}_K)$: $[\mathfrak{p}]$ para $\mathfrak{p} = \langle 2, 1+\sqrt{-17}\rangle$, $[\mathfrak{q}_1]$ para $\mathfrak{q}_1 = \langle 3, 1+\sqrt{-17}\rangle$, $[\mathfrak{q}_2]$ para $\mathfrak{q}_2 = \langle 3, 1-\sqrt{-17}\rangle$ y $[\mathcal{O}_K]$.

En el Ejemplo 1.18 se habían calculado las distintas formas reducidas para el discriminante $\Delta[\mathcal{O}_K] = -17 \cdot 4 = -68$, donde se habían obtenido $x^2 + 17y^2$, $2x^2 + 2xy + 9y^2$, $3x^2 + 2xy + 6y^2$ y $3x^2 - 2xy + 6y^2$. Por tanto, $h(D) = 4$ y el número de formas reducidas coincide con el cardinal del número de clases de $\mathcal{O}_K$.

Solo queda establecer la relación entre dichas formas y los ideales. Por el primer enunciado del Teorema 2.28 se tiene que

$$x^2 + 17y^2 \longleftrightarrow \left\langle 1, \frac{\sqrt{-68}}{2} \right\rangle = \langle 1, \sqrt{-17}\rangle = \mathcal{O}_K$$

$$2x^2 + 2xy + 9y^2 \longleftrightarrow \left\langle 2, \frac{-2+\sqrt{-68}}{2} \right\rangle = \langle 2, -1+\sqrt{-17}\rangle = \langle 2, 1+\sqrt{-17}\rangle = \mathfrak{p}$$

$$3x^2 + 2xy + 6y^2 \longleftrightarrow \left\langle 3, \frac{-2+\sqrt{-68}}{2} \right\rangle = \langle 3, -1+\sqrt{-17}\rangle = \langle 3, 1-\sqrt{-17}\rangle = \mathfrak{q}_2$$

$$3x^2 - 2xy + 6y^2 \longleftrightarrow \left\langle 3, \frac{2+\sqrt{-68}}{2} \right\rangle = \langle 3, 1+\sqrt{-17}\rangle = \mathfrak{q}_1,$$

y de esta manera tendríamos la relación completa entre las formas binarias cuadráticas de discriminante $D = -68$ y los ideales propios del orden $\mathcal{O}_K$ del cuerpo cuadrático $K = \mathbb{Q}(\sqrt{-17})$.

Con ello queda demostrado que podemos trabajar indistintamente con formas binarias cuadráticas de un discriminante negativo dado que con los ideales de los órdenes de los cuerpos cuadráticos de igual discriminante. Según nos convenga podemos elegir un método u otro y aplicar el Teorema 2.28 para obtener la equivalencia.

Las formas binarias cuadráticas son objetos de mayor importancia y trascendencia de lo que aparentemente se puede pensar. Gracias a ellas, Gauss probó resultados extremadamente fuertes aplicables a la Teoría de Números Algebraica, así como crear toda una teoría consistente y completa que permitiera estudiar los números desde el punto de vista de sus representaciones mediante dichas formas.

Una vez más se puede apreciar el increíble potencial de Gauss. No solamente elaboró la obra más importante sobre Teoría de Números de los últimos tiempos y unificó dicha teoría, sino que anticipó la que todavía estaba por llegar como nadie podría imaginar.

APÉNDICE A

Carl Friedrich Gauss: vida y obra

El 30 de abril de 1777 nació Johann Friedrich Carl Gauss, también conocido como *Princeps Mathematicorum* (el príncipe de los matemáticos) incluso en vida y considerado uno de los mayores genios de la historia, junto con Arquímedes y Newton.

Se crió en una época de transición: si bien sus primeros años de vida la sociedad se hallaba bajo el feudalismo y absolutismo germanos, luego se comenzó a desarrollar una nueva atmósfera de evolución en la cultura y la ciencia. Esto facilitó las oportunidades de poder crecer y establecer relaciones con otros científicos aun sin salir de su país. Además, la Revolución Francesa llegó cuando el matemático tenía tan solo doce años, suponiendo un cambió histórico que afectó a la mentalidad y desarrollo de la sociedad.

Gauss nació en Braunschweig, Alemania, en una familia de poca cultura; apenas sabían leer o escribir. Su familia paterna era campesina y su padre, Gebhard Dietrich Gauss, trabajó en diferentes oficios como jardinero, carnicero, albañil, asistente de comerciante o cajero en una pequeña casa de seguros, mientras que su madre, Dorothea Gauss, fue criada hasta convertirse en la segunda esposa de su marido. Se dice que Gauss ya corregía las cuentas de su padre a los tres años. Fue su madre, Dorothea, quien consiguió escolarizar a Gauss tras una intensa lucha con su esposo, y la primera persona que le motivó a estudiar fue precisamente su hermano, Friedrich Benz. En señal de gratitud por ello, Gauss adoptó el nombre de su tío como su segundo nombre.

Asistió a una escuela considerada una reliquia en la época, con un maestro llamado Büttner. El asistente de éste, Johann Martin Bartels, fue el apoyo de Gauss en el colegio y reconoció el talento del pequeño. Corrigió su lectura, le enseñó gramática y la ortografía del alto alemán estándar. Existe una leyenda que relata cómo Gauss, a los nueve años, consiguió hallar la suma de los 100 primeros números naturales en pocos minutos mediante una progresión aritmética.

Gracias a este talento precoz, el Duque de Braunschweig-Wolfenbuttel oyó hablar del joven Gauss y se interesó por él, dotándole de un estipendio para poder permitirse cursar estudios superiores. Con este dinero Gauss ingresó en el Collegium Carolinum, una institución pública de excelente calidad recientemente creada y con especialización en ciencias, dirigida hacia el personal militar y administrativo de Alemania.

Gauss permaneció allí de 1792 a 1795 y obtuvo el apoyo del profesor Hofrath von Zimmermann. En aquellos años la academia se convirtió en la vida de Gauss, aprove-

chando la maravillosa biblioteca de la institución con la que pudo actualizarse sobre las novedades matemáticas del momento. Por aquel entonces ya había descubierto su *Ley de los Mínimos Cuadrados* y aprendió a dominar en muy poco tiempo el latín y el griego; se apreciaba que Gauss tenía facilidad para las lenguas.

De 1795 a 1798 estudió en la Universidad de Göttingen, un centro con una de las mejores bibliotecas y recientemente reformado, enfocándose en las ciencias. Este período es considerado el de mayor esplendor intelectual para Gauss por la increíble cantidad de ideas matemáticas que esbozó en aquellos años y las cuales estuvo puliendo durante el resto de su vida hasta convertirlos en importantes teoremas. De hecho, fue en esta época, en 1796, cuando descubrió la construcción geométrica del heptadecágono, resultado de tal orgullo para el matemático que rompió su indecisión entre estudiar filología o matemáticas para decantarse por éstas últimas. Se dice que la satisfacción que obtuvo por ello hizo que quisiera dicho resultado como su epitafio.

Durante su estancia en Göttingen, Gauss estuvo plenamente centrado en sus investigaciones matemáticas. Apenas tenía vida social, únicamente se sabe de la existencia de su amigo Bolyai con quien se carteó en los años posteriores. La instrucción que recibió en aquella universidad le dotó de gran autonomía y desarrollo intelectual propio de manera que pudo elaborar una portentosa cantidad de ideas científicas en un breve período de tiempo, como ocurrió con Newton. Cabe destacar que fue en esta época cuando creó todo el contenido de su gran obra, *Disquisitiones Arithmeticae*. Gauss estaba enamorado de la Teoría de Números, la reina de las matemáticas para él, las cuales consideraba la reina de las ciencias.

En 1798 recibió su doctorado de la Universidad de Helmstedt, publicando su tesis en 1799 bajo el nombre de *Demostratio nova theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse* (Nuevas demostraciones del teorema de que toda función entera racional algebraica en una variable puede ser resuelta en factores reales de primero o segundo grado), resultado que se dio a conocer como el *Teorema fundamental del Álgebra*. A pesar de conocerse anterioriormente como el *Teorema de d'Alembert*, Gauss fue el primero en dar una demostración válida al teorema y mostró por qué las pruebas ya existentes de matemáticos como d'Alembert en 1746, Euler en 1749, Foncenet en 1759 o Lagrange en 1772 eran inadecuadas.

Se suele comparar su personalidad con la de Cauchy, otro gran matemático del siglo XIX, por su increíble diferencia y por su delicada relación, a pesar de ser ambos matemáticos con una mentalidad moderna con respecto a esta disciplina. Mientras que Gauss tardaba años en publicar sus resultados, Cauchy era extremadamente rápido. Por otro lado, Cauchy era un apasionado de la docencia, mientras que Gauss no tenía mucho interés en este ámbito, a pesar de tener discípulos como Dedekind o Kummer.

En cuanto a su vida personal, era un apasionado de la literatura europea y clásica antigua, así como de la política internacional, de la cual siempre estaba informado. Dominaba las lenguas extranjeras y estaba al día de las nuevas ciencias. Aunque no salió de Alemania en toda su vida, procuraba estar informado de la actualidad europea mediante periódicos y libros. Al ser su trabajo su fuente de satisfacción, le perturbaba cualquier obstáculo o entretenimiento que pudiera impedir su avance.

En la década de sus treinta años sufrió varias desdichas: por un lado, murieron su benefactor, el Duque de Brunswick, y su primera mujer, Johanna Elizabeth Rosina Osthoff; además, Alemania luchaba contra la invasión napoleónica. Esto provocó un amargo período en su vida que fue reconstruyendo posteriormente gracias a su madre y su nueva mujer, Friederica Wilhelmine Waldeck, con la que contrajo matrimonio un año después de su viudedad.

Gauss no solo contribuyó a la Teoría de Números. En 1827 publicó un artículo iniciándose en la geometría diferencial: *Disquisitiones generales circa superficies curvas*. Asimismo, en 1824 estableció sus conclusiones sobre el postulado de las superficies paralelas. Podría haberse considerado el padre de la geometría no euclidiana si hubiera profundizado más en esta área.

Tras la publicación de *Disquisitiones* se dedicó a la astronomía durante unos 20 años. Fue el primero en predecir una posición para el planeta enano Ceres en diciembre de 1801 e inventó el método para calcular órbitas celestes con base en ciertos datos observacionales. Todo esto lo plasmó en su obra *Theoria motus corporum coelestium in sectionibus conicis solem ambientium* de 1809, año en el que se le nombró director del observatorio de Göttingen. En dicho libro mostró las técnicas que dirigieron la astronomía computacional de los siglos posteriores.

La apertura de sus estudios a este ámbito permitió que Gauss obtuviera un gran reconocimiento científico e intelectual internacional que le dotaba de medios para poder vivir de ello e investigar. Además, el tratar áreas más empíricas de la ciencia le proveía de compendios teóricos para fomentar su creatividad matemática y científica.

Gauss encontró un importante resultado sobre los números complejos en 1811: para que la integral de línea de una función compleja sea cero, es suficiente que la función sea analítica en todo punto de la curva y dentro de la curva. Sin embargo, no lo publicó y únicamente lo escribió en una carta dirigida a Bessel. Fue Cauchy quien pudo atribuirse el resultado, enfocando el análisis complejo del siglo XIX.

En 1812 estableció las condiciones para definir la convergencia de las series hipergeométricas, introduciendo las principales series de la física matemática de su época. Gracias a esto se pudieron estudiar numerosas ecuaciones diferenciales de la física del siglo XX. A partir de 1820, Gauss comenzó a investigar en el mundo de la Geodesia.

Asimismo, hizo descubrimientos en la teoría electromagnética y en la teoría de la atracción newtoniana, creando la llamada teoría del potencial. De hecho, se dice que los avances matemáticos de Gauss en este campo fueron imprescindibles para el desarrollo de la teoría de la relatividad de Einstein, ya que dicha teoría depende de la geometría diferencial desarrollada por Riemann gracias a Gauss. Es más, la relatividad nació tras el estudio del cálculo tensorial de los matemáticos italianos Ricci y Levi-Civita, discípulos de Riemann y Christoffel, inspirados por el trabajo gaussiano.

Por otro lado, aunque Legendre se quedara a las puertas, fue Gauss quien anticipó el teorema de la distribución de los números primos en el conjunto de los números naturales, escribiéndolo en una tabla de logaritmos elaborada por él con catorce años.

En 1831 desarrolló una fructífera colaboración con el profesor de física Wilhelm Weber, que condujo a nuevos conocimientos sobre magnetismo como la búsqueda de

una representación de la unidad de magnetismo en términos de masa, carga y tiempo y al descubrimiento de las *leyes de circuito de Kirchhoff* en electricidad.

En 1835 formuló el *Teorema de Gauss* sobre electromagnetismo, del cual se derivaron dos de las cuatro ecuaciones de Maxwell. Ese mismo año también demostró el *Teorema de la divergencia de Gauss*, resultado que no se publicó hasta 1867.

Además, demostró algunos teoremas solamente conjeturados hasta entonces, como el *Teorema del número poligonal* de Fermat para $n = 3$, el *Último teorema de Fermat* para $n = 5$, la *regla de los signos* de Descartes o la *conjetura de Kepler para arreglos regulares*, y explicó el *pentagramma mirificum*. También desarrolló un algoritmo para determinar la fecha de Pascua e inventó el algoritmo FFT de Cooley-Turkey para calcular las Transformadas de Fourier discretas 160 años antes que Cooley y Turkey. Asimismo, fue el inventor del heliotropo, el magnetómetro y el telégrafo eléctrico.

Todo el desarrollo de su trabajo a lo largo de su vida quedó recogido en un diario intelectual que permaneció escondido en los papeles familiares hasta 1898. Dicho libro se compone de 19 páginas y 146 resultados, siendo el último del 9 de julio de 1814. Gracias a él se tiene la mayor fuente documental de resultados que Gauss no publicó. Siempre que se analiza algún descubrimiento matemático del siglo XIX se compara con dicho diario para corroborar que Gauss no lo demostrara previamente.

Resulta muy característica la faceta de Gauss de guardarse para sí mismo sus resultados, incluso aquellos de gran trascendencia y relevancia. Se especula que, en cierto modo, esta actitud fue motivada por el supuesto rechazo de la academia francesa a publicar *Disquisitiones Arithmeticae*, pero también se sostiene que se debe al lema del matemático: "*Pauca sed matura*" (pocos pero maduros). Dicho enunciado establece una filosofía de paciente e intensivo estudio con el paso de los años de sus investigaciones para poder llegar al más absoluto perfeccionismo. Se considera a Gauss una persona tremendamente minuciosa y ensimismada cuyo único fin en el desarrollo de sus descubrimientos era la satisfacción personal.

También es destacable su tratamiento de las matemáticas. Gauss poseía un enfoque purista matemático que le brindaba los grandes resultados probados en vida a la par que, mediante su estudio en la astronomía, el cálculo y la física, obtenía un pensamiento empírico para la ciencia. Además, el carácter revolucionario de su perspectiva guiaba los resultados demostrados hasta entonces en una dirección, motivando una nueva visión hacia campos todavía inexplorados y reestructurando las matemáticas. Se le considera el dueño de la perspectiva intelectual e histórica más avanzada de los matemáticos de la época. A pesar de ello, siempre mantuvo una visión de las matemáticas aferrada a la realidad y al mundo; las matemáticas para él surgían de problemas específicos que podían estudiarse de manera genérica. Este enfoque era muy apreciable en sus trabajos en ámbitos externos a las matemáticas. Se podría decir que Gauss era un término medio entre el empirismo del siglo XVIII y la matemática moderna.

Es por ello por lo que se considera el mayor matemático de la historia. Si pensamos en cualquier teorema actual, puede que su prueba dependa de algún resultado previamente probado por él. Se podría decir que los avances en la ciencia actual se deben, en gran parte, a su perfeccionista, rigurosa, abstracta y a la vez empírica mente.

APÉNDICE B
Algunas demostraciones del Capítulo 1

Demostración del Lema 1.33

Demostración. Dada la forma $f(x,y) = a_1x^2 + b_1xy + c_1y^2$, la acción de la matriz $V^{\pm}$ de la demostración del Teorema 1.20 transforma a f en la forma equivalente $\tilde{f} = a_1x^2 + (b_1 + 2a_1k)xy + (a_1k^2 + b_1k + c_1)y^2$ al aplicarse k veces. Esto implica que f y $g(x,y) = a_2x^2 + b_2xy + c_2y^2$ son equivalentes si tienen el mismo discriminante y si $b_1 \equiv b_2 \,(\text{mód } 2a_1)$. □

Demostración del Lema 1.34

Demostración. Gracias al Lema 1.33, basta probar que existe un entero B que satisface las congruencias

$$B \equiv b_1 \ (\text{mód } 2a_1), \qquad B \equiv b_2 \ (\text{mód } 2a_2),$$

para que $f_1 \circ f_2$ y $g_1 \circ g_2$ respectivamente y, en consecuencia, C será un entero, al estar determinado por el discriminante.

Las soluciones de la primera congruencia son de la forma $B = b_1 + 2a_1\delta_1$ para $\delta_1 \in \mathbb{Z}$. Por tanto, la condición necesaria y suficiente para resolver las dos congruencias a la vez es que

$$\frac{b_1 - b_2}{2} \equiv -a_1\delta_1 \ (\text{mód } a_2), \tag{B.1}$$

donde b_1 y b_2 tienen la misma paridad, por lo que la parte izquierda es un entero. Esto tendrá solución si y solo si $\text{mcd}(a_1, a_2) = n$ divide a $\frac{b_1-b_2}{2}$. Como se tiene $D = b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2$, despejando se obtiene que

$$\frac{b_1 + b_2}{2}\frac{b_1 - b_2}{2} = a_1c_1 - a_2c_2. \tag{B.2}$$

Como se cumple que $\text{mcd}(a_1, a_2, \frac{b_1+b_2}{2}) = 1$, (B.2) implica que n divide a $\frac{b_1-b_2}{2}$ como queríamos, por lo que (B.1) tiene solución.

Sea $k = mcm(a_1, a_2) = \frac{a_1 a_2}{n}$. El entero B mencionado anteriormente es único módulo $2k$, por lo que se puede escribir $B = B_0 + 2kt$ con B_0 fijado y t arbitrario. Gracias a esto se tiene que

$$B^2 = B_0^2 + 4ktB_0 + 4k^2t^2 = D + 4a_1a_2m \Longrightarrow B^2 \equiv B_0^2 \equiv D \ (\text{mód } 4k), \tag{B.3}$$

ya que $k \mid a_1a_2$ al ser el mínimo común múltiplo de a_1 y a_2.

El siguiente paso es escoger una t que cumpla $B^2 \equiv D \,(\text{mód } 4a_1a_2)$ para garantizar que C sea un entero. Esto se cumplirá si y solo si

$$\frac{D - B_0^2}{4k} \equiv B_0 t \ (\text{mód } n),$$

lo que se obtiene despejando la segunda igualdad de (B.3) y tomando módulo n. Además, cabe mencionar que la parte izquierda de esta congruencia es un entero. Por la definición de B_0 y la hipótesis de unicidad, B_0 tiene inversa módulo n, por lo que se puede escribir

$$t \equiv \frac{D - B^2}{4k} B_0^{-1} \ (\text{mód } n),$$

y t está determinado de manera única módulo n, por lo que se han encontrado todos los posibles B que son únicos módulo $2a_1a_2$.

Estas formas cumplen que $\text{mcd}(a_1, a_2, B) = 1$ ya que, si n dividiera a B, a_1 y a_2, entonces también dividiría a $(b_1 + b_2)/2$, lo que no puede ocurrir por hipótesis. □

Demostración del Lema 1.35

Demostración. Supongamos que estas formas son equivalentes mediante el cambio de variables $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$. Entonces, por las igualdades de (1.2) (usadas con la notación actual como aparece en el pie de página) se sigue que α y γ corresponden a las de la matriz. Por otro lado, β y δ han de satisfacer

$$\begin{aligned} \alpha\delta - \beta\gamma &= 1 \\ (b_1\gamma + 2a_1\alpha)\beta + (b_1\alpha + 2c_1\gamma)\delta &= b_2, \end{aligned}$$

y resolviendo este sistema utilizando las ecuaciones de (1.2) se obtiene que

$$\begin{aligned} 2a_1\alpha + (b_1 + b_2)\gamma &= 2a_2\delta \\ (b_1 - b_2)\alpha + 2c_1\gamma &= -2a_2\beta, \end{aligned}$$

lo que completa la prueba.

Para probar el recíproco, basta partir de las ecuaciones dadas para terminar en las congruencias anteriores. □

Demostración del Lema 1.36

Demostración. Usando el Lema 1.35, podemos encontrar enteros x_1 e y_1 para la equivalencia $f_1 \sim f_3$, de manera que

(1) $a_1x_1^2 + Bx_1y_1 + a_2Cy_1^2 = m_1$

(2) $2a_1x_1 + (B+N)y_1 \equiv 0 \,(\text{mód } 2m_1)$

(3) $(B-N)x_1 + 2a_2Cy_1 \equiv 0 \,(\text{mód } 2m_1)$

y enteros x_2 e y_2 para $f_2 \sim f_4$ tales que

(4) $a_2x_2^2 + Bx_2y_2 + a_1Cy_2^2 = m_2$

(5) $2a_2x_2 + (B+N)y_2 \equiv 0 \,(\text{mód } 2m_2)$

(6) $(B-N)x_2 + 2a_1Cy_2 \equiv 0 \,(\text{mód } 2m_2)$.

Con el fin de obtener $f_1 \circ f_2 \sim f_3 \circ f_4$, combinando estas ecuaciones existen enteros $X = x_1x_2 - Cy_1y_2$ e $Y = a_1x_1y_2 + a_2y_1x_2 + By_1y_2$ que cumplen

(7) $a_1a_2X^2 + BXY + CY^2 = m_1m_2$

(8) $2a_1a_2X + (B+N)Y \equiv 0 \,(\text{mód } 2m_1m_2)$

(9) $(B-N)X + 2CY \equiv 0 \,(\text{mód } 2m_1m_2)$.

Multiplicando (1) y (4) obtenemos (7). Para conseguir (8), hemos de multiplicar (2) y (5), y al tener f_1 y f_3 el mismo discriminante D por ser equivalentes, se puede sustituir $N^2 \equiv B^2 - 4a_1a_2C \,(\text{mód } 4m_1m_2)$.

Por último, para obtener (9), hemos de escribir:

$$U := \frac{B - \sqrt{D}}{2}X + CY.$$

De aquí se siguen las cuatro ecuaciones siguientes:

$$\begin{aligned}
[(B-\sqrt{D})x_1/2 + a_2Cy_1]\cdot[a_2x_2 + (B+\sqrt{D})y_2/2] &= a_2U \\
[a_1x_1 + (B+\sqrt{D})y_1/2]\cdot[(B-\sqrt{D})x_2/2 + a_1Cy_2] &= a_1U \\
[(B-\sqrt{D})x_1/2 + a_2Cy_1]\cdot[(B-\sqrt{D})x_2/2 + a_1Cy_2] &= (B-\sqrt{D})U/2 \\
C[a_1x_1 + (B+\sqrt{D})y_1/2]\cdot[a_2x_2 + (B+\sqrt{D})y_2/2] &= (B+\sqrt{D})U/2.
\end{aligned}$$

Igual que antes, sustituyendo $N \equiv \sqrt{D} \,(\text{mód } 4m_1m_2)$ todos los términos de la parte izquierda de las ecuaciones son múltiplos de m_1m_2; en consecuencia, los términos de la parte derecha deberán serlo también. Sumando las dos últimas ecuaciones obtenemos

$$a_2U \equiv a_1U \equiv BU \ (\text{mód } m_1m_2)$$

Como $\mathrm{mcd}(a_1, a_2, B) = 1$, esto implica que $U \equiv 0 \,(\mathrm{mód}\ m_1 m_2)$, de lo que se sigue que

$$U = \frac{(B - \sqrt{D})}{2} X + CY \equiv \frac{(B - N)}{2} X + CY \equiv 0 \ (\mathrm{mód}\ m_1 m_2)$$

consiguiendo la última congruencia deseada. □

APÉNDICE C

Método para hallar formas reducidas con números complejos

Existe otro método para encontrar la forma reducida asociada a una cierta forma binaria cuadrática de discriminante negativo empleando números complejos. Este método se debe a la acción de $SL(2,\mathbb{Z})$ sobre $\mathbb{H} = \{z \in \mathbb{C} \mid Im(z) > 0\}$, definida por

$$\gamma(z) := \frac{az+b}{cz+d} \quad \text{para} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \quad \text{y} \quad z \in \mathbb{H}. \tag{C.1}$$

Podemos afirmar que cada órbita hay exactamente un elemento en el *dominio fundamental restringido*

$$\mathcal{D} = \{z \in \mathbb{Z} : -\frac{1}{2} \leq Re(z) \leq 0, \quad |z| \geq 1\} \cup \{z \in \mathbb{H} : 0 \leq Re(z) < \frac{1}{2}, \quad |z| > 1\}.$$

La prueba se realiza de la manera siguiente: para el caso $|z| < 1$, mediante $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ sacamos z fuera del semicírculo, y si z está fuera de la banda $-1/2 \leq Re(z) \leq 1/2$ con cierto $\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ lo podremos meter dentro. Una iteración de estas matrices permite encontrar algorítmicamente una colección $\{\gamma_j\}_{j=1}^{N}$ tal que $(\gamma_1\gamma_2\cdots\gamma_N)(z) \in \mathcal{D}$.

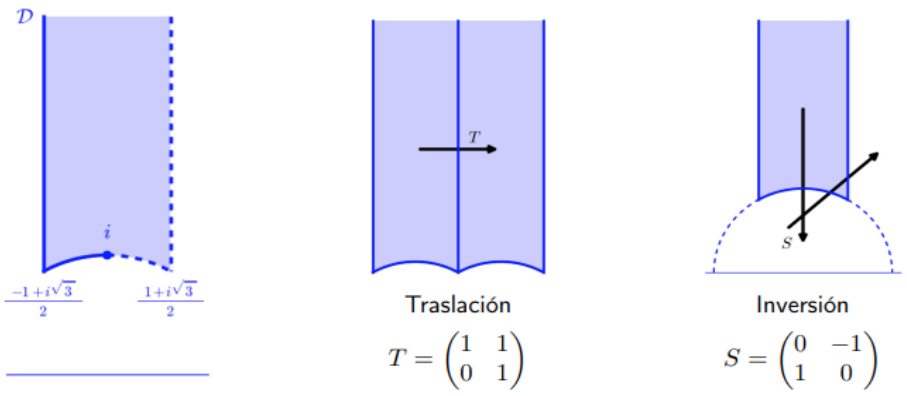


Figura C.1: Imagen extraída de [3].

A cada forma f le asociamos el $z \in \mathbb{H}$ tal que $f(z,1) = 0$. En la otra dirección, cada $z \in \mathbb{H}$ en una extensión cuadrática proviene de una forma f_z obtenida al homogeneizar el polinomio mínimo de z sobre $\mathbb{Z}$. Además, se tiene que $f_z \sim f_\omega$ si y sólo si $z = \gamma(\omega)$ con $\gamma \in SL(2,\mathbb{Z})$ y en consecuencia, por lo mencionado anteriormente, en cada clase hay exactamente una forma f_z con $z \in \mathcal{D}$. Para cada $f(x,y) = ax^2 + bxy + cy^2$ se tiene $z = (-b + i\sqrt{-d})/2a$, y la condición $z \in \mathcal{D}$ da precisamente las desigualdades que conforman la definición de una forma reducida.

Ejemplo C.1. Apliquemos este método utilizando el Ejemplo 1.21 para comprobar que se obtiene el mismo resultado. Sea $f(x,y) = 73x^2 + 54xy + 10y^2$, sabemos que $d = -4$ y

$$z = \frac{-b + i\sqrt{-d}}{2a} = \frac{-54 + 2i}{146} = \frac{-27 + i}{73}.$$

Queremos un $z \in \mathbb{H}$ que pertenezca a $\mathcal{D}$. Para nuestro z inicial se cumple que $-\frac{1}{2} \leq -\frac{27}{73} = Re(z) \leq 0$, pero $|z| = \left|\frac{27^2+1}{73^2}\right| = \frac{10}{73} < 1$, por lo que $z \notin \mathcal{D}$.

Transformando z mediante $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ obtenemos

$$z_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)(z) = \frac{0 \cdot z + 1}{1 \cdot z + 0} = \frac{73}{-27 + i} = \frac{27 + i}{10}$$

que no cumple las restricciones sobre $Re(z_1)$. Sin embargo, si a z_1 le aplicamos $\left(\begin{smallmatrix} 10 & -27 \\ 0 & 1 \end{smallmatrix}\right)$, resulta

$$z_2 = \left(\begin{smallmatrix} 10 & -27 \\ 0 & 1 \end{smallmatrix}\right)(z_1) = \frac{10 \cdot z - 27}{0 \cdot z + 1} = 10 \cdot \frac{27 + i}{10} - 27 = 27 + i - 27 = i$$

y obtenemos $z_2 = i$ que cumple $0 \leq Re(z) = 0 < \frac{1}{2}$ y $|z| = 1$, por lo que $z \in \mathcal{D}$. Como $z = i = \frac{0+2i}{2} = \frac{0+i\sqrt{-(-4)}}{2 \cdot 1}$, resulta $a = 1$, $b = 0$ y $c = -\frac{d-b^2}{4a} = \frac{-4-0}{-4} = 1$, por lo que este número complejo se asocia a la forma $x^2 + y^2$ como habíamos conseguido previamente.

APÉNDICE D
Resultados básicos

D.1. Módulos

Para esta sección se han consultado [12] y [13].

Definición D.1. Sea A un anillo. Un subconjunto N de un A-módulo M es un **submódulo** si, con la adición y con la multiplicación por los elementos de A, es un A-módulo.

Definición D.2. Sea $\{m_i\}_{i\in I}$ un conjunto de elementos de un módulo M.

(i) El A**-submódulo generado por** $\{m_i\}_{i\in I}$ es

$$\langle\{m_i\}_{i\in I}\rangle = \{m \in M : m = \sum_{i\in I} a_i m_i, \text{ con } a_i = 0 \text{ salvo un número finito}\}.$$

(ii) Decimos que $\{m_i\}_{i\in I}$ es un **sistema de generadores de** M si $\langle\{m_i\}_{i\in I}\rangle = M$.

(iii) Si I es un conjunto finito de índices, decimos que el módulo es **finitamente generado**.

(iv) Decimos que $\{m_i\}_{i\in I}$ es una **base** de M si $\langle\{m_i\}_{i\in I}\rangle = M$ y si $\sum_{i\in I} a_i m_i = 0$ implica que $a_i = 0$ para todo $i \in I$.

Teorema D.3. *Todo submódulo de un módulo libre sobre un dominio de ideales principales es libre de rango menor o igual que el del módulo.*

Teorema D.4. *Sea A un anillo unitario, M y N dos A-módulos y X una base de M. Entonces, cada aplicación $f : X \longrightarrow N$ se extiende a un único homomorfismo $f^* : M \longrightarrow N$.*

Teorema D.5. *Sea A un dominio de ideales principales y M un A-módulo con un generador finito de n elementos. Entonces todo submódulo de M admite un sistema de generadores finito con, a lo sumo, n elementos.*

Demostración. Sea $\{x_1, \ldots, x_n\}$ un sistema de generadores de M, L un A-módulo libre de rango n y sea $\{y_1, \ldots, y_n\}$ una base de L. Entonces, por el Teorema D.4 existe un

homomorfismo $f : L \longrightarrow M$ tal que $f(y_i) = x_i$ para cada $i = 1, \ldots, n$. Como $\mathrm{Im}(f)$ es un submódulo que contiene a un sistema de generadores de M, necesariamente ha de ser $\mathrm{Im}(f) = M$, luego es sobreyectiva. Ahora, si N es un submódulo de M, se cumple que $N = \mathrm{Im}(N)$, y por el Teorema D.3 tenemos que $f^{-1}(N)$ es un submódulo de L libre y de rango menor o igual que n. La imagen de una base de $f^{-1}(N)$ es un sistema generador de N. □

D.2. Teoría Algebraica de Números

Los resultados expuestos en esta sección han sido consultados en [17].

Definición D.6. Sea K un cuerpo de números. El **grado** de K sobre $\mathbb{Q}$ se denota como $[K : \mathbb{Q}]$.

Definición D.7. Se dice que $\alpha \in \mathbb{C}$ es un **número algebraico** si y solo si existe un polinomio no nulo con coeficientes racionales tal que α es raíz de dicho polinomio. Esto es equivalente a $[\mathbb{Q}(\alpha) \colon \mathbb{Q}] < \infty$.

Definición D.8. El **polinomio mínimo** de α es el único $P(x)$ mónico que cumple las condiciones descritas en la definición anterior.

Definición D.9. $\alpha \in \mathbb{C}$ es un **entero algebraico** si existe un $P \in \mathbb{Z}[x]$ mónico tal que $P(\alpha) = 0$.

Teorema D.10. *Son equivalentes:*

(i) α *es un entero algebraico.*

(ii) $(\mathbb{Z}[\alpha], +)$ *es finitamente generado.*

(iii) Existe un anillo $R \subset \mathbb{C}$ *tal que* $\alpha \in R$ *y* $(R, +)$ *es finitamente generado.*

(iv) Existe un subgrupo $(A, +) \subset (\mathbb{C}, +)$ *tal que* $\alpha A \subset A$ *y* A *es finitamente generado.*

Teorema D.11. *Sea* K *un cuerpo de característica 0. Un elemento* $c \in K$ *es un entero algebraico sobre* K *si y solo si* $\mathbb{Z}[c] = \{q(c) \mid q(x) \in \mathbb{Z}[x]\}$ *es un* $\mathbb{Z}$*-módulo finitamente generado. En tal caso, es libre de rango* $[\mathbb{Q}(c) : \mathbb{Q}]$.

Definición D.12. Dado un cuerpo de números K, el **anillo de enteros** $\mathcal{O}_K$ es el anillo formado por los enteros algebraicos de K, es decir, el conjunto de todos los $\alpha \in K$ que son raíces de los polinomios mónicos con coeficientes enteros.

La proposición siguiente determina la estructura de $\mathcal{O}_K$:

Proposición D.13. *Sea* K *un cuerpo de números.*

(i) $\mathcal{O}_K$ *es un subanillo de* $\mathbb{C}$ *cuyo cuerpo de fracciones es* K.

(ii) $\mathcal{O}_K$ *es un* $\mathbb{Z}$*-módulo libre de rango* $[K : \mathbb{Q}]$.

El segundo resultado de la Proposición D.13 induce el siguiente corolario:

Corolario D.14. *Si K es un cuerpo de números y $\mathfrak{a}$ es un ideal no nulo de $\mathcal{O}_K$, entonces el anillo cociente $\mathcal{O}_K/\mathfrak{a}$ es finito.*

Definición D.15. Dado un ideal no nulo $\mathfrak{a}$ del anillo $\mathcal{O}_K$, la **norma** de $\mathfrak{a}$ se define como $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$.

Observación D.16. El Corolario D.14 garantiza que $N(\mathfrak{a})$ es finito.

Definición D.17. Sea A un dominio de integridad. Se define el **cuerpo de fracciones de A** como el menor cuerpo que contiene a A, y se denota como $Frac(A)$.

Definición D.18. Un dominio A es **íntegramente cerrado** si $a \in Frac(A)$ es una raíz de un polinomio mónico con coeficientes en A, entonces $a \in A$.

Teorema D.19. *Todo dominio de factorización única es íntegramente cerrado.*

En general, los anillos de enteros de los cuerpos de números no son dominios de factorización única, pero tienen una propiedad de gran utilidad: son *dominios de Dedekind*.

Teorema D.20. *Sea $\mathcal{O}_K$ el anillo de enteros de un cuerpo de enteros K. Entonces $\mathcal{O}_K$ es un dominio de Dedekind, lo que significa que:*

(i) $\mathcal{O}_K$ es integramente cerrado en K, es decir, si $\alpha \in K$ satisface un polinomio mónico con coeficientes enteros en $\mathcal{O}_K$, entonces $\alpha \in \mathcal{O}_K$.

(ii) $\mathcal{O}_K$ es Noetheriano, es decir, dada cualquier cadena de ideales $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$, hay un entero n que cumple $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots$.

(iii) Cada ideal primo no nulo de $\mathcal{O}_K$ es maximal.

La propiedad más importante de los dominios de Dedekind es que tienen factorización única a nivel de ideales (importante ya que habíamos dicho que los anillos de enteros no siempre son dominios de factorización única). De manera más precisa:

Corolario D.21. *Si K es un cuerpo de números, entonces cualquier ideal no nulo $\mathfrak{a}$ de $\mathcal{O}_K$ se puede escribir como el producto*

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

de ideales primos $\mathfrak{p}_i$ para $i = 1, \ldots, r$, y la descomposición es única salvo por el orden.

Todo cuerpo cuadrático se puede escribir de forma única como $K = \mathbb{Q}(\sqrt{D})$, donde $D \neq 0, 1$ es un entero libre de cuadrados. Un invariante básico de K es su **discriminante** Δ_K, que se define como

$$\Delta_K = \begin{cases} D & \text{si } D \equiv 1 \text{ (mód 4)} \\ 4D & \text{en otro caso} \end{cases} \tag{D.1}$$

Nótese que $\Delta_K \equiv 0, 1 \pmod 4$ y que $K = \mathbb{Q}(\sqrt{\Delta_k})$, por lo que el cuerpo cuadrático queda determinado por su discriminante.

El siguiente paso es describir el anillos de enteros $\mathcal{O}_K$ de K. Escribiendo $K = \mathbb{Q}(\sqrt{D})$, con D un entero libre de cuadrados, se demuestra que

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

Usando el discriminante, la descripción de $\mathcal{O}_K$ puede ser escrita de la siguiente forma:

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{\Delta_K + \sqrt{\Delta_K}}{2}\right] \tag{D.3}$$

Teorema D.22. *Sea $K = \mathbb{Q}(\omega)$ un cuerpo de números con $\mathcal{O}_K = \mathbb{Z}[\omega]$. Sea $g(x) \in \mathbb{Z}[x]$ el polinomio mínimo de ω y sea $p \in \mathbb{Z}$ primo. Sea $\tilde{g}(x) = \tilde{g_1}(x)^{e_1} \cdots \tilde{g_r}(x)^{e_r} \in \mathbb{F}_p[x]$ la descomposición en factores primos de $\tilde{g}(x)$ que resulta $\tilde{g}(x) = g(x) \pmod p$. Entonces, la descomposición de $p\mathcal{O}_K$ en primos es $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, donde los $\mathfrak{p}_i$ primos tienen índice de ramificación igual a $\deg \tilde{g}_i$, es decir $N(\mathfrak{p}^i) = p^{f_i}$, $f_i = \deg \tilde{g}_i$. Es más, si $g_i \in \mathbb{Z}[x]$ (podría ser mónico) tal que $g_i(x) \equiv \tilde{g}_i(x) \pmod p$, entonces $\mathfrak{p}_i = \langle p, g_i(\omega) \rangle$.*

Observación D.23. Sabemos que $C(\mathcal{O}_K)$, el grupo de clases de $\mathcal{O}_K$, es un grupo. Esto se debe a la relación de equivalencia siguiente: dados dos ideales arbitrarios $\mathfrak{a}, \mathfrak{b} \in \mathcal{O}_K$, se dice que $\mathfrak{a}$ y $\mathfrak{b}$ están relacionados si y solo si existen $a, b \in \mathcal{O}_K$ tales que $a\mathfrak{a} = b\mathfrak{b}$.

A partir de esta relación de equivalencia, se definen el producto de dos clases de $C(\mathcal{O}_K)$ como $[\mathfrak{a}] \cdot [\mathfrak{b}] := [\mathfrak{a} \cdot \mathfrak{b}]$ y el elemento neutro $[\mathfrak{c}]$ con $\mathfrak{c} = \{\langle r \rangle : r \in \mathcal{O}_K, r \neq 0\}$. Como para todo ideal $\mathfrak{a}$ no nulo de $\mathcal{O}_K$ existe otro ideal $\mathfrak{b}$ no nulo de $\mathcal{O}_K$ tal que $\mathfrak{ab}$ es principal, se sigue $C(\mathcal{O}_K)$ es un grupo.

Teorema D.24. *Sea K un cuerpo de números de grado n. Clasificamos los automorfismos $K \longrightarrow \mathbb{C}$ de la siguiente forma:*

- *Hay r automorfismos reales $K \longrightarrow \mathbb{R}$.*
- *Hay $2s$ automorfismos complejos que no son reales $K \longrightarrow \mathbb{C} \backslash \mathbb{R}$.*

Entonces podemos afirmar que para toda clase $C \in C(\mathcal{O}_K)$ existe un ideal $\mathfrak{a} \in C$ tal que[1]

$$N(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_K|} \tag{D.4}$$

[1]El valor $\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s$ se denomina la constante de Minkowski y, de hecho, este teorema es una aplicación del famoso Teorema de Minkowski que afirma que cualquier conjunto convexo de $\mathbb{R}^n$ simétrico respecto al origen y con volumen mayor que 2^n contiene un punto de retículo no nulo, demostrado por Hermann Minkowski en 1889.

Definición D.25. Sea $n \in \mathbb{Z}$, p primo tal que $p \nmid n$. Definimos el **símbolo de Legendre** como:

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{si } n \text{ es cuadrado módulo } p \\ -1 & \text{si } n \text{ no es cuadrado módulo } p. \end{cases}$$

Teorema D.26 (Ley de Reciprocidad Cuadrática)**.** *Dados p, q primos impares distintos,*

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

Es decir,

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{si } p \equiv 1 \pmod 4 \text{ o } q \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right) & \text{si } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

D.2.1. Cálculo del cardinal del grupo de clases

Para entender la metodogía empleada al final del Capítulo 2, se realizará un ejemplo para entender cómo hallar el cardinal del grupo de clases con las herramientas de la Teoría de Números Algebraica.

Ejemplo D.27. Sea $K = \mathbb{Q}(\sqrt{-17})$, donde $\mathcal{O}_K = \mathbb{Z}[\sqrt{-17}]$ y el polinomio mínimo de $\sqrt{-17}$ sobre $\mathbb{Q}$ es $p(x) = x^2 + 17$. Por el Teorema D.24, en toda clase hay un ideal $\mathfrak{a}$ de norma

$$N(\mathfrak{a}) \leq \frac{4}{\pi}\sqrt{17} \sim 5,25 < 6.$$

Por tanto, es necesario estudiar los ideales de hasta norma 5. Para ello, utilizaremos el Teorema D.22, que nos ayudará a encontrar dichos ideales.

En el caso de $2\mathcal{O}$, se tiene que $\overline{p}(x) = x^2 + 17 \,(\text{mód } 2) \equiv x^2 + 1 \equiv (x+1)^2 \,(\text{mód } 2)$, por lo que

$$\mathfrak{p} = \langle 2, 1 + \sqrt{-17}\rangle, \quad \langle 2\rangle = \mathfrak{p}^2 \quad \text{con } N(\mathfrak{p}) = 2$$

y encontramos un ideal de norma 2 en K.

Para $3\mathcal{O}$, $\overline{p}(x) = x^2 + 17 \equiv x^2 - 1 \equiv (x+1)(x-1) \,(\text{mód } 3)$, de modo que

$$\mathfrak{q}_1 = \langle 3, 1 + \sqrt{-17}\rangle, \quad \mathfrak{q}_2 = \langle 3, 1 - \sqrt{-17}\rangle, \quad \langle 3\rangle = \mathfrak{q}_1\mathfrak{q}_2 \quad \text{con } N(\mathfrak{q}_i) = 3$$

y resultan dos ideales de norma 3 en K.

Para $4\mathcal{O}$ tenemos el $\langle 4\rangle = \langle 2\rangle^2 = \mathfrak{p}^4$, por lo que el único ideal de norma 4 es $\mathfrak{p}^2$.

En el caso $5\mathcal{O}$, $\overline{p}(x) = x^2 + 17 \equiv x^2 + 2 \,(\text{mód } 5)$, que resulta irreducible al estudiar los valores que toma en $\mathbb{F}_5$ y observar que no se anula para ningún valor, por lo que no tiene raíces. Esto hace que

$$\langle 5\rangle = \mathfrak{r} \quad \text{con } N(\mathfrak{r}) = 25$$

de modo que no hay ideales de norma 5.

Por tanto, hemos conseguido 4 clases: $[\mathcal{O}]$, $[\mathfrak{p}]$, $[\mathfrak{q}_1]$ y $[\mathfrak{q}_2]$. Queda ver que son diferentes entre ellos.

Sabemos que $[\mathcal{O}] \neq [\mathfrak{p}]$ ya que, de ser así, $\mathfrak{p}$ sería principal, pero eso no es posible dado que no existe ningún $\alpha_1 = a_1 + b_1\sqrt{-17} \in \mathbb{Z}[\sqrt{-17}]$ con $a_1, b_1 \in \mathbb{Z}$ tal que $N(\alpha) = a_1^2 + 17b_1^2 = 2$. Del mismo modo, $[\mathcal{O}] \neq [\mathfrak{q}_1]$ pues no existe ningún $\alpha_2 = a_2 + b_2\sqrt{-17} \in \mathbb{Z}[\sqrt{-17}]$ con $a_2, b_2 \in \mathbb{Z}$ tal que $N(\alpha) = a_2^2 + 17b_2^2 = 3$ y, análogamente, $[\mathcal{O}] \neq [\mathfrak{q}_2]$ pues $\mathfrak{q}_1$ y $\mathfrak{q}_2$ tienen la misma norma.

Por otro lado, $[\mathfrak{p}] \neq [\mathfrak{q}_i]$ ya que, si fuera cierto, $[\mathfrak{p}]^2 = [\langle 4\rangle] = [\mathcal{O}] = [\mathfrak{p}\mathfrak{q}_i] = [\mathfrak{p}][\mathfrak{q}_i]$, de modo que $\mathfrak{p}\mathfrak{q}_i$ debería ser principal, pero esto implicaría que existen $a_3, b_3 \in \mathbb{Z}$ tales que $a_3^2 + 17b_3^2 = 6$, lo cual es imposible.

Por último, sabemos que $[\mathfrak{q}_1] \neq [\mathfrak{q}_2]$ ya que, de lo contrario,

$$[\mathfrak{q}_1]^2 = [\mathfrak{q}_1][\mathfrak{q}_2] = [\langle 3\rangle] = [\mathcal{O}] \Longrightarrow [\mathfrak{q}_1]^2 = [\mathfrak{q}_1^2] = [\mathcal{O}] \Longrightarrow \mathfrak{q}_1^2 = \langle\alpha\rangle,$$

para cierto $\alpha = a + b\sqrt{-17} \in \mathcal{O}_K$ con $a, b \in \mathbb{Z}$. Esto implica que $|N(\alpha)| = N(\mathfrak{q}_1)^2 = 9$, por lo que $a^2 + 17b^2 = 9$. La única solución posible es $a = \pm 3$, $b = 0$, de modo que $\alpha = 3$, pero entonces sería $\mathfrak{q}_1^2 = \langle 3\rangle = \mathfrak{q}_1\mathfrak{q}_2$. Simplificando lo anterior resulta $\mathfrak{q}_1 = \mathfrak{q}_2$, lo que sería una contradicción.

APÉNDICE E

Conjeturas sobre el cardinal del grupo de clases

La información que se expondrá a continuación se ha consultado en [1], [11] y [22].

Ahora que se dispone tanto de las herramientas sobre formas binarias cuadráticas y sobre Teoría de Números Algebraica, no se puede omitir un hecho muy importante que Gauss expuso en *Disquisitiones Arithmeticae* y que ha sido objeto de estudio durante los últimos siglos. En su obra, el matemático formuló tres conjeturas importantes[1] sobre el número $h(D)$ de clases dado el discriminante de una forma binaria cuadrática.

La primera afirma que $h(D) \longrightarrow \infty$ cuando $D \longrightarrow -\infty$. Esta conjetura fue solventada por Hans Arnold Heilbronn [11] en 1934, resultando cierta.

Por otro lado, para un número bajo de clases, Gauss dio una lista de cuerpos cuadráticos imaginarios con el número de clases dado y conjeturó que no había más que esos. La demostración de esta fue resuelta por partes con el paso de los años.

En primer lugar, el caso $h(D) = 1$ se resolvió en 1952 gracias a Kurt Heegner, aunque con algunos errores que después se vieron que no eran esenciales, y posteriormente por Henry Frederick Baker y Johannes Stark en 1966 y 1967 respectivamente de manera independiente. Esta hipotésis es conocida como *el problema del número de clase uno de Gauss*, y se sabe que son $D = -3,-4,-7,-8,-11,-19,-43,-67,-163$ para discriminantes fundamentales, $D = -12,-16,-27,-28$ para no libres de cuadrados y $D = -4,-8,-12,-16,-28$ para discriminantes pares (conjetura original de Gauss).

El caso $h(D) = 2$ fue resuelto por Baker y Stark en 1971 y el caso $h(D) = 3$ fue demostrado por Joseph Oesterlé en 1985. Por último, para números hasta 100 se consiguió gracias a Watkins en 2004.

Cabe mencionar que el problema original de Gauss era ligeramente diferente y más fácil que el problema resuelto en la actualidad, ya que él se centró en discriminantes pares y los no libres de cuadrados.

La tercera conjetura mantiene que hay infinitos cuerpos cuadráticos reales con $h(D) = 1$. Esta es una cuestión abierta a día de hoy. Es posible, e incluso probable, que existan infinitos cuerpos cuadráticos reales para los que $h(D) = 1$, pero nadie ha

[1] [10] #303 y #304, págs. 374–377.

podido demostrarlo hasta ahora. La llamada "heurística de Cohen-Lenstra" apunta a que la proporción de primos p para los que $h(Q(\sqrt{p})) = 1$ está alrededor del 75,446 %, lo que en particular implica que $h(Q(\sqrt{p})) = 1$ para infinitos primos p. El motivo esencial por el que es más difícil acotar el número de clases para cuerpos cuadráticos reales que para cuerpos cuadráticos imaginarios es que en los reales el anillo de enteros tiene infinitas unidades (esto hace que un irreducible tenga infinitos asociados).

Bibliografía

[1] Bhand, A. and Murty, M.R.: Class numbers of quadratic fields, *Hardy-Ramanujan Journal*, **42** (2019) 17–25.

[2] Buell, D.A.: Binary quadratic forms: classical theory and modern computations. *Springer-Velag, New York*, (1989).

[3] Chamizo, F.: Ocho lecciones de teoría de números (2011) https://matematicas.uam.es/~fernando.chamizo/libreria/fich/lecc8.pdf. Acceso: 2022-02-18.

[4] Chowla, S.: An extension of Heilbronn's class-number theorem, *The Quaterly Journal of Mathematics*, **5** (1934) 304–307.

[5] Cox, D.A.: Primes of the form $x^2 + ny^2$, *Wiley, Hoboken*, (2013).

[6] Dujella, A.: Number theory, *Školska Knjiga, Zagreb*, **2** (2021).

[7] Euler, L.: Introductio in Analysin Infinitorum, *MM Bousquet, Lausanne*, **1** (1748) 214.

[8] Euler, L.: Novae demonstrationes circa divisores numerorum formae $xx + nyy$, *Nova Acta Academiae Scientiarum Imperialis Petropolitanae*, (1787) 47–74.

[9] Euler, L.: Opuscula analytica, tomus secundus, *St. Petersburg: Imperial Academy of Sciences*, (1785).

[10] Gauss, C.F.: Disquisitiones Arithmeticae (Spanish), *Enrique Pérez Arbeláez Collection, Academia Colombiana de Ciencias Exactas, Físicas y Naturales, Bogotá, Traducido del latín por Hugo Barrantes Campos, Michael Josephy y Ángel Ruiz Zúñiga; con un prefacio por Ruiz Zúñiga*, **10** (1995).

[11] Heilbronn, H.: On the class-number in imaginary quadratic fields, *The Quaterly Journal of Mathematics*, **5** (1934) 150–160.

[12] Ivorra, C.: Álgebra (2021), https://www.uv.es/ivorra/Libros/Al.pdf. Acceso: 2022-05-09.

[13] Ivorra, C.: Teoría Algebraica de Números (2021), https://www.uv.es/ivorra/Libros/TAl.pdf. Acceso: 2021-10-31.

[14] Lagrange, J.L.: Recherches d'analyse indéterminée, *Hist. De l'Ac. Des Sc.*, (1785).

[15] Legendre, A.M.: Essai sur la théorie des nombres, *Cambridge University Press, Cambridge*, (2009).

[16] Lemmermeyer, F.: Reciprocity laws: from Euler to Eisenstein, *Springer Monographs in Mathematics. Springer-Verlag, Berlin*, (2000).

[17] Marcus D.A.: Number fields, *Universitext, Springer, Cham*, (2018).

[18] Menares, R. (Organizador): Seminario CM (2020), https://www.mat.uc.cl/~rmenares/SeminarioCM.html. Acceso: 2022-05-20.

[19] Richmond, H.W.: A construction for a regular polygon of seventeen sides, *The quarterly journal of pure and applied mathematics*, **26** (1893) 206–207.

[20] The Sage Developers: SageMath, the Sage Mathematics Software System (Version SageMathCell) (2022), https://sagecell.sagemath.org/.

[21] Shepherd, R.L.: Binary quadratic forms and genus theory, *A Thesis Submitted to The University of North Carolina at Greensboro in Partial Fulfillment of the Requirements for the Degree Master of Arts, Faculty of the Graduate School, North Carolina*, (2013).

[22] Watkins, M.: Class numbers of imaginary quadratic fields, *Math. Comp.* **73** (2004) 907–938 .

[23] Weinberger, P.J.: Exponents of the class groups of complex quadratic fields, *Acta Arithmetica*, **22** (1973) 117–124.