Universidad de Valparaíso
Facultad de Ciencias
Instituto de Matemáticas

Cuerpos Cuadráticos Imaginarios con Número de Clases 2

Por
GASTÓN VERGARA HERMOSILLA

Tesis presentada para optar al grado de Licenciado en Matemáticas.

Profesor guía: Dra. Amalia Pizarro Madariaga

Valparaíso 2016

Comisión Examinadora:

- Dra. Amalia Pizarro M. (Universidad de Valparaíso)
- Dr. Rodrigo Castro M. (Universidad de Valparaíso)
- Dr. Ricardo Menares V. (Pontificia Universidad Católica de Valparaíso)

Dicen que dice la ley que somos iguales
nadie te dira en que sitio pues nadie lo sabe
dime, dime, para quien hicieron la carcel
porque el rico nunca entra y el pobre nunca sale...
Igual para todos, La Polla Records, 1999.

Índice general

Introducción

Esta tesis se enmarca en el área de Teoría de Números, es decir, estudiaremos propiedades aritméticas y análiticas de ciertos objetos algebraicos.

Nuestro principal objetivo en este trabajo es estudiar un caso particular del problema del número de clases de Gauss, en específico, mostraremos que se puede determinar de manera efectiva todos los cuerpos cuadráticos imaginarios con número de clases 2. Para esto, utilizaremos herramientas de la teoría de géneros, propiedades de las funciones L de Dirichlet y resultados generales de formas lineales en logaritmos de números algebraicos.

La principal motivación para el estudio de este problema surge en 1801, cuando Gauss en su libro *Disquisitiones Arithmeticae* conjetura que la cardinalidad del grupo de clases de ideales de un cuerpo de números $\mathbb{Q}(\sqrt{\mathtt{d}})$, la cual es denotada por $\mathtt{h}_{\mathbb{Q}(\sqrt{\mathtt{d}})}$, cumple que $\mathtt{h}_{\mathbb{Q}(\sqrt{\mathtt{d}})} \longrightarrow \infty$ cuando $\mathtt{d} \longrightarrow -\infty$. En 1934 Heilbronn, Hecke y Deuring demuestran la conjetura, y así surge la necesidad de encontrar un algoritmo que determine de manera efectiva los cuerpos cuadráticos imaginarios para cada número de clases. Los primeros avances importantes en la resolución de este problema fueron obtenidos por Heegner en 1952, Stark en 1967 y Baker en 1966, quienes de manera independiente obtuvieron la solución para el número de clases 1. Posteriormente, en 1971, Baker resuelve el problema para el caso del número de clases 2, y así en 1976, Goldfed, basado en resultados de curvas elípticas, da los simientos de la solución general del problema, la cual junto con Gross y Zagier, logran resolver en 1985.

A continuación describiremos brevemente cada capítulo de esta tesis.

En el Capítulo 1, introduciremos la noción de función L de Dirichlet y sus propiedades. Comenzaremos describiendo características elementales de caracteres en un contexto de grupos abelianos, para así dar lugar a la construcción de caracteres de Dirichlet, con especial enfasis en la descripción de caracteres asociados a cuerpos cuadáticos imaginarios. Posteriormente formalizaremos el concepto de serie de Dirichlet el cual nos permitirá definir las funciones L de Dirichlet y así poder centrarnos en el estudio de su continuidad análitica y la admisión de una ecuación funcional.

En el Capítulo 2, estableceremos una fórmula para obtener el número de clases de un cuerpo cuadrático imaginario. Para esto introduciremos los conceptos de reticulado complejo y función zeta de Dedekind de un cuerpo cuadrático, estudiaremos sus principales propiedades las cuales nos permitirán establecer una relación directa entre ambas definiciones, lo cual nos conducirá a encontrar estimaciones efectivas para el número de clases (ver Teorema 2.4). Por otro lado analizaremos la noción de función L de Dirichlet cuadrática, la cual nos brindará un valor eficiente para las funciones L en el caso de cuerpos cuadráticos reales e imaginarios (ver Teorema 2.3). Con estas herramientas podremos establecer un resultado debido a Dirichlet para obtener el número de clases de un cuerpo cuadrático imaginario (ver Teorema 2.3).

En el Capítulo 3, presentaremos resultados generales de formas cuadráticas, formas lineales en logaritmos y teoría de géneros. Comenzaremos revisando definiciones relevantes de la teoría de formas cuadráticas binarias, las cuales nos permitiran tener una clasificación en términos de equivalencia, determinantes y discriminantes de dichas formas. Por otro lado presentaremos resultados básicos sobre la teoría de géneros de formas cuadráticas, teniendo como principales referencias los textos de B. Jones [**13**] y D. Cox [**7**]. Por último estudiaremos la noción de altura de números algebraicos, la cual da los cimientos a los avances hechos por Baker en 1966 en materia de formas lineales en logaritmos, los cuales son unos de los principales sustentos para nuestro objetivo principal.

En el Capítulo 4, mostraremos que es posible determinar de manera efectiva cada cuerpo cuadrático imaginario con número de clases 2. Comenzaremos presentando uno de los principales resultados de Baker en [**23**], en el cual se relaciona ciertos números de clases con una serie en terminos de formas cuadráticas binarias, dando una idea de su demostración (ver Teorema 4.1). Este resultado, conformará uno de los principales argumentos para demostrar la solución del problema del número de clases 2 (ver Teorema 4.2).

Para finalizar, hemos incluido dos apéndices, en el primero trataremos algunos tópicos generales de teoría algebraica de números, donde destacamos el estudio de la factorización única de ideales, normas, trazas y discriminantes de un cuerpo de números y propiedades de cuerpos cuadráticos, culminando con la revisión de las principales definiciones y propiedades del grupo de clases de ideales. En el segundo apéndice presentaremos una tabla con los números de clases de los cuerpos cuadráticos imaginarios $\mathbb{Q}(\sqrt{-\mathtt{d}})$, donde $\mathtt{d}$ es libre de cuadrados y $1 \leqslant \mathtt{d} < 500$.

Tabla de Notaciones

Símbolo	Significado
K	Cuerpo de Números
(a, b)	Máximo común divisor entre a y n
$\mathcal{O}_K$	Anillo de enteros sobre K
$Tr_K(\alpha)$	Traza de $\alpha \in K$
N_K	Norma de $\alpha \in K$
$N(\mathcal{A})$	Norma absoluta del ideal $\mathcal{A}$
d_K	Discriminante del cuerpo K
$w(K)$	Número de raices de la unidad en K
I_K	Conjunto de ideales fraccionarios de K
P_K	Conjunto de ideales fraccionarios principales de K
Cl_K	Grupo de clases de ideales de K
h_K	Número de clases de ideales de K
χ	Carácter de K
$\left(\frac{d_K}{n}\right)_{\mathcal{K}}$	Símbolo de Kronecker asociado al discriminante d_K
χ_K	Carácter cuadrático de K
$f(s, a_n)$	Serie de Dirichlet
$Re(z)$	Parte real del número complejo z
$\zeta(s)$	Función Zeta de Riemann
$\theta(s)$	Serie Theta de Jacobi

Símbolo	Significado
$Z(s)$	Función Zeta completada
$L(s, f)$	Transformada de Mellin de f
$L(s, \chi)$	Función L de Dirichlet
$\Lambda(s, \chi)$	Función L de Dirichlet completada
$\tau(n, \chi)$	Suma de Gauss asociada a χ
$\zeta_K(s)$	Función zeta de Dedekind de K
$\mathbf{SL}_2(\mathbb{Z})$	Grupo de matrices de 2×2 con entradas en $\mathbb{Z}$ y determinante igual a 1
$M(f)$	Medida de Mahler del polinomio $f(x)$
$h(\alpha)$	Altura (de Weil) del número algebraico α
$f(x) \sim g(x)$	$f(x)$ es asintótica a $g(x)$, es decir, $\lim_{x\longrightarrow\infty} \frac{f(x)}{g(x)} = 1$
$f = O(g)$	Existen constantes k y $M > 0$ tales que $\lvert f(x)\rvert \leqslant k\lvert g(x)\rvert$ para cada $\lvert x\rvert > M$

Capítulo 1

Funciones L de Dirichlet

El objetivo de este capítulo es hacer una revisión de las principales nociones y propiedades que definen a las funciones L de Dirichlet, destacando la continuidad analítica y el hecho que satisface una ecuación funcional.

1. Caracteres

Consideremos G un grupo abeliano finito. Un homomorfismo χ de G en $\mathbb{C}^\times$, se denomina **cáracter** de G, χ tiene las propiedades;

1. $\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$, para cada α, $\beta \in G$.
2. $\chi(e_G) = 1$, donde e_G es el neutro de G.
3. $\chi(\alpha^{-1}) = \chi^{-1}(\alpha) = \overline{\chi(\alpha)}$.

Los caracteres de G forman un grupo denotado por $\widehat{G}$ y que será llamado **grupo dual**, donde

$$\chi_1\chi_2(\alpha) = \chi_1(\alpha)\chi_2(\alpha), \text{ para cada } \alpha \in G.$$

La función identidad es su elemento neutro y lo llamaremos carácter trivial χ_0, y dado $\chi \in \widehat{G}$, su inverso es definido como $\chi^{-1}(\alpha) = \overline{\chi}(\alpha) := \overline{\chi(\alpha)}$.

Si G es un grupo abeliano orden m, dado $\chi \in \widehat{G}$ se tiene $\chi^m(\alpha) = 1$, y así $\chi(\alpha)$ es una raíz m-ésima de la unidad.

A continuación, revisaremos algunas propiedades de importancia en lo que viene.

Proposición 1.1 (Dirichlet). *Sea G un grupo abeliano, y χ un cáracter no trivial de $\widehat{G}$. Entonces*

$$\sum_{g \in G} \chi(g) = 0.$$

Demostración.

Para cada $h \in G$, tenemos

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg).$$

Pero, como g corre sobre todo G, también lo hace hg. Así

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g).$$

Por tanto, $\chi(h) = 1$ ó $\sum_{g \in G} \chi(g) = 0$. Como χ es no trivial, podemos escoger h de tal manera que la primera condición no sea cierta. Así, la Proposición es demostrada.

❏

TEOREMA 1.1 (Dirichlet). *Sean χ_1 y χ_2 dos caracteres distintos de un grupo abeliano finito G. Entonces*

$$\sum_{g \in G} \chi_1(g)\chi_2(g)^{-1} = 0.$$

Además, si $g \neq h$, entonces

$$\sum_{\chi \in \hat{G}} \chi_1(g) = 0.$$

Demostración.

Ver, Capítulo IV, Sección 1 de [9].

❏

DEFINICIÓN 1.1. *Llamaremos **cáracter de Dirichlet** a cada carácter*

$$\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times.$$

Es posible extender la definición de χ a $\mathbb{Z}$ mediante

$$\chi(a) = \begin{cases} \chi(a \ mod \ m) & si \ (a, m) = 1, \\ 0 & en \ otro \ caso. \end{cases}$$

Consideremos los enteros $\mathfrak{m}$, $\mathfrak{n}$ tales que $\mathfrak{m} \mid \mathfrak{n}$, χ' un cáracter (módulo $\mathfrak{m}$)*, y

$$\chi(\mathfrak{a}) = \begin{cases} \chi'(\mathfrak{a}) & \text{si } (\mathfrak{a}, \mathfrak{n}) = 1, \\ 0 & \text{en otro caso.} \end{cases}$$

Así, χ es un cáracter de Dirichlet (módulo $\mathfrak{n}$). En esta situación diremos que χ' **induce** a χ.

Definición 1.2. *Diremos que un cáracter es* ***primitivo*** *si éste no es inducido por ningún cáracter de módulo menor.*

Lema 1.2. *Consideremos los enteros coprimos* $\mathfrak{q}_1$, $\mathfrak{q}_2$ *y los caracteres de Dirichlet* χ_1, χ_2 *módulo* $\mathfrak{q}_1$ *y* $\mathfrak{q}_2$ *respectivamente. Definimos* $\chi(\mathfrak{n}) = \chi_1(\mathfrak{n})\chi_2(\mathfrak{n})$. *Entonces, el carácter* χ *es primitivo módulo* $\mathfrak{q}_1\mathfrak{q}_2$, *si y sólo si,* χ_1, χ_2 *son primitivos.*

Demostración. Ver pag. 283 de Montgomery y Vaughan [**8**]. ❏

Definición 1.3. *Sea* χ *un cáracter de Dirichlet (módulo n). Diremos que* $\mathfrak{m}$ *es un cuasiperiodo de* χ *si* $\chi(\mathfrak{m}) = \chi(\mathfrak{m}')$ *cuando* $\mathfrak{m} \equiv \mathfrak{m}'$ *(mod n) y* $(\mathfrak{m}\mathfrak{m}', \mathfrak{n}) = 1$. *El menor cuasiperiodo* $\mathfrak{m}$ *de* χ *es llamado* ***conductor*** *de* χ.

Para un revisión acabada de caracteres primitivos y conductores recomendamos consultar [**8**].

Ejemplo 1. *Al considerar* $\mathsf{G} = (\mathbb{Z}/8\mathbb{Z})^\times$, *definimos sus caracteres mediante la siguiente tabla:*

	χ_0	χ_1	χ_2	χ_3
1	*1*	*1*	*1*	*1*
3	*1*	*-1*	*-1*	*1*
5	*1*	*1*	*-1*	*-1*
7	*1*	*-1*	*1*	*-1*

*Notemos que χ' tiene como dominio $\mathbb{Z}/\mathfrak{m}\mathbb{Z}$.

Tenemos que $\chi_1\chi_2 = \chi_3$ *y* $\chi_i^2 = \chi_0$ *para cada* i*, así el grupo dual* $\widehat{G}$ *viene dado por el grupo de Klein.*

DEFINICIÓN 1.4. *Sean* n *un número entero y* m *un número natural impar. Definimos el* ***símbolo de Jacobi*** *como el producto de los símbolos de Legendre*[**] *correspondientes a los factores primos de* m*, es decir*

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)^{\alpha_1}\left(\frac{n}{p_2}\right)^{\alpha_2}\cdots\left(\frac{n}{p_r}\right)^{\alpha_r}$$

donde $m = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$*, con cada* p_i *primo.*

TEOREMA 1.3 (Fórmula general de reciprocidad cuadrática para el símbolo de Jacobi). [***]

$$\boxed{\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) \;=\; (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\;.}$$

DEFINICIÓN 1.5. *Diremos que un carácter de Dirichlet es* ***cuadrático****, si y sólo si,* $\chi^2 = 1$*, es decir* $\chi(n)^2 = 1$*, para cada entero* n*.*

Con esto vemos que un carácter de Dirichlet cuadrático sólo toma los valores $\{-1, 1\}$.

Ahora, notemos que un carácter cuadrático χ módulo p es inducido por el carácter primitivo χ' modulo q, con $q \mid p$, entonces χ es cuadrático si y sólo si, χ' es cuadrático.

[**]Para ver su definición ver apéndice A.

[***]Una idea de la demostración consiste en descomponer P y Q en sus factores primos irreducibles y reordenar mediante la fórmula de reciprocidad cuadrática para el símbolo de Legendre.

En lo que sigue demostraremos que los caracteres cuadráticos[****] provienen del símbolo de Kronecker.

DEFINICIÓN 1.6. *Diremos que* $\mathfrak{d}$ *es un* ***discriminante cuadrático****, si*

1. $\mathfrak{d} \equiv 1\,(mod 4)$ *y* $\mathfrak{d}$ *es libre de cuadrados, o*
2. $4 \mid \mathfrak{d}, \mathfrak{d}/4 \equiv 2$ *o* $3\,(mod 4)$ *y* $\mathfrak{d}/4$ *es libre de cuadrados.*

DEFINICIÓN 1.7. *Sea* $\mathfrak{d}$ *un discriminante cuadrático. Definimos el* ***símbolo de Kronecker*** $\left(\frac{\mathfrak{d}}{\mathfrak{n}}\right)_{\mathcal{K}}$ *por las siguientes relaciones:*

1. $\left(\frac{\mathfrak{d}}{\mathfrak{n}}\right)_{\mathcal{K}} = 0$, *cuando* $\mathfrak{n} \mid \mathfrak{d}$.
2. $\left(\frac{\mathfrak{d}}{2}\right)_{\mathcal{K}} = \begin{cases} 1 & si\ \mathfrak{d} \equiv 1\,(mod 8), \\ -1 & si\ \mathfrak{d} \equiv 5\,(mod 8), \end{cases}$
3. $\left(\frac{\mathfrak{d}}{\mathfrak{p}}\right)_{\mathcal{K}} = \left(\frac{\mathfrak{d}}{\mathfrak{p}}\right)$, *el símbolo de Legendre, si* $\mathfrak{p} > 2$,
4. $\left(\frac{\mathfrak{d}}{-1}\right)_{\mathcal{K}} = \begin{cases} 1 & si\ \mathfrak{d} > 0, \\ -1 & si\ \mathfrak{d} < 0, \end{cases}$
5. $\left(\frac{\mathfrak{d}}{\mathfrak{n}}\right)_{\mathcal{K}}$ *es una función totalmente multiplicativa de* $\mathfrak{n}$.

TEOREMA 1.4. *Sea* $\mathfrak{d}$ *un discriminante cuadrático. Entonces,* $\left(\frac{\mathfrak{d}}{\mathfrak{n}}\right)_{\mathcal{K}}$ *es un carácter cuadrático primitivo módulo* $\mid \mathfrak{d} \mid$*, y cada carácter cuadrático primitivo se da únicamente de esta manera.*

Demostración.

Consideremos el carácter cuadrático primitivo módulo 4, $\left(\frac{-4}{\mathfrak{n}}\right)_{\mathcal{K}}$ y los caracteres cuadráticos módulo 8 ; $\left(\frac{8}{\mathfrak{n}}\right)_{\mathcal{K}}$, $\left(\frac{-8}{\mathfrak{n}}\right)_{\mathcal{K}}$.
Supongamos que $\mathfrak{p}$ es un número primo tal que $\mathfrak{p} \equiv 1\,(\mathrm{mod}\,4)$, demostraremos que para cada entero $\mathfrak{n}$ se tiene $\left(\frac{\mathfrak{p}}{\mathfrak{n}}\right)_{\mathcal{K}} = \left(\frac{\mathfrak{n}}{\mathfrak{p}}\right)$. Para esto notemos que si $\mathfrak{q}$ es un

[****]En lo que sigue usaremos indistintamente los términos carácter cuadrático con carácter de Dirichlet cuadrático.

primo impar, entonces, por relación 3 del símbolo de Kronecker y por reciprocidad cuadrática, $\left(\frac{p}{q}\right)_{\mathcal{K}} = \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Además, $\left(\frac{p}{2}\right)_{\mathcal{K}} = (-1)^{p^2-1/8} = \left(\frac{2}{p}\right)$, y $\left(\frac{p}{-1}\right)_{\mathcal{K}} = 1 = \left(\frac{-1}{p}\right)$. Así, dado que estas dos funciones coinciden para todos los primos y en -1, y además ambas son totalmente multiplicativas, se sigue que $\left(\frac{p}{n}\right)_{\mathcal{K}} = 1 = \left(\frac{n}{p}\right)$, para cada entero n.

Supongamos que p es un número primo tal que $p \equiv 3 \pmod 4$, demostraremos que para cada entero n se tiene $\left(\frac{-p}{n}\right)_{\mathcal{K}} = \left(\frac{n}{p}\right)$. Para esto notemos que si q es un primo impar, entonces, por relación 3 del símbolo de Kronecker y por reciprocidad cuadrática, $\left(\frac{-p}{q}\right)_{\mathcal{K}} = \left(\frac{-p}{q}\right) = \left(\frac{q}{p}\right)$. Además, $\left(\frac{-p}{2}\right)_{\mathcal{K}} = (-1)^{(-p)^2-1/8} = (-1)^{p^2-1/8} = \left(\frac{2}{p}\right)$, y $\left(\frac{-p}{-1}\right)_{\mathcal{K}} = -1 = \left(\frac{-1}{p}\right)$. Así, dado que estas dos funciones coinciden para todos los primos y en -1, y además ambas son totalmente multiplicativas, se sigue que $\left(\frac{-p}{n}\right)_{\mathcal{K}} = 1 = \left(\frac{n}{p}\right)$, para cada entero n.

Ahora, supongamos que d_1 y d_2 son discriminantes cuadráticos con $(d_1, d_2) = 1$. Pongamos $d = d_1 d_2$. Supongamos que $\left(\frac{d_i}{q}\right)_{\mathcal{K}}$ es un carácter cuadrático primitivo módulo $|d_i|$ para $i = 1, 2$, demostraremos que $\left(\frac{d}{q}\right)_{\mathcal{K}}$ es un carácter cuadrático primitivo módulo $|d|$. Si q es un primo impar, entonces, por relación 3 del símbolo de Kronecker, $\left(\frac{d}{q}\right)_{\mathcal{K}} = \left(\frac{d}{q}\right) = \left(\frac{d_1}{p}\right)\left(\frac{d_2}{p}\right) = \left(\frac{d_1}{q}\right)_{\mathcal{K}}\left(\frac{d_2}{q}\right)_{\mathcal{K}}$. Además, por relación 2 del símbolo de Kronecker, tenemos que $\left(\frac{d}{2}\right)_{\mathcal{K}} = \left(\frac{d_1}{2}\right)_{\mathcal{K}}\left(\frac{d_2}{2}\right)_{\mathcal{K}}$, y por relación 4 del símbolo de Kronecker, tenemos que $\left(\frac{d}{-1}\right)_{\mathcal{K}} = \left(\frac{d_1}{-1}\right)_{\mathcal{K}}\left(\frac{d_2}{-1}\right)_{\mathcal{K}}$. Dado que $\left(\frac{d}{n}\right)_{\mathcal{K}} = \left(\frac{d_1}{n}\right)_{\mathcal{K}}\left(\frac{d_2}{n}\right)_{\mathcal{K}}$, cuando n es un número primo o $n = -1$, por multiplicidad de esta función, se sigue que esta propiedad se mantiene para todos los enteros n. Por tanto, por Lema 1.2, $\left(\frac{d}{n}\right)_{\mathcal{K}}$ es un carácter cuadrático primitivo módulo $|\, d \,|$. ❏

Notemos que los discriminantes de cuerpos cuadráticos de la forma $K = \mathbb{Q}(\sqrt{d})$ cumplen las relaciones que definen a los discriminantes cuadraticos, así,

podemos asociar a un cuerpo cuadrático un cáracter cuadrático. En lo que sigue, denotaremos por χ_K al cáracter cuadrático asociado al discriminante de $K = \mathbb{Q}(\sqrt{d})$.

DEFINICIÓN 1.8. *Diremos que un carácter tiene periodo* $k \in \mathbb{Z}_{\geqslant 0}$*, si y sólo si,* $\chi(n) = \chi(n+k)$*, para cada entero* n*.*

PROPOSICIÓN 1.2. *Sea* K *un cuerpo de números cuadrático con discriminante* d_K*. Entonces el carácter cuadrático* χ_K *tiene periodo* $|\, d_K \,|$*.*

Una observación que cabe destacar es el hecho que

$$\chi_K(-1+ \mid d_K \mid \mathbb{Z}) = \begin{cases} 1 & \text{si } K \text{ es cuadrático real,} \\ -1 & \text{si } K \text{ es cuadrático imaginario.} \end{cases}$$

Lo cual resulta del teorema anterior. En general, un carácter de Dirichlet que lleva -1 en 1 es llamado par, y un carácter de Dirichlet que lleva -1 en -1 es llamado impar. Así, el carácter de un cuerpo cuadrático real es par y el carácter de un cuerpo cuadrático imaginario es impar.

EJEMPLO 2. *Sea* $K = \mathbb{Q}(\sqrt{-3})$*, donde* $\mathcal{O}_K = \mathbb{Z}(\zeta_3)$[*****]*, el carácter cuadrático de Dirichlet viene dado por*

$$\chi_K : (\mathbb{Z}/3\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times, \;\; \chi_K(m) = \left(\frac{m}{3}\right)_{\mathcal{K}}.$$

2. Series de Dirichlet

En esta sección revisaremos algunos resultados generales de las series de Dirichlet.

DEFINICIÓN 1.9. *Una* ***serie de Dirichlet*** *es una expresión de la forma,*

$$f(s, a_n) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

donde $s \in \mathbb{C}$ *y* $\{a_n\}_{n \geqslant 0}$ *es una sucesión de números complejos.*

[*****]Donde ζ_3 es el grupo de raices 3-ésimas de la unidad.

TEOREMA 1.5 (Sumas de Abel). *Sean* $\{a_n\}_{n\geqslant 0}$ *y* $\{b_n\}_{n\geqslant 0}$ *dos sucesiones de números complejos. Entonces*

$$\sum_{n=m}^{N} a_n(b_n - b_{n-1}) = a_N b_N - a_m b_m - \sum_{n=m}^{N} b_{n-1}(a_n - a_{n-1}).$$

Demostración. Dadas las sucesiones $\{a_n\}_{n\geqslant 0}$ y $\{b_n\}_{n\geqslant 0}$, tenemos

$$\begin{aligned}\sum_{n=m}^{N} a_n b_n &= a_N b_N - a_m b_m + \sum_{n=m}^{N} a_{n-1} b_{n-1} \\ &= a_N b_N - a_m b_m - \sum_{n=m}^{N} b_{n-1} a_n + \sum_{n=m}^{N} a_{n-1} b_{n-1} + \sum_{n=m}^{N} b_{n-1} a_n \\ &= a_N b_N - a_m b_m - \sum_{n=m}^{N} b_{n-1}(a_n - a_{n-1}) + \sum_{n=m}^{N} b_{n-1} a_n.\end{aligned}$$

Reagrupando los términos obtenemos el resultado deseado.

❏

Si denotamos como $A_{l,m} := \sum_{n=l}^{m} a_n$ y $B_{m,m'} := \sum_{n=m}^{m'} b_n$ el Teorema de las sumas de Abel puede ser escrito como

$$B_{m,m'} = \sum_{m}^{m'-1} A_{m,n}(b_n - b_{n+1}) + A_{m,m'} b_{m'}.$$

LEMA 1.6. *Sean* $\alpha, \beta \in \mathbb{R}$ *tales que* $0 < \alpha < \beta$, *y* $z = x + iy \in \mathbb{C}$ *con* $Re(z) > 0$. *Entonces*

$$|e^{-\alpha z} - e^{\beta z}| \leqslant \left|\frac{z}{x}\right| (e^{-\alpha Re(z)} - e^{\beta Re(z)}).$$

Demostración.

Escribiendo

$$e^{-\alpha z} - e^{\beta z} = z \int_{\alpha}^{\beta} e^{-tz} dt,$$

tenemos

$$|e^{-\alpha z} - e^{\beta z}| \leqslant |z| \int_{\alpha}^{\beta} e^{-tz} dt = \frac{|z|}{x}(e^{-\alpha Re(z)} - e^{\beta Re(z)}).$$

❏

PROPOSICIÓN 1.3. *Sea* $f(s_0, a_n)$ *una serie de Dirichlet convergente. Entonces* $f(s, a_n)$ *converge uniformente para cada* $s \in \mathbb{C}$*, con* $Re(s) > Re(s_0)$*.*

Demostración.

Sin pérdida de generalidad podemos dejar fuera el término a_1 y así asumir que $a_1 = 0$ y además supongamos $s_0 = 0$ (pues podemos mirar la serie de Dirichlet $\sum_{n=0}^{\infty}(a_n n^{-s_0})n^{-s_0})$. Así, la serie $\sum_{n=1}^{\infty} a_n$ converge. Luego, para cada $\epsilon > 0$, existe un entero positivo N tal que si $l, m > N$, $\mid A_{l,m} \mid < \epsilon$. Por el Teorema de las sumas de Abel, tenemos,

$$\left|\sum_{n=l}^{m} \frac{a_n}{n^s}\right| = \left|A_{l,m}b_m - \sum_{n=l}^{m} A_{l,m}((n+1)n^{-s})\right| < \epsilon\left(1 + \sum_{n=l}^{m}\left|e^{-s\log n} - e^{-s\log(n+1)}\right|\right).$$

Aplicando el Lema 1.6, vemos que

$$\begin{aligned}\left|\sum_{n=l}^{m} \frac{a_n}{n^s}\right| &< \epsilon\left(1 + M\sum_{n=l}^{m} e^{-\mathrm{Re}(s)\log n} - e^{-\mathrm{Re}(s)\log(n+1)}\right)\\ &= \epsilon\left|1 + M(e^{-\mathrm{Re}(s)\log l}) - e^{-\mathrm{Re}(s)\log m}\right|\\ &< \epsilon(1+M).\end{aligned}$$

Donde $M = |s|/|\mathrm{Re}(s)|$. Así, para un N lo suficientemente grande, esto tiende a cero independientemente de s, por lo que la serie converge uniformemente en esta región. De esta manera concluye la demostración.

❏

COROLARIO 1.1. *El conjunto de convergencia de la serie de Dirichlet* $f(s, a_n)$ *contiene un semiplano abierto maximal, el cual llamaremos* ***semiplano de convergencia****.*

PROPOSICIÓN 1.4. *Sea* $f(s, a_n) = 0$ *en algún semiplano* $Re(s) > \sigma_0$*. Entonces,* $a_n = 0$*, para cada* $n \geqslant 0$*.*

Demostración.

Sin pérdida de generalidad, consideremos $a_n n^{-\sigma_0}$, con $\sigma_0 = 0$. Así, con el fin de tener que $f(s, a_n)$ converja a $s = 0$, debemos tener $a_n = O(1)$. Supongamos que existe $N \in \mathbb{N}$ tal que a_N es el primer término no nulo, entonces,

$$0 = a_N N^{-s} \left(1 + \sum_{n>N} \frac{a_n}{a_N} \left(\frac{n}{N} \right)^{-s} \right)$$

así, al multiplicar la expresión por N^s tenemos

$$0 = a_N \left(1 + \sum_{n>N} \frac{a_n}{a_N} \left(\frac{n}{N} \right)^{-s} \right)$$

Haciendo $s \longrightarrow +\infty + 0i$, tenemos $a_N = 0$, lo cual es una contradicción. De esta manera culmina la demostración.

❏

Corolario 1.2. *Sean* $f(s, a_n), f(s, b_n)$ *dos series de Dirichlet, tales que* $f(s, a_n) = f(s, b_n)$ *para cada Re*$(s) > \sigma_0$*. Entonces,* $a_n = b_n$ *para cada* $n \geqslant 0$*.*

Proposición 1.5. *Sean* $f(s, a_n)$, $f(s, b_n)$ *dos series de Dirichlet. Entonces*

$$f(s, a_n) f(s, b_n) = f(s, \sum_{d|n} a_d b_{n/d}).$$

Demostración.

Por definición sabemos que,

$$f(s, a_n) f(s, b_n) = \sum_{m=1}^{\infty} \sum_{l=1}^{\infty} \frac{a_m b_l}{(ml)^s}.$$

Haciendo la sustitución $n = ml$ y $d = m$, al simplificar tenemos,

$$f(s, a_n) f(s, b_n) = \sum_{n=1}^{\infty} \sum_{d|n} \frac{a_d b_{\frac{n}{d}}}{n^s} = f(s, \sum_{d|n} a_d b_{n/d}).$$

❏

2.1. Productos de Euler.

DEFINICIÓN 1.10. *Sean* n, m *dos enteros positivos relativamente primos y* $\{a_n\}_{n\geqslant 0}$ *una sucesión de números complejos. Diremos que* $\{a_n\}_{n\geqslant 0}$ *es multiplicativa si y sólo si,* $a_n a_m = a_{nm}$. *Similarmente, diremos que* $\{a_n\}_{n\geqslant 0}$ *es estrictamente multiplicativa si y sólo si,* $a_n a_m = a_{nm}$ *para cada par de enteros positivos.*

LEMA 1.7. *Sean* $\{a_n\}_{n\geqslant 0}$ *una sucesión multiplicativa acotada y* P *el conjunto de números primos. Entonces, la serie de Dirichlet* $f(s, a_n)$ *converge absolutamente para* $Re(s) > 1$, *y tiene como factorización*

$$f(s, a_n) = \prod_{p\in P}(1 + a_p p^{-s} + ... + a_{p^m} p^{-ms} + ...).$$

Demostración.

Como la sucesión $\{a_n\}_{n\geqslant 0}$ es una serie acotada y $\mathrm{Re}(s) > 1$[******], se sigue que la serie es absolutamente convergente. Ahora, sean S un conjunto finito de números primos y $N(S)$ el conjunto de enteros mayores que 1 que son factores primos pertenecientes a S. Así, considerando los factores primos, tenemos,

$$\sum_{n\in N(S)} \frac{a_n}{n^s} = \prod_{p\in S} \sum_{m=0}^{\infty} \frac{a_{p^m}}{p^{-ms}}.$$

Notemos que cuando S aumenta el lado izquierdo de la igualdad converge a $\sum_{n=1}^{\infty} a_n n^{-s}$. De esto tenemos que el producto infinito converge y es igual a $f(s, a_n)$. De esta mánera culmina la demostración.

❏

LEMA 1.8. *Sean* $\{a_n\}_{n\geqslant 0}$ *una sucesión estrictamente multiplicativa y* P *el conjunto de números primos. Entonces,*

$$f(s, a_n) = \prod_{p\in P} \frac{1}{1 - \frac{a_p}{p^s}}.$$

[******]Para detalles ver [**9**].

Demostración.

Dado que $\{a_n\}_{n\geqslant 0}$ es una sucesión estrictamente multiplicativa, tenemos $a_{p^m} = a_p^m$. Así, usando el Lema anterior se obtiene la Proposición.

❏

Con esto, si consideramos la sucesión constante igual a 1, definimos la **función zeta de Riemann** por

$$\zeta(s) = f(s, 1).$$

Así, por Lema anterior tenemos

$$\zeta(s) = \prod_{p\in P} \frac{1}{1 - \frac{1}{p^s}}.$$

A continuación, enunciaremos algunas propiedades importantes de la funcion zeta de Riemann. Para más detalles ver [**9**].

PROPOSICIÓN 1.6. *La función zeta es holomorfa no nula en el semiplano* $Re(s) > 1$.

Demostración.

Ver sección 3, cap. VI de Serre [**9**].

❏

PROPOSICIÓN 1.7.

$$\zeta(s) = \frac{1}{s-1} + \phi(s),$$

donde $\phi(s)$ *es una función holomorfa para* $Re(s) > 0$.

Demostración.

Ver sección 3, cap. VI de Serre [**9**].

❏

COROLARIO 1.3. *La función zeta tiene un polo singular en* $s = 1$.

3. Funciones L de Dirichlet

DEFINICIÓN 1.11. *Sea* χ *un carácter de Dirichlet (módulo* m*). Definimos la* ***función*** L ***de Dirichlet*** *asociada al carácter* χ *como*

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

donde $s \in \mathbb{C}$.

PROPOSICIÓN 1.8. *Sea* χ *un cáracter de Dirichlet no trivial (módulo* m*). Entonces* $L(s,\chi)$ *converge si* $Re(s) > 0$.

Demostración.

Por Proposición 1.1, sabemos que $\sum_{n=0}^{\infty} \chi(n)$ es acotada. Así, $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converge para cada s positivo. Por Proposición 1.3 la Proposición queda demostrada.

❏

Ahora, dado que los caracteres de Dirichlet son estrictamente multiplicativos, tenemos la factorización

$$L(s,\chi) = \prod_{p \in P} \frac{1}{1 - \frac{\chi(p)}{p^s}},$$

la cual se conoce como el **factor de Euler** de la función L.

En lo que sigue revisaremos las principales caracteristicas de la función Gamma, las cuales darán lugar a definiciones y propiedades fundamentales para demostrar que la función L de Dirichlet admite continuidad análitica en todo el plano complejo $\mathbb{C}$ y satisface la ecuación funcional que definiremos al final de esta sección.

DEFINICIÓN 1.12. *Sea* $s \in \mathbb{C}$ *con* $Re(s) > 0$. *Definimos la* ***función Gamma*** *como la integral absolutamente convergente*

$$\Gamma(s) = \int_0^{\infty} e^{-y} y^{s-1} dy.$$

PROPOSICIÓN 1.9. 1. *La función Gamma es análitica y admite una continuidad meromórfica en cada punto de* $\mathbb{C}$.

2. *La función Gamma sólo tiene polos simples en* $s = -n$, $n = 0, 1, 2, ...$ *con residuo* $\dfrac{(-1)^n}{n!}$.
3. *La función Gamma satisface las ecuaciones funcionales*
   a) $\Gamma(s+1) = s\Gamma(s)$,
   b) $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$,
   c) $\Gamma(s)\Gamma(s+\frac{1}{2}) = \frac{2\sqrt{\pi}}{2^{2s}}\Gamma(2s)$.
4. *La función Gamma toma los valores* $\Gamma(1/2) = \sqrt{\pi}$, $\Gamma(1) = 1$ *y* $\Gamma(k+1) = k!$ *para* $k = 0,\ 1, ...$

Demostración. Ver capítulo I de [**12**]. ❏

DEFINICIÓN 1.13. *Dado* $z \in \mathbb{C}$, *definimos la* ***serie Theta de Jacobi*** *como*

$$\theta(z) = \sum_{n\in\mathbb{Z}} e^{-\pi i n^2 z} = 1 + 2\sum_{n=1}^{\infty} e^{-\pi i n^2 z}.$$

Uno de nuestros objetivos en esta sección es demostrar que la función L de Dirichlet, admite una continuidad análitica en todo el plano complejo, y además satisface la ecuación funcional que definiremos al final de esta sección. La demostración dependerá de una representación integral de la función $L(s, \chi)$, la cual se realiza como una transformada de una serie Theta. Para esto, distingamos los casos par e impar en un cáracter de Dirichlet χ (módulo m).

DEFINICIÓN 1.14. *Definimos el* ***exponente*** $p \in [0, 1]$ *del carácter* χ *como el número que hace posible esta igualdad,*

$$\chi(-1) = (-1)^p \chi(1).$$

Consideremos la función Gamma asociada a χ

$$\Gamma(s, \chi) := \Gamma\left(\frac{s+p}{2}\right) = \int_0^{\infty} e^{-y} y^{(s+p)/2-1} dy.$$

Al sustituir $y \mapsto \pi n^2 y/m$, obtenemos

$$\left(\frac{m}{\pi}\right)^{\frac{s+p}{2}} \Gamma(s,\chi)\frac{1}{n^s} = \int_0^\infty n^p e^{-\pi n^2 y/m} y^{(s+p)/2-1} dy.$$

Si multiplicamos esta igualdad por $\chi(n)$, sumando sobre todos los $n \in \mathbb{N}$, tenemos

$$\left(\frac{m}{\pi}\right)^{\frac{s+p}{2}} \Gamma(s,\chi)L(s,\chi) = \int_0^\infty \sum_{n=1}^{\infty} n^p e^{-\pi n^2 y/m} y^{((s+p)/2)-1} dy. \tag{1.1}$$

Aquí, al intercambiar el orden de la serie y la integral, tenemos

$$\sum_{n=1}^{\infty}\int_0^\infty |n^p e^{-\pi n^2 y/m} y^{(s+p)/2-1}| dy \leqslant \left(\frac{m}{\pi}\right)^{\frac{\mathrm{Re}(s)+p}{2}} \Gamma\left(\frac{\mathrm{Re}(s)+p}{2}\right) \zeta\big(\mathrm{Re}(s)\big) < \infty.$$

Ahora, considerando la serie de la integral, tenemos

$$g(y) = \sum_{n=1}^{\infty} \chi(n) n^p e^{-\pi n^2 y/m},$$

surge de la serie Theta

$$\theta(z,\chi) = \sum_{n\in\mathbb{Z}} \chi(n) n^p e^{-\pi n^2 y/m}.$$

Dado que $\chi(n)n^p = \chi(-n)(-n)^p$ implica que

$$\theta(z,\chi) = \chi(0) + 2\sum_{n=1}^{\infty} \chi(n) n^p e^{-\pi n^2 y/m},$$

de modo que $g(y) = \dfrac{1}{2}(\theta(iy,\chi) - \chi(0))$ con $\chi(0) = 1$, si χ es el cáracter trivial, y $\chi(0) = 0$ en otro caso. Cuando $m = 1$, esta es la función Theta de Jacobi

$$\theta(z) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 z},$$

la cual se asocia con la función Zeta de Riemann. Vemos que el factor

$$L_\infty(s,\chi) := \left(\frac{m}{\pi}\right)^{\frac{s}{2}} \Gamma(s,\chi)$$

en 1.1 es el factor de Euler en infinitos primos. Así, uniendo a los factores de Euler $L_p(s) := \dfrac{1}{1-\chi(p)p^{-1}}$ de la factorización de $L(s,\chi)$, se da origen a la **función L de Dirichlet completada** de el cáracter χ:

$$\Lambda(s,\chi) := L_\infty(s,\chi)L(s,\chi).$$

Así, para esta función, 1.1 nos da

PROPOSICIÓN 1.10. *La función $\Lambda(s,\chi)$ admite la representación integral*

$$\Lambda(s,\chi) = \frac{c(\chi)}{2}\int_0^\infty \big(\theta(iy,\chi)-\chi(0)\big)y^{((s+p)/2)-1}dy$$

donde $c(\chi) = \left(\dfrac{m}{\pi}\right)^{\frac{p}{2}}$.

Notemos que los factores en la suma de las funciones L corren sólo en los números naturales, mientras que en las series Theta estos corren en todos los números enteros. Esta es la razón por la cual los factores n^p fueron incluidos a fin de vincular la función L con la serie Theta.

DEFINICIÓN 1.15. *Sea $f : \mathbb{R}_+^\times \longrightarrow \mathbb{C}$ una función continua. Definimos la* ***transformación de Mellin*** *como la integral impropia*

$$L(s,f) = \int_0^\infty \big(f(y)-f(\infty)\big)y^{s-1}dy,$$

donde $f(\infty) = \lim\limits_{y\to\infty} f(y)$ y la integral existen.

TEOREMA 1.9 (Principio de Mellin). *Sean $f, g : \mathbb{R}_+^\times \longrightarrow \mathbb{C}$ funciones continuas tales que*

$$f(y) = a_0 + O\left(e^{-cy^\alpha}\right), \quad g(y) = b_0 + O\left(e^{-cy^\alpha}\right),$$

para $y \longrightarrow \infty$, con c, α constantes positivas. Si estas funciones satisfacen la ecuación

$$f\left(\frac{1}{y}\right) = Cy^k g(y),$$

para algún número real $k > 0$ y algún número complejo $C \neq 0$, entonces,

1. *Las integrales* $L(s,f)$ *y* $L(s,g)$ *convergen absolutamente y uniformemente si* s *varia en un dominio compacto contenido en* $\{s \in \mathbb{C} : Re(s) > k\}$ *y por tanto son funciones holomorfas en* $\{s \in \mathbb{C} : Re(s) > k\}$. *Además, admiten continuidad holomórfica en* $\mathbb{C} \setminus \{0, k\}$.
2. *Satisfacen la ecuación funcional*

$$L(s,f) = CL(k-s,g).$$

Demostración.

Ver Teorema 1.4, cap. VII de [**11**].

❏

En lo que sigue, aplicaremos el principio de Mellin a la representación integral anterior. Demostraremos que la serie Theta $\theta(iy,\chi)$ satisface una transformación, como se asume en el Teorema 1.11. Para esto usaremos el siguiente Lema

LEMA 1.10. *Sean* a, b, μ *números reales, con* $\mu > 0$. *Entonces la serie*

$$\theta_\mu(a,b,z) = \sum_{g \in \mu\mathbb{Z}} e^{\pi i(a+g)^2 z + 2\pi i b g}$$

converge absolutamente y uniformemente en el dominio $Im(z) \geqslant \delta$, *para cada* $\delta > 0$, *y cada* $z \in \mathbb{H} = \{z \in \mathbb{C}\,;\, Im(z) > 0\}$, *y además tenemos la transformación*

$$\theta_\mu(a,b,-1/z) = e^{-2\pi i a b}\frac{\sqrt{z/i}}{\mu}\theta_{1/\mu}(-b,a,z).$$

Idea de la Demostración. Para demostrar la convergencia absoluta y uniforme la idea es acotar $\sum_{g\in\mu\mathbb{Z}} e^{\pi i(a+g)^2 z + 2\pi i b g}$ en una sucesión de compactos que cubren $\mathbb{H}$. Así también, la idea de la demostración de la transformación se basa en usar la fórmula para la suma de Poisson

$$\sum_{g\in\mu\mathbb{Z}} f(g) = \frac{1}{\mu}\sum_{g'\in 1/\mu\mathbb{Z}} \widehat{f}(g'),$$

para una determinada transformada de Fourier de una función de Shawartz f. Para más detalles ver principio sección 3, cap. VII de [**11**].

❏

Tenemos que la función $\theta_\mu(a, b, z)$ es uniformemente convergente en las variables a, b. Derivando p veces ($p = 0, 1$) en la variable a, obtenemos las función

$$\theta_\mu^p(a, b, z) = \sum_{g \in \mu\mathbb{Z}} (a + g)^p e^{\pi i(a+g)^2 + 2\pi i b g}.$$

Lo que implica que

$$\frac{d^p}{da^p}\theta_\mu(a, b, z) = (2\pi i)^p z^p \theta_\mu^p(a, b, z)$$

y

$$\frac{d^p}{da^p} e^{-2\pi i a b}\theta_{1/\mu}(-b, a, z) = (2\pi i)^p e^{-2\pi i a b}\theta_{1/\mu}^p(-b, a, z).$$

Al aplicar la derivada d^p/da^p a la transformación 1.4 se obtiene el siguiente corolario

Corolario 1.4. *Si* a, b, μ *números reales, con* $\mu > 0$, *tenemos la transformación*

$$\theta_\mu^p(a, b, -1/z) = \left(i^p e^{2\pi i a b}\mu\right)^{-1} \left(\frac{z}{i}\right)^{p+\frac{1}{2}} \theta_{1/\mu}^p(-b, a, z).$$

Definición 1.16. *Sea* $n \in \mathbb{Z}$, *llamaremos* ***suma de Gauss*** $\tau(n, \chi)$ ***asociada al cáracter de Dirichlet*** χ *(módulo* m*) como el número complejo*

$$\tau(n, \chi) = \sum_{\nu=0}^{m-1} \chi(\nu) e^{2\pi i \nu n/m}.$$

Si $n = 1$, *escribiremos* $\tau(\chi) = \tau(1, \chi)$.

Proposición 1.11. *Sea* χ *un cáracter de Dirichlet (módulo* m*). Entonces*

$$\tau(n, \chi) = \overline{\chi}(n)\tau(\chi) \quad y \quad |\tau(\chi)| = \sqrt{m}.$$

Demostración.

Para el primer caso, si $(n, m) = 1$ se sigue de $\chi(\nu n) = \chi(n)\chi(\nu)$. Si $d = (n, m) \neq 1$, ambos lados de la igualdad son cero. En efecto, como χ es un carácter primitivo, podemos escoger un $a \equiv 1 \pmod{m/d}$ tal que $a \not\equiv 1 \pmod{m}$ y $\chi(a) \neq 1$. Al multiplicar $\tau(n, \chi)$ por $\chi(a)$, como $e^{2\pi i \nu a n/m} = e^{2\pi i \nu n/m}$, tenemos $\chi(a)\tau(n, \chi) = \tau(n, \chi)$, y por tanto $\tau(n, \chi) = 0$.

Por otro lado, tenemos

$$\begin{aligned} |\tau(\chi)|^2 &= \tau(\chi)\overline{\tau(\chi)} = \tau(\chi) \sum_{\nu=0}^{m-1} \overline{\chi(\nu)} e^{-2\pi i \nu/m} = \sum_{\nu=0}^{m-1} \tau(\nu, \chi) e^{-2\pi i \nu/m} \\ &= \sum_{\nu=0}^{m-1} \sum_{\mu=0}^{m-1} \chi(u) e^{2\pi i \nu \mu/m} e^{2\pi i \nu/m} = \sum_{\mu=0}^{m-1} \chi(\mu) \sum_{\nu=0}^{m-1} e^{2\pi i \nu(\mu-1)/m}. \end{aligned}$$

Si $\mu = 1$ la última suma es igual a m. Para $\mu \neq 1$, $\xi = e^{2\pi i \nu(\mu-1)/m}$ es una m-raiz de la unidad distinta de 1, por tanto una raiz del polinomio

$$\frac{x^m - 1}{x - 1} = x^{m-1} + \cdots x + 1.$$

Por lo tanto $|\tau(\chi)|^2 = m\chi(1) = m$. De esta manera concluye la demostración.

❏

El siguiente resultado es referente a las series Theta $\theta(z, \chi)$.

Proposición 1.12. *Sea χ un cáracter de Dirichlet (módulo m). Entonces, tenemos la siguiente transformación*

$$\theta(-1/z, \chi) = \frac{\tau(\chi)}{i^p \sqrt{m}} \left(\frac{z}{i}\right)^{p+\frac{1}{2}} \theta(z, \overline{\chi}).$$

Demostración.

Tenemos

$$\theta(z, \chi) = \sum_{n \in \mathbb{Z}} \chi(n) n^p e^{\pi i n^2 z/m} = \sum_{a=0}^{m-1} \chi(a) \sum_{n \in \mathbb{Z}} (a + g)^p e^{\pi i (a+g)^2 z/m},$$

y así

$$\theta(z,\chi) = \sum_{a=0}^{m-1} \chi(a)\theta_m^p(a,0,z/m).$$

Por corolario 1.4, tenemos

$$\theta_m^p(a,0,-1/mz) = \frac{1}{i^p m}\left(\frac{mz}{i}\right)^{p+\frac{1}{2}} \theta_{1/m}^p(0,a,mz),$$

y esto nos da

$$\theta_{1/m}^p(0,a,mz) = \sum_{g\in\frac{1}{m}\mathbb{Z}} g^p e^{\pi i g^2 mz + 2\pi i a g} = \frac{1}{m^p}\sum_{n\in\mathbb{Z}} e^{2\pi i a n/m} n^p e^{\pi i n^2 z/m}.$$

Si multiplicamos esto por $\chi(a)$, entonces, al sumar sobre a, y dado que $\tau(n,\chi) = \overline{\chi}(n)\tau(\chi)$, hemos encontrado

$$\begin{aligned}
\theta(-1/z,\chi) &= \frac{1}{i^p m}\left(\frac{mz}{i}\right)^{p+\frac{1}{2}} \sum_{a=0}^{m-1} \chi(a)\theta_{1/m}^p(0,a,mz) \\
&= \frac{1}{i^p m^{p+1}}\left(\frac{mz}{i}\right)^{p+\frac{1}{2}} \sum_{n\in\mathbb{Z}} \left(\sum_{a=0}^{m-1} \chi(a) e^{2\pi i a n/m}\right) n^p e^{\pi i n^2 z/m} \\
&= \frac{1}{i^p\sqrt{m}}\left(\frac{z}{i}\right)^{p+\frac{1}{2}} \tau(\chi) \sum_{n\in\mathbb{Z}} \overline{\chi}(n) n^p e^{\pi i n^2 z/m} \\
&= \frac{\tau(\chi)}{i^p\sqrt{m}}\left(\frac{z}{i}\right)^{p+\frac{1}{2}} \theta(z,\chi).
\end{aligned}$$

❏

La continuidad análitica y la ecuación funcional para la función $\Lambda(s,\chi)$ se deducen rapidamente como se verá en el siguiente Teorema.

TEOREMA 1.11. *Sea χ un cáracter primitivo de Dirichlet no trivial. Entonces, la función* L *de Dirichlet completada $\Lambda(s,\chi)$ admite continuidad análitica en todo el plano complejo $\mathbb{C}$ y satisface la ecuación funcional*

$$\Lambda(s,\chi) = W(\chi)\Lambda(1-s,\overline{\chi})$$

donde el factor $W(\chi) = \dfrac{\tau(\chi)}{i^p\sqrt{m}}$ *tiene módulo 1.*

Demostración.

Sean $f(y) = \dfrac{c(x)}{2}\theta(iy,\chi)$, $g(y) = \dfrac{c(x)}{2}\theta(iy,\overline{\chi})$ y $c(x) = \left(\frac{\pi}{m}\right)^{p/2}$. Como $\chi(0) = \overline{\chi}$, tenemos

$$\theta(iy,\chi) = 2\sum_{n=1}^{\infty}\chi(n)n^p e^{-\pi n^2 y/m},$$

y por tanto $f(y) = O(e^{-\pi y/m})$, e igualmente $g(y) = O(e^{-\pi y/m})$. Ahora, por 1.10, tenemos

$$\Lambda(s,\chi) = \frac{c(x)}{2}\int_0^{\infty}\theta(iy,\chi)y^{\frac{s+p}{2}-1}dy.$$

Por lo tanto, obtenemos $\Lambda(s,\chi)$ y $\Lambda(s,\overline{\chi})$ como transformaciones de Mellin

$$\Lambda(s,\chi) = L(s',f) \quad \text{y} \quad \Lambda(s,\overline{\chi}) = L(s',g)$$

de las funciones $f(y)$ y $g(y)$ en el punto $s' = \dfrac{s+p}{2}$. Por la transformación 1.12 tenemos

$$f\left(\frac{1}{y}\right) = \frac{c(x)}{2}\theta(-1/iy,\chi) = \frac{c(x)\tau(\chi)}{2i^p\sqrt{m}}y^{p+\frac{1}{2}}\theta(iy,\overline{\chi}) = \frac{c(x)\tau(\chi)}{2i^p\sqrt{m}}y^{p+\frac{1}{2}}g(y).$$

Al aplicar Teorema 1.11, tenemos que $\Lambda(s,\chi)$ admite una continuidad analítica en la todo el plano complejo $\mathbb{C}$ y satisface la ecuación

$$\begin{aligned}\Lambda(s,\chi) &= L(\frac{s+p}{2},f) = W(\chi)L(p+\frac{1}{2}-\frac{s+p}{2},g) = W(\chi)L(\frac{1-s+p}{2},g)\\ &= W(\chi)\Lambda(1-s,\overline{\chi})\end{aligned}$$

con $W(\chi) = \dfrac{\tau(\chi)}{i^p\sqrt{m}}$. Ahora, al aplicar 1.11, tenemos $|W(\chi)| = 1$. Con esto concluye la demostración.

❏

Capítulo 2

Fórmula del Número de Clases de Dirichlet

El objetivo de este capítulo es obtener una fórmula para el número de clases de cuerpos cuadráticos imaginarios en términos de valores especiales de funciones L de Dirichlet.

1. Reticulados Complejos

Definición 2.1. *Un **reticulado complejo** es un subgrupo abeliano Λ de $\mathbb{C}$ de rango 2, es decir*

$$\Lambda = \lambda_1\mathbb{Z} \oplus \lambda_2\mathbb{Z}, \quad \lambda_1, \lambda_2 \in \mathbb{C}^\times, \ \lambda_1/\lambda_2 \notin \mathbb{R}.$$

Una base de Λ es un conjunto $\{\lambda_1, \lambda_2\}$, el cual determina completamente el reticulado*. Adoptaremos la convención que la base $\{\lambda_1, \lambda_2\}$ es ordenada y que además $\mathrm{Im}(\lambda_1/\lambda_2) > 0$.

Proposición 2.1. *Los conjuntos ordenados de números complejos no nulos $\{\lambda_1, \lambda_2\}$ y $\{\lambda_1', \lambda_2'\}$ son bases de un reticulado Λ, si y sólo si,*

$$\begin{pmatrix}\lambda_1'\\ \lambda_2'\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} \text{ para algún } \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}).$$

Demostración.
Ver cap. 10 de [**7**].

❏

Un **paralelogramo** en un reticulado Λ es un conjunto de la forma

$$\mathfrak{p}(\lambda_1, \lambda_2) = \{t_1\lambda_1' + t_2\lambda_2' : t_1, t_2 \in [0, 1]\}.$$

*Es decir, cada elemento de Λ queda determinado por los elementos del conjunto

Dado $\Lambda = \langle \lambda_1, \lambda_2 \rangle$ entonces el área del paralelogramo depende sólo de Λ, no del cambio de base. Esto es debido a que si $\{\lambda_1, \lambda_2\}$ y $\{\lambda_1', \lambda_2'\}$ son bases de un reticulado Λ, la aplicación lineal de la Proposición precedente que envia λ_i en λ_i' para $i = 1, 2$, preserva el aréa pues su determinante es 1.

2. Función L de Dirichlet de un Cuerpo Cuadrático

Recordemos que el carácter de un cuerpo cuadrático K, está determinado por el discriminante de K y el símbolo de Kronecker.

DEFINICIÓN 2.2. *Sean* K *un cuerpo cuadrático con discriminante* d_K *y denotaremos por* P *el conjunto de números primos. La* ***función*** L ***de Dirichlet cuadrática*** *de* K *está dada por*

$$L(s, \chi_K) = \sum_{n=1}^{\infty} \frac{\chi_K(n)}{n^s}.$$

En lo que sigue usaremos indistintamente los términos función L de Dirichlet cuadrática con función L cuadrática. Esta Proposición es una de las principales propiedades de las funciones L cuadráticas.

PROPOSICIÓN 2.2. *La función* L *cuadrática* $L(s, \chi_K)$ *es analítica en* $Re(s) > 0$.

Demostración.

Por Proposición 1.2, $\chi_K(n)$ depende sólo de n (mod $|d_K|$). Así, para cada $n_0 \in \mathbb{Z}_+$ tenemos,

$$\sum_{n=n_0}^{n_0+|d_K|-1} \chi_K(n) = 0,$$

ya que estamos sumando el carácter no trivial χ_K sobre el grupo $(\mathbb{Z}/|d_K|\mathbb{Z})^\times$. Por tanto, para cada $n \geqslant 1$,

$$\left| \sum_{k=1}^{n} \chi_K(k) \right| < C.$$

Así, por Proposición 1.3 tenemos que $L(s, \chi_K)$ es análitica si $\mathrm{Re}(s) > 0$, con lo cual concluye la demostración.

❏

El siguiente resultado nos proporciona un valor especial para funciones L cuadráticas.

PROPOSICIÓN 2.3. *Sea* K *un cuerpo cuadrático real. Entonces*

$$L(1, \chi_K) = -\frac{1}{\sqrt{|d_K|}} \sum_{r=1}^{|d_K|-1} \chi_K(r) \log(\sin(\pi r/|d_K|)).$$

Si K *es un cuerpo cuadrático imaginario, entonces*

$$L(1, \chi_K) = -\frac{\pi}{\sqrt{|d_K|^3}} \sum_{r=1}^{|d_K|-1} \chi_K(r) r.$$

3. Función Zeta de Dedekind

DEFINICIÓN 2.3. *Sea* K *un cuerpo de números. Llamaremos* ***función Zeta de Dedekind*** *de* K *a la expresión*

$$\zeta_K(s) = \sum_{\mathcal{A} \in \mathcal{O}_K} \frac{1}{N(\mathcal{A})^s}.$$

donde $N(\mathcal{A})$ *es la norma absoluta del ideal* $\mathcal{A}$[**].

En lo que sigue consideraremos funciones Zeta de Dedekind definidas sobre cuerpos cuadráticos.

La función Zeta de Dedekind se puede escribir como la serie de Dirichlet

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \quad a_n = \left|\left\{\mathcal{A} : N(\mathcal{A}) = n\right\}\right|.$$

Asi, para análizar la función $\zeta_K(s)$ necesitamos definir

[**]Definida en el Apéndice A

$$A_n := \sum_{k=1}^{n} a_k = \left|\left\{\mathcal{A} \,:\, N(\mathcal{A}) \leqslant n\right\}\right|, \quad n \geqslant 1,$$

y estimar $|A_n|$. Para llevar a cabo esta estimación, definimos para cada clase de ideales $\mathcal{C}$ de K

$$A_n(\mathcal{C}) = \left|\left\{\mathcal{A} \in \mathcal{C}\,;\, N_K(\mathcal{A}) \leqslant n\right\}\right|, \quad n \geqslant 1,$$

Así, $A_n = \sum_{\mathcal{C}} A_n(\mathcal{C})$. El problema de estimar cada $A_n(\mathcal{C})$ puede ser reducido al problema de estimar el número de las clases de ideales, el cual se puede abordar estimando el número de puntos de un reticulado de un disco, los siguientes resultados nos proporcionaran elementos que serán fundamentales para estos fines.

LEMA 2.1. *Sean K un cuerpo cuadrático imaginario con discriminante d_K, el ideal $\mathcal{A} = (c, -d + \sqrt{n})$, con c, $d \in K$, y α el área del paralelogramo generado por c y $-d + \sqrt{n}$. Entonces*

$$\frac{N_K(\mathcal{A})}{\alpha} = \frac{2}{\sqrt{|d_K|}}.$$

Demostración.

Ver cap. 10 de [7].

❏

LEMA 2.2. *Sea Λ un reticulado complejo, y denotemos α el área de uno de sus paralelogramos fundamentales*

$$p(\lambda_1, \lambda_2) = \left\{t_1\lambda_1' + t_2\lambda_2' \,:\, t_1,\, t_2 \in [0,1]\right\}.$$

Para cada $r > 0$, sea B_r la bola cerrada cerrada con centro en 0 de radio r. Entonces, existe una constante positiva C tal que

$$\left|\left|\{(\Lambda \setminus 0) \cap B_r\}\right| - \frac{\pi r^2}{\alpha}\right| \leqslant Cr, \qquad \textit{para cada } r \geqslant 1.$$

Demostración.

Fijemos un paralelogramo fundamental $\mathfrak{p}$, y para cada $\lambda \in \mathbb{C}$, denotemos por $\mathfrak{p}_\lambda$ la traslación en λ de $\mathfrak{p}$. Ahora, para cada $r \geqslant 0$, sea

$$\begin{aligned} n_1(r) &= \big|\lambda \in \Lambda : \mathfrak{p}_\lambda \subset B_r\big| \\ n_2(r) &= \big|\lambda \in \Lambda : \mathfrak{p}_\lambda \cap B_r \neq \emptyset\big|. \end{aligned}$$

Entonces

$$n_1(r) \leqslant |\Lambda \cap B_r| \leqslant n_2(r).$$

Sea $\delta > 0$ la mayor longitud de la diagonal de $\mathfrak{p}$, entonces, para cada $r \geqslant \delta$,

$$\pi(r-\delta)^2 \leqslant n_1(r)\alpha \leqslant \pi r^2 \leqslant n_2(r)\alpha \leqslant \pi(r+\delta)^2,$$

así, al dividir por α nos da

$$\frac{\pi(r-\delta)^2}{\alpha} \leqslant n_1(r) \leqslant \frac{\pi r^2}{\alpha} \leqslant n_2(r) \leqslant \frac{\pi(r+\delta)^2}{\alpha}.$$

Por tanto, $|\Lambda \cap B_r|$, $\pi r^2/\alpha \in [\pi(r+\delta)^2/\alpha, \pi(r+\delta)^2/\alpha]$.

Consecuentemente, el módulo de su diferencia es a lo más la longitud del intervalo,

$$\left||\Lambda \cap B_r| - \frac{\pi r^2}{\alpha}\right| \leqslant \left(\frac{4\pi\delta}{\alpha}\right) r, \quad \text{para cada } \ r \geqslant \delta.$$

La función $f(r) = \left||\Lambda \cap B_r| - \frac{\pi r^2}{\alpha}\right| / r$ es acotada en $[1, \delta]$, y así

$$\left||\Lambda \cap B_r| - \frac{\pi r^2}{\alpha}\right| \leqslant Cr, \quad \text{para cada } \ r \geqslant 1.$$

Por último, excluyendo 0 de $\Lambda \cap B_r$ cambia el lado izquierdo como máximo r, con $r \geqslant 1$. De esta manera, se concluye la demostración.

❏

Proposición 2.4. *Sean K un cuerpo cuadrático imaginario con discriminante d_K, w el número de raices de la unidad en K y h_K el número de clases de ideales de K. Entonces*

$$\left| A_n - \frac{2\pi h_K n}{w\sqrt{|d_k|}} \right| < C\sqrt{n}, \quad n \geqslant 1.$$

Demostración.

Sean $\mathcal{C}$ una clase de ideales de K, y $\mathcal{A}_o \in C^{-1}$ un ideal integral*** en la clase inversa de $\mathcal{C}$. Entonces, la correspondencia dada por

$$\mathcal{B} \longmapsto \mathcal{A}_o\mathcal{B}$$

define una biyección en los ideales fraccionarios de K. En particular, podemos restringir a la biyección de dos conjuntos de ideales integrales,

$$\{\mathcal{A} \in \mathcal{C} : N_K(\mathcal{A}) \leqslant n\} \longrightarrow \{\mathcal{A}' \in \mathcal{C} : \mathcal{A} \text{ es principal }, \mathcal{A}_o/\mathcal{A}', N_K(\mathcal{A}) \leqslant n \cdot N_K(\mathcal{A}_o)\}$$

equivalentemente,

$$\{\mathcal{A} \in \mathcal{C} : N_K(\mathcal{A} \leqslant n\} \longrightarrow \{(x) \subset \mathcal{A}_o : x \neq 0, |x| \leqslant \sqrt{n \cdot N_K(\mathcal{A}_o)}\}.$$

Al igual que en la discusión que conduce al Lema 2.2, definimos

$$A_n(\mathcal{C}) = \left|\{\mathcal{A} \in \mathcal{C} : N_K(\mathcal{A}) \leqslant n\}\right|, \quad n \geqslant 1.$$

Como los elementos asociados generan el mismo ideal, y dado que todas las unidades de $\mathcal{O}_K$ son raices de la unidad, pues K es un cuerpo imaginario cuadrático, la biyección del conjunto previo nos da

$$A_n(\mathcal{C}) = \frac{\left|\left((\mathcal{A}_o \setminus 0) \cap B_{\sqrt{n \cdot N_K(\mathcal{A}_o)}}\right)\right|}{w}. \tag{2.1}$$

Ahora, al tomar $\mathcal{A}_o = (c, -d + \sqrt{m})$ como en el Lema 2.1, y denotar como α_o el área de el paralelogramo generado por c y $-d + \sqrt{m}$. Por 2.1 , Lema 2.1 y Lema 2.2,

$$\left| A_n(\mathcal{C}) - \frac{2\pi n}{w\sqrt{|d_K|}} \right| = \frac{1}{w}\left| \left|\left((\mathcal{A}_o \setminus 0) \cap B_{\sqrt{n \cdot N_K(\mathcal{A}_o)}}\right)\right| - \frac{\pi n N_K(\mathcal{A}_o)}{\alpha_o} \right| < C\sqrt{n}.$$

***Definido en el Apéndice A.

La constante C depende de la clase de ideales $\mathcal{C}$. Finalmente, dado que

$$A_n = \sum_{\mathcal{C} \in Cl_K} A_n(\mathcal{C}), \quad n \geqslant 1,$$

suma sobre las clases de ideales, al usar desigualdad triangular, tenemos

$$\left| A_n - \frac{2\pi h_K n}{w\sqrt{|d_k|}} \right| \leqslant C\sqrt{n},$$

donde ahora la constante C no depende de la clase de ideales que se tome. De esta manera concluye la demostración.

❏

La siguiente Proposición nos muestra algunas de las principales propiedades de la función Zeta de Dedekind.

PROPOSICIÓN 2.5. *Sea* K *un cuerpo cuadrático imaginario. Entonces, la función Zeta de Dedekind* $\zeta_K(s)$ *es análitica si* $Re(s) > 1$. *Además, la función Zeta de Dedekind de* K *es el producto de la función Zeta de Riemann y la función* L *cuadrática de* K,

$$\zeta_K(s) = \zeta(s)L(s, \chi_K), \quad Re(s) > 1.$$

La función $\zeta_K(s)$ *se extiende meromorficamente al semiplano* $\{s > 0\}$, *y la extensión tiene sólo un polo simple en* $s = 1$ *con residuo* $L(1, \chi_K)$. *Esto es*

$$\zeta_K(s) = \frac{L(s, \chi_K)}{s-1} + \psi(s), \quad Re(s) > 0$$

donde ψ *es análitica. Por tanto*

$$\lim_{s \to 1}(s-1)\zeta_K(s) = L(1, \chi_K).$$

Demostración.

Por Proposición 2.4, tenemos

$$|A_n| - \frac{2\pi h_K n}{w\sqrt{|d_k|}} \leqslant \left| A_n - \frac{2\pi h_K n}{w\sqrt{|d_k|}} \right| \leqslant C\sqrt{n},$$

de modo que $|A_n| \leqslant C\sqrt{n}$. La función $\zeta_K(s)$ es análitica si $\mathrm{Re}(s) > 1$ por Proposición 1.3.

Ahora, como

$$\left\{\begin{array}{rcl} \zeta_K(s) & = & \displaystyle\prod_{p\in P}\prod_{p|p\mathcal{O}_K}(1-N_K(p)^s)^{-1} \\ \zeta(s)L(s,\chi) & = & \displaystyle\prod_{p\in P}(1-p^{-s})^{-1}(1-\chi(p)p^{-s})^{-1} \end{array}\right\}, \qquad \mathrm{Re}(s) > 1,$$

basta demostrar que para cada primo p racional,

$$\prod_{p|p\mathcal{O}_K}(1-N_K(p)^s)^{-1} = (1-p^{-s})^{-1}(1-\chi(p)p^{-s})^{-1}.$$

Por Proposición A.4, tenemos,

1. si $\chi_K(p) = 1$ entonces ambas partes son $(1-p^{-s})^2$.
2. si $\chi_K(p) = -1$ entonces ambas partes son $(1-p^{-2s})$.
3. si $\chi_K(p) = 0$ entonces ambas partes son $(1-p^{-s})$.

Por último, como $\zeta_K(s) = \zeta(s)L(s,\chi)$ la continuidad meromorfa de $\zeta_K(s)$ sigue de las propiedades de ζ y $L(s,\chi_K)$ para $\mathrm{Re}(s) > 1$. De esta manera concluye la demostración.

❏

4. Fórmula del Número de Clases

En esta sección utilizaremos la fuerza de la Proposición 2.4 para obtener una fórmula para el número de clases para cuerpos cuadráticos imaginarios. Si

$$a_n = \left|\left\{\mathcal{A} : N(\mathcal{A}) = n\right\}\right| \text{ y } A_n := \sum_{k=1}^{n} a_k, \quad n \geqslant 1,$$

entonces

$$\left|A_n - \frac{2\pi h_K n}{w\sqrt{|d_k|}}\right| < C\sqrt{n}, \quad n \geqslant 1.$$

Ahora, sea

$$a'_n = a_n - \frac{2\pi h_K n}{w\sqrt{|d_K|}}, \quad n \geqslant 1,$$

así, su suma parcial viene dada por

$$A'_n = A_n - \frac{2\pi h_K n}{w\sqrt{|d_K|}}, \quad n \geqslant 1.$$

Por tanto, $|A'_n| \leqslant C\sqrt{n}$, para cada $n \geqslant 1$, y así por Proposición 1.3, tenemos que la serie de Dirichlet

$$f(s, a'_n) = \sum_{n=1}^{\infty} \frac{a'_n}{n^s} = \zeta_K(s) - \frac{2\pi h}{w\sqrt{|d_K|}}\zeta(s)$$

es análitica si $\mathrm{Re}(s) > 1/2$, en particular es análitica en $s = 1$. Como

$$\zeta_K(s) \sim \frac{L(1, \chi_K)}{s-1} \text{ y } \zeta(s) \sim \frac{1}{s-1},$$

tenemos que

$$L(1, \chi_K) = \frac{2\pi h_K}{w\sqrt{|d_K|}}.$$

En resumen, la estimación de la Proposición 2.4 nos muestra que el número de clases de ideales de K se manifiesta en el residuo de la función Zeta de Dedekind $\zeta_K(s)$ en $s = 1$. Por Proposición 2.5, el residuo es $L(1, \chi_K)$, y así la Proposición 2.3 nos da la siguiente fórmula.

TEOREMA 2.3 (Fórmula de número de clases de cuerpos cuadráticos imaginarios de Dirichlet). *Sean* K *un cuerpo cuadrático imaginario con discriminante* d_K, w *el número de raices de la unidad en* K, h_K *el número de clases de ideales de* K *y* $L(s, \chi_K)$ *la función* L *cuadrática de* K. *Entonces*

$$\boxed{\frac{2\pi h_K}{w\sqrt{|d_K|}} \quad = \quad L(1, \chi_K).}$$

Para ver la relevancia de este Teorema veamos el siguiente Ejemplo.

Ejemplo 3. *Consideremos* $\mathsf{K} = \mathbb{Q}(\sqrt{-5})$*, cuyo discriminante es* $\mathsf{d}_{\mathsf{K}} = -20$*. Así, el cáracter cuadrático viene dado por*

$$\chi_{\mathsf{K}} : (\mathbb{Z}/20\mathbb{Z})^{\times} \longrightarrow \{\pm 1\}, \quad \chi_{\mathsf{K}}(\mathsf{t}) = \begin{cases} 1 & \text{si } \mathsf{t} \equiv 1, 3, 7, 9, \\ -1 & \text{si } \mathsf{t} \equiv 11, 13, 17, 19, \end{cases}$$

y

$$\mathsf{L}(1, \chi_{\mathsf{K}}) = -\frac{\pi}{|20|^{3/2}}(1 + 3 + 7 + 9 - 11 - 13 - 17 - 19).$$

Por tanto el número de clases de ideales es

$$\mathsf{h}_{\mathsf{K}} = \frac{w\sqrt{|\mathsf{D}_{\mathsf{K}}|}}{2\pi}\mathsf{L}(1, \chi_{\mathsf{K}}) = -\frac{2\sqrt{20}}{2\pi} \cdot \frac{\pi}{20^{3/2}}(-40),$$

y así el número de clases de ideales de $\mathbb{Q}(\sqrt{-5})$ *es 2.*

Existen múltiples fórmulas para el número de clases de cuerpos cuadráticos imaginarios, otro resultado de esto viene dado por el siguiente Teorema

Teorema 2.4. *Sean* K *un cuerpo cuadrático imaginario con discriminante* $\mathsf{d}_{\mathsf{K}} < -4$ *y* χ *su carácter asociado. Entonces tenemos la siguiente fórmula:*

$$\mathsf{h}_{\mathsf{K}} = \frac{1}{2 - \chi(2)} \sum_{0 < \mathsf{x} < |\mathsf{d}_{\mathsf{K}}|/2, (\mathsf{x}, \mathsf{d}_{\mathsf{K}}) = 1} \chi(\mathsf{x})$$

Demostración. Ver sección 4, capítulo 5 de [**3**]. ❑

Si aplicamos este Teorema al caso del cuerpo $\mathsf{K} = \mathbb{Q}(\sqrt{\mathsf{d}})$ con d primo de la forma $4\mathfrak{n} + 3$, como $-\mathsf{d} \equiv 1 \pmod 4$, en este caso $\mathsf{d}_{\mathsf{K}} = -\mathsf{d}$ y el valor del carácter $\chi(\mathsf{x})$ coincide con el símbolo de Legendre. Así, el número de sumandos en $\sum_{0<\mathsf{x}<\mathsf{d}/2}$ es impar ($(\mathsf{d}-1)/2 = 2\mathfrak{n}+1$). Además, $\chi(2) = 1$ si $\mathsf{d} \equiv 7 \pmod 8$ y $\chi(2) = -1$ si $\mathsf{d} \equiv 3 \pmod 8$. Con esto, obtenemos el siguiente Corolario

Corolario 2.1. *Si* d *es un número primo de la forma* $4\mathfrak{n} + 3$*, entonces el cuerpo* $\mathbb{Q}(\sqrt{-\mathsf{d}})$ *tiene número de clases impar.*

Capítulo 3

Formas Cuadráticas, Teoría de Géneros y Formas Lineales en Logaritmos

El objetivo de este capítulo es hacer un estudio de las relaciones que existen entre las formas cuadráticas, teoría de géneros y el problema del número de clases de Gauss, en específico estableceremos un nexo directo entre cierto conjunto de formas cuadráticas y el grupo de clases. Terminaremos enunciando un resultado de Baker el cual será clave para dar solución al caso del número de clases 2.

1. Formas Cuadráticas Binarias

A continuación revisaremos algunos conceptos básicos de formas cuadráticas binarias, para una revisión exhaustiva de las demostraciones recomendamos consultar [**7**].

Definición 3.1. *Una* ***forma cuadrática binaria*** *es un polinomio* $f(x,y) = ax^2+bxy+cy^2$*, con* a, b, $c \in \mathbb{Z}$ *no todos nulos. Diremos que una forma cuadrática binaria* $f(x,y)$ *es* ***primitiva*** *si* a, b, c *son relativamente primos.*

En lo que sigue usaremos indistintamente los términos formas cuadráticas binarias y formas cuadráticas.

Definición 3.2. *Diremos que dos formas cuadráticas* $f(x,y)$ *y* $g(x,y)$ *son* ***equivalentes*** *si* $f(x,y) = g(px + qy, rx + sy)$*, donde* p, q, r, $s \in \mathbb{Z}$ *y* $ps - qr = \pm 1$*. Por otro lado, diremos que las formas son* ***equivalentes propias*** *si* $ps - qr = 1$ *y son* ***equivalentes impropias*** *si* $ps - qr = -1$*.*

DEFINICIÓN 3.3. *Definimos el* ***determinante*** *de una forma cuadrática binaria* $f(x, y) = ax^2 + bxy + cy^2$ *como el número* $ac - b^2/4$. *Ademas, definimos el* ***discriminante*** *de* $f(x, y)$ *como el entero* $b^2 - 4ac$.

DEFINICIÓN 3.4. *Diremos que una forma cuadrática binaria* $f(x, y)$ *es* ***completa****, si y sólo si su discriminante no es un cuadrado perfecto.*

DEFINICIÓN 3.5. *Diremos que el entero* m *es* ***representado*** *por una forma cuadrática* $f(x, y)$*, si existen* x, $y \in \mathbb{Z}$ *tales que* $f(x, y) = m$. *Si tales* x, y *son relativamente primos, entonces diremos que* m *es* ***representado adecuadamente*** *en* $f(x, y)$.

Se puede demostrar que el determinante y el discriminante de una forma cuadrática binaria $f(x, y)$ son invariantes por equivalencia. Por otro lado, el signo del discriminante de una forma cuadrática tiene gran relevancia, en efecto, si consideramos la forma cuadrática $f(x, y) = ax^2 + bxy + cy^2$ con discriminante d, tenemos la identidad

$$4af(x, y) = (2ax + by)^2 - dy^2.$$

Si $d > 0$, entonces $f(x, y)$ representa enteros positivos y negativos, en este caso diremos que la forma es **indefinida**, si $d < 0$, entonces la forma representa sólo enteros positivos o sólo negativos, dependiendo del signo del coeficiente a, con éste caso diremos que $f(x, y)$ es **definida positiva** o **definida negativa** según sea el signo de a.

DEFINICIÓN 3.6. *Diremos que una forma reducida positiva* $f(x, y) = ax^2 + bx + cy^2$ *es* ***reducida*** *si*

$$|b| \leqslant a \leqslant c, \text{ y } b \geqslant 0 \text{ si } b = a \text{ o } a = c.$$

TEOREMA 3.1. *Una forma primitiva definida positiva es propiamente equivalente a una uńica forma reducida.*

DEFINICIÓN 3.7. *Diremos que dos formas cuadráticas están en la misma* ***clase*** *si ellas son propiamente equivalentes. Denotaremos por* $h(d)$ *el número de clases de las formas cuadráticas primitivas definidas positivas con discriminante* d.

LEMA 3.2. *Sean* $f(x,y) = ax^2 + bxy + cy^2$ *y* $f(x,y) = a'x^2 + b'xy + c'y^2$ *formas cuadráticas con discriminantes* d *tales que mcd*$(a, a', \frac{(b+b')}{2}) = 1$. *Entonces existe un único entero* B *módulo* $2aa'$ *tal que*

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

DEFINICIÓN 3.8. *Sean* $f(x,y) = ax^2+bxy+cy^2$ *y* $f(x,y) = a'x^2+b'xy+c'y^2$ *formas cuadráticas primitivas definidas positivas con discriminantes* $d < 0$ *tales que mcd*$(a, a', \frac{(b+b')}{2}) = 1$. *Definimos la* ***composición de Dirichlet*** *de* $f(x,y)$ *y* $g(x,y)$ *como*

$$F(x,y) = aa'x^2 + Bxy + \frac{B^2 - d}{4aa'}y^2,$$

donde B *es el entero determinado por el Lema 3.2.*

TEOREMA 3.3. *Sean* $d \equiv 0,\ 1 \pmod 4$ *un negativo, y* $C(d)$ *el conjunto de las clases de formas cuadráticas primitivas definidas positivas de discriminante* d. *Entonces la composión de Dirichlet induce una operación bien definida en* $C(d)$.

COROLARIO 3.1. *El conjunto* $C(d)$ *con la composición de Dirichlet es un grupo abeliano finito de orden* $h(d)$.

TEOREMA 3.4. *Sean* $f(x,y) = ax^2+bxy+cy^2$ *una forma cuadrática primitiva definida positiva de discriminante* $d < 0$ *y* $K = \mathbb{Q}(\sqrt{d})$. *Entonces, la aplicación*

$$f(x,y) \longmapsto (a, \frac{-b + \sqrt{d}}{2}),$$

define un isomorfismo entre $C(d)$ *y* Cl_K[*].

[*]Para una revisión acabada del conjunto Cl_K ver Apéndice A.

DEFINICIÓN 3.9. *Para un entero negativo* $d \equiv 0 \pmod 4$*, definimos la* ***forma principal del discriminante*** d *como* $x^2 - \frac{d}{4}y^2$.

2. Elementos de Teoría de Géneros

En esta sección revisaremos algunos aspectos básicos de la teoría de géneros de formas cuadráticas binarias, las demostraciones pueden ser consultadas en el capítulo VII de [**13**].

LEMA 3.5. *Sea* $d = 4n$*, para algún entero* n*. Entonces existe* $\chi : (\mathbb{Z}/d\mathbb{Z})^\times \to \{\pm 1\}$ *tal que* $\chi(p) = \left(\frac{d}{p}\right)$ *para cada primo* p *que no divide a* d.

LEMA 3.6. *Sean* $d = 4n$*, para algún entero* n *y* $f(x, y)$ *una forma cuadrática que representa un entero* m*. Entonces,* m *puede ser escrito como* d^2m'*, donde* $f(x, y)$ *representa adecuadamente a* m'.

LEMA 3.7. *Para cada forma primitiva* $f(x, y) = ax^2+bxy+cy^2$*, y cada entero* m*,* $f(x, y)$ *representa adecuadamente un número infinito de enteros relativamente primos con* m.

LEMA 3.8. *Sean* $d = -4n$*, para algún entero positivo* n*, y cada forma primitiva* $f(x, y)$ *con discriminante* d*. Entonces*

1. *Los valores en* $(\mathbb{Z}/\mathbb{Z}d)^\times$ *representados por la forma principal del discriminante* d *forman un subgrupo* H *de* $\ker(\chi)$.
2. *Los valores en* $(\mathbb{Z}/\mathbb{Z}d)^\times$ *representados por* $f(x, y)$ *forman una coclase de* H *en* $\ker(\chi)$.

DEFINICIÓN 3.10. *Sean* $d = -4n$*, para algún entero positivo* n*, y* H *el subgrupo mencionado en el Lema 3.8. Para cada coclase* H' *de* H*, definimos el* ***género*** *de* H'*, como el conjunto de todas las formas cuadráticas con discriminante* d *que representan* H' *módulo* d*. El género que contiene la clase de la identidad es llamado* ***género principal***.

TEOREMA 3.9. *Sean* $d = -4n$*, para algún entero positivo* n*, y* H *el subgrupo mencionado en el Lema 3.8. Si* H' *es una coclase de* H *en* $\ker(\chi)$ *y* p *un primo impar que no divide a* d*, entonces,* p *es representado por una forma reducida de discriminante* d *en el genéro de* H'*, si y sólo si,* $\langle p \rangle \in H'$*.*

3. Formas Lineales en Logaritmos de Números Algebraicos

En esta sección revisaremos algunas propiedades de las alturas de números algebraicos y algunos aspectos básicos de la teoría de formas lineales en logaritmos de números algebraicos. Para una revisión mas acabada recomendamos ver [**16**] y [**21**].

DEFINICIÓN 3.11. *Sea* $f(x) \in \mathbb{C}[x]$ *un polinomio no nulo. Se define la* ***medida de Mahler*** *de* $f(x)$ *como*

$$M(f) = \exp\left(\frac{1}{2\pi}\int_0^{2\pi} \log|f(e^{i\theta})|d\theta\right),$$

donde la integral es absolutamente convergente.

DEFINICIÓN 3.12. *Sea* α *un número algebraico, definimos su* ***altura*** *(de Weil) como*

$$h(\alpha) = \frac{1}{\deg \alpha} \log M(g_\alpha),$$

donde g_α *es el polinomio minimal de* α*.*

Sean α, α', α'', β, β', β'' números algebraicos con grado a lo más d. Supongamos que $|\alpha'| \neq 1$ y sea $\alpha'' = -1$. Sea A la altura de α, A' la altura de α', con A a lo más 2 y las alturas de β, β', β'' a lo más $H^{(\log H)^2}$, con $H > 0$. Supongamos además que $\log\alpha$, $\log\alpha'$, $\log\alpha''$[**] y son linealmente independientes sobre los racionales, esto da lugar al siguiente Teorema.

[**]Donde estamos considerando su rama principal. Recordar que la función compleja $\log z$ es una función multivaluada y su valor principal o rama principal se define como $\log|z| + i\theta$ donde $\theta \in [-\pi, \pi]$.

TEOREMA 3.10. *Sean* $\varepsilon > 0$, $\delta > 0$ *y*

$$|\beta \log \alpha + \beta' \log \alpha' + \beta'' \log \alpha''| < e^{-\delta H}.$$

Entonces $H < C(\log A)^{1+\varepsilon}$, *donde* $C = C(A', d, \varepsilon, \delta)$ *es efectivamente calculable.*

Demostración. Ver Sección 3 de [**23**]. ❏

Capítulo 4

Cuerpos Cuadráticos Imaginarios con Número de Clases 2

1. Introducción

En lo que sigue demostraremos un Teorema de 1971 debido a A. Baker el cual da solución al problema del número de clases 2. Para esto usaremos en primer lugar un resultado de Baker relacionado con formas lineales en logaritmos de números algebraicos.

Consideremos p, q primos tales que $p \equiv 1 \pmod 4$, $q \equiv 3 \pmod 4$ y supongamos que el cuerpo cuadrático $\mathbb{Q}(\sqrt{-pq})$ tiene número de clases 2. Denotaremos por d_k el discriminante de $\mathbb{Q}(\sqrt{k})$, con $k > 4$ y $\chi(n) = \left(\frac{|d_k|}{n}\right)_{\mathcal{K}}$ el cáracter cuadrático asociado a este cuerpo. Supongamos además que $(k, pq) = 1$ y consideremos la forma cuadrática de discriminante pq,

$$f = f(x, y) = x^2 + xy + \frac{1}{4}(1 + pq)y^2. \tag{4.1}$$

Teorema 4.1. *Tenemos*

$$\frac{d_k\sqrt{pq}}{2\pi} \sum_{x\in\mathbb{Z}} \sum_{y\in\mathbb{Z}} \frac{\chi(f)}{f} = h(k)h(-kpq)\log\varepsilon + h(kp)h(-kq)\log\eta, \quad (x, y) \neq (0, 0)$$

donde $h(l)$ *denota el número de clases de* $\mathbb{Q}(\sqrt{l})$*,* ε*,* η *denotan las unidades fundamentales de los cuerpos* $\mathbb{Q}(\sqrt{k})$*,* $\mathbb{Q}(\sqrt{kp})$ *respectivamente.*

Idea de la Demostración. En lo que sigue usaremos las siguientes notaciones $\chi(F) = \chi(F(x, y))$, $\chi_{pq}(n) = (-pq/n)$, $\chi_p(n) = (p/n)$, $\chi_q(n) = (-q/n)$ y $\chi'(n)$ denotará uno de los caracteres primitivos asociados al discriminante $-pq$. De los resultados anunciados por Baker en [**24**], tenemos

$$L(1, \chi)L(1, \chi\chi_{pq}) + L(1, \chi\chi_p)L(1, \chi\chi_q) = \frac{1}{2} \sum_{F} \sum_{x\in\mathbb{Z}} \sum_{y\in\mathbb{Z}} (\chi(F) + \chi\chi'(F))(F(x, y))^{-1}, \tag{4.2}$$

con $(x, y) \neq (0, 0)$, y F corriendo sobre las formas cuadráticas no equivalentes con discriminante $-pq$. Tomaremos f como en 4.1. Podemos ver que f está en el género principal, y f, f' están en géneros distintos; para los géneros impares y por tanto $h(-pq)$ de otro modo sería al menos 4. Además, la teoría de géneros de caracteres muestra que $\chi'(F) = 1$ si F está en el género principal y -1 en otro caso, es decir, tenemos $\chi'(f) = 1$, $\chi'(f') = -1$ para cada x, y. Por tanto, el lado derecho de 4.2 esta dado por

$$\sum_{x\in\mathbb{Z}} \sum_{y\in\mathbb{Z}} \chi(f) f^{-1}, \quad (x, y) \neq (0, 0).$$

Pero por otro lado, de Dirichlet se tiene que

$$L(1, \chi) = 2h(k) \log \varepsilon/\sqrt{k}, \quad L(1, \chi\chi_{pq}) = 2h(-kpq)\pi/\sqrt{kpq},$$

$$L(1, \chi\chi_p) = 2h(kp) \log \eta/\sqrt{kp}, \quad L(1, \chi) = 2h(-kq)\pi/\sqrt{kq},$$

y así el Teorema sigue. Para mayores detalles de la demostración consultar [**23**]. ❏

2. Teorema de Baker

TEOREMA 4.2 (Baker, 1971). *Los cuerpos cuadráticos imaginarios con número de clases 2 pueden ser efectivamente determinados.*

Demostración. Desde los resultados anunciados en [**22**] tenemos que d es un entero positivo libre de cuadrados con $d \not\equiv 3 \pmod 8$ y $h(-d) = 2$, entonces $d < 10^{500}$. Por tanto es suficiente asumir que $d \equiv 3 \pmod 8$ y $h(-d) = 2$.

Si d fuera algún primo, entonces por Corolario 2.1, $h(-d)$ sería impar.

Por otro lado, notemos que el discriminante de $\mathbb{Q}(\sqrt{-d})$ es de la forma $-4d$, luego si d es divisible por t primos impares, tenemos que $Cl_{\mathbb{Q}(\sqrt{-d})}$ tiene exactamente 2^{t-1} elementos de orden menor o igual a 2, entonces el $h(-d) > 2^{t-1}$*, así, si d es producto de t primos entonces $h(-d)$ sería mayor o igual a 4.

*Para detalles ver Proposición 3.11 y Teorema 7.7 de [**7**].

Por lo tanto, podemos asumir que $d = pq$, donde p, q son definidos como en la sección 1 de este capítulo. Podemos asumir $q > d^{1/4}$ y que $d > c$ para un número c calculable y suficientemente grande. El caso cuando $q \leqslant d^{1/4}$ puede ser tratado con los argumentos de [**22**], en efecto, por cálculo tenemos que los cuerpos cudráticos imaginarios en este caso vienen dados por $d = 123$ y $d = 267$[**].

Denotaremos por c_1, c_2, ... las Constantes absolutas que pueden ser calculadas explicitamente. Al considerar f como en 4.1 y las notaciones del Teorema 4.1, vemos desde los resultados de [**22**] que

$$\frac{k\sqrt{d}}{2\pi}\sum_{x\in\mathbb{Z}}\sum_{y\in\mathbb{Z}}\frac{\chi(f)}{f} = \frac{1}{6}\pi k\sqrt{d}\prod_{p|k}(1-p^{-2}) + B_0 + \sum_{r\in\mathbb{Z}^\times} B_r e^{\pi i r/k}, \quad (x,y)\neq(0,0),$$

donde $B_0 = -2\log p$ si k es potencia de un primo p, $B_0 = 0$ en otro caso y

$$B_r = 2e^{-z|r|\sqrt{d}/k}\sum_{y|r,\, y>0} y^{-1}\sum_{j=1}^{k}\chi(f(j,y))e^{2\pi i j r/yk}.$$

Así, siguiendo los argumentos de [**22**], tomando $k = 21$, pues $h(k) = 1$ y $\varepsilon = \left(\frac{1}{2}\right)(5+\sqrt{21})$, se tiene que

$$|\sum_{r\in\mathbb{Z}^\times} B_r e^{\pi i r/21}| \leqslant 4\cdot 21\xi(1-\xi)^{-2},$$

donde $\xi = e^{-\pi\sqrt{d}/21}$. Cuando d es grande tenemos $\xi < \frac{1}{2}$ y el número en la derecha es a lo más $e^{-\left(\frac{1}{10}\right)\sqrt{d}}$.

Así, con los argumentos de [**22**] y el Teorema 4.1 obtenemos

$$\left|h(-21d)\log\varepsilon + h(21p)h(-21q)\log\eta - \frac{64}{21}\pi\sqrt{d}\right| < e^{-\left(\frac{1}{10}\right)\sqrt{d}}$$

Esta es una desigualdad de la forma considerada en el Teorema 3.10 con $\alpha = \eta^{h(21p)}$, $\alpha' = \varepsilon$, $\beta = h(-21q)$, $\beta' = h(-21d)$, $\beta'' = \left(\frac{64}{21}\right)\sqrt{-d}$. Considerando las notaciones del esbozo de la demostracion del Teorema 4.1, tenemos

$$L(1,\chi\chi_p) = 2h(21p)\log\eta/\sqrt{21p},$$

[**]Para detalles recomendamos consultar pag. 425-426 de [**3**].

tiene valor absoluto a lo más $c_1 \log(21p)$ (por los argumentos del Capítulo 14 de [**18**]).

Con esto se puede ver que $\alpha \leqslant p^{c_2\sqrt{p}}$, y como además el conjugado de η es menor que 1, sigue que la altura de α es a lo más $A = p^{c_3\sqrt{p}}$. Además, vemos que la altura A' de α' es 5, y apelando nuevamente al esbozo de la demostración del Teorema 4.1 tenemos que las alturas de β, β', β'' son a lo más $H^{(\log H)^2}$, donde $H = \sqrt{d}^{***}$.

Así, aplicando el Teorema 3.10 con $d = 2$, $\delta = 1/10$ y cualquier $\varepsilon > 0$, concluimos que

$$\sqrt{d} < C(\sqrt{p}\log p)^{1+\varepsilon},$$

donde $C = C(\varepsilon)$ es efectivamente calculable. Pero nuestra suposición $q > d^{1/4}$ junto con $d = pq$ nos da $p < d^{3/4}$, y la desigualdad es claramente inconsistente si $\varepsilon < 1/3$. Esta contradicción establece el Teorema.

❏

3. Conclusiones

En 1971 A. Baker, junto con otros autores, lográn sintetizar de manera independiente elementos avanzados de la teoría algebraica de números junto con fórmulas explicitas propias de los métodos analíticos de la teoria de números, y así resolver un caso particular de un problema clásico formulado por Gauss en 1801, sentando las bases para una futura solución total del problema.

Por otro lado, de los resultados desarrollados por Baker en dichas investigaciones, surge el concepto de forma lineal en logaritmos de números algebraicos, el cual, es actualmente una fuerte herramienta usada, por ejemplo, para resolver problemas de estimaciones en ecuaciones diofanticas.

Con esto podemos ver como distintas lineas de investigación en teoría de números lográn confluir para desarrollar resultados relevantes en múltiples aspectos de las

***Para detalles ver sección 5 de [**23**].

matemáticas, y así dar solución y abrir nuevas interrogantes respecto a problemas clásicos o contemporaneos dentro de las ciencias exactas.

Apéndice A

Tópicos de Teoría Algebraica de Números

En lo que sigue K denotara una extensión finita sobre $\mathbb{Q}$ a la cual llamaremos cuerpo de números y $\mathcal{O}_{\mathsf{K}}$ el anillo de enteros sobre K, es decir, el conjunto de todos los $\alpha \in \mathsf{K}$ que son raices de un polinomio mónico con coeficientes enteros.

1. Factorización Única de Ideales

A continuación revisaremos algunos aspectos básicos de la teoría algebraica de números, incluyendo dominios de Dedekind, factorización de ideales y ramificación. Las demostraciones serán omitidas, sin embargo daremos referencias de éstas. Para un tratamiento completo de estos temas recomendamos consultar Borevich y Shaferevich [**3**], Lang [**4**] o Marcus [**6**].

La estructura básica del anillo de enteros $\mathcal{O}_{\mathsf{K}}$ es dada en la siguiente Proposición:

Proposición A.1. *Sea* K *un cuerpo de números.*

1. $\mathcal{O}_{\mathsf{K}}$ *es un subanillo de* $\mathbb{C}$ *cuyo cuerpo de fracciones es* K.
2. $\mathcal{O}_{\mathsf{K}}$ *es un* $\mathbb{Z}$*-módulo libre de rango* $[\mathsf{K} : \mathbb{Q}]$.

Demostración. Ver Teoremas y Corolarios 2 y 9 de [**6**].

❏

La parte 2. de la Proposición anterior tiene una consecuencia muy útil relacionada con los ideales de $\mathcal{O}_{\mathsf{K}}$:

Corolario A.1. *Sean* K *un cuerpo de números y* $\mathcal{A}$ *un ideal no nulo de* $\mathcal{O}_{\mathsf{K}}$. *Entonces, el cociente de anillos* $\mathcal{O}_{\mathsf{K}}/\mathcal{A}$ *es finito.*

En general, el anillo $\mathcal{O}_{\mathsf{K}}$ no es un dominio de factorización única, en efecto al considerar $\mathsf{K} = \mathbb{Q}(\sqrt{-5})$, el anillo $\mathcal{O}_{\mathsf{K}} = \mathbb{Z}[\sqrt{-5}]$ no tiene factorización única, pues $(-1 + 2\sqrt{-5}) \cdot (-1 - 2\sqrt{-5}) = 3 \cdot 7$ y $\frac{1}{3} \cdot (1 \pm 2\sqrt{-5}) \notin \mathbb{Z}[\sqrt{-5}]$.

TEOREMA A.1. $\mathcal{O}_{\mathsf{K}}$ *verifica:*

1. $\mathcal{O}_{\mathsf{K}}$ *es integralmente cerrado en* K*, es decir, si* $\alpha \in \mathsf{K}$ *satisface un polinomio mónico con coeficientes en* $\mathcal{O}_{\mathsf{K}}$*, entonces* $\alpha \in \mathcal{O}_{\mathsf{K}}$*.*
2. $\mathcal{O}_{\mathsf{K}}$ *es Noetheriano, es decir, dada una cadena de ideales* $\mathcal{A}_1 \subset \mathcal{A}_2 \subset \cdots$*, existe un entero* $\mathfrak{n}$ *tal que* $\mathcal{A}_{\mathfrak{n}} = \mathcal{A}_{\mathfrak{n}+1} = \cdots$*.*
3. *Cada ideal primo no nulo de* $\mathcal{O}_{\mathsf{K}}$ *es máximal.*

Demostración. La demostración de 1. es debido a las propiedades de los enteros algebraicos, Ver Ejercicio 4 Capítulo 2 de [**6**]. Los items 2. y 3. son consecuencias del corolario 1.1.

❏

En general, un dominio que verifica 1, 2 y 3 se conoce como **dominio de Dedekind.** La propiedad más importante de un dominio de Dedekind es que posee factorización única a nivel de ideales. Más precisamente

COROLARIO A.2. *Si* K *es un cuerpo de números, entonces un ideal no nulo en* $\mathcal{O}_{\mathsf{K}}$ *puede ser escrito como el producto*

$$\mathcal{A} = \mathcal{P}_1 \mathcal{P}_2 \cdots \mathcal{P}_{\mathfrak{r}}$$

de ideales primos, y su descomposición es única en ese orden. Además, los ideales $\mathcal{P}_{\mathfrak{i}}$*'s son los ideales primos de* $\mathcal{O}_{\mathsf{K}}$ *que contienen a* $\mathcal{A}$*.*

Demostración. Ver Capítulo 3, Teorema 16 de [**6**].

❏

Notemos que si $\mathcal{P}$ es ideal primo no nulo de $\mathcal{O}_{\mathsf{K}}$, el cociente de anillos $\mathcal{O}_{\mathsf{K}}/\mathcal{P}$ es finito por corolario A.1. Este cuerpo es llamado **cuerpo residual** de $\mathcal{P}$.
Sea L una extensión finita del cuerpo de números K. Si $\mathcal{P}$ es un ideal primo de

$\mathcal{O}_K$, entonces $\mathcal{P}\mathcal{O}_L$ es un ideal de $\mathcal{O}_L$, y así tiene una factorización prima

$$\mathcal{P}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r}$$

donde los $\mathfrak{P}_i^{e_i}$'s son los ideales no nulos de $\mathcal{O}_L$ que contienen a $\mathcal{P}$. El entero e_i lo llamaremos **índice de ramificación** de $\mathcal{P}$ en $\mathfrak{P}_i$. Cada primo $\mathfrak{P}_i$ que contiene a $\mathcal{P}$ da un cuerpo residual tal que $\mathcal{O}_K/\mathcal{P} \mid \mathcal{O}_L/\mathfrak{P}_i$, y su grado, el cual denotaremos por f_i, es el **grado de inercia** de $\mathcal{P}$ en $\mathfrak{P}_i$. La relación básica entre los e_i's y f_i's esta dada por el siguiente Teorema:

TEOREMA A.2. *Sean $K \subset L$ dos cuerpos de números, y $\mathcal{P}$ un ideal primo no nulo de $\mathcal{O}_K$. Entonces,*

$$\sum_{i=1}^{r} e_i f_i = [L : K].$$

donde los e_i's son los indices de ramificación y los f_i's son los grados de inercia mencionados anteriormente.

Demostración. Ver Teorema 21 de [**6**].

❏

Diremos que un ideal primo $\mathcal{P}$ de $\mathcal{O}_K$ **ramifica** en L si y sólo si, los indices de ramificación e_i's son mayores que 1. Se puede probar que sólo un número finito de ideales primos no nulos de $\mathcal{O}_K$ ramifican en L.
La siguiente propiedad muestra que la ramificación puede ser bien comprendida si la extension es de Galois.

TEOREMA A.3. *Sean L/K una extensión de Galois, y $\mathcal{P}$ un ideal primo no núlo de $\mathcal{O}_K$.*

1. *El grupo de Galois Gal(L/K) actua transitivamente en los primos no nulos de $\mathcal{O}_L$ que contienen a $\mathcal{P}$, es decir, si $\mathfrak{P}$ y $\mathfrak{P}$' son ideales primos de $\mathcal{O}_L$ que contienen a $\mathcal{P}$, existe $\sigma \in Gal(L \mid K)$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$.*
2. *Los ideales primos no nulos $\mathfrak{P}_1, ..., \mathfrak{P}_r$ de $\mathcal{O}_L$ que contienen a $\mathcal{P}$ tienen todos el mismo indice de ramificación e y el mismo grado de inercia f, y*

además

$$e\mathsf{f}\mathsf{r} = [\mathsf{L} : \mathsf{K}].$$

Demostración. Ver Teorema 23 de [**6**].

❏

Así dada una una extensión de Galois L/K, un ideal primo no nulo de $\mathcal{O}_\mathsf{K}$ ramifica si $e > 1$, en caso contrario diremos que no ramifica. Si $\mathcal{P}$ satisface la condición $e = \mathsf{f} = 1$, diremos que $\mathcal{P}$ se descompone completamente en L.

2. Norma, Traza y Discriminante

Como $\mathsf{K}/\mathbb{Q}$ es una extensión finita, K puede ser visto como un espacio vectorial finito dimensional sobre $\mathbb{Q}$, así, dado $\alpha \in \mathsf{K}$ definimos la aplicación

$$\begin{array}{rccc} \Phi_\alpha : & \mathsf{K} & \longrightarrow & \mathsf{K} \\ & \nu & \longmapsto & \alpha\nu \end{array}$$

la cual claramente es lineal sobre K.

Definición A.1. *Definimos la* ***traza*** *de* α *por* $\mathsf{Tr}_\mathsf{K}(\alpha) := \mathsf{Tr}(\Phi_\alpha)$ *y la* ***norma*** *de* α *por* $\mathsf{N}_\mathsf{K}(\alpha) := \det(\Phi_\alpha)$.

Lema A.4. *Sean* K *un cuerpo de números y* $\alpha \in \mathcal{O}_\mathsf{K}$. *Entonces* $\mathsf{Tr}_\mathsf{K}(\alpha)$, $\mathsf{N}_\mathsf{K}(\alpha) \in \mathbb{Z}$.

Definición A.2. *Sea* $\mathcal{A}$ *un ideal no nulo de* $\mathcal{O}_\mathsf{K}$. *Definimos la* ***norma absoluta*** *de* $\mathcal{A}$ *como*

$$\mathsf{N}(\mathcal{A}) := [\mathcal{O}_\mathsf{K} : \mathcal{A}] = \mid \mathcal{O}_\mathsf{K}/\mathcal{A} \mid .$$

Una consecuencia del hecho que $\mathcal{O}_\mathsf{K}$ tiene rango $[\mathsf{K} : \mathbb{Q}] = n$,

Definición A.3. *Sea* n *el rango del* $\mathbb{Z}$*-módulo libre* $\mathcal{O}_\mathsf{K}$. *Diremos que* $\{w_1, w_2, ..., w_n\} \subseteq \mathcal{O}_\mathsf{K}$ *es una* ***base integral*** *de* K, *si y sólo si,* $\mathcal{O}_\mathsf{K} = w_1\mathbb{Z} + w_2\mathbb{Z} + \ ... \ + w_n\mathbb{Z}$.

Definición A.4. *Llamaremos* ***incrustación*** *a todo homomorfismo de cuerpos inyectivo.*

PROPOSICIÓN A.2. *Sea* K *un cuerpo de números de grado* n. *Entonces, existen* $\sigma_1, ..., \sigma_n$ *incrustaciones distintas de* K *en* $\mathbb{C}$.

DEFINICIÓN A.5. *Definimos el* ***discriminante*** *de* K, *el cual denotaremos por* d_K, *como*

$$d_K := \det(w_i^{(j)})^2,$$

donde $\{w_1, w_2, ..., w_n\}$ *es una base integral de* K *y* $w_i^{(j)} = \sigma_j(w_i)$.

OBSERVACIÓN 1. *Dada una base integral* $\{w_1, w_2, ..., w_n\}$, *podemos definir de manera análoga el discriminante de* K *como*

$$d_K(\alpha_1, ..., \alpha_n) = \det(Tr_K(\alpha_i \cdot \alpha_j)).$$

DEFINICIÓN A.6. *Sea* σ *una incrustación de* K *en* $\mathbb{C}$. *Diremos que* σ *es* ***real*** *si* $\sigma(K) \subset \mathbb{R}$. *En otro caso diremos que* σ *es* ***compleja***, *en este caso su conjugado,* $\overline{\sigma}$, *esta definido por* $\overline{\sigma}(k) = \overline{\sigma(k)}$.

Ahora, si hay r_1 incrustaciones reales y r_2 pares conjugados de incrustaciones complejas, tenemos que $r_1 + 2r_2 = n$.

LEMA A.5. *Sea* $\mathcal{A}$ *un ideal no nulo de* $\mathcal{O}_K$. *Entonces existe* $\alpha \in \mathcal{A}$ *no nulo, tal que*

$$| N_K(\alpha) | \leqslant \left(\frac{2}{\pi}\right)^{r_2} N(\mathcal{A}) \mid d_k \mid^{\frac{1}{2}} .$$

3. Cuerpos Cuadráticos

DEFINICIÓN A.7. *Diremos que* K *es un* ***cuerpo de números cuadrático****, si y sólo si,* K *es un espacio vectorial de dimensión 2 sobre* $\mathbb{Q}$. *Tal cuerpo es de la forma*

$K = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$, $d \in \mathbb{Z} \setminus \{0, 1\}$ *libre de cuadrados.*

Si d *es positivo diremos que* K *es un cuerpo de números* ***cuadrático real****, y si* d *es negativo diremos que* K *es un cuerpo de números* ***cuadrático imaginario***.

En lo que sigue, salvo mención, K denotara un cuerpo de números cuadrático y nos referiremos a los cuerpos de números cuadráticos simplemente como cuerpos cuádraticos.

La función **conjugación** de K es

$$\overline{f} : K \longrightarrow K, \quad \overline{a + b\sqrt{d}} = a - b\sqrt{d},$$

el cual es un automorfismo y es una involución, es decir

$$\overline{\overline{x}} = x, \text{ para cada } x \in K.$$

Observemos que con esta notación la conjugación de K coincide con la conjugación compleja para el caso $d = -1$.

La función **traza** de K es el homomorfimo aditivo dado por

$$tr : K \longrightarrow \mathbb{Q}, \quad tr(\alpha) = \alpha + \overline{\alpha}.$$

Especificamente,

$$tr(a + b\sqrt{d}) = a + b\sqrt{d} + \overline{a + b\sqrt{d}} = 2a.$$

La función **norma** de K es el homomorfimo multiplicativo dado por

$$N_K : K \longrightarrow \mathbb{Q}, \quad N_K(\alpha) = \alpha\overline{\alpha}.$$

Especificamente,

$$N_K(a + b\sqrt{d}) = (a + b\sqrt{d})(\overline{a + b\sqrt{d}}) = a^2 - b^2 d.$$

Si K es un cuerpo cuadrático imaginario entonces su norma es positiva en $K^\times$.

Por otro lado, tenemos que $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, a dichos enteros los llamaremos **enteros racionales** de K. Un elemento α de $K \setminus \mathbb{Q}$ tiene como polinomio minimal

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - tr(\alpha)x - N_K(\alpha)$$

y, $\alpha = a + b\sqrt{d}$ es un entero, si y sólo si, su traza y su norma son enteros racionales de K.

PROPOSICIÓN A.3. *El anillo de enteros $\mathcal{O}_K$ de un cuerpo cuadrático K es de la forma*

$$\mathcal{O}_K = \mathbb{Z}[g], \quad g = \begin{cases} \frac{1+\sqrt{d}}{2} & si \ d \equiv \quad 1 \quad (mod 4), \\ \sqrt{d} & si \ d \equiv \ 2, 3 \quad (mod 4). \end{cases}$$

Demostración. Los elementos 1, g son linealmente independientes sobre $\mathbb{Z}$, pues lo son sobre $\mathbb{Q}$, probaremos que $\mathbb{Z} + g\mathbb{Z} = \mathcal{O}_K$. Como $g \in \mathcal{O}_K$, tenemos $\mathbb{Z} + g\mathbb{Z} \subseteq \mathcal{O}_K$.

Por otro lado, sea $\alpha \in \mathcal{O}_K$ de la forma $\frac{m}{2} + \frac{n}{2} \cdot \sqrt{d}$, con $m, n \in \mathbb{Z}$, $m^2 \equiv n^2 d(\text{ mod} 4)$. Si $d \equiv 1(\text{ mod} 4)$, entonces $m^2 \equiv n^2(\text{ mod} 4)$, y así m y n tienen la misma paridad, digamos $m = 2k + n$ con $k \in \mathbb{Z}$. Entonces $\alpha = k + n \cdot \frac{1+\sqrt{d}}{2} = k + n \cdot g$.

Si $d \equiv 2$ o $3(\text{ mod} 4)$ tenemos que m y n son pares. En efecto, si n fuese impar, entonces $n^2 \equiv 1(\text{ mod} 4)$, luego $m^2 \equiv n^2 \cdot d \equiv d(\text{ mod} 4)$ y por tanto $d \equiv 0$ 0 $1(\text{ mod} 4)$, lo cual es absurdo. Así, n es par y como $m^2 \equiv n^2 \cdot d \equiv 0(\text{ mod} 4)$ concluimos que m tambien es par. De esta manera concluye la demostración. ❏

Dado que el polinomio minimal del generador g de los enteros de K es cuadrático, y como $\mathcal{O}_K$ es un grupo abeliano, tenemos

$$\mathcal{O}_K = g\mathbb{Z} \oplus \mathbb{Z}.$$

TEOREMA A.6. *El discriminante de* $K = \mathbb{Q}(\sqrt{d})$ *está dado por*

$$d_K = \begin{cases} d & si\ d \equiv \quad 1 \quad (mod 4), \\ 4d & si\ d \equiv \ 2, 3 \quad (mod 4). \end{cases}$$

Con esta defínción de el discriminante, podemos describir los enteros de K como

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

Consideremos a un número entero y p un número primo. Una manéra de decidir si la congruencia $x^2 \equiv q(\text{mod } p)$ tiene o no solución, es definiendo la siguiente expresión.

DEFINICIÓN A.8. *Definimos el* ***símbolo de Legendre*** *entre* a *y el primo* p *como*

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

PROPOSICIÓN A.4. *Sean* K *un cuerpo de números cudrático con discriminante* d_K*,* σ *el automorfimo no trivial de* K*, y* p *un primo en* $\mathbb{Z}$*.*

1. *Si* $\left(\frac{d_k}{p}\right) = 0$*, entonces* $p\mathcal{O}_K = \mathcal{P}^2$ *para algún ideal primo no nulo* $\mathcal{P}$ *de* $\mathcal{O}_K$*.*
2. *Si* $\left(\frac{d_k}{p}\right) = 1$*, entonces* $p\mathcal{O}_K = \mathcal{P}\mathcal{P}'$*, donde* $\mathcal{P}$*,* $\mathcal{P}'$ *son ideales primos no nulos distintos en* $\mathcal{O}_K$*.*
3. *Si* $\left(\frac{d_k}{p}\right) = -1$*, entonces* $p\mathcal{O}_K$ *es ideal primo no nulo en* $\mathcal{O}_K$*.*

Demostración. Ver de Proposición 5.16 de [**7**].

❏

Una consecuencia importante de la Proposición anterior, viene dada por el siguiente corolario, el cual detecta primos que ramifican en K.

COROLARIO A.3. *Sean* K *un cuerpo de números cudrático con discriminante* d_K*, y* p *un primo en* $\mathbb{Z}$*. Entonces:*

1. p *ramifica en* K *si y sólo si,* p *divide a* d_K*.*
2. p *se separa completamente en* K*, si y sólo si,* $\left(\frac{d_k}{p}\right) = 1$*.*

4. Unidades de un Cuerpo Cuadrático

DEFINICIÓN A.9. *Llamaremos* ***unidad*** *de* K *a todos los elementos del anillo de enteros* $\mathcal{O}_K$ *que sean invertibles, y* ***grupo de unidades de*** K *a el grupo multiplicativo* $\mathcal{O}_K^\times$*.*

PROPOSICIÓN A.5. *Un elemento* $\alpha \in \mathcal{O}_K$ *es una unidad de* K*, si y sólo si,* $N_K(\alpha) = \pm 1$*.*

Demostración. Si $\alpha \in \mathcal{O}_{\mathsf{K}}$ es multiplicativamente invertible por $\beta \in \mathcal{O}_{\mathsf{K}}$, entonces

$$1 = \mathsf{N}_{\mathsf{K}}(1) = \mathsf{N}_{\mathsf{K}}(\alpha\beta) = \mathsf{N}_{\mathsf{K}}(\alpha)\mathsf{N}_{\mathsf{K}}(\beta),$$

de modo que $\mathsf{N}_{\mathsf{K}}(\alpha) = \pm 1$, pues ambas normas son números enteros. Por otro lado, si $\mathsf{N}(\alpha) = \pm 1$ entonces α es invertible por $\pm\overline{\alpha} \in \mathcal{O}_{\mathsf{K}}$, pues $\pm\alpha\overline{\alpha} = \pm\mathsf{N}_{\mathsf{K}}(\alpha) = 1$.

❏

Si $\mathsf{K} = \mathbb{Q}(\sqrt{\mathtt{d}})$ es un cuerpo cuadrático imaginario, entonces el grupo de unidades es

$$\mathcal{O}_{\mathsf{K}}^{\times} = \begin{cases} \{\pm 1, \pm \mathtt{i}\} & \text{si } \mathtt{d} = -1 \\ \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\} & \text{si } \mathtt{d} = -3 \quad (\text{donde } \zeta_3 = (-1+\sqrt{-3})/2), \\ \{\pm 1\} & \text{en otro caso.} \end{cases},$$

Si $\mathsf{K} = \mathbb{Q}(\sqrt{\mathtt{d}})$ es un cuerpo cuadrático real, entonces el grupo de unidades es de la forma

$$\mathcal{O}_{\mathsf{K}}^{\times} = \left\{ \pm\, \mathfrak{u}^{\mathtt{d}} \,:\, \mathtt{d} \in \mathbb{Z} \right\} \simeq (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$$

donde $\mathfrak{u} > 1$ es llamada **unidad fundamental**.

Definición A.10. *El simbolo* $w(\mathsf{K})$ *denotara el* ***número de raices de la unidad*** *en* K. *Así*

$$w(\mathsf{K}) = \begin{cases} 4 & \textit{si } \mathsf{K} = \mathbb{Q}(\mathtt{i}) \\ 6 & \textit{si } \mathsf{K} = \mathbb{Q}(\sqrt{-3}), \\ 2 & \textit{en otro caso.} \end{cases},$$

Para cuerpos cuadráticos imaginarios el número $w(\mathsf{K})$ describe completamente el grupo de unidades, para el caso de cuerpos cuadráticos reales, la unidad fundamental $\mathfrak{u}$ da la descripción completa.

La estructura del grupo de unidades es más complicada en el caso de cuerpos cuadráticos reales, esta es la razón de que la fórmula del número de clase es más sencilla en el caso imaginario.

Para una descripción del caso en que K no es cuadrático, consultar Teorema de las unidades de Dirichlet (el cual describe la estructura del grupo de unidades para cualquier cuerpo de números) en Jarvis [**2**].

5. Grupo de Clases de Ideales

DEFINICIÓN A.11. *Diremos que $\mathcal{B} \subseteq K$ es un* ***ideal fraccionario*** *de K, si y sólo si, $\mathcal{B} = \alpha\mathcal{A}$, donde $\alpha \in K^\times$ y $\mathcal{A}$ es un ideal de $\mathcal{O}_K$.*

Una manera equivalente de dar esta definición es la siguiente: Un ideal fraccionario $\mathcal{A}$ de $\mathcal{O}_K$ es un $\mathcal{O}_K$-módulo contenido en K tal que existe un $m \in \mathbb{Z}$ tal que $m\mathcal{A} \subseteq \mathcal{O}_K$.

En lo que sigue los ideales comunes de $\mathcal{O}_K$ los llamaremos ideales integrales para distinguirlos de los ideales fraccionarios.

Dado $\mathcal{P}$ un ideal primo de $\mathcal{O}_K$, definimos

$$\mathcal{P}^{-1} = \left\{x \in K : x\mathcal{P} \subseteq \mathcal{O}_K\right\}.$$

PROPOSICIÓN A.6. *Sea $\mathcal{A}$ un ideal fraccionario de K. Entonces*

1. *$\mathcal{A}$ es invertible, es decir, existe un ideal fraccionario $\mathcal{B}$ tal que $\mathcal{A}\mathcal{B} = \mathcal{O}_K$. El ideal $\mathcal{B}$ lo denotaremos $\mathcal{A}^{-1}$.*
2. *$\mathcal{A}$ puede ser escrito únicamente como un producto $\mathcal{A} = \prod_{i=1}^{r} \mathcal{P}_i^{r_i}$, $r_i \in \mathbb{Z}$, donde los $\mathcal{P}_i$'s son ideales primos distintos de $\mathcal{O}_K$.*

Demostración. Ver Ejercicio 31 capítulo 3 de [**6**].

❏

Denotaremos por I_K al conjunto de ideales fraccionarios de K, el cual es un grupo abeliano bajo la multiplicación de elementos de $\mathcal{O}_K$, donde

$$\mathcal{B} \cdot \mathcal{B}' = \alpha\mathcal{A} \cdot \alpha'\mathcal{A}' = \alpha\alpha'\mathcal{A}\mathcal{A}'.$$

Un **ideal fraccionario es principal**, si es de la forma

$$\mathcal{B} = \alpha \cdot (x), \text{ donde } (x) \text{ es un ideal principal de } \mathcal{O}_K.$$

Denotaremos por P_K al conjunto de ideales fraccionarios principales, el cual es un subgrupo del grupo multiplicativo I_K.

DEFINICIÓN A.12. *Llamaremos* ***grupo de clases de ideales*** *al grupo cociente*

$$Cl_K = I_K/P_K.$$

El orden del grupo de clases de ideales lo llamaremos número de clases de ideales, y lo denotaremos por h_K.

Así, un elemento del grupo de clases de ideales es una coclase de la forma $\mathcal{B}P_K$, y la multiplicación en C_K viene dada por

$$\mathcal{B}P_K \cdot \mathcal{B}'P_K = \mathcal{B}\mathcal{B}'P_K.$$

A continuación veremos que el número de clases de ideales es finito

TEOREMA A.7. *El grupo de clases de ideales* Cl_K *es finito.*

Demostración. Sean $\mathcal{A}$ un ideal fraccionario y $\mathcal{B}$ un representante de la coclase $\mathcal{A}^{-1}P_K$. Como $\mathcal{B} \subseteq \mathcal{O}_K$, por Lema A.5 existe $\beta \in \mathcal{B}$ no nulo, tal que

$$| N_K(\beta) | \leqslant \left(\frac{2}{\pi}\right)^{r_2} | d_k |^{\frac{1}{2}} N(\mathcal{B}).$$

Ahora, sea $\mathcal{C} = (\beta)\mathcal{B}^{-1} \in \mathcal{A}P_K$. Como $\beta \in \mathcal{B}$, cada elemento de $\mathcal{C}$ es integral y así $\mathcal{C} \subseteq \mathcal{O}_K$. Tenemos

$$N(\mathcal{C}) = | N_K(\beta) | N(\mathcal{B})^{-1} \leqslant \left(\frac{2}{\pi}\right)^{r_2} | d_k |^{\frac{1}{2}} = M,$$

pero sólo hay un número finito de ideales integrales cuya norma es a lo más M[*]. Por tanto, sólo puede haber un número finito de clases de ideales, lo cual concluye la demostración.

❏

[*] si consideramos la factorización de un ideal integral en primos, utilizando la multiplicabilidad de la norma, podemos observar que sólo puede haber un número finito de números primos cuya norma es delimitada por M.

Apéndice B

Tabla de Números de Clases

En lo que sigue $\mathfrak{h}$ denotara el número de clases del cuerpo cuadrático imaginario $\mathbb{Q}(\sqrt{-\mathfrak{d}})$, donde $\mathfrak{d}$ es libre de cuadrados y $1 \leqslant \mathfrak{d} < 500$, para detalles recomendamos consultar pag. 425-426 de [**3**].

$\mathfrak{d}$	$\mathfrak{h}$	$\mathfrak{d}$	$\mathfrak{h}$	$\mathfrak{d}$	$\mathfrak{h}$	$\mathfrak{d}$	$\mathfrak{h}$	$\mathfrak{d}$	$\mathfrak{h}$
1	1	31	3	62	8	93	4	123	2
2	1	33	4	65	8	94	8	127	5
3	1	34	4	66	8	95	8	129	12
5	2	35	2	67	1	97	4	130	4
6	2	37	2	69	8	101	14	131	5
7	1	38	6	70	4	102	4	133	4
10	2	39	4	71	7	103	5	134	14
11	1	41	8	73	4	105	8	137	8
13	2	42	4	74	10	106	6	138	8
14	4	43	1	77	8	107	3	139	3
15	2	46	4	78	4	109	6	141	8
17	4	47	5	79	5	110	12	142	4
19	1	51	2	82	4	111	8	143	10
21	4	53	6	83	3	113	8	145	8
22	2	55	4	85	4	114	8	146	16
23	3	57	4	86	10	115	2	149	14
26	6	58	2	87	6	118	6	151	7
29	6	59	3	89	12	119	10	154	8
30	4	61	6	91	2	122	10	155	4

d	h	d	h	d	h	d	h	d	h
157	6	214	6	273	8	331	3	395	8
158	8	215	14	274	12	334	12	397	6
159	10	217	8	277	6	335	18	398	20
161	16	218	10	278	14	337	8	399	16
163	1	219	4	281	20	339	6	401	20
165	8	221	16	282	8	341	28	402	16
166	10	222	12	283	3	345	8	403	2
167	11	223	7	285	16	346	10	406	16
170	12	226	8	286	12	347	5	407	16
173	14	227	5	287	14	349	14	409	16
174	12	229	10	290	20	353	16	410	16
177	4	230	20	291	4	354	16	411	6
178	8	231	12	293	18	355	4	413	20
179	5	233	12	295	8	357	8	415	10
181	10	235	2	298	6	358	6	417	12
182	12	237	12	299	8	359	19	418	8
183	8	238	8	301	8	362	18	419	9
185	16	239	15	302	12	365	20	421	10
186	12	241	12	303	10	366	12	422	10
187	2	246	12	305	16	367	9	426	24
190	4	247	6	307	3	370	12	427	2
191	13	249	12	309	12	371	8	429	16
193	4	251	7	310	8	373	10	430	12
194	20	253	4	311	19	374	28	431	21
195	4	254	16	313	8	377	16	433	12
197	10	255	12	314	26	379	3	434	24
199	9	257	16	317	10	381	20	435	4
201	12	258	8	318	12	382	8	437	20
202	6	259	4	319	10	383	17	438	8
203	4	262	6	321	20	385	8	439	15
205	8	263	13	322	8	386	20	442	8
206	20	265	8	323	4	389	22	443	5
209	20	266	20	326	22	390	16	445	8
210	8	267	2	327	12	391	14	446	32
211	3	269	22	329	24	393	12	447	14
213	8	271	11	330	8	394	10	449	20

d	h	d	h	d	h	d	h	d	h
451	6	462	8	471	16	483	4	497	24
453	12	463	7	473	12	485	16	498	8
454	14	465	16	474	20	487	7	499	3
455	20	466	8	478	8	489	20		
457	8	467	7	479	25	491	9		
458	26	469	16	481	16	493	12		
461	30	470	20	482	20	494	28		

Bibliografía

[1] M. Ram Murty, J. Esmonde. *Problems in Algebraic Number Theory.* Second Edition, Springer, 2005.

[2] F. Jarvis. *Algebraic Number Theory.* Undergraduate Mathematics Series, Springer, 2014.

[3] Z. I. Borevich, I. R. Shafarevich. *Number Theory.* Academic Press Inc, 1966.

[4] S. Lang. *Algebraic Number Theory.* Second Edition, Springer, 1994.

[5] K. Ireland, M. Rosen. *A Classical Introduction to Modern Number Theory.* Springer-Verlag, 1990.

[6] D. Marcus. *Number Fields.* Springer-Verlag, New York Inc, 1977.

[7] D. Cox. *Primes Of The Form* $\mathfrak{x}^2 + \mathfrak{n}\mathfrak{y}^2$*: Fermat, Class Field Theory, and Complex Multiplication.* John Wiley y Sons, Inc, 1989.

[8] H. Montgomery, R. Vaughan. *Multiplicative Number Theory I. Classical Theory.* Cambridge University Press, 2006.

[9] J. P. Serre. *A Course in Arithmetic.* Springer, 1996.

[10] T. Apostol. *Introduction to Analytic Number Theory.* Springer-Verlag, 1976.

[11] J. Neukirch. *Algebraic Number Theory.* Springer, 1976.

[12] H. Bateman. *Higuer Trascendental Functions, Vol. I.* McGraw-Hill, New York Toronto London, 1953.

[13] B. W. Jones. *The Arithmetic Theory of Quadratic Forms.* The Carus Mathematical Monographs Number 10, The Mathematical Association of America - John Wiley and Sons, 1967.

[14] C. Gauss. *Disquisitiones Arithmeticae.* English traducción por A. Clarke, revisado por W. Waterhouse, Springer-Verlag, 1986.

[15] D. Goldfeld. *Gauss' Class Number Problems for Imaginary Quadratic Fields.* Bulletin of the American Mathematical Society, 13 (1985), pp. 23-37.

[16] E. Bombieri, W. Gubler. *Heights in Diophantine Geometry.* Volume 4 of New Mathematical Monographs, Cambridge University Press, 2006.

[17] H. Iwaniec. *Topics in Classical Automorphic Forms.* Graduate Studies in Mathematics, Volume 17, American Mathematical Society, 1997.

[18] H. Davenport. *Multiplicative Number Theory.* Graduate Texts in Mathematics 74, Springer-Verlag, 1980.

[19] A. Baker, A. Schinzel. *On the Least Integers Represented by the Genera of Binary Quadratic Forms.* Acta Arithmetica, Vol XVIII,1971, pp. 137-144.

[20] A. Baker. *Linear Forms in the Logarithms of Algebraic Numbers.* Mathematika 13, 1966, 204-216.

[21] ————-. *Contributions to the Theory of Diophantine Equations I: On the Representation of Integers By Binary Forms* . Philos. Trans. Royal Society (1968), pp. 173-208.

[22] ————-. *A remark on the class number of quadratic fields.* Bulletin London Mathematical Society. 1 (1969), pp. 98-102.

[23] ————-. *Imaginary quadratic fields with class number 2.* Annals of Math, Second Series, Vol. 94, No. 1 (Jul., 1971), pp. 139-152.

[24] ————-. *On the Class Number of Imaginary Quadratic Fields.* Bulletin of the American Mathematical Society, Vol. 77, No. 5 (Sep., 1971), pp. 678-684.