La Fórmula del Número de Clases y Valores Especiales de Funciones L: Desde Dirichlet y Dedekind hasta Stark

Elkin Oveimar Quintero Vanegas
Matemático.

Universidad Nacional de Colombia
Facultad de Ciencias
Departamento de Matemáticas
Bogotá, D.C.
Junio de 2011

La Fórmula del Número de Clases y Valores Especiales de Funciones L: Desde Dirichlet y Dedekind hasta Stark

Elkin Oveimar Quintero Vanegas
Matemático.

Trabajo de tesis para optar al título de
Magister en Ciencias - Matemáticas

Director
Eduardo Dueñez, Ph.D.
Profesor Asistente, Universidad de Texas en San Antonio

Codirector
Victor Samuel Albis, Ph.D.
Profesor Titular, Universidad Nacional de Colombia

Universidad Nacional de Colombia
Facultad de Ciencias
Departamento de Matemáticas
Bogotá, D.C.
Junio de 2011

Título en español

La Fórmula del Número de Clases y Valores Especiales de Funciones L: Desde Dirichlet y Dedekind hasta Stark

Title in English

The Class Number Formula and Special Values of L-functions: From Dirichlet and Dedekind to Stark

Resumen: En este trabajo se estudian aplicaciones aritméticas de la teoría de funciones zeta y L, enfatizando la interpretación de sus valores en $s = 1$ (ó, equivalentemente, en $s = 0$, vía la ecuación funcional respectiva). Los casos clásicos de la función zeta de Riemann y las funciones L de Dirichlet conducen de manera natural al estudio de la sucesión de los números primos, o de primos en progresiones aritméticas (como hace Dirichlet en su renombrado teorema). El valor en $s = 1$ de una función L cuadrática de Dirichlet se interpreta a través de su celebrada fórmula de número de clases vía el número de clases y regulador de un cuerpo de números cuadráticos (ó, de manera más clásica, usando formas cuadráticas de un discriminante dado). La fórmula de número de clases más general obtenida por Dedekind se aplica a las funciones zeta que llevan su nombre (y que incluyen la de Riemann). En el capítulo final explicamos de manera general más generalizaciones del concepto de función L así como las conjeturas de Stark que relacionan los valores de aquéllas en $s = 0$ con una cantidad aritmética profunda conocida como el regulador de Stark asociado a una representación de Galois de un cuerpo de números algebraicos.

Abstract: We study arithmetic applications of the theory of zeta and L-functions with an emphasis on the interpretation of their values at $s = 1$ (equivalently at $s = 0$, through the respective functional equation). The classical cases of the Riemann zeta-function and Dirichlet L-functions lead naturally to the study of the sequence of all primes, or of primes in arithmetic progressions (as in Dirichlet's renown theorem). The value at $s = 1$ of a quadratic Dirichlet L-function is interpreted through his celebrated Class Number Formula via the class number and regulator of a quadratic number field (or, more classically, using quadratic forms of a given discriminant). The more general class number formula obtained by Dedekind applies to zeta functions named after him (and which include Riemann's). In a concluding chapter we survey further generalizations of the concept of L-function alongside open conjectures of Stark relating their values at $s = 0$ with a deep arithmetic quantity known as the Stark regulator attached to a Galois representation of a number field.

Palabras clave: función L, función zeta de Riemann, función zeta de Dedekind, formas cuadráticas binarias, regulador de unidades, fórmula de número de clases, conjeturas de Stark.

Keywords: L-function, Riemann zeta function, Dedekind zeta function, binary quadratic forms, regulator of units, class number formula, Stark's conjectures.

Dedicado a

Mis padres, y a Leider y Deiby.

Agradecimientos

Mis agradecimientos a Jhon Jaiver Rodriguez y Leonardo Chacón por acompañar de una manera u otra la discusión y realización de este escrito.

Al profesor Victor Albis por sus comentarios y ayudas prestadas en el momento indicado.

Finalmente al profesor Eduardo Dueñez por haberme guiado página tras página en un campo en el que mi conocimiento inicial no era suficiente para afrontar el camino, motivo por el cual en muchos instantes su paciencia tuvo que ser infinita.

Índice general

Introducción

El objetivo de esta tesis es el de servir como introducción al estudio de una fascinante intersección entre los enfoques analíticos y algebraicos a la teoría de números. En particular, deseamos introducir al lector al estudio de aplicaciones de la teoría de funciones zeta y L. El tema común que trasciende capítulos específicos es el de las implicaciones aritméticas de las propiedades analíticas de tales funciones.

Las funciones L (para nuestros propósitos, las funciones zeta son casos especiales de funciones L) son funciones meromorfas de una variable compleja s. Existe una gran variedad de tales funciones, pasando por la clásica función zeta de Riemann, que se generaliza a la función zeta de Dedekind de un cuerpo de números algebraico arbitrario K en el capítulo 5, sin olvidar las también clásicas funciones L de Dirichlet y su generalización a funciones L de Hecke en el capítulo 7. Todas estas han sido utilizadas como herramientas en el estudio de problemas íntimamente aritméticos. Nuestro trabajo en el capítulo 1, inicia con la función L más sencilla, la función zeta de Riemann $\zeta(s)$, y algunas de sus más elementales aplicaciones a la teoría de números.

Posteriormente nuestra atención se enfoca al estudio de las funciones L usadas por Dirichlet en su demostración del teorema de primos en progresiones aritméticas, el cual se encuentra en el capítulo 4. Curiosamente, el aspecto central de tal demostración es la no anulación de cierta función L en $s = 1$. Dirichlet encontró una genial demostración de la no anulación de la función L proporcionando una *fórmula de número de clases* para el valor $L(1, \chi_d)$ en términos de dos cantidades numéricas íntimamente relacionadas con las propiedades aritméticas de un cuerpo cuadrático (una extensión algebraica $\mathbb{Q}(\sqrt{d})$ del cuerpo $\mathbb{Q}$ de números racionales obtenida al adjuntar $\sqrt{d}$ cuando d no es un cuadrado perfecto), a saber su número de clases h_d (un entero positivo) y su regulador R_d (un número real, el cual no es nulo). Siguiendo la exposición histórica presentamos la interpretación de h_d tanto como número de clases de formas cuadráticas binarias, así como de clases de ideales. (Es quizás desafortunado que la nomenclatura *fórmula de número de clases* no mencione al regulador, pues como hemos mencionado éste juega un papel tan importante como el número de clases, aunque inicialmente tal importancia no sea patente).

El resto de este trabajo retoma la evolución histórica del estudio de valores de funciones L en $s = 1$, procediendo a la demostración de la fórmula de número de clases de Dedekind expuesta en el capítulo 6, que generaliza la fórmula de Dirichlet al usar la función zeta de Dedekind de un cuerpo de números algebraicos arbitrario K. La demostración de este hermoso resultado involucra partes iguales de análisis y aritmética y representa la culminación teórica de la tesis, sintetizando resultados previos relativos a la función zeta de Riemann

y funciones L de Dirichlet. Es de mencionar que se hace un estudio de las funciones L de Dedekind en el punto $s = 0$ debido a la ecuación funcional que ellas satisfacen, pues finalmente la conjetura de Stark se enuncia alrededor de este punto.

En el último capítulo se exponen funciones L generalizadas tales como funciones L de Hecke y de Artin. Como colofón, y sirviendo de conclusión natural a los temas tocados en esta tesis a nivel de maestría, se explica el concepto de regulador de Stark y su conexión conjetural, también debida a Stark y otros investigadores, con los valores especiales $L(0, \chi)$ (naturalmente con $L(1, \chi)$ gracias a la ecuación funcional) de funciones L de Artin. Las conjeturas generales de Stark son objeto de estudio vigoroso y profundo actualmente no sólo por su interés intrínseco, sino también por sus conexiones con el famoso Problema 12 de Hilbert, que sigue en gran medida abierto.

CAPÍTULO 1

La función zeta de Riemann $\zeta(s)$.

La primera parte de este trabajo, será dedicada al estudio de la función zeta de Riemann, la cual, se define como una serie de Dirichlet y posteriormente, se enfoca desde el punto de vista del análisis complejo, para así estudiar algunas de sus propiedades más básicas que tendrán relación con el contenido de posteriores capítulos. El estudio de esta función es muy amplio, y si alguien está interesado en hacer una lectura profunda, puede remitirse, por ejemplo al libro [Tit86].

Para no ir en contra con la notación dada en la mayoría de la bibliografía, si $s \in \mathbb{C}$ se escribirá a s como $s = \sigma + it$.

1.1. Notas para el capítulo.

1.1.1. Series de Dirichlet.

Definición 1.1.1. *Una función aritmética es una función sobre* $\mathbb{N}$ *con valores complejos.*

El conjunto de las funciones aritméticas se denota con $\mathcal{A}$. Sean $f, g \in \mathcal{A}$ se definen las siguientes operaciones:

- $(f + g)(n) := f(n) + g(n)$.
- $(f * g)(n) := \sum_{d|n} f(d)g(n/d)$.

La última operación se conoce como la convolución de Dirichlet. Con estas dos operaciones, $\mathcal{A}$ es un anillo conmutativo sin divisores de cero con identidad. La función que cumple esta labor es la función $I(n)$ definida así:

$$I(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1. \end{cases}$$

Definición 1.1.2. *Una función aritmética f no idénticamente nula, se llama multiplicativa si*

$$f(nm) = f(n)f(m) \qquad \text{cuando } (n,m) = 1,$$

y completamente multiplicativa si

$$f(nm) = f(n)f(m) \qquad \text{para todo } n, m \in \mathbb{N}.$$

Claramente la función $u(n) = 1$ para cada $n \in \mathbb{N}$, es una función completamente multiplicativa.

Definición 1.1.3. *Sean $f \in \mathcal{A}$ y $s \in \mathbb{C}$. Se conoce como la serie de Dirichlet asociada a la función f, a la serie $F(s)$ definida por*

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

Si se quiere ver a $F(s)$ como una función de variable compleja, se tiene que estudiar su región de convergencia.

Dado que $|n^s| = n^\sigma$, se obtiene

$$\left|\frac{f(n)}{n^s}\right| = \frac{|f(n)|}{n^\sigma} \leq \frac{|f(n)|}{n^{\sigma_0}}, \qquad \text{si } \sigma_0 \leq \sigma.$$

Por tanto, si la serie de Dirichlet converge absolutamente para $s_0 = \sigma_0 + it_0$, entonces converge también absolutamente para todo s tal que $\sigma \geq \sigma_0$. Esto da origen a la siguiente definición:

Definición 1.1.4. *Se llama abscisa de convergencia absoluta de la serie de Dirichlet $F(s)$ al número real*

$$\sigma_a = \text{ínf}\left\{\sigma \ : \sum_{n=1}^{\infty} \frac{f(n)}{n^\sigma} \ \textit{converge absolutamente}\right\}.$$

Se hace la convención de que $\sigma_a = -\infty$ si la serie converge absolutamente para todo $\sigma \in \mathbb{R}$, y $\sigma_a = +\infty$ si la serie no converge absolutamente para todo $\sigma \in \mathbb{R}$.

Dadas dos series de Dirichlet $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ y $G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$ absolutamente convergentes para $\sigma > \sigma_0$, se definen las siguientes operaciones:

- $F(s) + G(s) = \sum_{n=1}^{\infty} \frac{f(n)+g(n)}{n^s}$.
- $F(s)G(s) = \sum_{n=1}^{\infty} \frac{(f*g)(s)}{n^s}$.

Pero no solo el estudio de la convergencia absoluta en las series de Dirichlet es importante, y para estudiar la convergencia de una serie, surge de manera natural la siguiente definición:

Definición 1.1.5. *Se llama abscisa de convergencia de una serie de Dirichlet $F(s)$ al número real*

$$\sigma_c = \text{ínf}\left\{\sigma \ : \sum_{n=1}^{\infty} \frac{f(n)}{n^{\sigma}} \ \textit{converge}\right\}.$$

Gracias a la anterior definición, se sigue el siguiente teorema:

Teorema 1.1.6. *Una serie de Dirichlet converge uniformemente sobre cada subconjunto compacto contenido en el interior del semiplano de convergencia $\sigma > \sigma_c$.*

Además se tiene el siguiente teorema importante:

Teorema 1.1.7 (Fórmula generalizada de inversión de Möbius)**.** *Si α es completamente multiplicativa, se tiene que*

$$G(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right) \qquad \textit{si y solo si} \qquad F(x) = \sum_{n \leq x} \mu(n)\alpha(n) G\left(\frac{x}{n}\right).$$

Para un mayor estudio de las series de Dirichlet, se puede consultar por ejemplo [Apo76].

1.1.2. Algunos apartes de análisis complejo.

En la teoría de funciones analíticas, juega un papel importante el siguiente teorema de Weierstrass.

Teorema 1.1.8. *Sean $f_n(s)$ funciones analíticas en Ω_n. Si la sucesión $\{f_n\}$ converge a alguna función f en Ω uniformemente sobre los compactos de Ω, entonces $f(s)$ es analítica en Ω. Más aún, $f_n'(s)$ converge uniformemente a $f'(s)$ sobre cada compacto de Ω.*

Una demostración a este teorema se puede encontrar en [Ahl79].

Corolario 1.1.9. *Si $\{f_n(s)\}$ es una sucesión de funciones analíticas en G, y si la serie*

$$f(s) = \sum_{n=1}^{\infty} f_n(s),$$

converge uniformemente sobre cada compacto de G, entonces la función f es analítica en G y su derivada f', puede ser calculada derivando la serie término a término.

Un importante teorema que relaciona los ceros de un producto infinito es el siguiente:

Teorema 1.1.10. *Sean $a_1, a_2, \ldots$ una sucesión de números complejos con la condición de que $|a_1| \leq |a_2| \leq \cdots \leq |a_n| \leq \cdots$, y que $\lim_{n\to\infty} \frac{1}{|a_n|} = 0$. Entonces existe una función entera $G(s)$, que tiene por ceros sólo a los números a_n, ceros, con multiplicidad el número de veces que aparezca en la sucesión.*

El siguiente corolario es una consecuencia inmediata del anterior teorema:

Corolario 1.1.11. *Sea $a_1, a_2, \ldots$ una sucesión que satisface las condiciones del anterior teorema, entonces la función $G(s)$,*

$$G(s) = s^m \prod_{n=1}^{\infty} \left(1 - \frac{s}{a_n}\right) \exp\left(\frac{s}{a_n} + \frac{1}{2}(\frac{s}{a_n})^2 + \cdots + \frac{1}{n-1}(\frac{s}{a_n})^{n-1}\right),$$

es entera y tiene por ceros sólo a los números $0, a_1, a_2 \ldots$

Una demostración del teorema se puede encontrar en [Kar79].

Lema 1.1.12. *Sean $[a, b] \in \mathbb{R}$ y ϕ una función de variable compleja, continua sobre el espacio $\Omega \times [a, b]$ tal que para cada $t \in [a, b]$, $\phi(s, t)$ es analítica en Ω. Si $F(s) = \int_a^b \phi(s, t)dt$, entonces F es analítica en Ω y*

$$F'(s) = \int_a^b \frac{\partial \phi}{\partial s}.$$

Una demostración a esto se puede encontrar en las notas electrónicas del profesor R. Ash [AW04].

Teorema 1.1.13 (Identidad de Abel)**.** *Para cualquier función aritmética $a(n)$, sea $A(x) = \sum_{n \leq x} a(n)$, en donde $A(x) = 0$ si $x < 1$. Si f tiene derivada continua sobre el intervalo $[y, x]$, entonces se tiene*

$$\sum_{y < n \leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

Teorema 1.1.14 (Tauberiano de Shapiro)**.** *Sea $\{a(n)\}$ una sucesión no negativa tal que*

$$\sum_{n \leq x} \left[\frac{x}{n}\right] a(n) = x \log x + O(x),$$

para cada $x \geq 1$. Entonces

$$\sum_{n \leq x} \frac{a(n)}{n} = \log x + O(1).$$

La demostración de los últimos teoremas, se encuentra en [Apo76].

1.1.3. La función gamma de Euler $\Gamma(s)$

La función gamma de Euler $\Gamma(s)$, puede ser introducida desde distintos enfoques matemáticos, según sea el caso. Para nuestro interés, es de mayor utilidad la definición desde el punto de vista del análisis complejo, mediante el producto infinito.

Definición 1.1.15. *Se conoce como la constante de Euler a*

$$\gamma = \lim_{n \to \infty} \left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log(n)\right) = 0,57772157 \ldots$$

Esta constante, da origen a la función gamma $\Gamma(s)$, la cual está dada por la siguiente igualdad:

$$\frac{1}{\Gamma(s)} = s \exp(\gamma s) \prod_{n=1}^{\infty} \left(1 + \frac{s}{n}\right) e^{-\frac{s}{n}}.$$

La función $\Gamma(s)$ así definida, es una función analítica en todo el plano complejo, excepto en los puntos $s = 0, -1, -2, \ldots$, en donde tiene polos todos de orden 1, gracias al corolario 1.1.11.

Algunas de las propiedades más importantes de esta función son las siguientes:

1. $\Gamma(s) = \frac{1}{s} \prod_{n=1}^{\infty} \left(1 + \frac{1}{n}\right)^s \left(1 + \frac{s}{n}\right)^{-1}$.
2. $\Gamma(s) = \lim_{n\to\infty} \frac{1\cdot 2\cdots(n-1)n^s}{s(s+1)\cdots(s+n-1)}$.
3. $\Gamma(s+1) = s\Gamma(s)$.
4. Si $\mathrm{Re}(s) > 0$,
$$\Gamma(s) = \int_0^{\infty} e^{-u} u^{s-1} du. \tag{1.1}$$
5. $\Gamma(1/2) = \sqrt{\pi}$.

A la propiedad 3, se le conoce como la ecuación funcional de la función gamma de Euler.

Para el lector interesado, estas propiedades están demostradas en [Kar79].

1.2. La función zeta de Riemann

Definición 1.2.1. *Dada la función completamente multiplicativa $u(n)$, su serie de Dirichlet denotada por $\zeta(s)$ es*
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{u(n)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Observación 1.2.2. *$\zeta(s)$ es una función de variable compleja en el semiplano de $\mathbb{C}$ tal que $\sigma > 1$, y se llama la función zeta de Riemann. Además $\sigma_c = \sigma_a$.*

Demostración. Si $\sigma > 1$, sea $1 < \sigma_0 < \sigma$, luego,
$$|\zeta(s)| \leq \sum_{n=1}^{\infty} \frac{1}{|n^s|} \leq \sum_{n=1}^{\infty} \frac{1}{n^{\sigma_0}} \leq 1 + \int_1^{\infty} \frac{dx}{x^{\sigma_0}} = 1 + \frac{1}{\sigma_0 - 1}.$$
Así, cuando $\sigma > 1$, $\zeta(s)$ está bien definida como una función de variable compleja; además, al combinar el teorema 1.1.6 con el teorema 1.1.8 de Weierstrass, se concluye que es una función analítica en el semiplano $\mathrm{Re}(s) > 1$. □

Teorema 1.2.3 (Producto de Euler.)**.** *Para $\mathrm{Re}(s) > 1$ se tiene la siguiente igualdad:*
$$\zeta(s) = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1},$$
donde el producto recorre todos los números primos.

Demostración. Sea $x \geq 2$, se define

$$\zeta_x(s) = \prod_{p \leq x} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Además,

$$\left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{n=0}^{\infty} \frac{1}{p^{sn}}.$$

Por tanto, de la anterior igualdad se obtiene lo siguiente:

$$\zeta_x(s) = \prod_{p \leq x} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p \leq x} \sum_{n=0}^{\infty} \frac{1}{p^{ns}}.$$

Dado que $\sigma > 1$, se tiene $\left|\frac{1}{p^s}\right| < 1$, así que $\sum_{n=0}^{\infty} \frac{1}{p^{ns}}$ es una serie absolutamente convergente, de tal manera que se puede hacer la multiplicación término a término y se obtiene

$$\zeta_x(s) = \left(\sum_{m_1=0}^{\infty} \frac{1}{p_1^{m_1 s}}\right)\left(\sum_{m_2=0}^{\infty} \frac{1}{p_2^{m_2 s}}\right) \cdots \left(\sum_{m_k=0}^{\infty} \frac{1}{p_k^{m_k s}}\right) = \sum_{m_1=0}^{\infty} \sum_{m_2=0}^{\infty} \cdots \sum_{m_k=0}^{\infty} \frac{1}{\left(p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}\right)^s},$$

donde $2 = p_1 < p_2 < \cdots < p_k \leq x$, son los primos menores o iguales a x; por tanto se tiene la igualdad:

$$\zeta_x(s) = \sum_{n \leq x} \frac{1}{n^s} + \sum_{m \in T} \frac{1}{m^s},$$

en donde,

$$T = \{m \in \mathbb{N} : m > x \text{ y si } p \text{ es un primo tal que } p|m \text{ entonces } p \leq x\}. \tag{1.2}$$

La anterior igualdad, se da gracias a la factorización única de los números naturales en factores primos. Por otro lado,

$$\left|\sum_{m \in T} \frac{1}{m^s}\right| \leq \sum_{m \in T} \frac{1}{m^\sigma} < \sum_{m > x} \frac{1}{m^\sigma} \leq \frac{1}{x^\sigma} + \int_x^{\infty} \frac{du}{u^\sigma} = \frac{\sigma + 1}{\sigma - 1} x^{1-\sigma}, \tag{1.3}$$

luego,

$$\zeta_x(s) = \sum_{n \leq x} \frac{1}{n^s} + O\big(x^{1-\sigma}\big).$$

Dado que $\sigma > 1$, cuando se hace $x \to \infty$ se tiene que $x^{1-\sigma} \to 0$. Por tanto, al tomar el límite cuando $x \to \infty$ en la última igualdad se tiene

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \lim_{x \to \infty} \zeta_x(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s).$$

□

Un hecho importante en la demostración del anterior teorema, como se mencionó en su momento, es la descomposición única en factores primos de los números naturales. Este hecho es fundamental, como veremos en cápitulos posteriores.

Nuestro siguiente objetivo, es demostrar el siguiente teorema.

Teorema 1.2.4. *La función $\zeta(s)$ tiene una extensión holomorfa a $\mathbb{C} \setminus \{1\}$ la cual verifica la ecuación funcional*

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

Existen diferentes métodos para demostrar esta expresión (ver por ejemplo [Tit86]); aquí se presenta una demostración debida a Riemann, en la cual utiliza la sumación de Poisson de las series de Fourier para demostrar el siguiente lema. La demostración del lema, para efectos prácticos de nuestro trabajo, no hace un aporte significativo, de manera que, si alguien está interesado en ella, puede remitirse a [Kar79].

Lema 1.2.5. *Sean $\alpha \in \mathbb{R}$, y τ un número real positivo. Si $\theta(\tau, \alpha) = \sum_{-\infty}^{\infty} \exp\left(-\pi(n+\alpha)^2\tau\right)$, entonces*

$$\theta(1/\tau, \alpha) = \sqrt{\tau}\sum_{-\infty}^{\infty} \exp(-\pi n^2 x + 2\pi i n\alpha). \tag{1.4}$$

Demostración del teorema. Por la fórmula de la integral para la función Γ (ecuación (1.1)), se tiene que si $\mathrm{Re}(s) > 1$, entonces,

$$\Gamma\left(\frac{s}{2}\right) = \int_0^\infty e^{-u}u^{s/2-1}du = n^s\int_0^\infty e^{-\pi n^2 x}\pi^{s/2}x^{s/2-1}dx,$$

en donde se ha hecho el cambio de variable $u = \pi n^2 x$. Por tanto,

$$\pi^{-s/2}n^{-s}\Gamma(s/2) = \int_0^\infty e^{-\pi n^2 x}x^{s/2-1}dx;$$

de esta manera, se obtiene

$$\begin{aligned}
\pi^{-s/2}\Gamma(s/2)\zeta(s) &= \sum_{n=1}^{\infty}\int_0^\infty e^{-\pi n^2 x}x^{s/2-1}dx \\
&= \lim_{N\to\infty}\sum_{n=1}^{N}\int_0^\infty e^{-\pi n^2 x}x^{s/2-1}dx \\
&= \lim_{N\to\infty}\int_0^\infty x^{s/2-1}\left(\sum_{n=1}^{N} e^{-\pi n^2 x}\right)dx \\
&= \int_0^\infty x^{s/2-1}\theta_1(x)dx - \lim_{N\to\infty}\int_0^\infty x^{s/2-1}\left(\sum_{n>N} e^{-\pi n^2 x}\right)dx,
\end{aligned}$$

en donde $\theta_1(x) = \sum_{n=1}^{\infty} e^{-\pi n^2 x}$. Además, para todo $x > 0$ se tiene

$$\sum_{n>N} e^{-\pi n^2 x} < \int_N^\infty e^{-\pi u^2 x}du = \frac{1}{2\sqrt{\pi x}}\int_{\pi N^2 x}^\infty e^{-t}t^{-1/2}dt,$$

al utilizar el cambio de variable $t = \pi x u^2$; luego,

$$\sum_{n>N} e^{-\pi n^2 x} < \frac{1}{2\sqrt{\pi x}} \int_0^\infty e^{-t} t^{-1/2} = \frac{\Gamma(1/2)}{2\sqrt{\pi x}} = \frac{1}{2\sqrt{x}}.$$

Por otro lado,

$$\sum_{n>N} e^{-\pi n^2 x} < \sum_{n=(N+1)^2}^{\infty} e^{-\pi n x} \leq \int_{N^2}^\infty e^{-\pi u x} du = \int_{\pi x N^2}^\infty \frac{e^{-v}}{\pi x} dv = \frac{e^{-\pi x N^2}}{\pi x},$$

al hacer el cambio de variable $v = \pi x u$. Entonces

$$\begin{aligned}\left| \int_0^\infty x^{s/2-1} \Big(\sum_{n>N} e^{-\pi n^2 x} \Big) dx \right| &\leq \int_0^{1/N} \frac{x^{\sigma/2-1}}{2\sqrt{x}} dx + \int_{1/N}^\infty \frac{x^{\sigma/2-1} e^{-\pi x N^2}}{\pi x} dx \\ &= \frac{1}{2} \int_0^{1/N} x^{(\sigma-1)/2-1} dx + \frac{1}{\pi} \int_{1/N}^\infty x^{\sigma/2-2} e^{-\pi x N^2} dx,\end{aligned}$$

y al realizar el cambio de variable $u = \pi x N^2$ en la segunda integral, se obtiene

$$\begin{aligned}&= \frac{1}{\sigma-1} \left(\frac{1}{N} \right)^{\frac{\sigma-1}{2}} + \frac{1}{\pi} \int_{\pi N}^\infty \left(\frac{u}{\pi N} \right)^{\sigma/2-2} \frac{e^{-u}}{\pi N^2} du \\ &= \frac{1}{\sigma-1} \left(\frac{1}{N} \right)^{\frac{\sigma-1}{2}} + \frac{1}{\pi^{\sigma/2} N^{\sigma/2}} \int_{\pi N}^\infty u^{\sigma/2-2} e^{-u} du.\end{aligned}$$

Como $\pi N \leq u$, entonces $u^{-2} \leq (\pi N)^{-2}$, así se tiene la desigualdad,

$$\begin{aligned}&\leq \frac{1}{\sigma-1} \left(\frac{1}{N} \right)^{\frac{\sigma-1}{2}} + \pi^{-\sigma/2} N^{-\sigma/2} \int_{\pi N}^\infty (\pi N)^{-2} u^{\sigma/2} e^{-u} du \\ &= \frac{1}{\sigma-1} \left(\frac{1}{N} \right)^{\frac{\sigma-1}{2}} + \pi^{-2-\sigma/2} N^{-\sigma/2-2} \int_{\pi N}^\infty u^{\sigma/2} e^{-u} du \\ &\leq \frac{1}{\sigma-1} \left(\frac{1}{N} \right)^{\frac{\sigma-1}{2}} + \pi^{-2-\sigma/2} \left(\frac{1}{N} \right)^{\sigma/2+2} \Gamma\left(\frac{\sigma}{2} + 1 \right).\end{aligned}$$

De tal manera, se puede concluir por la última expresión, que

$$\lim_{N\to\infty} \int_0^\infty x^{s/2-1} \Big(\sum_{n>N} e^{-\pi x n^2} \Big) dx = 0,$$

y, por tanto, que

$$\pi^{-s/2} \Gamma(s/2) \zeta(s) = \int_0^\infty x^{s/2-1} \theta_1(x) dx. \tag{1.5}$$

Utilizando el lema 1.2.5 ($\alpha = 0$), se tiene que

$$2\theta_1(x) + 1 = \theta(x, 0) = x^{-1/2} \theta(1/x, 0) = x^{-1/2} (2\theta_1(1/x) + 1),$$

es decir,

$$\theta_1\left(\frac{1}{x} \right) = x^{1/2} \theta_1(x) + \frac{x^{1/2}}{2} - \frac{1}{2}, \tag{1.6}$$

luego,

$$\begin{aligned}\int_0^\infty x^{s/2-1}\theta_1(x)dx &= \int_0^1 x^{s/2-1}\theta_1(x)dx + \int_1^\infty x^{s/2-1}\theta_1(x)dx \\ &= -\int_1^\infty y^{1-s/2}\theta_1\left(\frac{1}{y}\right)\left(\frac{-1}{y^2}\right)dy + \int_1^\infty x^{s/2-1}\theta_1(x)dx\end{aligned}$$

al hacer el cambio $x = 1/y$ en la primera integral de la igualdad; por tanto, si se utiliza la ecuación (1.6) se tiene,

$$\begin{aligned}&= \int_1^\infty y^{-s/2-1}\theta_1(1/y)dy + \int_1^\infty x^{s/2-1}\theta_1(x)dx \\ &= \int_1^\infty x^{-s/2-1}x^{1/2}\theta_1(x)dx + \int_1^\infty x^{-s/2-1}\left(\frac{x^{1/2}}{2} - \frac{1}{2}\right)dx + \int_1^\infty x^{s/2-1}\theta_1(x)dx \\ &= \int_1^\infty \left(x^{-s/2-1/2} + x^{s/2-1}\right)\theta_1(x)dx + \int_1^\infty \frac{x^{-s/2-1/2}}{2}dx - \int_1^\infty \frac{x^{-s/2-1}}{2}dx \\ &= \int_1^\infty \left(x^{-s/2-1/2} + x^{s/2-1}\right)\theta_1(x)dx + \frac{1}{s-1} - \frac{1}{s} \\ &= \int_1^\infty \left(x^{-s/2-1/2} + x^{s/2-1}\right)\theta_1(x)dx + \frac{1}{s(s-1)}. \qquad (1.7)\end{aligned}$$

Como $\theta_1(x) = O(e^{-\pi x})$, el hecho de que la función $\int_1^\infty \left(x^{-s/2-1/2} + x^{s/2-1}\right)e^{-\pi x}dx$ sea entera, garantiza que $\int_1^\infty \left(x^{-s/2-1/2} + x^{s/2-1}\right)\theta_1(x)dx$ es convergente para cada $s \in \mathbb{C}$. Por consiguiente, se quiere ver que $\int_1^\infty \left(x^{-s/2-1/2} + x^{s/2-1}\right)e^{-\pi x}dx$ es entera.

Para demostrar esto, se toman las funciones $f_k(s) = \int_1^k x^{s/2-1}e^{-\pi x}dx$. Teniendo como referencia el lema 1.1.12, se toman como intervalo a $[1, k]$, y a $\phi(s, x) = x^{s/2-1}e^{-\pi x} = e^{(s/2-1)\ln x - \pi x}$. Como $x \geq 1$, $\phi(s, x)$ es continua en $\mathbb{C} \times [1, k]$, además para cada $x \in [1, k]$, se tiene que $\phi(s, x)$ es entera, por tanto se concluye que $f_k(s)$ es entera. De esta forma, se tiene $\{f_k(s)\}$, una sucesión de funciones enteras, y $\lim f_k(s) = \int_1^\infty \phi(s, t) = f(s)$. A continuación se ve que $f(s)$ es entera.

Sea $K \subset \mathbb{C}$, un subconjunto compacto, por tanto existe $\tau \in \mathbb{N}$, con $\tau = 2l$, tal que $K \subset B(0, \tau)$, así,

$$\begin{aligned}\left|\int_1^\infty x^{s/2-1}e^{-\pi x}dx - \int_1^k x^{s/2-1}e^{-\pi x}dx\right| &= \left|\int_k^\infty x^{s/2-1}e^{-\pi x}dx\right| \\ &\leq \int_k^\infty x^{l-1}e^{-\pi x}dx = L(l, k) \overset{k\to\infty}{\longrightarrow} 0.\end{aligned}$$

Por tanto, $\{f_k(s)\}$ converge uniformemente a $f(s)$ sobre cada subconjunto compacto de $\mathbb{C}$, luego, aplicando el teorema de Weierstrass, $f(s)$ es una función entera. De manera análoga, se tiene que $\int_1^\infty x^{-s/2-1/2}e^{-\pi x}dx$ también lo es, así se concluye que $\int_1^\infty (x^{s/2-1} + x^{-s/2-1/2})e^{-\pi x}dx$ es una función entera.

De esta manera, se garantiza que la función $\int_1^\infty (x^{s/2-1} + x^{-s/2-1/2})\theta_1(x)dx$ está bien definida para cada $s \in \mathbb{C}$. Mediante un razonamiento similar al anterior, se llega a que $\int_1^\infty x^{s/2-1}\theta_1(x)dx$ es entera, y por tanto que

$$\int_1^\infty \big(x^{s/2-1} + x^{-s/2-1/2}\big)\theta_1(x)dx$$

es una función entera.

Por tanto, si se pone

$$A(s) = \pi^{s/2}\Gamma^{-1}(s/2)\bigg(\frac{1}{s(s-1)} + \int_1^\infty (x^{-s/2-1/2} + x^{s/2-1})\theta_1(x)dx\bigg), \tag{1.8}$$

se tiene gracias a que Γ^{-1} es entera, y al anterior análisis, que $A(s)$ es una función analítica por lo menos en $\mathbb{C} \setminus \{0, 1\}$. Además, como Γ^{-1} tiene un cero simple en $s = 0$,

$$\begin{aligned}\lim_{s\to 0} A(s) &= \lim_{s\to 0}\left(\frac{\pi^{s/2}\Gamma^{-1}(s/2)}{s(s-1)} + \pi^{s/2}\Gamma^{-1}(s/2)\int_1^\infty (x^{-s/2-1/2} + x^{s/2-1})\theta_1(x)dx\right)\\ &= \lim_{s\to 0}\frac{\pi^{s/2}\Gamma^{-1}(s/2)}{s(s-1)} = \lim_{s\to 0}\frac{\pi^{s/2}e^{\gamma s/2}\prod\left(1-\frac{s}{2n}\right)^{-1}}{2(s-1)} = -1/2;\end{aligned}$$

pero como $\Gamma(1/2) = \sqrt{\pi}$, $\lim_{s\to 1} A(s) = \infty$. Luego $A(s)$ es una función analítica en $\mathbb{C}\setminus\{1\}$. Por otro lado, si $\mathrm{Re}(s) > 1$, se tiene que $A(s) = \zeta(s)$, por tanto $A(s)$ extiende analíticamente a la función $\zeta(s)$.

Si se escribe $1 - s$ en lugar de s, gracias a la ecuación (1.5) y a la ecuación (1.7), se obtiene lo siguiente:

$$\begin{aligned}\pi^{-(1-s)/2}\Gamma(\frac{1-s}{2})\zeta(1-s) &= \int_1^\infty (x^{-1/2(1-s+1)} + x^{1/2(1-s-2)}\theta_1(x)dx + \frac{1}{(1-s)(1-s-1)}\\ &= \int_1^\infty (x^{-1/2(-s+2)} + x^{1/2(-s-1)})\theta_1(x)dx + \frac{1}{s(s-1)}\\ &= \pi^{-s/2}\Gamma(s/2)\zeta(s).\end{aligned}$$

Con esto se demuestra lo querido en el teorema. A la ecuación

$$\pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s) = \pi^{-s/2}\Gamma(s/2)\zeta(s). \tag{1.9}$$

se le conoce como la ecuación funcional de la función $\zeta(s)$ zeta de Riemann. □

Observación 1.2.6. *La función $\zeta(s)$ tiene un polo simple en $s = 1$, cuyo residuo es 1.*

$$\begin{aligned}\lim_{s\to 1}(s-1)\zeta(s) &= \lim_{s\to 1}\left(\frac{\pi^{s/2}\Gamma^{-1}(s/2)}{s} + (s-1)\pi^{s/2}\Gamma^{-1}(s/2)\int_1^\infty (x^{-1/2(-s+2)} + x^{1/2(-s-1)})\theta_1(x)dx\right)\\ &= \lim_{s\to 1}\frac{\pi^{s/2}\Gamma^{-1}(s/2)}{s} = 1.\end{aligned}$$

Sea $\xi(s)$ definida de la siguiente manera:

$$\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s), \tag{1.10}$$

entonces $\xi(s)$ es una función entera y

$$\xi(s) = \xi(1-s), \tag{1.11}$$

como se ve mediante un cálculo directo.

1.3. La serie de los recíprocos de los primos.

Es de conocimiento general el hecho que la serie de los recíprocos de los números primos diverge. Ahora se va a estudiar el comportamiento asintótico que esta tiene, y obtener el resultado

$$\sum_{p\leq x}\frac{1}{p} \sim \log\log x.$$

La demostración de esto utiliza la identidad de Abel (Teorema 1.1.13); pero además de ello, se necesita el siguiente teorema.

Teorema 1.3.1. *Para cada $x \geq 1$ se tiene*

$$\sum_{p\leq x}\frac{\log p}{p} = \log x + O(1).$$

La demostración de este teorema, es una consecuencia lógica entre

$$\sum_{p\leq x}\left[\frac{x}{p}\right]\log p = x\log x + O(x),$$

cuya demostración puede encontrarse en el libro [Apo76, cap 3] y el teorema Tauberiano demostrado por Shapiro (Teorema 1.1.14).

Con estos resultados, se puede enunciar y demostrar nuestro próximo teorema.

Teorema 1.3.2. *Existe una constante A tal que*

$$\sum_{p\leq x}\frac{1}{p} = \log\log x + A + O\left(\frac{1}{\log x}\right)$$

para cada $x \geq 2$. De aquí, se deduce que $\sum_{p\leq x}\frac{1}{p} \sim \log\log x$.

Demostración. Sean

$$a(n) = \begin{cases} 1 & \text{si } n \text{ es primo} \\ 0 & \text{en otro caso} \end{cases}$$

y $A(x) = \sum_{p\leq x} \frac{\log p}{p}$. Entonces,

$$\sum_{p\leq x} \frac{1}{p} = \sum_{n\leq x} \frac{a(n)}{n} = \sum_{n\leq x} \frac{a(n)\log n}{n\log n},$$

por tanto, si se toma $\alpha(n) = \frac{a(n)\log n}{n}$ y $f(x) = \frac{1}{\log x}$ en la identidad de Abel (Teorema 1.1.13), dado que $A(t) = 0$ cuando $t < 2$, se tiene

$$\begin{aligned}\sum_{p\leq x} \frac{1}{p} &= \frac{A(x)}{\log x} - \int_1^x \frac{A(t)}{-t\log^2 t}dt \\ &= \frac{A(x)}{\log x} + \int_2^x \frac{A(t)}{t\log^2 t}dt.\end{aligned}$$

Del teorema 1.3.1 se tiene que $A(x) = \log x + R(x)$ donde $R(x) = O(1)$; entonces

$$\begin{aligned}\sum_{p\leq x} \frac{1}{p} &= \frac{\log x + R(x)}{\log x} + \int_2^x \frac{\log t + R(t)}{t\log^2 t}dt \\ &= 1 + \frac{R(x)}{\log x} + \int_2^x \frac{dt}{t\log t} + \int_2^x \frac{R(t)}{t\log^2 t}dt;\end{aligned}$$

pero $\int_2^x \frac{dt}{t\log t} = \log\log x - \log\log 2$ y

$$\int_2^x \frac{R(t)}{t\log^2 t}dt = \int_2^\infty \frac{R(t)}{t\log^2 t}dt - \int_x^\infty \frac{R(t)}{t\log^2 t}dt.$$

La integral impropia existe, pues $R(x) = O(1)$. Además,

$$\int_x^\infty \frac{R(t)}{t\log^2 t}dt = O\bigg(\int_x^\infty \frac{dt}{t\log^2 t}\bigg) = O\bigg(\frac{1}{\log x}\bigg),$$

cuando se hace el cambio $u = \log t$. Así,

$$\begin{aligned}\sum_{p\leq x} \frac{1}{p} &= 1 + O\bigg(\frac{1}{\log x}\bigg) + \log\log x - \log\log 2 + O\bigg(\frac{1}{\log x}\bigg) \\ &= \log\log x + A + O\bigg(\frac{1}{\log x}\bigg),\end{aligned}$$

cuando se hace $A = 1 - \log\log 2$. Por tanto, se obtiene el resultado querido, de donde se desprende fácilmente que

$$\sum_{p\leq x} \frac{1}{p} \sim \log\log x.$$

□

CAPÍTULO 2

Caracteres de Dirichlet y funciones L de Dirichlet.

En este capítulo se pretende dar una exposición de manera similar a la hecha en el anterior capítulo, sobre las funciones L de Dirichlet hasta presentar por último resultado, la ecuación funcional que ellas satisfacen.

2.1. Notas para el capítulo.

2.1.1. Caracteres de un grupo G.

Definición 2.1.1. *Un homomorfismo de un grupo abeliano finito G al grupo multiplicativo de los números complejos, se llama un carácter del grupo G, es decir, una función $f : G \to \mathbb{C}^*$ tal que*

$$f(ab) = f(a)f(b) \text{ para cada } a, b \in G.$$

El carácter f_0 tal que $f_0(a) = 1$ para cada $a \in G$, se llama el carácter principal del grupo G.

Observación 2.1.2. *Dado que $f(e) = 1$, en donde e es el elemento neutro del grupo G, $|f(a)| = 1$ para cada $a \in G$.*

Sea k el orden del grupo G, entonces

$$1 = f(e) = f(a^k) = f(a)^k.$$

Luego $f(a)$ es una raíz k-ésima de 1 para cada $a \in G$, de donde se sigue que $|f(a)| = 1$.

Teorema 2.1.3. *Sea $\tilde{G} = \{f : G \to \mathbb{C} \mid f \text{ es un carácter}\}$. Si se dota a $\tilde{G}$ con la operación $\cdot$ tal que $(f \cdot g)(a) = f(a)g(a)$, entonces $\tilde{G}$ es un grupo, en donde el inverso de f es $\overline{f}$, donde $\overline{f}(a) = \overline{f(a)}$. Su elemento neutro es f_0.*

El grupo $\tilde{G}$ se llama el grupo de los caracteres de G. Algunas de sus propiedades son las siguientes:

- Si G es cíclico, entonces también lo es $\tilde{G}$. Además tienen el mismo orden.

- Si $G \cong G_1 \times \cdots \times G_k$, entonces $\tilde{G} \cong \tilde{G}_1 \times \cdots \times \tilde{G}_k$.
- Si $a \in G$ es un elemento de orden m, entonces, para cada $f \in \tilde{G}$, se tiene que $f(a)$ es una raíz m-ésima de la unidad.

Lema 2.1.4 (Relaciones de ortogonalidad)**.** *Sea G un grupo abeliano finito, entonces*

1. $\sum_{a\in G} f(a) = 0$ *para cada* $f \neq f_0$.
2. $\sum_{f\in\tilde{G}} f(a) = 0$ *para cada* $a \in G$ *en donde* $a \neq e$.
3. $\sum_{a\in G} f_0(a) = |G| = \sum_{f\in\tilde{G}} f(e)$.

El lector interesado, puede entontrar la demostración de estas propiedades en los suplementos del libro [BS66].

Definición 2.1.5. *Un carácter numérico módulo k, es un carácter del grupo abeliano finito $(\mathbb{Z}/k\mathbb{Z})^*$.*

Un carácter numérico χ módulo k se llama primitivo, si para cada divisor d de k en donde $1 < d < k$, existe un entero $a \equiv 1 \pmod{d}$, con $(a, k) = 1$, tal que $\chi(a) \neq 1$. En caso contrario, decimos que el carácter χ no es primitivo.

Teorema 2.1.6. *Sea χ un carácter numérico módulo k, entonces χ no es primitivo si y solo si $\chi(a) = \chi(b)$ cada vez que $(a, k) = (b, k) = 1$ y $a \equiv b \pmod{d}$ para algún $d|k$ con $d > 1$.*

$\Rightarrow$. Como χ no es primitivo, existe algún divisor propio d de k tal que para cada $l \equiv 1 \pmod{d}$, entonces $\chi(l) = 1$. Además como $(a, k) = (b, k) = 1$ y $a \equiv b \pmod{d}$, entonces existe a' tal que $aa' \equiv 1 \pmod{k}$, y además $aa' \equiv ba' \pmod{d}$. Por tanto,

$$\chi(aa') = 1 = \chi(ba')$$

Como $\chi(a') \neq 0$, entonces se obtiene $\chi(a) = \chi(b)$.

Para el otro lado, es simplemente tomar $b = 1$. □

Observación 2.1.7. *Si χ es un carácter no primitivo módulo k, entonces restringido a $\left(\mathbb{Z}/d\mathbb{Z}\right)^*$, es un carácter numérico χ^* módulo d, en donde d es el número que existe en el anterior teorema. Se dice que χ^* induce al carácter χ, o χ es inducido por χ^*; es decir,*

$$\chi^*(m) = \chi(a)$$

para cada $m \in \left(\mathbb{Z}/d\mathbb{Z}\right)^*$, en donde a es un elemento que nos da el lema 2.1.8. Por el anterior teorema, la función χ^*, esta bien definida. O equivalentemente

$$\chi(m) = \begin{cases} \chi^*(m) & si \quad (m, k) = 1 \\ 0 & si \quad (m, k) > 1, \end{cases}$$

para cada $m \in \left(\mathbb{Z}/k\mathbb{Z}\right)^*$.

2.1.2. Un lema de teoría clásica de números.

Para hacer válida la anterior observación, se necesita de un lema, en donde el teorema chino de los restos juega un papel importante.

Lema 2.1.8. *Si $d|k$, entonces $a \in \left(\mathbb{Z}/d\mathbb{Z}\right)^*$ si, y solo si, existe $b \in \left(\mathbb{Z}/k\mathbb{Z}\right)^*$, tal que $a \equiv b$ (mód d).*

Demostración. Sea $k = dp_1^{\alpha_1} \cdots p_n^{\alpha_n}$, la descomposición de k, y sean $p_1, \cdots, p_i$ los primos que dividen a d, y $p_{i+1}, \cdots, p_k$ los primos que no están en la descomposición canónica de d. Por el teorema chino de los restos, el siguiente sistema tiene una solución:

$$\begin{array}{ll} x \equiv a & (\text{mód } d) \\ x \equiv 1 & (\text{mód } p_{i+1}) \\ \vdots & \\ x \equiv 1 & (\text{mód } p_n) \end{array}$$

Sea b la solución de ese sistema; la equivalencia $a \equiv b \pmod{d}$, es inmediata, lo único a verificar, es que $b \in \left(\mathbb{Z}/k\mathbb{Z}\right)^*$. Dado que $a \equiv b \pmod{d}$, y $(a,d) = 1$, entonces $(b,d) = 1$; además $(b, p_{i+1}) = \cdots = (b, p_n) = 1$. Entonces debido a la propiedad $(s,t) = 1$ y $(u,t) = 1$ se tiene que $(su,t) = 1$, se obtiene que $(b,k) = 1$, con lo cual queda demostrado el lema.

El resultado recíproco, es inmediato. □

2.2. Caracteres de Dirichlet.

Definición 2.2.1. *Dado un carácter numérico χ módulo k, χ se puede extender a $\mathbb{Z}$ mediante:*

$$\chi(a) = \begin{cases} \chi(a) & si\ (k,a) = 1 \\ 0 & si\ (k,a) \neq 1. \end{cases}$$

La extensión de χ así definida, se llama un carácter de Dirichlet módulo k. Por otro lado, el carácter de Dirichlet correspondiente al carácter númerico χ_0, se le conoce como el carácter principal de Dirichlet módulo k.

2.2.1. Propiedades de los caracteres de Dirichlet.

Observación 2.2.2 (Propiedades)**.** *Sea χ un carácter de Dirichlet módulo k, entonces:*

1. $\chi(a) = 0$ si y solo si $(a,k) > 1$.
2. $\chi(a) = \chi(b)$ si $a \equiv b \pmod{k}$.
3. $\chi(ab) = \chi(a)\chi(b)$ para cada $a, b \in \mathbb{Z}$.

4.
$$\sum_{a\in\mathbb{Z}/k\mathbb{Z}} \chi(a) = \begin{cases} \phi(k) & si\ \chi = \chi_0 \\ 0 & si\ \chi \neq \chi_0. \end{cases}$$

5.
$$\sum_{\chi\in\widetilde{\mathbb{Z}/k\mathbb{Z}}} \chi(a) = \begin{cases} \phi(k) & si\ a = e \\ 0 & si\ a \neq e. \end{cases}$$

Las propiedades $1-3$ son de fácil verificación, pero lo más importante de esas propiedades, es que ellas caracterizan completamente los caracteres de Dirichlet módulo k. En efecto; si $\eta : \mathbb{Z} \to \mathbb{C}^*$ cumple las condiciones $1-3$, para cada $\overline{a} \in (\mathbb{Z}/k\mathbb{Z})^*$, hagamos

$$\chi(\overline{a}) = \eta(a).$$

Por la condición 2, χ no depende de la elección de a, ademas $\chi(\overline{a}) \neq 0$ por la condición 1, también, si $(a,k) = (b,k) = 1$, por la condición 3, dado que $(ab,k) = 1$, entonces

$$\chi(\overline{a}\overline{b}) = \chi(\overline{ab}) = \eta(ab) = \eta(a)\eta(b) = \chi(\overline{a})\chi(\overline{b}).$$

Por tanto, χ es un carácter numérico módulo k, y así el correspondiente carácter de Dirichlet χ coincide con la función η; por tanto η es un carácter de Dirichlet módulo k.

Las propiedades 4 y 5, se deducen directamente del lema 2.1.4, y del hecho que $\chi(a) = 0$ si y solo si $(a,k) > 1$, si y solo si $a \notin (\mathbb{Z}/k\mathbb{Z})^*$; por tanto, los términos que hay de más en la suma, son términos nulos.

Adicionalmente, se tiene la siguiente relación de ortogonalidad:

Proposición 2.2.3 (Relación de ortogonalidad)**.** *Sean $\chi_0, \chi_2, \ldots, \chi_{\phi(k)}$ los diferentes caracteres módulo k, y sean m, n dos enteros tales que $(k,n) = 1$, entonces*

$$\sum_{r=1}^{\phi(k)} \chi_r(m)\overline{\chi}_r(n) = \begin{cases} \phi(k) & si\ m \equiv n \pmod{k} \\ 0 & si\ m \not\equiv n \pmod{k}. \end{cases}$$

Un carácter del cual se hablará con frecuencia, es el generado por el simbolo de Kronecker $\left(\frac{a}{b}\right)$. El carácter $\chi_k \pmod{k}$ se define como

$$\chi_k(n) = \left(\frac{k}{n}\right).$$

2.3. Funciones L de Dirichlet.

Definición 2.3.1. *Para χ un carácter de Dirichlet módulo k, se define la función L de Dirichlet asociada al carácter de Dirichlet χ, como la serie de Dirichlet asociada a la función completamente multiplicativa χ, es decir;*

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

donde $s \in \mathbb{C}$, *y* $\sigma > 1$.

Algunas propiedades que se necesitarán en capítulos más adelante (cuyas demostraciones pueden ser encontradas en [Apo76]) son las siguientes:

Si χ es un carácter no principal y $x > 1$, entonces:

$$\sum_{n \leq x} \frac{\chi(n)}{n} = L(1, \chi) + O\left(\frac{1}{x}\right) \tag{2.1}$$

$$\sum_{n \leq x} \frac{\chi(n) \log n}{n} = -L'(1, \chi) + O\left(\frac{\log x}{x}\right). \tag{2.2}$$

Dirichlet estudió estas funciones como funciones de variable real, pero después de los estudios realizados por Riemann a su función zeta como función de variable compleja, se realizó el mismo trabajo a las funciones L de Dirichlet, y se obtuvieron resultados análogos como el siguiente:

Teorema 2.3.2. *$L(s, \chi)$ es una función analítica y satisface el producto de Euler:*

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}. \tag{2.3}$$

Demostración. La analiticidad de la función es inmediata gracias a su definición, por tanto, se verifica sólo el producto de Euler. Sea $L_x(s) = \prod_{p \leq x} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$, se observa la siguiente igualdad: $\left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \sum_{n=0}^{\infty} \frac{\chi(p)^n}{p^{ns}}$.

Gracias a que esta última serie converge uniformemente y $\chi(p)$ es una función completamente multiplicativa, se puede realizar la multiplicación término a término, y obtener:

$$L_x(s) = \prod_{p \leq x} \sum_{n=0}^{\infty} \frac{\chi(p^n)}{p^{ns}} = \sum_{n \leq x} \frac{\chi(n)}{n^s} + \sum_{m \in T} \frac{\chi(m)}{m^s},$$

en donde T es el conjunto descrito en la ecuación (1.2). Se observa nuevamente el papel que juega en esta demostración la descomposición única de los números naturales en factores primos. Además, como

$$\left| \sum_{m \in T} \frac{\chi(m)}{m^s} \right| < \sum_{m \in T} \frac{1}{m^s};$$

al hacer el mismo razonamiento que se hizo en la ecuación (1.3), y tomar el límite de x hacia el infinito, se obtiene:

$$\prod_p \left(1 - \frac{\chi(p)}{p}\right)^{-1} = \lim_{x \to \infty} L_x(s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

tal como se queria. □

Observación 2.3.3. *Dado que el anterior resultado es válido para cualquier carácter de Dirichlet, al tomar el carácter principal módulo k, se tiene la siguiente igualdad:*

$$L(s,\chi_0) = \zeta(s)\prod_{p|k}\left(1-\frac{1}{p^s}\right), \tag{2.4}$$

en donde $\zeta(s)$ es la función zeta de Riemann.

Proposición 2.3.4. *$L(s,\chi_0)$ es una función analítica en $\mathbb{C}\setminus\{1\}$, y en $s=1$, posee un polo simple cuyo residuo es*

$$\prod_{p|k}\left(1-\frac{1}{p}\right) = \phi(k).$$

La demostración de esta proposición es consecuencia inmediata de la ecuación (2.4) y la Observación 1.2.6.

Pero un resultado análogo se puede demostrar para $\chi \neq \chi_0$, solo que para ello el camino a recorrer es un poco más extenso. Se necesita primero hablar de las sumas de Gauss, y por tanto, de caracteres primitivos. Una vez se tenga demostrado el resultado para los caracteres primitivos, se puede extender a cuaquier carácter $\chi \neq \chi_0$ módulo k, gracias al siguiente lema:

Lema 2.3.5. *Sea χ^* un carácter primitivo modulo k_1, y χ un carácter inducido por χ^* módulo k, entonces para* $\operatorname{Re} s > 1$ *se tiene:*

$$L(s,\chi) = L(s,\chi^*)\prod_{\substack{p|k\\ p\nmid k_1}}\left(1-\frac{\chi^*(p)}{p^s}\right).$$

Demostración. Como $\chi(p)=0$ y $\chi^*(p)\neq 0$ si y sólo si $p|k$ y $p\nmid k_1$, debido a la observación 2.1.7, y a la ecuación (2.3), se tiene

$$L(s,\chi) = \prod_p\left(1-\frac{\chi(p)}{p^s}\right)^{-1} = \prod_p\left(1-\frac{\chi^*(p)}{p^s}\right)^{-1}\prod_{\substack{p|k\\ p\nmid k_1}}\left(1-\frac{\chi^*(p)}{p^s}\right) = L(s,\chi^*)\prod_{\substack{p|k\\ p\nmid k_1}}\left(1-\frac{\chi^*(p)}{p^s}\right),$$

con lo cual queda demostrado el lema. □

2.3.1. Sumas de Gauss.

Ahora, se va a hablar de las sumas de Gauss, las cuales juegan un importante papel en el transcurso de la parte final de esta sección para llegar al objetivo que se quiere, que es la continuación analítica de las funciones L de Dirichlet.

Definición 2.3.6. *Dado χ un carácter módulo k, se define por la siguiente igualdad la suma de Gauss asociada al carácter χ:*

$$G(n,\chi) = \sum_{m=1}^{k}\chi(m)e^{\frac{2\pi i n m}{k}}.$$

Lema 2.3.7. *Si χ es un carácter primitivo módulo k, entonces*

$$G(1,\chi)\overline{\chi}(n) = G(n,\chi)$$

para cada $n \in (\mathbb{Z}/k\mathbb{Z})^*$.

Demostración. Dado que $(n,k) = 1$, entonces el conjunto $\{nm \mid m \in (\mathbb{Z}/k\mathbb{Z})^*\}$, es un sistema reducido de residuos módulo k, por tanto, debido a que $\chi(m) = \overline{\chi}(n)\chi(nm)$, pues $\chi(n)\overline{\chi}(n) = 1$, se tiene:

$$\begin{aligned} G(n,\chi) &= \sum_{m=1}^{k} \chi(m) e^{\frac{2\pi i n m}{k}} = \sum_{(m,k)=1} \chi(m) e^{\frac{2\pi i n m}{k}} = \sum_{(nm,k)=1} \overline{\chi}(n)\chi(nm) e^{\frac{2\pi i n m}{k}} \\ &= \overline{\chi}(n) \sum_{(r,k)=1} \chi(r) e^{\frac{2\pi i r}{k}} = \overline{\chi}(n) G(1,\chi). \end{aligned}$$

□

Observación 2.3.8. *Si χ es un carácter primitivo módulo k, entonces*

$$|G(1,\chi)|^2 = k.$$

Demostración.

$$\begin{aligned} |G(1,\chi)|^2 = G(1,\chi)\overline{G(1,\chi)} &= G(1,\chi) \sum_{n=1}^{k} \overline{\chi}(n) e^{-\frac{2\pi i n}{k}} = \sum_{n=1}^{k} G(n,\chi) e^{-\frac{2\pi i n}{k}} \\ &= \sum_{n=1}^{k} \sum_{m=1}^{k} \chi(m) e^{\frac{2\pi i m n}{k} - \frac{2\pi i n}{k}} = \sum_{n=1}^{k} \sum_{m=1}^{k} \chi(m) e^{\frac{2\pi i n}{k}(m-1)} \\ &= \chi(1)k + \sum_{m=1}^{k-1} \chi(m+1) \sum_{n=1}^{k} e^{\frac{2\pi i n m}{k}}; \end{aligned}$$

pero

$$\sum_{n=1}^{k} e^{\frac{2\pi i n m}{k}} = \sum_{n=0}^{k-1} e^{\frac{2\pi i n m}{k}} = \left(\frac{e^{2\pi i m} - 1}{e^{(2\pi i m/k)} - 1} \right).$$

Como $m \in \mathbb{N}$, entonces $e^{2\pi i m} = \cos(2\pi m) + i \sin(2\pi m) = 1$, de donde se concluye que

$$\sum_{n=1}^{k} e^{\frac{2\pi i n m}{k}} = 0.$$

De esto, se tiene que

$$|G(1,\chi)|^2 = k\chi(1) = k.$$

□

Dado que los caracteres módulo k son completamente multiplicativos, se tiene

$$\chi^2(-1) = 1;$$

es decir, $\chi(-1) = \pm 1$. Por tanto, surge de manera natural la siguiente definición:

Definición 2.3.9. *Sea χ un carácter módulo k tal que $\chi(-1) = 1$, entonces χ se llama un carácter par; en caso contrario, $\chi(-1) = -1$, se llama un carácter impar.*

Observación 2.3.10. *Si χ es un carácter primitivo par, entonces*

$$G(1, \overline{\chi}) = \overline{G(1, \chi)}; \tag{2.5}$$

mientras que si χ es impar,

$$-G(1, \overline{\chi}) = \overline{G(1, \chi)}. \tag{2.6}$$

Esto se sigue de manera inmediata del lema 2.3.7 y de la anterior definición.

2.3.2. Ecuación funcional.

Antes de demostrar la ecuación funcional, se necesita de un lema adicional, análogo al lema 1.2.5 que se utilizó en el caso de la función zeta de Riemann.

Lema 2.3.11. *Sea χ un carácter primitivo módulo k. Se define $\theta(x, \chi)$ por*

$$\theta(x, \chi) = \sum_{-\infty}^{\infty} \chi(n) e^{-\frac{\pi n^2 x}{k}} \quad \textit{para } x > 0,$$

y $\theta_1(x, \chi)$ por

$$\theta_1(x, \chi) = \sum_{-\infty}^{\infty} n\chi(n) e^{-\frac{\pi n^2 x}{k}} \quad \textit{para } x > 0.$$

Entonces se cumplen las siguientes relaciones:

$$G(1, \overline{\chi})\theta(x, \chi) = \sqrt{\frac{k}{x}}\theta(1/x, \overline{\chi}), \tag{2.7}$$

$$G(1, \overline{\chi})\theta_1(x, \chi) = i\sqrt{\frac{k}{x^3}}\theta_1(1/x, \overline{\chi}). \tag{2.8}$$

Demostración. Primero, se va a demostrar la ecuación (2.7).

$$\begin{aligned} G(1, \overline{\chi})\theta(x, \chi) &= G(1, \overline{\chi}) \sum_{n=-\infty}^{\infty} \chi(n) e^{-\frac{\pi n^2 x}{k}} = \sum_{n=-\infty}^{\infty} G(n, \overline{\chi}) e^{-\frac{\pi n^2 x}{k}} \\ &= \sum_{n=-\infty}^{\infty} \sum_{m=1}^{k} \overline{\chi}(m) e^{\frac{2\pi i n m}{k} - \frac{\pi n^2 x}{k}}. \end{aligned}$$

Por el lema 1.2.5, si se hace $\alpha = n/k$, y $\tau = x/k$, se obtiene de la última igualdad que

$$\begin{aligned} G(1, \overline{\chi})\theta(x, \chi) &= \sum_{m=1}^{k} \overline{\chi}(m) \sqrt{\frac{k}{x}} \sum_{n=-\infty}^{\infty} e^{-\frac{\pi(kn+m)^2}{kx}} \\ &= \sqrt{\frac{k}{x}} \left(\overline{\chi}(1) \sum_{\substack{n \in \mathbb{Z} \\ n \equiv 1 \mod k}} e^{-\frac{\pi n^2}{kx}} + \overline{\chi}(2) \sum_{\substack{n \in \mathbb{Z} \\ n \equiv 2 \mod k}} e^{-\frac{\pi n^2}{kx}} + \cdots + \overline{\chi}(k) \sum_{\substack{n \in \mathbb{Z} \\ n \equiv 0 \mod k}} e^{-\frac{\pi n^2}{kx}} \right). \end{aligned}$$

Dado que $\chi(a) = \chi(b)$ si $a \equiv b \pmod{k}$, se tiene

$$\begin{aligned} G(1,\overline{\chi})\theta(x,\chi) &= \sqrt{\frac{k}{x}}\Bigg(\sum_{\substack{n\in\mathbb{Z} \\ n\equiv 1 \mod k}} \overline{\chi}(n)e^{-\frac{\pi n^2}{kx}} + \cdots + \sum_{\substack{n\in\mathbb{Z} \\ n\equiv 0 \mod k}} \overline{\chi}(n)e^{-\frac{\pi n^2}{kx}} \Bigg) \\ &= \sqrt{\frac{k}{x}} \sum_{n=-\infty}^{\infty} \overline{\chi}(n)e^{-\frac{\pi n^2}{kx}} = \sqrt{\frac{k}{x}}\theta(1/x,\overline{\chi}). \end{aligned} \tag{2.9}$$

Para demostrar la otra igualdad, se deriva término a término la ecuación (1.4) con respecto a α, y se obtiene:

$$\frac{i}{\sqrt{\tau^3}} \sum_{n=-\infty}^{\infty} (n+\alpha)e^{-\frac{\pi(n+\alpha)^2}{\tau}} = \sum_{n=-\infty}^{\infty} ne^{-\pi n^2\tau + 2\pi i n\alpha}.$$

Al reemplazar τ por x/k, y α por m/k, se tiene:

$$i\sqrt{\frac{k}{x^3}} \sum_{n=-\infty}^{\infty} (kn+m)e^{-\frac{\pi(kn+m)^2}{kx}} = \sum_{n=-\infty}^{\infty} ne^{-\frac{\pi n^2 x}{k} + \frac{2\pi i n m}{k}}. \tag{2.10}$$

Por tanto

$$\begin{aligned} G(1,\overline{\chi})\theta_1(x,\chi) &= G(1,\overline{\chi}) \sum_{n=-\infty}^{\infty} n\chi(n)e^{-\frac{\pi n^2 x}{k}} = \sum_{n=-\infty}^{\infty} nG(n,\overline{\chi})e^{-\frac{\pi n^2 x}{k}} \\ &= \sum_{m=1}^{k} \sum_{n=-\infty}^{\infty} n\overline{\chi}(m)e^{\frac{2\pi i n m}{k} - \frac{\pi n^2 x}{k}}. \end{aligned}$$

Al utilizar la ecuación (2.10) en esta parte, nos queda:

$$\begin{aligned} G(1,\overline{\chi})\theta_1(x,\chi) &= \sum_{m=1}^{k} \overline{\chi}(m) i\sqrt{\frac{k}{x^3}} \sum_{n=-\infty}^{\infty} (kn+m)e^{-\frac{\pi(kn+m)^2}{kx}} \\ &= i\sqrt{\frac{k}{x^3}} \sum_{m=1}^{k} \overline{\chi}(m) \sum_{n=-\infty}^{\infty} (kn+m)e^{-\frac{\pi(kn+m)^2}{kx}}. \end{aligned}$$

Al hacer el mismo procedimiento que se realizó en la ecuación (2.9), se obtiene

$$\begin{aligned} G(1,\overline{\chi})\theta_1(x,\chi) &= i\sqrt{\frac{k}{x^3}} \sum_{n=-\infty}^{\infty} n\overline{\chi}(n)e^{-\frac{\pi n^2}{kx}} \\ &= i\sqrt{\frac{k}{x^3}}\theta_1(1/x,\overline{\chi}). \end{aligned}$$

De esta manera, queda demostrado el lema. □

Con las herramientas que se han construido hasta el momento, se puede ahora enunciar uno de los importantes teoremas en la teoría de las funciones L de Dirichlet, como lo es la continuación analítica a $\mathbb{C}$.

Teorema 2.3.12. *Sea χ un carácter primitivo módulo k. Entonces la función $L(s,\chi)$ puede extenderse analíticamente a todo el plano complejo.*

Demostración. La demostración del teorema, será dividida en dos partes, es decir, se tratarán los casos por separado de un carácter primitivo par, y el de un carácter primitivo impar. Para la primera parte, se supone entonces que $\chi(-1) = 1$.

Por la ecuación de la integral para la función Γ, al hacer la sustitución $u = \pi n^2 x/k$, se obtiene

$$n^{-s}\pi^{-s/2}k^{s/2}\Gamma(s/2) = \int_0^\infty x^{s/2-1}e^{-\frac{\pi n^2 x}{k}}dx.$$

De esta manera, al multiplicar por $\chi(n)$, y hacer la suma sobre los naturales, se obtiene para $\mathrm{Re}(s) > 1$:

$$L(s,\chi)\pi^{-s/2}k^{s/2}\Gamma(s/2) = \int_0^\infty x^{s/2-1}\left(\sum_{n=1}^\infty \chi(n)e^{-\frac{\pi n^2 x}{k}}\right)dx.$$

El cambio de la integral con la suma, se justifica de manera similar a la forma en que se hizo con la función zeta de Riemann. Dado que

$$\theta(x,\chi) = 2\sum_{n=1}^\infty \chi(n)e^{-\frac{\pi n^2 x}{k}},$$

se tiene que

$$\begin{aligned} L(s,\chi)\pi^{-s/2}k^{s/2}\Gamma(s/2) &= \frac{1}{2}\int_0^\infty x^{s/2-1}\theta(x,\chi)dx \\ &= \frac{1}{2}\int_1^\infty x^{-s/2-1}\theta(1/x,\chi)dx + \frac{1}{2}\int_1^\infty x^{s/2-1}\theta(x,\chi)dx. \end{aligned}$$

La última línea es válida, después de partir la integral en dos; la primera se toma de 0 a 1, y luego se hace el cambio de variable $x = 1/y$. La segunda de 1 a ∞. Por la ecuación (2.7), se tiene entonces

$$\begin{aligned} L(s,\chi)\pi^{-s/2}k^{s/2}\Gamma(s/2) &= \frac{1}{2}\int_1^\infty x^{-s/2-1}\sqrt{\frac{x}{k}}G(1,\chi)\theta(x,\overline{\chi})dx + \frac{1}{2}\int_1^\infty x^{s/2-1}\theta(x,\chi)dx \\ &= \frac{G(1,\chi)}{2\sqrt{k}}\int_1^\infty x^{-s/2-1/2}\theta(x,\overline{\chi})dx + \frac{1}{2}\int_1^\infty x^{s/2-1}\theta(x,\chi)dx. \end{aligned}$$

Dado que χ es un carácter par, por la ecuación (2.5) y la observación 2.3.8, se tiene

$$L(s,\chi)\left(\frac{\pi}{k}\right)^{-s/2}\Gamma(s/2) = \frac{\sqrt{k}}{2G(1,\overline{\chi})}\int_1^\infty x^{-s/2-1/2}\theta(x,\overline{\chi})dx + \frac{1}{2}\int_1^\infty x^{s/2-1}\theta(x,\chi)dx. \tag{2.11}$$

Si ahora se toma $\chi(-1) = -1$, entonces

$$\pi^{-\frac{s+1}{2}}k^{\frac{s+1}{2}}\Gamma\left(\frac{s+1}{2}\right)n^{-s} = \int_0^\infty ne^{-\frac{\pi n^2 x}{k}}x^{s/2-1/2}dx.$$

Por tanto, para $\mathrm{Re}(s) > 1$, se tiene

$$\begin{aligned} L(s,\chi)\pi^{-\frac{s+1}{2}}k^{\frac{s+1}{2}}\Gamma\left(\frac{s+1}{2}\right) &= \int_0^\infty x^{s/2-1/2}\left(\sum_{n=-\infty}^{\infty} n\chi(n)e^{-\frac{\pi n^2 x}{k}}\right)dx = \frac{1}{2}\int_0^\infty x^{s/2-1/2}\theta_1(x,\chi)dx \\ &= \frac{1}{2}\int_1^\infty x^{-s/2-3/2}\theta_1(1/x,\chi)dx + \frac{1}{2}\int_1^\infty x^{s/2-1/2}\theta_1(x,\chi)dx \\ &= \frac{1}{2}\int_1^\infty x^{-s/2-3/2}\frac{G(1,\chi)x^{3/2}}{i\sqrt{k}}\theta_1(x,\overline{\chi})dx + \frac{1}{2}\int_1^\infty x^{s/2-1/2}\theta_1(x,\chi)dx \\ &= \frac{G(1,\chi)}{2i\sqrt{k}}\int_1^\infty x^{-s/2}\theta_1(x,\overline{\chi})dx + \frac{1}{2}\int_1^\infty x^{s/2-1/2}\theta_1(x,\chi)dx. \end{aligned}$$

Debido a que χ es un carácter impar, por la ecuación (2.6) y la observación 2.3.8, se tiene:

$$L(s,\chi)\left(\frac{\pi}{k}\right)^{-\frac{s+1}{2}}\Gamma\left(\frac{s+1}{2}\right) = \frac{\sqrt{k}}{-2iG(1,\overline{\chi})}\int_1^\infty x^{-s/2}\theta_1(x,\overline{\chi})dx + \frac{1}{2}\int_1^\infty x^{s/2-1/2}\theta_1(x,\chi)dx. \tag{2.12}$$

De manera análoga al caso de la función zeta de Riemann, se muestra que las integrales involucradas en las ecuaciones (2.11) y (2.12), son funciones enteras. Por tanto, se ha conseguido demostrar, que para cualquier carácter primitivo χ módulo k, la función $L(s,\chi)$ puede extenderse analíticamente sobre $\mathbb{C}$. □

Observación 2.3.13. *Por el lema 2.3.5, el anterior resultado es válido para cualquier carácter $\chi \neq \chi_0$ módulo k. Es decir, si $\chi \neq \chi_0$ es un carácter módulo k, la función $L(s,\chi)$ es una función entera.*

Gracias a la similitud de las ecuaciones (2.11) y (2.12), se puede hablar de la función $\xi(s,\chi)$, y su ecuación funcional, como se verá a continuación.

Teorema 2.3.14 (Ecuación Funcional)**.** *Sean χ un carácter primitivo módulo k, y*

$$\delta = \begin{cases} 0 & si \quad \chi(-1) = 1 \\ 1 & si \quad \chi(-1) = -1, \end{cases}$$

$$\xi(s,\chi) = \left(\frac{\pi}{k}\right)^{-\frac{s+\delta}{2}}\Gamma\left(\frac{s+\delta}{2}\right)L(s,\chi).$$

Entonces

$$\xi(1-s,\overline{\chi}) = \frac{i^\delta\sqrt{k}}{G(1,\chi)}\xi(s,\chi).$$

Demostración. La demostración es inmediata, al reemplazar s por $1-s$, y χ por $\overline{\chi}$ en las ecuaciones (2.11) y (2.12). □

CAPÍTULO 3

La fórmula del número de clases de Dirichlet.

En este capítulo se va a relacionar un concepto analítico, como es el número de clases de formas de discriminante d, con un concepto algebraico como es el número de clases de ideales del anillo de enteros $\mathcal{O}_K = \mathbb{A} \cap \mathbb{Q}(\sqrt{\Delta})$, en donde Δ es un entero libre de cuadrados y $\mathbb{A}$ es el conjunto de enteros algebraicos. Los números Δ y d se relacionan por la siguiente igualdad:

$$d = \begin{cases} 4\Delta & \text{si } \Delta \equiv 2, 3 \pmod 4 \\ \Delta & \text{si } \Delta \equiv 1 \pmod 4. \end{cases}$$

La primera parte se basa principalmente en los trabajos que realizó Dirichlet a las formas binarias cuadráticas.

3.1. Notas para el capítulo.

Teorema 3.1.1 (La ecuación de Pell)**.** *Si $d > 0$, existe $1 < \epsilon = x_0 + y_0\sqrt{d}$ tal que cualquier solución de la ecuación*

$$x^2 - dy^2 = 1$$

puede obtenerse como $\pm\epsilon^n$, en donde $n = \pm 1 \pm 2 \pm 3 \ldots$. Esta solución ϵ se llama la solución fundamental de la ecuación de Pell.

3.2. Formas cuadráticas de discriminante d. Finitud del número de clases.

Definición 3.2.1. *Una forma cuadrática binaria es un polinomio homogéneo $f(x, y)$ de grado 2 con coeficientes enteros; es decir, un polinomio que tiene la siguiente forma:*

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

En el estudio general se excluyen aquellas formas que se pueden factorizar, por lo cual se supone que $a \neq 0$ y $c \neq 0$. Por tanto,

$$\begin{aligned} ax^2+bxy+cy^2 &= \tfrac{1}{a}\Big(a^2x^2+abxy+acy^2\Big) \\ &= \tfrac{1}{a}\Big[\big(ax+b/2y\big)^2-\big(b^2/4-ac\big)y^2\Big]. \end{aligned}$$

Si $b^2/4-ac$ es un cuadrado perfecto entonces la forma se puede factorizar en factores lineales; por tanto se supone que $d/4=b^2/4-ac$ no es cuadrado perfecto; d se llama el discriminante de la forma cuadrática. Se observa fácilmente que $d\equiv 0$ o $d\equiv 1 \pmod 4$.

Además si d es de esta forma, entonces hay una forma cuadrática cuyo discriminante es d, es decir:

$$f(x,y)=\begin{cases} x^2-\frac{d}{4}y^2 & \text{si } d\equiv 0 \pmod 4 \\ x^2+xy-\frac{d-1}{4}y^2 & \text{si } d\equiv 1 \pmod 4. \end{cases}$$

Hay una importante distinción que hacer entre las formas de discriminante positivo y aquellas cuyo discriminante es negativo. Sea $f(x,y)=ax^2+bxy+cy^2$ una forma de discriminante negativo, entonces:

$$\begin{aligned} 4af(x,y) &= 4a^2x^2+4abxy+4acy^2 \\ &= (2ax+by)^2+(4ac-b^2)y^2, \end{aligned}$$

de modo que la última expresión siempre es positiva, y es cero solo cuando $x=y=0$. Por tanto, dos números distintos que sean representados por la forma deben tener el mismo signo. En este caso la forma se dice positiva si $a>0$ o negativa en caso contrario.

Observación 3.2.2. *Si $g(x,y)$ es una forma cuadrática negativa, entonces $-g(x,y)$ es una forma cuadrática positiva y además las dos tienen el mismo discriminante, por tanto, las formas a considerar cuando $d<0$ son formas positivas, a menos que se mencione lo contrario.*

Si se considera ahora una forma $f(x,y)$ con discriminante positivo, entonces se tiene:

$$\begin{aligned} 4af(x,y) &= (2ax+by)^2-dy^2 \\ &= (2ax+by-\sqrt{d}y)(2ax+by+\sqrt{d}y) \\ &= 4a^2y^2(x/y-\phi)(x/y-\psi), \end{aligned}$$

donde $\phi=\frac{-b+\sqrt{d}}{2a}$ y $\psi=\frac{-b-\sqrt{d}}{2a}$.

Por tanto, si x/y está entre los números ϕ y ψ, la forma toma valores negativos, en caso contrario toma valores positivos, por tal motivo se dice que la forma es indefinida.

En adelante se considerarán solo las formas cuadráticas que cumplen $(a,b,c)=1$. Tales formas son llamadas formas cuadráticas primitivas.

Notación 3.2.3. *La forma cuadrática $f(x,y)=ax^2+bxy+cy^2$ se denotará indistintamente como $\{a,b,c\}$ indicando cuales son los coeficientes de la forma mencionada, o simplemente $f(x,y)$ si no hay lugar a confusión.*

Observación 3.2.4. $f(x,y)=X^T\begin{pmatrix} a & b/2 \\ b/2 & c\end{pmatrix}X$, *entonces si* $A=\begin{pmatrix} a & b/2 \\ b/2 & c\end{pmatrix}$, $d=-4\det A$.

Definición 3.2.5. *Dos formas cuadraticas* $f(x,y)$, $g(x',y')$ *se dicen mutuamente relacionadas si existe una matriz* $A \in M_{2\times 2}(\mathbb{Z})$ *tal que* $\begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} x' \\ y' \end{pmatrix}$ *en donde* $\det A^2 = 1$. *Si además* $\det A = 1$ *entonces las formas se llaman equivalentes.*

Claramente se tiene que dos formas equivalentes tienen el mismo discriminate.

Se define una relación de equivalencia $\sim$ sobre el conjunto de las formas cuadraticas de discriminante d dada por

$$f(x,y) \sim g(x,y)$$

si y sólo si las formas son equivalentes.

El objetivo ahora, es demostrar que el conjunto de las formas de discriminante d partido por la anterior relación de equivalencia $\sim$, es un conjunto finito. Tal conjunto se va a denotar por Cl_K.

Una pregunta que surge de inmediato, es saber si dos formas cuadráticas son equivalentes de manera única, o si por el contrario hay más de una matriz la cual hace posible que $f(x,y) \sim g(x,y)$. Se tiene el siguiente teorema:

Teorema 3.2.6. *Si dos formas* $f(x,y)$, $g(x,y)$ *de discriminante* $d < 0$ *son equivalentes, entonces la equivalencia se lleva a cabo mediante* w_d *matrices diferentes, en donde:*

$$w_d = \begin{cases} 6 & \text{si } d = -3. \\ 4 & \text{si } d = -4. \\ 2 & \text{en otro caso.} \end{cases}$$

Para el caso $d > 0$, la situación es un poco más complicada, pues más adelante se verá que se deben buscar soluciones de la ecuación

$$t^2 - du^2 = 4$$

gracias a la ecuación (3.3). Esta ecuación recibe también el nombre de ecuación de Pell. Por el teorema 3.1.1, todas las soluciones de la anterior ecuación son de la forma $\pm\epsilon^n$, por esta razón si $d > 0$ se considera a $w_d = 1$.

Dada una forma $f(x,y)$ de discriminate d, se desea ahora hallar una forma equivalente a ella, pero que sea más sencilla o reducida que la que se tiene. El concepto de reducida se especificará a continuación. El procedimiento que se muestra es válido únicamente para formas definidas positivas. Para el caso de las formas indefinidas el lector puede consultar por ejemplo [Dir99].

Al considerar una forma positiva $\{a,b,c\}$, como $a > 0$:

- Si $c < a$ entonces se hace $x = Y$ y $y = -X$ para obtener la forma equivalente $\{c,-b,a\}$.
- Si $|b| > a$ se hace la sustitución $x = X + uY$ y $y = Y$ en donde u es tal que $|b_1| = |b + 2ua| < a$ para obtener la forma equivalente $\{a,b_1,c_1\}$ donde c_1 cumple que $b_1^2 - 4ac_1 = d$.

Por tanto, la forma $\{a,b,c\}$ puede ser reducida en un número finito de pasos a una forma equivalente $\{a',b',c'\}$ en donde $|b'| \leq a' \leq c'$. Mediante una modificación en el anterior algoritmo se obtiene el siguiente teorema válido para todo d.

Teorema 3.2.7. *En cada clase de formas siempre hay una la cual satisface la condición*

$$|b| \leq |a| \leq |c|.$$

A partir de esto se puede ver fácilmente que cualquier forma definida positiva es equivalente a una cuyos coeficientes satisfacen:

$$\begin{cases} -a < b \leq a & \text{si } c > a \\ 0 \leq b \leq a & \text{si } c = a \end{cases} \tag{3.1}$$

Si una forma cuadrática se encuentra como se acaba de plantear, ella se llama una forma reducida. En este caso se tiene el siguiente teorema:

Teorema 3.2.8. *Dos formas cuadráticas del mismo discriminante $d < 0$ son equivalentes si y sólo si, ellas tienen la misma forma reducida.*

Se denota por $h(d)$ el número de clases de formas primitivas de discriminante d. Gracias al teorema 3.2.7 se puede probar que:

Teorema 3.2.9. *$h(d)$ es un número finito.*

Demostración. Si $d > 0$, entonces se tiene que

$$|ac| \geq b^2 = d + 4ac > 4ac,$$

por tanto $ac < 0$. Además

$$4a^2 \leq 4|ac| = d - b^2 \leq d,$$

luego

$$|a| \leq \frac{\sqrt{d}}{2},$$

de manera que $|b| \leq \frac{\sqrt{d}}{2}$. Por tanto, hay sólo finitos valores para a y para b, e inmediatamente para c.

Si $d < 0$

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

así que $0 < a < \sqrt{\frac{|d|}{3}}$. Al razonar como antes, el resultado se demuestra. □

Definición 3.2.10. *Si todas las formas reducidas de discriminante d son primitivas, el discriminante es llamado un discriminante fundamental.*

Es fácil ver que un discriminante fundamental es aquel tal que no se puede expresar de la forma $d = d_0 t^2$ en donde d_0 es un discriminante y $t > 1$. Por tanto, si $d \equiv 0 \pmod 4$, entonces $d/4$ es 2 o 3 módulo 4.

3.3. Reinterpretación en términos de ideales.

Dado D un discriminante fundamental, se considera el cuerpo cuadrático $K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{d})$ donde d es tal que:

$$D = \begin{cases} 4d & \text{si } D \equiv 0 \pmod 4 \\ d & \text{si } D \equiv 1 \pmod 4. \end{cases}$$

Además se considera también el anillo de enteros $\mathcal{O}_K$ de K, el cual está conformado por los enteros algebraicos que están contenidos en K. En tal caso, se tiene que $\mathcal{O}_K$ es:

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

o equivalentemente

$$\mathcal{O}_K = \left\{ \frac{x}{2} + \frac{y\sqrt{d}}{2} \mid x, y \in \mathbb{Z} \right\}. \tag{3.2}$$

Recordamos que en estos casos, $\mathcal{O}_K$ es una anillo de Dedekind.

Definición 3.3.1. *El discriminante Δ del cuerpo $\mathbb{Q}(\sqrt{d})$ se define como:*

$$\Delta = \begin{cases} d & \textit{si } d \equiv 1 \pmod 4 \\ 4d & \textit{si } d \equiv 2, 3 \pmod 4. \end{cases}$$

En este caso, vemos que el discriminate de $\mathbb{Q}(\sqrt{d})$ es D.

Definición 3.3.2. *Si α y α^{-1} estan en $\mathcal{O}_K$ entonces α se llama una unidad de $\mathcal{O}_K$.*

Observación 3.3.3. *Una condición necesaria y suficiente para que α sea una unidad, es que $N(\alpha) = \pm 1$.*

Dada esta condición combinada con la ecuación (3.2), se tiene que para encontrar las unidades $\alpha = \frac{x}{2} + \frac{y\sqrt{d}}{2}$ de $\mathcal{O}_K$, hay que buscar las soluciones de

$$\pm 4 = x^2 - dy^2. \tag{3.3}$$

Si $d < 0$ estas ecuaciones tienen finitas soluciones, ellas son $\{1, \zeta, \zeta^2, \zeta^3 = -1, \zeta^4, \zeta^5\}$ en donde $\zeta = \frac{1+\sqrt{-3}}{2}$ si $d = -3$, $\{1, i, -1, -i\}$ si $d = -1$ y $\{1, -1\}$ en otro caso.

Si $d > 0$, por el teorema 3.1.1, la ecuacion (3.3) tiene infinitas soluciones, además existe una tal que $\pm\epsilon_0^n$ son todas las unidades de $\mathcal{O}_K$. Tal unidad ϵ_0 se llama la unidad fundamental de K.

Observación 3.3.4. *Se observa que si ϵ es la solución fundamental de la ecuación de Pell, y $N(\epsilon_0) = -1$, entonces $\epsilon_0^2 = \epsilon$. En caso contrario $\epsilon = \epsilon_0$.*

Definición 3.3.5. *Sea I un ideal de $\mathcal{O}_K$. Se sabe que $\mathcal{O}_K/I$ es un conjunto finito, por esto definimos la norma de I como $N(I) = |\mathcal{O}_K/I|$.*

Notación 3.3.6. *Si $\alpha = a + b\sqrt{d}$, entonces por α' se entenderá el número $\alpha' = a - b\sqrt{d}$.*

Dados I, J ideales de $\mathcal{O}_K$, se define la siguiente relación de equivalencia sobre ellos:

$$I \sim J \text{ sii existe } \gamma \in K \setminus \{0\} \text{ tal que } \gamma I = J.$$

A partir de esta relación de equivalencia, si se denota por F_K el conjunto de todos los ideales; al partir por la relación de equivalencia y denotar por $h_0 = |F_K/\sim|$ el número de clases de ideales, entonces se quiere establecer la relación entre h_0 y $h(d)$.

Sea I un ideal de $\mathcal{O}_K$ y $\{\alpha_1, \alpha_2\}$ una base para I que satisface

$$\alpha_1\alpha_2' - \alpha_1'\alpha_2 = N(I)\sqrt{D}; \tag{3.4}$$

se construye la siguiente forma cuadrática:

$$f(x,y) = \frac{N(\alpha_1 x + \alpha_2 y)}{N(I)} = ax^2 + bxy + cy^2,$$

donde $a = N(\alpha_1)/N(I)$, $b = [N(\alpha_1 + \alpha_2) - N(\alpha_1) - N(\alpha_2)]/N(I)$ y $c = N(\alpha_2)/N(I)$. Como $\alpha_1 + \alpha_2$, α_1, $\alpha_2 \in I$, se tiene que los números $a, b, c \in \mathbb{Z}$. Además el discriminante de $f(x,y)$ es $b^2 - 4ac = [\alpha_1\alpha_2' - \alpha_1'\alpha_2]^2/N(I)^2 = D$.

Observación 3.3.7. *De esta manera se ha relacionado la forma $f(x,y)$ con el ideal I. Además no es complicado ver que si $\{\beta_1, \beta_2\}$ es otra base para I que cumple la condición de la ecuación* (3.4)*, entonces la forma obtenida es equivalente a f. En efecto:*

Dado que $\alpha_1\alpha_2' - \alpha_1'\alpha_2 = N(I)\sqrt{D} = \beta_1\beta_2' - \beta_1'\beta_2$, si

$$\begin{aligned} \alpha_1 &= a_{1,1}\beta_1 + a_{1,2}\beta_2 \\ \alpha_2 &= a_{2,1}\beta_1 + a_{2,2}\beta_2, \end{aligned}$$

entonces $a_{1,1}a_{2,2} - a_{1,2}a_{2,1} = 1$. Se sigue que las formas obtenidas son equivalentes.

Teorema 3.3.8. *Cualquier forma $\{a, b, c\}$ de discriminante D se relaciona con un ideal I de $\mathcal{O}_K$ cuya base $\{\alpha_1, \alpha_2\}$ cumple con la condición de la ecuación* (3.4)*.*

Demostración. Si $D < 0$, entonces $a > 0$. Al tomar $\alpha_1 = a$, $\alpha_2 = \frac{b-\sqrt{D}}{2}$, se tiene que $N(I) = a$ y

$$\frac{N(\alpha_1 x + \alpha_2 y)}{a} = ax^2 + bxy + cy^2.$$

Si $D > 0$, al tomar $\alpha_1 = a\sqrt{D}$, y $\alpha_2 = \frac{(b-\sqrt{D})\sqrt{D}}{2}$, se tiene que $N(I) = -aD$ y

$$\frac{N(\alpha_1 x + \alpha_2 y)}{-aD} = ax^2 + bxy + cy^2.$$

□

Con lo construido hasta el momento, cada forma se ha relacionado con un ideal I de $\mathcal{O}_K$ y cada forma equivalente a f pertenece a I. Sin embargo, si $I \sim J$ es tal que $I = \gamma J$ y $N(\gamma) < 0$ se tiene que si $I = \{\alpha_1, \alpha_2\}$, $J = \{\gamma\alpha_1, \gamma\alpha_2\}$ y por tanto

$$\gamma\alpha_1(\gamma\alpha_2)' - (\gamma\alpha_1)'\gamma\alpha_2 = N(\gamma)[\alpha_1\alpha_2' - \alpha_1'\alpha_2] = N(\gamma)N(I)\sqrt{D},$$

de manera que la base $\{\gamma\alpha_1, \gamma\alpha_2\}$ para J no cumple con la condición (3.4). Para forzar este hecho, se pone la condición adicional que $N(\gamma) > 0$ y se define la siguiente relación de equivalencia:

Definición 3.3.9. *Sean I, J ideales de $\mathcal{O}_K$. Si existe $\gamma \in K \setminus \{0\}$ tal que $I = \gamma J$ y $N(\gamma) > 0$, entonces se dice que I, J son equivalentes en el sentido estricto. Esto se escribe mediante*

$$I \approx J.$$

Teorema 3.3.10. *Formas cuadráticas equivalentes se relacionan con ideales equivalentes en el sentido estricto. Recíprocamente, si dos formas se relacionan con ideales los cuales son equivalentes en el sentido estricto, ellas son equivalentes.*

Demostración. ($\Leftarrow$). Si $I = \gamma J$ en donde $N(\gamma) > 0$, y además g se relaciona con J, y f se relaciona con I, entonces

$$g = \frac{N(\beta_1 x + \beta_2 y)}{N(J)} = \frac{N(\gamma\alpha_1 x - \gamma\alpha_2 y)}{N(J)} = \frac{N(\alpha_1 x - \alpha_2 y)}{N(I)},$$

luego g está relacionada con I, por tanto $g \sim f$. □

Si ahora h denota el número de clases de ideales en el sentido de equivalencia estricto, entonces según el anterior teorema $h = h(d)$. Además si $I \sim J$, entonces:

- Si $D < 0$, siempre $N(\gamma) > 0$, por tanto $\sim$ y $\approx$ son la misma relación, es decir $h = h_0$.
- Si $D > 0$ y la unidad fundamental ϵ_0 de K satisface que $N(\epsilon_0) = -1$, entonces $I = \gamma J = \epsilon\gamma J$. Dado que $N(\gamma)$ o $N(\epsilon_0\gamma)$ es positiva, se tiene que $I \approx J$.
- Si $D > 0$ y $N(\epsilon_0) = 1$, puede suceder que $I \not\approx J$. Como

  $$[I]_\sim = \{I | I \sim J \text{ y } N(\gamma) > 0\} \cup \{I | I \sim J \text{ y } N(\gamma) < 0\}$$

  se tiene que de la clase de ideales de $[I]_\sim$ se obtienen dos clases de ideales en el sentido estricto, es decir $h = 2h_0$.

De ahí se tiene que

$$h_0 = \begin{cases} h & \text{si } D < 0 \text{ o si } D > 0 \text{ y } N(\epsilon_0) = -1 \\ \frac{h}{2} & \text{si } D > 0 \text{ y } N(\epsilon_0) = 1. \end{cases} \tag{3.5}$$

De esta forma se ha encontrado una manera sencilla de relacionar el número de clases de ideales con el número de clases de formas.

3.4. El valor de $h(d)$.

El siguiente objetivo ahora es determinar el valor exacto de $h(d)$. Sin embargo, primero se necesita contar de cuántas maneras distintas la ecuación $f(x,y) = k$ es soluble.

3.4.1. Soluciones de $f(x,y) = k$

Definición 3.4.1. *La pareja (x,y) se dice una solución propia de $f(x,y) = k$ si satisface la ecuación y además $(x,y) = 1$.*

Se enuncia el siguiente teorema sin presentar su demostración.

Teorema 3.4.2. *Sean (x_1,y_1) y (x_2,y_2) dos soluciones propias correspondientes a $f(x,y) = k$, entonces*

$$2ax_1 + (b+\sqrt{d})y_1 = (2ax_2 + (b+\sqrt{d})y_2)\left(\frac{t+u\sqrt{d}}{2}\right),$$

donde t,u satisfacen

$$t^2 - du^2 = 4.$$

Definición 3.4.3. *Sea $d > 0$. Se dice que una solución propia de $f(x,y) = k$ es una solución primaria de f si cumple:*
Si $L = 2ax + (b+\sqrt{d})y$, entonces

$$\overline{L} > 0 \quad y \quad 1 \leq \left|\frac{L}{\overline{L}}\right| < \epsilon^2,$$

donde ϵ es la solución fundamental de la ecuación de Pell.

Dado que hay $h(d)$ formas primitivas de discriminante d, de cada clase se selecciona un representante f_i tal que $f_1, f_2, \ldots, f_{h(d)}$ sea un sistema completo.

Teorema 3.4.4. *Sean $k > 0$, $(k,d) = 1$, y $R(k)$ el número total de soluciones primarias de*

$$k = f_1(x,y), \ \cdots \ , k = f_{h(d)}(x,y).$$

Entonces

$$R(k) = w_d \sum_{n|k} \left(\frac{d}{n}\right).$$

Demostración. Al considerar las soluciones de la congruencia $l^2 \equiv d \pmod{4k}$ cuando $0 \leq l < 2k$, para una solución dada l se puede determinar m tal que $l^2 - 4km = d$. Esto da una forma $\{k,l,m\}$ la cual es primitiva y cuyo discriminante es d, por tanto, es equivalente a una y solo una de las f_i. Por el teorema 3.2.6, hay w_d soluciones primarias propias correspondientes a cada l. Por tanto el número total de soluciones primarias propias a $k = f_1(x,y), \ \cdots \ , k = f_{h(d)}(x,y)$ es

$$w_d \sum_{t|k} \left(\frac{d}{t}\right);$$

también el número de soluciones primarias es

$$R(k) = w_d \sum_{\substack{g^2|k \\ g>0}} \sum_{t\left|\frac{k}{g^2}\right.} \left(\frac{d}{tg^2}\right).$$

Dado que $(k,d)=1$, se tiene que $(g^2,d)=1$ y por tanto

$$R(k) = w_d \sum_{\substack{g^2|k \\ g>0}} \sum_{t\left|\frac{k}{g^2}\right.} \left(\frac{d}{tg^2}\right) = w_d \sum_{m|k} \left(\frac{d}{m}\right).$$

□

Teorema 3.4.5.

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{1\le k\le N \\ (k,d)=1}} \sum_{m|k} \left(\frac{d}{m}\right) = \frac{\phi(|d|)}{|d|} L(1,\chi_d)$$

Demostración. Si se denota con $A(N,d,m)$ al número de enteros positivos que no exceden N/m y son coprimos con d, entonces

$$\begin{aligned}
\frac{1}{N} \sum_{\substack{1\le k\le N \\ (k,d)=1}} \sum_{m|k} \left(\frac{d}{m}\right) &= \frac{1}{N} \sum_{m=1}^{\infty} \left(\frac{d}{m}\right) \sum_{\substack{1\le k\le N \\ (k,d)=1 \\ m|k}} 1 \\
&= \frac{1}{N} \sum_{m=1}^{\infty} \left(\frac{d}{m}\right) \sum_{\substack{1\le k\le N/m \\ (k,d)=1}} 1 \\
&= \sum_{m=1}^{\infty} \left(\frac{d}{m}\right) \frac{A(N,d,m)}{N}. \qquad (3.6)
\end{aligned}$$

Dado que $A(N,d,m) < N/m$, y que $A(N,d,m)$ no crece como m, entonces la serie en (3.6) es uniformemente convergente y además para m fijo

$$\lim_{N\to\infty} \frac{A(N,d,m)}{N} = \frac{\phi(|d|)}{|d|} \frac{1}{m},$$

pues como $A(N,d,m) = \sum_{k\le N/m} \chi_0(k)$, por la propiedad 4 en la observación (2.2.2) se tiene que si $N/m = k|d| + s$ en donde $0 \le s < |d|$, entonces

$$\frac{A(N,d,m)}{N} = \frac{k\phi(|d|)}{N} + O(1/N).$$

Por tanto

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{1\le k\le N \\ (k,d)=1}} \sum_{m|k} \left(\frac{d}{m}\right) = \lim_{N\to\infty} \sum_{m=1}^{\infty} \left(\frac{d}{m}\right) \frac{A(N,d,m)}{N} = \frac{\phi(|d|)}{|d|} L(1,\chi_d).$$

□

Teorema 3.4.6. *Sean $m > 0$ y una elipse o una hipérbola centrada en el origen (en el último caso, se toman las dos ramas de la hipérbola junto con las dos líneas rectas que pasan a través del origen). Se denota con I el área dentro de la región. Si se multiplica cada punto por $\sqrt{N}$, se denota con $U(N)$ al número de puntos en el retículo de la figura ampliada cuyas coordenadas satisfacen:*

$$x \equiv x_0 \pmod{m}, \quad y \equiv y_0 \pmod{m}.$$

Entonces

$$\lim_{N\to\infty} \frac{U(N)}{N} = \frac{I}{m^2}.$$

Demostración. Al formar un retículo en la figura original con líneas rectas ortogonales tales que

$$x = \frac{x_0 + rm}{\sqrt{N}}, \qquad y = \frac{y_0 + sm}{\sqrt{N}},$$

se tiene un retículo de cuadrados cuyo lado mide $m/\sqrt{N}$. Si se denota por $W(N)$ el número de cuadrados cuyas esquinas suroestes están dentro de la elipse o la hipérbola, entonces $U(N) = W(N)$. Dado que el área de cada cuadrado en el retículo es m^2/N, se sigue del teorema fundamental de cálculo que

$$I = \iint dydx = \lim_{N\to\infty} \frac{m^2}{N} W(N),$$

de donde se concluye el resultado. □

Se conoce el valor de $R(k)$, además $R(k) = \sum_f R(k,f)$ si $R(k,f)$ es el número de representaciones propias de k por la forma f. Ahora se va a evaluar el promedio de $R(k,f)$, es decir

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{1\le k\le N \\ (k,d)=1}} R(k,f),$$

y ver que no depende de f, de manera que se podría hallar el valor de $h(d)$ de una manera más fácil. Para este objetivo, se utiliza un teorema del cual sólo daremos su enunciado y su demostración puede ser consultada por ejemplo en [Dav80].

Teorema 3.4.7. *Si x, y son pares de un sistema completo de residuos módulo $|d|$, hay exactamente $|d|\phi(|d|)$ pares de elementos x, y tal que $(f(x,y), d) = 1$.*

Teorema 3.4.8.

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{1\le k\le N \\ (k,d)=1}} R(k,f) = \begin{cases} \frac{2\pi}{\sqrt{|d|}} \frac{\phi(|d|)}{|d|} & si\ d < 0 \\ \\ \frac{\log \epsilon}{\sqrt{d}} \frac{\phi(d)}{d} & si\ d > 0. \end{cases}$$

Demostración. Si $d < 0$, entonces

$$\sum_{\substack{1\le k\le N \\ (k,d)=1}} R(k,f)$$

es el número de pares de enteros (x, y) que satisfacen

$$0 < f(x, y) \leq N, \quad (f(x, y), d) = 1.$$

La segunda condición fuerza a x, y a recorrer un sistema completo de residuos módulo $|d|$. De ahí es suficiente considerar entonces los pares de enteros x, y que satisfacen

$$f(x, y) \leq N, \qquad x \equiv x_0 \pmod{|d|}, \qquad y \equiv y_0 \pmod{|d|}. \tag{3.7}$$

Ahora, si $d > 0$, argumentando como antes, se necesita el número de puntos (x, y) que satisfacen

$$\begin{gathered} f(x, y) \leq N, \qquad \overline{L} > 0, \qquad 1 \leq \Big|\frac{L}{\overline{L}}\Big| < \epsilon^2, \\ x \equiv x_0 \pmod{d}, \qquad y \equiv y_0 \pmod{d}. \end{gathered} \tag{3.8}$$

Por el teorema 3.4.6, tal número de puntos es $U(N)$, además

$$\sum_{\substack{(x,y) \\ (f(x,y),d)=1}} U(N) = \sum_{\substack{1 \leq k \leq N \\ (k,d)=1}} R(k, f).$$

Por tanto

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{1 \leq k \leq N \\ (k,d)=1}} R(k, f) = \lim_{N\to\infty} \frac{1}{N} \sum_{\substack{(x,y) \\ (f(x,y),d)=1}} U(N).$$

Por el teorema 3.4.6, $\lim_{N\to\infty} \frac{U(N)}{N}$ no depende de f ni de (x, y); así

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{1 \leq k \leq N \\ (k,d)=1}} R(k, f) = |d|\phi(|d|)\frac{I}{d^2}.$$

Si se logra ver que

$$I = \begin{cases} \frac{2\pi}{\sqrt{|d|}} & \text{si } d < 0 \\ \\ \frac{\log \epsilon}{\sqrt{d}} & \text{si } d > 0, \end{cases}$$

el teorema será demostrado.

Si $d < 0$, el área de la elipse $f(x, y) \leq 1$ es bien conocida. Su valor es $2\pi/\sqrt{|d|}$ tal como se quiere.

Si $d > 0$, la condición representa un sector de la hipérbola acotada por dos líneas rectas a través del origen. Se puede asumir que $a > 0$. Dado que

$$L = 2ax + (b + \sqrt{d})y, \quad \overline{L} = 2ax + (b - \sqrt{d})y,$$

entonces se tiene que

$$L\overline{L} = 4af(x, y),$$

y de ahí $L > 0$.

El área requerida de la hipérbola es $I = \iint dxdy$ en donde la región de integración es sobre $L\overline{L} \leq 4a$, $\overline{L} > 0$ y $1 \leq L/\overline{L} < \epsilon^2$. Si se hace la sustitución

$$\xi = \frac{L}{2\sqrt{a}}, \qquad \eta = \frac{\overline{L}}{2\sqrt{a}},$$

se tiene que

$$I = \frac{1}{\sqrt{d}} \iint d\xi d\eta,$$

donde la región de integración es sobre $\xi\eta \leq 1$, $\eta > 0$, $\eta < \xi < \epsilon^2\eta$; luego

$$\begin{aligned} \sqrt{d}I &= \int_0^1 \int_{\xi/\epsilon^2}^{\xi} d\eta d\xi + \int_1^{\epsilon} \int_{\xi/\epsilon^2}^{1/\xi} d\eta d\xi \\ &= \log \epsilon. \end{aligned}$$

Con lo cual el teorema queda demostrado. □

Teorema 3.4.9.

$$h(d) = \begin{cases} \frac{w_d\sqrt{|d|}}{2\pi} L(1, \chi_d) & si\ d < 0 \\ \\ \frac{\sqrt{d}}{\log \epsilon} L(1, \chi_d) & si\ d > 0. \end{cases}$$

Demostración. Por el anterior teorema se tiene que

$$\lim_{N\to\infty} \sum_f \sum_{\substack{1\leq k\leq N \\ (k,d)=1}} R(k, f) = h(d) \lim_{N\to\infty} \sum_{\substack{1\leq k\leq N \\ (k,d)=1}} \frac{R(k, f)}{N}. \tag{3.9}$$

Por otro lado, gracias al teorema 3.4.4 se tiene que

$$\sum_f \sum_{\substack{1\leq k\leq N \\ (k,d)=1}} R(k, f) = w_d \sum_{\substack{1\leq k\leq N \\ (k,d)=1}} \sum_{m|k} \left(\frac{d}{m}\right).$$

Por el teorema 3.4.5 se obtiene entonces que

$$\lim_{N\to\infty} \frac{1}{N} \sum_f \sum_{\substack{1\leq k\leq N \\ (k,d)=1}} R(k, f) = \lim_{N\to\infty} \frac{w_d}{N} \sum_{\substack{1\leq k\leq N \\ (k,d)=1}} \sum_{m|k} \left(\frac{d}{m}\right) = w_d \frac{\phi(|d|)}{|d|} L(1, \chi_d),$$

y este límite junto con el dado en la ecuación (3.9) da el resultado que se quiere. Se ha descrito la relación entre el número de clase $h(d)$ y el valor $L(1, \chi)$. Esa relación se conoce como la fórmula de Dirichlet. □

Observación 3.4.10. *Gracias a la observación 3.3.4 y a la ecuación* (3.5) *se tiene*

$$h_0 = \begin{cases} \frac{w_d\sqrt{|d|}}{2\pi} L(1, \chi_d) & si\ d < 0 \\ \frac{\sqrt{d}}{2\log \epsilon_0} L(1, \chi_d) & si\ d > 0. \end{cases}$$

donde ϵ_0 es la unidad fundamental de $\mathbb{Q}(\sqrt{d})$.

CAPÍTULO 4

El teorema de Dirichlet sobre los primos en progresiones aritméticas.

El objetivo de este capítulo, es estudiar el número de primos en una progresión aritmética. Dirichlet demostró el siguiente teorema:

Teorema 4.0.11 (Dirichlet)**.** *Si* $(h, n) = 1$*, entonces la progresión aritmética* $nk+h$ *donde* $k \in \mathbb{N}$*, contiene un número infinito de primos.*

4.1. La no anulación de $L(1, \chi)$ cuando $\chi \neq \chi_0$.

Inicialmente, se va a ver que para probar el teorema, es suficiente demostrar que $L(1, \chi) \neq 0$ para todo caracter numérico módulo k diferente de χ_0.

Se ve inmediatamenta que el teorema de Dirichlet es una consecuencia directa del siguiente teorema, pues en caso de que haya un número finito de primos $p \equiv h \pmod{n}$, el lado izquierdo sería finito, mientras que el lado derecho del teorema tiende a infinito cuando $x \to \infty$.

Teorema 4.1.1. *Si* $(h, n) = 1$*, entonces para cada* $x > 1$

$$\sum_{\substack{p \leq x \\ p \equiv h \pmod{n}}} \frac{\log p}{p} = \frac{1}{\phi(n)} \log x + O(1),$$

donde la suma se extiende sobre todos los números primos $p \leq x$ *los cuales son congruentes con* $h \pmod{n}$*.*

Se puede ver la relación entre los teoremas 1.3.1 y 4.1.1 como el hecho que cada clase de equivalencia h tal que $(h, n) = 1$, aporta la "misma cantidad" infinita de números primos en la suma a mano izquierda, pues esta suma no depende de h. Es esta una demostración diferente del teorema 1.3.1.

Una vez demostrado este teorema, al razonar de manera similar a la demostración del teorema 1.3.2 se sigue el teorema de Dirichlet. La demostración del anterior teorema es inmediata si se logra probar el siguiente lema auxiliar:

Lema 4.1.2. *Si $x > 1$ se tiene que*

$$\sum_{\substack{p\leq x\\ p\equiv h \pmod n}} \frac{\log p}{p} = \frac{1}{\phi(n)}\log x + \frac{1}{\phi(n)}\sum_{r=2}^{\phi(n)} \overline{\chi}_r(h)\sum_{p\leq x}\frac{\chi_r(p)\log p}{p} + O(1);$$

y adicionalmente se logra demostrar que para cada $\chi \neq \chi_0$ se tiene que

$$\sum_{p\leq x}\frac{\chi(p)\log p}{p} = O(1). \tag{4.1}$$

Para obtener este resultado, el siguiente lema es de gran ayuda:

Lema 4.1.3. *Para $x > 1$ y $\chi \neq \chi_0$ se tiene que*

$$\sum_{p\leq x}\frac{\chi(p)\log p}{p} = -L'(1,\chi)\sum_{m\leq x}\frac{\mu(m)\chi(m)}{m} + O(1).$$

Se ve que este lema implica el resultado de la ecuación (4.1) si se logra demostrar que

$$\sum_{m\leq x}\frac{\mu(m)\chi(m)}{m} = O(1). \tag{4.2}$$

Lema 4.1.4. *Para $x > 1$ y $\chi \neq \chi_0$ se tiene que*

$$L(1,\chi)\sum_{m\leq x}\frac{\mu(m)\chi(m)}{m} = O(1).$$

Por tanto, si $L(1,\chi) \neq 0$ cuando $\chi \neq \chi_0$, se puede obtener el resultado querido en la ecuación (4.2), con lo cual se demuestra el teorema (4.1.1), y de ahí que la prueba del teorema de Dirichlet dependa fuertemente del hecho que

$$L(1,\chi) \neq 0.$$

Demostración. Para la demostración de este lema, se utilizará la fórmula generalizada de inversión de Möbius, la cual se encuentra en los anexos del primer capítulo.

Si

$$G(x) = x\sum_{m\leq x}\frac{\chi(m)}{m},$$

dado que χ es completamente multiplicativa, se tiene que

$$F(x) = \sum_{m\leq x}\mu(m)\chi(m)G\left(\frac{x}{m}\right),$$

donde $F(x) = x$. Por la ecuación (2.1), se tiene que $G(x) = xL(1,\chi) + O(1)$, de modo que:

$$x = \sum_{m\leq x}\mu(m)\chi(m)\left\{\frac{x}{m}L(1,\chi) + O(1)\right\} = xL(1,\chi)\sum_{m\leq x}\frac{\mu(m)\chi(m)}{m} + O(x).$$

Si se divide todo por x, se obtiene el resultado del lema. □

Demostración del lema (4.1.3).

Demostración. Dado que

$$\sum_{m\leq x}\frac{\chi(m)\Lambda(m)}{m}=\sum_{p\leq x}\frac{\chi(p)\log p}{p}+O(1),$$

en donde $\Lambda(m)$ es la función de Mangoldt, el lema es válido si se demuestra que

$$\sum_{m\leq x}\frac{\chi(m)\Lambda(m)}{m}=-L'(1,\chi)\sum_{m\leq x}\frac{\mu(m)\chi(m)}{m}+O(1). \tag{4.3}$$

Dado que $\Lambda(m)=\sum_{d|m}\mu(d)\log(m/d)$, entonces se tiene que

$$\sum_{m\leq x}\frac{\chi(m)}{m}\sum_{d|m}\mu(d)\log(m/d)=\sum_{d\leq x}\frac{\mu(d)\chi(d)}{d}\sum_{cd\leq x}\frac{\chi(c)\log c}{c},$$

puesto que χ es completamente multiplicativo. Además, si se utiliza la fórmula (2.2) que se encuentra en la página 17, se tiene que

$$\sum_{c\leq x/d}\frac{\chi(c)\log c}{c}=-L'(1,\chi)+O\bigg(\frac{\log(x/d)}{x/d}\bigg),$$

y por tanto se obtiene

$$\sum_{m\leq x}\frac{\chi(m)\Lambda(m)}{m}=-L'(1,\chi)\sum_{d\leq x}\frac{\mu(d)\chi(d)}{d}+O\bigg(\sum_{d\leq x}\frac{1}{d}\frac{\log(x/d)}{x/d}\bigg). \tag{4.4}$$

Como

$$\sum_{d\leq x}\log d=\log[x]!=[x]\log x+O(x),$$

entonces el término dentro de O en la ecuación (4.4) cumple que

$$\frac{1}{x}\sum_{d\leq x}\big(\log x-\log d\big)=\frac{1}{x}\bigg([x]\log x-\sum_{d\leq x}\log d\bigg)=O(1). \tag{4.5}$$

Por tanto, las ecuaciones (4.4) y (4.5) demuestran la ecuación (4.3) y así el lema es válido. □

Demostración del lema (4.1.2)

Demostración. Se va a utilizar la proposición 2.2.3 que se encuentra en la página 16. Por tanto, cuando $(h,n)=1$ y $p\equiv h \pmod n$, se tiene que

$$\sum_{p\leq x}\sum_{r=1}^{\phi(n)}\frac{\chi_r(p)\overline{\chi}_r(h)\log p}{p}=\phi(n)\sum_{\substack{p\leq x\\ p\equiv h \pmod n}}\frac{\log p}{p}.$$

Si se escribe aparte el término correspondiente al carácter χ_0, entonces se tiene

$$\phi(n) \sum_{\substack{p\leq x \\ p\equiv h \pmod n}} \frac{\log p}{p} = \overline{\chi}_1(h) \sum_{p\leq x} \frac{\chi_0(p)\log p}{p} + \sum_{r=2}^{\phi(n)} \overline{\chi}_r(h) \sum_{p\leq x} \frac{\chi_r(p)\log p}{p}.$$

Como $\chi_0(p) = 1$ solo cuando $(p, n) = 1$, entonces el primer término al lado derecho queda:

$$\sum_{\substack{p\leq x \\ (p,n)=1}} \frac{\log p}{p} = \sum_{p\leq x} \frac{\log p}{p} - \sum_{\substack{p\leq x \\ p|n}} \frac{\log p}{p} = \sum_{p\leq x} \frac{\log p}{p} + O(1),$$

pues el número de primos que divide a n es finito. De esta forma se tiene que:

$$\phi(n) \sum_{\substack{p\leq x \\ p\equiv h \pmod n}} \frac{\log p}{p} = \sum_{p\leq x} \frac{\log p}{p} + \sum_{r=2}^{\phi(n)} \overline{\chi}_r(h) \sum_{p\leq x} \frac{\chi_r(p)\log p}{p} + O(1).$$

Al utilizar el resultado del teorema 1.3.1 y dividir esta última expresión por $\phi(n)$ se obtiene el resultado. □

Con este resultado y la ecuación (4.1), el teorema 4.1.1 queda demostrado siempre y cuando sea cierto que $L(1, \chi) \neq 0$.

4.2. $L(1, \chi) \neq 0$

Para demostrar esto, se dividirá la prueba en dos casos distintos. En el primero de ellos se supondrá que χ es un carácter complejo, y el segundo caso se hará pensando en que χ es un carácter real.

4.2.1. $L(1, \chi) \neq 0$ para todo carácter no principal con valores complejos

Dado que χ es complejo, si $L(1, \chi) = 0$, entonces $L(1, \overline{\chi}) = 0$ y como $\chi \neq \overline{\chi}$, se tiene que hay un número par de caracteres para los cuales $L(1, \chi) = 0$. Sea $N(n)$ el número de tales caracteres, se quiere probar que $N(n) = 0$. Para este propósito, se necesita primero demostrar la siguiente fórmula asintótica.

Lema 4.2.1. *Si $\chi \neq \chi_0$ y $L(1, \chi) = 0$, se tiene que*

$$L'(1, \chi) \sum_{m\leq x} \frac{\mu(m)\chi(m)}{m} = \log x + O(1).$$

Demostración. Al utilizar nuevamente la fórmula de inversión generalizada de Möbius con

$$G(x) = x \sum_{m\leq x} \frac{\chi(m)}{m} \log(x/m) = x \log x \sum_{m\leq x} \frac{\chi(m)}{m} - x \sum_{m\leq x} \frac{\chi(m)\log m}{m},$$

se obtiene

$$F(x) = x\log x = \sum_{m\leq x}\mu(m)\chi(m)G(x/m).$$

Gracias a las ecuaciones (2.1) y (2.2) se obtiene:

$$\begin{aligned} G(x) &= x\log x\Big\{L(1,\chi)+O(1/x)\Big\} + x\Big\{L'(1,\chi)+O\Big(\frac{\log x}{x}\Big)\Big\} \\ &= O(\log x) + xL'(1,\chi). \end{aligned}$$

De ahí se tiene que

$$\begin{aligned} x\log x &= \sum_{m\leq x}\mu(m)\chi(m)\Big\{O\Big(\log\frac{x}{m}\Big)+\frac{x}{m}L'(1,\chi)\Big\} \\ &= xL'(1,\chi)\sum_{m\leq x}\frac{\mu(m)\chi(m)}{m} + O\Big(\sum_{m\leq x}\log\frac{x}{m}\Big). \end{aligned}$$

El término dentro de O, por la ecuación (4.5) es $O(x)$, por tanto se tiene que

$$\log x = L'(1,\chi)\sum_{m\leq x}\frac{\mu(m)\chi(m)}{m} + O(1).$$

□

Con este resultado adicional, ahora se procede a dar una demostración en la cual $L(1,\chi)\neq 0$ cuando χ es complejo.

Lema 4.2.2. *Para $x>1$ se tiene que*

$$\sum_{\substack{p\leq x\\ p\equiv 1 \pmod n}}\frac{\log p}{p} = \frac{1-N(n)}{\phi(n)}\log x + O(1).$$

Demostración. Para este propósito, se utilizará el lema 4.1.2 con $h=1$. Se obtiene así que

$$\sum_{\substack{p\leq x\\ p\equiv 1 \pmod n}}\frac{\log p}{p} = \frac{1}{\phi(n)}\log x + \frac{1}{\phi(n)}\sum_{r=2}^{\phi(n)}\sum_{p\leq x}\frac{\chi_r(p)\log p}{p} + O(1). \tag{4.6}$$

Si $L(1,\chi)\neq 0$ el lema 4.1.4 dice que

$$\sum_{p\leq x}\frac{\chi(p)\log p}{p} = O(1).$$

Por el contrario, si $L(1,\chi)=0$, el anterior lema dice que

$$\sum_{p\leq x}\frac{\chi(p)\log p}{p} = -\log x + O(1),$$

y así, la ecuación (4.6) se convierte en:

$$\sum_{\substack{p\leq x\\ p\equiv 1 \pmod n}} \frac{\log p}{p} = \frac{\log x}{\phi(n)}[1-N(n)] + O(1).$$

□

Este lema implica directamente que $N(n) = 0$, pues en caso contrario, como es un número par, se tiene que $N(n) \geq 2$, así cuando $x \to \infty$ en el lema anterior, el miembro a mano izquierda es positivo, mientras que el miembro a mano derecha tiende a $-\infty$, lo cual no puede ser. Por tal motivo $N(n) = 0$, es decir $L(1,\chi) \neq 0$ cuando χ es un carácter complejo.

4.2.2. $L(1,\chi) \neq 0$ para todo carácter no principal con valores reales.

Se observa que $L(1,\chi) \neq 0$ es una consecuencia de la fórmula de número de clases dada en el teorema 3.4.9, sin embargo se va a proporcionar una demostración más directa. Históricamente hablando, Dirichlet no sabía la continuación analítica de la función $L(s,\chi)$, motivo por el cual, su razonamiento lo condujo a la fórmula de número de clases para probar que $L(1,\chi) \neq 0$.

Si se supone por el contrario que $L(1,\chi) = 0$ para algún carácter real, entonces la función $F(s) = \zeta(s)L(s,\chi)$ es una función analítica y no tiene singularidad alguna si $\mathrm{Re}(s) > 0$. Además si $\mathrm{Re}(s) > 1$ se tiene que

$$F(s) = \left(\sum_{m=1}^{\infty} \frac{1}{m^s}\right)\left(\sum_{m=1}^{\infty} \frac{\chi(m)}{m^s}\right) = \sum_{m=1}^{\infty} \frac{1 * \chi(m)}{m^s}$$

gracias al producto de series de Dirichlet; además $1 * \chi(m)$ es una función multiplicativa, y por ser χ un carácter real, $\chi(m) = 0$ o $\chi(m) = \pm 1$. Por tanto, si $p^k | m$ se tiene que

$$1 * \chi(m) = \sum_{i=0}^{k} \chi(p)^i = \begin{cases} 1 & \text{si } \chi(p) = 0 \text{ o si } \chi(p) = -1 \text{ y } k = 2l \\ k+1 & \text{si } \chi(p) = 1 \\ 0 & \text{si } \chi(p) = -1 \text{ y } k = 2l+1. \end{cases}$$

Sea $h(m)$ definida por

$$h(m) = \begin{cases} 1 & \text{si } m = a^2 \\ 0 & \text{en otro caso,} \end{cases}$$

de modo que $1 * \chi(p^k) \geq h(p^k)$. Por otro lado,

$$\sum_{m=1}^{\infty} \frac{h(m)}{m^s} = \sum_{m=1}^{\infty} \frac{1}{(m^2)^s} = \zeta(2s),$$

la cual converge absolutamente si $\mathrm{Re}(s) > 1/2$. Además, como $F(s)$ no tiene singularidades cuando $\mathrm{Re}(s) > 0$, $F(s)$ se puede expresar mediante una serie de Taylor al rededor de $x_0 > 0$ tal que si $0 < x \leq x_0$, la serie converja.

$$F(x) = \sum_{d=0}^{\infty} \frac{F^{(d)}(x_0)}{d!}(x - x_0)^d. \tag{4.7}$$

Si se toma $x_0 > 1/2$ entonces

$$\begin{aligned}(-1)^d F^d(x_0) &= (-1)^d \sum_{m=1}^{\infty} \frac{1 * \chi(m)}{m^{x_0}} (-\log m)^d \\ &\geq (-1)^d \sum_{m=1}^{\infty} \frac{h(m)}{m^{x_0}} (-\log m)^d \\ &= (-1)^d D^d \Big(\sum_{m=1}^{\infty} \frac{h(m)}{m^s} \Big) \Big|_{s=x_0} \\ &= (-1)^d D^d (\zeta(2s)) \big|_{s=x_0} \\ &= (-2)^d \zeta^d(2x_0) \geq 0.\end{aligned}$$

Por tanto se tiene que

$$\begin{aligned}F(x_0) = \sum_{d=0}^{\infty} \frac{F^d(x_0)}{d!}(x - x_0)^d &= \sum_{d=0}^{\infty} \frac{(-1)^d F^d(x_0)}{d!}(x_0 - x)^d \\ &\geq \sum_{d=0}^{\infty} \frac{(-2)^d \zeta^d(2x_0)}{d!}(x_0 - x)^d \\ &= \sum_{d=0}^{\infty} \frac{\zeta^d(2x_0)}{d!}(2x - 2x_0)^2 = \zeta(2x).\end{aligned}$$

Como $x_0 > 1/2$, por la ecuación (4.7) $F(x)$ existe, pero por el anterior razonamiento $F(1/2) \geq \zeta(1) = +\infty$, lo cual es una contradicción. Así se concluye que $L(1, \chi) \neq 0$.

Con este resultado se ha completado entonces la demostración del teorema 4.1.1, y como se mencionó anteriormente, este teorema implica el teorema de Dirichlet, del cual se va a ver a continuación una fórmula asintótica similar a la descrita en el teorema 1.3.2.

4.3. Fórmula asintótica para primos en progresiones aritméticas

Teorema 4.3.1.

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod n}} \frac{1}{p} \sim \frac{1}{\phi(n)} \log\log x.$$

Demostración. Sean

$$a_{a,n}(m) = \begin{cases} 1 & \text{si } m \equiv a \pmod n \text{ y } m \text{ es primo.} \\ 0 & \text{en otro caso.} \end{cases}$$

$$A_{h,n}(x) = \sum_{\substack{p \leq x \\ p \equiv h \pmod n}} \frac{\log p}{p},$$

entonces

$$\sum_{\substack{p\leq x\\ p\equiv h \pmod n}} \frac{1}{p} = \sum_{m\leq x} \frac{a_{h,n}(m)}{m}.$$

Utilizando el teorema de Abel, como $A_{h,n}(t) = 0$ cuando $t < 2$, se obtiene

$$\begin{aligned}\sum_{\substack{p\leq x\\ p\equiv h \pmod n}} \frac{1}{p} &= \frac{A_{h,n}(x)}{\log x} + \int_2^x \frac{A_{h,n}(t)}{t\log^2 t}dt \\ &= \frac{1}{\phi(n)} + \frac{1}{\phi(n)}O\bigg(\frac{1}{\log x}\bigg) + \frac{1}{\phi(n)}\int_2^x \frac{dt}{t\log t} + \frac{1}{\phi(n)}\int_2^x \frac{R_{h,n}(t)}{t\log^2 t}dt \\ &= \frac{1}{\phi(n)}\big[\log\log x - \log\log 2 + 1\big] + \frac{1}{\phi(n)}O\bigg(\frac{1}{\log x}\bigg),\end{aligned}$$

en donde se ha utilizado el teorema 4.1.1, y $R_{h,n}(t) = O(1)$. De esta última ecuación se sigue el resultado querido. □

CAPÍTULO 5

Una breve introducción a la teoría algebraica de números.

En este capítulo, se pondrán sin demostración algunos resultados básicos de teoría algebraica de números. La mayoría de los resultados enunciados acá, se encuentran demostrados en libros tales como [BS66, cap. 2] y [Neu99, cap. 1]; por tal motivo, si el lector está interesado en profundizar los resultados expuestos, está ampliamente invitado a consultar alguna de estas referencias.

5.1. Apartes de teoría algebraica de números.

Definición 5.1.1. *Sea K un cuerpo, se dice que K es un cuerpo de números si:*

i. K es un subcuerpo de $\mathbb{C}$.

ii. K es una extensión finita de $\mathbb{Q}$, con $n = [K, \mathbb{Q}]$.

A los elementos de K se les llama números algebraicos. Dado que $K = \mathbb{Q}(\alpha)$ para algún $\alpha \in K$, si $\beta \in K$ entonces β anula algún polinomio de grado menor o igual a n con coeficientes en $\mathbb{Z}$. Tal polinomio no necesariamente es mónico. En caso que el polinomio sea mónico se tiene la siguiente distinción:

Definición 5.1.2. *El conjunto de elementos de K que anulan algún polinomio mónico con coeficientes en $\mathbb{Z}$ se llama el conjunto de enteros algebraicos de K. Tal conjunto se denota con $\mathcal{O}_K$.*

Observación 5.1.3. *$\mathcal{O}_K$ es un anillo; más aún, $\mathcal{O}_K$ es un dominio de Dedekind.*

Proposición 5.1.4. *$\mathcal{O}_K$ es un grupo libre de rango n sobre $\mathbb{Z}$, es decir, existen $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathcal{O}_K$ tal que si $\alpha \in \mathcal{O}_K$, existen $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ donde*

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n.$$

El conjunto conformado por $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ se conoce como una base entera para $\mathcal{O}_K$.

Como cada extensión finita de $\mathbb{Q}$ es separable, se utilizan las propiedades de traza y norma con las notaciones habituales para un elemento $\alpha \in K$: $Tr_{K/\mathbb{Q}}(\alpha)$ y $N_{K/\mathbb{Q}}(\alpha)$ respectivamente.

Definición 5.1.5. *El discriminante de una base $\alpha_1, \alpha_2, \ldots, \alpha_n$ para K se define como:*

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(Tr_{K/\mathbb{Q}}(\alpha_i \alpha_j)).$$

Algunas propiedades que se verifican del discriminante de una base son las siguientes:

a. $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Q}$.

b. $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}$ si y solo si $\alpha_i \in \mathcal{O}_K$.

c. $\Delta(\beta_1, \beta_2, \ldots, \beta_n) = \det B^2 \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ en donde B es la matriz cambio de base de la base $\{\beta_1, \beta_2, \ldots, \beta_n\}$ a la base $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

De las propiedades *b.* y *c.* se deduce que si $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ y $\{\beta_1, \beta_2, \ldots, \beta_n\}$ son bases para $\mathcal{O}_K$, entonces $\Delta(\beta_1, \beta_2, \ldots, \beta_n) = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$, luego el discriminante de las bases para $\mathcal{O}_K$ es siempre el mismo, por tanto se define de manera natural:

Definición 5.1.6. *El discriminante de un cuerpo de números K, denotado por Δ_K, es el discriminante de cualquier base para $\mathcal{O}_K$.*

Si K es un cuerpo de números de grado n sobre $\mathbb{Q}$, existen exactamente n encajes distintos de K en el cuerpo $\mathbb{C}$. Esos encajes se clasifican de la siguiente manera:

Definición 5.1.7. *Si la imagen del cuerpo K bajo el encaje σ está contenido en $\mathbb{R}$, tal encaje se llama real; en caso contrario, el encaje es llamado complejo.*

Observación 5.1.8. *Si σ es un encaje complejo, entonces $\sigma \neq \overline{\sigma}$, de manera que hay un número par de encajes complejos.*

Se va a denotar por r_1 el número de encajes reales de K, y por r_2 el número de encajes complejos no conjugados de K, de manera que se tenga $n = r_1 + 2r_2$.

Definición 5.1.9. *Sea $\alpha_1, \alpha_2, \ldots, \alpha_n$ un conjunto de vectores linealmente independientes en $\mathbb{R}^n$, el conjunto $\mathfrak{M}$ que consta de los vectores de la forma*

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n,$$

donde $a_i \in \mathbb{Z}$, es llamado un retículo completo sobre $\mathbb{R}^n$, y $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ una base para $\mathfrak{M}$.

Además, si

$$T = \{a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n \mid 0 \leq a_i < 1\},$$

T es llamado un paralelepipedo fundamental del retículo $\mathfrak{M}$.

Es conveniente dotar a $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ con la siguiente norma:

$$||x||^2 = \sum_{i \leq r_1} x_i^2 + 2 \sum_{r_1 < i \leq r_2} |x_i|^2. \tag{5.1}$$

El hecho que aparezca dos veces la norma al cuadrado de los elementos complejos, modifica el diferencial de volumen en $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ a la siguiente relación:

$$d\,\mathrm{Vol} = 2^{r_2} dx_1 \cdots dx_{r_1} d\,\mathrm{Re}\, x_{r_1+1} d\,\mathrm{Im}\, x_{r_1+1} \cdots d\,\mathrm{Re}\, x_{r_1+r_2} d\,\mathrm{Im}\, x_{r_1+r_2}. \tag{5.2}$$

La métrica que se utiliza en $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ será entonces la inducida por la anterior norma.

El covolumen del retículo $\mathfrak{M}$ se define como:

$$\mathrm{CoVol}(\mathfrak{M}) = \mathrm{Vol}(\mathbb{R}^n/\mathfrak{M}) = \mathrm{Vol}(T).$$

Esta teoría fue trabajada ampliamente por Minkowski, y frecuentemente es llamada la *geometría de los números*; sin embargo, acá sólo se utilizarán algunas herramientas básicas sin entrar en detalle. Si se consideran los n encajes de K en $\mathbb{C}$ tal que $\sigma_1, \sigma_2, \ldots, \sigma_{r_1}$ son los r_1 encajes reales, y $\sigma_{r_1+1}, \overline{\sigma}_{r_1+1}, \sigma_{r_1+2}, \overline{\sigma}_{r_1+2}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+r_2}$ los encajes complejos; se tiene el siguiente homomorfismo:

$$\begin{aligned} j : K &\longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ x &\longrightarrow (\sigma_i(x))_{i \leq r_1+r_2}. \end{aligned} \tag{5.3}$$

Además se considera

$$\begin{aligned} N : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} &\longrightarrow \mathbb{C} \\ (x_i) &\longrightarrow \prod_{i \leq r_1} x_i \prod_{r_1 < i \leq r_1+r_2} x_i \overline{x}_i. \end{aligned}$$

Se observa que $N \circ j(\alpha) = N_{K/\mathbb{Q}}(\alpha)$. Si se considera también el homomorfismo para cada $x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ tal que $N(x) \neq 0$:

$$\begin{aligned} l : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} &\longrightarrow \mathbb{R}^{r_1+r_2} \\ (x_i) &\longrightarrow (a_i \log |x_i|) \end{aligned} \tag{5.4}$$

donde $a_i = 1$ si $i \leq r_1$ y $a_i = 2$ si $r_1 < i \leq r_1 + r_2$. Este homomorfismo es llamado logarítmico, y se cumple que si $\lambda = l \circ j$, entonces

$$\sum \lambda_i(x) = \log |N_{K/\mathbb{Q}}(x)|. \tag{5.5}$$

Teorema 5.1.10. *Si $\mathfrak{M} = j(\mathcal{O}_K)$, $\mathfrak{M}$ es un retículo completo de K y*

$$\mathrm{CoVol}\,\mathfrak{M} = \sqrt{|\Delta_K|}.$$

Teorema 5.1.11 (del punto en el retículo de Minkowski)**.** *Si $\mathfrak{M}$ es un retículo completo en un espacio vectorial euclideano V (esp. vect. sobre $\mathbb{R}$ con una forma bilineal simétrica definida positiva) y $X \subset V$ un conjunto convexo tal que si $x \in X$, se tiene que $-x \in X$ y tal que*

$$\mathrm{Vol}(X) > 2^n \ \mathrm{CoVol}\,\mathfrak{M},$$

entonces existe un punto $\gamma \in \mathfrak{M}$ tal que $\gamma \in X$.

Teorema 5.1.12. *Si $\mathfrak{a} \neq 0$ es un ideal de $\mathcal{O}_K$, entonces $\mathfrak{M} = j(\mathfrak{a})$ es un retículo completo y su covolumen está dado por:*

$$\mathrm{CoVol}\,\mathfrak{M} = \sqrt{|\Delta_K|}(\mathcal{O}_K : \mathfrak{a}).$$

Ahora se va a dar una definición generalizada de lo que se conoce como ideal de un anillo:

Definición 5.1.13. *Por un ideal fraccionario de K se conocerá a un conjunto $0 \neq \mathfrak{a} \subset K$ el cual es un $\mathcal{O}_K$-módulo finitamente generado.*

Observación 5.1.14. *$\mathfrak{a} \neq 0$ es un ideal fraccionario de K, si y solo si, existe $c \in K^*$ tal que $c\mathfrak{a} \subset \mathcal{O}_K$ es un ideal.*

Como cada ideal de $\mathcal{O}_K$ es un ideal fraccionario ($c = 1$) de K, a ellos se les conoce como ideales enteros de K.

Definición 5.1.15. *Si se considera $0 \neq \mathfrak{a}$ un ideal entero, entonces $(\mathcal{O}_K : \mathfrak{a})$ es finito, y se define la norma del ideal $\mathfrak{a}$ como*

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

Algunas de las propiedades más importantes de la norma de ideales son las siguientes:

i. Si $\alpha \in \mathcal{O}_K$, entonces $\mathfrak{N}((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$.

ii. $\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$.

Proposición 5.1.16. *Los ideales fraccionarios forman un grupo abeliano. Tal grupo J_K es llamado el grupo de ideales de K.*

Teorema 5.1.17. *Cada ideal fraccionario $\mathfrak{a} \neq 0$ admite una representación única de la forma*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v(\mathfrak{p})},$$

donde el producto recorre los ideales primos de $\mathcal{O}_K$ y $v(\mathfrak{p}) \in \mathbb{Z}$ con la condición que $v(\mathfrak{p}) = 0$ para casi todo $\mathfrak{p}$.

Definición 5.1.18. *Los ideales fraccionarios principales, $(\alpha) = \alpha\mathcal{O}_K$ donde $\alpha \in K^*$, forman un subgrupo de J_K denotado por P_K. El grupo cociente*

$$Cl_K = J_K/P_K$$

se llama el grupo de las clases de ideales de K.

Observación 5.1.19. *Se tiene la siguiente cadena exacta:*

$$1 \to \mathcal{O}_K^* \longrightarrow K^* \longrightarrow J_K \longrightarrow Cl_K \to 1$$

Se quiere ahora ver que el orden de Cl_K es finito, y para ello se necesita fuertemente el siguiente lema:

Lema 5.1.20. *Sea $\mathfrak{a} \neq 0$ un ideal de $\mathcal{O}_K$, entonces existe un elemento $\alpha \in \mathfrak{a}$ tal que*

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}\mathfrak{N}(\mathfrak{a}).$$

Con este lema, se obtiene el siguiente teorema, del cual se presenta un bosquejo de su demostración.

Teorema 5.1.21. *El grupo de las clases de ideales de K es finito y su orden es denotado por $h_K = (J_K : P_K)$.*

Demostración. Si $\mathfrak{p} \neq 0$ es un ideal primo de $\mathcal{O}_K$, entonces $\mathcal{O}_K/\mathfrak{p}$ es una extensión finita de $\mathbb{Z}/p\mathbb{Z}$ donde $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, y como hay sólo un número finito de ideales primos que cumplen esta condición, existe un número finito de ideales cuya norma es menor o igual a p, es decir, hay un número finito de ideales $\mathfrak{a} \in \mathcal{O}_K$ tal que

$$\mathfrak{N}(\mathfrak{a}) \leq M$$

para M un número fijo. Por tanto, si se logra probar que para cada $\mathfrak{a}$ existe $\mathfrak{a}' \in [\mathfrak{a}]$ tal que $\mathfrak{N}(\mathfrak{a}') \leq M$, el resultado del teorema queda demostrado. Dado que para $\mathfrak{a}^{-1}$ existe $\gamma \in K^*$ tal que $\mathfrak{b} = \gamma\mathfrak{a}^{-1} \subset \mathcal{O}_K$ por el lema anterior, existe $\alpha \in \mathfrak{b}$ tal que

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}\mathfrak{N}(\mathfrak{b}),$$

es decir $\mathfrak{N}((\alpha)\mathfrak{b}^{-1}) \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}$. Como $\alpha\mathfrak{b}^{-1} \in [\mathfrak{a}]$ pues $\alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a}$, el teorema queda así demostrado. □

5.2. Unidades y S-unidades de $\mathcal{O}_K$

Si se considera el grupo de unidades de $\mathcal{O}_K$

$$\mathcal{O}_K^* = \{\epsilon \in \mathcal{O}_K \mid N_{K/\mathbb{Q}}(\epsilon) = \pm 1\},$$

es interesante estudiar la estructura de este grupo. Sin embargo, en este escrito se pondrán solo puntos relevantes de las unidades de $\mathcal{O}_K$, y luego se verán algunos resultados de las $S-$*unidades*, las cuales están más acordes al propósito de este trabajo; además ellas son una definición más general de la definición de unidad.

Si se considera el homomorfismo λ, por la ecuación (5.5) se tiene que para cada unidad $\epsilon \in \mathcal{O}_K$

$$\sum \lambda_i(\epsilon) = 0,$$

entonces se tiene el siguiente teorema:

Teorema 5.2.1. *El conjunto $\lambda(\mathcal{O}_K^*)$ es un retículo completo contenido en el hiperplano $\mathcal{H}_0$ de $\mathbb{R}^{r_1+r_2}$ formado por los elementos*

$$\mathcal{H}_0 = \{x \in \mathbb{R}^{r_1+r_2} \mid \sum x_i = 0\}.$$

Notación 5.2.2. *Se notará a r como $r = \dim \mathcal{H}_0 = r_1 + r_2 - 1$.*

Teorema 5.2.3 (Dirichlet)**.** *Existen elementos $\epsilon_1, \epsilon_2, \ldots, \epsilon_r \in \mathcal{O}_K^*$ tal que para cada $\alpha \in \mathcal{O}_K^*$, existen únicos $a_1, a_2, \ldots, a_r \in \mathbb{Z}$ y η es una raíz de la unidad contenida en K tal que*

$$\alpha = \eta \epsilon_1^{a_1} \epsilon_2^{a_2} \cdots \epsilon_r^{a_r}.$$

Es decir, $\mathcal{O}_K^*$ es un grupo finitamente generado de rango r.

Definición 5.2.4. *El conjunto $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_r\}$ es llamado un conjunto de unidades fundamentales de K.*

Se tiene también que el conjunto formado por $\{\lambda(\epsilon_1), \ldots, \lambda(\epsilon_r)\}$ es una base para el hiperplano $\mathcal{H}_0$. Si se toma la forma $d\xi_1 \cdots d\xi_r$ en $\mathcal{H}_0$ como el elemento de volumen en $\mathcal{H}_0$, se tiene que

$$R_K = \mathrm{CoVol}(\lambda(\mathcal{O}_K^*)) = \int_{\mathcal{H}_0/\lambda(\mathcal{O}_K^*)} d\xi_1 \cdots d\xi_r$$

es llamado el regulador de unidades del cuerpo K. Se notará simplemente por R si no hay lugar a confusión.

Dado que $x \in \mathcal{H}_0/\lambda(\mathcal{O}_K^*)$ si

$$x = \xi_1 \lambda(\epsilon_1) + \cdots \xi_r \lambda(\epsilon_r),$$

cada vez que $0 \leq \xi_i < 1$, se verifica que R se puede hallar como el valor absoluto del determinante de un menor arbitrario de rango r de la siguiente matriz:

$$\begin{pmatrix} \lambda_1(\epsilon_1) & \cdots & \lambda_{r_1+r_2}(\epsilon_1) \\ \vdots & & \vdots \\ \lambda_1(\epsilon_r) & \cdots & \lambda_{r_1+r_2}(\epsilon_r) \end{pmatrix}. \tag{5.6}$$

Como el vector $l = 1/\sqrt{r_1 + r_2}(1, \ldots, 1) \in \mathbb{R}^{r_1+r_2}$ tiene norma 1 y es ortogonal a $\mathcal{H}_0$, se obtiene:

Observación 5.2.5. *El elemento de volumen usual en $\mathcal{H}_0$ inducido por la inclusión $\mathcal{H}_0 \to \mathbb{R}^{r_1+r_2}$ es $\sqrt{r_1 + r_2}$ veces el elemento $d\xi_1 \cdots d\xi_r$.*

El anterior manejo a las unidades de $\mathcal{O}_K$, es un tratamiento clásico y es el que ayuda a verificar las conjeturas de Stark en el caso de la función zeta de Dedekind (que aunque no se ha hablado de función zeta de Dedekind, ni de conjeturas de Stark, más adelante se retoman como un caso particular). Sin embargo, se puede modificar ligeramente la definición de unidad y debilitarla un poco vía localizaciones, y definir lo que se conoce como S-unidades que está acorde con el proposito de este trabajo.

Sea X un conjunto de ideales primos de un anillo $\mathfrak{A}$, se denota por $\mathfrak{A}(X)$ el siguiente conjunto:

$$\mathfrak{A}(X) = \left\{ \frac{a}{b} \mid a, b \in \mathfrak{A},\, b \notin \mathfrak{p}\ \forall \mathfrak{p} \in X \right\}.$$

Claramente se tiene que si X está conformado por un único ideal primo, el anillo $\mathfrak{A}(X)$ es la localización $\mathfrak{A}_{\mathfrak{p}}$ de $\mathfrak{A}$ mediante $\mathfrak{p}$, el cual es un anillo local, y si $\mathfrak{a}$ es su ideal máximal, las unidades a de $\mathfrak{A}_{\mathfrak{p}}$ son los elementos tal que $a \notin \mathfrak{a}$. El interés se centra ahora en las unidades de $\mathfrak{A}(X)$ para ciertos conjuntos especiales X.

Sea S un conjunto finito de ideales primos de $\mathcal{O}_K$, y sea X el conjunto de todos los ideales primos de $\mathcal{O}_K$ excepto aquellos que están en S. Si se pone

$$\mathcal{O}_K^S = \mathcal{O}_K(X),$$

las unidades de $\mathcal{O}_K^S$ son llamadas las S-unidades de $\mathcal{O}_K$. Tal conjunto se denotará por K^S.

Esta definición como se habia mencionado antes, debilita la definición de unidad de $\mathcal{O}_K$, ya que $a \in \mathcal{O}_K^*$, si y solo si, $a \notin \mathfrak{p}$ para cada ideal primo, mientras que $a \in K^S$ si a está a lo más en los ideales primos que pertenecen a S.

Si se denota por $Cl_K^S = Cl(\mathcal{O}_K^S)$ el grupo de S-clases de K se tiene la siguiente proposición:

Proposición 5.2.6. *La siguiente sucesión es exacta:*

$$1 \to \mathcal{O}_K^* \longrightarrow K^S \longrightarrow \bigoplus_{\mathfrak{p} \in S} K^*/\mathcal{O}_{\mathfrak{p}}^* \longrightarrow Cl_K \longrightarrow Cl_K^S \to 1,$$

y además $K^*/\mathcal{O}_{\mathfrak{p}}^* \cong \mathbb{Z}$, donde $\mathcal{O}_{\mathfrak{p}}$ es la localización de $\mathcal{O}_K$ por el ideal primo $\mathfrak{p}$.

Se siguen como corolarios los siguientes:

Corolario 5.2.7. *$K^S \cong \mu(K) \times \mathbb{Z}^{\#S+r}$ donde $\mu(K)$ es el conjunto de las raices de la unidad contenidas en K.*

Corolario 5.2.8. *El grupo de las S-clases Cl_K^S es finito.*

5.3. La función zeta de Dedekind.

Con las notaciones y definiciones introducidas hasta el momento, se puede definir la función zeta de Dedekind.

Definición 5.3.1. *La función zeta de Dedekind asociada al cuerpo K se define como:*

$$\zeta_K(s) = \sum \frac{1}{\mathfrak{N}(\mathfrak{a})^s},$$

donde la suma recorre sobre los ideales enteros de K.

Como se puede observar, la función zeta de Riemann no es más que la función zeta de Dedekind asociada al cuerpo $\mathbb{Q}$, y tal como ella, se tienen propiedades similares a las descritas en el capítulo 1. A continuación se presenta esta función en términos de un producto de Euler.

Proposición 5.3.2. *La función $\zeta_K(s)$ converge absoluta y uniformemente para todo número complejo s tal que $\mathrm{Re}(s) > 1$, y además se tiene que*

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \mathfrak{N}(\mathfrak{p})^{-s}\right)^{-1},$$

donde el producto recorre todos los ideales primos de K.

La demostración de esta proposición sigue los mismos pasos realizados en el teorema 1.2.3 de la función zeta de Riemann, solo que acá se utiliza el hecho que cada ideal entero de K se factoriza de manera única en ideales primos tal como se mencionó en el teorema 5.1.17. Por tanto, su demostración es omitida.

En un estudio más profundo de la función $\zeta_K(s)$, se logra demostrar que ella se puede prolongar analíticamente y cumple una ecuación funcional análoga a la que cumple la función zeta de Riemann. Esta demostración, debida a Hecke, generaliza las herramientas utilizadas en el capítulo 1, como por ejemplo el estudio de una serie theta asociada a $\zeta_K(s)$, estudio que en estas páginas no será hecho, pues esto llevaría quizá algunos capítulos adicionales, y ese no es uno de los objetivos propuestos, por tanto el teorema solo se enunciará.

Si para cada encaje real se toma el término $L_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2)$, y para cada encaje complejo el término $L_{\mathbb{C}}(s) = 2(2\pi)^s\Gamma(s)$, dado que hay r_1 encajes reales y r_2 encajes complejos, se tiene el factor

$$L_\infty(s) = L_{\mathbb{R}}^{r_1}(s)L_{\mathbb{C}}^{r_2}(s). \tag{5.7}$$

Estos términos salen de manera parecida a como salió el término $\pi^{-s/2}\Gamma(s/2)$ en la demostración del teorema 1.2.4.

Teorema 5.3.3. *La función*

$$Z_K(s) = |\Delta_K|^{s/2}L_\infty(s)\zeta_K(s)$$

puede ser extendida analíticamente a $\mathbb{C} \setminus \{0, 1\}$ y satisface la ecuación funcional

$$Z_K(s) = Z_K(1 - s).$$

Con esto se concluyen algunos de los resultados de la teoría algebraica de números que serán utilizados en los capítulos finales.

CAPÍTULO 6

La fórmula del número de clases de Dedekind.

El objetivo de este capítulo, es hallar el valor del residuo de la función $\zeta_K(s)$ en el punto $s = 1$, y finalmente, relacionar este resultado con el número de clases de Dirichlet. Para ello, son necesarios algunos resultados previos.

6.1. El número de clases de Dedekind.

Gracias al corolario 5.2.1, y a que el vector

$$l^* = (\underbrace{1, \ldots, 1}_{r_1 veces}, \underbrace{2, \ldots, 2}_{r_2 veces}) \notin \mathcal{H}_0,$$

el conjunto formado por los elementos

$$l^*, \lambda(\epsilon_1), \ldots, \lambda(\epsilon_r) \tag{6.1}$$

es una base para $\mathbb{R}^{r_1+r_2}$. Por tanto, para cada $x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ tal que $N(x) \neq 0$, se tiene que

$$l(x) = \xi l^* + \xi_1 \lambda(\epsilon_1) + \cdots + \xi_r \lambda(\epsilon_r) \tag{6.2}$$

donde $\xi, \xi_1, \ldots, \xi_r \in \mathbb{R}$. Sea w el número de raices de la unidad contenidas en K;

Definición 6.1.1. *Sea X el subconjunto de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ tal que:*

a. Si $x \in X$, entonces $N(x) \neq 0$.

b. Los elementos $\xi_1, \ldots, \xi_r$ en la representación de (6.2) cumplen las desigualdades $0 \leq \xi_i < 1$.

c. Si x_1 es la primera componente de x, entonces $0 \leq \arg x_1 < 2\pi/w$.

En caso que $r_1 > 0$, la última condición no es otra cosa que $x > 0$. Además el conjunto X es un cono en el cual el punto $0 \notin X$.

Lema 6.1.2. *Si $y \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ y $N(y) \neq 0$, entonces y se puede escribir de manera única como*

$$y = j(\epsilon)x$$

donde $x \in X$ y ϵ es una unidad de $\mathcal{O}_K$. Además si $\epsilon \neq 1$, se tiene que $y \notin X$.

Demostración. Al representar $l(y)$ en terminos de la base dada en la ecuación (6.1) se tiene que

$$l(y) = \gamma l^* + \gamma_1 \lambda(\epsilon_1) + \cdots + \gamma_r \lambda(\epsilon_r).$$

Si para cada $i = 1, \ldots, r$ se toma

$$k_i = \lfloor \gamma_i \rfloor \qquad \text{y} \qquad \xi_i = \gamma_i - k_i,$$

sea $\eta = \epsilon_1^{k_1} \cdots \epsilon_r^{k_r}$, entonces si $z = j(\eta^{-1})y$ se tiene que

$$l(z) = l(y) + \lambda(\eta^{-1}) = \gamma l^* + \xi_1 \lambda(\epsilon_1) + \cdots + \xi_r \lambda(\epsilon_r).$$

Sea $m \in \mathbb{N}$ tal que

$$0 \leq \arg z_1 - \frac{2\pi m}{w} < \frac{2\pi}{w}$$

y sea $\varsigma \in K$ la raíz primitiva de la unidad contenida en K tal que $\arg \sigma_1(\varsigma) = 2\pi/w$. Se tiene entonces que el punto

$$x = j(\varsigma^{-m})z \in X,$$

pues $l(x) = l(z)$ ya que $\lambda(\varsigma^{-m}) = (\log |\sigma_i(\varsigma^{-m})|) = 0$, y

$$\arg x_1 = \arg z_1 - m \arg \sigma_1 \varsigma < \frac{2\pi}{w}.$$

Con las construcciones anteriores, se tiene ahora que

$$y = j(\eta)z = j(\eta)j(\varsigma^m)x = j(\varsigma^m \eta)x,$$

donde $x \in X$ y $\varsigma^m \eta$ es una unidad de $\mathcal{O}_K$. La demostración de la unicidad es estándar a este tipo de demostraciones, por tanto será omitida. □

Con el anterior lema, el siguiente teorema es inmediato:

Teorema 6.1.3. *En cada clase de números asociados de K hay uno y solo un número para el cual su representación geométrica en $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ está en X.*

Demostración. Sea $\alpha \in K$, por el anterior lema se tiene que

$$j(\alpha) = j(\epsilon)x$$

donde $x \in X$ y ϵ es una unidad de $\mathcal{O}_K$. Sea $\beta = \epsilon^{-1}\alpha$, entonces $j(\beta) \in X$ pues

$$j(\beta) = j(\epsilon^{-1}\alpha) = x.$$

El teorema queda demostrado ya que por la última parte del lema 6.1.2, si $\gamma \neq \alpha$ y es asociado a α, se tiene que $\gamma = \epsilon\alpha$ donde $\epsilon \neq 1$, por tanto

$$j(\gamma) = j(\epsilon\alpha) = j(\epsilon)x \notin X.$$

□

Si se considera ahora la siguiente función:

$$\mathfrak{Z}(s) = \sum_{x \in \mathfrak{M} \cap Y} \frac{1}{|N(x)|^s}, \qquad (s > 1) \tag{6.3}$$

donde $\mathfrak{M}$ es un retículo completo en $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ cuyo covolumen está dado por Δ y Y es un cono en $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ tal que el origen no está en Y, se tiene

Teorema 6.1.4. *La serie $\mathfrak{Z}(s)$ converge para cada $s > 1$ y*

$$\lim_{s \to 1}(s-1)\mathfrak{Z}(s) = \frac{v}{\Delta},$$

donde v es el volumen del conjunto T dado por:

$$T = \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |N(x)| \leq 1\} \cap Y.$$

Demostración. Sea $k > 0$, se denotará por $\mathfrak{M}_k$ el retículo obtenido al multiplicar cada punto de $\mathfrak{M}$ por un factor k. Como una base para $\mathfrak{M}_k$ es una base para $\mathfrak{M}$ multiplicado por el factor k, se tiene que

$$\Delta_k = \frac{\Delta}{k^n}.$$

Por un argumento similar al dado en la demostración del teorema 3.4.6, si $U(k)$ es el número de puntos del reticulo $\mathfrak{M}_k$ contenidos en el conjunto T, se tiene que el volumen v está dado por

$$v = \lim_{k \to \infty} U(k)\frac{\Delta}{k^n} = \Delta \lim_{k \to \infty} \frac{U(k)}{k^n}. \tag{6.4}$$

Como $U(k)$ es también el número de puntos del retículo $\mathfrak{M}$ contenidos en la expansión kT de T por un factor de k, se tiene que el número de puntos $x \in \mathfrak{M} \cap X$ para los cuales $|N(x)| \leq k^n$ es $U(k)$ (pues $x \in kT$ sii $|N(x)| \leq k^n$).

Si se ordenan los puntos de $\mathfrak{M} \cap X$ en una sucesión $\{x_i\}$ tal que

$$0 < |N(x_1)| \leq |N(x_2)| \leq \cdots \leq |N(x_i)| \leq \cdots$$

donde $|N(x_i)| = k_i^n$, se tiene que los puntos $x_1, x_2, \ldots, x_i \in k_i T$, luego $U(k_i) \geq i$ y dado que para cada $\epsilon > 0$ se tiene que $x_i \notin (k_i - \epsilon)T$, entonces

$$U(k_i - \epsilon) < i \leq U(k_i).$$

Por tanto se tiene lo siguiente:

$$\frac{U(k_i - \epsilon)}{(k_i - \epsilon)^n}\left(\frac{k_i - \epsilon}{k_i}\right)^n < \frac{i}{k_i^n} \leq \frac{U(k_i)}{k_i^n},$$

y al tomar el límite cuando i va al infinito, k_i también va al infinito, y por la ecuación (6.4) se tiene que:

$$\lim_{i \to \infty} \frac{i}{|N(x_i)|} = \frac{v}{\Delta}.$$

Luego para cada $\epsilon > 0$, existe $N_0 \in \mathbb{N}$ tal que si $i > N_0$

$$\left(\frac{v}{\Delta} - \epsilon\right)\frac{1}{i} < \frac{1}{|N(x_i)|} < \left(\frac{v}{\Delta} + \epsilon\right)\frac{1}{i},$$

por tanto

$$\left(\frac{v}{\Delta}-\epsilon\right)^s \sum_{i=N_0+1} \frac{1}{i^s} < \sum_{i=N_0+1} \frac{1}{|N(x_i)|^s} < \left(\frac{v}{\Delta}+\epsilon\right)^s \sum_{i=N_0+1} \frac{1}{i^s}$$

para cada $s > 1$. Por otro lado se tiene que

$$\lim_{s\to 1}(s-1)\sum_{i\leq N_0} \frac{1}{|N(x_i)|^s} = 0 \qquad \text{y} \qquad \lim_{s\to 1}(s-1)\sum_{i\leq N_0} \frac{1}{i^s} = 0.$$

Este hecho y la observación 1.2.6 permite concluir que

$$\frac{v}{\Delta}-\epsilon \leq \liminf_{s\to 1} \mathfrak{Z}(s) \leq \limsup_{s\to 1} \frac{v}{\Delta}+\epsilon.$$

Por tanto el teorema queda probado. □

Como en la anterior fórmula aparece el volumen del conjunto T, ahora se va a calcular tal valor. Hay que tener en cuenta que si ϵ es una unidad de $\mathcal{O}_K$, entonces la transformación en $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ dada por $x \to j(\epsilon)x$ preserva el volumen de una región, pues el determinante de la transformación es $|N_{K/\mathbb{Q}}(\epsilon)| = 1$.

Teorema 6.1.5. *El volumen del conjunto T está dado por la fórmula*

$$v = \frac{2^{r_1}(2\pi)^{r_2}R}{w}.$$

Calcular el volumen v directamente no es sencillo, por esta razón se calculará un volumen que está relacionado con v. Se tendrá en cuenta que la norma utilizada en $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ es la definida en la ecuación (5.2).

Demostración. Sea como antes, ς la raíz de la unidad contenida en K tal que $\arg \sigma_1(\varsigma) = 2\pi/w$. Para cada $0 \leq k \leq r$ se consideran los conjuntos T_k donde:

$$\begin{aligned} T &\longrightarrow T_k \\ x &\longrightarrow j(\varsigma^k)x \end{aligned}$$

Por lo mencionado antes de este teorema, T_k tiene el mismo volumen de T. Dado que

$$\begin{aligned} &|N(j(\varsigma^k)x)| = |N(x)||N(\varsigma^k)| = |N(x)|, \\ &l(j(\varsigma^k)x) = \lambda(\varsigma^k) + l(x) = l(x) \\ &\arg(j(\varsigma^k)x)_1 = \arg x_1 + \tfrac{2\pi k}{w}, \end{aligned}$$

entonces $x \in T_k$ si

a. $0 \leq |N(x)| < 1$.

b. Los escalares ξ_i de la ecuación (6.2) cumplen que $0 \leq \xi_i < 1$.

c. $\frac{2\pi k}{w} \leq \arg x_1 < \frac{2\pi(k+1)}{w}$.

Por tanto, $T = T_0, T_1, \ldots, T_{w-1}$ son conjuntos dos a dos disjuntos. Sea $T' = \bigcup T_k$ y

$$\overline{T} = \{x \in T' \,|\, x_1 > 0, x_2 > 0, \ldots, x_{r_1} > 0\}.$$

Sea el punto $\eta = (\delta_1, \ldots, \delta_{r_1}, 1, \ldots, 1) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ donde $\delta_i \in \{-1, 1\}$. La transformación dada por $x \to j(\eta)x$ preserva el volumen de $\overline{T}$, y la imagen de $\overline{T}$ bajo la transformación, es un subconjunto de T'. Al considerar las 2^{r_1} posibles transformaciones, la unión de las imágenes de todas ellas coincide con T', por tanto

$$\text{Vol}(T') = 2^{r_1} \text{Vol}(\overline{T}).$$

Como $\text{Vol}(T')$ es w veces el volumen v del conjunto T, entonces

$$v = \frac{2^{r_1}}{w} \text{Vol}(\overline{T}), \tag{6.5}$$

de manera que es suficiente calcular el volumen del conjunto $\overline{T}$. Al retomar la ecuación (5.5), dado que $|N_{K/\mathbb{Q}}(\epsilon_i)| = 1$ para cada unidad fundamental, entonces por la descomposición de la ecuación (6.2), se tiene que para $x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$

$$\log |N(x)| = \xi(r_1 + 2r_2) = n\xi,$$

por tanto, el coeficiente ξ en la descomposición de la ecuación (6.2) está dado por

$$\xi = \frac{\log |N(x)|}{n},$$

y así se obtiene que

$$l(x) = \frac{\log |N(x)|}{n} l^* + \xi_1 \lambda(\epsilon_1) + \cdots + \xi_r \lambda(\epsilon_r); \tag{6.6}$$

de manera que al tomar la componente i-ésima del vector $l(x)$ se tiene

$$l_i(x) = \frac{a_i \log |N(x)|}{n} + \sum_{k \leq r} \xi_k \lambda_i(\epsilon_k),$$

donde a_i se toma como en la ecuación (5.4). Para calcular el volumen de $\overline{T}$, es conveniente hacer el cambio de variable siguiente:

$$\begin{array}{rl} x_k = \rho_k & k \leq r_1 \\ \left.\begin{array}{l} y_k = \rho_{r_1+k} \cos \phi_k \\ z_k = \rho_{r_1+k} \sin \phi_k \end{array}\right\} & r_1 < k \leq r_1 + r_2 \end{array}$$

donde $x_{r_1+k} = y_k + iz_k$. Un cálculo directo da el valor del jacobiano como

$$J = \rho_{r_1+1} \cdots \rho_{r_1+r_2}. \tag{6.7}$$

El conjunto $\overline{T}$ queda descrito de la siguiente forma en términos de las variables $\{\rho_i\}$, $\{\phi_k\}$:

a. $0 \leq \phi_i < 2\pi$.

b. $\rho_1 > 0, \ldots, \rho_{r_1+r_2} > 0$ y $\prod \rho_i^{a_1} \leq 1$.

c. Los coeficientes ξ_i en la ecuación

$$\log \rho_j^{a_j} = \frac{a_j}{n} \log \left(\prod_i \rho_i^{a_i} \right) + \sum_i \xi_i \lambda_j(\epsilon_i),$$

satisfacen que $0 \leq \xi_i < 1$.

Al hacer el cambio de variable a $\{\xi, \xi_1, \ldots, \xi_r\}$ dado por

$$\log \rho_j^{a_j} = \frac{a_j}{n} \log \xi + \sum_i \xi_i \lambda_j(\epsilon_i), \tag{6.8}$$

se tiene que

$$\xi = \prod \rho_i^{a_i}.$$

Por tanto, el conjunto $\overline{T}$ queda determinado en las variables $\xi, \xi_1, \ldots, \xi_r$ por las condiciones

$$0 \leq \xi \leq 1, \qquad 0 \leq \xi_i < 1 \quad \text{para cada } i = 1, 2, \ldots, r.$$

El jacobiano de esta última transformación es:

$$\begin{aligned} J &= \det \begin{pmatrix} \frac{\rho_1}{n\xi} & \rho_1 \lambda_1(\epsilon_1) & \cdots & \rho_1 \lambda_1(\epsilon_r) \\ \vdots & \vdots & & \vdots \\ \frac{\rho_{r_1+r_2}}{n\xi} & \frac{\rho_{r_1+r_2}}{2} \lambda_{r_1+r_2}(\epsilon_1) & \cdots & \frac{\rho_{r_1+r_2}}{2} \lambda_{r_1+r_2}(\epsilon_r) \end{pmatrix} \\ &= \frac{\rho_1 \cdots \rho_{r_1+r_2}}{n\xi 2^{r_2}} \det \begin{pmatrix} 1 & \lambda_1(\epsilon_1) & \cdots & \lambda_1(\epsilon_r) \\ \vdots & \vdots & & \vdots \\ 2 & \lambda_{r_1+r_2}(\epsilon_1) & \cdots & \lambda_{r_1+r_2}(\epsilon_r) \end{pmatrix} \\ &= \frac{\rho_1 \cdots \rho_{r_1+r_2}}{n\xi 2^{r_2}} nR = \frac{R}{2^{r_2} \rho_{r_1+1} \cdots \rho_{r_1+r_2}}. \end{aligned} \tag{6.9}$$

En el último determinante, se ha tenido en cuenta la ecuación (5.6). Con estos cambios de variable, dado que el producto de los dos jacobianos presentados en (6.7) y (6.9) es $R/2^{r_2}$, y que el elemento de volumen según la ecuación (5.1) es

$$2^{r_2} dx_1 \cdots dx_r \, d \operatorname{Re} x_{r_1+1} d\Im x_{r_1+1} \cdots d \operatorname{Re} x_{r_1+r_2} d\Im x_{r_1+r_2},$$

el volumen de $\overline{T}$ queda expresado de la siguiente forma:

$$\begin{aligned} \operatorname{Vol} \overline{T} &= \frac{R}{2^{r_2}} \int_0^{2\pi} \cdots \int_0^{2\pi} \int_0^1 \cdots \int_0^1 2^{r_2} d\xi d\xi_1 \cdots d\xi_r d\phi_1 \cdots d\phi_{r_2} \\ &= (2\pi)^{r_2} R. \end{aligned}$$

Gracias a la expresión dada en la ecuación (6.5), se tiene entonces que

$$v = \frac{2^{r_1} (2\pi)^{r_2}}{w} R$$

tal como se quería. □

Con estos argumentos, entonces se puede calcular el siguiente límite:

Teorema 6.1.6 (Número de clases de Dedekind.)**.**

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}Rh_K}{w\sqrt{|\Delta_K|}}$$

donde h_K es el número de clases de ideales de K, R es el regulador del cuerpo, y w es el número de raices de la unidad contenidas en K.

Demostración. Para demostrar este resultado, se va a partir la función zeta de Dedekind en funciones parciales de la siguiente manera:

$$\zeta_K(s,C) = \sum_{\mathfrak{a}\in\hat{C}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s},$$

donde $\hat{C}$ es el conjunto de ideales enteros que pertenecen a la clase C, de manera que se satisface la siguiente igualdad:

$$\zeta_K(s) = \sum_{C} \zeta_K(s,C).$$

Si se logra demostrar que

$$\lim_{s\to 1}(s-1)\zeta_K(s,C) = \frac{2^{r_1}(2\pi)^{r_2}R}{w\sqrt{|\Delta_K|}},$$

el resultado del teorema será inmediato.

Sea $\mathfrak{a}' \in C^{-1}$ un ideal fijo. La aplicación de $\hat{C} \to P_K$ tal que $\mathfrak{a} \to \mathfrak{a}\mathfrak{a}' = (\alpha)$ para algún $\alpha \in K^*$, es una función inyectiva si se toman elementos no asociados, pues $(\alpha) = (\epsilon\alpha)$ para cada $\epsilon \in \mathcal{O}_K^*$. Dado que

$$\mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{a}') = |N_{K/\mathbb{Q}}(\alpha)|,$$

se puede tomar

$$\zeta_K(s,C) = \mathfrak{N}(\mathfrak{a}')^s \sum_{(\alpha)\equiv 0 \pmod{\mathfrak{a}'}} \frac{1}{|N_{K/\mathbb{Q}}(\alpha)|^s} \tag{6.10}$$

donde la suma se toma sobre un conjunto de representantes no asociados. Para ello se utiliza el teorema 6.1.3. Sea $\mathfrak{M}$ el retículo en $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ que consiste de las imagenes $j(\alpha)$, donde $\alpha \in \mathcal{O}_K$ tal que $\alpha \equiv 0 \pmod{\mathfrak{a}'}$, es decir, $\mathfrak{M} = j(\mathcal{O}_K \cap \mathfrak{a}')$. La serie (6.10) puede verse entonces como

$$\zeta_K(s,C) = \mathfrak{N}(\mathfrak{a}')^s \sum_{x\in\mathfrak{M}\cap X} \frac{1}{|N(x)|^s}.$$

Por el teorema 6.1.4, el teorema 6.1.5 y el teorema 5.1.12, se tiene que

$$\lim_{s\to 1}(s-1)\zeta_K(s,C) = \frac{v}{\Delta}\mathfrak{N}(\mathfrak{a}') = \frac{2^{r_1}(2\pi)^{r_2}R}{w\sqrt{|\Delta_K|}}.$$

Con esto queda demostrado el teorema. □

Gracias al teorema 5.3.3, sigue de inmediato el siguiente corolario.

Corolario 6.1.7. *La función $Z_K(s)$ tiene polos simples en $s = 0$ y $s = 1$ cuyos residuos son:*

$$-\frac{2^{r_1+r_2}h_K R}{w} \qquad y \qquad \frac{2^{r_1+r_2}h_K R}{w}$$

respectivamente.

Demostración. Por la ecuación (5.7), se tiene que $L_\infty(1) = \pi^{-r_2}$, por tanto

$$\lim_{s\to 1}(s-1)Z_K(s) = \lim_{s\to 1}(s-1)|\Delta_K|^{s/2}L_\infty(s)\zeta_K(s) = \frac{2^{r_1+r_2}Rh_k}{w}.$$

El residuo en $s = 0$ sale de la ecuación funcional que cumple $Z_K(s)$:

$$\lim_{s\to 0} sZ_K(s) = \lim_{s\to 1}(1-s)Z_K(1-s) = \lim_{s\to 1}(1-s)Z_K(s) = -\frac{2^{r_1+r_2}Rh_k}{w}.$$

□

Gracias al residuo de la función $Z_K(s)$ en $s = 0$, se puede verificar de manera fácil el siguiente corolario:

Corolario 6.1.8. *La función $\zeta_K(s)$ tiene un cero de orden r en $s = 0$ y su primer coeficiente en el desarrollo de Taylor al rededor de cero es*

$$-\frac{Rh_K}{w}.$$

Demostración. Dado que la función Γ tiene un polo de orden 1 en $s = 0$, $L_\infty(s)$ tiene un polo de orden $r_1 + r_2$ en $s = 0$, además

$$\lim_{s\to 0} s^{r_1+r_2}L_\infty(s) = 2^{r_1+r_2},$$

al expresar la función Γ como en la definición. Por tanto

$$\lim_{s\to 0}\frac{\zeta_K(s)}{s^r} = \lim_{s\to 0}\frac{Z_K(s)}{s^r|\Delta_K|^{s/2}L_\infty(s)} = -\frac{Rh_K}{w}.$$

□

6.2. Las funciones $\zeta_{K,S}$

La siguiente función no es más que una generalización de la función zeta de Dedekind, y las demostraciones de los resultados que se obtienen, siguen las mismas pautas, por tanto los teoremas que se presentan a continuación no serán demostrados.

Definición 6.2.1. *Por un lugar de K, se entenderá una clase de equivalencia de valores absolutos no triviales sobre el cuerpo K.*

Un conocido teorema dice que cada lugar de K viene de la valuación $\mathfrak{p}-$ádica para un primo $\mathfrak{p}$, o es el valor absoluto de los encajes de K. A los últimos se les conoce como lugares infinitos, y por S_∞ se denotará el conjunto de tales lugares.

Sea S un conjunto finito de lugares de K tal que $S_\infty \subset S$. Para $\mathrm{Re}(s) > 1$, la función zeta de Dedekind incompleta está dada por

$$\zeta_{K,S}(s) = \prod_{\mathfrak{p}\notin S}(1 - \mathfrak{N}(\mathfrak{p})^{-s})^{-1}.$$

En este caso, al hablar de ideal fraccionario de K, se habla de un O_K^S-módulo, y se denota por h_S el número de clases de ideales de K respecto al anillo O_K^S. Por el corolario 5.2.7, si $r = \#S - 1$ existen unidades $u_1, \ldots, u_r$ tal que $\{u_1, u_2, \ldots, u_r\}$ es una base para K^S. Dado un lugar arbitrario $\mathfrak{p}_0 \in S$,

$$R_S = \left| \det_{\substack{1\leq i\leq r \\ \mathfrak{p}\in S\setminus\{\mathfrak{p}_0\}}} (\log |u_i|_\mathfrak{p}) \right|$$

es llamado el $S-$regulador de K, y no depende de la elección de $\mathfrak{p}_0$.

Con estas definiciones, se generaliza el corolario 6.1.8 mediante la siguiente proposición:

Proposición 6.2.2. *La función $\zeta_{K,S}(s)$ satisface que*

$$\zeta_{K,S}(s) \sim -\frac{h_S R_S}{w} s^r$$

en una vecindad de $s = 0$.

No se puede dar por terminado este capítulo sin antes relacionar la función zeta de Dedekind con la función L de Dirichlet.

Teorema 6.2.3. *La función zeta de Dedekind de un cuerpo cuadrático de discriminante D satisface la siguiente igualdad:*

$$\zeta_K(s) = \zeta(s)L(s,\chi)$$

Dado que $\zeta(s)$ tiene un polo en $s = 1$ con residuo 1, entonces se tiene:

Si $D > 0$, entonces $r_1 = 2$ y $r_2 = 0$, por tanto, según el teorema 6.1.6,

$$L(1,\chi) = \lim_{s\to 1}(s-1)\zeta(s)L(s,\chi) = \lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2R}{\sqrt{d}}h.$$

El regulador R de un cuerpo cuadrático cuando $D > 0$ es $R = \log \epsilon_0$, donde ϵ_0 es la unidad fundamental de $\mathcal{O}_K$.

Si $D < 0$, entonces $r_1 = 0$ y $r_2 = 1$, por tanto el regulador del cuerpo es 1, y según el teorema 6.1.6,

$$L(1,\chi) = \lim_{s\to 1}(s-1)\zeta(s)L(s,\chi) = \lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2\pi}{w_d\sqrt{|d|}}h.$$

Esto es justo lo que nos dice la observación 3.4.10. Luego hasta el momento, la función zeta de Riemann, las funciones L de Dirichlet y finalmente, la función zeta de Dedekind, están profundamente relacionadas.

CAPÍTULO 7

Conjeturas de Stark sobre valores especiales de funciones L más generales.

En este último capítulo, se dará una pequeña explicación sin entrar en detalle acerca de funciones L más generales como lo son las L de Hecke y las L de Artin; se presentará su ecuación funcional, y como cierre de este escrito, se expondrá la conjetura de Stark en su forma más simple, ya que a través de los años ha sido reformulada y generalizada, que solo entender su enunciado nos llevaría quizá un escrito similar a este. El lector interesado en entrar en los detalles expuestos puede consultar por ejemplo [Neu99, Tat84, Ser77].

7.1. Las funciones L de Hecke.

Antes de presentar las funciones L de Hecke, es necesario algunas notaciones básicas. Sea $\mathfrak{f}$ un ideal entero de K, sea

$$I(\mathfrak{f}) = \{\mathfrak{a} \,|\, \mathfrak{a} \text{ es ideal fraccionario de } K \text{ y es primo relativo a } \mathfrak{f}\}.$$

Por primo relativo se entenderá un ideal $\mathfrak{a}$ tal que ningún ideal primo que divide a $\mathfrak{f}$ aparece en la descomposición de $\mathfrak{a}$; $P(\mathfrak{f})$ está definido por $P(\mathfrak{f}) = P_K \cap I(\mathfrak{f})$; y además

$$K(\mathfrak{f}) = \{\alpha \in K \,|\, (\alpha) \in P(\mathfrak{f})\}.$$

Por $K_{\mathfrak{f}}$ se notará el conjunto formado por aquellos elementos $\alpha \in K(\mathfrak{f})$ tal que $\alpha \equiv 1 \mod {}^*\mathfrak{f}$, en donde $\alpha \equiv 1 \mod {}^*\mathfrak{f}$ significa

$$\alpha \equiv 1 \mod \mathfrak{f}\mathcal{O}_T$$

con $T = \cup_{\mathfrak{p}|\mathfrak{f}}\mathfrak{p}$. Finalmente por $P_{\mathfrak{f}}$ se entenderá el subgrupo de $P(\mathfrak{f})$ formado por los ideales principales (α) tal que $\alpha \in K_{\mathfrak{f}}$.

Definición 7.1.1. *Sea $\chi : I(\mathfrak{f}) \longrightarrow \mathbb{C}$ un carácter del grupo $I(\mathfrak{f})$. Si existe un homomorfismo continuo χ_∞ de $(\mathbb{R} \otimes_{\mathbb{Q}} K)^* \longrightarrow \mathbb{C}$ que satisface*

$$\chi((\alpha)) = \frac{1}{\chi_\infty(\alpha)}$$

para cada $\alpha \in K_{\mathfrak{f}}$, entonces el carácter χ se llama un carácter de Hecke módulo $\mathfrak{f}$ y χ_∞ es llamado su tipo infinito.

Cabe recordar que $\mathbb{R} \otimes_{\mathbb{Q}} K \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ si $1 \otimes \alpha \to (\sigma_i(\alpha))$ en donde $\{\sigma_i\}$ se toma como en la ecuación (5.3).

Definición 7.1.2. *Si el carácter de Hecke χ módulo $\mathfrak{f}$ es tal que $\chi'|_{I(\mathfrak{f})} = \chi$ en donde χ' es un carácter de Hecke módulo $\mathfrak{f}'$ y $\mathfrak{f}'$ es el ideal más grande para el cual se tiene la restricción, entonces $\mathfrak{f}'$ es llamado el conductor del carácter χ.*

Definición 7.1.3. *Sea $(p_\sigma) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ donde σ recorre el conjunto de encajes de K, se dice que (p_σ) es un elemento admisible si $p_\sigma \in \{0, 1\}$ cada vez que σ sea real, y $p_\sigma p_{\overline{\sigma}} = 0$ si σ es complejo y $p_\sigma, p_{\overline{\sigma}} \in \mathbb{Z}^+ \cup \{0\}$.*

Si para los elementos en $\mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$, las operaciones realizadas se hacen componente a componente, entonces el caracter χ_∞ se puede expresar de la siguiente manera:

Proposición 7.1.4. *Si χ es un carácter de Hecke módulo $\mathfrak{f}$ y χ_∞ es su tipo infinito, entonces existen elementos únicos $p, q \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ donde p es un elemento admisible tal que*

$$\chi_\infty(x) = N(x^p |x|^{-p+iq}).$$

Como los elementos p, q determinan el carácter χ_∞, entonces se dice que el carácter χ es de tipo (p, q).

Definición 7.1.5. *Para un carácter de Hecke χ módulo $\mathfrak{f}$, se define la función L de Hecke asociada a χ como*

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

donde el producto recorre todos los ideales primos de K, excepto aquellos que dividen a $\mathfrak{f}$.

Como ya se mencionó anteriormente, Hecke logró demostrar que este tipo de funciones L se podía prolongar analíticamente a todo el plano complejo, excepto a lo más algunos puntos. Su demostración utiliza herramientas generales a las descritas en el capítulo 1, motivo por el cual no se expondrá. Además sería un esfuerzo innecesario, pues John Tate en su tesis doctoral dirigida por Emil Artin en 1950, hizo una demostración más transparente de este hecho utilizando idéles, objetos matemáticos que fueron introducidos por Weil y Chevaley en los años treintas y cuarentas.

La importancia del trabajo de Tate, es que fue justamente él, el primero en usar análisis de Fourier adélico, en donde las funciones L surgen de manera natural, y hace que su demostración sea mucho más sencilla. Además interpretó los caracteres de Hecke como *representaciones automorfas* del grupo $GL(1)$ de idéles del cuerpo K, de manera que abrió la puerta a generalizaciones de representaciones automorfas de otros grupos, por ejemplo $GL(N)$ cuando $N > 1$. En el caso que $N = 2$ y $K = \mathbb{Q}$, corresponde justamente a las formas modulares clásicas y sus respectivas funciones L.

Lo que realmente se destaca de la continuación analítica, es que en la demostración realmente se prueba lo siguiente:

Teorema 7.1.6. *Si*

$$\Lambda(s,\chi) = (|\Delta_K|\mathfrak{N}(\mathfrak{f}))^{s/2} L_\infty(s) L(s,\chi),$$

entonces ella admite una continuación analítica a

$$\mathbb{C} \setminus \{Tr(-p+iq)/n, 1 + Tr(p+iq)/n\},$$

donde Tr es la suma de las componentes del vector x, y además satisface la ecuación funcional

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

donde $|W(\chi)| = 1$.

Se observa que si el carácter χ es el trivial módulo $\mathcal{O}_K$, la función L de Hecke no es otra cosa que la función zeta de Dedekind asociada al cuerpo K, como se puede verificar gracias al teorema 5.3.3, función de la cual se conoce más que la ecuación funcional, pues también se conoce el valor de los residuo en sus dos polos. Luego las funciones L de Hecke son generalizaciones de las tres funciones mencionadas anteriormente: zeta de Riemann, L de Dirichlet y zeta de Dedekind.

En el caso en que $K = \mathbb{Q}$, ver la relación entre las funciones L de Hecke y las funciones L de Dirichlet es sencillo, pues se tiene lo siguiente:

Proposición 7.1.7. *Existe una biyección entre los caracteres de Dirichlet y los caracteres de Hecke de $\mathbb{Q}$ cuyo orden es finito.*

Demostración. Dado un carácter de Dirichlet χ módulo k, si se toma $\mathfrak{f} = k\mathbb{Z}$, se define la función χ_{Hec} por:

$$\chi_{Hec}(\mathfrak{a}) = \chi(a)$$

para cada $\mathfrak{a} \in I(\mathfrak{f})$. Esta relación está bien definida ya que $\mathbb{Z}$ es DIP. Además como $\mathbb{R} \otimes \mathbb{Q} \cong \mathbb{R}$, el tipo infinito de χ_{Hec} es el carácter trivial si χ es par, o el carácter signo $(x \to x/|x|)$ si χ es un carácter impar. De esta manera χ_{Hec} es un carácter de Hecke y se tiene la igualdad

$$L(s,\chi) = L(s,\chi_{Hec}).$$

□

7.2. Las funciones L de Artin.

Así como se hizo con las funciones L de Hecke, se necesitan algunas nociones previas antes de definir la función L de Artin, pero no se entrará en el detalle de sus demostraciones.

Sean F, K cuerpos de números tal que F/K es una extensión de Galois finita.

Definición 7.2.1. *Sea $G = \mathrm{Gal}(F/K)$ y sea $\rho : G \to GL(V)$ una representación compleja de G. La función*

$$\begin{aligned} \chi : G &\to \mathbb{C} \\ g &\to \chi(g) = Tr\rho(g), \end{aligned}$$

donde Tr es la función traza, se llama el carácter de G asociado a la representación ρ.

Teorema 7.2.2. *Dos representaciones de G son isomorfas si y solo si, tienen asociado el mismo carácter.*

Un poco de formalismo lleva a hablar del carácter inducido y del carácter obtenido por inflación. Si $H \leq G$ cuyo orden es h y χ es un carácter de H, entonces

$$\mathrm{Ind}_H^G \chi(\sigma) = \frac{1}{h} \sum_{\substack{\tau \in G \\ \tau^{-1}\sigma\tau \in H}} \chi(\tau^{-1}\sigma\tau)$$

es el carácter inducido por χ de H a G; y si χ es un carácter de G/H, se denota por

$$\mathrm{Infl}\, \chi = \chi \circ \pi$$

donde π es la proyección de G a G/H, al carácter obtenido por inflación.

Una notación estándar que se incluirá es la siguiente: Si w es un lugar que divide a v, se denotará por $\mathfrak{k}_w$ el cuerpo de residuos $\mathcal{O}_L/\mathfrak{P}_w$.

Si v es un lugar finito de K, sea

$$\mathfrak{p}_v = \{x \in \mathcal{O}_K \mid |x|_v < 1\},$$

entonces el cuerpo de residuos $\mathfrak{k}_v = \mathcal{O}_K/\mathfrak{p}_v$ tiene $Nv = p_v^{\deg(v)}$ elementos, donde p_v es la caracteristica de $\mathfrak{k}_v$ y $\deg(v)$ es el grado de la extensión de $\mathfrak{k}_v$ sobre $\mathbb{F}_{p_v}$. Si se define la acción de G sobre los lugares de F dada por $(\sigma, w) \to \sigma w$ donde

$$|x|_{\sigma w} = |x^{\sigma^{-1}}|_w,$$

se tiene que $\mathfrak{P}_{\sigma w} = \mathfrak{P}_w^{\sigma}$.

Definición 7.2.3. *Sea w es un lugar arquimediano y x_w la imagen de x mediante el encaje w, entonces*

$$|x|_w = \begin{cases} |x_w| & \textit{el valor absoluto de } x_w \textit{ si el encaje } w \textit{ es real;} \\ x_w \overline{x}_w & \textit{la norma usual al cuadrado de } x_w \textit{ si el encaje } w \textit{ es complejo.} \end{cases}$$

Si w es un lugar de F, se define el grupo de descomposición G_w como

$$G_w = \{\sigma \in G \mid \sigma w = w\}.$$

Se observa por la definición que

$$G_{\tau w} = \{\sigma \in G \mid \sigma\tau w = \tau w\} = \tau^{-1} G_w \tau,$$

además que G actúa transitivamente sobre los lugares de F que dividen a un lugar fijo v de K. Esto se tiene gracias a que F/K es normal, y por tanto la factorización de $\mathfrak{p}$ en F se da como

$$\mathfrak{p}_v = [\mathfrak{P}_{w_1} \cdots \mathfrak{P}_{w_r}]^e.$$

Por tanto los grupos G_{w_i} son grupos conjugados. Dado que para cada $\sigma \in G_w$ se tiene que $\sigma(\mathfrak{P}_w) = \mathfrak{P}_w$, entonces σ induce un automorfismo $\overline{\sigma}$ sobre $\mathfrak{k}_w$. Se tiene entonces la siguiente definición:

Definición 7.2.4. *El grupo de inercia I_w de w se define como*

$$I_w = \{\sigma \in G_w \mid \overline{\sigma} \text{ es el elemento trivial de } \mathrm{Gal}(\mathfrak{k}_w/\mathfrak{k}_v)\}.$$

Proposición 7.2.5. *La extensión $\mathfrak{k}_w/\mathfrak{k}_v$ es cíclica, es decir, el grupo de Galois $\mathrm{Gal}(\mathfrak{k}_w/\mathfrak{k}_v)$ es cíclico, y es generada por el automorfismo de Frobenius*

$$Fr_w : x \mapsto x^{Nv}.$$

Este hecho es un resultado estándar de la teoría de cuerpos, además se tiene la siguiente proposición:

Proposición 7.2.6. *El cociente G_w/I_w es isomorfo a $\mathrm{Gal}(\mathfrak{k}_w/\mathfrak{k}_v)$ mediante $\sigma \mapsto \overline{\sigma}$.*

Definición 7.2.7. *Abusando de la notación, se denotará por Fr_w cualquier elemento $\sigma \in G_w$ tal que $\bar{\sigma}$ es el automorfismo de Frobenius de $\mathfrak{k}_w/\mathfrak{k}_v$ definido en la proposición 7.2.5.*

Observación 7.2.8. *Se observa que dos tales elecciones de Fr_w difieren por composición con un elemento $\sigma \in I_w$. En particular, si I_w es trivial entonces Fr_w está únicamente definido.*

En caso que G_w sea cíclico, se dice que el lugar w es no ramificado, en caso contrario, el lugar será ramificado. Si cada lugar w que divide a v es no ramificado, entonces el lugar v se llama un lugar no ramificado, en caso contrario, será un lugar ramificado.

Si w es un lugar arquimediano, entonces G_w es generado por un elemento σ_w de orden 1 o 2 según sea el caso, si w es un lugar real o complejo respectivamente.

Definición 7.2.9. *Sea $H \leq G$ un subgrupo de G, se define V^H como:*

$$V^H = \{v \in V \mid \sigma v = v \ \forall \sigma \in H\}.$$

Con estas notaciones dadas, se puede definir entonces la función L de Artin:

Definición 7.2.10. *Para $\mathrm{Re}(s) > 1$ se define la función L de Artin como*

$$L(s, V) = \prod_v \det(1 - N(v)^{-s}\rho(Fr_w)|_{V^{I_w}})^{-1}$$

donde v recorre los lugares finitos de K, para cada v se tiene que w es un lugar arbitrario de F que divide a v, y Fr_w es el elemento de Frobenius descrito en la observación 7.2.8.

En el caso en que w es un lugar de F que divide a v, y v sea un lugar ramificado, se tiene que I_w no es trivial, por tanto Fr_w no está únicamente definido, sino que varía sobre la clase lateral de I_w que induce el automorfismo de Frobenius de $\mathrm{Gal}(\mathfrak{k}_w/\mathfrak{k}_v)$. Esta es la razón por la cual en la definición aparece la restricción a V^{I_w}, pues ella implica que $\rho(\sigma_1)|_{V^{I_w}} = \rho(\sigma_2)|_{V^{I_w}}$ para cualquier par de elementos σ_1, σ_2 en una misma clase lateral, de manera que el factor $\det(1 - Nv^{-s}\rho(Fr_w)|_{V^{I_w}})$ está bien definido en términos de w. Se observa que si I_w es trivial, entonces $V^{I_w} = V$, y por la observación 7.2.8, el elemento de Frobenius está bien definido.

Por otro lado, Fr_w depende de la elección de w. Sin embargo, si w, w' son lugares que dividen a v, ellos difieren por la acción de algún elemento $\sigma \in G$, pues la acción por conjugación es transitiva. Por tanto $\rho(\sigma)$ conjuga los elementos $\rho(Fr_w)$ y $\rho(Fr_{w'})$, de manera que los determinantes considerados en la definición coinciden. Gracias a esto, se tiene que la definición anterior no depende de la elección de w.

Para hablar acerca de la ecuación funcional de las funciones L presentadas en los capítulos anteriores, se ha tenido que introducir algunos términos adicionales dependiendo del número de lugares reales o complejos de K. En este caso se debe proceder de manera análoga, solo que las dimensiones de algunos espacios juegan un papel importante. Sean

$$a_1 = \sum_{v \text{ real}} \dim(V^{G_w}), \qquad\qquad a_2 = \sum_{v \text{ real}} \operatorname{codim}(V^{G_w}),$$

luego el término a multiplicar en la función L de Artin está dado por

$$L_{v|\infty}(s) = L_{\mathbb{C}}(s)^{r_2\chi(1)} L_{\mathbb{R}}(s)^{a_1} L_{\mathbb{R}}(s+1)^{a_2},$$

en donde $L_{\mathbb{R}}$ y $L_{\mathbb{C}}$ son definidas como en la ecuación (5.7).

Si $S' = \{v |\, v \text{ es finito y se ramifica en } F\}$, para w un lugar de F elegido arbitrariamente que divide a v, sea $I_w = G_0 \supseteq G_1 \supseteq \cdots$ la sucesión de grupos de ramificación de $\mathfrak{P}_w/\mathfrak{p}_v$. Si se denota por $g_i = \#G_i$, y

$$f(\chi, v) = \sum_{i=0} \frac{g_i}{g_0} \operatorname{codim} V^{G_i},$$

se tiene la siguiente definición:

Definición 7.2.11. *El ideal*

$$f(\chi) = \prod_{v \in S'} \mathfrak{p}_v^{f(\chi, v)},$$

recibe el nombre de el conductor de Artin asociado a χ.

Con estas notaciones previas, se puede enunciar el próximo teorema:

Teorema 7.2.12. *Si*

$$\Lambda(s, \chi) = (|\Delta_K|^{\chi(1)} \mathfrak{N}(f(\chi))^{s/2} L_{v|\infty}(s) L(s, \chi),$$

la función $\Lambda(s, \chi)$ admite una continuación meromorfa al plano complejo, y satisface la ecuación funcional

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

en donde $|W(\chi)| = 1$.

A diferencia de las anteriores funciones L, en las cuales se demostró que la función involucrada en la ecuación funcional, es una función analítica en casi todo el plano complejo, la continuación analítica de la función L de Artin no es conocida, y este es justo uno de los muchos problemas abiertos en esta área.

Conjetura 7.2.13 (Artin)**.** *Las funciones L de Artin de caracteres irreducibles no triviales son funciones enteras.*

Desde luego la función L de Artin de un carácter irreducible trivial es la función zeta de Dedekind, y como se observó en el anterior capítulo, esta tiene un único polo.

Por otro parte, se puede demostrar que un carácter de Hecke de orden finito del cuerpo K corresponde de manera única con el carácter de una representación de Galois de dimensión 1 de cierta extensión finita F/K, de manera que las funciones L de Artin generalizan las funciones L de Hecke.

7.3. Las conjeturas de Stark.

El último objetivo de este trabajo, será enunciar una versión de la conjetura de Stark en su forma más simple, y para ello se va a utilizar la función L de Artin relativa a un conjunto de lugares finitos S.

Sea S un conjunto finito de lugares de K tal que $S_\infty \subset S$, se dice que

$$L(s,\chi) = L_S(s,\chi) = \prod_{v \notin S} \det(1 - N(v)^{-s}\rho(Fr_w)|_{V^{I_w}})^{-1}$$

es la función L de Artin relativa al conjunto S. Como antes, w es un lugar arbitrario de F el cual divide a v, y nuevamente $\rho(Fr_w)$ no depende de la elección de w.

Por S_F se denota el subconjunto de lugares de F tal que

$$S_F = \{w \mid w \text{ divide a } v \text{ para algún } \ v \in S\};$$

Y será el grupo abeliano libre de base S_F. Se define el conjunto X por

$$X = \Big\{ \sum_{w \in S_F} n_w w \in Y | \sum_{w \in S_F} n_w = 0 \Big\}. \tag{7.1}$$

Se observa que si se hace actuar G sobre los conjuntos Y y X, ellos adquieren una estructura de G-módulos y se tiene la siguiente cadena exacta:

$$\begin{array}{ccccccc} 0 \longrightarrow X \longrightarrow & Y & \longrightarrow \mathbb{Z} & \longrightarrow 0. \\ & \sum n_w w & \longrightarrow \sum n_w & \end{array}$$

Bajo estas condiciones, si se supone que:

$$L(s,\chi) = c(\chi)s^{r(\chi)} + O(s^{r(\chi)+1}) \tag{7.2}$$

en una vecindad de $s = 0$, es decir, el primer término en la serie de Taylor al rededor de $s = 0$ es $c(\chi) \neq 0$, se tiene la siguiente proposición:

Proposición 7.3.1. *El exponente $r(\chi)$ en la ecuación (7.2) satisface la igualdad*

$$r(\chi) = \Big(\sum_{v \in S} \dim V^{G_w} \Big) - \dim V^G = \dim_{\mathbb{C}} \mathrm{Hom}_G(V^*, \mathbb{C} \otimes_{\mathbb{Z}} X),$$

en donde a $\mathbb{C} \otimes_{\mathbb{Z}} X$ se le asocia una estructura de $\mathbb{C}[G]-$módulo.

Observación 7.3.2. *La eleeción de w en la anterior proposición solo depende de v, pues dado que todos los G_w son conjugados,* $\dim_{\mathbb{C}} V^{G_w}$ *solo depende de v. Además, una consecuencia no inmediata de esta proposición, y que solo se menciona en este escrito, es que para cada $\alpha \in \mathrm{Aut}(\mathbb{C})$ se tiene que $r(\chi)^\alpha = r(\chi^\alpha)$ donde $\chi^\alpha = \alpha \circ \chi$.*

Como nuestro objetivo ahora es enunciar la conjetura de Stark en su versión más simple, necesitamos introducir el tipo de regulador necesario para tal fin.

Sea U el grupo de las S_K-unidades de K, es decir

$$U = \{x \in K|\ |x|_w = 1\ \forall w \notin S_F\}, \tag{7.3}$$

al considerar el siguiente homomorfismo de módulos sobre $\mathbb{Z}[G]$

$$\begin{aligned} \lambda : U &\longrightarrow \mathbb{R} \otimes_{\mathbb{Z}} X \\ u &\longrightarrow \lambda(u) = \sum_{w \in S_F} \log |u|_w \otimes w \end{aligned}$$

se obtiene el siguiente teorema:

Teorema 7.3.3. *El kernel de λ es el conjunto $\mu(K)$ y su imagen es un retículo completo de rango $\#S - 1$ en $\mathbb{R} \otimes_{\mathbb{Z}} X$.*

Se resalta del anterior teorema, que es parte fundamental en la demostración del teorema de las S-unidades que generaliza el teorema de las unidades de Dirichlet.

Si se hace el producto tensorial de U con $\mathbb{R}$ y con $\mathbb{C}$, λ induce un isomorfismo

$$\mathbb{R} \otimes U \xrightarrow{\sim} \mathbb{R} \otimes X \qquad\qquad \mathbb{C} \otimes U \xrightarrow{\sim} \mathbb{C} \otimes X$$

de módulos sobre $\mathbb{R}[G]$ ($\mathbb{C}[G]$ respectivamente) donde el isomorfismo está dado por $1 \otimes \lambda$. Este isomorfismo se denotará aún por λ.

Esto implica que las representaciones de $\mathbb{Q} \otimes U$ y $\mathbb{Q} \otimes X$ son isomorfas sobre $\mathbb{Q}$, y por tanto si

$$f : \mathbb{Q} \otimes X \longrightarrow \mathbb{Q} \otimes U$$

es el isomorfismo de módulos sobre $\mathbb{Q}[G]$, se llama todavía por f la complificación

$$f : \mathbb{C} \otimes X \xrightarrow{\sim} \mathbb{C} \otimes U.$$

Dado que si W es un módulo sobre $\mathbb{C}[G]$, entonces $\mathrm{Hom}(W, \mathbb{C} \otimes X)$ es un módulo sobre $\mathbb{C}[G]$ donde la acción está dada por

$$(g\phi)(w) = g\phi(g^{-1}w)$$

para $\phi \in \mathrm{Hom}(W, \mathbb{C} \otimes X)$, $g \in \mathbb{C}[G]$ y $w \in W$, por tanto se le puede asociar una estructura de módulo sobre $\mathbb{C}[G]$ a V^*, ya que

$$V^* = \mathrm{Hom}(V, \mathbb{C}),$$

donde la acción sobre $\mathbb{C}$ es la trivial. Así el automorfismo $\lambda \circ f$ de $\mathbb{C} \otimes X$ induce por funtorialidad el automorfismo

$$\begin{array}{ccc} \mathrm{Hom}_G(V^*, \mathbb{C} \otimes X) & \xrightarrow{(\lambda \circ f)_V} & \mathrm{Hom}_G(V^*, \mathbb{C} \otimes X) \\ \phi & \to & \lambda \circ f \circ \phi. \end{array}$$

Definición 7.3.4. *Se define el regulador de Stark asociado a f como*

$$R(\chi, f) = \det((\lambda \circ f)_V).$$

Dada la definición de $(\lambda \circ f)_V$, el regulador depende unicamente de f, más no de la realización V del carácter χ. Se observa que gracias a la proposición 7.3.1, el regulador de Stark es el determinante de un automorfismo de un espacio vectorial complejo de dimensión $r(\chi)$.

Por último, se denotará por $\mathbb{Q}(\chi)$ la extensión abeliana finita de $\mathbb{Q}$ que se obtiene al adjuntar todos los valores $\chi(\sigma)$ para cada $\sigma \in G$. Con estas notaciones introducidas, se puede enunciar la conjetura de Stark para funciones L de Artin.

Conjetura 7.3.5. *Sean F/K una extensión de Galois finita de cuerpos numéricos, $G = \mathrm{Gal}(F/K)$, χ el carácter de una representación finito-dimensional de G sobre $\mathbb{C}$, y sea f como antes. Si se define el número complejo $A(\chi, f) = \frac{R(\chi,f)}{c(\chi)}$, entonces*

$$\begin{cases} A(\chi, f) \in \mathbb{Q}(\chi) & y \\ A(\chi, f)^\alpha = A(\chi^\alpha, f) & \text{para todo } \alpha \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}). \end{cases}$$

Proposición 7.3.6. *El regulador de Stark $R(\chi_0, f)$ (del carácter trivial χ_0 de la extensión trivial K/K) es un múltiplo racional del regulador R_K de las unidades de K, para cualquier elección del isomorfismo $f : \mathbb{Q} \otimes X \to \mathbb{Q} \otimes U$.*

Demostración. Dado que la representación es la trivial, entonces $V = \mathbb{C}$, de manera que $\mathrm{Hom}_G(V^*, \mathbb{C} \otimes X) \cong \mathbb{C} \otimes X$.

Sean $f, f' : \mathbb{Q} \otimes X \to \mathbb{Q} \otimes U$ dos aplicaciones diferentes. Dado que una base con coeficientes racionales para $\mathbb{Q} \otimes X$ sigue siendo una base para $\mathbb{C} \otimes X$, entonces las respectivas complificaciones f, f' pueden ser evaluadas en una base con coeficientes racionales.

Por otro lado, como

$$\lambda \circ f' = (\lambda \circ f) \circ (f^{-1} \circ f'),$$

entonces $\det((\lambda \circ f')_{\mathbb{C}}) = A \det((\lambda \circ f)_{\mathbb{C}})$, donde A es un número racional, más explicitamente, A es el determinante de un isomorfismo de $\mathbb{C} \otimes X$ evaluado en una base racional, cuyas imágenes son racionales. Por tanto, es suficiente demostrar que el resultado es válido para alguna elección particular de f.

Como el conjunto de lugares está compuesto por los encajes de K, se tiene lo siguiente:

$$\begin{aligned} X &= \left\{ \sum_\sigma n_\sigma \sigma \mid \sum_\sigma n_\sigma = 0 \right\} \\ &= \left\{ \sum_{\sigma \in S \setminus \{\sigma\}} n_\sigma (\sigma - \sigma_0) \right\} \end{aligned}$$

para cualquier lugar fijo $\sigma_0 \in S$. Luego $\{\sigma_i - \sigma_{r_1+r_2}\}_{i \le r}$ es una base para X. Si

$$\begin{aligned} f : X &\longrightarrow U, & \lambda : U &\longrightarrow \mathbb{R} \otimes X \\ \sigma_i - \sigma_{r_1+r_2} &\longrightarrow \epsilon_i & \epsilon_i &\longrightarrow \sum_{j \le r_1+r_2} \log |\sigma_j^{a_j}(\epsilon_i)| \otimes \sigma_j \end{aligned}$$

donde a_j se toma como en la ecuación(5.4). Entonces se tiene el homomorfismo $\lambda \circ f$ definido sobre la base $\{\sigma_i - \sigma_{r_1+r_2}\}$ por

$$\begin{aligned}\lambda \circ f(1 \otimes (\sigma_i - \sigma_{r_1+r_2})) &= \sum_{j \leq r_1+r_2} \lambda_j(\epsilon_i) \otimes \sigma_j \\ &= \sum_{j \leq r} \lambda_j(\epsilon_i) \otimes (\sigma_j - \sigma_{r_1+r_2}).\end{aligned}$$

Se ve fácilmente que la matriz asociada a la aplicación $\lambda \circ f$ en la base $\{\sigma_i - \sigma_{r_1+r_2}\}$ está dada por

$$(\lambda_j(\epsilon_i))_{j,i \leq r}.$$

Por tanto el valor de su determinante es justamente R, el regulador del cuerpo K gracias a la ecuación (5.6). De esta manera el resultado se demuestra. □

Corolario 7.3.7. *La Conjetura de Stark es válida para la función zeta de Dedekind ζ_K de un cuerpo de números algebraicos K (es decir, para el carácter χ_0 de Galois de la extensión trivial K/K).*

La demostración es inmediata a partir de la fórmula del número de clases de Dedekind, y de la proposición 7.3.6.

Por tanto, se tiene que al menos de manera cualitativa (módulo un múltiplo racional no nulo inespecífico), el caso más sencillo de la Conjetura de Stark captura de manera sumamente elegante los resultados más importantes de la tesis.

Es interesante ver que esta conjetura relaciona dos números de los cuales se piensa que ambos son trascendentes, mediante un cociente, que es un número algebraico. Más aún, está relacionando un número con una propiedad analítica como lo es $c(\chi)$, y un número con una propiedad algebraica, como lo es el regulador de Stark, pues detras de él, están involucradas las unidades fundamentales de ciertos anillos de enteros.

Es de mencionar que las conjeturas generales de Stark siguen abiertas salvo en casos muy especiales, tales como el caso de que χ toma valores racionales, es decir, cuando $\mathbb{Q}(\chi) = \mathbb{Q}$.

Finalmente, se hace un último comentario que relaciona las conjeturas de Stark con un problema abierto desde hace más de un siglo.

Como se hizo mención atrás, la conjetura descrita en este escrito, es la presentación más sencilla de tales conjeturas. A traves de los años, diversos matemáticos trabajando en el tema, han reformulado de diversas maneras la conjetura de Stark. Una de esas formulaciones, en el caso explícito en que G sea un grupo abeliano y la representación sea de grado 1, dice vagamente hablando, que existen elementos de F tales que el regulador de Stark surge a partir de tales elementos. Estos elementos llamados unidades de Stark, son lo que se cree, puedan ser los elementos buscados para solucionar el problema 12 de Hilbert, el cual en el caso general permanece abierto; pues se conoce solución únicamente cuando el cuerpo es $\mathbb{Q}$ (que es el teorema de Kronecker), o cuando el cuerpo es una extensión imaginaria de $\mathbb{Q}$ de grado 2.

8

Bibliografía

[Ahl79] L. V. Ahlfors. *Complex Analysis.* MacGraw-Hill, Inc, New York, third edition, 1979.

[Apo76] T. M. Apostol. *Introduction to Analytic Number Theory.* Springer, 1976.

[AW04] R. Ash and Novinger W. *Complex Variables.* http://www.math.uiuc.edu/∼r-ash/CV.html, Illinois University, second edition, 2004.

[BF06] David Burns and Matthias Flach. On the equivariant Tamagawa number conjecture for Tate motives. II. *Doc. Math.*, Extra Vol.:133–163 (electronic), 2006.

[BK90] Spencer Bloch and Kazuya Kato. L-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, volume 86 of *Progr. Math.*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990.

[BS66] Borevich and Shafarevich. *Number Theory.* Academic Press, 1966.

[Coh93] Henri Cohen. *A course in Computational Algebraic Number Theory.* Springer, 1993.

[Dav80] H. Davenport. *Multiplicative Number Theory.* Springer-Verlag, New York, 1980. 2nd ed.

[Ded68] Richard Dedekind. *Gesammelte mathematische Werke. Bände I–III.* Herausgegeben von Robert Fricke, Emmy Noether und öystein Ore. Chelsea Publishing Co., New York, 1968.

[Dir37] P. G. L. Dirichlet. Beweis des satzes, dass jede unbegrenzte arithmetische progression, deren erstes glied und differenz ganze zahlen ohne gemeinschaftlichen factor sind, unendlich viele primzahlen enthält. *Abhand. Ak. Wiss. Berlin*, 48, 1837.

[Dir99] P. G. L. Dirichlet. *Lectures on number theory*, volume 16 of *History of Mathematics.* American Mathematical Society, Providence, RI, 1999. Supplements by R. Dedekind, Translated from the 1863 German original and with an introduction by John Stillwell.

[Ell75] W. J. Ellison. *Les nombres premiers.* Hermann, 1975.

[FPR94] Jean-Marc Fontaine and Bernadette Perrin-Riou. Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 599–706. Amer. Math. Soc., Providence, RI, 1994.

[Kar79] A. A. Karatsuba. *Fundamentos de la teoría analítica de los números*. Editorial Mir, Moscú, 1979. Traducido del Ruso al Español por V. Fernández.

[LD69] G. Lejeune Dirichlet. *Mathematische Werke. Bände I, II.* Herausgegeben auf Veranlassung der Königlich Preussischen Akademie der Wissenschaften von L. Kronecker. Chelsea Publishing Co., Bronx, N.Y., 1969.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Pop99] Cristian D. Popescu. On a refined Stark conjecture for function fields. *Compositio Math.*, 116(3):321–367, 1999.

[Rie59] B. Riemann. über die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monat. Preus. Akad. Wiss.*, pages 671–680, 1859.

[Rub96] Karl Rubin. A Stark conjecture "over $\mathbf{Z}$" for abelian L-functions with multiple zeros. *Ann. Inst. Fourier (Grenoble)*, 46(1):33–62, 1996.

[Ser77] Jean Pierre Serre. *Linear Representations of Finite Groups*. Springer-Verlag, 1977. Traslated from the French by Leonard L. Scott.

[Sta71] H. M. Stark. Values of L-functions at $s = 1$. I. L-functions for quadratic forms. *Advances in Math.*, 7:301–343 (1971), 1971.

[Sta75] H. M. Stark. L-functions at $s = 1$. II. Artin L-functions with rational characters. *Advances in Math.*, 17(1):60–92, 1975.

[Sta76] H. M. Stark. L-functions at $s = 1$. III. Totally real fields and Hilbert's twelfth problem. *Advances in Math.*, 22(1):64–84, 1976.

[Sta77] H. M. Stark. Hilbert's twelfth problem and L-series. *Bull. Amer. Math. Soc.*, 83(5):1072–1074, 1977.

[Tat84] John Tate. *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*, volume 47 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1984. Lecture notes edited by Dominique Bernardi and Norbert Schappacher.

[Tat09] John Tate. *Introduction to the Stark Conjectures*. IAS/Park City Mathematics Institute Series, American Mathematical Society, 2009. Park City Mathematics Institute. A aparecer en "The Arithmetic of L-Functions".

[Tit86] E. C. Titchmarsh. *The theory of the Riemann zeta-function*. The Clarendon Press Oxford University Press, New York, second edition, 1986. Edited and with a preface by D. R. Heath-Brown.