Lecturas Matemáticas
Volumen **35** *(1) (2014), páginas 25–56*
ISSN 0120–1980

Valores especiales de funciones L: Dirichlet, Dedekind y Stark

Special values of $L-$functions: Dirichlet, Dedekind and Stark

Elkin O. Quintero
Universidade de São Paulo, Brasil

Resumen. El objetivo de este escrito es servir como introducción al estudio de una fascinante intersección entre los enfoques analíticos y algebraicos a la teoría de números. En particular, se desea introducir al lector al estudio de la teoría de las llamadas funciones zeta y L. El tema común que trasciende secciones específicas de este trabajo es el de las implicaciones aritméticas de las propiedades analíticas de tales funciones. Las funciones L son funciones meromorfas de una variable compleja s. Existe una gran variedad de tales funciones, empezando por la clásica función zeta de Riemann, que se generaliza a la función zeta de Dedekind de un cuerpo de números algebraicos arbitrario K, sin olvidar las funciones L de Dirichlet y sus generalizaciones a las funciones L de Hecke y Artin. Todas han sido utilizadas como herramientas en el estudio de problemas profundamente aritméticos.

Key words and phrases. Zeta function, $L-$functions, Riemann, Dirichlet, Stark, class number.

Abstract. The aim of this paper is to serve as an introduction to the study of the fascinating intersection between analytic and algebraic approaches to number theory. In particular, we want to introduce the reader to the study of the theory of zeta and L functions. The common theme that transcends specific sections of the paper is the arithmetic implications of the analytical properties of such functions. The L functions are meromorphic functions of a complex variable s. There are a variety of such functions, beginning with the classical Riemann's zeta function, which is generalized to the Dedekind's zeta function of an arbitrary algebraic number field K, without forgetting the Dirichlet's L functions and their generalizations to Hecke and Artin L functions. All have been used as tools in the study of arithmetical problems.

2010 AMS Mathematics Subject Classification. 11M06, 11M36, 11M41

1. Introducción

En la segunda sección recordamos algunas de las propiedades más elementales de la función zeta de Riemann, la más simple de las funciones L. En la siguiente, nuestra atención se enfoca en el estudio de las funciones L introducidas por Dirichlet en su demostración del teorema de la infinitud de primos en las progresiones aritméticas. Dirichlet proporciona una fórmula del número de clases para el valor $L(1,\chi)$ en términos de dos cantidades numéricas íntimamente relacionadas con las propiedades aritméticas de un cuerpo cuadrático, a saber el número de clases h_d, y su regulador R_d.

Luego, en la cuarta sección, se retoma la evolución histórica del estudio de valores de funciones L en $s=1$, procediendo a la demostración de la fórmula del número de clases de Dedekind, que generaliza aquella de Dirichlet. La demostración de este hermoso resultado involucra partes iguales de análisis y aritmética, sintetizando resultados previos relativos a la función zeta de Riemann y las funciones L de Dirichlet. Cabe mencionar que hacemos un estudio de las funciones L de Dedekind en el punto $s=0$, pues las llamadas conjeturas de Stark se enuncian alrededor de este punto.

Finalmente, en la última sección, se exponen funciones L más generales como las de Hecke y las de Artin. Como colofón, y sirviendo de conclusión natural a los temas expuestos, se explica el concepto de *regulador de Stark* y su conexión conjetural, también debida a Stark y otros investigadores, con los valores especiales de $L(0,\chi)$ de las funciones L de Artin.

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

La función zeta de Riemann conocida ampliamente por la *famosa conjetura de Riemann sobre sus ceros*, es la función más simple de todas las funciones L. En seguida mencionamos hechos importantes de la función $\zeta(s)$, y a lo largo del escrito, se verán las relaciones que hay con las otras funciones L.

Para no ir en contra de la notación dada en la mayoría de la bibliografía, dado un $s\in\mathbb{C}$ lo escribiremos siempre así: $s=\sigma+it$.

Definición 2.1. Si $s\in\mathbb{C}$, donde $\Re(s)>1$, se define la función zeta de Riemann por la serie

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

Para esta función se tiene el siguiente teorema.

Teorema 2.2. [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.

Además, es bien conocido que la función $\zeta(s)$ posee una extensión holomorfa a $\mathbb{C} \setminus \{1\}$, tal como lo expresa el siguiente resultado:

Teorema 2.3. *La función* $\zeta(s)$ *tiene una extensión holomorfa* $\mathbb{C} \setminus \{1\}$ *la cual verifica la ecuación funcional*

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

además en $s = 1$ *posee un polo simple, cuyo residuo es 1.*

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

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

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

$$\xi(s) = \xi(1-s), \tag{2}$$

como se ve mediante un cálculo directo, gracias a la ecuación funcional del teorema 2.3.

3. Funciones L de Dirichlet.

Para hablar de funciones L de Dirichlet, es necesario hablar de los llamados *caracteres de Dirichlet*.

Definición 3.1. Si $\chi : \mathbb{Z} \to \mathbb{S}^1 \cup \{0\} \subset \mathbb{C}$ satisface las siguientes condiciones

$$\begin{array}{ll} \chi(ab) = \chi(a)\chi(b) & \text{para cada } a, b \in \mathbb{Z}\,; \\ \chi(a) = 0 & \text{solamente si } (a,k) \neq 1, \end{array}$$

entonces χ se llama un *carácter de Dirichlet módulo* k. Si además, 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 $\chi(a) \neq 1$, el carácter se dice *primitivo*. En caso contrario, decimos que el carácter χ *no es primitivo*.

Proposición 3.2. *Sea* χ *un carácter 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 divisor propio* d *de* k*.*

Demostración. Supongamos que χ no es primitivo; así 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 lo recíproco, basta tomar $b = 1$. ☑

Definición 3.3. 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 por la anterior proposición. Se dice que χ^* *induce el carácter* χ, o que χ es *inducido por* χ^*.

Observación 3.4. Dado k, existen exactamente $\phi(k)$ caracteres módulo k. El carácter $\chi(a) = 1$ para cada $(a, k) = 1$ será denotado por χ_0 y es llamado el *carácter principal* módulo k.

Un carácter del cual se hablará con frecuencia, es el generado por el *símbolo de Kronecker* $\left(\frac{a}{b}\right)$. Este carácter $\chi_k \pmod{k}$ se define por la relación

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

Definición 3.5. Para un carácter de Dirichlet χ módulo k, se define la *función L de Dirichlet asociada al carácter de Dirichlet* χ así:

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

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

Algunas propiedades que se necesitarán posteriormente son las siguientes (sus demostraciones pueden encontrarse, por ejemplo, en [1]).

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

$$\sum_{n\leq x} \frac{\chi(n)}{n} = L(1, \chi) + O\left(\frac{1}{x}\right) \tag{3}$$

$$\sum_{n\leq x} \frac{\chi(n)\log n}{n} = -L'(1, \chi) + O\left(\frac{\log x}{x}\right). \tag{4}$$

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

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}. \tag{5}$$

Observación 3.7. Dado que el anterior resultado es válido para cualquier carácter de Dirichlet, se tiene la siguiente igualdad:

$$L(s,\chi_0)=\zeta(s)\prod_{p|k}\left(1-\frac{1}{p^s}\right), \tag{6}$$

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

Dado que $\zeta(s)$ tiene un polo de orden 1 en $s=1$, por la anterior observación se tiene que $L(s,\chi_0)$ es una función analítica en $\mathbb{C}\setminus\{1\}$, y en $s=1$, posee un polo simple cuyo residuo es

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

Un resultado similar se puede demostrar para $\chi\neq\chi_0$, solo que para ello el camino a recorrer es más extenso. Una vez se tenga demostrado el resultado para los caracteres primitivos, se puede extender a cualquier carácter $\chi\neq\chi_0$ módulo k, gracias al siguiente lema:

Lema 3.8. *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 $p\nmid k_1$, se tiene

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

con lo cual queda demostrado el lema. ☑

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

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

Por tanto, surge de manera natural la siguiente distinción:

Definición 3.9. Sea χ un carácter módulo k. Si $\chi(-1)=1$, entonces χ se llama un *carácter par*; en caso contrario, $\chi(-1)=-1$, se llama un *carácter impar*.

Esta distinción es necesaria para hablar de otro resultado análogo al de la función zeta de Riemann que satisfacen las funciones L de Dirichlet como lo es la ecuación funcional. Más precisamente, se tiene el

Teorema 3.10. *Sea $\chi \neq \chi_0$ un carácter primitivo módulo k. Entonces la función $L(s,\chi)$ puede extenderse analíticamente a todo el plano complejo. Además, si*

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

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

entonces se satisface la siguiente ecuación funcional:

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

donde $\overline{\chi}$ es el carácter conjugado de χ y $G(1,\chi) = \sum_{m=1}^{k}\chi(m)e^{\frac{2\pi m}{k}}$. ☑

Observación 3.11.

$$\left|\frac{i^\delta\sqrt{k}}{G(1,\chi)}\right|^2 = 1$$

4. La fórmula del número de clases de Dirichlet.

Aquí vamos ahora a encontrar la primera relación entre análisis y álgebra, ya que se va a relacionar un concepto analítico, como es el número de clase de formas de discriminante d, con un concepto algebraico como es el número de clases de ideales del anillo de enteros $\mathcal{O}_K = \mathbb{A} \cap \mathbb{Q}(\sqrt{\Delta})$ del cuerpo numérico $K = \mathbb{Q}(\sqrt{\Delta})$, en donde $\mathbb{A}$ es el conjunto de los enteros algebraicos y Δ está relacionado con d mediante la siguiente igualdad:

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

Tendremos en cuenta el siguiente teorema importante, conocido como la *ecuación de Pell.*

Teorema 4.1. [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. ☑

Si tenemos una forma cuadrática binaria $f(x,y) = \{a,b,c\} = ax^2 + bxy + cy^2$ donde $ac \neq 0$, y de tal forma que no se pueda factorizar (lo que implica que $d/4 = b^2/4 - ac$ no es un cuadrado perfecto), el discriminante d de la forma es entonces 0 o 1 módulo 4. Además, si la forma satisface $(a, b, c) = 1$, tal forma se llama *primitiva*.

Se puede considerar una *relación de equivalencia* entre formas cuadráticas utilizando la siguiente representación:

$$\{a, b, c\} = X^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} X, \qquad \{a', b', c'\} = X'^T \begin{pmatrix} a' & b'/2 \\ b'/2 & c' \end{pmatrix} X'$$

donde $X = \begin{pmatrix} x \\ y \end{pmatrix}$, $X' = \begin{pmatrix} x' \\ y' \end{pmatrix}$. Entonces diremos que las dos formas son *equivalentes*: $\{a, b, c\} \sim \{a', b', c'\}$ si existe una matriz $A \in M_{2\times 2}(\mathbb{Z})$ tal que $X = AX'$ y $\det A = 1$.

Teorema 4.2. *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:*

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

En el caso $d > 0$, la situación es más complicada, ya que se deben buscar soluciones de la ecuación

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

Por el teorema de la ecuación de Pell, dichas soluciones vienen dadas de la forma $\pm\epsilon^n$. Por esta razón si $d > 0$ se considera $w_d = 1$.

Si denotamos con Cl_K, $K = \mathbb{Q}(\sqrt{\Delta})$, al conjunto de todas las clases de formas de discriminante d módulo la relación de equivalencia $\sim$, y con $h(d)$ al número de clases de formas primitivas de discriminante d, entonces, gracias a la siguiente proposición, el hecho de que $h(d)$ sea finito sale de manera inmediata.

Teorema 4.3. *En cada clase de formas siempre hay una que satisface la condición*

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

Demostración. Si la forma es positiva, como $a > 0$, entonces

- 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 $b_1^2 - 4ac_1 = d$.

Este proceso para al cabo de un número finitos pasos. El caso general se puede obtener mediante una variación de este algoritmo. ☑

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

$$\begin{cases} -a < b \leq a & \text{si } c > a \\ 0 \leq b \leq a & \text{si } c = a \end{cases} \tag{7}$$

Si una forma cuadrática se encuentra como se acaba de plantear, ella se llama una *forma reducida*.

Definición 4.4. Si $\#Cl_K = h(d)$, entonces d se llama un *discriminante fundamental*.

Se observa que un discriminante fundamental D es aquel que no se puede expresar de la forma $D = d_0 t^2$ en donde d_0 es un discriminante. Por tanto, si $D \equiv 0$ módulo 4, $D/4$ es 2 o 3 módulo 4.

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

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

y también se considera el anillo de enteros $\mathcal{O}_K$ de K, el cual en este caso particular está conformado por:

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

A través de un cálculo sencillo, se tiene que el discriminante Δ del cuerpo K coincide justamente con D. Por otro lado, dado que las unidades α de $\mathcal{O}_K$ satisfacen $N_{K/\mathbb{Q}}(\alpha) = \pm 1$, para buscar las unidades se deben buscar por tanto soluciones de

$$\pm 1 = x^2 - dy^2.$$

Si $d < 0$ estas ecuaciones tienen un número finito de 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 4.1, la anterior ecuación 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. Obsérvese que si ϵ es la solución fundamental de la ecuación de Pell y $N_{K/\mathbb{Q}}(\epsilon_0) = -1$, entonces $\epsilon_0^2 = \epsilon$. En caso contrario $\epsilon = \epsilon_0$.

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

$$\alpha_1\alpha_2' - \alpha_1'\alpha_2 = N(I)\sqrt{D}\,, \tag{8}$$

donde $\alpha' = a - b\sqrt{d}$ si $\alpha = a + b\sqrt{d}$, y $N(I)$ es la norma del ideal. Se puede construir entonces la siguiente forma cuadrática:

$$f(x, y) = \frac{N(\alpha_1 x + \alpha_2 y)}{N(I)}.$$

Con este procedimiento se ha relacionado cada ideal con base $\{\alpha_1, \alpha_2\}$ a una forma cuadrática. Lo importante es que su recíproco también es verdadero lo que nos permite enunciar el siguiente teorema:

Teorema 4.5. *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* (8).

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

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

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

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

Definición 4.6.

i) Si I, J son ideales de $\mathcal{O}_K$ tales que existe $\gamma \in K \setminus \{0\}$ y satisface $\gamma J = I$, I, J se llaman *equivalentes* y escribimos $I \sim J$.
ii) Si γ en el anterior item satisface que $N_{K/\mathbb{Q}}(\gamma) > 0$, I, J se llaman *estrictamente equivalentes* y escribimos $I \approx J$.

Teorema 4.7. *Dos formas cuadráticas son equivalentes si y solo si sus respectivos ideales son equivalentes en el sentido estricto.*

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 denotamos por F_K el conjunto de todos los ideales de $\mathcal{O}_K$, $h_0 = \#(F_K/_\sim)$, $h = \#(F_K/_\approx)$, se tiene que $h = h(d)$ y además

$$h_0 = \begin{cases} h & \text{si } D < 0 \text{ o si } D > 0 \text{ y } N(\epsilon_0) = -1 \\ \frac{h}{2} & \text{si } D > 0 \text{ y } N(\epsilon_0) = 1. \end{cases} \tag{9}$$

Con esta última ecuación, se han relacionado dos números con características aparentemente muy diferentes.

Veamos ahora el valor exacto de h para finalmente obtener la fórmula de Dirichlet, donde además de eso, se relaciona con el valor $L(1, \chi_d) \neq 0$.

Definición 4.8. La pareja (x, y) se dice una *solución propia* de $f(x, y) = k$ si satisface la ecuación y además $(x, y) = 1$.

Definición 4.9. 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

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

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 4.10

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

Teorema 4.11 *Sean $m > 0$ y una elipse o una hipérbola centrada en el origen (en el último caso, se toma 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

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

se tiene un retículo cuadrado cuyo lado mide $m/\sqrt{N}$. Si se denota por $W(N)$ el número de cuadrados cuyas esquinas suroeste 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. ☑

Si $R(k,f)$ es el número de representaciones propias de k por la forma f, 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.

Teorema 4.12.

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

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

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

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

$$f(x,y)\le N, \quad x\equiv x_0 \pmod{|d|}, \quad y\equiv y_0 \pmod{|d|}. \tag{10}$$

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

$$\begin{aligned} &f(x,y)\le N, \quad \overline{L}>0, \quad 1\le \Big|\frac{L}{\overline{\overline{L}}}\Big| < \epsilon^2,\\ &x\equiv x_0 \pmod{d}, \quad y\equiv y_0 \pmod{d}. \end{aligned} \tag{11}$$

Por el teorema 4.11, tal número de puntos es $U(N)$, además

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

Por tanto,

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

Por el teorema 4.11, $\lim_{N\to\infty} \frac{U(N)}{N}$ no depende de f ni de (x,y); así

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

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 quedará demostrado.

Si $d<0$, el área de la elipse $f(x,y)\le 1$ 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 acotado 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 $L\overline{L}\le 4a$, $\overline{L}>0$ y $1\le L/\overline{L}<\epsilon^2$. Al calcular esta integral se tiene que $I=\log\epsilon/\sqrt{d}$, con lo cual el teorema queda demostrado. ☑

Teorema 4.13.

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

Observación 4.13. Gracias a la ecuación (9) se tiene

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

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

5. La función L de Dedekind.

Ahora vamos a recordar algunos resultados básicos de teoría algebraica de números. La mayoría de los resultados enunciados acá, se encuentran demostrados en libros tales como [2, cap. 2] y [3, cap. 1]; por tal motivo, si el lector está interesado en profundizar los resultados expuestos, está ampliamente invitado a consultar alguna de estas referencias.

Sea K una extensión finita de $\mathbb{Q}$ de dimensión n. Sea $\mathcal{O}_K$ es el conjunto de enteros algebraicos de K.

Proposición 5.1. *$\mathcal{O}_K$ es un grupo libre de rango n sobre $\mathbb{Z}$, es decir, existen $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathcal{O}_K$ tales 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.

El discriminante del cuerpo de números K, será denotado por Δ_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 5.2. 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 5.3. 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 tiene $n = r_1 + 2r_2$. Además, se tendrá en cuenta el siguiente orden para dichos encajes: $\sigma_1, \sigma_2, \ldots, \sigma_{r_1}$ 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.

Definición 5.4. 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 *paralelepípedo fundamental del retículo* $\mathfrak{M}$.

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

$$||x||^2 = \sum_{i \leq r_1} x_i^2 + 2 \sum_{r_1 < i \leq r_2} |x_i|^2. \tag{12}$$

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

$$d\,\mathrm{Vol} = 2^{r_2} dx_1 \cdots dx_{r_1} d\,\mathrm{Re}\, x_{r_1+1} d\,\mathrm{Im}\, x_{r_1+1} \cdots d\,\mathrm{Re}\, x_{r_1+r_2} d\,\mathrm{Im}\, x_{r_1+r_2}. \tag{13}$$

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 se le llama *geometría de los números*; sin embargo, acá sólo utilizamos algunas herramientas básicas sin entrar en detalles. Dado el orden a los encajes, se tiene el siguiente homomorfismo:

$$\begin{aligned} j : K &\longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ x &\longrightarrow (\sigma_i(x))_{i \leq r_1+r_2}. \end{aligned} \tag{14}$$

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 $N(x) \neq 0$:

$$\begin{aligned} l : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} &\longrightarrow \mathbb{R}^{r_1+r_2} \\ (x_i) &\longrightarrow (a_i \log |x_i|) \end{aligned} \tag{15}$$

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

$$\sum \lambda_i(x) = \log |N_{K/\mathbb{Q}}(x)|. \tag{16}$$

Teorema 5.5. *Si* $\mathfrak{M} = j(\mathcal{O}_K)$, $\mathfrak{M}$ *es un retículo completo de* K *y*

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

Teorema 5.6. *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:*

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

Si consideramos el grupo de ideales fraccionaros J_K de $\mathcal{O}_K$ se tiene que:

Definición 5.7. 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 5.8. 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 5.9. *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 presentamos un bosquejo de su demostración.

Teorema 5.10. *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 $\mathfrak{a} \in \mathcal{O}_K$ tales 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. ☑

Teorema 5.11. *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 5.12. Se notará a r como $r = \dim \mathcal{H}_0 = r_1 + r_2 - 1$.

Teorema 5.13. [Dirichlet] *Existen elementos $\epsilon_1, \epsilon_2, \ldots, \epsilon_r \in \mathcal{O}_K^*$ tales 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 5.14. El conjunto $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_r\}$ se llama 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

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

se llama *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:

$$\begin{pmatrix} \lambda_1(\epsilon_1) & \cdots & \lambda_{r_1+r_2}(\epsilon_1) \\ \vdots & & \vdots \\ \lambda_1(\epsilon_r) & \cdots & \lambda_{r_1+r_2}(\epsilon_r) \end{pmatrix}. \tag{17}$$

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 5.15. 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 $d\xi_1 \cdots d\xi_r$.

Sin embargo, se puede modificar la definición al debilitar las unidades de $\mathcal{O}_K$ vía localización, y definir lo que se conoce como *S–unidades*.

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

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

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.

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 5.16. *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 5.17. $K^S \cong \mu(K) \times \mathbb{Z}^{\#S+r}$ *donde $\mu(K)$ es el conjunto de las raíces de la unidad contenidas en K.*

Corolario 5.18 *El grupo de las S-clases Cl_K^S es finito.*

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

Definición 5.19. 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 para ella, se tienen para las funciones zeta de Dedekind propiedades similares a las descritas en la sección 2. A continuación presentamos esta función en términos de un producto de Euler.

Proposición 5.20. *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.

En la demostración de esta proposición, similar a la función zeta de Riemann, se utiliza el hecho fundamental que cada ideal entero de K se factoriza de manera única en ideales primos.

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.

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

$$L_\infty(s) = L_{\mathbb{R}}^{r_1}(s)L_{\mathbb{C}}^{r_2}(s). \tag{18}$$

Teorema 5.21. *La función*

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

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

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

6. La fórmula del número de clases de Dedekind.

Ahora vamos a relacionar el residuo de la función $\zeta_K(s)$ en el punto $s = 1$, con el número de clases de Dedekind, y al final exponemos la función zeta de Dedekind incompleta.

Gracias a que el vector

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

el conjunto formado por los elementos

$$l^*, \lambda(\epsilon_1), \dots, \lambda(\epsilon_r) \tag{19}$$

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

$$l(x) = \xi l^* + \xi_1\lambda(\epsilon_1) + \cdots + \xi_r\lambda(\epsilon_r) \tag{20}$$

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

Definición 6.1. 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 $\xi_1, \dots, \xi_r$ en la representación de (20) cumplen las desigualdades $0 \leq \xi_i < 1$.
c. Si x_1 es la primera componente de x, entonces $0 \leq \arg x_1 < 2\pi/w$.

Teorema 6.2. *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.*

Si se considera ahora la siguiente función:

$$\mathfrak{Z}(s) = \sum_{x \in \mathfrak{M} \cap Y} \frac{1}{|N(x)|^s}, \qquad (s > 1) \tag{21}$$

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 6.3. *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:

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

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 6.4. *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 (13).

Demostración. Sea 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 (20) cumplen que $0 \leq \xi_i < 1$.

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

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,

$$\mathrm{Vol}(T') = 2^{r_1} \, \mathrm{Vol}(\overline{T}).$$

Como $\mathrm{Vol}(T')$ es w veces el volumen v del conjunto T, entonces

$$v = \frac{2^{r_1}}{w} \, \mathrm{Vol}(\overline{T}), \tag{22}$$

de manera que es suficiente calcular el volumen del conjunto $\overline{T}$. Al retomar la ecuación (16), dado que $|N_{K/\mathbb{Q}}(\epsilon_i)| = 1$ para cada unidad fundamental, entonces por la descomposición de la ecuación (20), 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 (20) está dado por

$$\xi = \frac{\log|N(x)|}{n},$$

y así se obtiene que

$$l(x) = \frac{\log|N(x)|}{n} l^* + \xi_1 \lambda(\epsilon_1) + \cdots + \xi_r \lambda(\epsilon_r); \tag{23}$$

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 (15). Para calcular el volumen de $\overline{T}$, es conveniente hacer el cambio de variable siguiente:

$$\begin{array}{rl} x_k = \rho_k & \qquad k \leq r_1 \\ \left.\begin{array}{r} y_k = \rho_{r_1+k} \cos\phi_k \\ z_k = \rho_{r_1+k} \sin\phi_k \end{array}\right\} & \quad r_1 < k \leq r_1 + r_2 \end{array},$$

donde $x_{r_1+k} = y_k + iz_k$. Un cálculo directo da el valor del jacobiano como

$$J = \rho_{r_1+1} \cdots \rho_{r_1+r_2}. \tag{24}$$

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

$$\log \rho_j^{a_j} = \frac{a_j}{n} \log \xi + \sum_i \xi_i \lambda_j(\epsilon_i) \tag{25}$$

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:

$$\begin{aligned} J = \det \begin{pmatrix} \frac{\rho_1}{n\xi} & \rho_1 \lambda_1(\epsilon_1) & \cdots & \rho_1 \lambda_1(\epsilon_r) \\ \vdots & \vdots & & \vdots \\ \frac{\rho_{r_1+r_2}}{n\xi} & \frac{\rho_{r_1+r_2}}{2} \lambda_{r_1+r_2}(\epsilon_1) & \cdots & \frac{\rho_{r_1+r_2}}{2} \lambda_{r_1+r_2}(\epsilon_r) \end{pmatrix} \\ = \frac{\rho_1 \cdots \rho_{r_1+r_2}}{n\xi 2^{r_2}} nR = \frac{R}{2^{r_2} \rho_{r_1+1} \cdots \rho_{r_1+r_2}}. \end{aligned} \tag{26}$$

Con estos cambios de variable, dado que el producto de los dos jacobianos (24) y (26) es $R/2^{r_2}$ y que el elemento de volumen según la ecuación (12) 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 (22), 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 6.5.[Número de clases de Dedekind.]

$$\lim_{s \to 1} (s-1) \zeta_K(s) = \frac{2^{r_1} (2\pi)^{r_2} R h_K}{w \sqrt{|\Delta_K|}}$$

donde h_K es el número de clases de ideales de K, R es el regulador del cuerpo, y w es el número de raíces de la unidad contenidas en K.

Gracias al teorema 6.5, se sigue de inmediato el siguiente corolario.

Corolario 6.6. *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.

Gracias al residuo de la función $Z_K(s)$ en $s = 0$, se puede verificar de manera fácil el siguiente corolario:

Corolario 6.7. *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*

$$-\frac{Rh_K}{w}.$$

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 presentados no los demostraremos.

Definición 6.8. 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 con S_∞ denotaremos 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 5.17, si $r = \#S - 1$ existen unidades $u_1, \ldots, u_r$ tales 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 6.7 mediante la siguiente proposición:

Proposición 6.9. *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 terminada esta parte sin antes relacionar la función zeta de Dedekind con la función L de Dirichlet.

Teorema 6.10. 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 6.5,

$$L(1,\chi) = \lim_{s\to 1}(s-1)\zeta(s)L(s,\chi) = \lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2R}{\sqrt{d}}h.$$

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 6.5,

$$L(1,\chi) = \lim_{s\to 1}(s-1)\zeta(s)L(s,\chi) = \lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2\pi}{w_d\sqrt{|d|}}h.$$

Esto es justo lo que nos dice la observación 4.13. Luego hasta el momento, la función zeta de Riemann, las funciones L de Dirichlet y finalmente, la función zeta de Dedekind, están profundamente relacionadas.

7. Conjeturas de Stark sobre valores especiales de funciones L más generales.

En esta última sección, se dará una pequeña explicación, sin entrar en detalles, acerca de funciones L más generales como lo son las L de Hecke y las L de Artin; se presentarán su ecuaciones funcionales, y como cierre de este escrito, se expondrá una conjetura de Stark en su forma más simple, ya que a través de los años, han sido reformuladas y generalizadas, 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 [3, 4, 5].

Antes de enunciar lo que son 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

$$K(\mathfrak{f}) = \{\alpha \in K \mid (\alpha) \in P(\mathfrak{f})\}.$$

Por $K_{\mathfrak{f}}$ se notará el conjunto formado por aquellos elementos $\alpha \in K(\mathfrak{f})$ tales 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) tales que $\alpha \in K_{\mathfrak{f}}$.

Definición 7.1. 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 (14).

Definición 7.2. 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 7.3. 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 carácter χ_∞ se puede expresar de la siguiente manera:

Proposición 7.4. *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 7.5. 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. 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 Chevalley en los años treinta y cuarenta.

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 en 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 lo que realmente se prueba es lo siguiente:

Teorema 7.6. *Sea χ un carácter módulo $\mathfrak{f}$ y $L(s,\chi)$ su función L asociada. Si se define*

$$\Lambda(s,\chi) = (|\Delta_K|\mathfrak{N}(\mathfrak{f}))^{s/2} L_\infty(s) L(s,\chi),$$

donde L_∞ es definido por la ecuación 18, y $\mathfrak{N}(\mathfrak{f})$ es la norma del ideal $\mathfrak{f}$, entonces $\Lambda(s,\chi)$ 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 evaluado, y p, q están dados por la proposición 7.4. Además se satisface la ecuación funcional

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

donde el número $W(\chi)$ que aparece en la ecuación, tiene norma 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 5.11, 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.

Así como se hizo con las funciones L de Hecke, se necesitan algunas nociones previas antes de definir la función L de Artin.

Sean F, K cuerpos de números tal que F/K es una extensión de Galois finita.

Definición 7.7. 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 7.8. *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 con

$$\mathrm{Infl}\,\chi = \chi \circ \pi$$

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 $\mathfrak{k}_{\mathfrak{w}}$ el cuerpo de residuos $\mathcal{O}_F/\mathfrak{P}_w$.

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 característica 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 7.9. Si w es un lugar arquimediano y x_w la imagen de x mediante el encaje w, entonces

$$|x|_w = \begin{cases} |x_w| & \text{el valor absoluto de } x_w \text{ si el encaje } w \text{ es real;} \\ x_w\overline{x}_w & \text{la norma usual al cuadrado de } x_w \text{ si el encaje } w \text{ es complejo.} \end{cases}$$

Si w es un lugar de F, se define el grupo de descomposición G_w como

$$G_w = \{\sigma \in G | \sigma w = w\}.$$

Se observa por la definición que

$$G_{\tau w} = \{\sigma \in G | \sigma\tau w = \tau w\} = \tau^{-1} G_w \tau,$$

además que G actúa transitivamente sobre los lugares de F que dividen a un lugar fijo v de K.

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 $[\sigma]$ sobre $\mathfrak{k}_w$. Se tiene entonces la siguiente definición:

Definición 7.10. El *grupo de inercia* I_w de w se define como

$$I_w = \{\sigma \in G_w \mid [\sigma] \text{ es el elemento trivial de } \operatorname{Gal}(\mathfrak{k}_w/\mathfrak{k}_v)\}.$$

Proposición 7.11. *La extensión $\mathfrak{k}_w/\mathfrak{k}_v$ es cíclica, es decir, el grupo de Galois* $\operatorname{Gal}(\mathfrak{k}_w/\mathfrak{k}_v)$ *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 7.12. *El cociente G_w/I_w es isomorfo a* $\operatorname{Gal}(\mathfrak{k}_w/\mathfrak{k}_v)$ *mediante $\sigma \mapsto [\sigma]$.*

Definición 7.13. Abusando de la notación, se denotará con Fr_w a cualquier elemento $\sigma \in G_w$ tal que $[\sigma]$ es el automorfismo de Frobenius de k_w/k_v definido en la proposición 7.11.

Observación 7.14. Se observa que dos de 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 unívocamente definido.

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 7.15. Sea $H \leq G$ un subgrupo de G, se define V^H como:

$$V^H = \{v \in V \mid \sigma x = x \ \forall x \in H\}.$$

Con estas notaciones dadas, se puede definir entonces la función L de Artin:

Definición 7.16 Para $\operatorname{Re}(s) > 1$ 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 7.14.

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 7.14, 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

$$a_1 = \sum_{v \text{ real}} \dim(V^{G_w}), \qquad a_2 = \sum_{v \text{ real}} \operatorname{codim}(V^{G_w}),$$

luego el término a multiplicar en la función L de Artin está dado por

$$L_{v|\infty}(s) = L_{\mathbb{C}}(s)^{r_2\chi(1)} L_{\mathbb{R}}(s)^{a_1} L_{\mathbb{R}}(s+1)^{a_2}.$$

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 7.17. El ideal

$$f(\chi) = \prod_{v \in S'} \mathfrak{p}_v^{f(\chi,v)},$$

recibe el nombre de *conductor de Artin asociado a* χ.

Con estas notaciones previas, se puede enunciar el próximo teorema:

Teorema 7.18. *Si*

$$\Lambda(s,\chi) = (|\Delta_K|^{\chi(1)}\mathfrak{N}(f(\chi))^{s/2} L_{v|\infty}(s) L(s,\chi),$$

la función $\Lambda(s,\chi)$ *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 ecuación funcional que ellas satisfacen son funciones analíticas 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 7.19. [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 la anterior sección, esta tiene polos en los puntos $s = 0$ y $s = 1$.

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 tales 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

$$X = \left\{ \sum_{w\in S_F} n_w w \in Y | \sum_{w\in S_F} n_w = 0 \right\}. \tag{27}$$

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:

$$L(s,\chi) = c(\chi)s^{r(\chi)} + O(s^{r(\chi)+1}) \tag{28}$$

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 7.20. *El exponente $r(\chi)$ en la ecuación (28) satisface la igualdad*

$$r(\chi) = \left(\sum_{v\in S} \dim V^{G_w}\right) - \dim V^G = \dim_{\mathbb{C}} \operatorname{Hom}_G(V^*, \mathbb{C}\otimes_{\mathbb{Z}} X),$$

en donde a $\mathbb{C}\otimes_{\mathbb{Z}} X$ se le asocia una estructura de $\mathbb{C}[G]-$módulo.

Observación 7.21. La elección de w en la anterior proposición sólo 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 $\alpha \in \operatorname{Aut}(\mathbb{C})$ 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

$$U = \{x \in K | \; |x|_w = 1 \; \forall w \notin S_K\}, \tag{29}$$

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 7.22. *El kernel de λ es el conjunto $\mu(K)$ y su imagen es un retículo completo de rango $\#S - 1$ en $\mathbb{R}\otimes_{\mathbb{Z}} X$.*

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 denota 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 $\operatorname{Hom}(W, \mathbb{C}\otimes X)$ es un módulo sobre $\mathbb{C}[G]$ donde la acción está dada por

$$(g\phi)(w) = g\phi(g^{-1}w)$$

para $\phi \in \operatorname{Hom}(W, \mathbb{C}\otimes X)$, $g \in \mathbb{C}[G]$ y $w \in W$, por tanto se le puede asociar una estructura de módulo sobre $\mathbb{C}[G]$ a V^*, ya que

$$V^* = \operatorname{Hom}(V, \mathbb{C}),$$

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

$$\begin{array}{ccc} \mathrm{Hom}_G(V^*, \mathbb{C} \otimes X) & \stackrel{(\lambda \circ f)_V}{\longrightarrow} & \mathrm{Hom}_G(V^*, \mathbb{C} \otimes X) \\ \phi & \to & \lambda \circ f \circ \phi. \end{array}$$

Definición 7.23. 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 únicamente de f. más no de la realización V del carácter χ. Se observa que gracias a la proposición 7.20, 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 $\mathbb{Q}$ tal que se le adjunta 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 7.24. *Sean F/K una extensión de Galois finita de cuerpos numéricos, sea $G = \mathrm{Gal}(F/K)$, χ el carácter de una la representación finito dimensional de G sobre $\mathbb{C}$, y sea f como antes. Si*

$$A(\chi, f) = \frac{R(\chi, f)}{c(\chi)} \in \mathbb{C},$$

entonces

$$\begin{cases} A(\chi, f) \in \mathbb{Q}(\chi) & \textit{y} \\ A(\chi, f)^\alpha = A(\chi^\alpha, f) & \textit{para todo } \alpha \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}) \end{cases}$$

Como se puede observar en el caso de la función zeta de Dedekind, dado que $\chi(\mathfrak{p}) = 1$ para cada ideal primo, entonces $\mathbb{Q}(\chi_0) = \mathbb{Q}$, por tanto $A(\chi_0, f)^\alpha = A(\chi_0^\alpha, f)$ de manera trivial.

Para ver que $A(\chi_0, f) \in \mathbb{Q}$, dado que el conjunto de lugares está compuesto por los encajes de K, se observa lo siguiente:

$$\begin{aligned} X &= \left\{ \sum_\sigma n_\sigma \sigma \mid \sum_\sigma n_\sigma = 0 \right\} \\ &= \left\{ \sum_{\sigma \in S \smallsetminus \{\sigma\}} n_\sigma (\sigma - \sigma_0) \right\} \end{aligned}$$

para cualquier lugar fijo $\sigma_0 \in S$. Luego $\{\sigma_i - \sigma_{r_1+r_2}\}_{i\leq r}$ es una base para X. Si

$$\begin{aligned} f : X &\longrightarrow U, & \lambda : U &\longrightarrow \mathbb{R}\otimes X \\ \sigma_i - \sigma_{r_1+r_2} &\longrightarrow \epsilon_i & \epsilon_i &\longrightarrow \sum_{j\leq r_1+r_2} \log|\sigma_j^{a_j}(\epsilon_i)| \otimes \sigma_j \end{aligned}$$

donde a_j se toma como en la ecuación(15) gracias a la definición 7.9. Entonces

$$\begin{aligned} \lambda \circ f(1\otimes(\sigma_i - \sigma_{r_1+r_2})) &= \sum_{j\leq r_1+r_2} \lambda_j(\epsilon_i)\otimes\sigma_j \\ &= \sum_{j\leq r} \lambda_j(\epsilon_i)\otimes(\sigma_j - \sigma_{r_1+r_2}) \end{aligned}$$

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. Así, $A(\chi_0, f)$ queda expresado como

$$A(\chi_0, f) = \frac{R}{c(\chi)} = -\frac{w}{h} \in \mathbb{Q}.$$

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 detrás de él, están involucradas las unidades fundamentales de ciertos anillos de enteros.

Referencias

[1] T. M. Apostol, *Introduction to Analytic Number Theory*. Springer: New York, 1976.
[2] Z. I Borevich & I. R. Shafarevich, Number Theory. Academic Press: New York, 1966.
[3] Jürgen Neukirch, *Algebraic Number Theory*. Springer–Verlag: Berlin, 1999.
[4] John Tate, *Les conjectures de Stark sur les fonctions L d'Artin en s* = 0. Progress in Mathematics. Birkhäuser: Boston, 1984.
[5] J.–P. Serre, *Linear Representations of Finite Groups*. Springer–Verlag: New York, 1977.
[6] H. M. Stark, *Hilbert's twelfth problem and L-series*. Bull. Amer. Math. Soc. **83** (1977), 1072–1074.

(Recibido en abril de 2013. Aceptado para publicación en abril de 2014)

Elkin O. Quintero
Departamento de Matemáticas
Universidade de São Paulo, São Paulo, Brasil
e-mail: eoquinro@ime.usp.br