XXXVI Semana de la Matemática
Pontificia Universidad Católica de Valparaíso
7 - 9 de Octubre 2009

Funciones L - de Artin

Amalia Pizarro Madariaga
Universidad de Tarapacá

Índice

1. Introducción

En las siguientes notas, quisieramos presentar un introducción a las funciones L - de Artin, el cual es un tópico que juega un rol central en la teoría de números.

Además nos gustaría dar una visión general de la variedad de funciones L y algunos progresos recientes de problemas nuevos y antiguos.

Esta funciones son un ejemplo especial de las series de Dirichlet. Ellas tienen en común que sus representaciones en serie pueden ser escritas como un producto de Euler, es decir, un producto tomado sobre los números primos. El ejemplo más famoso es la función zeta de Riemann

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

Dos de los siete problemas del milenio son a cerca de funciones L: la Hipótesis de Riemann (todos los ceros de la $\zeta(s)$ están en la recta crítica $\mathrm{Re}(s) = 1/2$) y la conjetura de Birch y Swinnerton-Dyer (el rango del grupo Mordell-Weil de una curva elítpica es el orden del cero de la función L asociada $L_E(s)$ en $s = 1$).

En la primera parte, estudiaremos los conceptos necesarios de la teoría algebraica de números y representaciones de grupos para poder definir las funciones L - de Artin.

En la segunda parte, definiremos la función L - de Artin y demostraremos algunas de sus propiedades fundamentales.

Finalmente daremos una revisión a importantes problema resueltos y otros aun abiertos de la teoría de números, como la conjetura de Artin sobre la holomorfía de la funciones L - de Artin sujeto a la veracidad de la conjetura de Selberg y la conjetura de Taniyama-Shimura.

2. Conceptos previos

En este capítulo se introducirán los conceptos necesarios sobre teoría algebraica de números y representaciones de grupos para entender las definiciones y propiedades de las funciones L.

De aquí en adelante, consideraremos L/K una extensión de Galois con $\mathcal{G} = Gal(L/K)$.

Llamaremos *cuerpo de números* a cualquier extensión algebraica finita de $\mathbb{Q}$.

Si K es un cuerpo de números, diremos que un elemento $x \in K$ es un *entero algebraico* si satisface una ecuación

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0,$$

donde $a_i \in \mathbb{Z}$. El conjunto de los enteros algebraicos en K será denotado por $\mathcal{O}_K$ y será llamado *anillo de enteros.*

Sea K un cuerpo de números y L/K una extensión finita de cuerpos. Un ideal primo no nulo en $\mathcal{O}_K$ usualmente será llamado *primo de* K. Notar que $\mathcal{O}_K \subseteq \mathcal{O}_L$.
Sean $\mathfrak{p}$ y $\mathfrak{b}$ primos en $\mathcal{O}_K$ y $\mathcal{O}_L$ respectivamente. Diremos que $\mathfrak{b}$ *está sobre* $\mathfrak{p}$ si $\mathfrak{b} \cap \mathcal{O}_K = \mathfrak{p}$. La siguiente proposición nos ayuda a describir la acción del grupo de Galois $\mathcal{G}$ sobre los primos $\mathfrak{b}$ sobre $\mathfrak{p}$.

Proposición 2.1. *Sean $\mathfrak{p}$ un ideal maximal de $\mathcal{O}_K$ y sean $\mathfrak{b}_1$ y $\mathfrak{b}_2$ dos ideales primos en $\mathcal{O}_L$ sobre $\mathfrak{p}$. Entonces existe $\sigma \in \mathcal{G}$ tal que $\sigma(\mathfrak{b}_1) = \mathfrak{b}_2$.*

Demostración. Supongamos que $\mathfrak{b}_2 \neq \sigma(\mathfrak{b}_1)$ para cualquier $\sigma \in \mathcal{G}$. Entonces por el teorema chino de los restos, existe $x \in \mathcal{O}_L$ tal que

$$\begin{aligned} x &\equiv 0 \pmod{\mathfrak{b}_1} \\ x &\equiv 1 \pmod{\sigma(\mathfrak{b}_2)}, \text{ para todo } \sigma \in \mathcal{G} \end{aligned}$$

Definimos el siguientes elemento, llamado norma de x

$$N_{L/K}(x) = \prod_{\sigma \in \mathcal{G}} \sigma(x). \tag{2.1}$$

Este elemento está en $\mathcal{O}_L \cap K = \mathcal{O}_K$ y está en $\mathfrak{b}_1 \cap \mathcal{O}_K = \mathfrak{p}$. Pero $x \notin \sigma(\mathfrak{b}_2)$, pues $\sigma(x) \notin \mathfrak{b}_2$. Esto contradice que la norma de x está en $\mathfrak{p}$. □

Concluimos entonces que la acción es transitiva.

Corolario 2.1. *Existe un número finito de ideales $\mathfrak{b}$ sobre $\mathfrak{p}$*

Teorema 2.1. *(Kummer) Si $\mathcal{O}_K$ es un anillo de enteros, entonces cada uno de sus ideales no nulos puede ser escrito únicamente como un producto de ideales primos.*

2.1. Factorización de primos en extensiones

Sea L/K una extensión de Galois con $n = [L : K]$ y $\mathfrak{p}$ un ideal primo en $\mathcal{O}_K$. Por el teorema de Kummer, el ideal $\mathfrak{p}\mathcal{O}_L$ tiene una factorización única

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{b}_1^{e_1} \cdots \mathfrak{b}_r^{e_r}, \qquad e_1 \geq 1$$

en primos de $\mathcal{O}_L$. Es claro que un primo $\mathfrak{b}$ en $\mathcal{O}_L$ está en la factorización si y solo si $\mathfrak{b}$ está sobre $\mathfrak{p}$. Cada $e_i = e_{\mathfrak{b}_i/\mathfrak{p}}$ será llamado *índice de ramificación* de $\mathfrak{b}_i$ sobre $\mathfrak{p}$ y denotaremos por $f_{\mathfrak{b}_i/\mathfrak{p}}$ al grado de la extensión de cuerpos $\mathcal{O}_L/\mathfrak{b}$ sobre $\mathcal{O}_K/\mathfrak{p}$ y será llamado *grado del cuerpo residual*. Diremos que un ideal $\mathfrak{b}_i$ en la factorización es *no ramificado* si $e_i = 1$. En caso contrario

será llamado *ramificado*. Diremos que $\mathfrak{p}$ es no ramificado si todos los $\mathfrak{b}_i$ son no ramificados, en otro caso será llamado ramificado. Definimos la norma de un ideal primo como

$$N_{L/K}(\mathfrak{b}) = \mathfrak{p}^{f_{\mathfrak{b}/\mathfrak{p}}}.$$

Proposición 2.2. $f_{\mathfrak{b}/\mathfrak{p}} = [l_{\mathfrak{b}} : k_{\mathfrak{p}}]$.

Demostración. Por definición, $N_{L/K}(\mathfrak{b}) = \mathfrak{p}^{f_{\mathfrak{b}/\mathfrak{p}}}$. Tomando $N_{K/\mathbb{Q}}$ a ambos lados

$$|l_{\mathfrak{b}}| = N_{L/\mathbb{Q}}(\mathfrak{b}) = N_{L/\mathbb{Q}}(\mathfrak{p})^{f_{\mathfrak{b}/\mathfrak{p}}} = |k_{\mathfrak{p}}|^{f_{\mathfrak{b}/\mathfrak{p}}}.$$

De esta forma,

$$[l_{\mathfrak{b}} : k_{\mathfrak{p}}] = \log_{k_{\mathfrak{p}}} |l_{\mathfrak{b}}| = f_{\mathfrak{b}/\mathfrak{p}}.$$

□

Proposición 2.3. *Sea $M/L/K$ una torre de cuerpo y $\mathfrak{p}$ un ideal primo en $\mathcal{O}_K$, $\mathfrak{q}$ un primo en $\mathcal{O}_L$ sobre $\mathfrak{p}$ y $\mathfrak{b}$ un primo en $\mathcal{O}_M$ sobre $\mathfrak{q}$. Entonces,*

$$\begin{aligned} e_{\mathfrak{b}/\mathfrak{p}} &= e_{\mathfrak{b}/\mathfrak{q}} e_{\mathfrak{q}/\mathfrak{p}} \\ f_{\mathfrak{b}/\mathfrak{p}} &= f_{\mathfrak{b}/\mathfrak{q}} f_{\mathfrak{q}/\mathfrak{p}}. \end{aligned}$$

Demostración. Se deduce de las propiedades multiplicativas de grados de extensiones y de la norma. □

Proposición 2.4.

$$\sum_{\mathfrak{b}/\mathfrak{p}} e_{\mathfrak{b}/\mathfrak{p}} f_{\mathfrak{b}/\mathfrak{p}} = n.$$

Demostración. Supongamos que $\mathfrak{p} = \prod_i \mathfrak{b}_i$. Como la norma es multiplicativa,

$$\mathfrak{p}^n = N_{L/K}(\mathfrak{p}) = \prod_{\mathfrak{b}/\mathfrak{p}} N_{L/K}(\mathfrak{b}^{e_{\mathfrak{b}}/\mathfrak{p}}) = \prod_{\mathfrak{b}/\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{b}/\mathfrak{p}}}.$$

□

2.2. Automorfismo de Frobenius

Fijemos un primo $\mathfrak{b}$ sobre $\mathfrak{p}$ y denotemos por $l_{\mathfrak{b}}$ y $k_{\mathfrak{p}}$ a los cuerpos residuales $\mathcal{O}_L/\mathfrak{b}$ y $\mathcal{O}_K/\mathfrak{p}$ respectivamente, donde $f_{\mathfrak{b}/\mathfrak{p}}$ es el grado de la extensión $l_{\mathfrak{b}}/k_{\mathfrak{p}}$.

Definimos el *grupo de descomposición de $\mathfrak{b}$ sobre $\mathfrak{p}$* como el subgrupo de $\mathcal{G}$ que deja fijo el ideal $\mathfrak{b}$, es decir

$$G_{\mathfrak{b}} = \{\sigma \in \mathcal{G} : \sigma(\mathfrak{b}) = \mathfrak{b}\}.$$

Como $\mathcal{G}$ actúa transitivamente sobre los primos, si hay $g_\mathfrak{p}$ diferentes primos sobre $\mathfrak{p}$, entonces $|G_\mathfrak{b}| = \frac{n}{g_\mathfrak{p}} = e_\mathfrak{p} f_\mathfrak{p}$.

Además a cada $\sigma \in G_\mathfrak{b}$ induce un automorfismo $\overline{\sigma} \in Gal(l_\mathfrak{b}/k_\mathfrak{p})$

$$\overline{\sigma} : l_\mathfrak{b} \to l_\mathfrak{b}\,, \qquad a \bmod \mathfrak{b} \mapsto \sigma(a) \bmod \mathfrak{b}. \tag{2.2}$$

luego tenemos un homomorfismo de $G_\mathfrak{b} \to Gal(l_\mathfrak{b}/k_\mathfrak{p})$.
El núcleo del homomorfismo (2.2) será llamado *grupo de inercia* de $\mathfrak{b}$ y será denotado por $T_\mathfrak{b}$; está formado por los automorfismos de $G_\mathfrak{b}$ que inducen el automorfismo trivial en el cuerpo de clases residuales.

Se define la norma absoluta de $\mathfrak{p}$ como $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$. Sea $p = \mathfrak{b} \cap \mathbb{Z}$. Entonces $N(\mathfrak{p})$ es una potencia de p. Como $l_\mathfrak{b}/k_\mathfrak{p}$ es una extensión de cuerpos finitos, el grupo $Gal(l_\mathfrak{b}/k_\mathfrak{p})$ es cíclico y generado por la función $x \mapsto x^{N(\mathfrak{p})}$. Podemos escoger un elemento $\sigma_{\mathfrak{b}/\mathfrak{p}} \in G_\mathfrak{b}$ cuya imagen en $Gal(l_\mathfrak{b}/k_\mathfrak{p})$ es este generador que será llamado *automorfismo de Frobenius* de $\mathfrak{b}$ y verifica

$$\sigma_{\mathfrak{b}/\mathfrak{p}}(x) \equiv x^{N(\mathfrak{p})} \qquad (\mathrm{mod}\, \mathfrak{b}).$$

Notar que el Frobenius está definido solo mod $T_\mathfrak{b}$. Para $\mathfrak{p}$ no ramificado, el Frobenius está bien definido pues $T_\mathfrak{b}$ es trivial.

Proposición 2.5. *La aplicación $\sigma \mapsto \overline{\sigma}$ es sobreyectiva.*

Demostración. Por el teorema chino de los restos y por el hecho que el grupo multiplicativo de un cuerpo finito es cíclico, podemos escoger un generador a en el grupo de unidades de $\mathcal{O}_L/\mathfrak{b}$ el cual es divisible por todos los conjugados de $\mathfrak{b}$ por el grupo de Galois.
Sea

$$F(x) = \prod_{\sigma \in \mathcal{G}} (x - \sigma(a)).$$

Es claro que $F(a) \equiv 0 \pmod{\mathfrak{b}}$. Entonces

$$F(a^{N(\mathfrak{p})}) \equiv F(a)^{N(\mathfrak{p})} \equiv 0 \pmod{\mathfrak{b}},$$

luego tendríamos para algún $\sigma \in \mathcal{G}$, $\sigma(a) = a^{N(\mathfrak{p})}$. Supongamos que σ no está en el grupo de descomposición. En ese caso, $\sigma^{-1}(\mathfrak{b}) \neq \mathfrak{b}$ y por la elección de a, $a \equiv 0 \pmod{\sigma^{-1}(\mathfrak{b})}$ y esto implicaría que $\sigma(a) \equiv 0 \pmod{\mathfrak{b}}$, lo cual es una contradicción. De esta forma este automorfismo está en el grupo de descomposición. □

Además, de la sucesión exacta

$$1 \to T_\mathfrak{b} \to G_\mathfrak{b} \to Gal(l_\mathfrak{b}/k_\mathfrak{p}) \to 1$$

se tiene el isomorfismo

$$G_\mathfrak{b}/T_\mathfrak{b} \simeq Gal(l_\mathfrak{b}/k_\mathfrak{p}).$$

2.3. Teoría de Representaciones de Grupos.

Sea G un grupo finito y $\rho : G \to GL(V)$, una representación lineal de G. Llamaremos *subrepresentación* a cualquier subespacio $W \subseteq V$ que es preservado por la acción de G. Si una representación V no tiene subrepresentaciones no triviales, diremos que V es *irreducible*.

Si (V_1, ρ_1) y (V_2, ρ_2) son dos representaciones de G, definimos la suma directa entre estas representaciones como la representación $(V_1 \oplus V_2, \rho_1 \oplus \rho_2)$, donde $\rho_1 \oplus \rho_2(v_1, v_2) = v_1 \oplus v_2$. Se verifica que toda representación puede ser escrita como suma directa de representaciones irreducibles. (Ver Serre [7])

Dos representaciones (V_1, ρ_1) y (V_2, ρ_2) son equivalentes si V_1 y V_2 son isomorfos.

Definimos el *caracter* de una representación (V, ρ) como la función

$$\chi_\rho : G \Rightarrow \mathbb{C}, \qquad \chi_\rho(\sigma) = \text{traza}\, \rho(\sigma).$$

Verifica que $\chi_\rho(1)$=dim(V) y $\chi_\rho(\sigma\tau\sigma^{-1}) = \chi_\rho(\tau)$, para todo $\sigma, \tau \in G$. En general, cualquier función $g : G \to \mathbb{C}$ que verifique $g(\sigma\tau\sigma^{-1}) = g(\tau)$ será llamada *función de clases*.
Notar que dos representaciones son *equivalentes* si y solo si sus caracteres son iguales.
Ejemplos:

(a) $\rho : G \Rightarrow GL(V)$, dim$(V)$=1 y $\rho(\sigma) = 1$ para todo $\sigma \in G$. Esta representación será llamada representación *trivial*.

(b) Sea G un grupo con $|G| = n$ y sea V un espacio vectorial de dimensión n con base $\{e_i\}_{i \in G}$. Definimos para $j \in G$, $\rho(j) := \rho_j$, donde $\rho_j(e_i) = e_{ij}$. Esta representación será llamada *representación regular*. Denotamos por r_G al caracter de la representación regular. Verifica, $r_G(\sigma) = 0$, para $\sigma \neq 1$ y $r_G(1) = n = |G|$. Además,

$$r_G = \sum_\chi \chi(1)\chi$$

donde la suma recorre todos los caracteres irreducibles.

Para dos caracteres φ y ψ de G definimos

$$(\varphi, \psi) = \frac{1}{g} \sum_{\sigma \in G} \varphi(\sigma)\overline{\psi}(\sigma), \qquad g = |G|$$

donde $\overline{\psi}$ denota la conjugación compleja de ψ. Para χ y χ' irreducibles se verifica

$$(\chi, \chi') = \begin{cases} 1, & \text{si } \chi = \chi' \\ 0, & \text{si } \chi \neq \chi' \end{cases}$$

Esta aplicación define un producto escalar en el espacio de los caracteres de G, donde los irreducibles forman una base ortonormal. Mas aun, sea

$$V = V_1 \oplus \ldots \oplus V_r$$

una descomposición de V en representaciones irreducibles, con caracter χ. Si W es una representación irreducible con caracter χ', el número de V_i isomorfos a W está dado por (χ, χ'), pues

$$(\chi, \chi') = (\chi_1, \chi') + \ldots + (\chi_r, \chi').$$

Sea $H \subset G$. A cada representación $\rho : G \to GL(V)$ de G le podemos asociar una representación que será la restricción de ρ a H. Esta función será denotada por Res_H^G.
En la otra dirección, nos gustaría poder aumentar a G representaciones de H. Sea W una subrepresentación de Res_H^G que denotaremos por $\theta : H \to GL(W)$.
Para cada $s \in G$ denotemos por sH al conjunto de los productos st, con $t \in H$ y diremos que sH es una *clase lateral izquierda* de H conteniendo a s. El conjunto de las clases laterales izquierdas de H será denotado por G/H. Si escogemos un elemento de cada clase lateral de H, obtenemos un subconjunto R de G llamado *sistema de representantes* de G/H.
Si σ es una clase lateral, definimos el subespacio W_σ de V como $\rho_s W$ para cualquier $s \in \sigma$. La suma de ellas $\sum_{\sigma \in G/H} W_\sigma$ es una subrepresentación de V.
Diremos que una representación $\rho : G \to Gl(V)$ es *inducida* por la representación $\theta : H \to GL(W)$ si $V = \bigoplus_{\sigma \in G/H} W_\sigma$. En ese caso denotamos la denotamos por Ind_H^G.
Con respecto al caracter. Denotemos por χ_θ al caracter de la representación θ. Entonces

$$Ind_H^G \chi(g) = \frac{1}{|H|} \sum_{s \in G,\ s^{-1}us \in H} \chi_\theta(s^{-1}us)$$

A continuación , daremos dos teoremas de gran importancia en teoría de funciones L. Para las demostraciones ver [7].

Teorema 2.2. *(Reciprocidad de Frobenius) Si ψ es una función de clases sobre H y φ es una función de clases sobre G, entonces*

$$(\psi, Res_\varphi)_H = (Ind_\psi, \varphi)_G.$$

Teorema 2.3. *(Teorema de Brauer) Todo caracter χ de G es una combinación lineal con coeficientes enteros de caracteres $\widetilde{\chi}_i$ inducidos de caracteres χ_i de grado 1 asociados a subgrupos H_i de G.*

3. Funciones L - de Artin

En este capítulo, definiremos la función L - de Artin y mostraremos algunas de sus propiedades esenciales.

Sea L/K una extensión de Galois de cuerpos de números con grupo de Galois $\mathcal{G}$ y sea (ρ, V) una representación de $\mathcal{G}$. Definimos *la función L - de Artin* como

$$L(s, \chi, L/K) = \prod_{\mathfrak{p}} \big(\det(\mathrm{Id} - N(\mathfrak{p})^{-s} \rho(\varphi_{\mathfrak{b}/\mathfrak{p}}); V^{I_{\mathfrak{b}}}) \big)^{-1}, \tag{3.3}$$

donde el producto es tomado sobre todos los primos de K, $\mathfrak{b}$ es un ideal primo sobre $\mathfrak{p}$ y $V^{I_{\mathfrak{b}}}$ es el subespacio de invariantes en V bajo el grupo de inercia $I_{\mathfrak{b}}$.

Notar que diferentes elecciones de $\mathfrak{b}'$ sobre $\mathfrak{p}$ dan homomorfismos conjugados a $\rho(\varphi_{\mathfrak{b}/\mathfrak{p}})$, lo cual no cambia el determinante.

Si $\lambda_{1,\mathfrak{p}}, \ldots, \lambda_{m_{\mathfrak{p}},\mathfrak{p}}$ son los valores propios de $\rho(\varphi_{\mathfrak{b}/\mathfrak{p}})$ actuando sobre $V^{I_{\mathfrak{b}}}$, entonces $m_{\mathfrak{p}} \leq n = \chi(1)$ y

$$\det(\mathrm{Id} - N(\mathfrak{p})^{-s} \rho(\varphi_{\mathfrak{b}/\mathfrak{p}}); V^{I_{\mathfrak{b}}}) = \prod_{i=1}^{m_p} \big(1 - N(\mathfrak{p})^{-s} \lambda_{i,\mathfrak{p}}\big) = \prod_{i=1}^{n} \big(1 - N(\mathfrak{p})^{-s} \lambda_{i,\mathfrak{p}}\big),$$

donde ponemos $\lambda_{i,\mathfrak{p}} = 0$ si $n \geq i > m_{\mathfrak{p}}$. Se tiene entonces,

$$\begin{aligned}
\log \det(\mathrm{Id} - N(\mathfrak{p})^{-s} \rho(\varphi_{\mathfrak{b}/\mathfrak{p}}); V^{I_{\mathfrak{b}}}) &= \log \prod_{i=1}^{n} \big(1 - N(\mathfrak{p})^{-s} \lambda_{i,\mathfrak{p}}; V^{I_{\mathfrak{b}}}\big) \\
&= \sum_{i=1}^{n} \log(\mathrm{Id} - N(\mathfrak{p})^{-s} \rho(\varphi_{\mathfrak{b}/\mathfrak{p}}); V^{I_{\mathfrak{b}}}) \\
&= \sum_{i=1}^{n} \sum_{l=1}^{\infty} \frac{\lambda_{i,\mathfrak{p}}^{l}}{l} N(\mathfrak{p})^{-sl} \\
&= \sum_{l=1}^{\infty} \frac{\chi(\varphi_{\mathfrak{b}/\mathfrak{p}}^{l})}{l} N(\mathfrak{p})^{-sl},
\end{aligned}$$

lo cual implica

$$\log(L(s, \chi, L/K)) = -\sum_{\mathfrak{p}} \sum_{l=1}^{\infty} \frac{\chi(\varphi_{\mathfrak{b}/\mathfrak{p}}^{l})}{l} N(\mathfrak{p})^{-sl}. \tag{3.4}$$

Notar que la función L - de Artin es una función analítica en el semiplano $\mathrm{Re}(s) > 1$ y converge absolutamente y uniformemente en el semiplano $\mathrm{Re}(s) > 1 + \delta$, para todo $\delta > 0$. Enunciaremos a continuación algunas de las propiedades mas importantes de las funciones L - de Artin.

Teorema 3.1. *Si $\chi = \mathbf{1}$ es el caracter de la representación trivial, entonces*

$$L(s, \mathbf{1}, L/K) = \zeta_K(s).$$

Demostración. Sale de la definición. □

Teorema 3.2. *Si χ, χ' son dos caracteres de $\mathcal{G}$, entonces*

$$L(s, \chi + \chi', L/K) = L(s, \chi, L/K)L(s, \chi', L/K).$$

Demostración. Sale de (3.4). □

Teorema 3.3. *Supongamos que tenemos un cuerpo de cuerpos de números $K \subset M \subset L$ con $Gal(L/K) = G$ y $Gal(L/M) = H$. Si χ es una caracter de H, entonces*

$$L(s, \chi, L/M) = L(s, , Ind_H^G \chi, L/K).$$

Demostración. Ver [2], pág. 522. □

Teorema 3.4. *Para una extensión de cuerpos de números L'/K, con $L' \supseteq L \supseteq K$ y χ un caracter de $Gal(L/M)$ se tiene*

$$L(s, \chi, L'/K) = L(s, \chi, L/K).$$

Demostración. Sea $\mathfrak{b}'|\mathfrak{b}|\mathfrak{p}$ primos de $L'|L|K$. La proyección $Gal(L'/K) \to Gal(L/K)$ induce homomorfismos sobreyectivos

$$G_{\mathfrak{b}'} \to G_{\mathfrak{b}}, \qquad I_{\mathfrak{b}'} \to I_{\mathfrak{b}}, \qquad G_{\mathfrak{b}'}/I_{\mathfrak{b}'} \to G_{\mathfrak{b}}/I_{\mathfrak{b}}.$$

La última función lleva el automorfismo de Frobenius $\varphi_{\mathfrak{b}/\mathfrak{p}}$ en $\varphi_{\mathfrak{b}'/\mathfrak{p}}$, ya que son conjugados pues $\mathfrak{b}$ también es primo en L', luego $\mathfrak{b}$ y $\mathfrak{b}'$ son primos en L' sobre $\mathfrak{p}$ y dan el mismo Frobenius. □

Teorema 3.5. *Si L/K es una extensión de cuerpos de números, entonces*

$$\zeta_L(s) = \zeta_K(s) \prod_{\chi \neq 1} L(s, \chi, L/K)^{\chi(1)},$$

donde χ recorre los caracteres no triviales de $Gal(L/K)$.

Demostración. Como $Ind_{\{1\}}^{\mathcal{G}} \chi_0 = r_{\mathcal{G}}$, se tiene que

$$\zeta_L(s) = L(L/L, \chi_0, s) = L(L/K, Ind_{\{1\}}^{\mathcal{G}} \chi_0, s),$$

pero $r_{\mathcal{G}} = \sum_{\chi} \chi(1)\chi$, luego

$$\begin{aligned} \zeta_L(s) &= L(L/K, \sum_{\chi} \chi(1)\chi, s) \\ &= \zeta_K(s) \prod_{\chi \neq 1} L(s, \chi, L/K)^{\chi(1)} \end{aligned}$$

□

Otra propiedad analítica, que no analizaremos en detalle, pero que no podemos dejar de mencionar, es la existencia de una ecuación funcional para la función L - de Artin. Se define la función L - extendida como

$$\Lambda(s, \chi, L/K) = c(\chi, L/K)^{s/2} L_{\infty}(s, \chi, L/K) L(s, \chi, L/K),$$

donde $c(\chi, L/K)$ es una constante que depende de dos invariantes de la extensión (el discrimimante y el conductor de Artin) y $L_{\infty}(s, \chi, L/K)$ es un producto de factores gama. Esta función tiene una continuación meromorfa a todo el plano satisfaciendo la ecuación funcional

$$\Lambda(s, \chi, L/K) = \omega_{\chi} \Lambda(1 - s, \overline{\chi}, L/K),$$

con $\omega \in \mathbb{C}$ de valor absoluto 1. Para ver más detalles de las propiedades analíticas de las funciones L ver [2], pág. 540 y [10].

4. Problemas abiertos

4.1. La Conjetura de Artin

Una de las más fundamentales conjeturas en teoría algebráica de números es la siguiente:

Conjetura de Artin: Sea L/K una extensión de Galois finita con grupo de Galois $\mathcal{G}$. Para cualquier caracter irreducible χ de $\mathcal{G}$ la función L - de Artin $L(s, \chi, L/K)$ tiene una continuación analítica para todo s, excepto posiblemente por un polo en $s = 1$ de orden igual a la multiplicidad de la representación trivial.

En el caso que χ es 1- dimensional y L/K abeliana, Artin relacionó funciones L - de Artin con L - funciones de Hecke, de las cuales sabemos tienen continuación analítica (ley de reciprocidad).

Teorema 4.1. *Sea L/K una extensión abeliana y $\chi \neq 1$ un caracter irreducible de $\mathcal{G}$. Entonces existe un caracter de Hecke π_χ tal que*

$$L(s, \chi, L/K) = L(s, \pi_\chi). \tag{4.5}$$

Artin demostró este teorema por medio de la teoría de cuerpos de clases y, en particular, el teorema de densidad de Chebotarev, el cual afirma lo siguiente. Sea $C \subset \mathcal{G}$ un conjunto cerrado bajo conjugación. Denotemos por $\pi_C(x)$ el número de ideales primos $\mathfrak{p}$ de K no ramificados en L, para los cuales $\sigma_\mathfrak{p} \subset C$ y los cuales tienen norma $N(\mathfrak{p}) \leq x$ en K. El teorema de densidad de Chebotarev afirma

$$\pi_C(x) \sim \frac{\sharp C}{\sharp G}\pi(x). \tag{4.6}$$

Este teorema se puede considerar como un análogo del teorema de los números primos en progresiones aritméticas.

Por el teorema de Brauer, todo caracter χ puede ser escrito como

$$\chi = \sum_i n_i \mathrm{Ind}_{H_i}^{\mathcal{G}} \psi_i$$

donde los H_i son nilpotentes, los ψ_i son 1-dimensionales y los n_i enteros, luego

$$\begin{aligned} L(s, \chi, L/K) &= \prod_i L(s, \psi_i, L/L^{H_i})^{n_i} \\ &= \prod_i L(s, \pi_{\psi_i})^{n_i} \qquad \text{(por (4.5))} \end{aligned}$$

lo cual implica que cualquier función L - de Artin tiene una continuación meromorfa a todo el plano complejo (ver [6]).

El teorema de Brauer también implica la conjetura de Artin si $\mathcal{G}$ es nilpotente o supersoluble, pues en ese caso toda representación de $\mathcal{G}$ es inducida por una representación 1-dimensional de un subgrupo de $\mathcal{G}$ (Ver [7], pág. 66).

La conjetura de Artin fue probada por A.Weil cuando K es un cuerpo de funciones.

En el caso de caracteres 2-dimensionales, el problema ha sido dividido según la imagen de la representación, por ejemplo cíclica, diedral, tetraedral, octaedral, o icosaedral. Para los casos cíclico y diedral, se conocen resultados de Hecke. Para el caso octaedral,tenemos el trabajo de J. Tunnel [8].

Khare [3] probó que la conjetura de Serre implica la conjetura de Artin. Otro importante teorema es el de Langlands-Tunnell: si χ es 2-dimensional con imagen soluble, la conjetura de Artin es válida y en ese caso $L(s, \chi, L/K)$ es igual a la función L de una representacion automorfa de $GL(\mathbb{A}_K)$, donde $\mathbb{A}_K$ es el anillo de adeles de K.

4.2. La conjetura de Selberg

En 1989, Selberg [5] definió una clase general de series de Dirichlet que poseen un producto de Euler, continuación analítica y una ecuación funcional del tipo Riemann (más algunas condiciones) y formuló algunas conjeturas fundamentales concernientes a ellas. Esta clase de Selberg se convirtió mientras tanto en un objeto importante de investigación pero todavía no se ha entendido del todo. Se conjeturó que la clase de Selberg consiste de las funciones L automorfas y que el análogo de la Hipótesis de Riemann se cumple para todos estos elementos.

La clase de Selberg $\mathcal{S}$ es una familia de funciones $\mathcal{L}(s)$ de funciones de variable compleja s satisfaciendo las siguientes propiedades:

(a) (Serie de Dirichlet) Para $\mathrm{Re}(s) > 1$,

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

donde $a_1 = 1$ y escribimos $a_n(\mathcal{L}) = a_n$ para los coeficientes de la serie de Dirichlet.

(b) (Continuación analítica) $\mathcal{L}(s)$ se extiende a una función meromorfa y existe un entero $m \geq 0$ tal que $(s-1)^m \mathcal{L}(s)$ es una función entera de orden finito.

(d) (Ecuación funcional) Existen números $Q > 0, \alpha_i > 0, \mathrm{Re}(r_i) \geq 0$ tal que la función

$$\Lambda(s) = Q^s \prod_{i=1}^{d} \Gamma(\alpha_i s + r_i) \mathcal{L}(s)$$

satisface

$$\Lambda(s) = \omega \overline{\Lambda(1-s)}$$

para algún $\omega \in \mathbb{C}$ con $|\omega| = 1$.

(e) (Producto de Euler) $\mathcal{L}(s)$ satisface

$$\mathcal{L}(s) = \prod_{p\, primo} \mathcal{L}_p(s)$$

donde

$$\mathcal{L}_p(s) = \exp\left(\sum_{k=1}^{\infty} \frac{b_{p^k}}{p^{ks}} \right),$$

donde $b_{p^k} = O(p^{k\theta})$, para algún $\theta < 1/2$.

(f) (Hipótesis de Ramanujan) $a_n = O(n^{\varepsilon})$, para todo $\varepsilon > 0$.

Ejemplos conocidos de elementos en $\mathcal{S}$ son la función zeta de Riemann, las funciones L automorfas y las L - series de Dirichlet. Esta clase es cerrada bajo multiplicación, luego tiene sentido introducir la noción de elementos primitivos. Diremos entonces que $\mathcal{L} \in \mathcal{S}$ es primitiva si $\mathcal{L} = \mathcal{L}_1\mathcal{L}_2$ implica $\mathcal{L} = \mathcal{L}_1$ o $\mathcal{L} = \mathcal{L}_2$. Se probó que la factorización en elementos primitivos es única.
Selberg conjeturó:

Conjetura A: Para toda $\mathcal{L} \in \mathcal{S}$, existe un entero positivo $n_{\mathcal{L}}$ tal que

$$\sum_{p \leq x} \frac{|a_{\mathcal{L}}(p)|^2}{p} = n_{\mathcal{L}} \log\log x + O(1)$$

donde $n_{\mathcal{L}}$ depende de la factorización de $\mathcal{L}$.

Conjetura B: Para funciones primitivas $\mathcal{L}_1$ y $\mathcal{L}_2$ se tiene

$$\sum_{p \leq x} \frac{a_{\mathcal{L}_1}(p)\overline{a_{\mathcal{L}_2}(p)}}{p} = \begin{cases} \log\log x + O(1), & \text{si } \mathcal{L}_1 = \mathcal{L}_2 \\ O(1), & \text{en otro caso} \end{cases}$$

De alguna forma, las funciones primitivas forman un sistema ortogonal. Se puede probar que la Conjetura B implica la Conjetura A.

M.R. Murty [5] probó lo siguiente:

Teorema 4.2. *La Conjetura B implica la conjetura de Artin.*

Demostración. Podemos suponer $K = \mathbb{Q}$. Entonces tenemos

$$L(s, \chi, L/\mathbb{Q}) = \prod_i L(s, \phi_i, L/\mathbb{Q})^{m_i},$$

donde ϕ_i son todas las representaciones irreducibles m_i-dimensionales de $Gal(L/\mathbb{Q})$. Para probar la conjetura de Artin para $L(s, \chi, L/\mathbb{Q})$, basta probar que $L(s, \phi_i, L/\mathbb{Q})$ es entera para cada ϕ_i.

Usando las propiedades básicas de las funciones L - de Artin y el teorema de Brauer, se puede probar que para cada ϕ irreducible m-dimensional

$$L(s, \phi) = L(s, \phi, L/\mathbb{Q}) = \prod_j^m F_j(s)^{e_j},$$

donde F_j son funciones primitivas en $\mathcal{S}$ y e_j enteros. Comparando los coeficientes de Dirichlet en ambos lados y aplicando la conjetura B, por el teorema de densidad de Chebotarev (4.6)

sobre estos coeficientes se puede probar que

$$\sum_{j=1}^{m} e_j^2 = 1,$$

lo que implica $m = 1$ y $e_j = \pm 1$. Luego $L(s, \phi) = F(s)$ o $1/F(s)$, donde $F(s)$ es primitiva y analítica en todas partes excepto posiblemente en $s = 1$. Como $L(s, \phi)$ tiene un cero trivial, el último caso no es posible, luego se puede concluir que $L(s, \phi) = F(s)$ es entera y primitiva. □

4.3. La conjetura de Langlands

El programa de Langlands predice una correspondencia entre dos tipos de objetos. Por un lado tenemos ciertos objetos artiméticos y por otro lado representaciones automorfas. Ambos objetos producen funciones L y la correspondencia estaría definida por la igualdad de esas funciones. Un caso especial es la conjetura de Taniyama-Shimura. De esta forma, el programa de Langlands busca unificar teoría de representaciones, teoría de números y geometría aritmética algebraica.

Conjetura de reciprocidad de Langlands: Sea L/K una extensión finita de Galois con grupo $\mathcal{G}$ y sea χ un caracter m- dimensional de $\mathcal{G}$. Entonces existe una representación cuspidal automorfa π_χ de $\mathrm{GL}_m(\mathbb{A}_K)$ tal que

$$L(s, \chi, L/K) = L(s, \pi_\chi).$$

Daremos una breve descripción de las funciones L asociadas a representaciones automorfas. Para más detalles ver [5] y [4].

Sea K un cuerpo de números. Para cada valuación v sobre K, sea K_v la completación y $\mathcal{O}_v$ su anillo de enteros. Consideremos los elementos $\alpha = \prod_v \alpha_v$, donde α_v pertenece a $\mathcal{O}_v$ para finitos v. Estos elementos serán llamados adeles. Este conjunto de elementos es un anillo y será llamado anillo de adeles $\mathbb{A}_K$ de K. [1] Notar que K puede ser incrustado en $\mathbb{A}_K$ con la función $\alpha \mapsto (\alpha, \alpha, \ldots)$.

Para $m \geq 1$, sea $GL_m(\mathbb{A}_K)$ el grupo de matrices de $m \times m$ sobre $\mathbb{A}_K$ cuyo determinante es una unidad en $\mathbb{A}_K$. Para un caracter fijo ϕ del grupo $K^* \setminus GL_1(\mathbb{A}_K)$, sea $L^2 := L^2(GL_m(K) \setminus GL_m(\mathbb{A}_K), \phi)$ el espacio de funciones medibles f sobre $GL_m(K) \setminus GL_m(\mathbb{A}_K)$ verificando algunas condiciones de integrabilidad.

[1] Este producto es en realidad un anillo topológico. No consideramos el producto de todos los K_v pues no tiene algunas propiedades de compacidad que se requieren.

La representación regular derecha R de $GL_m(K)$ sobre L^2 está dada por

$$(R(g)f)(\alpha) = f(\alpha g),$$

para cada $f \in L^2$ y $\alpha, g \in GL_m(\mathbb{A}_K)$. Una representación automorfa es un subcuociente de la representación regular derecha de $GL_m(\mathbb{A}_K)$ sobre L^2.

Se tiene que cada representación irreducible π puede factorizar como el producto tensorial

$$\pi = \otimes_v \pi_v,$$

donde π_v son representaciones irreducibles de $GL_m(\mathbb{Q}_v)$. Para ciertas valuaciones (no ramificadas), si A_v es una clase de conjugación asociada a π_v, definimos

$$L(s, \pi_v) = \det(1 - A_v N(\mathfrak{p})^{-s})^{-1}$$

donde $\mathfrak{p}$ es un primo de K asociado a v. En otro caso, definimos $L(s, \pi_v)$ como un producto de factores gamma.

Notar que la conjetura de Artin es un caso especial de la conjetura de reciprocidad de Langlands. Murty [5] también probó con respecto a esto:

Teorema 4.3. *La conjetura B de Selberg implica la conjetura de reciprocidad de Langlands para extensiones $K/\mathbb{Q}$ solubles.*

4.4. La conjetura de Taniyama-Shimura

En esta sección, daremos algunas ideas del contenido de esta conjetura, que nos dará una importante relación entre las funciones L - de Artin y la demostración del último teorema de Fermat.

En el siglo 16, Fermat afirmó que todas las soluciones enteras de la ecuación diofántica

$$X^n + Y^n = Z^n, \qquad \text{con } 3 \leq n \in \mathbb{N}$$

son triviales, i.e, $XYZ = 0$.

La conjetura de Taniyama-Shimura data del año 1955. Afirma que para cualquier curva elítptica definida sobre $\mathbb{Q}$, existe una forma modular tal que ambos objetos tienen la misma función L.

En 1975, Frey [1] observó que un contraejemplo para el último teorema de Fermat daría un contraejemplo para la conjetura de Taniyama-Shimura.

En 1995 Wiles, Taylor y otros [9] probaron una parte esencial de la conjetura de Taniyama-Shimura.

Ribet probó en 1989 que la conjetura de Taniyama-Shimura implica el último teorema de Fermat.

Lo que Ribet en realidad probó, es que la curva elíptica $y^2 = x(x - a^n)(x + b^n)$, done a y b son soluciones eventuales de la ecuación $a^n + b^n = c^n$ posee necesariamente propiedades contradictorias con la conjetura de Taniyama-Shimura, luego si ésta es verdadera, tal curva no puede existir.

4.5. Formas modulares

Denotamos por $SL_2(\mathbb{Z})$ al grupo modular

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ a, b, c, d \in \mathbb{Z}, \ ad - bc = 1 \right\}.$$

Si $\mathcal{H}$ denota el semi plano superior complejo, una función holomorfa $f : \mathcal{H} \to \mathbb{C}$ es una forma modular de peso k para $SL_2(\mathbb{Z})$ si

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \qquad \text{para todo } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

y f "holomorfa en el infinito". Esta última condición puede ser afirmada diciendo que f tiene una expansión de Fourier de la forma

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}.$$

Para cada número natural N, definimos el subgrupo $\Gamma_0(N)$ definido como el subgrupo de matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $SL_2(\mathbb{Z})$ tal que $c \equiv 0 \pmod{N}$.

Una forma modular de peso k sobre $\Gamma_0(N)$ es definida de manera análoga.

4.6. Curvas elípticas y sus funciones L.

Una curva elíptica sobre un cuerpo K es una curva cúbica no-singular $f(X, Y) = 0$ con un punto en el infinito. Si char$(K) \neq 2, 3$, puede ser escrita como

$$Y^2 = X^3 + aX + b, \qquad \text{with } a, b \in K.$$

Se define

$$E(K) = \{(x, y) \in K^2 : \ f(x, y) = 0\} \cup \infty.$$

Para cada primo p, sea N_p el número de soluciones de la congruencia

$$Y^2 \equiv X^3 + aX + b \qquad (\text{mod } p).$$

Si

$$a_p = p - N_p = p + 1 + \sharp E(\mathbb{F}_p),$$

definimos la función L de la curva elíptica como

$$L_E(s) = \prod_{p|\Delta} \left(1 - \frac{a_p}{p^s}\right)^{-1} \prod_{p\nmid\Delta} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}.$$

Este producto de Euler converge para $\text{Re}(s) > 3/2$ y en este semiplano podemos escribir

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

Esto define los a_n, los cuales coinciden con a_p cuando n es primo.

Por otro lado, consideremos formas modulares en $\Gamma_0(N)$ con ciertas propiedades con respecto a N y a primos p (llamadas *new form*). A tales f podemos asociarles funciones L definidas como

$$L_f(s) = \prod_{p|N} \left(1 - \frac{a_p}{p^s}\right)^{-1} \prod_{p\nmid N} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s+1-k}}\right).$$

La conjetura de Taniyama-Shimura (ahora conocida también como teorema de modularidad) probada por Wiles y Taylor afirma en realidad lo siguiente: *Para toda curva elíptica E, existe una forma modular (new form) f de peso 2 para algún subgrupo de congruencia $\Gamma_0(N)$ tal que $L_E(s) = L_f(s)$.*

Referencias

[1] G. Frey, *Links between elliptic curves and solutions of* $A - B = C$, J. Indian Math. Soc. **125** (1987), 117–145.

[2] J.Neukirch, *Algebraic number theory*, Springer-Verlag, Berlin, 1999.

[3] Chandrashekhar Khare, *Remarks on mod p forms of weight one*, International Mathematics Research Notices (1997), no. 3.

[4] M. Ram Murty, *A motivated introduction to the Langlands program*, Advances in Number Theory (1993), 33–76.

[5] ———, *Selberg's conjectures and Artin L - functions*, Bull. Amer. Math. Soc. **31** (1994).

[6] R. Murty, *On Artin L - functions*, Class field theory—its centenary and prospect (Tokyo, 1998), Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, pp. 13–29.

[7] J-P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1996.

[8] J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. Amer. Math. Soc. (N.S.) **5** (1981), 173–175.

[9] A. Wiles, *Modular elliptic curves and Fermat's, last theorem*, Ann. Math. **141** (1995), 443–551.

[10] M. Ram Murty y V. Kummar Murty, *Non-vanishing of L- functions and applications*, vol. 157, Birkhauser, 1997.