Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(184)693-715, junio-septiembre de 2023. doi: https://doi.org/10.18257/raccefyn.1914

Artículo original

La función zeta sobre superficies abstractas de Riemann: Un primer acercamiento

The zeta function on abstract Riemann surfaces: A first approach

Yamidt Bermudez-Tobón[1,*], Bilson Castro[2,4], Pedro Hernandez-Rizzo[3]

[1] Universidad del Valle, Cali, Colombia
[2] ICMAT, Madrid España
[3] Universidad de Antioquia, Medellín, Colombia
[4] Universidad Autónoma de Madrid, Madrid, España

Resumen

El principal objetivo de este artículo es estudiar una de las funciones análogas a la función zeta. Precisamente, presentamos y probamos algunas de las propiedades de la función zeta asociada a una superficie abstracta de Riemann con cuerpo de constantes finito. El resultado principal, será el de establecer la equivalencia entre la hipótesis de Riemann en este contexto con la llamada cota de Hasse-Weil para el número de puntos racionales sobre la mencionada superficie (ver Teorema 6). Este artículo de caracter divulgativo presenta de forma ordenada y rigurosa, centrándose en los resultados del área sin contribuciones originales, los distintos conceptos y resultados fundamentales de la teoría a través de una presentación amena y de una adecuada bibliografía. A modo de conclusión se ilustra, de manera informal, como establecer la conjetura de Birch–Swinnerton-Dyer, uno de los llamados *Problemas del Milenio* (**Wiles**, 2006).

Palabras clave: Hipótesis de Riemann; Riemann-Roch; curva algebraica; función zeta; cota de Hasse-Weil

Abstract

The aim of this paper is to study one of the analogous functions to the zeta function. Precisely, we present and prove properties of the zeta function associated to an abstract Riemann surface with with a finite field of constants. The main result will be to establish the equivalence between the Riemann hypothesis in this context with the so-called Hasse-Weil bound for the number of rational points on the mentioned surface (see Theorem 6). This expository paper presents in an orderly and rigorous way, focusing on the results of the area without original contributions, the different concepts and fundamental results of the theory through a pleasant presentation and an adequate bibliography. By way of conclusion it is illustrated, in an informal way, how to establish the Birch–Swinnerton conjecture, one of the so-called ”Millennium Problems”). (**Wiles**, 2006)

Keywords: Riemann hypothesis; Riemann-Roch; algebraic curve; Zeta function; Hasse–Wei bound.

Citación: Bermudez-Tobón Y, Castro B, Hernandez-Rizzo P. La función zeta sobre superficies abstractas de Riemann: Un primer acercamiento. Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales. 47(184)693-715, junio-septiembre de 2023. doi: https://doi.org/10.18257/raccefyn.1914

Editor: Francisco José Marcellán Español

***Correspondencia:**
Yamidt Bermudez Tobon;
yamidt.bermudez@correounivalle.edu.co

Recibido: 2 de mayo de 2023
Aceptado: 27 de julio de 2023
Publicado en línea: 8 de septiembre de 2023

Este artículo está bajo una licencia de Creative Commons Reconocimiento-NoComercial-Compartir Igual 4.0 Internacional

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(184)693-715, junio-septiembre de 2023. doi: https://doi.org/10.18257/raccefyn.1914

Introducción

En su único artículo relacionado con la teoría de números, *Ueber die Anzahl der Primzahlem unter einer gegebenen Grosse* (en traducción propia, *sobre la cantidad de números primos menores que una magnitud dada*) Riemann presenta y desarrolla las principales propiedades de la que hoy es conocida como la *función zeta de Riemann*. Esta se define para cada número complejo s, con $\mathrm{Re}(s) > 1$, por $\xi(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Él afirmó, sin demostración, que la extensión de esta a todos los números complejos poseía sus ceros no-triviales sobre la recta $\mathrm{Re}(s) = 1/2$ (ya que los ceros triviales de dicha extensión son los enteros pares no negativos). Desde entonces esta afirmación permanece sin demostración o ejemplo que la refute, conocida como la *hipótesis de Riemann*.

El origen de la hipótesis no podría ser más "místico": comprender la distribución de los números primos. Estos últimos hacen parte de la naturaleza propia de las matemáticas, la física y el universo. Esta secuencia de números está presente en diversos fenómenos de las matemáticas y permea teorías, por mencionar algunas, como la variable compleja, la teoría de números, los sistemas dinámicos, la teoría de grafos, la geometría algebraica y la criptografía. En todas estas áreas, hace presencia o bien la función zeta de Riemann o bien sus generalizaciones o funciones análogas. Y por si fuera poco, un sinnúmero de aplicaciones en física e ingeniería tienen asidero en ciertas funciones zeta y funciones zeta locales. Por mencionar algunas, la comprensión de la teoría de cuerdas, fenómenos relacionados a la cuantización de las fuerzas fundamentales (**Sierra**, 2019) (**Castro** & **Maecha**, 2004), Neuroingeniería (**Domenica** & **Vincent**, 2009), la seguridad informática. En lo referente a esto último, siendo un poco mas concretos, podemos de manera corta precisar lo siguiente: la base de toda la criptografía moderna radica en la esporádica aparición de los números primos. Todos los protocolos, algoritmos y normas criptográficas parten de la idea de que es imposible prever cuándo surgirá el siguiente número primo. De este modo, un atacante debe probar todas las posibles combinaciones para intentar entrar en un sistema. Actualmente, debido a la fortaleza de estos algoritmos y al poder de los ordenadores, un atacante tardaría una media de entre 20 y 30 años en intentar forzarlos. Sin embargo, si se demostrara la veracidad de la hipótesis de Riemann, el trabajo del atacante se simplificaría enormemente (**Koblitz**, 1994).

El principal objetivo de este artículo es estudiar una de las funciones análogas a la función zeta. Precisamente, presentamos y probamos algunas de las propiedades de la función zeta asociada a una superficie abstracta de Riemann definida sobre un cuerpo finito. El resultado principal, es establecer la equivalencia entre la hipótesis de Riemann en este contexto con la llamada cota de Hasse-Weil para el número de puntos racionales sobre la mencionada superficie. Este resultado no solo permitió establecer una diferencia significativa con la conjetura en el caso más conocido de funciones zeta sobre los números complejos, sino, que, por el contrario, permitió dar una prueba de lo que hoy es conocido como teorema de Hasse–Weil (**Weil**, 1979), (**Weil**, 1948). Un objetivo secundario, pero no menos importante, es el de provisionar la incipiente literatura en español que existe sobre temas relacionados con la geometría aritmética y, en consecuencia, este artículo puede ser entendido como una invitación al estudio de esta importante área de las matemáticas, en donde se enmarcan problemáticas como las aquí estudiadas.

Así como la función original de Riemann y su hipótesis han generado impacto y un desarrollo extraordinario en las matemáticas, esta versión análoga jugó un papel determinante en el siglo XX, en la década de los 40, en el área de la geometría aritmética. No solo por su demostración en sí, sino también, por el valor histórico del contexto dramático en que se gestaron las ideas que llevaron a la demostración de esta equivalencia. Para mayores detalles ver (**Hindry**, 2012) y las referencias ahí citadas.

En su tesis doctoral, Emil Artin fue el pionero en considerar la función zeta de Dedekind, un análogo para las funciones zeta de Riemann definidas sobre cuerpos de números al-

gebraicos. No obstante, la versión de Artin fue definida para extensiones de cuerpos de funciones algebraicas sobre un cuerpo finito. A pesar de que la hipótesis de Riemann no fue el tema principal de su tesis, si fue el primero en mencionar como un hecho curioso, que la función zeta por él definida, para ciertos polinomios en una variable con coeficientes en el cuerpo de funciones, los ceros no-triviales de esta tenían parte real $\frac{1}{2}$. Estas ideas fueron consolidadas en los desarrollos posteriores de Deuring, Hasse y Schmidt y alcanzan su esplendor con la demostración de la versión de la hipótesis en este contexto para curvas elípticas por Hasse.

Este tipo de analogías, entre afirmaciones válidas para cuerpos de números algebraicos y cuerpos de funciones algebraicas, no eran extrañas en la época. En efecto, Kronecker fue el pionero en este tipo de tratamientos, cautivando a un gran número de matemáticos, entre ellos Weil. Es André Weil, que con su visión profunda e innovadora, transforma los esbozos previos en una obra monumental. En efecto, inicia con la demostración del análogo de la hipótesis para curvas, proponiendo su extensión para variedades de dimensión superior que durante mucho tiempo fueron conocidas como las conjeturas de Weil y luego como los teoremas de Deligne-Grothendieck, siendo el motor propulsor de un desarrollo estupendo de la geometría algebraica. Y no fue solo eso, hoy por hoy la cota de Hasse–Weil juega un papel determinante en las aplicaciones relacionadas con el desarrollo de la teoría de códigos, tecnologías de la información y en la construcción de curvas "con muchos puntos racionales" conocidas como curvas maximales. Para conocer mayores detalles de esta fantástica parte de la historia de las matemáticas recomendamos (**Roquette**, 2018) y para estudiar más sobre los alcances teóricos de lo iniciado por Weil recomendamos (**Milne**, 2017) y las referencias allí citadas.

Para orientar al lector, proporcionamos algunos detalles sobre el contenido de las secciones. La segunda y tercera sección son reservadas a la presentación de las superficies abstractas de Riemann y a una revisión rápida de los principales resultados relacionados con ellas, como por ejemplo, el teorema de Riemann–Roch. La cuarta sección es dedicada al estudio de propiedades y resultados principales de la función zeta definida sobre una superficie abstracta de Riemann con cuerpo de constantes finito. La quinta sección es dedicada a los preliminares y a la demostración del resultado principal de este artículo, esto es, la equivalencia entre la hipótesis de Riemann en este contexto y la cota de Hasse–Weil. La sexta y última sección, la que esperamos sea una invitación a continuar con el estudio de estos fascinantes temas, ilustra de manera informal como se puede establecer con lo aprendido en las secciones previas. Por un lado, la conjetura de Birch–Swinnerton-Dyer, uno de los llamados *Problemas del Milenio* (**Wiles**, 2006) y, por otro lado, el teorema de Deligne-Grothendieck.

Superficies abstractas de Riemann: Una revisión rápida

En esta sección se presentan las *superficies abstractas de Riemann*, como los objetos donde tiene asidero la teoría de funciones zeta propuesta por Weil. Estas superficies se encuentran en estrecha relación con la teoría de cuerpos de funciones algebraicas en una variable. Esta relación, que también es destacada en esta sección, será crucial para los objetivos de este artículo. Para mayores detalles de lo aquí expuesto, recomendamos (**Roquette**, 2018), (**Lorenzini**, 1996, Cap V).

Definición 1. *Sea K un cuerpo. Una valuación de K con grupo de valores $\mathbb{Z}$ es una función sobreyectiva $\nu : K \to \mathbb{Z} \cup \{\infty\}$ que satisface:*

- $\nu(ab) = \nu(a) + \nu(b)$, *para cada* $a, b \in K^*$.
- $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$, *para cada* $a, b \in K^*$.
- $\nu(0) = \infty$.

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(184)693-715, junio-septiembre de 2023. doi: https://doi.org/10.18257/raccefyn.1914

Si existe K_0 un subcuerpo de K tal que $\nu(c)=0$, para cada $c\in K_0^*$, entonces se dice ν es una *valuación con cuerpo de constantes* K_0.

Ejemplo 1. Sea z un elemento trascendente sobre $\mathbb{C}$, $\mathbb{C}[z]$ el anillo de polinomios en la variable z y $\mathbb{C}(z)$ su cuerpo de fracciones. Para cualquier función racional $h=\frac{f}{g}\in\mathbb{C}(z)$, con $\text{mcd}(f,g)=1$ y un elemento $z_0\in\overline{\mathbb{C}}:=\mathbb{C}\cup\{\infty\}$, definimos $o(h,z_0)$ como el número entero asociado al orden del cero o polo de h en z_0, esto es, el menor entero m tal que $h=(z-z_0)^m\frac{f}{g}$, donde $f,g\in\mathbb{C}[z]$ y $f(z_0)\neq 0$, $g(z_0)\neq 0$. Así, se define la función sobreyectiva

$$\begin{array}{rcl} \nu_{z_0}:\mathbb{C}(z) & \longrightarrow & \mathbb{Z}\cup\{\infty\} \\ h & \mapsto & o(h,z_0) \end{array}$$

Es fácil verificar que ν_{z_0} es una valuación con grupo de valores $\mathbb{Z}$ y con cuerpo de constantes $\mathbb{C}$. Más aún, la recíproca también es cierta: Si $\nu:\mathbb{C}(z)\to\mathbb{Z}\cup\{\infty\}$ es una valuación con cuerpo de constantes $\mathbb{C}$, entonces existe $z_0\in\mathbb{C}$ tal que $\nu=\nu_{z_0}$. En efecto, se darán dos casos:

1. Sí $\nu(z)\geq 0$, entonces $\nu(h)\geq 0$ para todo $h\in\mathbb{C}[z]$. Por la sobreyectividad de ν, existe $h=\frac{f}{g}\in\mathbb{C}(z)$, no nulo, tal que $\nu(h)>0$. En consecuencia, $\nu(f)=\nu(g\cdot h)=\nu(g)+\nu(h)>0$. Por el Teorema Fundamental del álgebra (TFA), existen $a,z_1,\ldots,z_n\in\mathbb{C}$ tales que $f=a(z-z_1)\cdots(z-z_n)$, de donde al tomar su valuación $\nu(f)=\nu(z-z_1)+\cdots+\nu(z-z_n)>0$ y así, $\nu(z-z_0)>0$ para algún $z_0:=z_j$. Consecuentemente, $\nu(z-c)=0$ para cada $c\in\mathbb{C}$ y $c\neq z_0$. En efecto, $0=\nu(c-z_0)=\nu(z-z_0-(z-c))\geq\min\{\nu(z-z_0),\nu(z-c)\}$, por lo tanto $\nu(z-c)=0$, ya que $\nu(z-z_0)>0$.

   Nuevamente, como aplicación del TFA, cada $h\in\mathbb{C}(z)^*$ se escribe de modo único como $h=b\prod_{c\in\mathbb{C}}(z-c)^{m_c}$, donde $b\in\mathbb{C}^*$, $m_c\in\mathbb{Z}$ y $m_c=0$ para casi todo $c\in\mathbb{C}$. De aquí, se sigue que
   $$\nu(h)=\sum_{c\in\mathbb{C}}m_c\nu(z-c)=m_{z_0}\nu(z-z_0).$$

   En conclusión, $\nu(z-z_0)$ es un generador del grupo $\nu(\mathbb{C}(z)^*)=\mathbb{Z}$, que al ser $\nu(z-z_0)>0$, concluimos $\nu(z-z_0)=1$.

2. Sí $\nu(z)<0$. Entonces para $f=a_0+\cdots+a_nz^n\in\mathbb{C}[z]$, un polinomio no-nulo de grado n, se sigue $\nu(a_nz^n)=n\nu(z)<\nu(a_jz^j)$ con $j=0,\ldots,n-1$. Así, para f se tiene que, $\nu(f)=n\nu(z)=grado(f)\nu(z)$, *ya que el mínimo es alcanzado una única vez, (**Stichtenoth**, 2008, pag. 5)* .

   Ahora, para cada $h=\frac{f}{g}\in\mathbb{C}(z)^*$ con f y g de grados n y m, respectivamente, se tiene
   $$\nu(h)=\nu(f)-\nu(g)=(n-m)\nu(z).$$

   En particular, $\nu(z)$ es un generador del grupo $\nu(\mathbb{C}(z)^*)=\mathbb{Z}$ y ya que $\nu(z)<0$, concluimos que $\nu(z)=-1$, esto es, $\nu(\frac{1}{z})=1$ *(es decir,"la valuación con un único cero en el infinito").*

En realidad, el ejemplo anterior es la demostración, con las adaptaciones naturales, de la siguiente proposición.

Proposición 1. *Sea K un cuerpo algebraicamente cerrado, z un elemento trascendente sobre K y $K(z)$ el cuerpo de fracciones racionales en la variable z. Existe una biyección entre los puntos de la recta proyectiva $\mathbb{P}^1_K:=K\cup\infty$ y las valuaciones de $K(z)|K$ con grupo de valores $\mathbb{Z}$ y cuerpo de constantes K.*

La Proposición 1 motiva la siguiente definición.

Definición 2. *Sea $L|K$ una extensión de cuerpos. El conjunto*

$$S_{L|K} := \{\nu | \ \nu \text{ es valuación de } L|K \text{ con } \nu|_K = 0\},$$

es llamado superficie abstracta de Riemann de $L|K$.

A la luz de la Definición 2, la Proposición 1 afirma que $S_{K(z)|K}$ está en biyección con la recta proyectiva $\mathbb{P}^1_K$, si K es algebraicamente cerrado. En otras palabras, $S_{K(z)|K}$ define en realidad un objeto que podríamos considerar como cierta geometría. Esto no es casualidad, en realidad, las superficies abstractas de Riemann son relacionadas a objetos geométricos concretos. Para conocer más acerca esta relación y el estudio topológico de estos objetos, ver (**Chevalley**, 1951, Cap I) o (**Rosen**, 2010, Cap V). Un caso relevante es cuando K es un cuerpo algebraicamente cerrado. En este caso es posible demostrar que toda superficie abstracta de Riemann corresponde al modelo no-singular de una curva algebraica proyectiva y así, son ejemplos de superficies (conexas y compactas) de Riemann (ver, por ejemplo, (**Lorenzini**, 1996, p. 241)). En realidad, una de las principales consecuencias del teorema de Riemann-Roch, que será presentado en esta sección, es la de determinar morfismos $S_{L|K} \to \mathbb{P}^n_K$ y las condiciones para que este sea una inmersión. En este último caso, la imagen C de $S_{L|K}$ por este morfismo corresponde a una curva algebraica proyectiva suave. Desde un enfoque amplio, uno de los objetivos de este artículo es exhibir ciertas propiedades aritméticas de estos objetos y de como ellas están relacionadas a invariantes (topológicos-) geométricos y viceversa. En efecto, a continuación veremos lo que de alguna forma justifica el nombre de superficie de Riemann para estos objetos, ya que definen un recubrimiento ramificado de la recta proyectiva.

Considere $L|K$ un *cuerpo de funciones algebraicas en una variable sobre K*, esto es, L es una extensión de K, con grado de trascendencia igual a 1 sobre K. Para $h \in L \setminus K$, una trascendente sobre K, tenemos que $[L : K(h)]$ es finita y, en particular, algebraica. De esta forma, los cuerpos de funciones algebraicas son los análogos en la teoría de cuerpos de funciones a los cuerpos de números algebraicos en la teoría de números, entendiendo por estos últimos, aquellos cuerpos que son extensiones finitas de los números racionales.

Ahora, para cada $w \in S_{L|K}$, siendo w un homomorfismo de grupos sobre $K(h)^*$, se sigue que $w(K(h)^*)$ es un subgrupo no trivial de $\mathbb{Z}$, digamos $w(K(h)^*) = e\mathbb{Z}$ para algún entero $e > 0$. Definimos $e_w := e$ por el *índice de ramificación de w sobre $K(z)$*. De esta forma, es fácil verificar que $\frac{1}{e_w} w_{|_{K(h)}} \in S_{K(h)|K}$ y, por consiguiente, define la función:

$$\begin{array}{ccc} S_{L|K} & \longrightarrow & S_{K(h)|K} \\ w & \mapsto & \dfrac{1}{e_w} w_{|_{K(h)}}. \end{array}$$

Si K es algebraicamente cerrado, la Proposición 1 permite establecer la función

$$h : S_{L|K} \longrightarrow \mathbb{P}^1_K \tag{1}$$

donde para cada $w \in S_{L|K}$, $h(w)$ será el único valor asociado a w sobre la recta proyectiva $K \cup \{\infty\}$ el cual es llamado de *valor de h en w*. Así mismo, el entero $w(h)$ es llamado *orden de h en el punto w*. Por construcción, si $w(h) \geq 0$ entonces $h(w) \in K$ es la única constante tal que $w(h - h(w)) > 0$. Por el contrario, si $w(h) < 0$, entonces $h(w) = \infty$. En resumen, cada $h \in L \setminus K$ define una función $h : S_{L|K} \to \mathbb{P}^1_K$. En aras de la completitud, si $h \in K$, digamos $h = c \in K$, se define (naturalmente) la función constante por $h(w) = c$ para cada $w \in S_{L|K}$. En definitiva, cada $h \in L$ define la función $h : S_{L|K} \to \mathbb{P}^1_K$.

Ahora, para $w \in S_{L|K}$ el subanillo de L, denominado *anillo de valuación* de w, es $\mathcal{O}_w := \{h \in L | \ w(h) \geq 0\}$. Este es un anillo de valuación, local, con cuerpo de fracciones L y único ideal maximal $\mathfrak{m}_w := \{w \in L | \ w(h) > 0\}$. El cociente $K_w := \mathcal{O}_w/\mathfrak{m}_w$, define un cuerpo llamado el *cuerpo residual* de w. Ya que $K \subseteq \mathcal{O}_w$ y $K \cap \mathfrak{m}_w = \{0\}$, se sigue $K \subseteq K_w$.

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(184)693-715, junio-septiembre de 2023. doi: https://doi.org/10.18257/raccefyn.1914

Por otro lado, si $w \in S_{L|K}$ es una valuación *que extiende a* v, esto es, $v = w_{|_{K(h)}}$, se sigue que $\mathcal{O}_v \subseteq \mathcal{O}_w$ y $\mathfrak{m}_v = \mathfrak{m}_w \cap \mathcal{O}_v$. Esto permite identificar $K_v \subseteq K_w$ y, en consecuencia, definir $f_{w|v} := [K_w : K_v]$ el *índice de inercia de w sobre* v.

Un resultado importante y con aplicaciones destacables en la teoría de cuerpos de funciones en una variable es la siguiente desigualdad, que será presentada sin demostración. Para conocer demostraciones de este resultado sugerimos (**Samuel** & **Zariski**, 2013, Thm. 19, p. 55) o (**Stichtenoth**, 2008, Prop. 1.1.3 p.13). Para números algebraicos, el resultado análogo es la de una igualdad. Para conocer ejemplos donde la desigualdad es estricta, visite (**Samuel** & **Zariski**, 2013, §11, p. 62).

Teorema 1 (Desigualdad Fundamental)**.** *Sean $L|L_0$ una extensión de cuerpos finita (por ejemplo, sí $L_0 = K(h)$) y v una valuación de L_0 con grupo de valores $\mathbb{Z}$. Considere $w_1, \ldots, w_m$ todas las valuaciones de L que extienden a la valuación v. Denote por $e_1, \ldots, e_m$ y $f_1, \ldots, f_m$ sus índices de ramificación y de inercia, respectivamente. Entonces*

$$e_1 f_1 + \cdots + e_m f_m \leq [L : L_0]$$

En particular, $m \leq [L : L_0] < \infty$

Una consecuencia elemental de la desigualdad fundamental es que $[K_v : K] < \infty$, para cada $v \in S_{L|K}$. Esto permite definir el *grado* de una valuación, que denotamos por $\mathrm{d}(v) := [K_v : K]$. Ahora, diremos que v es un *punto racional* de $S_{L|K}$ si $\mathrm{d}(v) = 1$. El conjunto de puntos racionales, será denotado por $S^{\mathrm{rac}}_{L|K}$.

En general, el conjunto de puntos racionales de $S_{L|K}$ es un subconjunto propio. Por el contrario, si K es un cuerpo algebraicamente cerrado, entonces todos los puntos de la superficie son racionales, esto es, $S_{L|K} = S^{\mathrm{rac}}_{L|K}$.

Divisores y teorema de Riemann-Roch

Sea $L|K$ un cuerpo de funciones algebraicas en una variable sobre K. Definimos un *divisor* D de $S_{L|K}$ por la suma formal

$$D = \sum_{v \in S_{L|K}} n_v \cdot v$$

con $n_v \in \mathbb{Z}$ para cada $v \in S_{L|K}$, y llamado la *la multiplicidad de D en* v, donde $n_v = 0$ para casi todo v.

Se denotará por $\mathrm{Div}(L|K)$ el conjunto de divisores $S_{L|K}$. Claramente, a partir de la definición, admite una estructura de grupo abeliano libre, con suma "componente a componente": para $D = \sum n_v v$ y $E = \sum m_v v$ divisores $D + E := \sum (n_v + m_v)v$. Más aún, tenemos un homomorfismo de grupos abelianos:

$$\begin{array}{rccl} \partial : \mathrm{Div}(L|K) & \longrightarrow & \mathbb{Z} & \\ D & \mapsto & \partial(D) := \sum n_v \mathrm{d}(v). & \end{array} \tag{2}$$

En particular, si K es algebraicamente cerrado, entonces $\partial(D) = \sum n_v$.

El divisor $D = \sum n_v v$ es llamado *efectivo* si $n_v \geq 0$, para cada v. Esta propiedad del divisor D, que denotamos por $D \geq 0$, permite dotar de un orden parcial al grupo $\mathrm{Div}(L|K)$, como sigue: para $D = \sum n_v v$ y $E = \sum m_v v$ divisores, $D \leq E$ si y solo si $0 \leq E - D$.

En definitiva, $\mathrm{Div}(L|K)$ es un grupo abeliano libre y parcialmente ordenado.

Ejemplo 2. Sean $L|K$ un cuerpo de funciones algebraicas, $h \in L$ con K algebraicamente cerrado. Se sabe que h define una función $h : S_{L|K} \to \mathbb{P}^1_K$ y también define naturalmente dos divisores sobre $S_{L|K}$:

- **Divisor de ceros:** $(h)_0 = \sum_{h(\nu)=0} \nu(h)\nu$.
- **Divisor de polos:** $(h)_\infty = \sum_{h(\nu)=\infty} \nu(h)\nu$.

Generalizando lo anterior, considere $L|K$ un cuerpo de funciones algebraicas, con K no necesariamente algebraicamente cerrado, y $h \in L$ una función algebraica. Defina el *divisor principal* por:

$$(h) := \sum_{\nu \in S_{L|K}} \nu(h)\nu = (h)_0 - (h)_\infty,$$

donde $(h)_0 := \sum_{\nu(h)>0} \nu(h)\nu$ y $(h)_\infty := \sum_{\nu(h)<0} -\nu(h)\nu$ son llamados *divisores de ceros y polos* asociados a h, respectivamente. Observe que si $h \in K$ entonces $(h) = 0$, ya que $\nu(h) = 0$, para toda $\nu \in S_{L|K}$.

El Ejemplo 2 muestra una relación de los divisores y las funciones definidas sobre superficies de Riemann. En realidad, existen relaciones más concretas y con importantes consecuencias teóricas, como lo muestra la siguiente digresión.

Para $D = \sum n_\nu \nu$ un divisor de $L|K$, se define el K-espacio vectorial:

$$L(D) := \left\{ h \in L |\, \nu(h) \geq -n_\nu, \forall \nu \in S_{L|K} \right\}.$$

Grosso modo, a partir del Ejemplo 2, este espacio contiene a las funciones cuyas multiplicidades sobre sus ceros y polos son controladas por las multiplicidades de ν en D. Un problema importante de la teoría de superficies abstractas de Riemann es relacionado al cálculo de la dimensión de estos espacios. Una respuesta conclusiva la da el teorema de Riemann-Roch, que será presentado más adelante.

Ejemplo 3. Sea $L = K(z)$, con K algebraicamente cerrado. Considere $D = \sum n_c \nu_c + n_\infty \nu_\infty$, donde $c \in K$ está en correspondencia con el polinomio irreducible $f_c := (z-c)$ en $K[z]$ (ver Ejemplo 1). Denote por $d := \partial(D) = \sum n_P + n_\infty$. Así,

$$L(D) = \{ h \in K(z) |\, \nu_c(h) \geq -n_c,\, \nu_\infty(h) \geq -n_\infty \}.$$

Ahora, defina la función racional $f := \prod {f_c}^{-n_c} \in K(z)$, (determinada por D). Esta función, cumple $\nu_c(f) = -n_c$, para cada $c \in K$, y $\nu_\infty(f) = \sum n_c$, ya que los polos de $f(z)$ están en correspondencia con los ceros de $f(z^{-1})$. De aquí, es fácil ver que

$$\begin{aligned} L(D) &= \{ fh |\, h \in K(z),\, \nu_c(fh) \geq -n_c,\, \nu_\infty(fh) \geq -n_\infty \} \\ &= \{ fh |\, h \in K(z),\, \nu_c(h) \geq 0,\, \nu_\infty(h) \geq -d \} \\ &= \{ fh |\, h \in K[z],\, \nu_\infty(h) \geq -d \} \\ &= \{ fh |\, h \in K[z], grado(h) \leq d \}. \end{aligned}$$

Así, $L(D)$ es un K-espacio vectorial de dimensión $d+1$, siempre que $d \geq 0$, cuya base es definida por $\{f, xf, \ldots, x^d f\}$. En caso contrario, su dimensión será cero. En resumen,

$$\dim_K L(D) = \begin{cases} d+1 & \text{si } d \geq 0 \\ 0 & \text{si } d < 0. \end{cases} \tag{3}$$

Ahora para $h \in L \setminus K$, motivados por los ejemplos anteriores, surgen inmediatamente dos preguntas: ¿Son, en general, $(h)_0$ y $(h)_\infty$ no-nulos? y ¿por qué las sumas de $(h)_0$ y $(h)_\infty$ son finitas? Para responder a ellas, observemos que basta responderlas para $(h)_\infty$, ya que $(h^{-1})_\infty = (h)_0$. Ahora, a partir de los comentarios previos y posteriores en la construcción de la función h en (1), si $h \in L \setminus K$ es tal que $\nu(h) < 0$ para $\nu \in S_{L|K}$, tenemos que $\nu|_K = \nu_\infty$. En otras palabras, ν es una extensión de la valuación ν_∞ de $S_{K(h)|K}$. Consecuentemente, la primera pregunta se responde garantizando la existencia de una extensión para v_∞. No obstante, este es uno de los problemas centrales de la teoría de superficies abstractas de

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(184)693-715, junio-septiembre de 2023. doi: https://doi.org/10.18257/raccefyn.1914

Riemann, cuya demostración se desvía un poco de los intereses de este artículo y por tal motivo asumiremos su existencia. Para un estudio exhaustivo de este tema vea (**Chevalley**, 1951), p. 15-18. Ahora, por el Teorema 1, tenemos que la cantidad de extensiones es acotada por $[L : K(h)]$, que siempre es finito, y así la suma en $(h)_\infty$ será finita. En resumen, la digresión aquí hace parte de la demostración de la siguiente proposición.

Proposición 2. *Sea $L|K$ un cuerpo de funciones algebraicas y D un divisor. Si $D = 0$ entonces $L(D) = K$, es decir, toda función algebraica sin polos es constante. Además, el número de polos y de ceros de una función algebraica $h \in L$ no-constante es finito.*

Más aún, se podría probar que para cada $h \in L$ no-constante la cantidad de ceros y de polos, contados con multiplicidad, son los mismos. Precisamente, $\partial(h) = 0$. Este resultado, conocido como la *fórmula producto*, es crucial en la teoría de funciones algebraicas. Sin embargo, su demostración se aleja un poco del alcance de este artículo. Para conocer su demostración y varias de sus aplicaciones ver (**Chevalley**, 1951, Cap II) o (**Neukirch**, 1999, Cap I).

Volviendo al objetivo de determinar la dimensión del espacio $L(D)$, presentamos el siguiente resultado que contiene el primer hecho relevante en esta dirección.

Proposición 3. *Sea $L|K$ un cuerpo de funciones algebraicas. Entonces,*

1. $\dim\ L(D) < \infty$*, para cada divisor D. En realidad, si $D \geq 0$,* $\dim\ L(D) \leq 1 + \partial(D)$.
2. **(Teorema de Riemann)** *Existe un entero g_0 tal que* $\dim L(D) \geq \partial(D) + 1 - g_0$*, para cualquier divisor D.*

Una aplicación importante del teorema de Riemann es que garantiza la existencia de funciones "meromorfas" sobre una superficie abstracta de Riemann, esto es, funciones $h \in L$ con $(h)_\infty \neq 0$. Por ejemplo, para $\nu \in S_{L|K}$ podemos garantizar que existe una función $h \in L$ con ν su único polo. En efecto, usando el teorema de Riemann, se sigue que, si $D = n\nu$ y $n >> 0$, $\dim L(n\nu) \geq n \cdot d(\nu) + 1 - g_0 > 1$, esto es, existe $h \in L$ no constante con polo en ν. Para entender mejor el origen e importancia de esta problemática ver (**Chevalley**, 1951, Ch. II).

Por otro lado, el teorema de Riemann garantiza la existencia de un entero g_0 tal que $g_0 \geq \partial(D) - \dim_K L(D) + 1$, para todo divisor D. Esto permite definir

$$g_{L|K} := \max\{\partial(D) - \dim_K L(D) + 1 | D \in \mathrm{Div}(L|K)\}.$$

Este entero es llamado el *género* de $L|K$. El género es el invariante más importante de un cuerpo de funciones algebraicas y, como veremos más adelante, es fundamental para el desarrollo teórico. Observe que, $g_{L|K} \geq 0$ ya que si $D = 0$, por la Proposición 2, $\dim_K L(D) = 1$.

Ejemplo 4. Si $K(z)|K$ es el cuerpo de las funciones racionales con K algebraicamente cerrado. Entonces, por el Ejemplo 3, se sigue

$$\dim L(D) = \begin{cases} \partial(D) + 1 & \text{si } \partial(D) \geq 0 \\ 0 & \text{si } \partial(D) < 0. \end{cases}$$

De donde, $g_{K(z)|K} = 0$. La recíproca también es cierta, pero su demostración escapa un poco de los intereses de este artículo. Para mayores detalles ver (**Stichtenoth**, 2008, Ch. 1).

Ahora, denote por $\varepsilon(D) := \dim L(D) - \partial(D) - 1 + g_{L|K}$ el término de corrección en el teorema de Riemann. En la literatura, este término es conocido como *índice de especialización del divisor D*. Roch, un estudiante de Riemann, logró determinar intrínsecamente el valor

de $\varepsilon(D)$ como la dimensión de un cierto espacio de formas diferenciales asociadas al divisor D. Este es conocido como el teorema de Riemann-Roch. Una de sus versiones equivalentes, presentada a continuación, será empleada con frecuencia en este artículo.

Teorema 2 (Riemann-Roch)**.** *Sea $L|K$ un cuerpo de funciones algebraicas. Existen un entero $g_{L|K}$ y un divisor $\mathscr{K}$ tal que para cada divisor D tenemos que*

$$\dim_K L(D) = \partial(D) + 1 - g_{L|K} + \dim_K L(\mathscr{K} - D).$$

Para mayores detalles sobre los prerrequisitos y prueba de esta versión,

recomendamos (**Stichtenoth**, 2008, Ch. 1). Aquí, el divisor $\mathscr{K}$, conocido como *divisor canónico*, es definido por una forma diferencial λ sobre $L|K$. Algunas de sus principales características son consecuencia del teorema 2, listadas en el siguiente corolario:

Corolario 1. *Bajo la notación del Teorema 2 se siguen:*

1. $\partial(\mathscr{K}) = 2g_{L|K} - 2$ *y* $\dim_K L(\mathscr{K}) = g_{L|K}$.
2. $\dim_K L(D) = \partial(D) + 1 - g_{L|K}$, *sí* $\partial(D) > 2g - 2$.

Esto da por terminado los resultados previos necesarios para iniciar con el estudio de las funciones zeta en este contexto. El lector interesado en profundizar en algunas de las temáticas relacionadas con lo aquí expuesto le recomendamos (**Stichtenoth**, 2008, Ch. 1), (**Chevalley**, 1951, Ch. II).

Función Zeta y propiedades fundamentales

Considere K un cuerpo de números algebraicos, esto es, una extensión finita de los números racionales $\mathbb{Q}$ y $\mathscr{O}_K$ el anillo de enteros algebraicos de K, es decir, la clausura integral de $\mathbb{Z}$ en K (y así un dominio de Dedekind). Como fue mencionado en la introducción, definimos la función: $\zeta_K(s) = \sum \frac{1}{N(\mathfrak{a})^s}$, para $s \in \mathbb{C}$ y $\mathrm{Re}(s) > 1$, donde la suma es tomada sobre el conjunto de ideales $\mathfrak{a}$ no-nulos de $\mathscr{O}_K$ y $N(\mathfrak{a}) = \#(\mathscr{O}_K/\mathfrak{a})$, es la llamada *norma* del ideal $\mathfrak{a}$. Esta familia de funciones, conocidas por funciones zeta de Dedekind, corresponde a una generalización de la conocida función zeta de Riemann. En efecto, para $K = \mathbb{Q}$ y $\mathscr{O}_{\mathbb{Q}} = \mathbb{Z}$, todo ideal no-nulo $\mathfrak{a}$ es de la forma $\mathfrak{a} = n\mathbb{Z}$, donde $n \in \mathbb{N}$, y así $N(\mathfrak{a}) = \#(\mathbb{Z}/n\mathbb{Z}) = n$.

Es a partir de esta generalización, desde la que es posible formular la siguiente construcción análoga de una familia de funciones zeta y en la cual Weil basó sus estudios.

Sea $L|K$ un cuerpo de funciones algebraicas. Recuerde que, L es una extensión finita del cuerpo de funciones racionales $K(z)$ y supondremos a partir de esta sección que su cuerpo de constantes K es finito con q elementos. Si denotamos por $\mathscr{O}_{L|K} := \{f \in L |\ \nu(f) \geq 0, \forall \nu \in S_{L|K}\}$, es posible probar que $\mathscr{O}_{L|K}$ es un *dominio de Dedekind* (esto es, un anillo noetheriano de dimensión 1 e integralmente cerrado (**Atiyah** & **Macdonald**, 1969, Thm. 9.3, p. 95)) con cuerpo cociente L. Ahora, para cada divisor $D = \sum n_\nu \nu$ de $L|K$ definimos la *norma* de D como $N(D) := q^{\partial(D)}$. Esto permite presentar la función zeta de Dedekind–Weil en términos de divisores:

$$\zeta_{L|K}(s) = \sum_{D \geq 0} \frac{1}{N(D)^s} = \sum_{D \geq 0} q^{-s\partial(D)}, \text{ donde } \mathrm{Re}(s) > 1,$$

y la suma es sobre los divisores D efectivos de $L|K$. Esta propuesta, basada en los trabajos de Artin, fue presentada por primera vez por F. K. Schmidt. Para mayores detalles de esta fantástica parte de la historia de las matemáticas ver (**Roquette**, 2018).

A continuación discutiremos algunas de las propiedades de este tipo de funciones zeta como, por ejemplo, su convergencia. Antes de probar resultados concretos, serán necesarias algu-

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(184)693-715, junio-septiembre de 2023. doi: https://doi.org/10.18257/raccefyn.1914

nas manipulaciones formales.

Para cada divisor D, definimos la *serie lineal completa* como el conjunto de divisores efectivos:

$$|D| := \{D + (h) | \, h \in L(D) \setminus \{0\}\}.$$

En realidad, $|D|$ no es más que la proyectivización del espacio vectorial $L(D)$ y así es un conjunto algebraico de dimensión $l(D) := \dim_K L(D) - 1$. En efecto, para $E_0 = D + (h_0)$ y $E_1 = D + (h_1)$, donde $h_0, h_1 \in L(D)$, tenemos $E_0 = E_1$ si y solo si $(h_0/h_1) = (h_0) - (h_1) = D + (h_0) - (D + (h_1)) = 0$ si y solo si $h_0 = \lambda h_1$, para algún $\lambda \in K^*$, por la Proposición 2. Ahora, como $\#K = q$, concluimos que $\#|D| = \frac{q^{l(D)}-1}{q-1}$.

Por otra parte, $|D|$ es el conjunto que parametriza los divisores positivos *linealmente equivalentes* a D, esto es, una relación de equivalencia definida sobre $\mathrm{Div}(S_{L|K})$ por: $E \equiv D$ si y solo si $E - D = (h)$, para alguna $h \in L$. Denotamos por $\overline{D}$ la clase de equivalencia definida por el divisor D. Es fácil probar que $|D|$, $l(D)$ y $\partial(D)$ solo dependen de la clase $\overline{D}$. En efecto, si $E = D + (h)$, para alguna $h \in L$, que podemos suponer $h \in L^*$ (ya que el caso $h = 0$ es trivial) entonces

- Por la *fórmula producto* (ver comentarios posteriores a la Proposición 2), tenemos $\partial(E) = \partial(D)$.
- Tenemos: $E_0 \in |D|$ si y solo si $E_0 = D + (h_0)$ si y solo si $E_0 = E + (h_0 \cdot h^{-1})$ si y solo si $E_0 \in |E|$.
- Tenemos isomorfismo $L(E) \simeq L(D)$ de K-espacios vectoriales, dado por $h_0 \mapsto h_0 \cdot h$. En consecuencia, $l(D) = l(E)$.

A partir de esta notación y resultados, se sigue que:

$$\zeta_{L|K}(s) = \sum_{\partial(\overline{D}) \geq 0} \#|\overline{D}| q^{-s\partial(\overline{D})} = \sum_{\partial(\overline{D}) \geq 0} \frac{q^{l(\overline{D})} - 1}{q-1} q^{-s\partial(\overline{D})}.$$

Antes de garantizar la convergencia de esta serie, distinguiremos dos valores importantes de grupos asociados a nuestros divisores. El primero de ellos es $\rho > 0$, el generador del grupo $\rho\mathbb{Z}$ que corresponde a la imagen $\partial(Div(L|K))$ por el homomorfismo de grupos (2). Por otra parte, el grupo de clases de equivalencia por equivalencia lineal:

$$\mathscr{C}^0_{L|K} = \frac{\text{Grupo de divisores de grado 0 de } L|K}{\text{Grupo de divisores principales de } L|K},$$

es un grupo finito, si K es finito (ver, por ejemplo, (**Lorenzini**, 1996, Ch. VII, Thm. 7.13)). Denotaremos el orden de este grupo por $\mathfrak{h}$.

De esta forma, a partir de estos resultados y aplicación del Corolario 1, tenemos

$$\begin{aligned} \zeta_{L|K}(s) &= \frac{1}{q-1}\Bigg(\sum_{0 \leq \partial(\overline{D}) \leq 2g-2} q^{l(\overline{D}) - s\partial(\overline{D})} + \\ &+ \sum_{\substack{n\rho > 2g-2 \\ n \geq 0}} \mathfrak{h} q^{1-g+(1-s)\rho n} - \sum_{n \geq 0} \mathfrak{h} q^{-s\rho n} \Bigg). \end{aligned} \tag{4}$$

Proposición 4. *La serie $\zeta_{L|K}(s)$ es convergente para cada $s \in \mathbb{C}$, con $Re(s) > 1$.*

Proof. Para la convergencia, basta estudiar la convergencia de cada sumando en (4). El primer sumando es finito. Ahora, por la existencia de divisores canónicos, tenemos $\rho \cdot n \geq (2g-2)+\rho$. Así, el segundo y tercer sumando son series geométricas cuya convergencia se dará para $Re(s) > 1$, si $2g-2+\rho \geq 0$. Esto último vale si y solo si $g > 0$ o $\rho > 1$. Para este último caso, concluimos que:

$$\begin{aligned} \zeta_{L|K}(s) &= \frac{1}{q-1}\Bigg(\sum_{0\leq\partial(\overline{D})\leq 2g-2} q^{l(\overline{D})-s\partial(\overline{D})} + \\ &+ \frac{\mathfrak{h}q^{1-g+(1-s)(2g-2+\rho)}}{1-q^{(1-s)\rho}} - \frac{\mathfrak{h}}{1-q^{-s\rho}}\Bigg). \end{aligned} \tag{5}$$

Ahora, en el caso que $g = 0$ y $\rho = 1$, vimos que $L|K$ es isomorfo al cuerpo de funciones racionales, obteniendo que $\mathfrak{h} = 1$, ya que todo divisor de grado cero es principal. En conclusión, se sigue que:

$$\begin{aligned} \zeta_{L|K}(s) &= \frac{1}{q-1}\left(\frac{q}{1-q^{1-s}} - \frac{1}{1-q^{-s}}\right) \\ &= \frac{1}{(1-q^{1-s})(1-q^{-s})}. \end{aligned} \tag{6}$$

□

Corolario 2. *La función $\zeta_{L|K}(s)$ admite una extensión analítica a todo $\mathbb{C}$, con polos simples para s tomando valores $s \equiv 0 \mod (\frac{2\pi i}{\rho \ln(q)})$, o bien, $s \equiv 1 \mod (\frac{2\pi i}{\rho \ln(q)})$.*

Proof. En efecto, primero observe que a partir de las ecuaciones (5) y (6), tenemos $\zeta_{L|K}(s)$ es una función racional en q^s con coeficientes en $\mathbb{Q}$ y así admite una extensión, como una función meromorfa, a todo $\mathbb{C}$. Para obtener los polos, basta nuevamente analizar los denominadores de (5) y (6), para obtener inicialmente que

$$\begin{aligned} \exp(s\rho\ln(q)) = 1 &\iff s\rho\ln(q) = 2k\pi i, \text{ para cada } k \in \mathbb{Z} \\ &\iff s = k\frac{2\pi i}{\rho\ln(q)}. \end{aligned}$$

Un análisis análogo para $(1-s)\rho$, nos lleva a concluir $s = 1 + k\frac{2\pi i}{\rho\ln(q)}$, para cada $k \in \mathbb{Z}$. □

Ahora, estamos preparados para mostrar *la ecuación funcional* para las funciones zeta de Dedekind–Weil, que es la versión análoga de la ecuación funcional para las funciones zeta de Riemann y zeta de Dedekind. Para mayores detalles acerca esta última en el estudio de funciones de una variable compleja, recomendamos (**Roquette**, 2018).

Teorema 3 (Ecuación funcional)**.** *La función $\zeta_{L|K}(s)$, satisface la ecuación*

$$\zeta_{L|K}(s) = q^{g-1-s(2g-2)}\zeta_{L|K}(1-s).$$

En otras palabras, la función $q^{s(g-1)}\zeta_{L|K}(s)$ es invariante respecto a la transformación $s \mapsto 1-s$, esto es, para cada $s \in \mathbb{C}$ vale la igualdad

$$q^{s(g-1)}\zeta_{L|K}(s) = q^{(1-s)(g-1)}\zeta_{L|K}(1-s).$$

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(184)693-715, junio-septiembre de 2023. doi: https://doi.org/10.18257/raccefyn.1914

Proof. En primera instancia, será probada la veracidad de la ecuación funcional para $g \neq 0$ o $\rho \neq 1$. En este caso, la función zeta se reduce a estudiar los dos sumandos:

$$z_1(s) = \sum_{0 \leq \partial(\overline{D}) \leq 2g-2} q^{l(\overline{D})-s\partial(\overline{D})},$$

$$z_2(s) = \frac{\mathfrak{h} q^{1-g+(1-s)(2g-2+\rho)}}{1-q^{(1-s)\rho}} - \frac{\mathfrak{h}}{1-q^{-s\rho}}.$$

Iniciamos, denotando por $\mathscr{K}$ (la clase por equivalencia lineal de) un divisor canónico. Ya que, $\partial(\mathscr{K}) = 2g-2$, se sigue $0 \geq \partial(\overline{D}) \geq 2g-2$ si y solo si $0 \geq \partial(\mathscr{K} - \overline{D}) \geq 2g-2$, lo que nos permite reescribir:

$$z_1(s) = \sum_{0 \leq \partial(\overline{D}) \leq 2g-2} q^{l(\mathscr{K}-\overline{D})-s\partial(\mathscr{K}-\overline{D})}.$$

Por aplicación del teorema de Riemann-Roch, tenemos que

$$\begin{aligned} l(\mathscr{K}-\overline{D}) - s\partial(\mathscr{K}-\overline{D}) &= l(\mathscr{K}-\overline{D}) - s\partial(\mathscr{K}) + s\partial(\overline{D}) \\ &= l(\overline{D}) - \partial(\overline{D}) - 1 + g - s(2g-2) + s\partial(\overline{D}) \\ &= (g-1) - s(2g-2) + l(\overline{D}) - (1-s)\partial(\overline{D}). \end{aligned}$$

A partir de ahí,

$$\begin{aligned} z_1(s) &= \sum_{0 \leq \partial(\overline{D}) \leq 2g-2} q^{(g-1)-s(2g-2)+l(\overline{D})-(1-s)\partial(\overline{D})} \\ &= q^{(g-1)-s(2g-2)} \sum_{0 \leq \partial(\overline{D}) \leq 2g-2} q^{l(\overline{D})-(1-s)\partial(\overline{D})} \\ &= q^{(g-1)-s(2g-2)} z_1(1-s). \end{aligned}$$

Lo que prueba la invarianza de $z_1(s)$. Por otro lado, para $z_2(s)$ se tiene que:

$$\begin{aligned} z_2(1-s) &= \frac{\mathfrak{h} q^{1-g+(1-(1-s))(2g-2+\rho)}}{1-q^{(1-(1-s))\rho}} - \frac{\mathfrak{h}}{1-q^{-(1-s)\rho}} \\ &= q^{1-g+s(2g-2)} \left(-\frac{\mathfrak{h}}{1-q^{-s\rho}} + \frac{\mathfrak{h} q^{1-g+(1-s)(2g-2+\rho)}}{1-q^{(1-s)\rho}} \right) \\ &= q^{1-g+s(2g-2)} z_2(s). \end{aligned}$$

En conclusión, $\zeta_{L|K}(s)$ satisface la ecuación funcional para cada $g \neq 0$ o $\rho \neq 1$.

Para el caso $g = 0$ y $\rho = 1$ basta seguir la secuencia de ecuaciones, a partir de la ecuación (8):

$$\begin{aligned} \zeta_{L|K}(1-s) &= \frac{1}{(1-q^{1-(1-s)})(1-q^{-(1-s)})} \\ &= q^{1-2s} \left(\frac{1}{(1-q^{-s})(1-q^{1-s})} \right) \\ &= q^{1-2s} \zeta_{L|K}(s). \end{aligned}$$

□

Leonard Euler demostró que la función zeta de Riemann se describe en términos de productos que involucran a los números primos. Esta formulación deja en evidencia la estrecha relación de la función zeta con la teoría (analítica) de números, la cual es determinada por:

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}},\ \mathrm{Re}(s) > 1.$$

Para una demostración de este resultado y sus implicaciones en las funciones de una variable compleja, recomendamos (**Lins-Neto**, 2016, Teorema 27, p. 389). A continuación, presentamos la formulación y demostración de un análogo de este resultado para $\zeta_{L|K}$. En este contexto, esta representación permitirá establecer una relación entre los ceros de $\zeta_{L|K}$ y los puntos racionales sobre cierta superficie abstracta de Riemann, el objetivo principal de este artículo. Mencionamos que en los resultados aquí presentados asumiremos cierta familiaridad con la convergencia de productos de funciones de una variable compleja. Para mayores detalles ver (**Lins-Neto**, 2016, Cap. 5, §4).

Proposición 5. *Sea $S_{L|K}$ una superficie abstracta de Riemann definida sobre un cuerpo de funciones algebraicas, con cuerpo de constantes finito. Entonces, para cada $Re(s) > 1$ se tiene:*

$$\zeta_{L|K}(s) = \prod_{\nu} \frac{1}{1-N(\nu)^{-s}},$$

donde $\nu \in S_{L|K}$.

Proof. Sea m un entero positivo. Como consecuencia de la finitud del grupo $\mathscr{C}^0_{L|K}$, se sigue que el conjunto de puntos $\nu \in S_{K|F}$ cuyo grado $\mathrm{d}(\nu)$ sea menor o igual a m es finito. Así, podemos definir nuestra sucesión de productos parciales y, por la fórmula de Newton para series binomiales, tenemos que

$$\prod_{\mathrm{d}(\nu)\leq m} \frac{1}{1-N(\nu)^{-s}} = \prod_{\mathrm{d}(\nu)\leq m} (1+N(\nu)^{-s}+N(\nu)^{-2s}+\cdots)$$

donde $N(k\cdot\nu) = q^{k\mathrm{d}(\nu)}$ es la norma del divisor $k\cdot\nu$. Observemos, que al multiplicar dos series del tipo $(1+N(\nu_1)^{-s}+N(2\nu_1)^{-s}+\cdots)(1+N(\nu_2)^{-s}+N(2\nu_2)^{-s}+\cdots)$, cada sumando de este producto es de la forma $N(k\nu_1+l\nu_2)$ para $k\geq 0, l\geq 0$. De esto se sigue que:

$$\prod_{\mathrm{d}(\nu)\leq m} \frac{1}{1-N(\nu)^{-s}} = \sum_{D\geq 0}^{*} N(D)^{-s}$$

donde el símbolo "$*$" es para representar que la suma es sobre aquellos divisores positivos $D = \sum n_\nu \nu$, con $\mathrm{d}(\nu)\leq m$. En consecuencia:

$$\sum_{D\geq 0}^{*} N(D)^{-s} = \sum_{\substack{D\geq 0\\ \partial(D)\leq m}} N(D)^{-s} + \sum_{\substack{D\geq 0\\ \partial(D)> m}}^{*} N(D)^{-s}$$

En definitiva, se sigue que

$$\begin{aligned}\left|\prod_{\mathrm{d}(\nu)\leq m} \frac{1}{1-N(\nu)^{-s}} \sum_{\substack{D\geq 0\\ \partial(D)\leq m}} N(D)^{-s}\right| &= \left|\sum_{\substack{D\geq 0\\ \partial(D)> m}}^{*} N(D)^{-s}\right| \\ &\leq \sum_{\substack{D\geq 0\\ \partial(D)> m}}^{*} N(D)^{-r} \\ &< \sum_{\substack{D\geq 0\\ \partial(D)> m}} N(D)^{-r}\end{aligned}$$

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(184)693-715, junio-septiembre de 2023. doi: https://doi.org/10.18257/raccefyn.1914

donde $r := \mathrm{Re}(s)$ y este último sumando tiende a cero cuando $m \to \infty$ debido a la convergencia absoluta de $\zeta_{L|K}$. □

Como lo anticipamos, una consecuencia importante de este teorema es

Corolario 3. *Los ceros de la función $\zeta_{L|K}$ se encuentran en la franja $0 \leq Re(s) \leq 1$.*

Proof. Claramente, por la Proposición 5, se tiene que $\zeta_{L|K}$ no tiene ceros en la región $\mathrm{Re}(s) > 1$. En consecuencia, por la ecuación funcional, Teorema 3, se sigue que $\zeta_{L|K}$ no tiene ceros en $\mathrm{Re}(s) < 0$. □

A partir de este resultado y la analogía con la función zeta de Riemann, es natural proponer la conjetura (que, en realidad, en este contexto es conocido como el Teorema de Hasse-Weil (**Weil**, 1948)), que por la misma analogía anterior, llamaremos de **Hipótesis de Riemann**: Los ceros de la función $\zeta_{L|K}$ están todos en la recta $\mathrm{Re}(s) = \frac{1}{2}$.

Nuestro objetivo será mostrar que la Hipótesis de Riemann en este contexto es equivalente a una cota sobre los puntos racionales de la superficie abstracta de Riemann asociada al cuerpo de funciones algebraicas con cuerpo de constantes finito. Para esto, será necesario introducir las siguientes herramientas y objetos. Sea $L|K$ una extensión de cuerpos, como hasta ahora. Denotamos por K_m la única extensión (salvo isomorfismos) de K de grado m. Definimos por el *compositio*, que denotamos por LK_m, el menor cuerpo que contiene a L y a K_m. Se puede demostrar que $LK_m|K_m$ es un cuerpo de funciones algebraicas (ver (**Milne**, 2020, Cáp I) o (**Weil**, 1995)), cuyo cuerpo de constantes es dado por K_m y, así, finito. Esto permite definir la superficie abstracta de Riemann $S_{LK_m|K_m}$ y, así, el número de puntos racionales, $N_m := \#S^{\mathrm{rac}}_{LK_m|K_m}$. Para cada entero positivo m, los puntos racionales de $S_{LK_m|K_m}$ serán esenciales en la equivalencia principal de este artículo. El siguiente teorema deja en evidencia esta importancia y abre el camino hacia la "traducción" del análogo de la hipótesis de Riemann a un problema aritmético.

Teorema 4. *Si N_m representa el número de puntos racionales de la superficie de Riemann $S_{LK_m|K_m}$, para cada $m \geq 1$, entonces para cada $s \in \mathbb{C}$, con $Re(s) > 1$,*

$$\zeta_{L|K}(s) = \exp\left(\sum_{m=1}^{\infty} N_m q^{-ms}\right). \tag{7}$$

Proof. Como la rama principal del logaritmo está bien definida en $\mathrm{Re}(s) > 1$ y la convergencia absoluta del producto infinito, en la Proposición 5, se sigue que

$$\begin{aligned}
\log(\zeta_{L|K}(s)) &= \log\left(\prod_{\nu} \frac{1}{1-N(\nu)^{-s}}\right) \\
&= \sum_{\nu} \log\left(\frac{1}{1-N(\nu)^{-s}}\right) \\
&= -\sum_{\nu} \log\left(1-N(\nu)^{-s}\right) \\
&= -\sum_{\nu}\sum_{i=1}^{\infty} \frac{1}{i} N(\nu)^{-is},
\end{aligned}$$

donde la última igualdad es consecuencia de la expansión en series de potencia de la función

logaritmo $\log(1-z)$. Ya que $r := \mathrm{Re}(s) > 1$, tenemos que

$$\begin{aligned}\sum_{\nu}\sum_{i=1}^{\infty}\frac{1}{i}|N(\nu)^{-is}| &= \sum_{\nu}\sum_{i=1}^{\infty}\frac{1}{i}N(i\nu)^{-r} < \sum_{\nu}\sum_{i=1}^{\infty}N(i\nu)^{-r}\\ &< \sum_{D\geq 0}N(D)^{-r} = \zeta_{L|K}(r),\end{aligned}$$

y ya que $\zeta_{L|K}(r) < \infty$, se prueba que $\log(\zeta_{L|K}(s))$ converge absolutamente en el semiplano $\mathrm{Re}(s) > 1$. En consecuencia, $\zeta_{L|K}(s) = \exp(-\sum_{\nu}\sum_{i=1}^{\infty}\frac{1}{i}N(\nu)^{-is})$, si $\mathrm{Re}(s) > 1$. Por otro lado, debido a la convergencia absoluta, tenemos la siguiente secuencia de igualdades al reordenar la serie:

$$\begin{aligned}\sum_{\nu}\sum_{i=1}^{\infty}\frac{1}{i}N(\nu)^{-is} &= \sum_{\nu}\sum_{i=1}^{\infty}\frac{1}{i}q^{-i\mathrm{d}(\nu)s}\\ &= \sum_{m=1}^{\infty}\sum_{\substack{i,\nu\\ \mathrm{d}(\nu)\cdot i=m}}\frac{1}{i}q^{-ms}\\ &= \sum_{m=1}^{\infty}\sum_{\mathrm{d}(\nu)|m}\frac{\mathrm{d}(\nu)}{m}q^{-ms}.\end{aligned}$$

La conclusión del teorema es consecuencia del lema a seguir. □

Lema 1. *$N_m = \sum_{d(\nu)|m} d(\nu)$, para cada entero positivo m.*

Proof. Sea $\nu \in S_{L|K}$ y sea $w \in S_{LK_m|K_m}$ una extensión de ν. Como $LK_m|K_m$ es una extensión separable por constantes (ver (**Milne**, 2020, Cáp I)) entonces se sigue que w es no-ramificado y, así, $K_w = K_m K_\nu$. Por lo tanto,

$$\begin{aligned}w \text{ es racional} &\Leftrightarrow K_\nu \subseteq K_m\\ &\Leftrightarrow \partial(\nu)|m.\end{aligned}$$

Ahora, por el Teorema 1, que en este caso es realmente una igualdad, se tiene que el número de extensiones de ν a LK_m es igual a

$$\begin{aligned}\frac{m}{e_{w|\nu}f_{w|\nu}} &= \frac{m}{[K_m:K_\nu]}\frac{[K_\nu:K]}{[K_\nu:K]} = \frac{m[K_\nu:K]}{m}\\ &= [K_\nu:K] = \mathrm{d}(\nu).\end{aligned}$$

Esto indica que todas las extensiones son racionales y, así, el número de puntos racionales de $S_{LK_m|K_m}$ es igual a $\sum_{\mathrm{d}(\nu)|m}\mathrm{d}(\nu)$ para cada entero positivo m. □

Observación 1. *Lo anterior nos dice que para cada entero positivo m, $N_m = \sum_{d(\nu)|m} d(\nu)$, en otras palabras,*

$$N_m = \sum_{d|m} d\#\{\textit{divisores primos}\, L|K \,\textit{de grado}\, d\}.$$

*Luego, por la fórmula de inversión de Möbius (**Rosen**, 2010, Ch. 7), tenemos que*

$$\begin{aligned}m\#\{\nu \in S_{L|K} \,|\, \partial(\nu) = d\} &= \sum_{d|m}\mu(\frac{m}{d})N_d\\ \#\{\nu \in S_{L|K} \,|\, d(\nu) = d\} &= \frac{1}{m}\sum_{d|m}\mu(\frac{m}{d})N_d.\end{aligned}$$

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(184)693-715, junio-septiembre de 2023. doi: https://doi.org/10.18257/raccefyn.1914

*Ahora, en lugar de determinar para cada entero m el número de divisores primos de $L|K$ de grado m, determinaremos el número N_m de puntos racionales de $S_{LK_m|K_m}$. Así, en analogía con la fórmula de Riemann para el número exacto de primos menor o igual que una cantidad dada x (**Lins-Neto**, 2016, Cap. 5, §5.2), fijaremos nuestro objetivo a hallar una fórmula para el número N_m de los puntos K_m-racionales de la superficie abstracta de Riemann $S_{LK_m|K_m}$ en términos de m y de los ceros de la función $\zeta_{L|K}(s)$.*

Sobre la Hipótesis de Riemann

En esta sección será mostrado el resultado principal de este artículo: la equivalencia entre el análogo de la hipótesis de Riemann y la cota para los puntos racionales de una superficie abstracta de Riemann sobre extensiones de cuerpos de funciones algebraicas con cuerpo de constantes finito. A partir de esta equivalencia, es que Weil demuestra la hipótesis, garantizando la validez de dicha cota, conocido hoy como Teorema de Hasse–Weil (**Weil**, 1948). La prueba posteriormente fue simplificada por Bombieri usando el conocido *truco de Stepanov* en su famoso artículo (**Bombieri**, 1974). No obstante, una primera demostración de la Hipótesis la había dado Helmut Hasse, desafiado por Mordell y Davenport (estudiante de este último), para curvas de género uno o *curvas elípticas*, lo que explica su inclusión en el nombre del Teorema. Para conocer mayores detalles de esta fantástica historia recomendamos **Roquette**, 2018, Chap. 7.

A continuación, presentaremos los principales resultados sobre la función $\zeta_{L|K}$ usando una notación más conveniente. Para cada s, tal que $\mathrm{Re}(s) > 1$, tenemos

$$\zeta_{L|K}(s) = \sum_{D\geq 0} q^{-s\partial(D)}$$

la cual, al considerar la sustitución $t = q^{-s}$, resulta en la función:

$$Z(t) = \sum_{D\geq 0} t^{\partial(D)} \tag{8}$$

con $|t| < q^{-1}$. Con esta nueva presentación, la función $\zeta_{L|K}(s)$ se reescribe en términos de la función $Z(t)$ así: Si $g = 0$, entonces $Z(t) = \frac{1}{(1-qt)(1-t)}$. Si $g \geq 1$, entonces

$$Z(t) = \frac{1}{q-1}\left(\sum_{0\leq\partial(\overline{D})\leq 2g-2} q^{l(\overline{D})}t^{\partial(\overline{D})} + \frac{\mathfrak{h}q^g t^{2g-1}}{1-qt} - \frac{\mathfrak{h}}{1-t}\right). \tag{9}$$

En consecuencia, $Z(t)$ es una función racional para cada $t \in \mathbb{C}$ con polos simples en $t = 1$ y en $t = \frac{1}{q}$. Esto es, $Z(t) = \frac{P(t)}{(1-qt)(1-t)}$, donde $P(t) \in \mathbb{Z}[t]$. A partir de esta última descripción, queremos determinar algunas propiedades del polinomio $P(t)$. En efecto,

- Por la teoría de los residuos para funciones de una variable compleja, se sigue

$$\begin{aligned}\mathrm{Res}(Z(t),1) &= \lim_{t\to 1}(t-1)Z(t) = \lim_{t\to 1}\frac{-P(t)}{1-qt}\\ &= \frac{P(1)}{q-1} = \frac{\mathfrak{h}}{q-1},\end{aligned}$$

  concluyendo así que, $P(1) = \mathfrak{h}$.

- Haremos un estudio exhaustivo de la expresión (9). Si $g = 1$, entonces, en este caso,

$2g-2=0$ y de ahí, como aplicación del teorema de Riemann-Roch, se obtiene

$$\begin{aligned}\sum_{\partial(\overline{D})=0} q^{l(\overline{D})}t^{\partial(\overline{D})} &= \sum_{\substack{\partial(\overline{D})=0\\ l(\overline{D})=0}} q^{l(\overline{D})} + \sum_{\substack{\partial(\overline{D})=0\\ l(\overline{D})=1}} q^{l(\overline{D})} \\ &= (\mathfrak{h}-1)+q.\end{aligned} \tag{10}$$

Esto lleva a la expresión

$$\begin{aligned}Z(t) &= \frac{1}{q-1}\left(\mathfrak{h}-1+q+\frac{\mathfrak{h}qt}{1-qt}+\frac{\mathfrak{h}}{1-t}\right) \\ &= \frac{1+(\mathfrak{h}-q-1)t+qt^2}{(1-qt)(1-t)}.\end{aligned}$$

- Ahora, supongamos $g \geq 2$. En este caso, es fácil verificar con ayuda del divisor canónico, que tenemos

$$\begin{aligned}\mathfrak{h} &= \#\{\text{clases de divisores de grado } 0\} \\ &= \#\{\text{clases de divisores de grado } \ 2\text{g-2}\}.\end{aligned}$$

Esto implica, a partir de (9), que

$$\begin{aligned}Z(t) = \frac{1}{q-1}((\mathfrak{h}-1+q)t^0 &+ \sum_{1\leq\partial(\overline{D})\leq 2g-3} q^{l(\overline{D})}t^{\partial(\overline{D})} \\ &+ ((\mathfrak{h}-1)q^{g-1}+q^g)t^{2g-2} + \frac{\mathfrak{h}q^g t^{2g-1}}{1-qt} - \frac{\mathfrak{h}}{1-t}).\end{aligned} \tag{11}$$

En definitiva, a partir de (10) y (11), podemos concluir que: $P(t)$ es un polinomio de grado $2g$, su término constante $P(0)$ es igual a 1 y su coeficiente principal es q^g.

Corolario 4 (Ecuación funcional)**.** *La función $(\frac{1}{t})^{g-1}Z(t)$ es invariante por la transformación $t \to \frac{1}{qt}$. En forma equivalente, la función racional $(\frac{1}{t})^g P(t)$ es invariante respecto a la transformación $t \to \frac{1}{qt}$.*

Proof. Observe que la primera de estas afirmaciones es fácil de verificar $Z(t)$ ya que a partir del Teorema 3, se satisface:

$$(\frac{1}{t})^{g-1}Z(t) = (qt)^{g-1}Z(\frac{1}{qt}).$$

Para la segunda afirmación, basta sustituir $Z(t)$ para obtener:

$$\frac{(\frac{1}{t})^{g-1}P(t)}{(1-qt)(1-t)} = \frac{(qt)^{g-1}P(\frac{1}{qt})}{(1-\frac{1}{t})(1-\frac{1}{qt})}.$$

llevándonos a concluir que, $(\frac{1}{t})^g P(t) = (qt)^g P(\frac{1}{qt})$. □

Corolario 5. *Los ceros de la función $Z(t)$ se encuentran en la franja $\frac{1}{q} \leq |t| \leq 1$.*

Proof. Por la Proposición 5, tenemos que para cada $|t| < \frac{1}{q}$, $Z(t) = \prod_{v\in S_{L|K}} \frac{1}{1-t^{\mathrm{d}(v)}}$. En consecuencia, como aplicación de los Corolarios 3 y 4, se sigue que los ceros de $Z(t)$ se encuentran en $\frac{1}{q} \leq |t| \leq 1$. □

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(184)693-715, junio-septiembre de 2023. doi: https://doi.org/10.18257/raccefyn.1914

En consecuencia, a partir del Corolario 5, podemos reformular la **Hipótesis de Riemann** en los nuevos términos, como: Los ceros de la función $Z(t)$ se ubican sobre la circunferencia $|t| = q^{-\frac{1}{2}}$.

De esta forma, nuestro objetivo se reorienta ahora a relacionar el estudio de los ceros de $Z(t)$ con el estudio de los ceros de $P(t)$. Para esto, consideremos a $P(t)$ como un polinomio de la forma $\sum_{i=0}^{2g} n_i t^i$, para $n_i \in \mathbb{Z}$. A partir del Corolario 4, tenemos al comparar coeficientes en la ecuación funcional que:

$$n_{2g-i} = q^{g-i} n_i \; i = 1, \ldots, g.$$

En particular, ya que $n_0 = P(0) = 1$, se sigue que $n_{2g} = q^g$, es decir, reobtenemos el resultado acerca del coeficiente principal de $P(t)$. Ahora bien, $P(t)$ como producto de factores lineales, debe ser de la forma $P(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$, donde $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ son los recíprocos de los ceros de $Z(t)$ contados con multiplicidades. Más aún, cada α_i es un número algebraico, ya que $Q(t) = t^{2g} P(\frac{1}{t}) \in \mathbb{Z}[t]$ es un polinomio mónico para el cual es fácil verificar que $Q(\alpha_i) = 0$ para cada $i = 1, \ldots, 2g$. A partir de esta factorización y el Corolario 4, se sigue de la relación entre los factores que

$$\alpha_i \alpha_{i+g} = q, \text{ para cada } i = 1, \ldots, g. \tag{12}$$

En este sentido, en términos de los α_i, la Hipótesis de Riemann ahora afirma que:

$$|\alpha_i| = \sqrt{q}, \text{ para cada } i = 1, \ldots, 2g. \tag{13}$$

Y a partir de la ecuación 12, tenemos la formulación equivalente: $\overline{\alpha_i} = \alpha_{g+i}$, para cada $i = 1, \ldots, 2g$.

Observación 2. *Una de las primeras consecuencias importantes de la Hipótesis de Riemann, o bien por el Teorema de Hasse-Weil, es que el número de clases* $\mathfrak{h} = P(1) = \prod_{i=1}^{2g}(1 - \alpha_i)$*, es acotada por*

$$(\sqrt{q} - 1)^{2g} \leq \mathfrak{h} \leq (\sqrt{q} + 1)^{2g}.$$

En efecto, $\mathfrak{h} = |\mathfrak{h}| = \prod_{i=1}^{2g} |1 - \alpha_i|$*. Así, por la desigualdad triangular,* $|\alpha_i| - 1 \leq |\alpha_i - 1| \leq |\alpha_i| + 1$ *y por la versión de la Hipótesis de Riemann en 12, se tendría que* $|\alpha_i| = \sqrt{q}$ *para* $i = 1, \ldots, 2g$ *y de ahí se sigue la afirmación. Esta es, sin duda, una motivación adicional para establecer nuestra conexión e invitar al lector al estudio de la demostración de este fascinante resultado.*

El siguiente teorema será el puente que nos permitirá establecer la conexión que presentará a la hipótesis de Riemann en términos aritméticos, que es el resultado principal de este artículo.

Teorema 5. *Para cada entero positivo m, se satisface que* $N_m = 1 + q^m - \sum_{i=1}^{2g} \alpha_i^m$*, donde* $N_m = \#S^{rac}_{LK_m|K_m}$ *y* $[K_m : K] = m$*.*

Proof. Por la versión adaptada del Teorema 4 a la función $Z(t)$, precisamente de la expresión (7), se sigue que para cada $|t| < \frac{1}{q}$

$$Z(t) = \exp\left(\sum_{m=1}^{\infty} \frac{1}{m} N_m t^m\right). \tag{14}$$

Luego,

$$\frac{Z'(t)}{Z(t)} = \frac{d}{dt}\log(Z(t)) = \sum_{m=1}^{\infty} N_m t^{m-1}. \tag{15}$$

De esta forma, sabiendo que $Z(t) = \frac{\prod_{i=1}^{2g}(1-\alpha_i t)}{(1-t)(1-qt)}$, se obtiene la siguiente expresión

$$\begin{aligned}
\frac{d}{dt}\log(Z(t)) &= \frac{d}{dt}\log\left(\frac{\prod_{i=1}^{2g}(1-\alpha_i t)}{(1-t)(1-qt)}\right) \\
&= \frac{d}{dt}\left(\sum_{i=1}^{2g}\log(1-\alpha_i t) - \log(1-t) - \log(1-qt)\right) \\
&= \frac{d}{dt}\sum_{m=1}^{\infty}\left(\frac{1}{m}(1+q^m-\sum_{i=1}^{2g}\alpha_i^m)\right)t^m \\
&= \sum_{m=1}^{\infty}\left(1+q^m-\sum_{i=1}^{2g}\alpha_i^m\right)t^{m-1}.
\end{aligned}$$

Para la conclusión del teorema, bastará comparar los coeficientes de esta última ecuación y las de la expresión (15). □

A partir de la colección de resultados previos es fácil llegar a la conclusión deseada:

Teorema 6 (Equivalencia con la Hipótesis de Riemann)**.** *La hipótesis de Riemann para superficies abstractas de Riemann con cuerpo de constantes finito es equivalente al estimativo, para cada entero $m \geq 1$, y cuerpo de funciones algebraicas de género $g \geq 2$:*

$$|N_m - q^m - 1| \leq 2gq^{\frac{m}{2}}$$

Proof. Por el Teorema 5, se sigue el estimativo:

$$|N_m - q^m - 1| \leq \sum_{i=1}^{2g}|\alpha_i|^m.$$

La hipótesis de Riemann afirma que $|\alpha_i| = \sqrt{q}$, para cada $i = 1,\ldots,2g$. De donde, $|N_m - q^m - 1| \leq 2gq^{\frac{m}{2}}$.

Recíprocamente, como $P(t) = Z(t)(1-qt)(1-t)$ se tiene por (15) del Teorema 5 y la expansión de la serie geométrica:

$$\begin{aligned}
\frac{P'(t)}{P(t)} &= \frac{d}{dt}\log(P(t)) = \frac{Z'(t)}{Z(t)} - \frac{q}{1-qt} - \frac{1}{1-t} \\
&= \sum_{m=1}^{\infty}(N_m - q^m - 1)t^{m-1}.
\end{aligned} \tag{16}$$

Por hipótesis se tiene que $|N_m - q^m - 1| \leq 2gq^{\frac{m}{2}}$ para cada $m \geq 1$ y, en consecuencia, por la fórmula del radio de Hadamard (**Lins-Neto**, 2016, Cap. 2, Tma. 5), se tiene para R radio de convergencia de (16) que $R \geq \frac{1}{\lim\limits_{m\to\infty}(2g)^{\frac{1}{m}}q^{\frac{1}{2}}} = q^{-\frac{1}{2}}$.

Por otro lado, como $\frac{P'(t)}{P(t)}$ es holomorfa en el círculo $|t| < q^{-\frac{1}{2}}$, ya que $P(t)$ no tiene ceros en este conjunto, se sigue por la ecuación funcional que $P(t)$ no tiene ceros en $\frac{1}{|qt|} > \frac{1}{qq^{-\frac{1}{2}}} =$

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(184)693-715, junio-septiembre de 2023. doi: https://doi.org/10.18257/raccefyn.1914

$q^{-\frac{1}{2}}$. En consecuencia, por el radio de convergencia anterior, los ceros de $Z(t)$ pertenecen a la circunferencia $|t| = q^{-\frac{1}{2}}$. □

A modo de conclusión: Conjetura BSD y Teorema de Deligne

L−funciones y la Conjetura BSD

Como fue mencionado en la introducción, la función zeta presentada aquí tiene una estrecha relación con una clase especial de funciones, conocidas como $L-$funciones, las cuales juegan un rol importante en áreas como la geometría, la teoría de números y (la fusión de estas) la geometría aritmética.

Al igual que la función zeta de Riemann, de manera resumida y sin menospreciar sus importantes consecuencias, las $L-$funciones también satisfacen cierta ecuación funcional, lo que permite su extensión analítica. Así mismo, se representa por medio de una productoria en términos de elementos primos y existe en este contexto lo que se conoce como la hipótesis de Riemann para las $L-$funciones (**Sarnak**, 2006).

Ahora bien, volviendo al papel de estas funciones en la geometría aritmética, abordaremos un caso importante de esta relación y sobre la cual se conjeturan problemas interesantes acerca la aritmética de una clase de curvas muy especiales en geometría, teoría de números y aplicaciones, conocidas como *curvas elípticas*.

Introduciremos cierto contexto geométrico. Sea $K = \mathbb{F}_p$ un cuerpo finito con p elementos y $\overline{K}$ representa su clausura algebraica. Una *curva algebraica plana proyectiva suave* es el conjunto de ceros

$$C = \left\{(x : y : z) \in \mathbb{P}^2(\overline{K}) \,|\, F(x,y,z) = 0\right\}$$

donde F es un polinomio homogéneo no constante, (absolutamente) irreducible y que no tiene ceros en común con F_X, F_Y y F_Z, sus derivadas parciales. Ejemplos bien conocidos de estas curvas, son las curvas *elípticas, E* definida por los ceros de $Y^2Z - X^3 - g_2XZ^2 - g_3Z^3$, con $\Delta := -16(4g_2^3 + 27g_3^2) \neq 0$ y $\text{char}(K) \neq 2,3$. El teorema de Weil acerca la hipótesis de Riemann en este contexto había sido probado antes por Hasse, como fue mencionado en la introducción a la Sección 5. Precisamente, $\#E(\mathbb{F}_p) = p + 1 - a_p$, donde $|a_p| \leq 2\sqrt{p}$ e indicamos por $\#E(K)$ la cardinalidad sobre K del conjunto de soluciones de la ecuación que define a E. En este caso la ecuación (14) puede ser descrita por $Z(E,t) = \exp\left(\sum_{m=1}^{\infty} \#E(\mathbb{F}_{p^m})\frac{t^m}{m}\right)$ y dos curvas elípticas E y E' son llamadas *aritméticamente equivalentes* si ellas definen las mismas funciones zeta o equivalentemente $\#E(\mathbb{F}_p) = \#E'(\mathbb{F}_p)$. Hacemos hincapié, en que no todas las preguntas sobre $E(\mathbb{F}_p)$ se reducen a determinar su valor $\#E(\mathbb{F}_p)$. En realidad, la cota es el aliciente para determinar su naturaleza y propiedades, como lo mostraremos con el raciocinio a continuación.

Suponga que la ecuación de E es definida sobre $\mathbb{Q}$ e imagine que quisiéramos determinar la naturaleza del conjunto $E(\mathbb{Q})$. En efecto, esto es lo que responde el Teorema de Mordell–Weil (**Silverman**, 2009, Ch. VIII), afirmando que este es un grupo abeliano finitamente generado. En particular, como consecuencia del teorema de clasificación de grupos abelianos finitamente generados, tenemos que $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{Tors}}$, para cierto $r \geq 0$. Aquí el *rango algebraico* de la curva elíptica es definido por el valor $r_E := r \geq 0$ y $E(\mathbb{Q})_{\text{Tors}}$ es el subgrupo de elementos de orden finita de $E(\mathbb{Q})$.

Ahora, la función $L(E,s)$ definida por la curva elíptica es la serie de Dirichlet (holomorfa) determinada por los valores de $\#E(\mathbb{F}_p)$, esto es, $L(E,s) = \sum_{n\geq 1} \frac{b_n}{n^s}$, donde a_n es definida siguiendo las reglas de generación: $b_1 = 1, b_p = \#E(\mathbb{F}_p), b_{p^l} = b_p b_{p^{l-1}} - b_{p^{l-2}}$ y $a_{mn} =$

$a_m a_n$, si $(m,n)=1$. Más aún se prueba, para $\mathrm{Re}(s)>\frac{3}{2}$, que:

$$L(E,s)=\prod_{p:\text{primo}}\left(1-a_p p^{-s}+p^{1-2s}\right)^{-1}.$$

Heurísticamente, podemos aproximarnos al valor $L(E,1)$ sustituyendo en la fórmula anterior $L(E,1)=\prod_{p:\text{primo}}\frac{p}{\#E(\mathbb{F}_p)}$. Y así, si $\#E(\mathbb{F}_p)>p$ ocurre a menudo entonces $L(E,1)=0$. En efecto, esto se logra probar y un hecho muy interesante es determinar el orden de este cero. Una de las razones detrás de esto es que empíricamente

$$\prod_{p\leq x}\frac{\#E(\mathbb{F}_p)}{p}\to\infty\Leftrightarrow E(\mathbb{Q})=\infty.$$

Pero más que esto, la gran afirmación continúa siendo un problema abierto a los días de hoy conocida como la conjetura de Birch–Swinnerton-Dyer, que da evidencia de que el orden de este cero para la función $L(E,s)$ en $s=1$ es igual a $r=r_E$ el rango algebraico de la función elíptica. En pocas palabras, el rango analítico coincide con el rango algebraico. Hasta ahora ha habido pocos avances en la resolución de esta conjetura, salvo los trabajos de Gross-Zaguier de 1986 (**Gross** & **Zagier**, 1986) para curvas de rango 0 y 1 y más recientemente se le otorgó la Medalla Fields a Manjul Bhargava por su demostración que el $62,5\%$ de las curvas elípticas satisfacen la conjetura BSD (**Bhargava** & **Shankar**, 2015).

Este es uno de los múltiples y variados resultados relacionados al estudio de las funciones zeta y, su generalización, las funciones L. No es en vano, cuando muchos matemáticos se han referido a ella como el problema más prolífico de las matemáticas y este artículo es evidencia de esto.

Geometría, aritmética y Teorema de Deligne

¿Qué tal si en lugar de una curva elíptica pensamos en determinar el "tamaño" y la "naturaleza" del conjunto de puntos $\mathbb{F}_q-$racionales, $V(\mathbb{F}_q)$ con $q=p^r$ y p :primo, de una variedad algebraica V proyectiva suave? Para esto estableceremos cierto contexto geométrico: Una *variedad algebraica proyectiva suave* es el conjunto de soluciones simultáneas

$$V:=\{(a_0:a_1:\cdots:a_n)\in\mathbb{P}^n(\overline{\mathbb{F}_p})\mid F_i(a_0,\ldots,a_n)=0,\forall 1\leq i\leq m\}$$

donde los polinomios F_i son homogéneos no-constantes, tales que el ideal que generan $(F_1,\ldots,F_m)\subseteq\mathbb{F}_p[x_0,\ldots,x_n]$ es un ideal primo y la matriz *jacobiana* $J_V=\left(\frac{\partial F_i}{\partial x_j}\right)$ tiene rango $n-\dim(V)$, donde $\dim(V)$ es la dimensión topológica de V. En este caso, la *función zeta de V* es por definición

$$Z(V,t):=\exp\left(\sum_{m=1}^{\infty}\#V(\mathbb{F}_{p^m})\frac{t^m}{m}\right).$$

Lo primero a observar es que $1\leq\#V(\mathbb{F}_{p^m})\leq p^{mn}$ y así la serie será convergente si $|t|<q^{-n}$. La generalización en este contexto de la Hipótesis de Riemann, fue conocida como la *Conjetura de Weil*, que fue demostrada por Pierre Deligne en 1974 (**Deligne**, 1974) y lo que le permitió a hacerse a la honrosa distinción de la medalla Fields. Precisamente, Grothendieck había demostrado que, si V es una variedad algebraica proyectiva suave de dimensión s entonces

$$Z(V,t)=\frac{P_1(t)P_3(t)\cdots P_{2s-1}(t)}{P_0(t)P_2(t)\cdots P_{2s}(t)}$$

donde $P_i(t)\in\mathbb{Z}[t]$, $P_i(0)=1$ y $\deg(P_i)=:b_i=\dim_{\mathbb{R}}H^i(\widetilde{V}(\mathbb{C}),\mathbb{R})$ es el *$i-$ésimo número de Betti* de la variedad compleja $\widetilde{V}(\mathbb{C})$ asociada a V, para cada $i=0,\ldots,2s$. A partir de esta

Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.
47(184)693-715, junio-septiembre de 2023. doi: https://doi.org/10.18257/raccefyn.1914

descomposición, Deligne demostró que para cada $i = 0, \ldots, 2s$ vale que

$$P_i(t) = \prod_{j=1}^{b_i}(1 - \alpha_{ij}t), \text{ donde } \alpha_{ij} \in \mathbb{C} \text{ y } |\alpha_{ij}| = p^{\frac{i}{2}}.$$

Este resultado y toda la maquinaria creada para su demostración permitieron un desarrollo espectacular de la geometría algebraica a mediados del siglo XX, entendida aquí como geometría arítmetica. Sin lugar a dudas este fue un resultado influyente en el desarrollo de la matemática de los últimos dos siglos y dejó en evidencia fuertes conexiones entre la geometría y la teoría de números, aparentemente, tan disímiles. Así mismo, es una consecuencia (elemental) de una de las problemáticas actuales que ha sido fuente de grandes resultados y desarrollos teóricos fascinantes, conocido como (la conjetura de la reciprocidad del) *Programa de Langlands*. Para profundizar más acerca de algunas de las consecuencias de estos resultados recomendamos (**Katz**, 1976), (**Katz** and **Messing**, 1974).

Contribución de los autores

Los autores afirmamos que el aporte de cada uno de los autores es igual en este trabajo.

Conflicto de intereses

Los autores declaran no tener conflicto de intereses con respecto al contenido de este artículo.

Agradecimientos y financiación

Este trabajo fue parcialmente financiado por el CODI, Universidad de Antioquia, Proyecto 2020-33305.

References

Atiyah, M. F., Macdonald, I. G. (1969). *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont.

Bhargava, M., Shankar, A. I. V. (2015). Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Annals of Mathematics, 181*(2), 587-621.

Bombieri, E. (1974). Counting points on curves over finite fields (d'après s.a.stepanov). *Lecture Notes in Mathematics*, Vol. 383.Springer, Berlin.

Castro, C., Maecha, J. (2004). Fractal supersymmetric qm, geometry probabity and the riemann hypothesis. *International Journal of Geometric Methods in Modern Physics*, *1*, 751-793.

Chevalley, C. (1951). *Introduction to the theory of algebraic functions of one variable*. Mathematical surveys; monographs.

Deligne, P. (1974). La conjecture de weil. i. *Publications Mathématiques de l'Institut des Hautes E´tudes Scientifiques*, *43*, 273-307.

Domenica, B., Vincent, W. (2009). The parietal cortex and the representation of time, space, number and other magnitudes. Philosophical Transactions of the Royal Society A, *364*, 1831-1840.

Gross, B., Zagier, D. (1986). Heegner points and derivatives ofl-series. *Invent Math, 84*, 225-320.

Hindry, M. (2012). La preuve par andré weil de l'hypothèse de riemann pour une courbe sur un corps fini. Henri Cartan & André Weil, math´ematiciens du XXe siècle, 4, 62-98.

Katz, N. M. (1976). An overview of deligne's proof of the riemann hypothesis for varieties over finite fields (hilbert's problem 8). *Proceedings of Symposia in Pure Mathematics,* 28, 275-305.

Katz, N. M., Messing, W. (1974). Some consequences of the riemann hypothesis for varieties over finite fields. *Inventiones mathematicae, 23*(1), 73-77.

Koblitz, N. (1994). *A course in number theory and cryptography.* Springer-Verlag, Berlin.

Lins-Neto, A. (2016). *Funcoes de uma variavel complexa.* Publicacoes do IMPA.

Lorenzini, D. (1996). *An invitation to arithmetic geometry.* American Mathematical Society, Providence, RI.

Milne, J. (2017). The riemann hypothesis over finite fields: From weil to the present day. Notices of the ICCM, *4*, 14-52.

Milne, J. (2020). *Algebraic number theory,* v.3.08. Personal web page.

Neukirch, J. (1999). *Algebraic number theory*. Springer-Verlag, Berlin.

Roquette, P. (2018). *The riemann hypothesis in characteristic p in historical perspective*. Springer, Cham.

Rosen, M. (2010). *Number theory in function fields.* Springer-Verlag, New York.

Samuel, P., Zariski, O. (2013). *Commutative algebra*, volume i. Dover Publications.

Sarnak, P. (2006). Problems of the millennium: The riemann hypothesis. *American Mathematical Society, 1*, 5-21.

Sierra, G. (2019). The riemann zeros as spectrum and the riemann hypothesis. *Symmetry, 494*, 2-37.

Silverman, J. H. (2009). *The arithmetic of elliptic curves.* Graduate texts in mathematics.

Stichtenoth, H. (2008). *Algebraic function fields and codes*. Springer Berlin Heidelberg.

Weil, A. (1979). *Sur les fonctions algébriques à corps de constantes fini.* https://doi.org/10.1007/978-1-4757-1705-1 34

Weil, A. (1948). *Sur les courbes algébriques et les variétés qui s' en déduisent.* Actualités Sci. Ind.

Weil, A. (1995). *Basic number theory.* Springer Berlin Heidelberg.

Wiles, A. (2006). The birch and swinnerton-dyer conjecture. *American Mathematical Society, 1*, 31-44.