La Hipótesis de Riemann en Campos de Funciones

Tesis que presenta:
María Liliana Rodríguez Salvador
para obtener el grado de
Maestra en Ciencias (Matemáticas)

Posgrado en Matemáticas
Departamento de Matemáticas
Universidad Autónoma Metropolitana-Iztapalapa

Asesora: Dra. Martha Rzedowski Calderón

Diciembre de 2011

II

Agradecimientos

A mi pequeño Lyan Santiago, por ser mi inspiración y motivación al realizar este trabajo de tesis.

A mi esposo Miguel González, cuyo apoyo, tenacidad y confianza me han sido de gran utilidad para que este trabajo fuese terminado.

En especial agradezco a mis padres Silvia Salvador y Casimiro Rodríguez, por su apoyo incondicional y por darme las herramientas necesarias para luchar en la vida.

Quisiera agradecer a la doctora Martha Rzedowski Calderón, del Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, por haber aceptado asesorarme durante este trabajo, así como también por sus consejos y sugerencias.

Deseo agradecer a mis entrañables amigos Liliana, Marco Antonio, Luis Felipe, Juan Francisco y Jaime, por su compañía y solidaridad a lo largo de este proyecto.

Agradezco a la doctora Laura Hidalgo Solís, de la Universidad Autónoma Metropolitana Iztapalapa, y al doctor Arturo Cueto Hernández, de la Universidad Autónoma Metropolitana Azcapotzalco, por la revisión y críticas que hicieron a este trabajo, y por su tiempo prestado.

A todos aquellos que de una manera u otra han colaborado en la realización de este trabajo, pero en particular al doctor Gabriel Daniel Villa Salvador y al Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional.

Finalmente agradezco el apoyo del CONACyT y del SNI.

Resumen

La Hipótesis de Riemann en Campos de Funciones es el análogo, ya resuelto, en campos de funciones de la famosa Hipótesis de Riemann. La definición de la función zeta $\zeta_K(s)$ de un campo de funciones K proviene de la extensión natural de la función usual de Riemann:

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

Se sabe que $\zeta(s)$ tiene una extensión meromorfa al plano complejo, con un único polo en $s = 1$, el cual es simple con residuo 1. Más aún, $\zeta(s)$ tiene ceros en $s = -2n$, $n \in \mathbb{N}$ y éstos son llamados los ceros triviales de $\zeta(s)$. Por otro lado, $\zeta(s)$ no tiene ceros diferentes a los triviales en $\mathbb{C}\backslash\{s \mid 0 \leq \mathbb{R}e\ s \leq 1\}$. La Hipótesis de Riemann establece que los ceros de $\zeta(s)$, aparte de los triviales, están en la recta $\mathbb{R}e\ s = \frac{1}{2}$.

La Hipótesis de Riemann sigue siendo un problema abierto. Sin embargo, para campos de funciones congruentes (es decir, cuyo campo de constantes es finito) la respuesta sí se conoce y es positiva. Esto fue demostrado por André Weil en 1941.

Teorema (Hipótesis de Riemann en Campos de Funciones).
Sea K/k un campo de funciones congruente. Entonces, los ceros de la función zeta $\zeta_K(s)$ están en la línea $\mathbb{R}e\ s = \frac{1}{2}$.

Como consecuencia tenemos que si K/k es un campo de funciones congruente, donde $|k| = q$, N_1 el número de divisores primos de grado 1 en K

y g el género de K, entonces

$$|N_1 - (q+1)| \leq 2g\sqrt{q}.$$

En el trabajo de tesis se presentan una demostración, basada en la de Enrico Bombieri, de la Hipótesis de Riemann en Campos de Funciones y algunas aplicaciones de este resultado, entre ellas: si K es un campo de funciones congruente de género 0, entonces K es un campo de funciones racionales. También, se presentan todos los posibles campos de funciones congruentes K con número de clases 1 y género mayor que 0.

Índice General

Introducción

El Problema de Basilea abre las puertas a la Función Zeta, la cual es el objeto matemático de la Hipótesis de Riemann. El Problema de Basilea se refiere a la serie:

$$\sum_{n=1}^{\infty} \frac{1}{n^2}.$$

El problema fue resuelto en 1735 por Leonhard Euler quien encontró que

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Alrededor de 1740, Euler considero la serie

$$\sum_{n=1}^{\infty} \frac{1}{n^s}$$

para valores enteros positivos de s.

La definición de la Función Zeta, $\zeta_K(s)$, de un campo de funciones K proviene de la extensión natural de la Función Zeta de Riemann:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \text{para } s \in \mathbb{C},\ \mathbb{R}e\ s > 1.$$

La función $\zeta(s)$ tiene una extensión meromorfa al plano complejo, con un único polo en $s = 1$, el cual es simple con residuo 1. Más aún, $\zeta(s)$ tiene ceros en $s = -2n$, $n \in \mathbb{N}$ y éstos son llamados los ceros triviales de $\zeta(s)$. Por otro lado, $\zeta(s)$ no tiene ceros diferentes a los triviales en $\mathbb{C}\backslash\{s \mid 0 \leq \mathbb{R}e\ s \leq 1\}$. La

Hipótesis de Riemann, propuesta por Bernhard Riemann en 1859, establece que los ceros de $\zeta(s)$, aparte de los triviales, están en la recta $\mathbb{R}e\ s = \frac{1}{2}$.

La Hipótesis de Riemann sigue siendo un problema abierto. Sin embargo, para campos de funciones congruentes la respuesta sí se conoce y es positiva. Esto fue demostrado por Helmut Hasse para campos de género 1 en 1936 y por André Weil para el caso general en 1941.

La demostración de la Hipótesis de Riemann que presentaremos se debe esencialmente a Enrico Bombieri, la cual es probablemente la más sencilla de las conocidas, pero aun ésta es bastante técnica.

En el presente trabajo se hace un estudio cuidadoso del tema, se presentan con detalle las demostraciones de casi todos los resultados y se añaden algunos ejemplos.

En el Capítulo 1 tratamos campos de funciones congruentes, es decir, campos de funciones con campo de constantes finito. En este capítulo estudiamos la Función Zeta y las Series L, así como sus ecuaciones funcionales. Además hallamos explícitamente $\zeta_K(s)$ para un campo de funciones elípticas K sobre k, con número de clases h y para $K = k(x, y)$ con $y^m = x$, $m \in \mathbb{N}$.

El Capítulo 2 está dedicado a la Hipótesis de Riemann en campos de funciones congruentes (Teorema 2.2.10). La demostración la hacemos en varias etapas. Primero se demuestra que las condiciones presentadas en el Teorema 2.1.8 son equivalentes. Después el objetivo es probar que las condiciones del Teorema 2.1.8 se cumplen para cualquier campo de funciones congruentes K; en el camino hacia nuestro objetivo nos encontraremos (Teorema 2.2.4) con una cota superior, en términos de q y del género de K, para $N_1 - (q+1)$, donde N_1 es el número de divisores primos de grado 1 en K y q es la cardinalidad del campo de constantes, la cual no es suficiente para deducir la Hipótesis de Riemann. Para obtener una cota inferior, se ha de proceder todavía con más cuidado.

Como aplicación de la Hipótesis de Riemann presentamos algunas estimaciones del número de divisores primos de grado n en un campo de

funciones congruente K/k. Otra consecuencia inmediata es que si K/k es un campo de funciones congruente de género 0, entonces K es un campo de funciones racionales. También se presentan todos los posibles campos de funciones congruentes K con número de clases 1 y género mayor que 0, se prueba que el Invariante μ de Iwasawa es igual a cero para campos de funciones congruentes y se comenta acerca de un análogo al Teorema de Brauer-Siegel para campos de funciones congruentes.

En el apéndice que está hacia el final del trabajo se presentan algunas definiciones y resultados a los que se hace referencia.

Capítulo 1

Campos de Funciones Congruentes

En este capítulo estudiamos la Función Zeta y las Series L, así como sus ecuaciones funcionales y la Fórmula del Producto para la Función Zeta. Como ejemplos, presentamos explícitamente $\zeta_K(s)$ para un campo de funciones elípticas K sobre k, con número de clases h y para $K = k(x, y)$ con $y^m = x$, $m \in \mathbb{N}$.

1.1. Extensiones de Constantes

Sean k y l campos finitos, $k \subseteq l$, $k = \mathbb{F}_q$, $l = \mathbb{F}_{q^f}$, $q = p^u$, p primo, $u \geq 1$. Notemos que $k = \{x \in \overline{\mathbb{F}}_p \mid x^q = x\}$, $l = \{x \in \overline{\mathbb{F}}_p \mid x^{q^f} = x\}$, donde $f = [l : k]$ y $\overline{\mathbb{F}}_p$ es la cerradura algebraica de $\mathbb{F}_p$.

Definición 1.1.1. Un campo de funciones K/k se llama ***congruente*** si k es finito.

Observemos el campo de constantes de la extensión de constantes en el siguiente ejemplo.

Ejemplo 1.1.2. Sean k_0 un campo de característica $p > 0$, u, v dos elementos algebraicamente independientes sobre k_0. Sean $k = k_0(u, v)$ y x una variable sobre k. Sea $K = k(x, y)$ tal que $y^p = ux^p + v$. Se tiene $[K : k(x)] = 1$ o p.

Sea k' el campo de constantes de K. Veremos que $k' = k$. Si $k' \neq k$, entonces $[k' : k] = [k'(x) : k(x)] \mid [K : k(x)]$, luego, $[k' : k] = p$ y $K = k'(x)$. Por tanto $y = u^{1/p}x + v^{1/p} \in k'(x)$, por lo que $u^{1/p}$, $v^{1/p} \in k'$ y $p = [k' : k] \geq \left[k\left(u^{1/p}, v^{1/p}\right) : k\right] = \left[k\left(u^{1/p}, v^{1/p}\right) : k\left(u^{1/p}\right)\right]\left[k\left(u^{1/p}\right) : k\right] = p \cdot p = p^2$, lo cual es absurdo. Así tenemos que $k' = k$.

Sea $l_0 = k\left(v^{1/p}\right)$ y sea $L = Kl_0$. Entonces $l_0 \bigcap K = k$, $u^{1/p} = \dfrac{y - v^{1/p}}{x} \in Kl_0 = L$, por lo tanto el campo de constantes l de L contiene propiamente a l_0 pues $l \supseteq k\left(u^{1/p}, v^{1/p}\right) \supsetneq l_0$.

Consideremos K/k un campo de funciones congruente y l una extensión finita de k. Sea $L = Kl$ la extensión de constantes, $[l : k] = f$. En el ejemplo anterior vimos que, en general, es posible que el campo de constantes de $L = Kl$ contenga propiamente a l. El siguiente teorema prueba que esto no sucede en el caso de campos de funciones congruentes.

Teorema 1.1.3. *Sean K/k un campo de funciones congruente, l una extensión finita de k y $L = Kl$ una extensión de constantes. Entonces el campo de constantes de L es l.*

Demostración. Sean $l = k(\xi)$ y $f = [l : k]$. Entonces

$$\mathrm{Irr}(\xi, x, k) | x^{q^f} - x = \prod_{\alpha \in l} (x - \alpha).$$

Se tiene $L = Kl = Kk(\xi) = K(\xi)$ con $\mathrm{Irr}(\xi, x, K) | \mathrm{Irr}(\xi, x, k)$, por lo que $\mathrm{Irr}(\xi, x, K) \in K[x] \bigcap l[x] = k[x]$, es decir, $\mathrm{Irr}(\xi, x, K) = \mathrm{Irr}(\xi, x, k)$. Entonces $[L : K] = \mathrm{deg}\mathrm{Irr}(\xi, x, K) = \mathrm{deg}\mathrm{Irr}(\xi, x, k) = [l : k] = f$. Si l' denota el campo de constantes de L, con $l \subseteq l'$, entonces $L = Kl'$ y por lo tanto, $[l' : k] = [L : K] = [l : k] = f$, lo cual implica que $l' = l$.

□

Teorema 1.1.4. *Sea $L = Kl$. Entonces $[L : K] = [l : k]$. Para $\mathfrak{A} \in D_K$, $d_L(\mathfrak{A}) = d_K(\mathfrak{A})$, más precisamente, $d_L(\mathrm{con}_{K/L}\mathfrak{A}) = d_K(\mathfrak{A})$. Finalmente, $g_L = g_K$.*

Demostración. En el Teorema A.32, se afirma la existencia de $\lambda_{L/K} \in \mathbb{Q}^+$, tal que $d_L(\mathfrak{A}) = \dfrac{d_K(\mathfrak{A})}{\lambda_{L/K}}$, para $\mathfrak{A} \in D_K$ y se tiene que $\lambda_{L/K} = \dfrac{[l : k]}{[L : K]}$. Por el Teorema 1.1.3 se tiene que $\lambda_{L/K} = 1$ y por lo tanto $d_L(\mathfrak{A}) = d_K(\mathfrak{A})$, para $\mathfrak{A} \in D_K$.

Ahora sea $\mathfrak{A} \in D_K$. Se tiene:

$$L_K(\mathfrak{A}) = \{x \in K \mid \upsilon_{\mathfrak{P}}(x) \geq \upsilon_{\mathfrak{P}}(\mathfrak{A}),\ \forall\, \mathfrak{P} \in \mathbb{P}_K\},$$

$$L_L(\mathfrak{A}) = \{y \in L \mid \upsilon_{\mathcal{P}}(y) \geq \upsilon_{\mathcal{P}}(\mathfrak{A}),\ \forall\, \mathcal{P} \in \mathbb{P}_L\}.$$

Sea $y = \displaystyle\sum_{i=1}^{n} a_i x_i$, $a_i \in l$, $x_i \in L_K(\mathfrak{A})$. Entonces

$$\begin{aligned} \upsilon_{\mathcal{P}}(y) &= \upsilon_{\mathcal{P}}\left(\sum_{i=1}^{n} a_i x_i\right) \geq \min_{1\leq i\leq n}\{\upsilon_{\mathcal{P}}(a_i x_i)\} = \min_{1\leq i\leq n}\{\upsilon_{\mathcal{P}}(a_i) + \upsilon_{\mathcal{P}}(x_i)\} \\ &\geq \min_{1\leq i\leq n} \upsilon_{\mathcal{P}}(x_i) = \min_{1\leq i\leq n} \upsilon_{\mathfrak{P}}(x_i) \geq \upsilon_{\mathfrak{P}}(\mathfrak{A}) = \upsilon_{\mathcal{P}}\left(\mathrm{con}_{L/K}(\mathfrak{A})\right), \end{aligned}$$

donde $\mathfrak{P} = \mathcal{P} \mid_K$ (recordemos que L/K no tiene divisores ramificados [Teorema A.31]). Esto demuestra que, $lL_K(\mathfrak{A}) \subseteq L_L(\mathfrak{A})$.

Recíprocamente, sea $y \in L_L(\mathfrak{A})$, es decir, $\upsilon_{\mathcal{P}}(y) \geq \upsilon_{\mathcal{P}}(\mathfrak{A})$, $\forall\ \mathcal{P} \in \mathbb{P}_L$. Sea $y = \displaystyle\sum_{i=1}^{n} a_i x_i$, $a_i \in l$, $x_i \in K$. De hecho, si $l = k(\xi)$, $[l : k] = f$, entonces podemos escribir, $y = a_0 + a_1\xi + ... + a_{f-1}\xi^{f-1}$, $a_i \in K$. Sean $y^{(1)} = y$, $y^{(2)}, ..., y^{(f)}$ los conjugados de y. Se tiene que

$$y^{(i)} = a_0 + a_1\xi^{(i)} + ... + a_{f-1}\left(\xi^{(i)}\right)^{f-1}.$$

Resolviendo estas ecuaciones para las $a_i's$, obtenemos:

$$a_i = \frac{\det \begin{bmatrix} 1 & \xi^{(1)} & \dots & y^{(1)} & \dots & \left(\xi^{(1)}\right)^{f-1} \\ . & . & \dots & . & \dots & . \\ . & . & \dots & . & \dots & . \\ . & . & \dots & . & \dots & . \\ 1 & \xi^{(f)} & \dots & y^{(f)} & \dots & \left(\xi^{(f)}\right)^{f-1} \end{bmatrix}}{\det \begin{bmatrix} 1 & \xi^{(1)} & \dots & \left(\xi^{(1)}\right)^{i} & \dots & \left(\xi^{(1)}\right)^{f-1} \\ . & . & \dots & . & \dots & . \\ . & . & \dots & . & \dots & . \\ . & . & \dots & . & \dots & . \\ 1 & \xi^{(f)} & \dots & \left(\xi^{(f)}\right)^{i} & \dots & \left(\xi^{(f)}\right)^{f-1} \end{bmatrix}} = \frac{b_i}{c_i}$$

con $c_i \in k^*$, $b_i = \sum_{j=1}^{f} t_j y^{(j)}$, $t_j \in l$.

Puesto que $y^{(j)}$ es conjugado de y y $\mathfrak{A} \in D_K$, tenemos $y \in L_L(\mathfrak{A}) \Rightarrow y^{(j)} \in L_L(\mathfrak{A})$. Por lo tanto

$$\begin{aligned} \upsilon_{\mathfrak{P}}(a_i) &= \upsilon_{\mathfrak{P}}\left(\sum_{j=1}^{f} \frac{t_j}{c_i} y^{(j)}\right) \geq \min_{1\leq j\leq f} \upsilon_{\mathfrak{P}}\left(\frac{t_j}{c_i} y^{(j)}\right) \\ &= \min_{1\leq j\leq f} \upsilon_{\mathfrak{P}}\left(t_j c_i^{-1} y^{(j)}\right) \\ &= \min_{1\leq j\leq f} \left(\upsilon_{\mathfrak{P}}(t_j) + \upsilon_{\mathfrak{P}}(c_i^{-1}) + \upsilon_{\mathfrak{P}}(y^{(j)})\right) \\ &= \min_{1\leq j\leq f} \left(\upsilon_{\mathfrak{P}}(t_j) - \upsilon_{\mathfrak{P}}(c_i) + \upsilon_{\mathfrak{P}}(y^{(j)})\right) = \min_{1\leq j\leq f} \upsilon_{\mathfrak{P}}\left(y^{(j)}\right) \\ &= \min_{1\leq j\leq f} \upsilon_{\mathcal{P}}\left(y^{(j)}\right) \geq \upsilon_{\mathcal{P}}(\mathfrak{A}) = \upsilon_{\mathfrak{P}}(\mathfrak{A}), \end{aligned}$$

luego $a_i \in L_K(\mathfrak{A})$, de donde $lL_K(\mathfrak{A}) \supseteq L_L(\mathfrak{A})$, así $lL_K(\mathfrak{A}) = L_L(\mathfrak{A})$.

En particular, tenemos

$$l_l(\mathfrak{A}) = \dim_l L_L(\mathfrak{A}) = \dim_k L_K(\mathfrak{A}) = l_k(\mathfrak{A}).$$

Sea $\mathfrak{A} \in D_K$ un divisor tal que

$$d_K(\mathfrak{A}) = d_L(\mathfrak{A}) > \text{máx}\{2g_K - 2, 2g_L - 2\}.$$

Por el Teorema de Riemann-Roch (Corolario A.25), se tiene

$$l_l(\mathfrak{A}^{-1}) = d_L(\mathfrak{A}) - g_L + 1, \;\; l_k(\mathfrak{A}^{-1}) = d_K(\mathfrak{A}) - g_K + 1.$$

Puesto que $l_l(\mathfrak{A}^{-1}) = l_k(\mathfrak{A}^{-1})$ y $d_L(\mathfrak{A}) = d_K(\mathfrak{A})$, concluimos $g_L = g_K$.

□

Teorema 1.1.5. *Sean $\mathcal{P}$ un lugar de $L = Kl$ y $\mathfrak{P} = \mathcal{P}\mid_K$. Entonces*

$$l(\mathcal{P}) = k(\mathfrak{P})l.$$

Demostración. Si L/l es cualquier extensión de K/k y $\mathcal{P}$ es un lugar de L sobre un lugar $\mathfrak{P}$ de K, entonces el campo residual $k(\mathfrak{P}) = \vartheta_{\mathfrak{P}}/\mathfrak{P}$, puede ser encajado de manera natural en $l(\mathcal{P}) = \vartheta_{\mathcal{P}}/\mathcal{P}$.

Puesto que $\mathfrak{P} = \mathcal{P}\mid_K$ se tiene que $\vartheta_{\mathcal{P}} \bigcap K = \vartheta_{\mathfrak{P}}$ y $\mathcal{P} \bigcap K = \mathfrak{P}$, de donde el mapeo natural $\vartheta_{\mathfrak{P}}/\mathfrak{P} \longrightarrow \vartheta_{\mathcal{P}}/\mathcal{P}$ es un monomorfismo de campos. Además $l(\mathcal{P}) \supseteq l$ y $l(\mathcal{P}) \supseteq k(\mathfrak{P})$. Ahora bien, se tiene que $k(\mathfrak{P})l \subseteq l(\mathcal{P})$.

Sea $z \in \vartheta_{\mathcal{P}}$. Entonces escribamos $z = \sum_{i=0}^{f-1} a_i \xi^i$, $a_i \in K$, donde $l = k(\xi)$. Basta probar que $a_i \in \vartheta_{\mathfrak{P}}$. Ahora, si $z^{(i)}$ es un conjugado de z, entonces $z^{(i)} = z^{\sigma} \in \vartheta_{\mathcal{P}^{\sigma}}$, $\sigma \in \mathrm{Gal}(l/k)$ y argumentando como en la demostración del Teorema 1.1.4, $a_i = \sum_{i=0}^{f} t_i z^{(i)}$, $t_i \in l$, $z^{(i)} \in \vartheta_{\mathcal{P}^{(i)}}$. Por lo tanto $a_i \in \vartheta_{\mathfrak{P}}$.

□

1.2. Divisores Primos en Extensiones de Constantes

Sean $k = \mathbb{F}_q$, $l = \mathbb{F}_{q^f}$, K/k un campo de funciones congruente y $L = Kl$ la extensión de constantes. Sea $\mathfrak{P}$ un lugar de K y sean $\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_h$ los lugares de L sobre $\mathfrak{P}$. Sabemos que $\mathfrak{P}$ no es ramificado y $\mathrm{con}_{L/K}(\mathfrak{P}) = \mathcal{P}_1 \cdots \mathcal{P}_h$. Como l/k es siempre de Galois (de hecho cíclica), L/K es de Galois y $d_{L/K}(\mathcal{P}_i/\mathfrak{P}) = d$, $1 \leq i \leq h$. Por el Teorema A.30 se tiene que

$dh = f = [l : k]$. Ahora bien, si $d_K(\mathfrak{P}) = [k(\mathfrak{P}) : k] = r$, esto implica que $k(\mathfrak{P}) = \mathbb{F}_{q^r}$. Similarmente, si $d_L(\mathcal{P}_i) = [l(\mathcal{P}_i) : l] = s$, entonces $l(\mathcal{P}_i) = \mathbb{F}_{q^{fs}}$. De donde, $k(\mathfrak{P})l = \mathbb{F}_{q^r}\mathbb{F}_{q^f} = \mathbb{F}_{q^{[r,f]}} = \mathbb{F}_{q^{fs}}$. Por lo tanto $fs = [r, f] = \dfrac{rf}{(r, f)}$, es decir, $s = \dfrac{r}{(r, f)}$.

Entonces, $d_L(\mathcal{P}_i) = s = \dfrac{d_K(\mathfrak{P})}{\big(d_K(\mathfrak{P}), f\big)}$.

De la Proposición A.29, se tiene que $d_L(\mathcal{P}_i)[l : k] = d_{L/K}(\mathcal{P}_i/\mathfrak{P})d_K(\mathfrak{P})$, es decir, $sf = dr$, entonces $d = \dfrac{sf}{r} = \dfrac{r}{(r, f)}\dfrac{f}{r} = \dfrac{f}{(r, f)}$, y por otro lado tenemos que $h = \dfrac{f}{d} = \dfrac{f}{\frac{f}{(r,f)}} = (r, f)$.

Esto está resumido en el siguiente teorema:

Teorema 1.2.1. *Sean $\mathfrak{P}$ un lugar de K y $\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_h$ los lugares de $L = Kl$ sobre $\mathfrak{P}$ y $[l : k] = f$. Entonces:*

(1) $d_{L/K}(\mathcal{P}_i \mid \mathfrak{P}) = \dfrac{f}{\big(d_K(\mathfrak{P}), f\big)}$.

(2) $h = \big(d_K(\mathfrak{P}), f\big)$.

(3) $d_L(\mathcal{P}_i) = \dfrac{d_K(\mathfrak{P})}{\big(d_K(\mathfrak{P}), f\big)}$.

□

Ahora estudiaremos el grupo de clases $C_{K,0} = D_{K,0}/P_K$. Recordemos que $C_K \cong C_{K,0} \bigoplus \mathbb{Z}$, con $C_K = D_K/P_K$.

Teorema 1.2.2. *Sea K/k un campo de funciones congruente. Entonces $\mid C_{K,0} \mid < \infty$.*

Demostración. Demostremos primero que si $m \in \mathbb{N}$, el número de divisores enteros de grado m es finito.

Sea $\mathfrak{A}$ un divisor entero de grado $\leq m$ y tengamos en cuenta que k es finito. Entonces $\mathfrak{A} = \prod_{\mathfrak{P} \in \mathbb{P}_K} \mathfrak{P}^{v_{\mathfrak{P}}(\mathfrak{A})} = \mathfrak{P}_1^{\alpha_1} \cdots \mathfrak{P}_r^{\alpha_r}$, con $\mathfrak{P}_i$ divisores primos y $\alpha_i \geq 0$, de aquí que $d_K(\mathfrak{A}) = \sum_{i=1}^{r} \alpha_i d_K(\mathfrak{P}_i) \leq m$, de donde obtenemos

que $r \leq m$, $d_K(\mathfrak{P}_i) \leq m$, $\alpha_i \leq m$. Como k es finito, el número de divisores primos de un grado dado es finito. Por lo tanto el número de divisores enteros de grado $m \in \mathbb{N}$ es finito.

Sean $m \geq g_K$ y C una clase de grado m. Por el Teorema de Riemann-Roch [A.23] tenemos que $N(C) = d(C) - g_K + 1 + N(WC^{-1})$ con W la clase canónica, entonces $N(C) \geq d(C) - g_K + 1 = m - g_K + 1 \geq 1$ y por lo tanto C contiene al menos un divisor entero $\mathfrak{A}$ de grado m. Así tenemos que el conjunto C_m que consiste de las clases de grado m es finito. Esto es

$$\mid C_m \mid = \mid \{C \mid d(C) = m\} \mid < \infty.$$

Ahora sean $\mathfrak{M}$ un divisor de grado $m \geq g_K$ y $\varphi : C_{K,0} \longrightarrow C_m$, definida por $\varphi(\overline{\mathfrak{A}}) = \overline{\mathfrak{A}\mathfrak{M}}$.

Veamos que φ está bien definida y es inyectiva. Sean $\overline{\mathfrak{A}}$, $\overline{\mathfrak{B}} \in C_{K,0}$. Tenemos: $\overline{\mathfrak{A}} = \overline{\mathfrak{B}} \Leftrightarrow \exists\ x \in K^*$ tal que $\mathfrak{A} = \mathfrak{B}(x)_K \Leftrightarrow \exists\ x \in K^*$ tal que $\mathfrak{A}\mathfrak{M} = \mathfrak{B}(x)_K\mathfrak{M} = \mathfrak{B}\mathfrak{M}(x)_K \Leftrightarrow \varphi(\overline{\mathfrak{A}}) = \varphi(\overline{\mathfrak{B}})$.

$\therefore \varphi$ está bien definida y es inyectiva.

Finalmente, veamos que φ es suprayectiva.

Sea $\mathfrak{D}$ un divisor de grado m, entonces $\mathfrak{D}\mathfrak{M}^{-1}$ es de grado 0 y $\varphi(\overline{\mathfrak{D}\mathfrak{M}^{-1}}) = \overline{\mathfrak{D}\mathfrak{M}^{-1}\mathfrak{M}} = \overline{\mathfrak{D}},\ \therefore \varphi$ es suprayectiva.

Concluimos

$$\mid C_{K,0} \mid = \mid C_m \mid < \infty.$$

□

Notación. $h_K = h = \mid C_{K,0} \mid$ denotará el ***número de clases*** del campo K.

Proposición 1.2.3. *El número de divisores enteros en una clase C de K es igual a* $\dfrac{q^{N(C)} - 1}{q - 1}$, $q = |k|$.

Demostración. Se tiene que $N(C)$ es el máximo número de divisores enteros linealmente independientes de C sobre k (Proposición A.22).

Sean $\mathfrak{A}_1, ..., \mathfrak{A}_n \in C$, donde $n = N(C)$, un conjunto maximal de divisores enteros linealmente independientes de C sobre k. Tomemos $\mathfrak{A}$ un divisor

arbitrario de C, entonces tenemos que $\dfrac{\mathfrak{A}_i}{\mathfrak{A}} = (x_i)_K$, $x_i \in K^*$, satisfaciendo que $\{x_1, ..., x_n\}$ es un subconjunto maximal linealmente independiente de $L(\mathfrak{A}^{-1})$ sobre k pues como $(x_i)_K = \mathfrak{A}^{-1}\mathfrak{A}_i$, $\forall i$, tenemos $x_1, ..., x_n \in L(\mathfrak{A}^{-1})$.

Sea $\varphi : L(\mathfrak{A}^{-1})\backslash\{0\} \longrightarrow \{\mathcal{C} \in C \mid \mathcal{C} \text{ es un divisor entero}\}$ definida por: $\varphi(\alpha) = (\alpha)_K\mathfrak{A}$. Veamos que φ está bien definida.

Sean $\alpha, \beta \in L(\mathfrak{A}^{-1})\backslash\{0\}$. Tenemos, $\varphi(\alpha) = \varphi(\beta) \Leftrightarrow (\alpha)_K\mathfrak{A} = (\beta)_K\mathfrak{A} \Leftrightarrow (\alpha)_K = (\beta)_K \Leftrightarrow \exists\ y \in k^*$ tal que $\beta = \alpha y$. Luego φ está bien definida y precisamente $q-1$ elementos de $L(\mathfrak{A}^{-1})\backslash\{0\}$ toman el mismo valor.

Sea $\mathfrak{B} \in C$ un divisor entero. Tenemos $\mathfrak{B}\mathfrak{A}^{-1} = (\alpha)_K$ para algún $\alpha \in L(\mathfrak{A}^{-1})\backslash\{0\}$. Luego $\varphi(\alpha) = (\alpha)_K\mathfrak{A} = \mathfrak{B}$. Por tanto φ es suprayectiva.

Ahora bien, como $\mid L\left(\mathfrak{A}^{-1}\right)\backslash\{0\} \mid = q^n - 1$, del hecho anterior tenemos que el número de divisores enteros en C es $\dfrac{q^n-1}{q-1} = \dfrac{q^{N(C)}-1}{q-1}$.

□

Definición 1.2.4. Sea $\rho_K = \rho := \text{mín}\{n \in \mathbb{N} \mid \exists \quad \mathfrak{A} \in D_K, d(\mathfrak{A}) = n\}$.

Por tanto, existe un divisor entero de grado $n \Leftrightarrow \rho \mid n$. Como la clase canónica es de grado $2g-2$, se tiene que $\rho \mid 2g-2$, con g el género de K. Probaremos más adelante que $\rho = 1$.

Teorema 1.2.5. *Sean n múltiplo de ρ y A_n el número de divisores enteros de grado n. Entonces, si $n > 2g-2$, se tiene $A_n = h\left(\dfrac{q^{n-g+1}-1}{q-1}\right)$.*

Demostración. Tenemos que

$$A_n = \sum_{\substack{C \in C_K \\ d(C)=n}} (\text{número de divisores enteros en } C) = \sum_{\substack{C \in C_K \\ d(C)=n}} \frac{q^{N(C)}-1}{q-1}.$$

Ahora, por el Teorema de Riemann-Roch (Corolario A.25) y ya que $n > 2g-2$, tenemos que $N(C) = d(C) - g + 1 = n - g + 1$.

Puesto que hay h clases de C de grado n, se tiene por la Proposición 1.2.3 que

$$A_n = h\left(\frac{q^{n-g+1}-1}{q-1}\right).$$

□

1.3. Función Zeta y Series L

Definición 1.3.1. Para un divisor primo $\mathfrak{P}$ de K, a la cardinalidad de $k(\mathfrak{P})$ le llamamos la ***norma de*** $\mathfrak{P}$ y la denotamos por $N(\mathfrak{P})$.

Notemos que si $f_{\mathfrak{P}} = [k(\mathfrak{P}) : k] = d_K(\mathfrak{P})$ y $|k| = q$, entonces

$$N(\mathfrak{P}) = |k(\mathfrak{P})| = q^{d_K(\mathfrak{P})}.$$

La definición anterior se puede extender para un divisor entero

$$\mathfrak{A} = \prod_{\mathfrak{P} \in \mathbb{P}_K} \mathfrak{P}^{\upsilon_{\mathfrak{P}}(\mathfrak{A})}$$

por

$$\begin{aligned} N(\mathfrak{A}) &= \prod_{\mathfrak{P} \in \mathbb{P}_K} N(\mathfrak{P})^{\upsilon_{\mathfrak{P}}(\mathfrak{A})} = \prod_{\mathfrak{P} \in \mathbb{P}_K} q^{d_K(\mathfrak{P})\upsilon_{\mathfrak{P}}(\mathfrak{A})} = q^{\sum_{\mathfrak{P} \in \mathbb{P}_K} d_K(\mathfrak{P})\upsilon_{\mathfrak{P}}(\mathfrak{A})} \\ &= q^{d_K(\mathfrak{A})} \end{aligned}$$

pues $d_K(\mathfrak{A}) = \sum_{\mathfrak{P} \in \mathbb{P}_K} d_K(\mathfrak{P})\upsilon_{\mathfrak{P}}(\mathfrak{A})$.

Claramente se tiene que $N(\mathfrak{AB}) = N(\mathfrak{A})N(\mathfrak{B})$, para $\mathfrak{A}, \mathfrak{B} \in D_K$.

Definición 1.3.2. Se define la ***Función Zeta de K*** por:

$$\zeta_K(s) = \sum_{\mathfrak{A} \text{ entero}} \frac{1}{\big(N(\mathfrak{A})\big)^s} = \sum_{\mathfrak{A} \text{ entero}} q^{-d_K(\mathfrak{A})s}.$$

Teorema 1.3.3. *La serie $\zeta_K(s)$ converge absoluta y uniformemente en subconjuntos compactos de $\{s \in \mathbb{C} \mid \mathbb{R}e\ s > 1\}$.*

Demostración. Sea $t = \dfrac{2g-2}{\rho}$.

Entonces

$$\begin{aligned} \zeta_K(s) &= \sum_{\mathfrak{A} \text{ entero}} \frac{1}{\big(N(\mathfrak{A})\big)^s} = \sum_{\mathfrak{A} \text{ entero}} \frac{1}{q^{d_K(\mathfrak{A})s}} \\ &= \sum_{n=0}^{\infty} \frac{A_{\rho n}}{q^{n\rho s}} = \sum_{n=0}^{t} A_{\rho n} q^{-n\rho s} + \sum_{n=t+1}^{\infty} A_{\rho n} q^{-n\rho s}. \end{aligned}$$

Por el Teorema 1.2.5 y puesto que $t = \dfrac{2g-2}{\rho}$, se tiene que

$$\sum_{n=t+1}^{\infty} A_{\rho n} q^{-n\rho s} = \frac{h}{q-1} \sum_{n=t+1}^{\infty} (q^{n\rho-g+1} - 1) q^{-n\rho s}.$$

Ahora,

$$\begin{aligned}
\sum_{n=t+1}^{\infty} \mid \left(q^{n\rho-g+1} - 1\right) q^{-n\rho s} \mid &= \sum_{n=t+1}^{\infty} \left(q^{n\rho-g+1} - 1\right) q^{-n\rho \mathbb{R}e\, s} \\
&= \sum_{n=t+1}^{\infty} \left(q^{n\rho-(g-1)} - 1\right) q^{-n\rho \mathbb{R}e\, s} \\
&= \sum_{n=t+1}^{\infty} \left(q^{n\rho-n\rho \mathbb{R}e\, s-(g-1)} - q^{-n\rho \mathbb{R}e\, s}\right) \\
&= \frac{1}{q^{g-1}} \sum_{n=t+1}^{\infty} \left(q^{1-\mathbb{R}e\, s}\right)^{n\rho} \\
&\quad - \sum_{n=t+1}^{\infty} \left(q^{-\mathbb{R}e\, s}\right)^{n\rho}.
\end{aligned}$$

□

Hagamos la sustitución $u := q^{-\rho s}$, $B_n := A_{\rho n}$. Entonces definimos

$$Z_K(u) := \zeta_K(s) = \sum_{n=0}^{\infty} B_n u^n.$$

La clase canónica W es de grado $2g-2$, hay $(h-1)$ clases C de grado $2g-2$ diferentes a la clase W y se tiene que $N(W) = g$, $N(C) = (2g-2) - g + 1 = g - 1$ para $C \neq W$, y $d(C) = 2g - 2$ (Corolarios A.24 y A.25).

Por lo tanto

$$A_{2g-2} = \sum_{\substack{C \in C_K \\ d(C)=2g-2}} \frac{q^{N(C)} - 1}{q-1} = \frac{q^g - 1}{q-1} + (h-1)\left(\frac{q^{g-1} - 1}{q-1}\right)$$

y $A_{\rho n} = h\left(\dfrac{q^{\rho n-g+1} - 1}{q-1}\right)$, para $n > \dfrac{2g-2}{\rho}$.

Proposición 1.3.4. *Sea* $t = \dfrac{2g-2}{\rho}$. *Entonces:*

$$B_j - (q^\rho + 1)B_{j-1} + q^\rho B_{j-2} = 0, \text{ para } j > t+2,$$

$$B_{t+2} - (q^\rho + 1)B_{t+1} + q^\rho B_t = q^{g+\rho-1}.$$

Demostración. Para $j > t+2$, tenemos:

$$j\rho > (t+2)\rho = t\rho + 2\rho = 2g - 2 + 2\rho \geq 2g \ \ (\text{pues } 2\rho - 2 \geq 0),$$

$$(j-1)\rho > (t+1)\rho = t\rho + \rho = 2g - 2 + \rho \geq 2g - 1 \ \ (\text{pues } \rho - 1 \geq 0),$$

$$(j-2)\rho > t\rho = 2g - 2.$$

Por lo tanto

$$\begin{aligned}
&B_j - (q^\rho + 1)B_{j-1} + q^\rho B_{j-2} \\
&= A_{j\rho} - (q^\rho + 1)A_{(j-1)\rho} + q^\rho A_{(j-2)\rho} \\
&= \frac{h}{q-1}\left[(q^{j\rho-g+1} - 1) - (q^\rho + 1)(q^{(j-1)\rho-g+1} - 1) + q^\rho(q^{(j-2)\rho-g+1} - 1)\right] \\
&= \frac{h}{q-1}\left[q^{j\rho-g+1} - 1 - q^{j\rho-g+1} + q^\rho - q^{(j-1)\rho-g+1} + 1 + q^{(j-1)\rho-g+1} - q^\rho\right] \\
&= 0
\end{aligned}$$

porque cada $A_{j\rho}$ cumple la hipótesis del Teorema 1.2.5.

Por otro lado,

$$\begin{aligned}
&B_{t+2} - (q^\rho + 1)B_{t+1} + q^\rho B_t \\
&= A_{t\rho+2\rho} - (q^\rho + 1)A_{t\rho+\rho} + q^\rho A_{t\rho} \\
&= A_{2g-2+2\rho} - (q^\rho + 1)A_{2g-2+\rho} + q^\rho A_{2g-2} \\
&= \frac{h}{q-1}\left[(q^{2g-2+2\rho-g+1} - 1) - (q^\rho + 1)(q^{2g-2+\rho-g+1} - 1)\right] \\
&+q^\rho\left[\frac{q^g - 1}{q-1} + (h-1)\left(\frac{q^{g-1} - 1}{q-1}\right)\right] \\
&= \frac{h}{q-1}(q^\rho - q^{g+\rho-1}) + q^\rho\left(\frac{q^g - 1}{q-1}\right) + (h-1)q^\rho\left(\frac{q^{g-1} - 1}{q-1}\right) \\
&= \frac{h}{q-1}(q^\rho - q^{g+\rho-1} + q^{\rho+g-1} - q^\rho) + \frac{1}{q-1}(q^{\rho+g} - q^\rho - q^{\rho+g-1} + q^\rho) \\
&= \frac{1}{q-1}(q^{\rho+g-1+1} - q^{\rho+g-1}) = \frac{1}{q-1}\left(q^{\rho+g-1}(q-1)\right) = q^{\rho+g-1}.
\end{aligned}$$

□

Ahora consideremos:

$$
\begin{aligned}
&(1-u)(1-q^{\rho}u)Z_K(u)\\
&=\big(1-(1+q^{\rho})u+q^{\rho}u^2\big)Z_K(u)\\
&=\sum_{n=0}^{\infty}B_nu^n-\sum_{n=0}^{\infty}(1+q^{\rho})B_nu^{n+1}+\sum_{n=0}^{\infty}q^{\rho}B_nu^{n+2}\\
&=\sum_{n=0}^{\infty}\big(B_n-(1+q^{\rho})B_{n-1}+q^{\rho}B_{n-2}\big)u^n \quad (\text{con } B_{-1}=B_{-2}=0),\\
&=\sum_{n=0}^{t+2}\big(B_n-(1+q^{\rho})B_{n-1}+q^{\rho}B_{n-2}\big)u^n \quad (\text{Proposición 1.3.4.})\\
&=\big(B_0-(1+q^{\rho})B_{-1}+q^{\rho}B_{-2}\big)+\big(B_1-(1+q^{\rho})B_0+q^{\rho}B_{-1}\big)u\\
&+\sum_{n=2}^{t+2}\big(B_n-(1+q^{\rho})B_{n-1}+q^{\rho}B_{n-2}\big)u^n\\
&=B_0+\big(B_1-(1+q^{\rho})B_0\big)u+\sum_{n=2}^{t+2}\big(B_n-(1+q^{\rho})B_{n-1}+q^{\rho}B_{n-2}\big)u^n\\
&=1+\big(B_1-(q^{\rho}+1)\big)u+\sum_{n=2}^{t+2}\big(B_n-(1+q^{\rho})B_{n-1}+q^{\rho}B_{n-2}\big)u^n\\
&=1+\big(B_1-(q^{\rho}+1)\big)u+\sum_{n=2}^{t+1}\big(B_n-(1+q^{\rho})B_{n-1}+q^{\rho}B_{n-2}\big)u^n+q^{g+\rho-1}u^{t+2},
\end{aligned}
$$

ya que $B_0=A_0=1,$ pues el único divisor entero de grado cero es η.

Es decir, $(1-u)(1-q^{\rho}u)Z_K(u)\in\mathbb{Z}[u]$ es un polinomio de grado $t+2$, al cual denotamos por $P_K(u)$. Tenemos $P_K(u)=a_0+a_1u+a_2u^2+\ldots+a_{t+2}u^{t+2}$, con $a_0=1$, $a_1=B_1-(q^{\rho}+1)$, $a_{t+2}=q^{g+\rho-1}$.

Teorema 1.3.5. *La función $Z_K(u)$ es una función racional y satisface que*

$$Z_K(u)=\frac{P_K(u)}{(1-u)(1-q^{\rho}u)},$$

donde $P_K(u)\in\mathbb{Z}[u]$ es un polinomio de grado $t+2=\dfrac{2g-2}{\rho}+2$.

Además, $\lim\limits_{u\to 1}(1-u)(1-q^{\rho}u)Z_K(u)=P_K(1)=h\dfrac{q^{\rho}-1}{q-1}.$

Demostración. Poniendo $B_{-1} = B_{-2} = 0$, tenemos:

$$\begin{aligned}
P_K(1) &= \sum_{n=0}^{t+2}(B_n - \big(1+q^\rho)B_{n-1} + q^\rho B_{n-2}\big) \\
&= \sum_{n=0}^{t+2}\big(B_n - B_{n-1} - q^\rho B_{n-1} + q^\rho B_{n-2}\big) \\
&= B_{t+2} - B_{-1} - q^\rho\big(B_{t+1} - B_{-2}\big) \\
&= A_{t\rho+2\rho} - q^\rho A_{t\rho+\rho} \\
&= A_{2g-2+2\rho} - q^\rho A_{2g-2+\rho} \\
&= h\left(\frac{q^{2g-2+2\rho-g+1}-1}{q-1}\right) - q^\rho h\left(\frac{q^{2g-2+\rho-g+1}-1}{q-1}\right) \\
&= \frac{h}{q-1}\big(q^{g+2\rho-1} - 1 - q^{g+2\rho-1} + q^\rho\big) \\
&= \left(\frac{q^\rho - 1}{q-1}\right)h.
\end{aligned}$$

Ahora,

$$\begin{aligned}
\lim_{u\to 1} Z_K(u)(1-u)(1-q^\rho u) &= \lim_{u\to 1}\frac{P_K(u)(1-u)(1-q^\rho u)}{(1-u)(1-q^\rho u)} \\
&= \lim_{u\to 1} P_K(u) \\
&= P_K(1) = h\frac{q^\rho - 1}{q-1}.
\end{aligned}$$

□

Corolario 1.3.6. *$Z_K(u)$ tiene un polo simple en $u = 1$.*

□

Para probar la igualdad $\rho = 1$, necesitamos otra expresión de $\zeta_K(s)$.

Teorema 1.3.7. *(Fórmula del Producto)*

$$\zeta_K(s) = \prod_{\mathfrak{P}\,\in\,\mathbb{P}_K}\big(1 - N(\mathfrak{P})^{-s}\big)^{-1}, \quad \mathbb{R}e\ s > 1.$$

Demostración. Sean $\mathfrak{P}$ primo y $d(\mathfrak{P}) = n$. Entonces

$$\begin{aligned}
a_{\mathfrak{P}} &= \big(1 - N(\mathfrak{P})^{-s}\big)^{-1} - 1 = \frac{1}{1-q^{-ns}} - 1 = \frac{q^{-ns}}{1-q^{-ns}} \\
&= \frac{1}{(1-q^{-ns})q^{ns}} = \frac{1}{q^{ns}-1}.
\end{aligned}$$

Se tiene que $\mid q^{ns}-1 \mid \geq \mid q^{ns} \mid -1 = q^{n\alpha}-1$, con $\alpha = \mathbb{R}e\ s > 1$.
Por lo tanto, $\mid a_{\mathfrak{P}} \mid \leq \dfrac{1}{q^{n\alpha}-1} \leq \dfrac{2}{q^{n\alpha}}$.
Ahora,

$$\mid \{\mathfrak{P} | d(\mathfrak{P}) = n\} \mid \leq A_n = h\left(\frac{q^{n-g+1}-1}{q-1}\right), \quad \text{con } n > 2g-2.$$

Entonces se tiene que:

$$\begin{aligned}\sum_{n>>0} \mid a_{\mathfrak{P}} \mid &\leq \sum_{n=0}^{\infty} h\left(\frac{q^{n-g+1}-1}{q-1}\right)\frac{2}{q^{n\alpha}} \\ &= \frac{h}{q-1}q^{-g+1}\sum_{n=0}^{\infty}\frac{2}{q^{n(\alpha-1)}} - \frac{h}{q-1}\sum_{n=0}^{\infty}\frac{2}{q^{n\alpha}} < \infty,\end{aligned}$$

por lo tanto, $\displaystyle\prod_{\mathfrak{P}\,\in\,\mathbb{P}_K}\left(1-N(\mathfrak{P})^{-s}\right)^{-1}$ es absolutamente convergente.

Reorganizando los términos del producto, obtenemos:

$$\begin{aligned}\prod_{\mathfrak{P}\,\in\,\mathbb{P}_K}\left(1-N(\mathfrak{P})^{-s}\right)^{-1} &= \prod_{\mathfrak{P}\,\in\,\mathbb{P}_K}\left(\frac{1}{1-N(\mathfrak{P})^{-s}}\right) \\ &= \prod_{\mathfrak{P}\,\in\,\mathbb{P}_K}\left(\sum_{n_{\mathfrak{P}}=0}^{\infty}\left(N(\mathfrak{P})^{-n_{\mathfrak{P}}s}\right)\right) \\ &= \sum N\left(\mathfrak{P}_1^{\alpha_1}\cdots\mathfrak{P}_r^{\alpha_r}\right)^{-s},\end{aligned}$$

donde la suma se toma sobre todos los conjuntos de primos $\{\mathfrak{P}_1,\ldots,\mathfrak{P}_r\}$, $\alpha_i \geq 0$, para $i = 1, ..., r$. Por lo tanto,

$$\sum_{\substack{\mathfrak{P}_1,\ldots,\mathfrak{P}_r \\ \alpha_i \geq\, 0}} N(\mathfrak{P}_1^{\alpha_1}\cdots\mathfrak{P}_r^{\alpha_r})^{-s} = \sum_{\mathfrak{A}\text{ entero}}\frac{1}{\left(N(\mathfrak{A})\right)^s} = \zeta_K(s).$$

□

Sean $|k| = q$, $l = \mathbb{F}_{q^f}$, $L = Kl$, la extensión de constantes. Queremos comparar $\zeta_L(s)$ con $\zeta_K(s)$ cuando $f = \rho$. Ahora, para $\mathfrak{P}$, lugar de K se tiene $\rho \mid d_K(\mathfrak{P})$ y si $\mathcal{P}_1, \ldots, \mathcal{P}_r$ son los primos de L sobre $\mathfrak{P}$, entonces (por el Teorema 1.2.1) $r = \left(d_K(\mathfrak{P}), \rho\right) = \rho$. Así pues, siempre hay ρ factores en L sobre cualquier divisor primo de K dado.

Además, tenemos $d_L(\mathcal{P}_i) = \dfrac{d_K(\mathfrak{P})}{\big(d_K(\mathfrak{P}), \rho\big)} = \dfrac{d_K(\mathfrak{P})}{\rho}$.

Por otro lado, $N(\mathcal{P}_i) = (q^\rho)^{d_L(\mathcal{P}_i)} = q^{\rho d_K(\mathfrak{P})/\rho} = q^{d_K(\mathfrak{P})} = N(\mathfrak{P})$.

Por lo tanto

$$\begin{aligned}
\zeta_L(s) &= \prod_{\mathcal{P} \in \mathbb{P}_L} \left(1 - \frac{1}{N(\mathcal{P})^s}\right)^{-1} = \prod_{\mathfrak{P} \in \mathbb{P}_K} \left(\prod_{\mathcal{P}|\mathfrak{P}} \left(1 - \frac{1}{N(\mathcal{P})^s}\right)^{-1}\right) \\
&= \prod_{\mathfrak{P} \in \mathbb{P}_K} \left(1 - \frac{1}{N(\mathfrak{P})^s}\right)^{-\rho} = \left(\prod_{\mathfrak{P} \in \mathbb{P}_K} \left(1 - \frac{1}{N(\mathfrak{P})^s}\right)\right)^{-\rho} \\
&= \zeta_K(s)^\rho.
\end{aligned}$$

Es decir, $\zeta_L(s) = \zeta_K(s)^\rho$. Por otra parte, por el Corolario 1.3.6, tanto $\zeta_L(s)$ como $\zeta_K(s)$ tienen un polo de orden 1 en $s = 0$ (o en $u = 1$ con el cambio de variable $u = q^{-\rho s}$), luego $\zeta_K(s)^\rho$ tiene un polo de orden ρ en $s = 0$. De aquí se sigue que $\rho = 1$.

Así, hemos probado el siguiente teorema:

Teorema 1.3.8. *(F. K. Schmidt) Sea K/k cualquier campo de funciones congruente y sea*

$$\rho = \text{mín}\{n \in \mathbb{N} \mid \exists\, \mathfrak{A} \in D_K, d(\mathfrak{A}) = n\}.$$

Entonces $\rho = 1$.

□

Corolario 1.3.9. *Tenemos que $Z_K(u) = \dfrac{P_K(u)}{(1-u)(1-qu)}$, donde $u = q^{-s}$, $P_K(u) \in \mathbb{Z}[u]$ es de grado $2g$, $P_K(u) = 1 + (A_1 - (q+1))u + \cdots + q^g u^{2g}$, $P_K(1) = h$, el número de clases de K.*

Demostración. Se había puesto $t = \dfrac{2g-2}{\rho}$, por lo que $B_n = A_{\rho n} = A_n$, $t = 2g - 2$ y $\dfrac{q^\rho - 1}{q-1} = 1$, ya que $\rho = 1$.

En el Teorema 1.3.5 teníamos que

$P_K(1) = h\dfrac{q^\rho - 1}{q-1}$ y $Z_K(u) = \dfrac{P_K(u)}{(1-u)(1-q^\rho u)}$, $P_K(u) \in \mathbb{Z}[u]$ un polinomio de grado $t+2 = \dfrac{2g-2}{\rho} + 2$.

Ahora sustituyendo las expresiones anteriores en el Teorema 1.3.5 obtenemos algo de lo requerido.

Por otro lado,

$$\begin{aligned}(1-u)(1-q^\rho u)Z_K(u) &= 1 + \big(B_1 - (q^\rho+1)\big)u \\ &\quad + \sum_{n=2}^{t+2} \big(B_n - (1+q^\rho)B_{n-1} + q^\rho B_{n-2}\big)u^n \\ &= 1 + \big(A_1 - (q+1)\big)u + \cdots\cdots + q^g u^{2g}.\end{aligned}$$

□

Corolario 1.3.10. *Si K es un campo de funciones congruente de género 0, entonces*

$$Z_K(u) = \frac{1}{(1-u)(1-qu)}.$$

Demostración. Se sigue del Corolario 1.3.9.

□

Ahora estudiaremos las series L de un campo de funciones congruente.

Definición 1.3.11. Un ***caracter*** χ de orden finito del grupo de clases C_K es un homomorfismo $\chi : C_K \longrightarrow \mathbb{C}^*$, de tal manera que existe $n \in \mathbb{N}$ con $\chi^n = 1$. Es decir, $\chi(C_K) \subseteq \{\xi \in \mathbb{C} \mid \xi^n = 1, \text{ para algún } n \in \mathbb{N}\}$.

Un caracter χ se puede extender a los divisores, $\chi : D_K \longrightarrow \mathbb{C}^*$, $\chi(\mathfrak{A}) = \chi(\mathfrak{A}P_K)$, P_K la clase principal.

Definición 1.3.12. Dado un caracter χ de orden finito sobre D_K, se define la ***serie L asociada a*** χ por:

$$L(s,\chi,K) = \sum_{\mathfrak{A}\text{ entero}} \chi(\mathfrak{A})\frac{1}{\big(N(\mathfrak{A})\big)^s},\ s \in \mathbb{C},\ \mathbb{R}e\ s > 1.$$

Teorema 1.3.13. *La serie* $\sum_{\mathfrak{A} \text{ entero}} \chi(\mathfrak{A}) \frac{1}{\left(N(\mathfrak{A})\right)^s}$ *converge absoluta y uniformemente en subconjuntos compactos de* $\{s \in \mathbb{R} \mid \mathbb{R}e\ s > 1\}$.

Demostración. Se sigue del Teorema 1.3.3 y del hecho de que $|\chi(\mathfrak{A})| = 1$ para todo $\mathfrak{A} \in D_K$.

□

La fórmula del producto se sigue inmediatamente del Teorema 1.3.7.

Teorema 1.3.14. *Para* $L(s, \chi, K)$ *tenemos*

$$L(s, \chi, K) = \prod_{\mathfrak{P} \in \mathbb{P}_K} \left(1 - \frac{\chi(\mathfrak{P})}{N(\mathfrak{P})^s}\right)^{-1}, \ \mathbb{R}e\ s > 1.$$

□

1.4. Ecuaciones Funcionales

Consideremos el caso $g = g_K = 0$. Entonces

$$Z_K(u) = \frac{1}{(1-u)(1-qu)} \quad \text{o} \quad \zeta_K(s) = \frac{1}{(1-q^{-s})(1-q^{1-s})}.$$

Se tiene:

$$\begin{aligned} q^{-s}\zeta_K(s) &= \frac{1}{(1-q^{-s})(q^s-q)} = \frac{1}{q^{-s}(q^s-1)q(q^{s-1}-1)} \\ &= q^{s-1}\frac{1}{(1-q^s)(1-q^{s-1})} = q^{s-1}\zeta_K(1-s). \end{aligned}$$

Es decir, $q^{-s}\zeta_K(s) = q^{s-1}\zeta_K(1-s)$, si $g = 0$.

Para $g > 0$, consideremos $u = q^{-s}$ y $Z_K(u) = \zeta_K(s)$.

Tenemos que $Z_K(u) = \dfrac{P_K(u)}{(1-u)(1-qu)}$, donde

$$P_K(u) = a_0 + a_1 u + \cdots + a_{2g}u^{2g}, a_0 = 1, a_{2g} = q^g.$$

Teorema 1.4.1. *Para* $0 \leq i \leq 2g$, *se cumple* $a_{2g-i} = a_i q^{g-i}$.

Demostración. Para $i = 0$, $a_{2g-0} = a_{2g} = q^g = a_0 q^{g-0}$.

En general tenemos $a_i = A_i - (q+1)A_{i-1} + qA_{i-2}$, donde A_i es el número de divisores enteros de grado i.

Recordemos, $A_i = \sum_{\substack{C \in C_K \\ d(C)=i}} \frac{q^{N(C)} - 1}{q-1}$.

Por el Teorema de Riemann-Roch [A.23], se tiene que

$$N(C) = d(C) - g + 1 + N(WC^{-1}) = i - g + 1 + N(WC^{-1}).$$

Ahora bien, $d(WC^{-1}) = 2g - 2 - i$ y cuando C recorre todas las clases de grado i, WC^{-1} recorre todas las clases de grado $2g - 2 - i$.

Como hay h clases de cada grado, con h el número de clases de K, se tiene que $(q-1)A_i = \sum_{d(C)=i} q^{N(C)} - \sum_{d(C)=i} 1 = \sum_{d(C)=i} q^{N(C)} - h$.

Así,

$$\begin{aligned}(q-1)A_i + h &= \sum_{d(C)=i} q^{N(C)} = \sum_{d(C)=i} q^{i-g+1+N(WC^{-1})} \\ &= q^{i-g+1} \sum_{d(C)=i} q^{N(WC^{-1})} = q^{i-g+1} \sum_{d(C)=2g-2-i} q^{N(C)} \\ &= q^{i-g+1}((q-1)A_{2g-2-i} + h).\end{aligned}$$

Por lo tanto

$$(q-1)A_{2g-2-i} = \frac{(q-1)A_i + h}{q^{i-g+1}} - h,$$

$$(q-1)A_{2g-1-i} = (q-1)A_{2g-2-(i-1)} = \frac{(q-1)A_{i-1} + h}{q^{i-g}} - h,$$

$$(q-1)A_{2g-i} = (q-1)A_{2g-2-(i-2)} = \frac{(q-1)A_{i-2} + h}{q^{i-g-1}} - h.$$

Entonces

$$\begin{aligned}
a_{2g-i} &= A_{2g-i} - (q+1)A_{2g-i-1} + qA_{2g-i-2} \\
&= \frac{1}{(q-1)}\left[\left(\frac{(q-1)A_{i-2}+h}{q^{i-g-1}} - h\right)\right. \\
&\quad \left. -(q+1)\left(\frac{(q-1)A_{i-1}+h}{q^{i-g}} - h\right) + q\left(\frac{(q-1)A_i+h}{q^{i-g+1}} - h\right)\right] \\
&= q^{g-i}(qA_{i-2} - (q+1)A_{i-1} + A_i) \\
&\quad + \frac{h}{q-1}\left(\frac{1}{q^{i-g-1}} - 1 - \frac{(q+1)}{q^{i-g}} + (q+1) + \frac{q}{q^{i-g+1}} - q\right) \\
&= q^{g-i}a_i \\
&\quad + \frac{h}{q-1}\left(\frac{1}{q^{i-g-1}} - 1 - \frac{1}{q^{i-g-1}} - \frac{1}{q^{i-g}} + q + 1 + \frac{1}{q^{i-g}} - q\right) \\
&= q^{g-i}a_i.
\end{aligned}$$

□

Corolario 1.4.2. *Se tiene que*

$$P_K\left(\frac{1}{qu}\right) = q^{-g}u^{-2g}P_K(u), \qquad u^{1-g}Z_K(u) = (qu)^{g-1}Z_K\left(\frac{1}{qu}\right).$$

Demostración. Tenemos:

$$\begin{aligned}
P_K\left(\frac{1}{qu}\right) &= a_0 + a_1\left(\frac{1}{qu}\right) + \cdots + a_{2g}\left(\frac{1}{qu}\right)^{2g} \\
&= \frac{1}{(qu)^{2g}}\sum_{i=0}^{2g} a_i(qu)^{2g-i} = q^{-2g}u^{-2g}\sum_{i=0}^{2g} a_i q^{g+g-i}u^{2g-i} \\
&= q^{-g}u^{-2g}\sum_{i=0}^{2g} a_i q^{g-i}u^{2g-i} = q^{-g}u^{-2g}\sum_{i=0}^{2g} a_{2g-i}u^{2g-i} \\
&= q^{-g}u^{-2g}P_K(u).
\end{aligned}$$

También:

$$\begin{aligned}
Z_K\left(\frac{1}{qu}\right) &= \frac{P_K\left(\frac{1}{qu}\right)}{\left(1-\frac{1}{qu}\right)\left(1-\frac{q}{qu}\right)} = \frac{q^{-g}u^{-2g}P_K(u)}{\left(\frac{qu-1}{qu}\right)\left(\frac{qu-q}{qu}\right)} \\
&= \frac{q^{-g}u^{-2g}P_K(u)}{\frac{q}{(qu)^2}(qu-1)(u-1)} = \frac{q^{-g}u^{-2g}P_K(u)}{\frac{1}{qu^2}(qu-1)(u-1)} \\
&= \frac{q^{-g}u^{-2g}P_K(u)}{(qu-1)(u-1)}qu^2 = q^{1-g}u^{2(1-g)}\frac{P_K(u)}{(1-u)(1-qu)} \\
&= q^{1-g}u^{2(1-g)}Z_K(u).
\end{aligned}$$

□

El Corolario 1.4.2 es la ecuación funcional de la función zeta en términos de la variable $u = q^{-s}$. Se tiene que $\zeta_K(s) = Z_K(q^{-s})$ y por lo tanto, en términos de la variable s, tenemos:

Teorema 1.4.3. *(Ecuación Funcional para la Función Zeta) Se tiene:*

$$q^{s(g-1)}\zeta_K(s) = q^{(1-s)(g-1)}\zeta_K(1-s), \quad \textit{para} \quad s \in \mathbb{C}.$$

En particular, $\zeta_K(s)$ es una función meromorfa en todo el plano complejo $\mathbb{C}$, con polos simples en

$$\left\{ s \mid q^{-s} = u \in \left\{1, \frac{1}{q}\right\}\right\} = \left\{ a + \frac{2\pi j}{\ln q} i \middle| j \in \mathbb{Z}, a = 0, 1 \right\}.$$

Demostración. Sea $u = q^{-s}$. Entonces

$$\begin{aligned} q^{s(g-1)}\zeta_K(s) &= u^{1-g}Z_K(u) = (qu)^{g-1}Z_K\left(\frac{1}{qu}\right) \\ &= q^{(1-s)(g-1)}Z_K(q^{s-1}) = q^{(1-s)(g-1)}\zeta_K(1-s). \end{aligned}$$

Ahora, en $Z_K(u) = \dfrac{P_K(u)}{(1-u)(1-qu)}$, el denominador se hace cero en $u = 1$ y en $u = \dfrac{1}{q}$. Por otro lado, $P_K(1) = h \neq 0$ (Corolario 1.3.9) y $P_K\left(\dfrac{1}{q}\right) = q^{-g}P_K(1) = q^{-g}h \neq 0$ (Corolario 1.4.2).

Entonces

$$\begin{aligned} \lim_{u\to q^{-1}}(u - q^{-1})Z_K(u) &= \lim_{u\to q^{-1}}\left(\frac{uq-1}{q}\right)Z_K(u) \\ &= \lim_{u\to q^{-1}} -q^{-1}(1-uq)Z_K(u) \\ &= \lim_{u\to q^{-1}}\left(\frac{-1}{q}\right)\left(\frac{(1-uq)P_K(u)}{(1-u)(1-uq)}\right) \\ &= \lim_{u\to q^{-1}}\left(\frac{-1}{q}\right)\left(\frac{P_K(u)}{1-u}\right) \\ &= \left(\frac{-1}{q}\right)\left(\frac{P_K\left(\frac{1}{q}\right)}{\left(1-\frac{1}{q}\right)}\right) = \frac{-P_K\left(\frac{1}{q}\right)}{q-1} = \frac{-q^{-g}P_K(1)}{q-1} \\ &= \frac{-q^{-g}h}{q-1} = \frac{-h}{q^g(q-1)} = \frac{-h}{q^{g+1}-q^g} \neq 0 \end{aligned}$$

es decir $\lim_{u\to q^{-1}}(u-q^{-1})Z_K(u)$ existe y es diferente de cero.

También,

$$\begin{aligned}\lim_{u\to 1}(u-1)Z_K(u) &= \lim_{u\to 1}\frac{(u-1)P_K(u)}{(1-u)(1-uq)} = \lim_{u\to 1}\frac{-(1-u)P_K(u)}{(1-u)(1-uq)}\\ &= \lim_{u\to 1}\frac{-P_K(u)}{(1-uq)} = \frac{-P_K(1)}{1-q} = \frac{-h}{1-q} = \frac{h}{q-1}\neq 0\end{aligned}$$

es decir $\lim_{u\to 1}(u-1)Z_K(u)$ existe y es diferente de cero.

Por lo tanto, $u=1$ y $u=q^{-1}$ son los únicos polos de $Z_K(u)$ y son simples.

En términos de la variable s tenemos:

$u=q^{-s}=1\Leftrightarrow q^s=e^{s\ln q}=1\Leftrightarrow s\ln q=2\pi ji,\ j\in\mathbb{Z}$

$\Leftrightarrow s=\dfrac{2\pi j}{\ln q}i,\ j\in\mathbb{Z},$

$u=q^{-s}=q^{-1}\Leftrightarrow q^s=q\Leftrightarrow q^{(s-1)}=1\Leftrightarrow e^{(s-1)\ln q}=1$

$\Leftrightarrow (s-1)\ln q=2\pi ji,\ j\in\mathbb{Z}\Leftrightarrow s=\dfrac{2\pi j}{\ln q}i+1,\ j\in\mathbb{Z}.$

□

Volviendo a las series L, sea χ un caracter de orden finito.

Proposición 1.4.4. *Si $\chi(C_{K,0})=1$, entonces*

$$L(s,\chi,K)=\zeta_K\left(s-\frac{2\pi i\alpha}{\ln q}\right),$$

donde C_0 es una clase de grado 1 y $\chi(C_0)=e^{2\pi i\alpha}$. Equivalentemente,

$$L(s,\chi,K)=Z_K(e^{2\pi i\alpha}u).$$

Demostración. Se tiene que $C_K\cong C_{K,0}\bigoplus\langle C_0\rangle$ con la identificación siguiente; si C es una clase arbitraria de grado n, $C=CC_0^{-n}C_0^n$. Entonces

$$\chi(C)=\chi(CC_0^{-n})\chi(C_0^n)=\chi(C_0)^n=e^{2\pi i\alpha n}.$$

Luego:

$$\begin{aligned} L(s,\chi,K) &= \sum_{\mathfrak{A}\text{ entero}} \frac{\chi(\mathfrak{A})}{\big(N(\mathfrak{A})\big)^s} = \sum_{C'\,\in\, C_{K,0}} \sum_{\substack{\mathfrak{A}\,\in\, C'C_0^n \\ \mathfrak{A}\text{ entero}}} \sum_{n=0}^{\infty} \frac{\chi(\mathfrak{A})}{\big(N(\mathfrak{A})\big)^s} \\ &= \sum_{C'\,\in\, C_{K,0}} \sum_{\substack{\mathfrak{A}\,\in\, C'C_0^n \\ \mathfrak{A}\text{ entero}}} \sum_{n=0}^{\infty} e^{2\pi i\alpha n} q^{-ns} \\ &= \sum_{C'\,\in\, C_{K,0}} \sum_{\substack{\mathfrak{A}\,\in\, C'C_0^n \\ \mathfrak{A}\text{ entero}}} \sum_{n=0}^{\infty} q^{\left(\frac{2\pi i\alpha}{\ln q} - s\right)n} \\ &= \sum_{\mathfrak{A}\text{ entero}} \frac{1}{N(\mathfrak{A})^{\left(s-\frac{2\pi i\alpha}{\ln q}\right)}} = \sum_{\mathfrak{A}\text{ entero}} \big(N(\mathfrak{A})\big)^{-\left(s-\frac{2\pi i\alpha}{\ln q}\right)} \\ &= \zeta_K\left(s - \frac{2\pi i\alpha}{\ln q}\right). \end{aligned}$$

En este desarrollo hemos usado que,

$$q^{\frac{2\pi i\alpha}{\ln q}} = e^{\ln q\,\frac{2\pi i\alpha}{\ln q}} = e^{\frac{2\pi i\alpha}{\ln q}\ln q} = e^{2\pi i\alpha}.$$

También que,

$$\zeta_K\left(s - \frac{2\pi i\alpha}{\ln q}\right) = Z_K\left(q^{-s} q^{\frac{2\pi i\alpha}{\ln q}}\right) = Z_K\big(e^{2\pi i\alpha} u\big).$$

□

Corolario 1.4.5. *Si $\chi(C_{K,0}) = 1$, entonces la serie L satisface la ecuación funcional:*

$$q^{s(g-1)} L(s,\chi,K) = \chi(W) q^{(1-s)(g-1)} L(1-s,\overline{\chi},K),$$

donde W es la clase canónica y $\overline{\chi}$ es el conjugado de χ, es decir,
$\overline{\chi}(\mathfrak{A}) := \overline{\chi(\mathfrak{A})} = \chi(\mathfrak{A}^{-1})$.

Demostración. Utilizando la notación de la Proposición 1.4.4 y la ecuación

funcional del Corolario 1.4.2, tenemos con $u' = e^{2\pi i\alpha}u$,

$$\begin{aligned} q^{s(g-1)}L(s,\chi,K) &= q^{s(g-1)}Z_K(u') = q^{s(g-1)}q^{g-1}(u')^{2(g-1)}Z_K\left(\frac{1}{qu'}\right) \\ &= q^{(s+1)(g-1)}q^{-s(2g-2)}(e^{2\pi i\alpha})^{2g-2}Z_K\left(\frac{1}{qu}e^{-2\pi i\alpha}\right) \\ &= q^{(s+1)(g-1)-2s(g-1)}(e^{2\pi i\alpha})^{2g-2}Z_K\left(\frac{e^{-2\pi i\alpha}}{qu}\right) \\ &= q^{(1-s)(g-1)}(e^{2\pi i\alpha})^{2g-2}Z_K\left(\frac{e^{-2\pi i\alpha}}{qu}\right), \end{aligned}$$

utilizando que $(u')^{2(g-1)} = u^{2(g-1)}(e^{2\pi i\alpha})^{2g-2} = q^{-s(2g-2)}(e^{2\pi i\alpha})^{2g-2}$.

Puesto que $d(W) = 2g-2$, $\chi(W) = (e^{2\pi i\alpha})^{2g-2}$, $\overline{\chi}(C_0) = e^{-2\pi i\alpha}$, se tiene:

$$\begin{aligned} q^{s(g-1)}L(s,\chi,K) &= q^{(1-s)(g-1)}\chi(W)Z_K\left(q^{s-1-\frac{2\pi i\alpha}{\ln q}}\right) \\ &= q^{(1-s)(g-1)}\chi(W)\zeta_K\left(1-s+\frac{2\pi i\alpha}{\ln q}\right) \end{aligned}$$

y $L(1-s,\overline{\chi},K) = \zeta_K\left(1-s-\left(-\frac{2\pi i\alpha}{\ln q}\right)\right) = \zeta_K\left(1-s+\frac{2\pi i\alpha}{\ln q}\right)$, de donde, $q^{s(g-1)}L(s,\chi,K) = q^{(1-s)(g-1)}\chi(W)L(1-s,\overline{\chi},K)$.

□

La ecuación funcional del Corolario 1.4.5 se cumple para cualquier caracter de orden finito. Sin embargo necesitamos dar una demostración diferente a la dada para el caso $\chi(C_{K,0}) = 1$.

Sea χ tal que $\chi(C_{K,0}) \neq 1$. Entonces $C_{K,0} \neq \{1\}$ y por lo tanto $g > 0$ (Proposición A.27). Sea C_0' una clase de grado 0 tal que $\chi(C_0') \neq 1$. Entonces tenemos,

$$\chi(C_0')\sum_{C_0 \in C_{K,0}}\chi(C_0) = \sum_{C_0 \in C_{K,0}}\chi(C_0'C_0) = \sum_{C_0 \in C_{K,0}}\chi(C_0),$$

es decir, $\big(\chi(C_0')-1\big)\left(\sum_{C_0 \in C_{K,0}}\chi(C_0)\right) = 0$, y puesto que, $\chi(C_0') \neq 1$, se sigue que, $\sum_{C_0 \in C_{K,0}}\chi(C_0) = 0$.

Sea C_1 una clase de grado 1. Entonces

$$\begin{aligned}
(q-1)L(s,\chi,K) &= (q-1)\sum_{\mathfrak{A}\text{ entero}} \chi(\mathfrak{A})\frac{1}{\left(N(\mathfrak{A})\right)^s} \\
&= \sum_{d(C)=0}^{\infty} (q-1)\left(\frac{q^{N(C)}-1}{q-1}\chi(C)q^{-d(C)s}\right) \\
&= \sum_{n=0}^{\infty}\sum_{C_0\,\in\, C_{K,0}} \chi(C_0C_1^n)q^{-ns}\left(q^{N(C_0C_1^n)}-1\right) \\
&= \sum_{C_0\,\in\, C_{K,0}} \chi(C_0)\sum_{n=0}^{\infty}\chi(C_1)^n\left(q^{N(C_0C_1^n)}-1\right)q^{-ns} \\
&= \sum_{C_0\,\in\, C_{K,0}} \chi(C_0)\sum_{n=0}^{2g-2}\chi(C_1)^n\left(q^{N(C_0C_1^n)}-1\right)q^{-ns} \\
&\quad + \sum_{C_0\,\in\, C_{K,0}} \chi(C_0)\sum_{n=2g-1}^{\infty}\chi(C_1)^n\left(q^{N(C_0C_1^n)}-1\right)q^{-ns}.
\end{aligned}$$

La segunda suma se hace 0 pues $\displaystyle\sum_{C_0\,\in\, C_{K,0}} \chi(C_0) = 0$. Por lo tanto

$$\begin{aligned}
(q-1)L(s,\chi,K) &= \sum_{C_0\,\in\, C_{K,0}} \chi(C_0)\sum_{n=0}^{2g-2}\chi(C_1)^n q^{N(C_0C_1^n)}q^{-ns} \\
&\quad - \sum_{C_0\,\in\, C_{K,0}} \chi(C_0)\sum_{n=0}^{2g-2}\chi(C_1)^n q^{-ns}.
\end{aligned}$$

Otra vez usando que $\displaystyle\sum_{C_0\,\in\, C_{K,0}} \chi(C_0) = 0$, obtenemos:

$$(q-1)L(s,\chi,K) = \sum_{C_0\,\in\, C_{K,0}} \chi(C_0)\sum_{n=0}^{2g-2}\chi(C_1)^n q^{N(C_0C_1^n)}q^{-ns}.$$

Poniendo $u = q^{-s}$, obtenemos:

$$(q-1)L(s,\chi,K) = \sum_{d(C)=0}^{2g-2} \chi(C)q^{N(C)}u^{d(C)},$$

el cual es un polinomio en u de grado $\leq 2g-2$.

Ahora, el coeficiente de u^{2g-2} es,

$$a = \sum_{d(C)=2g-2} \chi(C) q^{N(C)} = \sum_{C_0 \in C_{K,0}} \chi(WC_0) q^{N(WC_0)}.$$

Por el Teorema de Riemann-Roch [A.23] obtenemos:
$N(WC_0) = d(WC_0) - g + 1 + N(C_0^{-1})$ y $N(C_0^{-1}) = 0$, si $C_0 \neq P_K$, $N(P_K) = 1$, por lo que, $N(WC_0) = 2g - 2 - g + 1 = g - 1$, si $C_0 \neq P_K$ y $N(W) = g$.

Por lo tanto

$$\begin{aligned} a &= \sum_{\substack{C_0 \in C_{K,0} \\ C_0 \neq P_K}} \chi(W)\chi(C_0) q^{g-1} + \chi(W) q^g \\ &= \chi(W) \sum_{C_0 \in C_{K,0}} \chi(C_0) q^{g-1} + \chi(W)(q^g - q^{g-1}) \\ &= q^{g-1}(q-1)\chi(W) \neq 0. \end{aligned}$$

Luego $(q-1)L(s,\chi,K)$ es un polinomio de grado $2g-2$ y el coeficiente líder es $(q-1)\chi(W)q^{g-1}$.

Aplicando nuevamente el Teorema de Riemann-Roch [A.23] obtenemos:

$$\begin{aligned} &(q-1)L(s,\chi,K) = \sum_{d(C)=0}^{2g-2} \chi(C) q^{N(C)} u^{d(C)} \\ &= \sum_{d(C)=0}^{2g-2} \chi(C) q^{d(C)-g+1+N(WC^{-1})} u^{d(C)} \\ &= q^{g-1}u^{2g-2}\chi(W) \sum_{d(C)=0}^{2g-2} \chi(CW^{-1}) q^{-2g+2+d(C)+N(WC^{-1})} u^{d(C)-2g+2} \\ &= q^{g-1}u^{2g-2}\chi(W) \sum_{d(C)=0}^{2g-2} \overline{\chi(WC^{-1})} q^{d(W^{-1}C)+N(WC^{-1})} u^{d(W^{-1}C)} \\ &= q^{g-1}u^{2g-2}\chi(W) \sum_{d(C)=0}^{2g-2} \overline{\chi(WC^{-1})} q^{N(WC^{-1})} \left(\frac{1}{qu}\right)^{d(WC^{-1})} \\ &= q^{g-1}u^{2g-2}\chi(W) \sum_{d(C)=0}^{2g-2} \overline{\chi}(C) q^{N(C)} \left(\frac{1}{qu}\right)^{d(C)} \\ &= q^{g-1}u^{2g-2}\chi(W)(q-1)L(1-s,\overline{\chi},K) \\ &= q^{g-1}q^{-2s(g-1)}(q-1)\chi(W)L(1-s,\overline{\chi},K). \end{aligned}$$

Por lo tanto $L(s,\chi,K) = q^{(g-1)(1-2s)}\chi(W)L(1-s,\overline{\chi},K)$, o de otra manera $q^{s(g-1)}L(s,\chi,K) = q^{(1-s)(g-1)}\chi(W)L(1-s,\overline{\chi},K)$.

Resumiendo, tenemos:

Teorema 1.4.6. *(Ecuación Funcional para las Series L) En un campo de funciones congruente K/k, $|k| = q$, sea W la clase canónica. Sea χ un caracter de orden finito. Entonces*

$$q^{s(g-1)}L(s,\chi,K) = \chi(W)q^{(1-s)(g-1)}L(1-s,\overline{\chi},K).$$

□

Finalizamos este capítulo relacionando las series L con la función zeta de una extensión de constantes.

Sean K/k un campo de funciones congruente, $k = \mathbb{F}_q$ y sean $l = \mathbb{F}_{q^r}$, $L = Kl$. Sea χ_j el caracter de K tal que $\chi_j(C) = e^{\frac{2\pi ij}{r}}$ en todas las clases C de grado 1, por lo tanto $\chi_j(C_{K,0}) = 1$, $j = 1,\ldots,r$. Entonces tenemos el siguiente resultado:

Teorema 1.4.7.

$$\zeta_L(s) = \prod_{j=1}^{r} L(s,\chi_j,K).$$

Demostración. Primero notemos que si $a, b \in \mathbb{N}$, entonces se tiene

$$\prod_{n=1}^{a}\left(1 - e^{\frac{2\pi inb}{a}}z\right) = \left(1 - z^{\frac{a}{(a,b)}}\right)^{(a,b)}.$$

En efecto, las raíces de

$$\prod_{n=1}^{a}\left(1 - e^{\frac{2\pi inb}{a}}z\right)$$

son $z = e^{\frac{-2\pi inb}{a}}$, $n = 1,\ldots,a$.

Si $d = (a,b)$, entonces, $\dfrac{2\pi inb}{a} = \dfrac{2\pi indb_1}{da_1} = \dfrac{2\pi inb_1}{a_1}$, con $a = da_1$, $b = db_1$, $(a_1,b_1) = 1$. Se tiene el conjunto de índices

$$\{1,2,\ldots,a\} = \{1,\ldots,a_1,a_1+1,\ldots,2a_1,\ldots,(d-1)a_1+1,\ldots,da_1 = a\}$$

y

$$\frac{2\pi i(a_1+t)b_1}{a_1} = 2\pi i b_1 + \frac{2\pi i t b_1}{a_1}, \;\; 1 \leq t \leq a_1$$

de aquí que,

$$e^{\frac{-2\pi i(a_1+t)b_1}{a_1}} = e^{-2\pi i b_1} e^{\frac{-2\pi i t b_1}{a_1}}$$

pero, $e^{-2\pi i b_1} = \cos(-2\pi b_1) + i\sin(-2\pi b_1) = 1 + 0$, por lo que,

$$e^{\frac{-2\pi i(a_1+t)b_1}{a_1}} = e^{\frac{-2\pi i t b_1}{a_1}},$$

es decir, las raíces se repiten exactamente d veces y éstas son

$$\left\{ e^{\frac{-2\pi i t b_1}{a_1}} \right\}_{t=1}^{a_1}$$

las cuales son a_1-raíces de 1. Se tiene

$$e^{\frac{-2\pi i t b_1}{a_1}} = e^{\frac{-2\pi i t b}{a}}, t = 1, \ldots, a_1 = \frac{a}{d} = \frac{a}{(a,b)}.$$

Ahora,

$$\begin{aligned} \zeta_L(s) &= \prod_{\mathcal{P} \in \mathbb{P}_L} \left(1 - \frac{1}{(N(\mathcal{P}))^s}\right)^{-1} = \prod_{\mathfrak{P} \in \mathbb{P}_K} \prod_{\mathcal{P}|\mathfrak{P}} \left(1 - q^{-srd_L(\mathcal{P})}\right)^{-1} \\ &= \prod_{\mathfrak{P} \in \mathbb{P}_K} \prod_{\mathcal{P}|\mathfrak{P}} \left(1 - q^{-s\frac{rd_K(\mathfrak{P})}{(d_K(\mathfrak{P}),r)}}\right)^{-1} \qquad \text{(Teorema 1.2.1).} \end{aligned}$$

Hay $(r, d_K(\mathfrak{P}))$ factores $\mathcal{P}|\mathfrak{P}$, por lo tanto

$$\begin{aligned}
\zeta_L(s) &= \prod_{\mathfrak{P}\,\in\,\mathbb{P}_K} \left\{1-\big(N(\mathfrak{P})\big)^{-s\frac{r}{(r,d_K(\mathfrak{P}))}}\right\}^{-\left(r,d_K(\mathfrak{P})\right)} \\
&= \prod_{\mathfrak{P}\,\in\,\mathbb{P}_K}\prod_{n=1}^{r}\left(1-\frac{1}{\big(N(\mathfrak{P})\big)^{s}}e^{\frac{2\pi i n}{r}d_K(\mathfrak{P})}\right)^{-1} \\
&= \prod_{n=1}^{r}\left[\prod_{\mathfrak{P}\,\in\,\mathbb{P}_K}\left(1-\frac{e^{\frac{2\pi i n}{r}d_K(\mathfrak{P})}}{\big(N(\mathfrak{P})\big)^{s}}\right)^{-1}\right] \\
&= \prod_{n=1}^{r}\left[\prod_{\mathfrak{P}\,\in\,\mathbb{P}_K}\left(1-\big(N(\mathfrak{P})\big)^{-s}q^{d_K(\mathfrak{P})\frac{2\pi i n}{r\ln q}}\right)^{-1}\right] \\
&= \prod_{n=1}^{r}\left[\prod_{\mathfrak{P}\,\in\,\mathbb{P}_K}\left(1-\big(N(\mathfrak{P})\big)^{-\left(s-\frac{2\pi i n}{r\ln q}\right)}\right)^{-1}\right] \\
&= \prod_{n=1}^{r}\zeta_K\left(s-\frac{2\pi i n}{r\ln q}\right) = \prod_{n=1}^{r}L(s,\chi_n,K) \quad \text{(Proposición 1.4.4).}
\end{aligned}$$

□

Ejemplo 1.4.8. Sea k un campo finito con $|k| = q$. Sea K un campo de funciones elípticas sobre k con número de clases h. Entonces

$$\zeta_K(s) = \frac{1+\big(h-(q+1)\big)q^{-s}+q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}.$$

Demostración. Sea K un campo de funciones elípticas sobre k, entonces $g_K = g = 1$.

Por otro lado tenemos que $u = q^{-s}$ y

$$\zeta_K(s) = Z_K(u) = \frac{P_K(u)}{(1-u)(1-qu)},$$

con $P_K(u) \in \mathbb{Z}[u]$ un polinomio de grado $2g = 2$, de aquí que $P_K(u) = a_0 + a_1u + a_2u^2$, con $a_0 = 1$, $a_1 = A_1 - (q+1)$ y $a_2 = q^g = q$, pero

$$A_1 = h\left(\frac{q^{1-g+1}-1}{q-1}\right) = h\left(\frac{q^{1-1+1}-1}{q-1}\right) = h.$$

De aquí que

$$Z_K(u) = \frac{1+\big(h-(q+1)\big)u+qu^2}{(1-u)(1-qu)}$$

$$\zeta_K(s) = \frac{1 + \big(h - (q+1)\big)q^{-s} + qq^{-2s}}{(1-q^{-s})(1-qq^{-s})}.$$

Por lo tanto

$$\zeta_K(s) = \frac{1 + \big(h - (q+1)\big)q^{-s} + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}.$$

□

Ejemplo 1.4.9. Sean k un campo finito, con $|k| = q$ y $K = k(x,y)$ con $y^m = x$, $m \in \mathbb{N}$. Entonces

$$\zeta_K(s) = \frac{1}{(1-q^{-s})(1-q^{1-s})}.$$

Demostración. Tenemos que si $y^m = x$, $m \in \mathbb{N}$, entonces $y = \sqrt[m]{x}$ de aquí que $K = k(x,y) = k(x, \sqrt[m]{x}) = k(\sqrt[m]{x})$, porque $x = (\sqrt[m]{x})^m$.

Entonces $K = k(\sqrt[m]{x})$ es un campo de funciones racionales sobre k, luego $g_K = g = 0$.

Por lo tanto

$$\zeta_K(s) = \frac{1}{(1-q^{-s})(1-q^{1-s})}.$$

□

Capítulo 2

Hipótesis de Riemann

En el capítulo anterior definimos la función zeta de un campo de funciones. Esta defínción proviene de la extensión natural de la función usual de Riemann:

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

Se sabe que $\zeta(s)$ tiene una extensión meromorfa al plano complejo, con un único polo en $s = 1$, el cual es simple con residuo 1. Más aún, $\zeta(s)$ tiene ceros en $s = -2n$, $n \in \mathbb{N}$ y éstos son llamados los ceros triviales de $\zeta(s)$. Por otro lado, $\zeta(s)$ no tiene ceros diferentes a los triviales en $\mathbb{C}\backslash\{s \mid 0 \leq \mathbb{R}e\ s \leq 1\}$. La Hipótesis de Riemann establece que los ceros de $\zeta(s)$, aparte de los triviales, están en la recta $\mathbb{R}e\ s = \frac{1}{2}$. Esto último sigue siendo un problema abierto. Sin embargo, para los campos de funciones la respuesta sí se conoce y es positiva. Esto fue demostrado por André Weil en 1941 y el objetivo principal de este capítulo es dar una demostración de la Hipótesis de Riemann para campos de funciones y algunas aplicaciones.

2.1. El Número de Divisores Primos de Grado 1

Sea $k = \mathbb{F}_q$ un campo finito. Uno de nuestros objetivos es estimar el número de divisores primos de grado n en el campo de funciones congruente

K/k. Para ello usaremos frecuentemente la Función μ de Möbius y las Identidades de Newton. En seguida las presentaremos y probaremos algunas de sus propiedades principales.

Definición 2.1.1. Una ***función aritmética*** en $\mathbb{Q}$ es cualquier función $f : \mathbb{N} \longrightarrow \mathbb{Q}$. La ***Función μ de Möbius*** es la función $\mu : \mathbb{N} \longrightarrow \mathbb{Q}$, donde, si $n = \prod_{i=1}^{r} p_i^{a_i}$ es su descomposición en primos, entonces

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^r & \text{si } a_1 = \ldots = a_r = 1, \\ 0 & \text{en cualquier otro caso.} \end{cases}$$

Lema 2.1.2. *Se tiene*

$$\sum_{d|n} \mu(d) = \varepsilon(n) = \begin{cases} 1 & si\, n = 1, \\ 0 & si\, n > 1. \end{cases}$$

Demostración. Si $n = 1$, $\quad \sum_{d|1} \mu(d) = \varepsilon(1) = 1.$

Si $n > 1$, $n = \prod_{i=1}^{r} p_i^{a_i}$, con $r \geq 1$, p_i primo, $a_i \geq 1$.

$$\begin{aligned}
\sum_{d|n}\mu(d) &= \mu(1) + \sum_{\substack{d|n \\ d \text{ producto de primos distintos}}} \mu(d) \\
&= \mu(1) + \sum_{p_{i_1}|n}\mu(p_{i_1}) + \sum_{p_{i_1}p_{i_2}|n}\mu(p_{i_1}p_{i_2}) + \ldots + \\
&\quad \sum_{p_{i_1}p_{i_2}\cdots p_{i_{r-1}}|n}\mu(p_{i_1}p_{i_2}\cdots p_{i_{r-1}}) \\
&\quad + \sum_{p_{i_1}p_{i_2}\cdots p_{i_{r-1}}p_{i_r}|n}\mu(p_{i_1}p_{i_2}\cdots p_{i_{r-1}}p_{i_r}) \\
&= \binom{r}{0}(-1)^0 + \binom{r}{1}(-1)^1 + \binom{r}{2}(-1)^2 + \cdots + \\
&\quad \binom{r}{r-1}(-1)^{r-1} + \binom{r}{r}(-1)^r \\
&= \sum_{m=0}^{r}\binom{r}{m}(-1)^m \\
&= \big(1+(-1)\big)^r = 0.
\end{aligned}$$

□

Teorema 2.1.3. *(Fórmula de Inversión de Möbius) Sean f, g dos funciones aritméticas tales que*

$$g(n) = \sum_{d|n} f(d)$$

para $n \in \mathbb{N}$. Entonces

$$f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} g\left(\frac{n}{d}\right)\mu(d).$$

Demostración. Para dos funciones aritméticas h y k cualesquiera definimos el producto $h * k$ por

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

Éste es el llamado ***producto de convolución***. El conjunto de las funciones aritméticas junto con $*$ es un anillo conmutativo con elemento identidad ε.

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

Además, si denotamos por 1 a la función constante con valor 1, se tiene del Lema 2.1.2 que

$$(\mu * 1)(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) 1(d) = \sum_{d|n} \mu(d) 1\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) = \varepsilon(n),$$

es decir, $\mu = 1^{-1}$. Ahora bien, se tiene que

$$g(n) = \sum_{d|n} f(d),$$

es decir, $g = f * 1$, por lo que $f = g * 1^{-1} = g * \mu$, es decir,

$$f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right).$$

□

Ahora sean k cualquier campo y $K = k(X_1, X_2, \ldots, X_n)$ el campo de funciones racionales en n variables y sea $f(T) = \prod_{i=1}^{n}(T - X_i) \in K[T]$. Entonces

$$f(T) = T^n - \sigma_1 T^{n-1} + \sigma_2 T^{n-2} - \ldots + (-1)^s \sigma_s T^{n-s} + \ldots + (-1)^n \sigma_n,$$

donde σ_s es el s-ésimo polinomio elemental simétrico en $X_1, X_2, \ldots, X_n$, es decir,

$$\begin{aligned}
\sigma_0 &= 1 \\
\sigma_1 &= \sum_{i=1}^{n} X_i \\
\sigma_2 &= \sum_{i<j} X_i X_j \\
&\vdots \quad\quad \vdots \\
\sigma_s &= \sum_{i_1<\ldots<i_s} X_{i_1} \cdots X_{i_s} \\
&\vdots \quad\quad \vdots \\
\sigma_n &= X_1 \cdots X_n.
\end{aligned}$$

Sea $\rho_m = X_1^m + \ldots + X_n^m$, $m \geq 1$ y $\rho_0 = n$.

Teorema 2.1.4. *(Identidades de Newton) Se tiene:*

$$\rho_m - \rho_{m-1}\sigma_1 + \ldots + (-1)^{m-1}\rho_1\sigma_{m-1} + (-1)^m\sigma_m m = 0, \;\; 1 \leq m \leq n-1, y$$

$$\rho_m - \rho_{m-1}\sigma_1 + \ldots + (-1)^n\rho_{m-n}\sigma_n = 0, \;\; m \geq n.$$

Demostración. Consideremos las series $T^{1-n}f'(T)$ en el campo de las series de Laurent $K\big((T)\big)$ (K cualquier campo de característica 0). Tenemos:

$$\begin{aligned}
T^{1-n}f'(T) &= T^{1-n}f(T)\frac{f'(T)}{f(T)} \\
&= T^{1-n}\left(\sum_{i=0}^{n}(-1)^i\sigma_i T^{n-i}\right)\left(\sum_{i=1}^{n}\frac{1}{T-X_i}\right) \\
&= T\left(\sum_{i=0}^{n}(-1)^i\sigma_i T^{-i}\right)\left(\sum_{i=1}^{n}\sum_{m=0}^{\infty}X_i^m T^{-m-1}\right) \\
&= \left(\sum_{i=0}^{n}(-1)^i\sigma_i T^{-i}\right)\left(\sum_{m=0}^{\infty}\rho_m T^{-m}\right) \\
&= \sum_{m=0}^{\infty}\left(\sum_{s=0}^{m}(-1)^s\sigma_s\rho_{m-s}T^{-m}\right),
\end{aligned}$$

donde $\sigma_j = 0$, para $j > n$.

Por otro lado,

$$\begin{aligned}
T^{1-n}f'(T) &= T^{1-n}\left(\sum_{m=0}^{n-1}(n-m)(-1)^m\sigma_m T^{n-m-1}\right) \\
&= \sum_{m=0}^{n-1}(n-m)(-1)^m\sigma_m T^{-m}.
\end{aligned}$$

Igualando coeficientes en los desarrollos anteriores obtenemos las Identidades de Newton.

□

Proposición 2.1.5. *Sea $\psi(d)$ el número de polinomios mónicos irreducibles de grado d en $\mathbb{F}_q[T]$. Entonces*

$$\psi(n) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d.$$

Demostración. Se tiene que para $n \in \mathbb{N}$, el campo de descomposición de $X^{q^n} - X$ es $\mathbb{F}_{q^n}$. Si $f(x)$ es mónico irreducible de grado d, $d \mid n$, entonces $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$ y por lo tanto $f(x) \mid X^{q^n} - X$.

Recíprocamente, si $f(x) \mid X^{q^n} - X$ y $f(x)$ es mónico irreducible de grado d, entonces el campo de descomposición de $f(x)$, $\mathbb{F}_{q^d}$, está contenido en $\mathbb{F}_{q^n}$ y por lo tanto $d \mid n$.

Luego

$$X^{q^n} - X = \prod_{d|n} \prod_{\substack{\deg f = d \\ f \text{ mónico} \\ \text{irreducible}}} f(x).$$

Ahora, si contamos los grados obtenemos que, $q^n = \sum_{d|n} d\psi(d)$. Por la Fórmula de Inversión de Möbius aplicada a f y g, las dos funciones aritméticas definidas por $f(n) = n\psi(n)$ y $g(n) = q^n$ respectivamente, y consideramos además que $g(n) = q^n = \sum_{d|n} d\psi(d) = \sum_{d|n} f(d)$, para $n \in \mathbb{N}$, tenemos que,

$$n\psi(n) = f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

□

Recordamos que $k = \mathbb{F}_q$. Denotamos por k_r a $\mathbb{F}_{q^r}$, la extensión de grado $r \geq 1$ de k. Si K es un campo de funciones con campo de constantes k, K_r denota la extensión de constantes $Kk_r = K_r$ y K_r tiene a k_r como su campo exacto de constantes. Sean $Z_K(u) = \zeta_K(s)$ la función zeta de K, $u = q^{-s}$ y sean $Z_r(v) = \zeta_{K_r}(s)$ la función zeta de K_r, $v = (q^r)^{-s} = q^{-rs} = u^r$. Entonces, $Z_r(v) = Z_r(u^r)$.

El Teorema 1.4.7 prueba que $\zeta_{K_r}(s) = \prod_{j=1}^{r} L(s, \chi_j, K)$, donde χ_j es el caracter tal que $\chi_j(C) = \xi_r^j$ en todas las clases C de grado 1, $\xi_r = e^{\frac{2\pi i}{r}}$, $j = 1, \ldots, r$.

Ahora bien, por la Proposición 1.4.4

$$L(s, \chi_j, K) = \zeta_K\left(s - \frac{2\pi i j}{r \ln q}\right).$$

Se tiene

$$\zeta_K\left(s-\frac{2\pi ij}{r\ln q}\right)=Z_K\left(q^{-s}q^{\frac{2\pi ij}{r\ln q}}\right).$$

Puesto que, $q^{\frac{2\pi ij}{r\ln q}}=e^{\ln q\frac{2\pi ij}{r\ln q}}=e^{\frac{2\pi ij}{r}\ln q}=e^{\frac{2\pi ij}{r}}=\xi_r^j$, tenemos,

$$Z_r(u^r)=Z_r(v)=\zeta_{K_r}(s)=\prod_{j=1}^{r}L(s,\chi_j,K)=\prod_{j=1}^{r}Z_r(\xi_r^j u).$$

Es decir, hemos demostrado:

Teorema 2.1.6. *Si K_r es la extensión de constantes de grado r del campo K, se tiene*

$$Z_{K_r}(u^r)=\prod_{j=1}^{r}Z_K(\xi_r^j u),\ \textit{donde}\ u=q^{-s},\ \xi_r=e^{\frac{2\pi i}{r}}.$$

□

Si $K_0=\mathbb{F}_q(x)$, entonces tenemos $Z_0(u)=Z_{K_0}(u)=\dfrac{1}{(1-u)(1-qu)}$ y $Z_K(u)=\dfrac{P_K(u)}{(1-u)(1-qu)}=Z_0(u)P_K(u)$, de aquí que $P_K(u)=\dfrac{Z_K(u)}{Z_0(u)}$.

Ahora bien, $P_K(u)=\sum_{i=0}^{2g}a_iu^i$ con $a_{2g-i}=a_iq^{g-i}$, $0\le i\le 2g$, $a_0=1$, $a_{2g}=q^g$, $a_1=A_1-(q+1)$, con A_1 el número de divisores enteros de grado $1=$ número de divisores primos de grado 1. Se tiene $\deg(P_K(u))=2g$ y si $\omega_1^{-1},\ldots,\omega_{2g}^{-1}$ son las raíces de $P_K(u)$, entonces $P_K(u)=\prod_{i=1}^{2g}(1-\omega_iu)$.

Proposición 2.1.7. *Se tiene $q^g=\prod_{i=1}^{2g}\omega_i$, $N-(q+1)=-\sum_{i=1}^{2g}\omega_i$, donde N es el número de divisores primos de grado 1. Más aún,*

$$P_K(u)=0\Leftrightarrow P_K\left(\frac{1}{qu}\right)=0.$$

En particular, como

$$P_K(\omega_i^{-1})=0,\ \ \textit{tenemos}\ \ P_K\left(\frac{\omega_i}{q}\right)=0.$$

Demostración. De $P_K(u) = \sum_{i=0}^{2g} a_i u^i = \prod_{i=1}^{2g}(1-\omega_i u)$ se sigue que

$$q^g = a_{2g} = \prod_{i=1}^{2g}(-\omega_i) = \prod_{i=1}^{2g}\omega_i; \quad N-(q+1) = a_1 = -\sum_{i=1}^{2g}\omega_i.$$

Por otro lado, la ecuación funcional de $P_K(u)$ (Corolario 1.4.2) nos dice que $P_K\left(\frac{1}{qu}\right) = q^{-g}u^{-2g}P_K(u)$, por lo tanto

$$P_K(u) = 0 \Leftrightarrow P_K\left(\frac{1}{qu}\right) = 0.$$

Como ω_i^{-1} es raíz de $P_K(u)$ tenemos que $\frac{\omega_i}{q} = \frac{1}{q\omega_i^{-1}}$ también es raíz de $P_K(u)$.

□

Para $1 \leq i \leq 2g$, sea $\omega_i' = \frac{q}{\omega_i}$. Se tiene que $\omega_i' = \omega_i \Leftrightarrow \frac{1}{\omega_i} = \frac{\omega_i}{q} \Leftrightarrow \omega_i^2 = q \Leftrightarrow \omega_i = \pm\sqrt{q}$, por lo tanto podemos renumerar las inversas de las raíces de $P_K(u)$ como:

$$\omega_1, \omega_1', \ldots, \omega_f, \omega_f', \sqrt{q}, \ldots, \sqrt{q}, -\sqrt{q}, \ldots, -\sqrt{q}$$

con $f \leq g$, $\omega_i \neq \omega_i'$, $\omega_i\omega_i' = q$, $i = 1, \ldots, f$. Sea t el número de veces que aparece $\sqrt{q}$ y s el número de veces que aparece $-\sqrt{q}$, por lo que $2f+t+s = 2g$.

Puesto que $q^g = \prod_{i=1}^{2g}\omega_i$, se tiene $q^g = q^f q^{t/2}(-1)^s q^{s/2}$, se sigue que s es par y por lo tanto t también es par.

En particular podemos tomar $f = g$, esto es, las raíces de P_K son, $\omega_1, \omega_1', \ldots, \omega_g, \omega_g'$, donde $\omega_i\omega_i' = q$, $i = 1, \ldots, g$.

Así pues, tenemos $P_K(u) = \prod_{i=1}^{g}(1-\omega_i u)(1-\omega_i' u)$.

Teorema 2.1.8. *Las siguientes condiciones son equivalentes:*
(i) Los ceros de la función zeta $\zeta_K(s)$ están en la línea $\mathbb{R}e\, s = \frac{1}{2}$.

(*ii*) *Los ceros de la función* $Z_K(u)$ *están en el círculo* $|u| = q^{-1/2}$.

(*iii*) *Si* $\omega_1, \ldots, \omega_{2g}$ *son las inversas de las raíces de* $P_K(u)$, *entonces* $|\omega_i| = \sqrt{q}$, $i = 1, \ldots, 2g$.

Demostración.

$(i) \Leftrightarrow (ii)$. Se sigue del hecho de que $u = q^{-s}$, $|u| = q^{-\mathbb{R}e\, s}$, $Z_K(u) = \zeta_K(s)$.

$(ii) \Leftrightarrow (iii)$. Observemos que $Z_K(u) = \dfrac{P_K(u)}{(1-u)(1-qu)}$ y $P_K(1) = h_K \neq 0$, $P_K\left(\dfrac{1}{q}\right) = q^{-g} P_K(1) \neq 0$. Por lo tanto las raíces de $Z_K(u)$ son las raíces de $P_K(u)$ y éstas son ω_i^{-1}. Así que (ii) es equivalente a que $|\omega_i^{-1}| = |\omega_i|^{-1} = q^{-1/2}$, es decir, $|\omega_i| = \sqrt{q}$.

□

Nuestro objetivo es probar:

Hipótesis de Riemann. Las condiciones del Teorema 2.1.8 se cumplen para todo campo de funciones congruente.

La demostración se hará en varias etapas.

Proposición 2.1.9. *Sea* N *el número de divisores primos de grado 1 en* K. *Entonces, si la Hipótesis de Riemann se cumple,* $|N - (q+1)| \leq 2g\sqrt{q}$.

Demostración. Se tiene que $N - (q+1) = -\sum_{i=1}^{2g} \omega_i$ (Proposición 2.1.7), por lo que

$$|N - (q+1)| \leq \sum_{i=1}^{2g} |\omega_i| = 2g\sqrt{q}.$$

□

Proposición 2.1.10. *Sea* $r \in \mathbb{N}$. *La Hipótesis de Riemann se cumple para el campo* $K \Leftrightarrow$ *se cumple para el campo* K_r.

Demostración. Se tiene por el Teorema 2.1.6 y el comentario que le sigue

que

$$\begin{aligned} P_{K_r}(u^r) &= \frac{Z_{K_r}(u^r)}{Z_{0,K_r}(u^r)} = \prod_{j=1}^{r} \frac{Z_K(\xi_r^j u)}{Z_0(\xi_r^j u)} = \prod_{j=1}^{r} P_K(\xi_r^j u) \\ &= \prod_{j=1}^{r}\prod_{i=1}^{2g}(1-\omega_i\xi_r^j u) = \prod_{i=1}^{2g}(1-\omega_i^r u^r). \end{aligned}$$

Así, $P_{K_r}(u^r) = \prod_{i=1}^{2g}(1-\omega_i^r u^r)$ y por lo tanto $\omega_1^r, \ldots, \omega_{2g}^r$ son los inversos de los ceros de $P_{K_r}(u^r)$. Así pues, $|\omega_i| = \sqrt{q} \Leftrightarrow |\omega_i^r| = \sqrt{q^r}$, observando que $q^r = |\mathbb{F}_{q^r}|$ y $\mathbb{F}_{q^r}$ es el campo de constantes de K_r.

□

Sea N_r el número de divisores primos de grado 1 en K_r. Entonces:

Proposición 2.1.11. *Si existe $c > 0$ tal que $|N_r - (q^r + 1)| \leq cq^{r/2}$ para todo r, entonces la Hipótesis de Riemann se cumple para K.*

Demostración. Sea $P_K(u) = \prod_{i=1}^{2g}(1-\omega_i u)$.

Aplicando el operador $D = -u\frac{d}{du}\ln$ a ambos lados tenemos:

$$\begin{aligned} D\big(P_K(u)\big) &= -u\frac{d}{du}\ln\left(\prod_{i=1}^{2g}(1-\omega_i u)\right) = -u\left(\sum_{i=1}^{2g}\frac{d}{du}\ln(1-\omega_i u)\right) \\ &= \sum_{i=1}^{2g}\frac{\omega_i u}{1-\omega_i u} = \sum_{i=1}^{2g}\sum_{n=1}^{\infty}\omega_i^n u^n = \sum_{n=1}^{\infty}\left(\sum_{i=1}^{2g}\omega_i^n\right)u^n. \end{aligned}$$

Se tiene (Proposición 2.1.7) que $-\sum_{i=1}^{2g}\omega_i^n = N_n - (q^n+1)$. Nuestra hipótesis implica que:

$$\left|\sum_{i=1}^{2g}\omega_i^n\right| = |N_n - (q^n+1)| \leq cq^{n/2}.$$

Por lo tanto, si R es el radio de convergencia de la serie $\sum_{n=1}^{\infty}\left(\sum_{i=1}^{2g}\omega_i^n\right)u^n$,

se tiene que $R = \lim\limits_{n\to\infty} \sup \left(\left| \sum_{i=1}^{2g} \omega_i^n \right| \right)^{-1/n} \geq \lim\limits_{n\to\infty} \sup \left(cq^{n/2} \right)^{-1/n} = q^{-1/2}$, es decir, $R \geq \dfrac{1}{\sqrt{q}}$.

Por otro lado, $D\big(P_K(u)\big) = \displaystyle\sum_{i=1}^{2g} \frac{\omega_i u}{1-\omega_i u}$ implica que las únicas singularidades son $u = \omega_i^{-1}$, $1 \leq i \leq 2g$, por lo que $\min\limits_{1\leq i\leq 2g} |\omega_i^{-1}| = R \geq q^{-1/2}$, es decir, $|\omega_i| \leq \sqrt{q}$, $1 \leq i \leq 2g$.

Finalmente, por la Proposición 2.1.7 tenemos que

$$q^g = \prod_{i=1}^{2g} |\omega_i| \leq \prod_{i=1}^{2g} \sqrt{q} = q^g, \text{ lo cual implica que } |\omega_i| = \sqrt{q}, 1 \leq i \leq 2g.$$

□

2.2. Demostración de la Hipótesis de Riemann

Nuestro objetivo ahora es probar que las condiciones del Teorema 2.1.8 se cumplen para cualquier campo de funciones congruente K. Sea $k = \mathbb{F}_q$ el campo de constantes de K.

Primero notemos que para probar esto, por la Proposición 2.1.10 se puede suponer, extendiendo el campo de constantes si fuese necesario:
(I) $q = a^2$ es un cuadrado,
(II) $q > (g+1)^4$, g el género de K,
(III) K tiene un divisor primo de grado 1.

En efecto, $K_2 = K\mathbb{F}_{q^2}$ tiene como campo de constantes a $\mathbb{F}_{q^2}$, q^2 es un cuadrado. Como $q^2 > 1$, existe n tal que $q^{2n} = (q^n)^2 > (g+1)^4$, por lo que $K_{2n} = \mathbb{F}_{q^{2n}}K$ tiene como campo de constantes a $\mathbb{F}_{q^{2n}}$ y el género de K_{2n} es igual a g (Teorema 1.1.4) y $q^{2n} > (g+1)^4$. Finalmente, si $\mathfrak{P}$ es un divisor primo de grado m en K y $\mathcal{P}$ está sobre $\mathfrak{P}$ en $K_{2nm} = \mathbb{F}_{q^{2nm}}K$, por el Teorema 1.2.1 se tiene que $d_L(\mathcal{P}) = \dfrac{m}{(m, 2nm)} = \dfrac{m}{m} = 1$. Entonces K_{2nm} satisface (I), (II), (III).

Así pues, podemos suponer que K satisface (I), (II), (III). Sea N el número de divisores primos de grado 1 en K. Si $\sigma \in \mathrm{Aut}(K/\mathbb{F}_q)$, para cada lugar $\mathfrak{P}$, $\mathfrak{P}^\sigma$ es un lugar de K y las valuaciones respectivas satisfacen $\upsilon_{\mathfrak{P}^\sigma}(x) = \upsilon_{\mathfrak{P}}(\sigma^{-1}x)$.

Sea $\widetilde{\mathbb{F}}_q$ la cerradura algebraica de $k := \mathbb{F}_q$ y sea $\widetilde{K}$ la cerradura algebraica de K. Consideremos el Automorfismo de Frobenius:

$$\rho : \widetilde{K} \to \widetilde{K}, \quad \rho(x) = x^q, \quad \rho \in \mathrm{Aut}(\widetilde{K}/k).$$

Sea $\mathfrak{P}$ un divisor primo de K. Para cualquier $\sigma \in \mathrm{Aut}(K/k)$ consideremos $\mathfrak{P}^\sigma$ el divisor primo correspondiente. Explícitamente, si $\varphi_{\mathfrak{P}}$ es el lugar asociado a $\mathfrak{P}$, $\varphi_{\mathfrak{P}^\sigma}$ es el lugar $\sigma\varphi_{\mathfrak{P}}$ dado por

$$\varphi_{\mathfrak{P}^\sigma}(\alpha) = \sigma\varphi_{\mathfrak{P}}(\alpha) = \varphi_{\mathfrak{P}}(\sigma^{-1}\alpha),$$

para $\alpha \in K$.

Definimos $\mathfrak{P}^q$ como el divisor primo dado por el Automorfismo de Frobenius ρ, es decir,

$$\rho\varphi_{\mathfrak{P}}(\alpha) = \varphi_{\mathfrak{P}^q}(\alpha) = \varphi_{\mathfrak{P}}(\rho^{-1}\alpha) = \varphi_{\mathfrak{P}}(\alpha^{1/q}) = \varphi_{\mathfrak{P}}(\alpha)^{1/q}.$$

Observemos que $\mathfrak{P}^q$ no es la q-potencia de $\mathfrak{P}$.

Tenemos que los anillos de valuación de $\mathfrak{P}$ y $\mathfrak{P}^q$ están dados por:

$$\vartheta_{\mathfrak{P}} = \big\{\alpha \in K | \varphi_{\mathfrak{P}}(\alpha) \neq \infty\big\} \quad \text{y} \quad \vartheta_{\mathfrak{P}^q} = \big\{\alpha \in K | \varphi_{\mathfrak{P}^q}(\alpha) = \varphi_{\mathfrak{P}}(\alpha)^{1/q} \neq \infty\big\}.$$

Por lo tanto $\vartheta_{\mathfrak{P}} = \vartheta_{\mathfrak{P}^q}$, es decir, $\varphi_{\mathfrak{P}}$ y $\varphi_{\mathfrak{P}^q}$ son equivalentes. Usaremos la notación $\mathfrak{P} = \mathfrak{P}^q$ para indicar que $\varphi_{\mathfrak{P}} = \varphi_{\mathfrak{P}^q}$ en lugar del significado usual.

Proposición 2.2.1. *Tenemos que $\mathfrak{P} = \mathfrak{P}^q$ si y sólo si $d_K(\mathfrak{P}) = 1$.*

Demostración. Recordemos que $d_K(\mathfrak{P}) = [\vartheta_{\mathfrak{P}}/\mathfrak{P} : k]$ y que

$$\varphi_{\mathfrak{P}} : K \to (\vartheta_{\mathfrak{P}}/\mathfrak{P}) \bigcup \{\infty\}; \quad \varphi_{\mathfrak{P}^q} : K \to (\vartheta_{\mathfrak{P}^q}/\mathfrak{P}^q) \bigcup \{\infty\}.$$

Por lo que se tiene,

$\rho\varphi_{\mathfrak{P}}(y) = \varphi_{\mathfrak{P}}(y)^{1/q} = \varphi_{\mathfrak{P}}(y)$ para todo $y \in K$

$\Leftrightarrow \varphi_{\mathfrak{P}}(y) = \varphi_{\mathfrak{P}}(y)^q$ para todo $y \in K$

$\Leftrightarrow \varphi_{\mathfrak{P}}(y) = \infty$ o $\varphi_{\mathfrak{P}}(y) \in \mathbb{F}_q$ para todo $y \in K$

$\Leftrightarrow \vartheta_{\mathfrak{P}}/\mathfrak{P} = \vartheta_{\mathfrak{P}^q}/\mathfrak{P}^q = \mathbb{F}_q \Leftrightarrow d_K(\mathfrak{P}) = d_K(\mathfrak{P}^q) = 1.$

□

La Proposición 2.2.1 es uno de los resultados principales que estaremos usando en la demostración de la Hipótesis de Riemann. De hecho, los $N_1 = N$ divisores primos de grado 1 en K/k son precisamente aquellos tales que $\mathfrak{P} = \mathfrak{P}^q$.

Tenemos que la Hipótesis de Riemann es equivalente al hecho de que $|N - (q+1)| \leq 2g\sqrt{q}$ (Proposiciones 2.1.9, 2.1.10 y 2.1.11).

Por lo tanto, es suficiente mostrar que para alguna r suficientemente grande y $K_r := K\mathbb{F}_{q^r}$, se satisface $|N_r - (q^r+1)| \leq 2gq^{r/2}$, donde N_r denota el número de lugares $\mathfrak{P}$ tales que $\mathfrak{P}^{q^r} = \mathfrak{P}$.

La demostración de la Hipótesis de Riemann que presentamos se debe esencialmente a Enrico Bombieri ([1], [2], [13]).

La idea es construir una función u sobre K tal que todos los lugares de grado 1, con una excepción, sean ceros de u y, por otro lado, el grado de u no sea demasiado grande.

Se tiene $q = a^2$, pongamos $m = a-1$, $n = a+2g$, $r = m+an$. Entonces la desigualdad

$$N - (q+1) < (2g+1)\sqrt{q}$$

se escribe

$$N - 1 < q + 2g\sqrt{q} + \sqrt{q} = a^2 + 2ga + a = a(a+2g) + a = an + m + 1 = r + 1,$$

es decir, $N - 1 \leq r$.

Sea $\mathfrak{G}$ un divisor primo de grado 1 en K/k. Entonces

$$L\left(\mathfrak{G}^{-1}\right) \subseteq L\left(\mathfrak{G}^{-2}\right) \subseteq \ldots \subseteq L\left(\mathfrak{G}^{-n}\right) \subseteq \ldots.$$

Además como $\mathfrak{G}^{-\mathfrak{n}}\big|\mathfrak{G}^{-(n-1)}$, por el Teorema A.20 tenemos que
$l\left(\mathfrak{G}^{-n}\right)+d\left(\mathfrak{G}^{-n}\right)\leq l\left(\mathfrak{G}^{-(n-1)}\right)+d\left(\mathfrak{G}^{-(n-1)}\right)$, por lo tanto,
$0\leq l\left(\mathfrak{G}^{-n}\right)-l\left(\mathfrak{G}^{-(n-1)}\right)\leq d\left(\mathfrak{G}^{n}\right)+d\left(\mathfrak{G}^{-(n-1)}\right)=n-(n-1)=1.$

Sea $t\in\mathbb{N}$ y sea I_t el conjunto de las $i's$ tales que $1\leq i\leq t$ y que satisfacen $l\left(\mathfrak{G}^{-i}\right)-l\left(\mathfrak{G}^{-(i-1)}\right)=1$. Para cada $i\in I_t$, sea $u_i\in L\left(\mathfrak{G}^{-i}\right)\setminus L\left(\mathfrak{G}^{-(i-1)}\right)$. El divisor de polos de u_i es $\eta_{u_i}=\mathfrak{G}^{i}$.

Proposición 2.2.2. *El sistema $\{u_i|i\in I_t\}$ es una $k-$base de $L(\mathfrak{G}^{-t})$.*

Demostración. Si $\sum_{i\in\, I_t} a_iu_i=0$, $a_i\in k$ con algún $a_i\neq 0$, $v_{\mathfrak{G}}(a_iu_i)=-i$, por lo que cada sumando no cero tiene valuación diferente a cada una de las demás; por lo tanto $a_i=0$ para todo $i\in I_t$ y por lo tanto el sistema $\{u_i|i\in I_t\}$ es linealmente independiente.

Por otro lado,

$$l(\mathfrak{G}^{-t})=\sum_{i=1}^{t}\dim_k\frac{L(\mathfrak{G}^{-i})}{L(\mathfrak{G}^{-(i-1)})}=\sum_{i=1}^{t}\delta_i,$$

con

$$\delta_i=\begin{cases}0 & \text{si } i\notin I_t,\\ 1 & \text{si } i\in I_t,\end{cases}$$

por lo que $l(\mathfrak{G}^{-t})=|I_t|=|\{u_i|i\in I_t\}|$ lo cual prueba que $\{u_i|i\in I_t\}$ es base de $L(\mathfrak{G}^{-t})$.

□

Como caso particular de la Proposición 2.2.2 tomemos $t=m=a-1=\sqrt{q}-1$, a es una potencia de la característica, $n=a+2g$. Así, el conjunto $L\left(\mathfrak{G}^{-n}\right)^a=\{y^a|y\in\ L\left(\mathfrak{G}^{-n}\right)\}\subseteq K^a$ es un $k-$espacio vectorial de la misma dimensión que $L\left(\mathfrak{G}^{-n}\right)$.

El espacio $M=\left\{\sum_{i\in\, I_m}u_iy_i^a|y_i\in\ L\left(\mathfrak{G}^{-n}\right)\right\}$ es un $k-$espacio vectorial generado por $U=\{u_iu_j^a|i\in\ I_m, j\in\ I_n\}$. Notemos que como $a=\sqrt{q}$ es una potencia de la característica, K^a es un campo.

Proposición 2.2.3. *El conjunto U es linealmente independiente sobre k.*

Demostración. Como $u_j^a \in K^a$ y $k \subseteq K^a$, es suficiente probar que $\{u_i | i \in I_m\}$ es linealmente independiente sobre K^a.

Supongamos $\sum_{i \in I_m} u_i y_i^a = 0$ con algún $y_i \neq 0$. Esto implica que dos elementos tienen la misma valuación (Proposición A.18), es decir, $\exists\ y_i \neq 0,\ y_j \neq 0, i \neq j,$ con $\upsilon_{\mathfrak{G}}(u_i y_i^a) = \upsilon_{\mathfrak{G}}(u_j y_j^a)$, es decir, $-i + a\upsilon_{\mathfrak{G}}(y_i) = -j + a\upsilon_{\mathfrak{G}}(y_j)$, luego $i \equiv j$ mód a. Puesto que $i, j \in I_m,\ 1 \leq i, j \leq m = a-1 < a$, contradicción.

□

Como consecuencia de la Proposición 2.2.3 tenemos que

$$\dim_k M = |U| = |I_m||I_n| = l(\mathfrak{G}^{-m}) l(\mathfrak{G}^{-n}).$$

Por el Teorema de Riemann-Roch se tiene la desigualdad:

$$\begin{aligned} \dim_k M &= l(\mathfrak{G}^{-m}) l(\mathfrak{G}^{-n}) \geq (m-g+1)(n-g+1) \\ &= (a-g)(a+g+1) = a^2 + a - g(g+1) = q + \sqrt{q} - g(g+1). \end{aligned}$$

Ahora consideremos el $k-$espacio vectorial,

$$M' = \left\{ \sum_{i \in I_m} u_i^a y_i | y_i \in L\left(\mathfrak{G}^{-n}\right) \right\}.$$

Para $i \in I_m$ y $y_i \in L\left(\mathfrak{G}^{-n}\right)$ se tiene $u_i^a y_i \in L(\mathfrak{G}^{-am}\mathfrak{G}^{-n})$. Luego $M' \subseteq L\left(\mathfrak{G}^{-am}\mathfrak{G}^{-n}\right)$.

Nuevamente por el Teorema de Riemann-Roch (Corolario A.25), puesto que $d_K(\mathfrak{G}^{am}\mathfrak{G}^{n}) = ma + n = a^2 - a + a + 2g = q + 2g > 2g - 2$, se tiene $\dim_k M' \leq l(\mathfrak{G}^{-am}\mathfrak{G}^{-n}) = (q+2g) - g + 1 = q + g + 1$.

Ahora bien, por la elección $q > (g+1)^4$, se tiene

$$\sqrt{q} - g(g+1) > (g+1)^2 - g(g+1) = g + 1.$$

Es decir, $\dim_k M \geq q + \sqrt{q} - g(g+1) > q + g + 1 \geq \dim_k M'$.

Sea $\theta : M \to M', \quad \theta\left(\sum_{i \in I_m} u_i y_i^a\right) = \sum_{i \in I_m} u_i^a y_i.$

Entonces θ es $k-$lineal ya que $k^q = k$ y puesto que $\dim_k M > \dim_k M'$, $\ker\theta \neq \{0\}$. Así, existen $y_i \in L(\mathfrak{G}^{-n})$, $i \in I_m$ no todos cero tales que $\sum_{i\in I_m} u_i^a y_i = 0$. En particular se tiene que $u := \sum_{i\in I_m} u_i y_i^a \in L(\mathfrak{G}^{-r})\backslash\{0\}$, $u \in \ker\theta$. Si $\mathfrak{P}$ es cualquier divisor primo de grado 1 de K/k con $\mathfrak{P} \neq \mathfrak{G}$, entonces $\varphi_{\mathfrak{P}}(y_i) \neq \infty,\ \varphi_{\mathfrak{P}}(u_i) \neq \infty,\ i \in I_m$. Por la Proposición 2.2.1, $\mathfrak{P}$ satisface $\mathfrak{P} = \mathfrak{P}^q$, entonces para todo $\alpha \in K$, se tiene que $\varphi_{\mathfrak{P}}(\alpha) = \varphi_{\mathfrak{P}^q}(\alpha) = \varphi_{\mathfrak{P}}(\alpha)^{1/q}$, o equivalentemente, $\varphi_{\mathfrak{P}}(\alpha) = \varphi_{\mathfrak{P}}(\alpha)^q$, por lo que $\varphi_{\mathfrak{P}}(\alpha) \in \mathbb{F}_q$. Esto implica que para $a = \sqrt{q} = p^t$ se obtiene que $\varphi_{\mathfrak{P}}(\alpha)^a = \varphi_{\mathfrak{P}}(\alpha)$. Entonces, de $\sum_{i\in I_m} u_i^a y_i = 0$ obtenemos: $\varphi_{\mathfrak{P}}(u)^a = \sum_{i\in I_m} \varphi_{\mathfrak{P}}(u_i)^a \varphi_{\mathfrak{P}}(y_i)^q = \sum_{i\in I_m} \varphi_{\mathfrak{P}}(u_i)^q \varphi_{\mathfrak{P}}(y_i) = 0$.

Así pues, $\mathfrak{P}$ está en $\mathfrak{z}_u$, el divisor de ceros de u. Luego $\prod_{\substack{\mathfrak{P}\neq\mathfrak{G}\\ \deg_K\mathfrak{P}=1}} \mathfrak{P}|\mathfrak{z}_u$ y por lo tanto $d_K\left(\prod_{\substack{\mathfrak{P}\neq\mathfrak{G}\\ \deg_K\mathfrak{P}=1}} \mathfrak{P}\right) = N - 1 \leq d_K(\mathfrak{z}_u) = d_K(\eta_u) \leq d_K(\mathfrak{G}^r) = r$.

Así pues, hemos probado:

Teorema 2.2.4. *Se tiene* $N - (q+1) < (2g+1)\sqrt{q}$.

□

Para finalizar la demostración de la Hipótesis de Riemann debemos ahora hallar una cota inferior para $N-(q+1)$. La cota superior que hemos obtenido no es suficiente para deducir la Hipótesis de Riemann. Por ejemplo, si K es un campo de género uno y si ω_1 y ω_2 son las inversas de las raíces de $P_K(u)$, entonces $\omega_1 = q$ y $\omega_2 = 1$ satisfacen que $N = q - \sum_{i=1}^{2g} \omega_i + 1 = q - q - 1 + 1 = 0$, $\omega_1\omega_2 = q$, pero $|\omega_1| \neq \sqrt{q}$.

Para obtener una cota inferior, consideremos $\theta \in \mathrm{Aut}(K/k)$ un automorfismo y sea $\widetilde{k}$ la cerradura algebraica de k. Sea $\widetilde{K} = K\widetilde{k}$. Extendemos θ a $\widetilde{\theta} \in \mathrm{Aut}(\widetilde{K}/k)$ definiendo $\widetilde{\theta}(\alpha) = \alpha^q$ para todo $\alpha \in \widetilde{k}$. Sea $\mathfrak{P}$ cualquier divisor primo de grado d. Sea $K_d = K\mathbb{F}_{q^d}$. Entonces, del Teorema 1.2.1 tenemos que $\mathfrak{P}$ se descompone en d divisores primos de grado uno

$\mathcal{P}_1, \ldots, \mathcal{P}_d$ en K_d. Sean $\varphi_{\mathfrak{P}}$, $\varphi_{\mathfrak{P}^q}$, $\varphi_{\mathfrak{P}^\theta}$, $\varphi_{\mathcal{P}_i}$, $\varphi_{\mathcal{P}_i^q}$, $\varphi_{\mathcal{P}_i^{\widetilde{\theta}}}$ los lugares asociados a $\mathfrak{P}$, $\mathfrak{P}^q$, $\mathfrak{P}^\theta$, $\mathcal{P}_i$, $\mathcal{P}_i^q$, $\mathcal{P}_i^{\widetilde{\theta}}$, $1 \leq i \leq d$, respectivamente.

Se tiene que $\varphi_{\mathfrak{P}^\theta}(x) = \varphi_{\mathfrak{P}}(\theta^{-1}x)$ y $\varphi_{\mathfrak{P}^q}(x) = \varphi_{\mathfrak{P}}(x)^{1/q}$. Para $x \in K$, tenemos

$$\varphi_{\mathcal{P}_i^{\widetilde{\theta}}}(x) = \varphi_{\mathcal{P}_i}(\widetilde{\theta}^{-1}x) = \varphi_{\mathfrak{P}}(\theta^{-1}x) = \varphi_{\mathfrak{P}^\theta}(x)$$

y

$$\varphi_{\mathcal{P}_i^q}(x) = \varphi_{\mathcal{P}_i}(x)^{1/q} = \varphi_{\mathfrak{P}}(x)^{1/q}.$$

Para $\alpha \in \mathbb{F}_{q^d}$,

$$\varphi_{\mathcal{P}_i^{\widetilde{\theta}}}(\alpha) = \varphi_{\mathcal{P}_i}(\widetilde{\theta}^{-1}\alpha) = \varphi_{\mathcal{P}_i}(\alpha^{1/q}) = \varphi_{\mathcal{P}_i^q}(\alpha).$$

Por lo tanto $\mathfrak{P}^q = \mathfrak{P}^\theta \Leftrightarrow \mathcal{P}_i^q = \mathcal{P}_i^{\widetilde{\theta}}$ para todo $1 \leq i \leq d$.

Definimos $N^{(\theta)} := \sum_{\mathfrak{P}^\theta = \mathfrak{P}^q} d_K(\mathfrak{P})$. De lo anterior tenemos que $N^{(\theta)}$ es el número de divisores primos $\mathcal{P}$ de $K\widetilde{k}/\widetilde{k}$ tales que $\mathcal{P}^{\widetilde{\theta}} = \mathcal{P}^q$.

De manera análoga a como se hizo con el Teorema 2.2.4 se puede probar:

Teorema 2.2.5. *Con la notación de arriba se tiene*

$$N^{(\theta)} - (q+1) < (2g+1)\sqrt{q}.$$

□

Proposición 2.2.6. *Sea K un campo de funciones sobre k. Sea L una extensión geométrica de Galois de K con grupo de Galois G. Si $\theta \in \mathrm{Aut}(L/k)$ es tal que $\theta(K) = K$, entonces*

$$N^{(\theta)}(K) = [L:K]^{-1} \sum_{\sigma \in G} N^{(\theta\sigma)}(L).$$

Demostración. Sean $\mathcal{P}$ un divisor primo de L/k y $\mathfrak{P} = \mathcal{P}|_K$. Los lugares de L sobre $\mathfrak{P}^\theta$ son los lugares $(\mathcal{P}^\theta)^\sigma$, $\sigma \in G$ y sobre $\mathfrak{P}^q$ está el lugar $\mathcal{P}^q$ por lo que $\mathfrak{P}^\theta = \mathfrak{P}^q \Leftrightarrow \exists\, \sigma \in G$ tal que $(\mathcal{P}^\theta)^\sigma = (\mathcal{P}^{\theta\sigma}) = \mathcal{P}^q$.

Tenemos que si $\mathcal{P}, \mathcal{P}_1, \mathcal{P}_2$ son divisores primos en L sobre un divisor primo $\mathfrak{P}$ de K, puesto que G actúa transitivamente en $\{\mathcal{P} \in \mathbb{P}_L | \mathcal{P}|\mathfrak{P}\}$, se tiene

que si $\varphi_{\mathcal{P}_1}$ y $\varphi_{\mathcal{P}_2}$ denotan los lugares que corresponden a $\mathcal{P}_1, \mathcal{P}_2$, respectivamente, entonces $\mid \{\sigma \in G \mid \varphi_{\sigma\mathcal{P}_1} = \varphi_{\mathcal{P}_2}\} \mid = \mid \{\sigma \in G \mid \varphi_{\sigma\mathcal{P}} = \varphi_{\mathcal{P}}\} \mid$.

Ahora bien, $\varphi_{\sigma\mathcal{P}} = \varphi_{\mathcal{P}} \Leftrightarrow \varphi_{\sigma\mathcal{P}}(x) = \varphi_{\mathcal{P}}(\sigma^{-1}x)$ para todo $x \in \vartheta_{\mathcal{P}} \Leftrightarrow \sigma^{-1}x - x \in \ker \varphi_{\mathcal{P}} = \mathcal{P}$ para todo $x \in \vartheta_{\mathcal{P}} \Leftrightarrow \sigma^{-1}x \equiv x$ mód $\mathcal{P}$ para todo $x \in \vartheta_{\mathcal{P}} \Leftrightarrow \sigma^{-1} \in I_{L/K}(\mathcal{P} \mid \mathfrak{P}) \Leftrightarrow \sigma \in I_{L/K}(\mathcal{P} \mid \mathfrak{P})$, el grupo de inercia de $\mathcal{P}$ sobre $\mathfrak{P}$.

Por lo tanto, $\mid \{\sigma \in G \mid \varphi_{\sigma\mathcal{P}_1} = \varphi_{\mathcal{P}_2}\} \mid = e_{L/K}(\mathcal{P} \mid \mathfrak{P})$, el índice de ramificación de $\mathcal{P}$ sobre $\mathfrak{P}$. Sea $I = I_{L/K}(\mathcal{P}^\theta \mid \mathfrak{P}^\theta)$.

Así:

$$\begin{aligned}
\sum_{\sigma \in G} N^{(\theta\sigma)}(L) &= \sum_{\sigma \in G} \sum_{\mathcal{P}^{\theta\sigma} = \mathcal{P}^q} d_L(\mathcal{P}) = \sum_{\overline{\Psi} \in G/I} \sum_{\sigma \in I} \sum_{\mathcal{P}^{\theta\Psi\sigma} = \mathcal{P}^q} d_L(\mathcal{P}) \\
&= \sum_{\overline{\Psi} \in G/I} \sum_{\mathcal{P}^{\theta\Psi} = \mathcal{P}^q} e_{L/K}\left(\mathcal{P}^\theta \mid \mathfrak{P}^\theta\right) d_L(\mathcal{P}) \\
&= \sum_{\mathfrak{P}^\theta = \mathfrak{P}^q} \sum_{\mathcal{P} \mid \mathfrak{P}} e_{L/K}\left(\mathcal{P} \mid \mathfrak{P}\right) d_{L/K}\left(\mathcal{P} \mid \mathfrak{P}\right) d_K(\mathfrak{P}) \\
&= [L:K] \sum_{\mathfrak{P}^\theta = \mathfrak{P}^q} d_K(\mathfrak{P}) \text{ (Prop. A.29, Teorema A.30)} \\
&= [L:K] N^{(\theta)}(K).
\end{aligned}$$

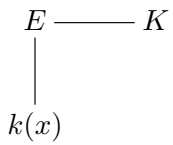
□

Sea $\theta \in \mathrm{Aut}(K/k)$ de orden finito y sea $E = K^{\langle\theta\rangle}$ el campo fijo. Entonces K/E es una extensión cíclica con grupo de Galois $\langle\theta\rangle$. Necesitaremos la siguiente proposición.

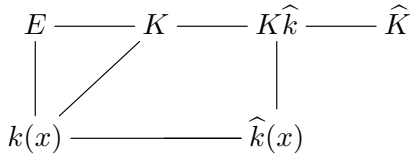
Proposición 2.2.7. *Sea E/k un campo de funciones congruente. Entonces existe un elemento $x \in E \backslash k$ tal que $E/k(x)$ es separable.*

Demostración. Como existe un divisor de grado 1 (Teorema 1.3.8), tenemos que existe un divisor primo $\mathfrak{P}$ de E de grado t con $(t, p) = 1$, $p = \mathrm{car}\ k$. Sea $m \in \mathbb{N}$ tal que $m > 2g - 1$ y $(m, p) = 1$. Entonces, por el Teorema de Riemann-Roch (Corolario A.26), existe un elemento $x \in E$ tal que $\eta_x = \mathcal{P}^m$. Por tanto $[E : k(x)] = mt$ y $(mt, p) = 1$, $p = \mathrm{car}\ E$, lo cual implica que $E/k(x)$ es separable. □

Sean K, θ y E como antes.



Sean $x \in E\backslash k$ con la propiedad de la Proposición 2.2.7, $\widehat{K}$ la cerradura de Galois de $K/k(x)$ y $\widehat{k}$ el campo de constantes de $\widehat{K}$. Tanto $\widehat{K}$ como $K\widehat{k}$ tienen como campo de constantes a $\widehat{k}$. Entonces θ se extiende a un elemento de $\mathrm{Aut}(\widehat{K}/\widehat{k}(x))$.



Extendiendo constantes de $\widehat{K}$ si fuese necesario, podemos suponer que si $|\ \widehat{k}\ | = \widehat{q}$, entonces $\widehat{q} = a^2$ es un cuadrado, $\widehat{q} > (g_{\widehat{K}} + 1)^4$, $\widehat{q} > (g_{K\widehat{k}} + 1)^4 = (g_K + 1)^4$ y $\widehat{K}$ tiene un divisor primo de grado 1.

Así pues, podemos suponer que K/k satisface:

1. K/k tiene un elemento $x \in K\backslash k$ tal que $K/k(x)$ es separable, $\widehat{K}$ la cerradura de Galois de $K/k(x)$ tiene campo de constantes k,
2. $|k| = q = a^2$ es un cuadrado, $q > (\widehat{g} + 1)^4$, $\widehat{g} = g_{\widehat{K}}$,
3. $\widehat{K}/k$ tiene un divisor primo de grado 1.

Proposición 2.2.8. *Sean* $m = [\widehat{K} : K]$, $n = [\widehat{K} : k(x)]$, $\theta \in \mathrm{Aut}(K/k)$. *Entonces* $N^{(\theta)} - (q+1) \geq -\dfrac{n-m}{m}(2\widehat{g}+1)\sqrt{q}$.

Demostración. Sea $H = \mathrm{Gal}(\widehat{K}/K)$, $G = \mathrm{Gal}(\widehat{K}/k(x))$. Entonces $\theta \in G$, $m = |H|$, $\quad n = |G|$.

Se tiene por la Proposición 2.2.6,

$$N^{(\theta)}(K) = \frac{1}{m}\sum_{h\in H} N^{(\theta h)}(\widehat{K}) \quad \text{y} \quad q+1 = N(k(x)) = \frac{1}{n}\sum_{\sigma\in G} N^{(\sigma)}(\widehat{K}),$$

y por el Teorema 2.2.5

$$\begin{aligned}\sum_{\sigma \in G} N^{(\sigma)}(\widehat{K}) &= \sum_{h \in H} N^{(\theta h)}(\widehat{K}) + \sum_{\sigma \in G \setminus \theta H} N^{(\sigma)}(\widehat{K}) \\ &\leq \sum_{h \in H} N^{(\theta h)}(\widehat{K}) + \sum_{\sigma \in G \setminus \theta H} ((q+1) + (2\widehat{g}+1)\sqrt{q}) \\ &= \sum_{h \in H} N^{(\theta h)}(\widehat{K}) + (n-m)\left((q+1) + (2\widehat{g}+1)\sqrt{q}\right).\end{aligned}$$

Como $\sum_{\sigma \in G} N^{(\sigma)}(\widehat{K}) = n(q+1)$, se tiene:

$$\begin{aligned}\sum_{h \in H} N^{(\theta h)}(\widehat{K}) &\geq n(q+1) - (n-m)\left((q+1) + (2\widehat{g}+1)\sqrt{q}\right) \\ &= m(q+1) - (n-m)(2\widehat{g}+1)\sqrt{q}.\end{aligned}$$

Finalmente, como $\sum_{h \in H} N^{(\theta h)}(\widehat{K}) = mN^{(\theta)}(K)$, tenemos

$$N^{(\theta)}(K) \geq (q+1) - \frac{(n-m)}{m}(2\widehat{g}+1)\sqrt{q}.$$

□

Corolario 2.2.9. *Sea K/k un campo de funciones congruente y sea θ un elemento de orden finito de* $\mathrm{Aut}(K/k)$*. Entonces k tiene una extensión finita k' con q' elementos tal que existe una constante $c > 0$ de manera que para todo $r \geq 1$ la extensión k'_r de grado r de k', $K'_r = Kk'_r$, satisface*

$$\mid N^{(\theta)}\left(K'_r\right) - \left(\left(q'\right)^r + 1\right) \mid \leq c\left(q'\right)^{r/2}.$$

Demostración. Sea k' una extensión de k que satisface la Proposición 2.2.8 y el Teorema 2.2.5. Entonces los números n, m, $\widehat{g}$ obtenidos en la Proposición 2.2.8 se mantienen fijos para extensiones de constantes (Teorema 1.1.4), por lo que para todo $r \geq 1$, se tiene $|k'_r| = (q')^r$,

$$-\frac{(n-m)}{m}(2\widehat{g}+1)\left(q'\right)^{r/2} \leq N^{(\theta)}\left(K'_r\right) - \left(\left(q'\right)^r + 1\right) \leq (2\widehat{g}+1)\left(q'\right)^{r/2}.$$

Con $c = \text{máx}\left\{\frac{(n-m)}{m}(2\widehat{g}+1), 2\widehat{g}+1\right\}$ obtenemos lo requerido.

□

Finalmente tenemos:

Teorema 2.2.10. *(HIPÓTESIS DE RIEMANN) Sea K/k un campo de funciones congruente, donde $|k| = q$. Entonces:*

(I) Los ceros de la función zeta $\zeta_K(s)$ están en la línea $\mathbb{R}e\, s = \frac{1}{2}$.

(II) Los ceros de la función $Z_K(u)$ están en el círculo $|u| = q^{-1/2}$.

(III) Si $\omega_1, \ldots, \omega_{2g}$, son las inversas de las raíces de $P_K(u)$, entonces $|\omega_i| = \sqrt{q}$, $i = 1, \ldots, 2g$.

(IV) Si N_1 denota el número de divisores primos de grado 1 en K, entonces $|N_1 - (q+1)| \leq 2g\sqrt{q}$.

Demostración. Se sigue del Teorema 2.1.8, las Proposiciones 2.1.9, 2.1.10, 2.1.11 y el Corolario 2.2.9.

□

2.3. Consecuencias de la Hipótesis de Riemann

Una consecuencia inmediata de la Hipótesis de Riemann es:

Teorema 2.3.1. *Sea K/k un campo de funciones congruente de género 0. Entonces K es un campo de funciones racionales.*

Demostración. Si N es el número de divisores primos de grado 1 en K,se tiene, aplicando la Proposición 2.1.9, $|N - (q+1)| \leq 2g\sqrt{q} = 0$, es decir, $N = q + 1$, por lo que K tiene divisores primos de grado 1. El resultado se sigue del Teorema A.28.

□

Nuestro objetivo ahora es estimar el número de divisores primos de grado n en K/k.

Teorema 2.3.2. *Si $K = \mathbb{F}_q(x)$ es el campo de funciones racionales sobre $\mathbb{F}_q$ y n_i es el número de divisores primos de grado i en K, entonces $n_1 = q + 1$ y $n_i = \frac{1}{i}\sum_{d|i} \mu\left(\frac{i}{d}\right) q^d$, $\forall\, i > 1$.*

Demostración. Los divisores primos distintos a $\mathfrak{P}_\infty$ están en correspondencia biyectiva con los polinomios irreducibles mónicos (Teorema A.19). Como $\mathfrak{P}_\infty$ es de grado 1, el resultado se sigue de la Proposición 2.1.5.

□

Ejemplo 2.3.3. Sea $K = \mathbb{F}_2(x)$ el campo de funciones racionales sobre $\mathbb{F}_2$ por el Teorema 2.3.2 tenemos que:

- $n_1 = q + 1 = 2 + 1 = 3$, es decir, tenemos 3 divisores primos de grado 1 en $\mathbb{F}_2(x)$ que corresponden a $x, x+1$ y $\dfrac{1}{x}$.

- $n_2 = \dfrac{1}{2}\displaystyle\sum_{d|2} \mu\left(\frac{2}{d}\right) 2^d = \frac{1}{2}\left(\mu\left(\frac{2}{1}\right)2^1 + \mu\left(\frac{2}{2}\right)2^2\right) = \frac{1}{2}\left(-2 + 2^2\right) = \dfrac{1}{2}(2) = 1$, es decir, tenemos 1 divisor primo de grado 2 en $\mathbb{F}_2(x)$ que corresponde a $x^2 + x + 1$.

- $n_3 = \dfrac{1}{3}\displaystyle\sum_{d|3} \mu\left(\frac{3}{d}\right) 2^d = \frac{1}{3}\left(\mu\left(\frac{3}{1}\right)2^1 + \mu\left(\frac{3}{3}\right)2^3\right) = \frac{1}{3}\left(-2 + 2^3\right) = \dfrac{1}{3}(6) = 2$, es decir, tenemos 2 divisores primos de grado 3 en $\mathbb{F}_2(x)$, los cuales corresponden a $x^3 + x^2 + 1$ y $x^3 + x + 1$.

Generalizaremos el método anterior para estimar el número de divisores primos de grado m en cualquier campo de funciones K sobre $k = \mathbb{F}_q$.

Sean K/k un campo de funciones, $x \in K\backslash k$, $[K : k(x)] < \infty$. Sea $\zeta_0(s)$ la función zeta de $k(x)$ y $\zeta(s)$ la función zeta de K. Sea N_m el número de divisores primos de grado m en K. Se tiene por el Teorema 1.3.7:

$$\zeta(s) = \prod_{\mathcal{P} \in \mathbb{P}_K} \left(1 - \frac{1}{(N(\mathcal{P}))^s}\right)^{-1} = \prod_{m=1}^{\infty} \left(1 - \frac{1}{q^{ms}}\right)^{-N_m}, \quad \mathbb{R}e\ s > 1.$$

Entonces

$$\begin{aligned}
\frac{\zeta'(s)}{\zeta(s)} &= [\ln\zeta(s)]' = \left[\sum_{m=1}^{\infty} -N_m\left(\ln\left(1-\frac{1}{q^{ms}}\right)\right)\right]' \\
&= \sum_{m=1}^{\infty} -N_m\left(\ln(q^{ms}-1)-\ln(q^{ms})\right)' \\
&= \sum_{m=1}^{\infty} -N_m\left(\frac{(q^{ms}-1)'}{q^{ms}-1} - m\ln q\right) \\
&= \sum_{m=1}^{\infty} -\left(\frac{(m\ln q)q^{ms}}{q^{ms}-1} - m\ln q\right)N_m \\
&= \sum_{m=1}^{\infty} -\left(\frac{(m\ln q)q^{ms} - m\ln q(q^{ms}-1)}{q^{ms}-1}\right)N_m \\
&= \sum_{m=1}^{\infty} -\left(\frac{(m\ln q)q^{ms} - (m\ln q)q^{ms} + m\ln q}{q^{ms}-1}\right)N_m \\
&= \sum_{m=1}^{\infty} -m(\ln q)N_m\left(\frac{1}{q^{ms}-1}\right) \\
&= -\sum_{m=1}^{\infty}\frac{(\ln q)mN_m}{q^{ms}}\left(\frac{q^{ms}}{q^{ms}-1}\right) \\
&= -\sum_{m=1}^{\infty}\frac{(\ln q)mN_m}{q^{ms}}\left(\sum_{r=0}^{\infty}\frac{1}{q^{rms}}\right) \\
&= -\ln q\left(\sum_{m=1}^{\infty}\sum_{r=0}^{\infty}\frac{mN_m}{q^{(r+1)ms}}\right) \\
&= -\ln q\left(\sum_{m=1}^{\infty}\sum_{r=1}^{\infty}\frac{mN_m}{q^{rms}}\right) \\
&= -\ln q\left(\sum_{t=1}^{\infty}\frac{c_t}{q^{ts}}\right),
\end{aligned}$$

con $c_t = \sum_{m} mN_m$, donde m recorre los números naturales tales que existe $r \in \mathbb{N}$ con $rm = t$, es decir, $c_t = \sum_{m|t} mN_m$.

Así tenemos:

$$\frac{\zeta'(s)}{\zeta(s)} = -\ln q\sum_{t=1}^{\infty}\left(\sum_{m|t} mN_m\right)\frac{1}{q^{ts}}, \quad \mathbb{R}e\ s > 1.$$

En particular para $K = k(x)$, tenemos:

$$\frac{\zeta_0'(s)}{\zeta_0(s)} = -\ln q \sum_{t=1}^{\infty} \left(\sum_{m|t} m n_m \right) \frac{1}{q^{ts}}, \quad \mathbb{R}e\ s > 1.$$

Por otro lado, $\zeta_0(s) = \dfrac{1}{(1-q^{1-s})(1-q^{-s})}$, por lo que

$$\begin{aligned}
\frac{\zeta_0'(s)}{\zeta_0(s)} &= [\ln \zeta_0(s)]' = \left(-\ln\left(1-q^{1-s}\right) - \ln\left(1-q^{-s}\right)\right)' \\
&= -\left(\frac{(1-q^{1-s})'}{1-q^{1-s}} + \frac{(1-q^{-s})'}{1-q^{-s}} \right) \\
&= -\ln q \left(\frac{q^{1-s}}{1-q^{1-s}} + \frac{q^{-s}}{1-q^{-s}} \right) \\
&= -\ln q \left(q^{1-s} \frac{1}{1-\frac{q}{q^s}} + q^{-s} \frac{1}{1-\frac{1}{q^s}} \right) \\
&= -\ln q \left(q^{1-s} \left(\sum_{n=0}^{\infty} \frac{q^n}{q^{ns}} \right) + q^{-s} \left(\sum_{n=0}^{\infty} \frac{1}{q^{ns}} \right) \right) \\
&= -\ln q \left(\sum_{n=0}^{\infty} \frac{q^{1-s} q^n + q^{-s}}{q^{ns}} \right) = -\ln q \left(\sum_{n=0}^{\infty} \frac{q^{-s}\left(q^{n+1}+1\right)}{q^{ns}} \right) \\
&= -\ln q \left(\sum_{n=0}^{\infty} \frac{q^{n+1}+1}{q^{s(n+1)}} \right) = -\ln q \left(\sum_{n=1}^{\infty} \frac{q^n+1}{q^{ns}} \right).
\end{aligned}$$

En particular, igualando coeficientes, obtenemos que $\displaystyle\sum_{m|t} m n_m = q^t + 1$, fórmula que es equivalente a la del Teorema 2.3.2.

Notación. Sean $f(x)$, $g(x)$ dos funciones de variable real. Si $g(x) \geq 0$, ponemos $f = O(g)$ si existe una constante $c > 0$ tal que $|f(x)| \leq c|g(x)|$ para x suficientemente grande.

Teorema 2.3.4.

$$\frac{\zeta'(s)}{\zeta(s)} = -\ln q \sum_{t=1}^{\infty} \left(\sum_{m|t} m N_m \right) \frac{1}{q^{ts}}, \quad \mathbb{R}e\ s > 1$$

y

$$n_m = \frac{q^m}{m} + O\left(\frac{q^{m/2}}{m} \right).$$

Demostración. La primera parte ya se probó en el transcurso de los comentarios anteriores. Ahora, por el Teorema 2.3.2 $n_m = \frac{1}{m}\sum_{i|m} q^i \mu\left(\frac{m}{i}\right) = \frac{q^m}{m} + \frac{1}{m}\sum_{\substack{i|m \\ i\neq m}} q^i \mu\left(\frac{m}{i}\right)$.

Por lo tanto

$$\begin{aligned}\left|n_m - \frac{q^m}{m}\right| &\leq \frac{1}{m}\sum_{i\leq \frac{m}{2}} q^i = \frac{q^{m/2}}{m}\left(\sum_{i\leq \frac{m}{2}} q^{i-m/2}\right) \leq \frac{q^{m/2}}{m}\sum_{r=0}^{\infty}\frac{1}{q^r} \\ &= \frac{q^{m/2}}{m}\left(\frac{1}{1-\frac{1}{q}}\right), \quad \forall\, m > 1.\end{aligned}$$

□

Por un lado tenemos que $\frac{\zeta'(s)}{\zeta(s)} = -\ln q \sum_{t=1}^{\infty}\left(\sum_{m|t} mN_m\right)\frac{1}{q^{ts}}$ y por otro lado $\frac{\zeta(s)}{\zeta_0(s)} = P_K(q^{-s}) = \prod_{i=1}^{2g}\left(1-\frac{\omega_i}{q^s}\right)$, donde $\omega_1, \ldots, \omega_{2g}$ son las inversas de las raíces de $P_K(u)$, con $u = q^{-s}$ y $|\omega_i| = \sqrt{q}$ por la Hipótesis de Riemann.

Ahora bien,

$$\left(\ln\left(\frac{\zeta(s)}{\zeta_0(s)}\right)\right)' = \left(\ln\left(P_K(q^{-s})\right)\right)'$$

$$\Rightarrow \left(\ln\left(\zeta(s)\right) - \ln\left(\zeta_0(s)\right)\right)' = \left(\ln\left(\prod_{i=1}^{2g}(1-\omega_i q^{-s})\right)\right)'$$

$$\begin{aligned}\Rightarrow \frac{\zeta'(s)}{\zeta(s)} - \frac{\zeta_0'(s)}{\zeta_0(s)} &= \left(\sum_{i=1}^{2g}\ln(1-\omega_i q^{-s})\right)' = \sum_{i=1}^{2g}\left(\ln(1-\omega_i q^{-s})\right)' \\ &= \sum_{i=1}^{2g}\ln q\frac{\omega_i q^{-s}}{1-\omega_i q^{-s}} = \ln q\sum_{i=1}^{2g}\frac{\omega_i q^{-s}}{1-\omega_i q^{-s}} \\ &= \ln q\sum_{i=1}^{2g}\sum_{n=1}^{\infty}\omega_i^n q^{-ns} = \ln q\sum_{n=1}^{\infty}\frac{s_n}{q^{ns}},\end{aligned}$$

donde $s_n = \sum_{i=1}^{2g}\omega_i^n$.

Por otro lado, $\dfrac{\zeta'(s)}{\zeta(s)} - \dfrac{\zeta_0'(s)}{\zeta_0(s)} = -\ln q \sum_{t=1}^{\infty} \left(\sum_{m|t} m(N_m - n_m) \right) \dfrac{1}{q^{ts}}$.

Por lo tanto $\sum_{m|t} m(N_m - n_m) = -s_t$.

Por la Fórmula de Inversión de Möbius, haciendo $f(m) = m(N_m - n_m)$ y $g(t) = -s_t$ tales que $-s_t = g(t) = \sum_{m|t} f(m) = \sum_{m|t} m(N_m - n_m)$, obtenemos $t(N_t - n_t) = f(t) = \sum_{m|t} \mu\left(\dfrac{t}{m}\right) g(m) = -\sum_{m|t} \mu\left(\dfrac{t}{m}\right) s_m$, es decir,

$N_t = n_t - \dfrac{1}{t} \sum_{m|t} \mu\left(\dfrac{t}{m}\right) s_m$, con $s_m = \sum_{i=1}^{2g} \omega_i^m$.

Como $|\omega_i| = q^{1/2}$, deducimos:

$$\begin{aligned} t|N_t - n_t| &\leq \sum_{m=1}^{t} |s_m| \leq \sum_{m=1}^{t} \sum_{i=1}^{2g} |\omega_i|^m = \sum_{m=1}^{t} 2gq^{m/2} \\ &= 2gq^{1/2} \frac{q^{t/2} - 1}{q^{1/2} - 1}. \end{aligned}$$

Por lo tanto, $N_t = n_t + O\left(\dfrac{q^{t/2}}{t}\right)$.

Resumiendo tenemos el siguiente teorema:

Teorema 2.3.5. *Sea K/k un campo de funciones congruente, donde $k = \mathbb{F}_q$. Si n_m y N_m denotan los divisores primos de grado m en $k(x)$ y K respectivamente, entonces:*

$$\begin{aligned} n_m &= \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) q^d, \quad \textit{para } m > 1 \textit{ y } n_1 = q + 1, \\ N_m &= n_m + O\left(\frac{q^{m/2}}{m}\right). \end{aligned}$$

Además,

$$\begin{aligned} \sum_{d|m} d(N_d - n_d) &= -s_m, \\ m(N_m - n_m) &= -\sum_{d|m} \mu\left(\frac{m}{d}\right) s_d, \end{aligned}$$

con $s_d = \sum_{i=1}^{2g} \omega_i^d$, *con* μ *la Función* μ *de Möbius.*

□

Corolario 2.3.6. *Sea* K/k *un campo de funciones congruente, donde* $k = \mathbb{F}_q$. *Si* N_m *denota los divisores primos de grado* m *en* K, *entonces*

$$N_m = \frac{q^m}{m} + O\left(\frac{q^{m/2}}{m}\right).$$

Demostración. Tenemos por el Teorema 2.3.5 que:
$\exists\ c_1 > 0$, tal que $|N_m - n_m| \leq c_1 \left|\frac{q^{m/2}}{m}\right| = c_1 \frac{q^{m/2}}{m}$ para m suficientemente grande y $\exists\ c_2 > 0$, tal que $\left|n_m - \frac{q^m}{m}\right| \leq c_2 \left|\frac{q^{m/2}}{m}\right| = c_2 \frac{q^{m/2}}{m}$ para m suficientemente grande, entonces

$$\begin{aligned} \left|N_m - \frac{q^m}{m}\right| &= \left|N_m - n_m + n_m - \frac{q^m}{m}\right| \leq |N_m - n_m| + \left|n_m - \frac{q^m}{m}\right| \\ &\leq c_1 \frac{q^{m/2}}{m} + c_2 \frac{q^{m/2}}{m} = (c_1 + c_2)\frac{q^{m/2}}{m} = c\frac{q^{m/2}}{m} = c\left|\frac{q^{m/2}}{m}\right|, \end{aligned}$$

luego $\exists\ c = (c_1 + c_2) > 0$, tal que $\left|N_m - \frac{q^m}{m}\right| \leq c\left|\frac{q^{m/2}}{m}\right|$ para m suficientemente grande y por lo tanto $N_m = \frac{q^m}{m} + O\left(\frac{q^{m/2}}{m}\right)$.

□

Finalizamos esta sección relacionando el número de divisores enteros con el número de divisores primos, así como comparando el número de divisores primos en extensiones de constantes.

Proposición 2.3.7. *Sea* K/k *un campo de funciones congruente, donde* $k = \mathbb{F}_q$ *y sea* K_n, *para cada* $n \in \mathbb{N}$, *la extensión de constantes de* K *de grado* n, *es decir,* $K_n = K\mathbb{F}_{q^n}$. *Sea* N_j *el número de divisores primos de grado* j *en* K *y sea* $N_1^{(n)}$ *el número de divisores primos de grado* 1 *en* K_n.

Entonces:

$$N_1^{(n)} = \sum_{d|n} dN_d \quad y \quad N_n = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) N_1^{(d)}.$$

Demostración. Por el Teorema 1.2.1 tenemos que si $d|n$ y $\mathfrak{P}$ es un divisor primo de grado d en K, entonces $\mathfrak{P}$ se descompone en $(d,n) = d$ divisores primos de grado $\dfrac{d}{(d,n)} = 1$ en K_n. Por tanto, para cada primo de grado d en K obtenemos d primos de grado 1 en K_n. Recíprocamente, si $\mathcal{P}$ es un primo de grado 1 en K_n, $\mathfrak{P} = \mathcal{P}|_K$, entonces por la Proposición A.29 se tiene $1 \cdot n = d_K(\mathfrak{P}) d_{K_n/K}(\mathcal{P}|\mathfrak{P})$, luego, $d_K(\mathfrak{P})|n$. Por tanto $N_1^{(n)} = \sum_{d|n} dN_d$. Ahora, por la Fórmula de Inversión de Möbius aplicada a $f(d) = dN_d$ y $g(n) = N_1^{(n)}$, obtenemos $nN_n = f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) N_1^{(d)}$.

□

Ahora, como en el capítulo anterior, denotemos por A_n al número de divisores enteros de grado n. Recordemos que

$$A_n = \sum_{d(C)=n} \frac{q^{N(C)}-1}{q-1} \quad \text{para todo } n \text{ y que} \quad A_n = h\left(\frac{q^{n-g+1}-1}{q-1}\right)$$

para $n > 2g_K - 2$, h el número de clases de K.

Teorema 2.3.8. *Se tiene que*

$$A_n = \sum_{\substack{k_1+2k_2+\cdots+nk_n=n \\ k_i \geq 0}} \prod_{i=1}^{n} \binom{k_i + N_i - 1}{k_i},$$

donde la suma recorre las particiones de n, es decir, las n-tuplas $(k_1, \ldots, k_n)$ con $k_i \geq 0$, $\sum_{i=1}^{n} ik_i = n$.

Demostración. Damos dos pruebas una analítica y otra de carácter combinatorio. Primero recordemos que $f(x) = \dfrac{1}{1-x} = \sum_{n=0}^{\infty} x^n$ para $|x| < 1$, por lo tanto si derivamos $p-1$ veces en ambos lados obtenemos:

$$\frac{1}{(1-x)^p} = \sum_{n=0}^{\infty} \binom{n+p-1}{p-1} x^n, \quad |x| < 1.$$

Ahora la función zeta es $Z_K(u) = \sum_{n=0}^{\infty} A_n u^n$, $u = q^{-s}$.

Por otro lado,

$$\begin{aligned}
\zeta_K(s) &= \prod_{\mathfrak{P}\in\,\mathbb{P}_K}\left(1-\frac{1}{(N(\mathfrak{P}))^s}\right)^{-1} = \prod_{n=1}^{\infty}\left(1-\frac{1}{q^{ns}}\right)^{-N_n}\\
&= \prod_{n=1}^{\infty}\left(\frac{(q^{ns}-1)^{-1}}{(q^{ns})^{-1}}\right)^{N_n} = \prod_{n=1}^{\infty}\left(\frac{q^{-ns}}{q^{-ns}}\left(\frac{q^{ns}}{q^{ns}-1}\right)\right)^{N_n}\\
&= \prod_{n=1}^{\infty}\left(\frac{1}{1-q^{-ns}}\right)^{N_n} = \prod_{n=1}^{\infty}\left(\frac{1}{1-u^n}\right)^{N_n}\\
&= \prod_{m=1}^{\infty}\left(\sum_{k_m=0}^{\infty}\binom{k_m+N_m-1}{N_m-1}(u^m)^{k_m}\right), \text{ luego}
\end{aligned}$$

$$Z_K(u) = 1+\sum_{t=0}^{\infty}\left(\sum_{\substack{k_1+2k_2+\cdots+nk_n=n\\ k_i\geq 0}}\prod_{i=1}^{t}\binom{k_i+N_i-1}{N_i-1}\right)u^t.$$

Puesto que $\binom{k_i+N_i-1}{N_i-1} = \binom{k_i+N_i-1}{k_i}$, la igualdad se tiene al igualar los coeficientes.

Ahora damos una demostración de tipo combinatorio.

Sea $g(k_1,\ldots,k_n)$ el número de distintos productos de k_1 primos de grado 1, k_2 primos de grado $2,\ldots,k_n$ primos de grado n.

Se tiene que $g(k_1,\ldots,k_n) = \prod_{i=1}^{n} f_i(k_i)$, donde $f_i(k_i)$ es el número de productos de k_i primos de grado i.

En general, si $\mathfrak{P}_1,\ldots,\mathfrak{P}_{N_i}$ son todos los primos de grado i, un producto de k_i de ellos tiene la forma general $\mathfrak{P}_1^{a_1}\cdots\mathfrak{P}_{N_i}^{a_{N_i}}$ con $a_1+\cdots+a_{N_i}=k_i$.

Estos productos se pueden hacer corresponder de manera biyectiva con las elecciones de N_i-1 elementos de un conjunto de k_i+N_i-1 elementos, a saber: los elementos: $a_1, a_1+a_2+1, \ldots, a_1+\cdots+a_{N_i}+(N_i-1)$, como se indica:

$$\begin{array}{ccccccc}
\mathfrak{P}_1\ldots\mathfrak{P}_1 & \sqcup & \mathfrak{P}_2\ldots\mathfrak{P}_2 & \sqcup & \cdots & \sqcup & \mathfrak{P}_{N_i}\ldots\mathfrak{P}_{N_i}\\
\leftrightarrow & \uparrow & \leftrightarrow & \uparrow & & \uparrow & \leftrightarrow\\
a_1 & a_1+1 & a_2 & a_1+a_2+2 & & a_1+\cdots+a_{N_i-1}+(N_i-1) & a_{N_i}
\end{array}$$

y por lo tanto $f_i(k_i) = \binom{k_i+N_i-1}{N_i-1}$.

Así pues,

$$\begin{aligned} A_n &= \sum_{k_1+2k_2+\cdots+nk_n=n} g(k_1,\ldots,k_n) = \sum_{k_1+2k_2+\cdots+nk_n=n} \prod_{i=1}^{n} f_i(k_i) \\ &= \sum_{k_1+2k_2+\cdots+nk_n=n} \prod_{i=1}^{n} \binom{k_i+N_i-1}{N_i-1}. \end{aligned}$$

□

2.4. Campos de Funciones con Número de Clases Pequeño

Por el capítulo anterior tenemos, que si $P_K(u)$ es el numerador de la función zeta de un campo de funciones congruente, entonces
$P_K(u) = a_0 + a_1u + \cdots + a_{2g}u^{2g}$, $u = q^{-s}$, $a_{2g-i} = a_iq^{g-i}$, $a_0 = 1$ y $a_{2g} = q^g$. Además, $a_i = A_i - (q+1)A_{i-1} + qA_{i-2}$.

Por otro lado,

$$P_K(u) = \prod_{i=1}^{2g}(1-\omega_iu), \quad |\omega_i| = q^{1/2}, \quad 1 \le i \le 2g.$$

Finalmente,

$$\begin{aligned} h = P_K(1) &= \sum_{i=0}^{2g} a_i = \sum_{i=0}^{g-1} a_i + a_g + \sum_{i=g+1}^{2g} a_i = \sum_{i=0}^{g-1} a_i + \sum_{i=0}^{g-1} a_{2g-i} + a_g \\ &= \sum_{i=0}^{g-1}(a_i + a_{2g-i}) + a_g = \sum_{i=0}^{g-1}\left(a_i\left(1+q^{g-i}\right)\right) + a_g \\ &= \prod_{i=1}^{2g}(1-\omega_i). \end{aligned}$$

Proposición 2.4.1. *Sean $g = g_K$ el género y $h = h_K$ el número de clases de K. Sea $S(q,g,r) = (q-1)\left[q^{2g-1} + 1 - 2gq^{(2g-1)/2}\right] - r(2g-1)(q^g-1)$. Entonces, si $S(q,g,r) > 0$, se tiene que $h > r$.*

Demostración. Sea K_{2g-1} la extensión de constantes de grado $2g-1$ de K. Por la Hipótesis de Riemann, aplicada a K_{2g-1} con campo de constantes $\mathbb{F}_{q^{2g-1}}$ (K_{2g-1} también es de género g), si N_1' es el número de divisores primos de grado 1 en K_{2g-1}, entonces

$$\left|N_1' - \left(q^{2g-1}+1\right)\right| \leq 2gq^{(2g-1)/2}$$

por lo que $N_1' \geq q^{2g-1}+1-2gq^{(2g-1)/2}$.

Ahora bien, si $d|2g-1$, un primo de grado d en K se descompone en $(d,2g-1)=d$ primos de grado $\dfrac{d}{(d,2g-1)}=1$ en K_{2g-1} (Teorema 1.2.1).

Por otro lado, si un primo de grado 1 en K_{2g-1} se restringe a un primo de grado d, entonces por la Proposición A.29 se tiene que $d|2g-1$.

También se tiene que, a lo más $2g-1$ lugares de grado 1 en K_{2g-1} se pueden restringir al mismo lugar en K. Si $\mathcal{P}_1,\ldots,\mathcal{P}_s$ son primos de grado 1 que se restringen al mismo primo $\mathfrak{P}$ en K, $s\leq 2g-1$, $\mathfrak{P}^{(2g-1)/d_K(\mathfrak{P})}$ es un divisor entero de grado $2g-1$ en K. Así, con a lo más $2g-1$ divisores de grado 1 en K_{2g-1} obtenemos un divisor entero de grado $2g-1$ en K. Como hay N_1' lugares de grado 1 en K_{2g-1}, existen al menos

$$\frac{N_1'}{2g-1} \geq \frac{q^{2g-1}+1-2gq^{(2g-1)/2}}{2g-1}$$

divisores enteros de grado $2g-1$ en K.

Se tiene,

$$A_{2g-1} = h\left(\frac{q^g-1}{q-1}\right) \geq \frac{q^{2g-1}+1-2gq^{(2g-1)/2}}{2g-1}.$$

Por lo tanto

$$h \geq \frac{\left(q^{2g-1}+1-2gq^{(2g-1)/2}\right)(q-1)}{(2g-1)(q^g-1)} = R.$$

Ahora tenemos que,

$$\begin{aligned} h \geq R &= \frac{\left(q^{2g-1}+1-2gq^{(2g-1)/2}\right)(q-1)}{(2g-1)(q^g-1)} \\ &= \frac{S(q,g,r)+r(2g-1)(q^g-1)}{(2g-1)(q^g-1)} \\ &= \frac{S(q,g,r)}{(2g-1)(q^g-1)}+r, \end{aligned}$$

entonces, si $S(q,g,r) > 0$ y como $(2g-1)(q^g-1) > 0$, tenemos que $\dfrac{S(q,g,r)}{(2g-1)(q^g-1)} > 0$, por ello $R > r$, lo cual implica que $h > r$.

□

Tenemos que, derivando con respecto a g,

$$S(q,g,1) = (q-1)\left[q^{2g-1} + 1 - 2gq^{(2g-1)/2}\right] - (2g-1)(q^g-1),$$

y

$$\begin{aligned}
S'(q,g,1) &= (q-1)\left[(2\ln q)(q^{2g-1}) - \left((2g\ln q)(q^{g-1/2}) + 2q^{g-1/2}\right)\right] \\
&\quad - [(2g-1)(\ln q)q^g + 2(q^g-1)] \\
&= (q-1)\left[(2\ln q)(q^{2g-1}) - (2g\ln q)(q^{g-1/2}) - 2q^{g-1/2}\right] \\
&\quad - [(2g\ln q)q^g - (\ln q)q^g + 2q^g - 2] \\
&= (2\ln q)q^g\left[(q^{g-1})(q-1) - gq^{-1/2}(q-1) - g + \frac{1}{2}\right] \\
&\quad -2q^{g-1/2}(q-1) - 2q^g + 2 \\
&= (2\ln q)q^g\left[(q^{g-1})(q-1) - g(q^{1/2} - q^{-1/2}) - g + \frac{1}{2}\right] \\
&\quad -2q^{g+1/2} + 2q^{g-1/2} - 2q^g + 2 \\
&= (2\ln q)q^g\left[(q^{g-1})(q-1) - g(q^{1/2} - q^{-1/2} + 1) + \frac{1}{2}\right] \\
&\quad -2q^g(q^{1/2} - q^{-1/2} + 1) + 2 \\
&= 2q^g\left[\ln q(q^{g-1})(q-1) - (g\ln q + 1)(q^{1/2} - q^{-1/2} + 1) + \frac{\ln q}{2}\right] \\
&\quad +2.
\end{aligned}$$

Sea $S_1(q,g,1) = \ln q(q^{g-1})(q-1) - (g\ln q + 1)(q^{1/2} - q^{-1/2} + 1) + \dfrac{\ln q}{2}$. Entonces

$$\begin{aligned}
S_1'(q,g,1) &= (\ln q)^2(q^{g-1})(q-1) - \ln q(q^{1/2} - q^{-1/2} + 1) \\
&= \ln q\left[\ln q(q^{g-1})(q-1) - (q^{1/2} - q^{-1/2} + 1)\right].
\end{aligned}$$

Si $S_2(q,g,1) = \ln q(q^{g-1})(q-1) - (q^{1/2} - q^{-1/2} + 1)$, tenemos $S_2'(q,g,1) = (\ln q)^2(q^{g-1})(q-1) > 0$.

Ahora podemos ver que $S(q,g,1)$ es creciente como función de g para $q = 4$, $g \geq 2$ o $q = 3$, $g \geq 3$ o $q = 2$, $g \geq 5$.

Si $q = 4$, $g \geq 2$, tenemos que $S_2(4,2,1) = 12\ln 4 - \dfrac{5}{2} > 0$, lo cual implica que $S_1'(4,2,1) > 0$, y como además $S_2'(q,g,1) > 0$, para $q = 4$, $g \geq 2$, tenemos $S_1'(q,g,1)$ es creciente y positiva, para $q = 4$, $g \geq 2$.

Ahora $S_1(4,2,1) = \dfrac{15}{2}\ln 4 - \dfrac{5}{2} > 0$, lo cual implica que $S'(4,2,1) > 0$, y como además $S_1'(q,g,1) > 0$, para $q = 4$, $g \geq 2$, tenemos $S'(q,g,1)$ es creciente y positiva, para $q = 4$, $g \geq 2$ y por lo tanto $S(q,g,1)$ es creciente para $q = 4$, $g \geq 2$.

Si $q = 3$, $g \geq 3$, tenemos que $S_2(3,3,1) = 18\ln 3 - \left(\dfrac{2+\sqrt{3}}{\sqrt{3}}\right) > 0$, lo cual implica que $S_1'(3,3,1) > 0$, y como además $S_2'(q,g,1) > 0$, para $q = 3$, $g \geq 3$, tenemos $S_1'(q,g,1)$ es creciente y positiva, para $q = 3$, $g \geq 3$.

Ahora $S_1(3,3,1) = \dfrac{37}{2}\ln 3 - (3\ln 3 + 1)\left(\dfrac{2+\sqrt{3}}{\sqrt{3}}\right) > 0$, lo cual implica que $S'(3,3,1) > 0$, y como además $S_1'(q,g,1) > 0$, para $q = 3$, $g \geq 3$, tenemos $S'(q,g,1)$ es creciente y positiva, para $q = 3$, $g \geq 3$ y por lo tanto $S(q,g,1)$ es creciente para $q = 3$, $g \geq 3$.

Si $q = 2$, $g \geq 5$, tenemos que $S_2(2,5,1) = 16\ln 2 - \left(\dfrac{1+\sqrt{2}}{\sqrt{2}}\right) > 0$, lo cual implica que $S_1'(2,5,1) > 0$, y como además $S_2'(q,g,1) > 0$, para $q = 2$, $g \geq 5$, tenemos $S_1'(q,g,1)$ es creciente y positiva, para $q = 2$, $g \geq 5$.

Ahora $S_1(2,5,1) = \dfrac{33}{2}\ln 2 - (5\ln 2 + 1)\left(\dfrac{1+\sqrt{2}}{\sqrt{2}}\right) > 0$, lo cual implica que $S'(2,5,1) > 0$, y como además $S_1'(q,g,1) > 0$, para $q = 2$, $g \geq 5$, tenemos $S'(q,g,1)$ es creciente y positiva, para $q = 2$, $g \geq 5$ y por lo tanto $S(q,g,1)$ es creciente para $q = 2$, $g \geq 5$.

Por otro lado,

$$\begin{aligned} S(4,2,1) &= 3(50-32) = 54 > 0, \\ S(3,3,1) &= 2(179 - 54\sqrt{3}) > 0, \\ S(2,5,1) &= 2(117 - 80\sqrt{2}) > 0. \end{aligned}$$

En consecuencia, tendremos:

Teorema 2.4.2. *Se tiene que $h_K > 1$ si $q = 4$, $g \geq 2$; $q = 3$, $g \geq 3$; $q = 2$, $g \geq 5$.*

□

Por otro lado:

Teorema 2.4.3. *Si $g \geq 1$, entonces para $q \geq 5$, $h_K > 1$.*

Demostración. Sea $P_K(u) = \prod_{i=1}^{2g}(1 - \omega_i u)$ el numerador de la función zeta de K. Entonces, por la Hipótesis de Riemann tenemos:

$$\begin{aligned} h &= P_K(1) = \prod_{i=1}^{2g}(1-\omega_i) = \left|\prod_{i=1}^{2g}(1-\omega_i)\right| = \prod_{i=1}^{2g}|1-\omega_i| \\ &\geq \prod_{i=1}^{2g}(|\omega_i|-1) = \prod_{i=1}^{2g}(\sqrt{q}-1) = (\sqrt{q}-1)^{2g} \\ &\geq (\sqrt{q}-1)^2 \geq (\sqrt{5}-1)^2 > 1, \end{aligned}$$

por lo tanto, $h > 1$.

□

Así pues, vemos que es muy limitado nuestro número de posibilidades para que un campo K tenga número de clases 1. Si $g = 0$, $h = 1$, pero si $g \geq 1$, sólo es posible $h = 1$ cuando: $q = 4$, $g = 1$; $q = 3$, $g = 1, 2$; $q = 2$, $g = 1, 2, 3, 4$.

Podemos estudiar la función $S(q, g, r)$ para diversos valores de r y dar criterios para que $h > r$. Aquí sólo presentamos los resultados para $2 \leq r \leq 10$ enumerando las posibilidades para g y q. Esto de ninguna manera nos dice que dada una posible terna (q, g, r) tal que $S(q, g, r) \leq 0$, necesariamente exista un campo con género g, campo de constantes $\mathbb{F}_q$ y que tenga número de clases $h = r$.

Teorema 2.4.4. *Sea K un campo de funciones congruente con campo de constantes $k = \mathbb{F}_q$ con género $g \geq 1$ y número de clases h, $2 \leq h \leq 10$. Entonces tenemos:*

(i) *Si* $h = 2$, *entonces* $q = 2, 3, 4$ *y*

$$\text{si } q = 4,\ g = 1,$$

$$\text{si } q = 3,\ g = 1 \text{ o } 2,$$

$$\text{si } q = 2,\ g \leq 5.$$

(ii) *Si* $h = 3$, *entonces* $q \leq 7$, $g \leq 6$.

(iii) *Si* $h = 4$, *entonces* $q \leq 8$, $g \leq 6$.

(iv) *Si* $h = 5$, *entonces* $q \leq 9$, $g \leq 7$.

(v) *Si* $h = 6$, *entonces* $q \leq 11$, $g \leq 7$.

(vi) *Si* $h = 7$, *entonces* $q \leq 13$, $g \leq 7$.

(vii) *Si* $h = 8$, *entonces* $q \leq 13$, $g \leq 8$.

(viii) *Si* $h = 9$, *entonces* $q \leq 16$, $g \leq 8$.

(ix) *Si* $h = 10$, *entonces* $q \leq 17$, $g \leq 8$.

Demostración. Únicamente obtendremos, para un valor de h fijo, una cota superior para q. Anteriormente (demostración del Teorema 2.4.3) obtuvimos que $h \geq (\sqrt{q} - 1)^{2g}$, entonces $h^{\frac{1}{2g}} \geq \sqrt{q} - 1$, de donde $h^{\frac{1}{2g}} + 1 \geq \sqrt{q}$, luego $(h^{\frac{1}{2g}} + 1)^2 \geq q$. Por lo tanto $q \leq \left(\sqrt{h} + 1\right)^2$.

Si $h = 2$, tenemos que $q \leq \left(\sqrt{2} + 1\right)^2 < 5.83$, luego $q \leq 5$.
Ahora si $h = 3$, tenemos que $q \leq \left(\sqrt{3} + 1\right)^2 < 7.47$, luego $q \leq 7$.
Si $h = 4$, tenemos que $q \leq \left(\sqrt{4} + 1\right)^2 = 9$, luego $q \leq 9$.
Si $h = 5$, tenemos que $q \leq \left(\sqrt{5} + 1\right)^2 < 10.47$, luego $q \leq 10$.
Si $h = 6$, tenemos que $q \leq \left(\sqrt{6} + 1\right)^2 < 11.89$, luego $q \leq 11$.
Si $h = 7$, tenemos que $q \leq \left(\sqrt{7} + 1\right)^2 < 13.29$, luego $q \leq 13$.
Si $h = 8$, tenemos que $q \leq \left(\sqrt{8} + 1\right)^2 < 14.65$, luego $q \leq 14$.
Si $h = 9$, tenemos que $q \leq \left(\sqrt{9} + 1\right)^2 = 16$, luego $q \leq 16$.
Si $h = 10$, tenemos que $q \leq \left(\sqrt{10} + 1\right)^2 < 17.32$, luego $q \leq 17$. □

Observación. El Teorema 2.4.4 puede ser mejorado fijando primero h, después g y finalmente los posibles q. Por ejemplo, si $h = 10$, $g = 6$, necesariamente $q = 2$ y no $q \leq 17$ como está enunciado en el teorema.

A continuación enunciamos el teorema que nos da todos los posibles campos K con número de clases 1 (con género ≥ 1). La demostración se basa en un análisis detallado de la función $P_K(u)$.

Teorema 2.4.5. *(LEITZEL, MADAN & QUEEN) [9, 10] Se tiene que, salvo isomorfismo, existen exactamente siete campos de funciones congruentes $K/\mathbb{F}_q$ con número de clases 1 y género $g \neq 0$. Si $K = \mathbb{F}_q(X, Y)$ es tal campo, entonces los siete campos están definidos por:*

(I) $q = 2$, $g = 1$, $Y^2 + Y = X^3 + X + 1$,

(II) $q = 2$, $g = 2$, $Y^2 + Y = X^5 + X^3 + 1$,

(III) $q = 2$, $g = 2$, $Y^2 + Y = (X^3 + X^2 + 1)(X^3 + X + 1)^{-1}$,

(IV) $q = 2$, $g = 3$, $Y^4 + XY^3 + (X^2 + X)Y^2 + (X^3 + 1)Y + (X^4 + X + 1) = 0$,

(V) $q = 2$, $g = 3$, $Y^4 + (X^3 + X + 1)Y + (X^4 + X + 1) = 0$,

(VI) $q = 3$, $g = 1$, $Y^2 = X^3 + 2X + 2$,

(VII) $q = 4$, $g = 1$, $Y^2 + Y = X^3 + \alpha$, $\alpha \in \mathbb{F}_4 \backslash \{0, 1\}$.

□

A continuación detallamos una de las técnicas para probar este tipo de resultado. Sea

$$1 = h = P_K(1) = \sum_{i=0}^{2g} a_i = \sum_{i=0}^{g-1} \left(\left(q^{g-i} + 1 \right) a_i \right) + a_g.$$

Sea $s_n = \sum_{i=1}^{2g} \omega_i^n$, donde $P_K(u) = \prod_{i=1}^{2g} (1 - \omega_i u)$. Entonces, por el Teorema 2.3.5, tenemos que $-s_n = \sum_{d|n} d(N_d - n_d)$.

Ahora,

$$\begin{aligned} u^{-2g}P_K(u) &= u^{-2g}\prod_{i=1}^{2g}(1-\omega_i u) = u^{-2g}\prod_{i=1}^{2g}u(u^{-1}-\omega_i) = \prod_{i=1}^{2g}(u^{-1}-\omega_i) \\ &= u^{-2g}\sum_{i=0}^{2g}a_i u^i = a_0u^{-2g} + a_1u^{-2g+1} + \cdots + a_{2g}, \end{aligned}$$

es decir, $\omega_1, \ldots, \omega_{2g}$ son las raíces de $u^{-2g}P_K(u) = Q_K(v)$, con $v = u^{-1}$. Se tiene que $Q_K(v) = b_0 + b_1v + \cdots + b_{2g}v^{2g} = \prod_{i=1}^{2g}(v-\omega_i)$ con $b_i = a_{2g-i} = q^{g-i}a_i$, $b_{2g} = a_0 = 1$.

Por las Identidades de Newton (Teorema 2.1.4), se tiene: $b_{2g-i} = a_i = (-1)^{2g-i}\sigma_i = (-1)^i\sigma_i$, donde σ_i es el $i-$ésimo polinomio elemental simétrico en $\omega_1, \ldots, \omega_{2g}$, por lo que $s_m + s_{m-1}a_1 + \cdots + s_1a_{m-1} + ma_m = 0$, $1 \leq m \leq 2g-1$.

Así:

$$\begin{aligned} s_1 + a_1 = 0, \quad & a_1 = -s_1, \\ s_2 + s_1a_1 + 2a_2 = 0, \quad & a_2 = \frac{-s_2 - s_1a_1}{2} = \frac{s_1^2 - s_2}{2}, \\ & a_3 = -\frac{s_1^3 - 3s_1s_2 + 2s_3}{6}, \\ & a_4 = \frac{s_1^4 - 6s_1^2s_2 + 8s_1s_3 + 3s_2^2 - 6s_4}{24}, \text{etc.} \end{aligned}$$

Por otro lado, como

$$n_d = \begin{cases} q+1 & , \quad d = 1 \\ \dfrac{1}{d}\displaystyle\sum_{f|d}\mu\left(\frac{d}{f}\right)q^f & , \quad d > 1 \end{cases}$$

y

$$s_n = -\sum_{d|n} d(N_d - n_d),$$

obtenemos, después de hacer todas las sustituciones:

$$\begin{aligned}
a_1 &= N_1 - (q+1), \\
2a_2 &= s_1^2 - s_2 = (N_1 - (q+1))^2 + \left(\sum_{d|2} d(N_d - n_d) \right) \\
&= (N_1 - (q+1))^2 + ((N_1 - n_1) + 2(N_2 - n_2)) \\
&= \left(N_1^2 - 2N_1(q+1) + (q+1)^2\right) \\
&\quad + \left((N_1 - (q+1)) + 2 \left(N_2 - \frac{1}{2} \sum_{f|2} \mu\left(\frac{2}{f}\right) q^f \right) \right) \\
&= \left(N_1^2 - 2N_1(q+1) + (q+1)^2\right) \\
&\quad + \left((N_1 - (q+1)) + 2 \left(N_2 - \frac{1}{2} \left(\mu\left(\frac{2}{1}\right) q^1 + \mu\left(\frac{2}{2}\right) q^2 \right) \right) \right) \\
&= N_1^2 - 2N_1(q+1) + (q+1)^2 + N_1 - (q+1) + 2N_2 - (-q + q^2) \\
&= N_1^2 - 2N_1(q+1) + (q+1)^2 + N_1 + 2N_2 - (1 + q^2) \\
&= N_1^2 - 2N_1(q+1) + (q^2 + 2q + 1) + N_1 + 2N_2 - (1 + q^2) \\
&= N_1^2 - (2q+1)N_1 + 2N_2 + 2q.
\end{aligned}$$

Para $g \geq 1$, se tiene $N_1 \leq 1$, pues si existiesen dos divisores primos de grado 1, digamos $\mathcal{P}_1, \mathcal{P}_2$, puesto que $h = 1$, $\dfrac{\mathcal{P}_1}{\mathcal{P}_2} = (x)$ sería principal y por tanto $[K : k(x)] = \deg(\eta_x) = \deg(\mathcal{P}_2) = 1$ (Teorema A.21); por lo que $g = 0$, lo cual es absurdo. Así $N_1 \leq 1$.

Ahora, si $q = 3$, $g = 2$, obtenemos:

$$\begin{aligned}
P_K(1) &= h = (q^2+1)a_0 + (q+1)a_1 + a_2 \\
&= 10 + 4a_1 + a_2 = \frac{-6 + N_1 + N_1^2 + 2N_2}{2}.
\end{aligned}$$

Por lo tanto $h = 1 \Leftrightarrow N_1^2 + N_1 + 2N_2 = 8$.

Por otro lado, por la Hipótesis de Riemann, se tiene que los recíprocos

de las raíces de $P_K(u)$ son: $\sqrt{3}e^{\pm i\theta_1}$, $\sqrt{3}e^{\pm i\theta_2}$, por lo que:

$$\begin{aligned}
P_K(u) &= \left(1-\sqrt{3}e^{i\theta_1}u\right)\left(1-\sqrt{3}e^{-i\theta_1}u\right)\left(1-\sqrt{3}e^{i\theta_2}u\right)\left(1-\sqrt{3}e^{-i\theta_2}u\right)\\
&= \left(1-\sqrt{3}e^{-i\theta_1}u-\sqrt{3}e^{i\theta_1}u+3u^2\right)\\
&\quad \left(1-\sqrt{3}e^{-i\theta_2}u-\sqrt{3}e^{i\theta_2}u+3u^2\right)\\
&= \left(1-\sqrt{3}[(\cos\theta_1-i\text{sen}\theta_1)+(\cos\theta_1+i\text{sen}\theta_1)]u+3u^2\right)\\
&\quad \left(1-\sqrt{3}[(\cos\theta_2-i\text{sen}\theta_2)+(\cos\theta_2+i\text{sen}\theta_2)]u+3u^2\right)\\
&= \left(1-2\sqrt{3}\cos\theta_1 u+3u^2\right)\left(1-2\sqrt{3}\cos\theta_2 u+3u^2\right)\\
&= 1+\left(-2\sqrt{3}\cos\theta_1\right)u+3u^2+\left(-2\sqrt{3}\cos\theta_2\right)u\\
&\quad +12\cos\theta_1\cos\theta_2 u^2-6\sqrt{3}\cos\theta_2 u^3+3u^2-6\sqrt{3}\cos\theta_1 u^3+9u^4\\
&= 1+(-2)\sqrt{3}(\cos\theta_1+\cos\theta_2)u+(6+12\cos\theta_1\cos\theta_2)u^2\\
&\quad +(-6)\sqrt{3}(\cos\theta_1+\cos\theta_2)u^3+9u^4
\end{aligned}$$

Comparando coeficientes obtenemos:

$$\begin{aligned}
a_1 = N_1-(q+1) = N_1-4 &= -2\sqrt{3}(\cos\theta_2+\cos\theta_1)\\
\Rightarrow \cos\theta_2+\cos\theta_1 = \frac{-(4-N_1)}{-2\sqrt{3}} &= \frac{(4-N_1)\sqrt{3}}{(2\sqrt{3})\sqrt{3}} = \frac{(4-N_1)\sqrt{3}}{6}\\
\Rightarrow \cos\theta_2+\cos\theta_1 &= \frac{(4-N_1)\sqrt{3}}{6}
\end{aligned}$$

$$\begin{aligned}
2a_2 &= N_1^2-(2q+1)N_1+2N_2+2q = N_1^2-7N_1+2N_2+6\\
&= 24\cos\theta_1\cos\theta_2+12
\end{aligned}$$

$$\Rightarrow \cos\theta_1\cos\theta_2 = \frac{N_1^2-7N_1+2N_2-6}{24}.$$

Como $N_1^2+N_1+2N_2=8$, obtenemos:

$$\begin{aligned}
\cos\theta_1\cos\theta_2 &= \frac{N_1^2-7N_1+2N_2-6}{24}\\
&= \frac{N_1^2-7N_1+2N_2-6+N_1-N_1}{24}\\
&= \frac{N_1^2+N_1+2N_2-8N_1-6}{24}\\
&= \frac{8-8N_1-6}{24} = \frac{2-8N_1}{24}\\
&= \frac{2(1-4N_1)}{2(12)} = \frac{1-4N_1}{12}.
\end{aligned}$$

Sea

$$\begin{aligned} f(x) &= (x-\cos\theta_1)(x-\cos\theta_2) \\ &= x^2 - x\cos\theta_2 - x\cos\theta_1 + \cos\theta_1\cos\theta_2 \\ &= x^2 - (\cos\theta_2+\cos\theta_1)x + \cos\theta_1\cos\theta_2 \\ &= x^2 + \left(\frac{(N_1-4)\sqrt{3}}{6}\right)x + \left(\frac{1-4N_1}{12}\right) \\ &= \frac{12x^2 + 2\sqrt{3}(N_1-4)x + (1-4N_1)}{12}, \end{aligned}$$

es decir, $\cos\theta_1$, $\cos\theta_2$ son las raíces de $f(x)$. Sin embargo notemos que se tiene:

$$\begin{aligned} 0 &\leq (1-\cos\theta_1)(1-\cos\theta_2) = f(1) = \frac{12+2\sqrt{3}(N_1-4)+(1-4N_1)}{12} \\ &= \frac{(12-8\sqrt{3}+1)+N_1(2\sqrt{3}-4)}{12} < 0, \end{aligned}$$

lo cual es absurdo. En consecuencia, si $q=3$ y $g=2$, entonces necesariamente $h>1$.

Ejemplo 2.4.6. Consideramos el caso I del Teorema 2.4.5, es decir, el campo $K=\mathbb{F}_2(X,Y)$ donde $Y^2+Y=X^3+X+1$. Entonces $h=1$, $q=2$, $g=1$. Tenemos $P_K(u)=1-2u+2u^2$ pues $a_1=h-(q+1)=1-(3)=2$.

Las raíces de $P_K(u)$ son $\omega_1^{-1}=\dfrac{1+i}{2}$ y $\omega_2^{-1}=\dfrac{1-i}{2}$. Luego $\omega_1=\dfrac{2}{1+i}$ y $\omega_2=\dfrac{2}{1-i}$. Observamos $|\omega_1|=\left|\dfrac{2}{1+i}\right|=\dfrac{2}{\sqrt{1^2+1^2}}=\dfrac{2}{\sqrt{2}}=\sqrt{2}$ y $|\omega_2|=\sqrt{2}$.

2.5. El Número de Clases de Campos de Funciones Congruentes

Sea $K/\mathbb{F}_q$ un campo de funciones congruente. Su función zeta está dada por $Z_K(u)=\dfrac{P_K(u)}{(1-u)(1-qu)}$, donde $P_K(u)=\displaystyle\sum_{i=0}^{2g} a_i u^i$, $a_{2g-i}=a_i q^{g-i}$ para $0\leq i\leq 2g$, y $g=g_K$ es el género de K (Teorema 1.4.1). Entonces $P_K(1)=h_K$ es el número de clases de K (Corolario 1.3.9).

Sea $K_n := K\mathbb{F}_{q^{l^n}}$ la extensión de constantes de grado l^n, donde l es un primo racional ($q = p^t$, $l = p$ o $l \neq p$). Entonces

$$Z_{K_n}(u^{l^n}) = \prod_{j=1}^{l^n} Z_K(\xi_{l^n}^j u),$$

donde ξ_{l^n} es cualquier l^n-ésima raíz primitiva de 1 en $\mathbb{C}^*$ (Teorema 2.1.6).

Tenemos $P_K(u) = \prod_{i=1}^{2g}(1 - \alpha_i^{-1}u)$ donde $\alpha_1, \ldots, \alpha_{2g}$ son las raíces de $P_K(u)$. Así que $P_{K_n}(u^{l^n}) = \prod_{i=1}^{2g}\prod_{j=1}^{l^n}(1 - \alpha_i^{-1}\xi_{l^n}^j u)$.

Por lo tanto, si h_n es el número de clases de K_n, tenemos:

$$\begin{aligned}
\frac{h_n}{h} &= \frac{P_{K_n}(1)}{P_K(1)} \\
&= \frac{\prod_{i=1}^{2g}\left(\prod_{j=1}^{l^n}(1 - \xi_{l^n}^j \alpha_i^{-1})\right)}{\prod_{i=1}^{2g}(1 - \alpha_i^{-1})} \\
&= \frac{\prod_{i=1}^{2g}\left[\left(\prod_{j=1}^{l^n-1}(1 - \xi_{l^n}^j \alpha_i^{-1})\right)(1 - \xi_{l^n}^{l^n} \alpha_i^{-1})\right]}{\prod_{i=1}^{2g}(1 - \alpha_i^{-1})} \\
&= \frac{\prod_{i=1}^{2g}\left[\left(\prod_{j=1}^{l^n-1}(1 - \xi_{l^n}^j \alpha_i^{-1})\right)(1 - \alpha_i^{-1})\right]}{\prod_{i=1}^{2g}(1 - \alpha_i^{-1})} \\
&= \prod_{i=1}^{2g}\prod_{j=1}^{l^n-1}(1 - \xi_{l^n}^j \alpha_i^{-1}).
\end{aligned}$$

Teorema 2.5.1. *Con la notación de arriba, sea l^{e_n} una potencia exacta de l que divide a h_n. Entonces*

$$e_n = \lambda n + \gamma$$

para n suficientemente grande, con $0 \leq \lambda \leq 2g$ y $\gamma \in \mathbb{Z}$.

Demostración. Tenemos

$$\frac{h_n}{h} = \prod_{j=1}^{l^n-1} \prod_{i=1}^{2g} (1 - \xi_{l^n}^j \alpha_i^{-1}) = \prod_{j=1}^{l^n-1} P_K(\xi_{l^n}^j).$$

Ahora, $P_K(T) \in \mathbb{Z}[T]$, por lo tanto $P_K(T)$ tiene la forma $P_K(T) = 1 + a_1 T + \ldots + q^g T^{2g}$. Sea

$$\begin{aligned} R_K(T) &= P_K(T+1) = 1 + a_1(T+1) + \ldots + q^g (T+1)^{2g} \\ &= b_0 + b_1 T + \ldots + b_{2g} T^{2g}. \end{aligned}$$

Tenemos,

$$P_K(\xi_{l^n}^j) = R_K(\xi_{l^n}^j - 1) = b_0 + b_1(\xi_{l^n}^j - 1) + \ldots + b_{2g}(\xi_{l^n}^j - 1)^{2g}. \qquad (2.1)$$

Notemos que $R_K(-1) = P_K(0) = a_0 = 1$. Por lo tanto existe $0 \leq \lambda \leq 2g$ tal que $l \nmid b_\lambda$. Elegimos el mínimo λ con esta propiedad.

En el campo de números ciclotómico $\mathbb{Q}(\xi_{l^n})/\mathbb{Q}$, l es totalmente ramificado y $(l) = (1 - \xi_{l^n})^{\varphi(l^n)} = \left(1 - \xi_{l^n}^j\right)^{\varphi(l^n)}$ para todo $(j, l) = 1$, donde φ es la función fi de Euler. Sea $\mathfrak{L} = (1 - \xi_{l^n})$ el ideal primo de $\mathbb{Q}(\xi_{l^n})$ arriba de l, es decir, $\upsilon_{\mathfrak{L}}(1 - \xi_{l^n}) = 1$. Si $j = l^m j_1$, $m < n$, $(j_1, l) = 1$, entonces

$$1 - \xi_{l^n}^j = 1 - \xi_{l^{n-m}}^{j_1} = (1 - \xi_{l^n})^{l^m} u$$

con u una unidad en $\mathbb{Q}(\xi_{l^n})$. Por lo tanto $\upsilon_{\mathfrak{L}}\left(1 - \xi_{l^n}^j\right) = l^m = \upsilon_{\mathfrak{l}}(j)$. Entonces, en (2.1) tenemos

$$\upsilon_{\mathfrak{L}}\left(b_i \left(\xi_{l^n}^j - 1\right)^i\right) = \upsilon_{\mathfrak{L}}(b_i) + i\upsilon_{\mathfrak{L}}\left(\xi_{l^n}^j - 1\right) = \upsilon_{\mathfrak{l}}(b_i)\varphi(l^n) + i\upsilon_{\mathfrak{l}}(j).$$

Sea ξ una raíz l^n-ésima primitiva de 1. Entonces, para $0 \leq i \leq \lambda - 1$,

$$\upsilon_{\mathfrak{L}}\left(b_i \left(\xi^j - 1\right)^i\right) \geq \varphi(l^n) + i > \lambda = \upsilon_{\mathfrak{L}}\left(b_\lambda (\xi - 1)^\lambda\right)$$

para n tal que $\varphi(l^n) > \lambda - i$.

Para $\lambda < i \leq 2g$,

$$v_{\mathfrak{L}}\left(b_i\left(\xi-1\right)^i\right) \geq i > \lambda = v_{\mathfrak{L}}\left(b_\lambda\left(\xi-1\right)^\lambda\right).$$

Por lo tanto, para una raíz l^n-ésima primitiva ξ de 1 con $\varphi(l^n) > \lambda$,

$$v_{\mathfrak{L}}\left(P_K\left(\xi\right)\right) = v_{\mathfrak{L}}\left(R_K\left(\xi-1\right)\right) = \lambda. \tag{2.2}$$

Sea $n_0 \in \mathbb{N}$ tal que $\varphi(l^{n_0}) > \lambda$. Para $n-1 > \lambda$ tenemos

$$\frac{h_n}{h_{n-1}} = \frac{h_n}{h}\left(\frac{1}{\left(\frac{h_{n-1}}{h}\right)}\right) = \frac{\prod\limits_{j=1}^{l^n-1} P_K(\xi_{l^n}^j)}{\prod\limits_{j=1}^{l^{n-1}-1} P_K(\xi_{l^{n-1}}^j)} = \prod_{\xi} P_K(\xi),$$

donde el último producto corre a través de todas las raíces l^n-ésimas primitivas de 1.

Usando (2.2) y el hecho de que hay $\varphi(l^n)$ raíces l^n-ésimas primitivas de 1, obtenemos:

$$\begin{aligned} v_l(h_n) &= v_l(h_{n-1}) + v_l\left(\prod_{\xi} P_K(\xi)\right) \\ &= v_l(h_{n-1}) + \frac{1}{\varphi(l^n)} v_{\mathfrak{L}}\left(\prod_{\xi} P_K(\xi)\right) \\ &= v_l(h_{n-1}) + \frac{1}{\varphi(l^n)}\phi(l^n)\lambda = v_l(h_{n-1}) + \lambda. \end{aligned}$$

Por lo tanto

$$v_l(h_n) = \lambda(n-n_0) + v_l(h_{n_0}) = \lambda n + (v_l(h_{n_0}) - n_0\lambda) = \lambda n + \gamma.$$

□

Observemos que el Teorema 2.5.1 dice que el Invariante μ de Iwasawa para campos de funciones congruentes es 0.

2.6. Análogo al Teorema de Brauer-Siegel

El Teorema de Brauer-Siegel es un teorema en campos númericos, es decir, extensiones finitas de $\mathbb{Q}$. Para un campo númerico F, sean d su discriminante, R su regulador y h su número de clases. Entonces

Teorema 2.6.1. *(Brauer-Siegel) Se tiene que* $\lim_{|d|\to\infty} \dfrac{\ln(hR)}{\ln\sqrt{|d|}} = 1$

□

El propósito de esta sección es presentar un análogo a este resultado. Sea K/k un campo de funciones congruente con $k = \mathbb{F}_q$. Todas las extensiones de K consideradas en esta sección tienen precisamente a k como su campo de constantes.

Tenemos que n_m, N_m son el número de divisores primos de grado m en los campos de funciones racionales $k(x)$ y K, respectivamente, entonces (Teorema 2.3.5):

$$\begin{aligned}
\left|n_m - \frac{q^m}{m}\right| &= \left|\sum_{\substack{d|m\\ d<m}} \mu\left(\frac{m}{d}\right) q^d\right| \leq \sum_{d=1}^{[m/2]} q^d = q\frac{q^{[m/2]}-1}{q-1} \\
&\leq 2\left(q^{[m/2]}-1\right) = 2q^{[m/2]} - 2 < 2q^{[m/2]} \leq 2q^{m/2} \\
&\therefore \left|n_m - \frac{q^m}{m}\right| < 2q^{m/2} \\
|N_m - n_m| &= \frac{1}{m}\left|\sum_{d|m} \mu\left(\frac{m}{d}\right) s^d\right| \leq \frac{1}{m}\left(\sum_{d=1}^{m}\left|\sum_{i=1}^{2g} \omega_i^d\right|\right) \\
&\leq \frac{1}{m}\left(\sum_{d=1}^{m}\left(\sum_{i=1}^{2g} |\omega_i^d|\right)\right) = \frac{1}{m}\left(\sum_{d=1}^{m}\left(\sum_{i=1}^{2g} |\omega_i|^d\right)\right) \\
&= \frac{1}{m}\left(\sum_{d=1}^{m}\left(\sum_{i=1}^{2g} q^{d/2}\right)\right) \\
&= \frac{2g}{m}\sum_{d=1}^{m} q^{d/2} = \frac{2g}{m} q^{1/2}\frac{q^{m/2}-1}{q^{1/2}-1} \leq \frac{2g}{m} 2(q^{m/2}-1) \\
&= \frac{4g}{m}(q^{m/2}-1) = \frac{4gq^{m/2}}{m} - \frac{4g}{m} \leq \frac{4gq^{m/2}}{m} \leq 4gq^{m/2} \\
&\therefore |N_m - n_m| \leq 4gq^{m/2}.
\end{aligned}$$

Ahora bien, el número de divisores enteros de grado $2g$ es

$$A_{2g} = h\frac{q^{g+1}-1}{q-1},$$

y se tiene

$$N_{2g} \geq n_{2g} - 4gq^g > \frac{q^{2g}}{2g} - 2q^g - 4gq^g = \frac{q^{2g}}{2g} - (4g+2)q^g.$$

Luego $h\dfrac{q^{g+1}-1}{q-1} = A_{2g} \geq N_{2g} > \dfrac{q^{2g}}{2g} - (4g+2)q^g$, por lo tanto

$$\begin{aligned} h &> \frac{q-1}{q^{g+1}-1}\left(\frac{q^{2g}}{2g} - (4g+2)q^g\right) \\ &= \frac{q^g}{2g}\frac{(q-1)}{q^g(q^{g+1}-1)}\left(q^{2g} - (4g+2)2gq^g\right) \\ &= \frac{q^g}{2g}\left[\frac{(q-1)}{(q^{g+1}-1)}\left(q^g - (4g+2)2g\right)\right] \geq \frac{q^g}{2g}\left(\frac{q-1}{q}\right)^2 \\ &= \frac{q^g}{2g}(C), \end{aligned}$$

donde g es suficientemente grande y $C = \left(\dfrac{q-1}{q}\right)^2$.

Teorema 2.6.2. *Si k permanece fijo, entonces* $\liminf\limits_{g\to\infty} \dfrac{\ln h}{g\ln q} \geq 1$.

Demostración. Se tiene $h \geq q^g\dfrac{C}{2g}$, C una constante y g suficientemente grande. Por tanto $\ln h \geq g\ln q + \ln C - \ln 2g$,

$$\frac{\ln h}{g\ln q} \geq \frac{g\ln q + \ln C - \ln 2g}{g\ln q} = 1 + \frac{\ln C}{g\ln q} - \frac{\ln 2g}{g\ln q}$$

y el lado derecho tiende a 1 cuando $g \to \infty$, ya que $\lim\limits_{g\to\infty} \dfrac{\ln C}{g\ln q} = 0$ y $\lim\limits_{g\to\infty} \dfrac{\ln 2g}{g\ln q} = \lim\limits_{g\to\infty} \dfrac{\frac{2}{2g}}{\ln q} = \lim\limits_{g\to\infty} \dfrac{2}{2g\ln q} = \lim\limits_{g\to\infty} \dfrac{1}{g\ln q} = 0$, de lo cual se sigue el teorema.

□

Para obtener un análogo al Teorema de Brauer-Siegel debemos probar que $\limsup\limits_{g\to\infty} \dfrac{\ln h}{g\ln q} \leq 1$. Esto sigue siendo un problema abierto. Probaremos que el resultado sí se cumple con una restricción.

Sea $\{K_\alpha\}_{\alpha\in\Lambda}$ una colección de campos de funciones congruentes, todos ellos con campo de constantes k. Para $\alpha \in \Lambda$, sea $m_\alpha = \text{ínf}\{[K_\alpha : k(x)]|x \in K_\alpha\backslash k\}$ y sea $g_\alpha > 0$, el género de K_α. Dado $\epsilon > 0$, existe un subconjunto finito Γ de Λ tal que $\forall\ \alpha \in \Lambda\backslash\Gamma$ se cumple $\dfrac{m_\alpha}{g_\alpha} < \epsilon$.

Teorema 2.6.3. *Para una colección de campos como la de arriba, se tiene* $\lim\limits_{\frac{m}{g}\to 0} \dfrac{\ln h}{g \ln q} = 1$, *con g el género de K, h el número de clases de K y m el mínimo entero tal que existe $x \in K\backslash k$ con $[K : k(x)] = m$.*

Demostración. Para un divisor entero $\mathfrak{A}$ de K tenemos por el Teorema de Riemann-Roch [A.23] $l(\mathfrak{A}^{-1}) \geq d(\mathfrak{A}) - g + 1$, por lo que $A_n \geq h\dfrac{q^{n-g+1}-1}{q-1}$ (ver Teorema 1.2.5) y por lo tanto si $\zeta_K(s)$ es la función zeta de K, $s \in \mathbb{R}$, $s > 1$, entonces

$$\begin{aligned}\zeta_K(s) &= \sum_{n=0}^{\infty} A_n q^{-ns} \geq \sum_{n=g}^{\infty} A_n q^{-ns} \geq \sum_{n=g}^{\infty} h\frac{q^{n-g+1}-1}{q-1}\frac{1}{q^{ns}} \\ &= \frac{h}{q^{gs}}\sum_{n=g}^{\infty}\frac{q^{n-g+1}-1}{q-1}\frac{1}{q^{(n-g)s}} = \frac{h}{q^{gs}}\sum_{n=0}^{\infty}\frac{q^{n+1}-1}{q-1}\frac{1}{q^{ns}} = \frac{h}{q^{gs}}\zeta_0(s),\end{aligned}$$

donde $\zeta_0(s)$ es la función zeta de $k(x)$.

Así, $\zeta_K(s) \geq \dfrac{h}{q^{gs}}\zeta_0(s)$, $s \in \mathbb{R}$, $s > 1$.

Por otro lado, $\zeta_K(s) = \displaystyle\prod_{\mathcal{P}\in\mathbb{P}_K}\left(1 - \frac{1}{N(\mathcal{P})^s}\right)^{-1}$.

Sea $\mathcal{P}$ un divisor primo de K de grado relativo t, $\mathfrak{P} = \mathcal{P}|_{k(x)}$. Entonces $d(\mathfrak{P})t = d(\mathcal{P})$ y $N(\mathcal{P}) = q^{d(\mathcal{P})} = q^{td(\mathfrak{P})}$ y

$$1 - \frac{1}{N(\mathcal{P})^s} = 1 - \frac{1}{q^{d(\mathcal{P})s}} = 1 - \frac{1}{q^{(d(\mathfrak{P}))ts}} \geq \left(1 - \frac{1}{q^{d(\mathfrak{P})s}}\right)^t,$$

pues si $\alpha > 1$,

$$1 - \frac{1}{\alpha^t} = \frac{\alpha^t - 1}{\alpha^t} = \frac{\displaystyle\prod_{i=1}^{t}(\alpha - \xi_t^i)}{\alpha^t} = \prod_{i=1}^{t}\left(1 - \frac{\xi_t^i}{\alpha}\right),$$

donde ξ_t es una raíz $t-$ésima de 1 primitiva

$$\begin{aligned}\Rightarrow 1-\frac{1}{\alpha^t} &= \left|1-\frac{1}{\alpha^t}\right| = \prod_{i=1}^{t}\left|1-\frac{\xi_t^i}{\alpha}\right| \geq \prod_{i=1}^{t}\left||1|-\left|\frac{\xi_t^i}{\alpha}\right|\right| = \prod_{i=1}^{t}\left|1-\frac{|\xi_t^i|}{\alpha}\right| \\ &\geq \prod_{i=1}^{t}\left(1-\frac{|\xi_t^i|}{\alpha}\right) = \left(1-\frac{1}{\alpha}\right)^t.\end{aligned}$$

Por tanto, si $\mathcal{P}_1,\ldots,\mathcal{P}_r$ son los divisores primos de K sobre $\mathfrak{P}$ y cada grado relativo es t_i, entonces $\sum_{i=1}^{r} t_i \leq m = [K:k(x)]$, luego

$$\prod_{i=1}^{r}\left(1-\frac{1}{N(\mathcal{P}_i)^s}\right) \geq \prod_{i=1}^{r}\left(1-\frac{1}{N(\mathfrak{P})^s}\right)^{t_i} \geq \left(1-\frac{1}{N(\mathfrak{P})^s}\right)^m.$$

De donde

$$\zeta_K(s) = \prod_{\mathcal{P}\in\mathbb{P}_K}\left(1-\frac{1}{N(\mathcal{P})^s}\right)^{-1} \leq \prod_{\mathfrak{P}\in\mathbb{P}_{k(x)}}\left(1-\frac{1}{N(\mathfrak{P})^s}\right)^{-m} = \zeta_0(s)^m.$$

Entonces $\zeta_0(s)^m \geq \zeta_K(s) \geq \frac{h}{q^{gs}}\zeta_0(s)$. Luego, $\zeta_0(s)^{m-1} \geq \frac{h}{q^{gs}}$. Tomando logaritmos, se tiene que $(m-1)\ln\zeta_0(s) \geq \ln h - gs\ln q$, entonces

$$s \geq \frac{\ln h}{g\ln q} - \frac{(m-1)\ln\zeta_0(s)}{g\ln q}.$$

Sean $\epsilon > 0$ y $s = 1+\epsilon$. Existe un subconjunto finito Γ de Λ tal que $\forall\ \alpha \in \Lambda\backslash\Gamma$ se cumple

$$\frac{m_\alpha}{g_\alpha} < \frac{\ln q}{\ln\xi_0(s)}\epsilon.$$

Entonces $m_\alpha - 1 < m_\alpha < \frac{\ln q}{\ln\xi_0(s)} g_\alpha\epsilon$, luego

$$\frac{(m_\alpha-1)\ln q\xi_0(s)}{g_\alpha\ln q} < \epsilon.$$

Así,

$$1+\epsilon \geq \frac{\ln h_\alpha}{g_\alpha\ln q} - \epsilon.$$

Por lo que $\limsup_{\frac{m}{g}\to 0}\frac{\ln h}{g\ln q} \leq 1$.

El resultado se sigue de lo anterior y el Teorema 2.6.2.

□

Teorema 2.6.4. *Sea K/k un campo de funciones congruente con $|k| = q$, género g y número de clases h. Se tiene $\left(\sqrt{q}-1\right)^{2g} \leq h \leq \left(\sqrt{q}+1\right)^{2g}$.*

Demostración. Puesto que $h = P_K(1) = |P_K(1)| = \prod_{i=1}^{2g} |1-\omega_i|$, $|\omega_i| = \sqrt{q}$ tenemos $\sqrt{q}-1 \leq |1-\omega_i| \leq \sqrt{q}+1$, y por lo tanto $\left(\sqrt{q}-1\right)^{2g} \leq h \leq \left(\sqrt{q}+1\right)^{2g}$.

□

Corolario 2.6.5. *Con las hipótesis del Teorema 2.6.4 y $g > 0$ tenemos*

$$\frac{2\ln\left(\sqrt{q}-1\right)}{2\ln q} \leq \frac{\ln h}{g\ln q} \leq \frac{2\ln\left(\sqrt{q}+1\right)}{\ln q}$$

Demostración. Tenemos por el Teorema que

$$\begin{array}{rccccc} & \ln\left(\sqrt{q}-1\right)^{2g} & \leq & \ln h & \leq & \ln\left(\sqrt{q}+1\right)^{2g} \\ \Rightarrow & 2g\ln\left(\sqrt{q}-1\right) & \leq & \ln h & \leq & 2g\ln\left(\sqrt{q}+1\right) \\ \Rightarrow & \dfrac{2g\ln\left(\sqrt{q}-1\right)}{g\ln q} & \leq & \dfrac{\ln h}{g\ln q} & \leq & \dfrac{2g\ln\left(\sqrt{q}+1\right)}{g\ln q} \\ \Rightarrow & \dfrac{2\ln\left(\sqrt{q}-1\right)}{\ln q} & \leq & \dfrac{\ln h}{g\ln q} & \leq & \dfrac{2\ln\left(\sqrt{q}+1\right)}{\ln q}. \end{array}$$

□

Ahora, para $n > 2g-2$, se tiene $A_n = h\left(\dfrac{q^{n-g+1}-1}{q-1}\right)$ (Teorema 1.2.5).

Por otro lado, $A_n = \sum_{p(n)} \prod_{i=1}^{n} \binom{k_i+N_i-1}{k_i}$, donde $p(n)$ es el conjunto de particiones de n (Teorema 2.3.8).

Tomando $n = 2g-1$, obtenemos la igualdad:

$$h\left(\frac{q^{(2g-1)-g+1}-1}{q-1}\right) = h\left(\frac{q^g-1}{q-1}\right) = A_{2g-1} = \sum_{p(2g-1)} \prod_{i=1}^{2g-1} \binom{k_i+N_i-1}{k_i}.$$

Sea $M = \max_{p(2g-1)} \prod_{i=1}^{2g-1} \binom{k_i+N_i-1}{k_i}$.

Entonces $M \leq h\left(\dfrac{q^g-1}{q-1}\right) \leq |p(2g-1)|M$.

Además, es un resultado conocido que

$$|p(2g-1)| < e^{T\sqrt{2g-1}},\ T = \pi\left(\frac{2}{3}\right)^{1/2}.$$

Por lo tanto se tiene $M \leq h\left(\dfrac{q^g-1}{q-1}\right) \leq e^{T\sqrt{2g-1}}M$. Así,

$$\begin{array}{rccccc}
 & \ln M & \leq & \ln\left(h\left(\dfrac{q^g-1}{q-1}\right)\right) & \leq & \ln\left(e^{T\sqrt{2g-1}}M\right) \\
\Rightarrow & \ln M & \leq & \ln h + \ln\left(q^g-1\right) - \ln(q-1) & \leq & \ln\left(e^{T\sqrt{2g-1}}\right) + \ln M \\
\Rightarrow & \ln M & \leq & \ln h + \ln\left(q^g-1\right) - \ln(q-1) & \leq & T\sqrt{2g-1} + \ln M \\
\Rightarrow & \dfrac{\ln M}{g\ln q} & \leq & \dfrac{\ln h}{g\ln q} + \dfrac{\ln\left(q^g-1\right) - \ln(q-1)}{g\ln q} & \leq & \dfrac{T\sqrt{2g-1}}{g\ln q} + \dfrac{\ln M}{g\ln q}
\end{array}$$

Ahora bien,

$$\begin{aligned}
\lim_{g\to\infty} \frac{\ln\left(q^g-1\right) - \ln(q-1)}{g\ln q} &= \lim_{g\to\infty} \frac{\dfrac{q^g\ln q}{q^g-1}}{\ln q} = \lim_{g\to\infty} \frac{q^g\ln q}{\left(q^g-1\right)\ln q} \\
&= \lim_{g\to\infty} \frac{q^g}{\left(q^g-1\right)} = 1
\end{aligned}$$

y

$$\lim_{g\to\infty} \frac{T\sqrt{2g-1}}{g\ln q} = \lim_{g\to\infty} \frac{\frac{1}{2}T(2g-1)^{-1/2}2}{\ln q} = \lim_{g\to\infty} \frac{T}{\sqrt{2g-1}\ln q} = 0,$$

de donde se tiene que $\lim\limits_{g\to\infty} \dfrac{\ln h}{g\ln q}$ existe $\Leftrightarrow$ $\lim\limits_{g\to\infty} \dfrac{\ln M}{g\ln q}$ existe.

En este caso, $\lim\limits_{g\to\infty} \dfrac{\ln h}{g\ln q} = \lim\limits_{g\to\infty} \dfrac{\ln M}{g\ln q} - 1$.

Por lo tanto, probar el análogo al Teorema de Brauer-Siegel equivale a probar que $\limsup\limits_{g\to\infty} \dfrac{\ln M}{g\ln q} \leq 2$.

Apéndice A

Definiciones y Resultados

Referimos a [13] para las demostraciones.

Definición A.1. Sea k cualquier campo. Un ***campo de funciones algebraicas*** K ***sobre*** k es una extensión de campos K de k, finitamente generada, con grado de transcendencia $r \geq 1$. El campo K recibe el nombre de ***campo de funciones de*** r ***variables***. Cuando K es un campo de funciones de una variable, sólo lo llamamos ***campo de funciones*** y escribimos K/k para denotarlo.

Definición A.2. Sean K/k y L/l dos campos de funciones. Se dice que L es una ***extensión de*** K si $K \subseteq L$ y $l \cap K = k$.

Definición A.3. Sea L/l una extensión de K/k. Se dice que L/K es una ***extensión de constantes*** si $L = Kl$.

Definición A.4. Sea K/k un campo de funciones. A la cerradura algebraica de k en K, esto es, el campo $k' = \{\alpha \in K \mid \alpha \text{ es algebraico sobre } k\}$ se le llama el ***campo de constantes de*** K.

Definición A.5. Dado un campo de funciones K, al grupo abeliano libre generado por los elementos de $\mathbb{P}_K$ se le llama ***grupo de divisores de*** K y es denotado por D_K, donde $\mathbb{P}_K = \{\mathfrak{P} \mid \mathfrak{P} \text{ es un divisor primo de } K\}$.

Definición A.6. Sea $\mathfrak{A}$ un divisor. Definimos el ***grado de*** $\mathfrak{A}$, el cual será denotado por $d_K(\mathfrak{A})$ o $d(\mathfrak{A})$ en caso de no haber confusión, por

$$d_K(\mathfrak{A}) = \sum_{\mathfrak{P}\in\mathbb{P}_K} f_{\mathfrak{P}}\upsilon_{\mathfrak{P}}(\mathfrak{A}), \text{ donde } \mathfrak{A} = \prod_{\mathfrak{P}\in\mathbb{P}_K} \mathfrak{P}^{\upsilon_{\mathfrak{P}}(\mathfrak{A})}.$$

Definición A.7. Sea S un conjunto de divisores primos de K y sea $\mathfrak{A}$ un divisor. Entonces se define

$$\Gamma(\mathfrak{A}|S) = \{x \in K | \upsilon_{\mathfrak{P}}(x) \geq \upsilon_{\mathfrak{P}}(\mathfrak{A}) \text{ para todo } \mathfrak{P} \in S\}.$$

Definición A.8. Sea $\mathfrak{A}$ cualquier divisor de K. Denotamos por $L_K(\mathfrak{A})$ o $L(\mathfrak{A})$ al $k-$espacio vectorial $\Gamma(\mathfrak{A}|\mathbb{P}_K)$, esto es,

$$L(\mathfrak{A}) = \{x \in K | \upsilon_{\mathfrak{P}}(x) \geq \upsilon_{\mathfrak{P}}(\mathfrak{A}) \text{ para todo } \mathfrak{P} \in \mathbb{P}_K\}.$$

Definición A.9. Dado $x \in K^*$, se define el ***divisor principal de*** x ***en*** K por $(x)_K = \prod_{\mathfrak{P}\in\mathbb{P}_K} \mathfrak{P}^{\upsilon_{\mathfrak{P}}(x)}$. Si no hay confusión posible, escribiremos (x) en lugar de $(x)_K$.

Definición A.10. El conjunto de los divisores principales $\{(x)_K | x \in K^*\}$ es un subgrupo de D_K. Este subgrupo es denotado por P_K y es llamado el ***subgrupo de divisores principales de*** K. El cociente $C_K = D_K/P_K$ es llamado el ***grupo completo de clases de divisores de*** K o grupo de clases de K.

Definición A.11. Un elemento $x \in K^*$ se llama ***divisible por un divisor*** $\mathfrak{A}$, lo cual será denotado por $\mathfrak{A}|x$, si $\mathfrak{A}|(x)_K$. Si x, $y \in K^*$, ponemos $x \equiv y$ mód $\mathfrak{A}$ si $x = y$ ó $\mathfrak{A}|x - y$.

Definición A.12. Se define el ***grado de una clase*** $C \in C_K$ por $d(C) = d(\mathfrak{A})$, donde $\mathfrak{A}$ es cualquier divisor que pertenece a C.

Definición A.13. Sea $D_{K,0} := \ker d = \{\mathfrak{A} \in D_K | d(\mathfrak{A}) = 0\}$ el ***subgrupo de divisores de grado 0***.

Definición A.14. El grupo $C_{K,0} = D_{K,0}/P_K$ se denomina ***grupo de clases de divisores de grado 0***.

Definición A.15. Si $C_{K,0}$ es finito, al número $h_K = |C_{K,0}|$ se le llama el ***número de clases del campo*** K.

Definición A.16. Sea $C \in C_K$. Se define la ***dimensión de la clase*** C por $N(C) = l(\mathfrak{A}^{-1})$, $\mathfrak{A} \in C$ cualquiera. Equivalentemente, $N(C) = l(\mathfrak{A})$, para cualquier $\mathfrak{A}^{-1} \in C$.

Definición A.17. A la clase C que consiste de los divisores de las diferenciales no cero de un campo de funciones se le llama la ***clase canónica*** y se le denota por $W = W_K$.

Proposición A.18. *Sean K cualquier campo y υ una valuación sobre K. Si $\sum_{i=1}^{n} a_i = 0$, $n \geq 2$, entonces existen $i \neq j$ tales que $\upsilon(a_i) = \upsilon(a_j)$.*

Teorema A.19. *Se tiene que $\{\upsilon_f, \upsilon_\infty | f(x) \in k[x]$ es mónico e irreducible$\}$ son todas las valuaciones υ sobre $k(x)$ tales que $\upsilon(a) = 0$ para $a \in k^*$. Además todas ellas son inequivalentes a pares y el campo residual es una extensión finita de k de grado igual al grado de $f(x)$ y 1, respectivamente. Finalmente, todas las valuaciones son discretas.*

Teorema A.20. *Para cualquier divisor $\mathfrak{A}$, $l(\mathfrak{A}) = \dim_k L(\mathfrak{A}) < \infty$. Si $\mathfrak{A}|\mathfrak{B}$, $l(\mathfrak{A}) + d(\mathfrak{A}) \leq l(\mathfrak{B}) + d(\mathfrak{B})$.*

Teorema A.21. *Para $x \in K \backslash k$, $d(\mathfrak{z}_x) = d(\eta_x) = N = [K : k(x)]$.*

Proposición A.22. *Sea $C \in C_K$ una clase cualquiera. Entonces tenemos que $N(C)$ es igual al máximo número de divisores enteros linealmente independientes de C. En particular este número es finito.*

Teorema A.23. *(TEOREMA DE RIEMANN-ROCH) Sea K/k un campo de funciones y sea $C \in C_K$ una clase cualquiera. Sea W la clase canónica y g el género de K. Entonces*

$$N(C) = d(C) - g + 1 + N\left(WC^{-1}\right).$$

Equivalentemente, si $\mathfrak{A}$ es cualquier divisor y ω cualquier diferencial diferente de cero, se tiene

$$l\left(\mathfrak{A}^{-1}\right) = d(\mathfrak{A}) - g + 1 + l\left((\omega)_K^{-1}\mathfrak{A}\right).$$

En otras palabras, se tiene

$$\delta(\mathfrak{A}) = l\left(\mathfrak{A}^{-1}\right) + d(\mathfrak{A}^{-1}) + g - 1 = l\left((\omega)_K^{-1}\mathfrak{A}\right) = N\left(WC^{-1}\right),$$

para $\mathfrak{A} \in C$.

Corolario A.24. *Sea W la clase canónica. Entonces*

$$N(W) = g, \;\; d(W) = 2g - 2.$$

Además $N(P_K) = 1$ y $d(P_K) = 0$ y para $C_0 \in C_{K,0}$ tal que $C_0 \neq P_K$, tenemos que $N(C_0^{-1}) = 0$ y $d(C_0) = 0$.

Corolario A.25. *Si $\mathfrak{A}$ es un divisor tal que $d(\mathfrak{A}) > 2g - 2$ ó $d(\mathfrak{A}) = 2g - 2$ y $\mathfrak{A} \notin W$, entonces $l(\mathfrak{A}^{-1}) = d(\mathfrak{A}) - g + 1$ y en particular $l(\mathfrak{A}^{-1}) \geq g - 1$. Equivalentemente, si $C \in C_K$ es tal que $d(C) > 2g - 2$ ó $d(C) = 2g - 2$ y $C \neq W$, entonces $N(C) = d(C) - g + 1$ y en particular $N(C) \geq g - 1$.*

Corolario A.26. *Sea $\mathfrak{P}$ un divisor primo y sea $n > 2g-1$ ($n > 0$, si $g = 0$). Entonces existe un elemento $x \in K$ tal que $\eta_x = \mathfrak{P}^n$, es decir, $(x)_K = \dfrac{\mathfrak{B}}{\mathfrak{P}^n}$, $\mathfrak{B}$ divisor entero primo relativo a $\mathfrak{P}$.*

Proposición A.27. *Si K/k es cualquier campo de funciones tal que $g_K = 0$, entonces $C_{K,0} = \{1\}$ y en consecuencia, $h_K = 1$.*

Teorema A.28. *Sea K/k un campo de funciones. Si $K = k(x)$ entonces $g_K = 0$. Recíprocamente, si $g_K = 0$, entonces K es un campo de funciones racionales o es una extensión cuadrática de $k(x)$. Más aún, K contiene divisores primos de grado 1 o 2. Finalmente, $K = k(x) \Leftrightarrow$ existe al menos un divisor primo de grado 1.*

Proposición A.29. *Si $d_L(\mathcal{P}) = [l(\mathcal{P}) : l]$, $d_K(\mathfrak{P}) = [k(\mathfrak{P}) : k]$, entonces $d_L(\mathcal{P})[l : k] = d_{L/K}(\mathcal{P}/\mathfrak{P})d_K(\mathfrak{P})$.*

Teorema A.30. *Sea L/l una extensión de K/k. Sea $\mathfrak{P}$ un lugar de K y sean $\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_h$ los lugares de L sobre $\mathfrak{P}$. Entonces*

$$[L : K] = \sum_{i=1}^{h} d_{L/K}(\mathcal{P}_i \mid \mathfrak{P}) e_{L/K}(\mathcal{P}_i \mid \mathfrak{P}).$$

Teorema A.31. *Sea L/l una extensión algebraica separable de K/k y supongamos que $L = Kl$, es decir, L es una extensión de constantes de K. Entonces no hay divisores primos de L ramificados o inseparables sobre K.*

Teorema A.32. *Sea L/K una extensión arbitraria de campos de funciones. Existe $\lambda_{L/K} \in \mathbb{Q}$, $\lambda_{L/K} > 0$, que depende sólo de L y de K, tal que para todo $\mathfrak{A} \in D_K$, $d_L(\mathfrak{A}) = \dfrac{d_K(\mathfrak{A})}{\lambda_{L/K}}$. En particular $d_L(\mathfrak{A}) = 0 \Leftrightarrow d_K(\mathfrak{A}) = 0$ y por lo tanto $\mathrm{con_{L/K}}$ induce un homomorfismo de grupos*

$$\overline{\mathrm{con_{L/K}}} : C_{K,0} \longrightarrow C_{L,0}.$$

Finalmente, si $[L : K] < \infty$, entonces $\lambda_{L/K} = \dfrac{[l : k]}{[L : K]}$.

Conclusiones

En este trabajo se presentó una demostración de la Hipótesis de Riemann en campos de funciones congruentes, la cual nos dice que si K/k es uno de tales campos con $|k| = q$, entonces:

(I) Los ceros de la función zeta $\zeta_K(s)$ están en la línea $\mathbb{R}e\ s = \frac{1}{2}$.

(II) Los ceros de la función $Z_K(u)$ están en el círculo $|u| = q^{-1/2}$.

(III) Si $\omega_1, \ldots, \omega_{2g}$, son las inversas de las raíces de $P_K(u)$, entonces $|\omega_i| = \sqrt{q}$, $i = 1, \ldots, 2g$.

(IV) Si N_1 denota el número de divisores primos de grado 1 en K, entonces $|N_1 - (q+1)| \leq 2g\sqrt{q}$.

Este último punto nos fue de gran utilidad para muchas de las aplicaciones.

Entre las consecuencias de la Hipótesis de Riemann en campos de funciones congruentes obtuvimos que si K es un campo de funciones congruente de género 0, entonces K es un campo de funciones racionales.

Se determinó el número n_i de divisores primos de grado i en $\mathbb{F}_q(x)$ y se ilustró con un ejemplo en $\mathbb{F}_2(x)$. Esto nos ayudó en la estimación del número N_m de divisores primos de grado m en cualquier campo de funciones K sobre $\mathbb{F}_q$. Se obtuvo una relación del número N_m con el número A_n de divisores enteros de grado n y con el número $N_1^{(d)}$ de divisores primos de grado 1 en la extensión de constantes de grado d.

Nos auxiliamos de la función $S(q, g, r)$ para obtener que si $q = 4$, $g \geq 2$, o bien $q = 3$, $g \geq 3$, o bien $q = 2$, $g \geq 5$, entonces el número de clases h_K es mayor que 1. Además, si $g \geq 1$ y $q \geq 5$, tenemos $h_K > 1$, vemos que es muy limitado nuestro número de posibilidades para que un campo K tenga número de clases 1. En efecto, si $g = 0$, $h = 1$, pero si $g \geq 1$, sólo es posible $h = 1$ cuando: $q = 4$, $g = 1$; $q = 3$, $g = 1, 2$; $q = 2$, $g = 1, 2, 3, 4$. En el Teorema 2.4.5 se presentan todos los posibles campos con número de clases 1 y género mayor que 0. En un ejemplo verificamos explícitamente la Hipótesis de Riemann para el primer caso de los mencionados en el teorema anterior.

Para poder probar un análogo al Teorema de Brauer-Siegel debemos tener que $\limsup_{g\to\infty} \dfrac{\ln h}{g \ln q} \leq 1$, lo cual es un problema abierto. Sin embargo probamos que el resultado sí se cumple con una restricción.

Bibliografía

[1] E. Bombieri, *Counting points on curves over finite fields*, Séminaire Bourbaki, 25ème année(1972/1973), Exp. No. 430, pp.234-241. Lecture Notes in Math., Vol. 383, Springer, Berlin, 1974.

[2] P. Borwein, S. Choi, B. Rooney and A. Weirathmueller, *The Riemann Hypothesis: A Resource for the Afficionado and Virtuoso Alike*, Springer-Canadian Mathematical Society, Canada, 2008.

[3] J. Derbyshire, *Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics*, England, 2003.

[4] M. D. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, Berlin, 1986.

[5] W. Fulton, *Algebraic Curves: An Introduction to Algebraic Geometry*, Addison-Wesley Publishing Company, Advanced Book Program, Inc., 1989.

[6] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörpern I*, J. Reine Angew. Math. 175, pp.55-62, 1936.

[7] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörpern II*, J. Reine Angew. Math. 175, pp.69-88, 1936.

[8] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörpern III*, J. Reine Angew. Math. 175, pp.193-208, 1936.

[9] J. R. C. Leitzel and M. L. Madan, *Algebraic function fields with equal class number*, Acta Arith. 30, pp.169-177, 1976.

[10] J. R. C. Leitzel, M. L. Madan and C. S. Queen, *Algebraic function fields with small class number*, Journal of Number Theory 7, pp.11-27, 1975.

[11] J. E. Marsden y M. J. Hoffman, *Variable Compleja*, Trillas, México, 1996.

[12] B. Riemann, *Ueber die Anzahl der Primzahlen unter einer gegebeben Grösse*, Monatsber. Königl. Preuss. Akad. Wiss. Berlin 1859, pp.671-680.

[13] G. D. Villa Salvador, *Topics in the Theory of Algebraic Function Fields*, Mathematics: Theory and Applications, Birkäuser Boston, Inc., Boston, MA, 2006.

[14] A. Weil, *On the Riemann Hypothesis in Function Fields*, Proc. Nal. Acad. Sci. U. S. A. 27, pp.345-347, 1941.

Índice Alfabético

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

ACTA DE EXAMEN DE GRADO

No. 00069
Matrícula: 208180131

LA HIPOTESIS DE RIEMANN EN CAMPOS DE FUNCIONES

En México, D.F., se presentaron a las 11:00 horas del día 13 del mes de diciembre del año 2011 en la Unidad Iztapalapa de la Universidad Autónoma Metropolitana, los suscritos miembros del jurado:

DRA. MARTHA RZEDOWSKI CALDERON
DR. ARTURO CUETO HERNANDEZ
DRA. LAURA HIDALGO SOLIS

Bajo la Presidencia de la primera y con carácter de Secretaria la última, se reunieron para proceder al Examen de Grado cuya denominación aparece al margen, para la obtención del grado de:

MAESTRA EN CIENCIAS (MATEMÁTICAS)

DE: MARIA LILIANA RODRIGUEZ SALVADOR

y de acuerdo con el artículo 78 fracción III del Reglamento de Estudios Superiores de la Universidad Autónoma Metropolitana, los miembros del jurado resolvieron:

APROBAR

Acto continuo, la presidenta del jurado comunicó a la interesada el resultado de la evaluación y, en caso aprobatorio, le fue tomada la protesta.

MARIA LILIANA RODRIGUEZ SALVADOR

ALUMNA

REVISÓ

LIC. JULIO CESAR DE LARA ISASSI
DIRECTOR DE SISTEMAS ESCOLARES

DIRECTOR DE LA DIVISIÓN DE CBI

DR. JOSE ANTONIO DE LOS REYES HEREDIA

PRESIDENTA

DRA. MARTHA RZEDOWSKI CALDERON

VOCAL

DR. ARTURO CUETO HERNANDEZ

SECRETARIA

DRA. LAURA HIDALGO SOLIS