La función Z de un cuerpo de funciones algebraicas

Ricardo Podestá
(UNC – CONICET)

Segundo Encuentro Regional de Teoría de Números
1 y 2 de Junio de 2012, Córdoba.

Plan de la charla

1. Cuerpos de funciones algebraicas.
2. La función Z de un cuerpo de funciones.
3. El L-polinomio de un cuerpo de funciones.
4. Hasse-Weil y la Hipótesis de Riemann.

1. CUERPOS DE FUNCIONES ALGEBRAICAS

(a) Lugares

(b) Riemann-Roch

(c) Divisores

(d) Ejemplos

Sea K un cuerpo.

Definición

El **cuerpo de funciones racionales** $K(x)$ sobre K es el cuerpo de fracciones de $K[x]$.

- O sea, si x trascendente sobre K,

$$K(x) = \{\frac{f(x)}{g(x)} : f(x), g(x) \in K[x], g(x) \neq 0\}$$

- todo $z \in K(x)$ se escribe en forma única

$$z = a \prod_{i=1}^{r} p_i(x)^{n_i}$$

$a \in K$, $n_i \in \mathbb{Z}$ y $p_i(x) \in K[x]$ irreducibles, $i = 1, \ldots, r$, $r \in \mathbb{N}$.

Definición

Un **cuerpo de funciones algebraicas** F **sobre** K, F/K, es un cuerpo extensión $F \supset K$ tal que F es una extensión algebraica finita de $K(x)$ para algún $x \in F$ trascendente sobre K.

- El *cuerpo de constantes* de F/K es

$$K \subseteq \tilde{K} = \{z \in F : z \text{ algebraico}/K\} \subsetneq F$$

- Si K es perfecto, por el teorema del elemento primitivo,

$$F = K(x, y)$$

$$\phi(y) = 0, \quad \phi(T) \in K(x)[T]$$

Definición

Sea $F = K(x)$ y $p(x) \in K[x]$ irreducible y sea

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], (f, g) = 1, p(x) \nmid g(x) \right\}$$

Se tiene

- $\mathcal{O}_{p(x)}$ es un anillo
- $K \subsetneq \mathcal{O}_{p(x)} \subsetneq F$
- Si $z = \frac{f(x)}{g(x)} \notin \mathcal{O}_{p(x)}$ entonces $z^{-1} = \frac{g(x)}{f(x)} \in \mathcal{O}_{p(x)}$
- $\mathcal{O}_{p(x)} = K[x]_{\mathfrak{p}}$ es la localización de $K[x]$ en $\mathfrak{p} = \langle p(x) \rangle$
- $\mathcal{O}_{p(x)}$ es un anillo local

Definición

Un **anillo de valuación** de F/K es un anillo $K \subsetneq \mathcal{O} \subsetneq F$, tal que

$$z \in F \qquad \Rightarrow \qquad z \in \mathcal{O} \quad \text{ó} \quad z^{-1} \in \mathcal{O}$$

- $\mathcal{O}$ es un anillo local, i.e. $\mathcal{O}$ tiene un único ideal maximal

$$P = \mathcal{O} \backslash \mathcal{O}^*$$

- $\mathcal{O}$ es un DIP.
- Si $x \in F^*$ entonces

$$x \in P \qquad \Leftrightarrow \qquad x^{-1} \notin \mathcal{O}$$

- $\widetilde{K} \subseteq \mathcal{O}$ y $\widetilde{K} \cap P = \{0\}$.

Definición

Un **lugar** de F/K es el ideal maximal P de algún anillo de valuación $\mathcal{O}$ de F/K. Ponemos

$$\mathcal{L}_F = \{P : P \text{ es un lugar de } F/K\}$$

- $|\mathcal{L}_F| = \infty$
- dado $P \in \mathcal{L}_F$, si $P = t\mathcal{O}$, t se dice *elemento primo* de P
- todo $z \in F^*$ se escribe unívocamente de la forma

$$z = t^k u$$

$$k \in \mathbb{Z}, \quad u \in \mathcal{O}^*.$$

Definición

Una **valuación discreta** de F/K es una función

$$v : F \to \mathbb{Z} \cup \{\infty\}$$

que cumple

- $v(x) = \infty \quad \Leftrightarrow \quad x = 0$
- $v(xy) = v(x) + v(y)$
- $v(x + y) \geq \text{mín}\{v(x), v(y)\}$
- $v(z) = 1$ para algún $z \in F$
- $v(a) = 0$ para todo $a \in K^*$

Resulta que

- $v(ax) = v(x)$ para todo $a \in K^*$
- $v(x^{-1}) = -v(x)$, para todo $x \in F^*$.
- $v(z^k) = kv(z)$, para todo $k \in \mathbb{Z}$.
- v es sobreyectiva.

La valuación de P

A cada $P \in \mathcal{L}_F$ le asociamos la valuación

$$v_P : F \to \mathbb{Z} \cup \{\infty\}$$

$$t^k u \mapsto k$$

$$0 \mapsto \infty$$

- En términos de v_P tenemos

$$\begin{aligned} P &= \{z \in F : v_P(z) > 0\} \\ \mathcal{O}^* &= \{z \in F : v_P(z) = 0\} \\ \mathcal{O} &= \{z \in F : v_P(z) \geq 0\} \end{aligned}$$

1a. Lugares y valuaciones

- $F_P = \mathcal{O}/P$ es el cuerpo residual.
- el mapa residual es $\pi_P : F \to F_P \cup \infty$

$$x \mapsto x(P) = \begin{cases} x + P & x \in \mathcal{O}, \\ \infty & x \notin \mathcal{O}. \end{cases}$$

- Se tiene $K \hookrightarrow F_P$.

Definición

Dado $P \in \mathcal{L}_F$, el **grado** de P es

$$\deg P = [F_P : K] = \dim_K F_P.$$

- Vale

$$1 \leq \deg P = [F : K(x)] < \infty$$

para todo $0 \neq x \in P$.

1a. Lugares y valuaciones

Sea K es algebraicamente cerrado

- entonces $F_P = K$, o sea $\deg P = 1$, para todo $P \in \mathcal{L}_F$
- $z \in F$ define una función

$$z : \mathcal{L}_F \to K \cup \{\infty\}$$

$$P \mapsto z(P)$$

donde las $x \in \widetilde{K} = K$ son las funciones constantes, $x(P) = x$.

- Si $z \in F$, tenemos

$$z(P) = \begin{cases} z & z \in K^*, \forall P \in \mathbb{P}_F \\ 0 & z \in P = \mathcal{O} \setminus \mathcal{O}^* \\ \infty & z \notin \mathcal{O} \end{cases}$$

En el caso general

- dados $z \in F$, $P \in \mathcal{L}_F$ definimos:

$$P \text{ es un } \textbf{cero} \text{ de } z \quad \Leftrightarrow \quad z(P) = 0 \quad \Leftrightarrow \quad v_P(z) > 0,$$

$$P \text{ es un } \textbf{polo} \text{ de } z \quad \Leftrightarrow \quad z(P) = \infty \quad \Leftrightarrow \quad v_P(z) < 0.$$

- Dado $x \in F^*$,

$$\mathcal{Z} = \{P \in \mathcal{L}_F : P \text{ cero de } x\}$$

$$\mathcal{N} = \{P \in \mathcal{L}_F : P \text{ polo de } x\}$$

- Se prueba que todo $x \in F^*$ tiene un número finito de ceros y polos, es decir

$$|\mathcal{Z}| < \infty, \qquad |\mathcal{N}| < \infty\,.$$

Los anillos $\mathcal{O}_{p(x)}$

Sea $F = K(x)$ y $p(x) \in K[x]$ irreducible. Tenemos el anillo de valuación

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], \quad (f,g) = 1, \quad p(x) \nmid g(x) \right\}$$

Luego,

$$\mathcal{O}^*_{p(x)} = \left\{ \frac{f(x)}{g(x)} \in \mathcal{O}_{p(x)} : p(x) \nmid f(x) \right\}$$

y por lo tanto

$$P_{p(x)} = \mathcal{O}_{p(x)} \setminus \mathcal{O}^*_{p(x)} = \left\{ \frac{f(x)}{g(x)} : p(x) \nmid g(x), p(x) \mid f(x) \right\} \in \mathcal{L}_F$$

Los anillos $\mathcal{O}_{p(x)}$

- Como

$$P_{p(x)} = \left\{ p(x)^k \, \frac{f(x)}{g(x)} : p \nmid g, p \nmid f, k \in \mathbb{N} \right\} = p(x) \cdot \mathcal{O}_{p(x)}$$

  $p(x)$ es un elemento primo de $P_{p(x)}$.

- Si $p(x) = x - \alpha$, $\alpha \in K$, ponemos $\mathcal{O}_\alpha = \mathcal{O}_{x-\alpha}$ y $P_\alpha = P_{x-\alpha}$.

  En particular,

$$\mathcal{O}_\alpha = \left\{ \frac{f(x)}{g(x)} : g(\alpha) \neq 0 \right\}$$

$$P_\alpha = \left\{ \frac{f(x)}{g(x)} : f(\alpha) = 0, g(\alpha) \neq 0 \right\} = (x - \alpha)\mathcal{O}_\alpha$$

El anillo $\mathcal{O}_\infty$

Hay otro anillo de valuación,

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], \quad (f,g) = 1, \quad \deg f \leq \deg g \right\}$$

Luego,

$$\mathcal{O}_\infty^* = \left\{ \frac{f(x)}{g(x)} \in \mathcal{O}_{p(x)} : \deg f(x) = \deg g(x) \right\}$$

y por lo tanto

$$P_\infty = \mathcal{O}_\infty \setminus \mathcal{O}_\infty^* = \left\{ \frac{f(x)}{g(x)} : \deg f(x) < \deg g(x) \right\}$$

es un lugar de $F = K(x)$.

Teorema

Sea $F = K(x)$ un cuerpo de funciones racionales. Si $P = P_{p(x)}$, $p(x) \in K[x]$ irreducible, entonces

- *La valuación v_P está dada por*

$$v_P(z) = k \qquad si \qquad z = p(x)^k \frac{f(x)}{g(x)}$$

con $k \in \mathbb{Z}$, $f, g \in K[x]$ y $p(x) \nmid f(x)$, $p(x) \nmid g(x)$.

- $K(x)_P \simeq K[x]/(p(x))$ *y* $\deg P = \deg p(x)$.
- *Si $\alpha \in K$ entonces* $\deg P_\alpha = 1$ *y el mapa residual de $z \in F$ es*

$$z(P) = z(\alpha) = \begin{cases} f(\alpha)/g(\alpha) & g(\alpha) \neq 0, \\ \infty & g(\alpha) = 0, \end{cases}$$

si $z = f(x)/g(x)$, $(f, g) = 1$.

Teorema (continuación)

Si $F = K(x)$ es un cuerpo de funciones racionales,

- $\deg P_\infty = 1$, $P_\infty = \frac{1}{x}\mathcal{O}_\infty$ *y*

$$v_\infty(\tfrac{f(x)}{g(x)}) = \deg g(x) - \deg f(x)$$

- *Para $z \in K(x)$, el mapa residual es*

$$z(P_\infty) = z(\infty) = \begin{cases} a_n/b_m & n = m, \\ 0 & n < m, \\ \infty & n > m, \end{cases}$$

si $z = a_n x^n + \cdots + a_0/b_m x^m + \cdots + b_0$, $a_n, b_m \neq 0$.

- *Estos son todos los lugares de $F = K(x)$, es decir*

$$\mathcal{L}_{K(x)} = \{P_{p(x)} : p(x) \in K[x] \text{ irreducible }\} \cup \{P_\infty\}$$

Sea K algebraicamente cerrado en F ($\tilde{K} = K$).

Definición

El **grupo de divisores** de F/K, $\mathcal{D}_F$, es el grupo abeliano libre generado por $\mathcal{L}_F$. O sea,

$$\mathcal{D}_F = \left\{ D = \sum_{i=1}^{k} n_i P_i : k \in \mathbb{N},\ n_i \in \mathbb{Z},\ P_i \in \mathcal{L}_F \right\}.$$

- la $+$ en $\mathcal{D}_F$ es

$$\sum_i n_i P_i + \sum_i n_i' P_i = \sum_i (n_i + n_i')\, P_i$$

- el cero es

$$0 = 0 \cdot P$$

Definición

Un divisor $D = n_1 P_1 + \cdots + n_k P_k$ se dice **efectivo** si

$$D \geq 0 \quad \Leftrightarrow \quad n_i \geq 0 \qquad i = 1, \ldots, k$$

Los divisores efectivos forman un semigrupo que denotamos

$$\mathcal{D}_F^+ = \{D \in \mathcal{D}_F : D \geq 0\}$$

y se tiene

$$\mathcal{L}_F \subsetneq \mathcal{D}_F^+ \subsetneq \mathcal{D}_F$$

Definición

Dado $x \in F^*$, el **divisor de ceros** y el **divisor de polos** de x son

$$(x)_0 = \sum_{P \in \mathcal{Z}} v_P(x)\, P \geq 0$$

$$(x)_\infty = -\sum_{P \in \mathcal{N}} v_P(x)\, P \geq 0$$

respectivamente. El **divisor principal** de x es

$$(x) = (x)_0 - (x)_\infty = \sum_{P \in \mathcal{L}_F} v_P(x)\, P$$

Definición

El **grado** de $D \in \mathcal{D}_F$ es

$$\deg(\sum_i n_i P_i) = \sum_i n_i \deg P_i$$

- $$\deg : \mathcal{D}_F \to \mathbb{Z}$$

  es un homomorfismo con núcleo

  $$\ker \deg = \{D \in \mathcal{D}_F : \deg D = 0\} =: \mathcal{D}_F^0$$

- $$\deg(x)_0 = \deg(x)_\infty = [F : K(x)]$$

  y por lo tanto

  $$\deg(x) = 0$$

Definición

Definimos el **grupo de divisores principales** de F/K

$$\mathcal{P}_F = \{(x) : x \in F^*\}$$

y el **grupo de clases de divisores**

$$\mathcal{C}_F = \mathcal{D}_F/\mathcal{P}_F$$

- $\mathcal{P}_F$ es grupo abeliano

$$(x) + (y) = (xy) \qquad x, y \in F^*$$

- $D \sim D' \Leftrightarrow [D] = [D'] \Leftrightarrow D = D' + (x)$ para algún $x \in F^*$.

Definición

Dado $A \in \mathcal{D}_F$, el **espacio de Riemann-Roch** asociado es

$$\mathcal{L}(A) = \{x \in F^* : (x) + A \geq 0\} \cup \{0\}$$

- $x \in \mathcal{L}(A) \setminus \{0\} \quad \Leftrightarrow \quad v_P(x) \geq -n_P(A)$ para todo $P \in \mathcal{L}_F$.
- $\mathcal{L}(A) \neq \{0\} \quad \Leftrightarrow \quad$ existe $A' \in D_F^+, A' \sim A$, o sea

$$A' = A + (x)$$

Hechos básicos:

- $\mathcal{L}(A)$ es un K-espacio vectorial y

$$\dim A := \dim \mathcal{L}(A) < \infty$$

- $A' \sim A \quad \Rightarrow \quad \dim A' = \dim A \quad$ y $\quad \deg A' = \deg A.$
- $\deg A < 0 \quad \Rightarrow \quad \dim A = 0.$
- Si $\deg A = 0$, entonces

$$A \text{ es principal} \quad \Leftrightarrow \quad \dim A \geq 1 \quad \Leftrightarrow \quad \dim A = 1.$$

Definición

el **género** de un cuerpo de funciones algebraicas F/K es

$$0 \leq g = \max_{A \in \mathcal{D}_F} \{\deg A - \dim A + 1\} < \infty$$

Teorema (Riemann)

Sea F/K de género g. Para todo $A \in \mathcal{D}_F$ se tiene

1. $\dim A \geq \deg A + 1 - g$
2. $\dim A = \deg A + 1 - g$ *para* $\deg A$ *suficientemente grande.*

Como corolario del Teorema de Riemann-Roch se tiene que

$$\deg A \geq 2g - 1 \quad \Rightarrow \quad \dim A = \deg A + 1 - g.$$

Proposición

Si $F = K(x)$ entonces $g = 0$.

Prueba. Notar que

$$(x)_0 = v_0(x)P_0 = P_0, \qquad (x)_\infty = -v_\infty(x)P_\infty = P_\infty.$$

Para $0 \leq s \leq r$ vale

$$(x^s) = s(x) = sP_0 - sP_\infty \geq -sP_\infty \geq -rP_\infty$$

luego,

$$1, x, x^2, \ldots, x^r \in \mathcal{L}(rP_\infty) = \{z \in F : (z) \geq -rP_\infty\} \cup \{0\}$$

Como éstos son linealmente independientes se tiene

$$r + 1 \leq \dim(rP_\infty) = \deg(rP_\infty) + 1 - g = r + 1 - g$$

para r suficientemente grande. Luego $g \leq 0$, y así $g = 0$. □

1d. Ejemplos (cuerpos racionales)

Caracterización de los cuerpos de funciones racionales

$$F/K \text{ es racional} \quad \Leftrightarrow \quad \begin{cases} g = 0, \\ \exists\, A \in \mathcal{D}_F \text{ con } \deg A = 1. \end{cases}$$

1d. Ejemplos (cuerpos elípticos)

Definición

F/K se dice un **cuerpo de funciones elípticas** si

- $g = 1$,
- existe $A \in \mathcal{D}_F$ con $\deg A = 1$.

1d. Ejemplos (cuerpos elípticos)

Teorema (Caracterización de los cuerpos elípticos)

- *Sea F/K un cuerpo de funciones elípticas. Entonces existen $x, y \in F$ tales que $F = K(x, y)$ donde*
  - *si $\chi(K) \neq 2$*

$$y^2 = f(x) = ax^3 + bx^2 + cx + d \in K[x], \qquad a \neq 0$$

    con $f(x)$ sin cuadrados.
  - *si $\chi(K) = 2$,*

$$y^2 = \begin{cases} ax^3 + bx^2 + cx + d & a \neq 0, \\ x + \frac{1}{ax+b} & a, b \in K, a \neq 0. \end{cases}$$

- *Recíprocamente, si $F = K(x, y)$ donde x, y satisfacen una ecuación como arriba, entonces F/K es un cuerpo de funciones elípticas y $\tilde{K} = K$.*

1d. Ejemplos (cuerpos elípticos)

Ejemplo (funciones meromorfas de la esfera de Riemann)

- Una **función elíptica** con respecto a un retículo

$$\Gamma = \mathbb{Z}\gamma_1 \oplus \mathbb{Z}\gamma_2 \subset \mathbb{C}$$

es una función meromorfa $f(z)$ en $\mathbb{C}$ periódica en Γ, o sea

$$f(z+\gamma) = f(z) \qquad \gamma \in \Gamma$$

$$f(\gamma) \neq \infty \qquad \gamma \in \Gamma$$

- Las funciones elípticas sobre Γ forman un subcuerpo $\mathcal{M}(\Gamma)$ de las funciones meromorfas de $\mathbb{C}$ y $\mathbb{C} \subset \mathcal{M}(\Gamma)$.

1d. Ejemplos (cuerpos elípticos)

Ejemplo (funciones meromorfas de la esfera de Riemann)

- El paradigma de función elíptica es la $\wp$ de **Weierstraß**

$$\wp(z) = \frac{1}{z^2} + \sum_{0 \neq \gamma \in \Gamma} \frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2}$$

y su derivada $\wp'(z)$

$$\wp'(z) = -2 \sum_{\gamma \in \Gamma} \frac{1}{(z-\gamma)^3}$$

1d. Ejemplos (cuerpos elípticos)

Ejemplo (funciones meromorfas de la esfera de Riemann)

- Se prueba que

$$\mathcal{M}(\Gamma) = \mathbb{C}(\wp(z), \wp'(z))$$

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

donde $f(T) = 4T^3 - g_2 T - g_3 \in \mathbb{C}[T]$ es sin cuadrados y

$$g_2 = 60 \sum_{0 \neq \gamma \in \Gamma} \gamma^{-4}, \qquad g_2 = 140 \sum_{0 \neq \gamma \in \Gamma} \gamma^{-6}$$

- Luego, $\mathcal{M}(\Gamma)/\mathbb{C}$ es un cuerpo de funciones elípticas.

1d. Ejemplos (cuerpos hiperelípticos)

Definición

F/K se dice un **cuerpo de funciones hiperelípticas** si

- $g \geq 2$,
- existe $A \in \mathcal{D}_F$ con $\deg A = 2$ y $\dim A = 2$.

Están caracterizados como los

$$F = K(x, y)$$

$$y^2 = f(x) \in K[x]$$

con $f(x)$ sin cuadrados y

$$\deg f = 2g + 1, 2g + 2$$

1d. Ejemplos (extensiones cíclicas de $K(x)$)

Teorema

Sea $F = K(x, y)$ *definido por*

$$y^n = a \prod_{i=1}^{s} p_i(x)^{n_i}, \qquad s > 0, a \in K^*, n_i \in \mathbb{Z},$$

los $p_i(x)$ *irreducibles en* $K[x]$, $\chi(K) \nmid n$ *y* $(n, n_i) = 1$, $1 \leq i \leq s$.

Entonces

$$\tilde{K} = K, \qquad [F : K(x)] = n$$

y

$$g = \tfrac{n-1}{2}\Big(-1 + \sum_{i=1}^{s} \deg p_i(x)\Big) - \tfrac{d-1}{2}$$

donde $d = \big(n, \sum_{i=1}^{s} n_i \cdot \deg p_i(x)\big)$.

1d. Ejemplos (tipo-Fermat)

Ejemplo

- El cuerpo $F = K(x, y)$ definido por

$$ax^n + by^n = c$$

donde

$$a, b, c \in K^*, \quad \chi(K) \nmid n,$$

se llama de **tipo-Fermat** y

$$g = \frac{(n-1)^2}{2} - \frac{(n-1)}{2} = \frac{(n-1)(n-2)}{2}.$$

1d. Ejemplos (cuerpos Hermitianos)

Ejemplo

- El cuerpo de funciones $H = \mathbb{F}_{q^2}(x, y)$ donde

$$x^{q+1} + y^{q+1} = 1$$

se llama **cuerpo de funciones Hermitiano** y

$$g = \tfrac{1}{2}q(q-1).$$

- Notar que H es un caso particular de tipo-Fermat, con
  - $K = \mathbb{F}_{q^2}$,
  - $n = q + 1$,
  - $a = b = c = 1$.

1d. Ejemplos (cuártica de Klein)

Ejemplo

- El cuerpo de funciones $F = K(x, y)$ definido por la ecuación

$$x^3 + y^3 x + y = 0$$

se llama la **cuártica de Klein**.

- Se puede ver que

$$g = \tfrac{1}{2}(4-1)(4-2) = 3.$$

2. LA FUNCIÓN ZETA DE UN CUERPO DE FUNCIONES

(a) La función Z en $F/\mathbb{F}_q$.

(b) Convergencia.

(c) Producto de Euler.

(d) Extensiones constantes.

(e) Ecuación funcional.

2a. La función Z en $F/\mathbb{F}_q$

- Recordar que tenemos

$$\mathcal{L}_F \subset \mathcal{D}_F^+ \subset \mathcal{D}_F, \qquad \mathcal{C}_F = \mathcal{D}_F/\mathcal{P}_F$$

- Si $n \in \mathbb{Z}$, ponemos

$$\begin{aligned} \mathcal{D}_F^n &= \{A \in \mathcal{D}_F : \deg A = n\} \\ \mathcal{C}_F^n &= \{A \in \mathcal{C}_F : \deg [A] = n\} \end{aligned}$$

2a. La función Z en $F/\mathbb{F}_q$

Definición

Para $n \geq 0$, interesan los números

$$\begin{aligned} A_n &= \#\{A \in \mathcal{D}_F^+ : \deg A = n\} \\ B_n &= \#\{P \in \mathcal{L}_F : \deg P = n\} \end{aligned}$$

Lema

$A_n < \infty$ y $B_n < \infty$ para todo $n \geq 0$.

Notar que

- $A_0 = 1$
- $A_1 = B_1 = N = \#\{P \in \mathcal{L}_F : \deg\ P = 1\}$
- $B_n \leq A_n$

2a. La función Z en $F/\mathbb{F}_q$

Definición

El grupo de clases de divisores de grado 0

$$Pic_0(F) = \mathcal{C}_F^0 = \mathcal{D}_F^0/\mathcal{P}_F = \{[A] \in \mathcal{C}_F : \deg[A] = 0\}$$

Proposición

$\mathcal{C}_F^0$ es un grupo finito y el orden $h = h_F = |\mathcal{C}_F^0|$ se llama el **número de clase** *de F.*

Definición

$$0 < \partial = \text{mín}\{\deg A : A \in \mathcal{D}_F,\ \deg A > 0\}.$$

La imagen del homomorfismo $\deg : \mathcal{D}_F \to \mathbb{Z}$ es el subgrupo generado por ∂,

$$\deg(D_F) = \langle \partial \rangle \subseteq \mathbb{Z}$$

luego

$$A \in \mathcal{D}_F \quad \Rightarrow \quad \deg A = k\partial, \quad k \in \mathbb{Z}$$

O sea,

$$A_n = 0 \quad \text{si} \quad \partial \nmid n$$

2a. La función Z en $F/\mathbb{F}_q$

Definición

La **función zeta** de F es

$$Z(t) = Z_F(t) = \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}[\![t]\!].$$

Lema

Tenemos

1. *Si* $[C] \in \mathcal{C}_F$, *entonces*

$$\#\{A \in [C] : A \geq 0\} = \frac{q^{\dim[C]} - 1}{q - 1}$$

2. *Si* $n > 2g - 2$, *con* $\partial \mid n$, *entonces*

$$A_n = h \cdot \frac{q^{n+1-g} - 1}{q - 1}$$

2b. Convergencia de Z

Proposición

La función $Z(t)$ converge en $B(0, \frac{1}{q})$. Más aún,

1. *Si $g = 0$ entonces*

$$Z(t) = \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right)$$

2b. Convergencia de Z

Proposición

- *Si* $g \geq 1$, *entonces* $Z(t) = F(t) + G(t)$, *donde*

$$F(t) = \frac{1}{q-1} \sum_{\deg[C]=0}^{2g-2} q^{\dim[C]}\, t^{\deg[C]} \in \mathbb{Q}[t],$$

$$G(t) = \frac{h}{q-1}\left(\frac{q^{1-g}(qt)^{2g-2+\partial}}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right)$$

Proposición (Producto de Euler)

Para $|t| < \frac{1}{q}$, $Z(t)$ *se puede escribir como el producto*

$$Z(t) = \prod_{P \in \mathcal{L}_F} \frac{1}{1 - t^{\deg P}}$$

absolutamente convergente. En particular,

$$Z(t) \neq 0$$

Prueba.

$$\prod_{P\in\mathcal{L}_F}(1-t^{\deg P})^{-1} \text{ abs. conv.} \Leftrightarrow \prod_{P\in\mathcal{L}_F}(1-t^{\deg P}) \text{ abs. conv.}$$

Como $\mathcal{L}_F \subseteq \mathcal{D}_F^+$,

$$\sum_{P\in\mathcal{L}_F}|t|^{\deg P} = \sum_{n=0}^{\infty} B_n|t|^n \leq \sum_{n=0}^{\infty} A_n|t|^n < \infty, \qquad |t| < \tfrac{1}{q}.$$

Luego $\prod_{P\in\mathcal{L}_F}(1-t^{\deg P})^{-1}$ converge absolutamente en $|t| < \frac{1}{q}$.

Ahora,

$$\prod_{P\in\mathcal{L}_F}\frac{1}{1-t^{\deg P}} = \prod_{P\in\mathcal{L}_F}\sum_{n=0}^{\infty}t^{n\deg P} = \prod_{P\in\mathcal{L}_F}\sum_{n=0}^{\infty}t^{\deg nP}$$

$$= \sum_{A\in\mathcal{D}_F^+}t^{\deg A} = \sum_{n=0}^{\infty}A_n t^n = Z(t)$$

donde usamos la serie geométrica. □

2d. La función Z de extensiones constantes

Para cada $r \geq 1$ sea

$$F_r = F\mathbb{F}_{q^r} \subseteq F\overline{\mathbb{F}}_q$$

- $F_r/\mathbb{F}_{q^r}$ es un cuerpo de funciones, extensión de $F/\mathbb{F}_q$,
- F_r/F es una extensión cíclica de grado r,
- $\mathbb{F}_{q^r}$ es el cuerpo de constantes de F_r,
- $g(F_r/\mathbb{F}_{q^r}) = g(F/\mathbb{F}_q)$,
- Si $P \in \mathcal{D}_F^n$ existen $P_1, \ldots, P_d \in \mathcal{L}_{F_r}$ con $d = (r, n)$ tales que

$$P_i \mid P, \quad e(P_i, P) = 1 \quad \text{y} \quad \deg P_i = \frac{n}{d}$$

para $i = 1, \ldots, d$

2d. La función Z de extensiones constantes

Proposición

Si $Z_r(t)$ denota la función zeta de F_r, se tiene

$$Z_r(t^r) = \prod_{\zeta^r=1} Z(\zeta t) = \prod_{k=1}^{r} \zeta(e^{2\pi ik/r} t)$$

para todo $t \in \mathbb{C}$

Prueba. Si $m \geq 1, r \geq 1$ y $d = (m, r)$ tenemos

$$(X^{r/d} - 1)^d = \prod_{\zeta^r=1} (X - \zeta^m)$$

Tomando $X = t^{-m}$ y multiplicando por t^{mr} se obtiene

$$(1 - t^{mr/d})^d = \prod_{\zeta^r=1} \left(1 - (\zeta t)^m\right)$$

2d. La función Z de extensiones constantes

Basta tomar $|t| < 1/q$. Tenemos

$$Z_r(t^r) = \prod_{P \in \mathcal{L}_F} \prod_{P'|P} (1 - t^{r \deg P'})^{-1}$$

Para $P \in \mathcal{L}_F$ fijo, con $d = (r, \deg P)$. Entonces

$$\prod_{P'|P} (1 - t^{r \deg P'}) = \prod_{i=1}^{d} (1 - t^{r \frac{\deg P}{d}}) = (1 - t^{r \frac{\deg P}{d}})^d = \prod_{\zeta^r = 1} (1 - (\zeta t)^{\deg P})$$

Luego,

$$Z_r(t^r) = \prod_{\zeta^r = 1} \prod_{P \in \mathcal{L}_F} (1 - (\zeta t)^{\deg P})^{-1} = \prod_{\zeta^r = 1} Z(\zeta t)$$

□

Corolario

$$\partial = 1$$

Prueba. Para ζ^{∂} vale

$$Z(\zeta t) = \prod_{P \in \mathcal{L}_F} (1 - (\zeta t)^{\deg P})^{-1} = \prod_{P \in \mathcal{L}_F} (1 - t^{\deg P})^{-1} = Z(t).$$

Luego,

$$Z_{\partial}(t^{\partial}) = \prod_{\zeta^{\partial}=1} Z(\zeta t) = Z(t)^{\partial}.$$

- $Z_{\partial}(t^{\partial})$ tiene un polo simple en $t = 1$,
- $Z(t)^{\partial}$ tiene un polo de orden ∂ en $t = 1$.

Luego, $\partial = 1$. □

Teorema (Corolario del Corolario)

1. *Si* $g = 0$ *entonces* F *es racional y*

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

2. *Si* $g \geq 1$ *entonces* $Z(t) = F(t) + G(t)$, *donde*

$$\begin{aligned} F(t) &= \frac{1}{q-1} \sum_{\deg[C]=0}^{2g-2} q^{\dim[C]} t^{\deg[C]} \\ G(t) &= \frac{h}{q-1} \left(\frac{q^g t^{2g-1}}{1-qt} - \frac{1}{1-t} \right) \end{aligned}$$

2e. La ecuación funcional

Proposición (Ecuación funcional)

$$Z(t) = q^{g-1}\, t^{2g-2}\, Z(\tfrac{1}{qt})$$

3. EL POLINOMIO L DE UN CUERPO DE FUNCIONES

(a) El L-polinomio y sus propiedades.

(b) Los números N_r, S_r y B_r.

(c) La función Z de Pellikaan.

Definición

El L-**polinomio** de F es

$$L(t) = L_F(t) = (1-t)(1-qt)Z(t)$$

Notar que

- $L(t)$ es un polinomio de grado $\leq 2g$.
- $L(t)$ contiene toda la información sobre los A_n, pues

$$Z(t) = \sum_{n=0}^{\infty} A_n t^n.$$

Teorema (parte 1)

1. $L(t) \in \mathbb{Z}[t]$ y $\deg L(t) = 2g$.
2. $L(t) = q^g t^{2g} L(\frac{1}{qt})$.
3. $L(1) = h$.
4. *Si* $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g}$ *entonces*
   1. $a_0 + \cdots + a_{2g} = h$,
   2. $a_0 = 1 = L(0)$ y $a_{2g} = q^g$,
   3. $a_{2g-i} = q^{g-i} a_i$ *para* $1 \leq i \leq g$,
   4. $a_1 = N - (q+1)$ *donde*

$$N = \#\{P \in \mathcal{L}_F : \deg P = 1\}$$

Teorema (parte 2)

1. *$L(t)$ se factoriza en $\mathbb{C}[t]$ de la forma*

$$L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t).$$

Los números complejos $\alpha_1, \ldots, \alpha_{2g}$ son enteros algebraicos y satisfacen $\alpha_i \alpha_{g+i} = q$, para $i = 1, \ldots, g$.

2. *Si*

$$L_r(t) = (1 - t)(1 - q^r t)Z_r(t)$$

denota el L-polinomio de la extensión $F_r = F\mathbb{F}_{q^r}$, entonces

$$L_r(t) = \prod_{i=1}^{2g}(1 - \alpha_i^r t).$$

Ejemplo (cuerpos racionales)

Si $g = 0$ entonces $L(t) = 1$ y

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

En particular

$$h = 1$$

Ejemplo (cuerpos elípticos / curvas elípticas)

Como $g = 1$ entonces $L(t) = 1 + a_1 t + a_2 t^2$ y con

$$a_1 = N - (q+1), \qquad a_2 = q^g$$

Luego,

$$Z(t) = \frac{1 + (N - (q+1))t + qt^2}{(1-t)(1-qt)}$$

y

$$h = L(1) = N$$

3b. Los números N_r, S_r y B_r

El teorema anterior dice que los números

$$N_r := N(F_r) := \#\{P \in \mathcal{L}_{F_r} : \deg P = 1\}$$

pueden ser calculados si se conoce $L_r(t)$, o sea, si se conoce $L(t)$.

Corolario

Para todo $r \geq 1$,

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r$$

Prueba. Si $L_r(t) = \sum_{i=1}^{2g} a_{i,r} t^i$, sabemos que $a_{1,r} = N_r - (q^r + 1)$ y como $L_r(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t)$ entonces $a_{1,r} = -\sum_{i=1}^{2g} \alpha_i^r$. □

3b. Los números N_r, S_r y B_r

Si los N_r son conocidos para suficientes r's, se pueden calcular los coeficientes de $L(t)$. Sea

$$S_r = N_r - (q^r + 1).$$

Corolario

- *Vale*

$$\frac{L'(t)}{L(t)} = \sum_{r=1}^{\infty} S_r \, t^{r-1}$$

- $a_0 = 1$ *y*

$$i a_i = S_i a_0 + S_{i-1} a_1 + \cdots + S_1 a_{i-1}, \qquad i = 1, \ldots, g.$$

Luego, dado $N_1, \ldots, N_g$ *podemos determinar* $L(t)$ *y las ecuaciones* $a_{2g-i} = q^{g-i} a_i$, $i = 0, \ldots, g$.

Prueba.

- Tenemos

$$\begin{aligned}\frac{L'(t)}{L(t)} &= \sum_{i=1}^{2g} \frac{-\alpha_i}{(1-\alpha_i t)} = \sum_{i=1}^{2g}(-\alpha_i)\sum_{r=0}^{\infty}(\alpha_i t)^r \\ &= \sum_{r=1}^{\infty}\Big(\sum_{i=1}^{2g} -\alpha_i^r\Big)t^{r-1} = \sum_{r=1}^{\infty} S_r\, t^{r-1}\end{aligned}$$

- Como

$$a_1+2a_2t+\cdots+2g\,a_{2g}\,t^{2g} = (a_0+a_1t+\cdots+a_{2g}t^{2g})\sum_{r=1}^{\infty} S_r\, t^{r-1}$$

basta compararar los coeficientes de $t^0, t^1, \ldots, t^{g-1}$. □

Ejemplo (Cuártica de Klein)

- Sea $F = K(x, y)$ con

$$y^3 + x^3 y + x = 0$$

- Se prueba que

$$g = \begin{cases} 0 & \chi(K) = 7 \\ 3 & \chi(K) \neq 7 \end{cases}$$

- Sea $K = \mathbb{F}_2$ y $F_r = F\mathbb{F}_2^r$. Se puede ver que

$$N_1 = 3 \qquad N_2 = 5 \qquad N_3 = 24$$

- Luego

$$L(t) = 1 + a_1 t + a_2 t^2 + a_3 t^3 + a_4 t^4 + a_5 t^5 + 2^3 t^6$$

Ejemplo (Cuártica de Klein)

- Como
$$a_{6-i} = 2^{3-i} a_i, \qquad 0 \leq i \leq 3$$
tenemos
$$a_5 = 4a_1 \qquad a_4 = 2a_2$$
- Como
$$S_r = N_r - (2^r + 1)$$
se tiene
$$\begin{aligned} S_1 &= N_1 - (2+1) = 3 - 3 = 0 \\ S_2 &= N_2 - (2^2+1) = 5 - 5 = 0 \\ S_3 &= N_3 - (2^3+1) = 24 - 9 = 15 \end{aligned}$$

Ejemplo (Cuártica de Klein)

- Como
$$ia_i = S_i a_0 + S_{i-1} a_1 + \cdots + S_1 a_{i-1}$$
para $i = 1, \ldots, 3$ tenemos
  - $a_1 = S_1 a_0 = 0 = a_5$
  - $2a_2 = S_2 a_0 + S_1 a_1 = 0 = a_4$
  - $3a_3 = S_3 a_0 + S_2 a_1 + S_1 a_2 = S_3 = 15 \quad \Rightarrow \quad a_3 = 5$
- Luego
$$L(t) = 1 + 5t^3 + 8t^6$$
y
$$h = L(1) = 14 \qquad \text{y} \qquad L(t) = 8t^6 L(\tfrac{1}{2t})$$

Ejemplo (Cuártica de Klein)

Podemos calcular $L_2(t)$ y $L_3(t)$.

$$L_2(t) = (1-t)(1-q^2t)Z_2(t) \qquad Z_2(t^2) = Z(t)Z(-t)$$

Luego,

$$\begin{aligned} L_2(t^2) &= (1-t^2)(1-(qt)^2)Z(t)Z(-t) \\ &= (1-t^2)(1-(qt)^2)\frac{L(t)}{(1-t)(1-qt)}\frac{L(-t)}{(1+t)(1+qt)} \\ &= L(t)L(-t) = (1+5t^3+8t^6)(1-5t^3+8t^6) \\ &= (8t^6+1)^2-(5t^3)^2 = 64t^{12}-9t^6+1 \end{aligned}$$

y por lo tanto

$$L_2(t) = 8^2t^6 - 9t^3 + 1$$

Ejemplo (Cuártica de Klein)

Ahora

$$L_3(t) = (1-t)(1-q^3t)Z_3(t)$$

$$Z_3(t^3) = Z(t)Z(\omega t)Z(\omega^2 t)$$

con $\omega^3 = 1$, $\omega \neq 1$ y $\omega^2 + \omega + 1 = 0$.
Luego,

$$L_3(t^3) = (1-t^3)(1-(qt)^3)Z(t)Z(\omega t)Z(\omega^2 t)$$

Ejemplo (Cuártica de Klein)

Ahora

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)}$$

$$Z(\omega t) = \frac{L(\omega t)}{(1-\omega t)(1-\omega qt)}$$

$$Z(\omega^2 t) = \frac{L(\omega^2 t)}{(1-\omega^2 t)(1-\omega^2 qt)}$$

$$L(t) = 1 + 5t^3 + 8t^6 = L(\omega t) = L(\omega^2 t)$$

Luego

$$L_3(t^3) = L(t)^3 = (1 + 5t^3 + 8t^6)^3$$

$$L_3(t) = (1 + 5t + 8t^2)^3 = 8^3 t^6 + \cdots$$

3b. Los números N_r, S_r y B_r

Recordemos que

$$B_n = \#\{p \in \mathcal{L}_F : \deg P = n\} \leq A_n$$

Lema (Relación entre N_r y B_d)

$$N_r = \sum_{d|r} d \cdot B_d$$

Prueba. Todo $P \in \mathcal{L}_F$ de grado $d \mid r$ se descompone como d lugares de grado 1 en $F_r = F\mathbb{F}_{q^r}$ y las extensiones P' de P en F_r/F tienen grado $\deg P' > 1$ si $\deg P \nmid r$. $\square$

Lema (Relación entre S_r y B_d)

$$B_r = \frac{1}{r} \sum_{d|r} \mu(\tfrac{r}{d})(q^d - S_d)$$

donde μ es la función de Möbius.

Prueba. Por la fórmula de inversión de Möbius

$$r \cdot B_r = \sum_{d|r} \mu(\tfrac{r}{d}) \cdot N_d$$

y

$$\sum_{d|r} \mu(\tfrac{r}{d}) = 0, \qquad r > 1.$$

3b. Los números N_r, S_r y B_r

Sea

$$z(t) = \sum_{r=0}^{\infty} \frac{N_r}{r} t^r$$

Proposición (descripción alternativa de $Z(t)$)

$$Z(t) = e^{z(t)} = \prod_{d=1}^{\infty} (1 - t^d)^{-B_d}$$

Prueba. (1) Veamos que $z(t) = \ln \prod_{d=1}^{\infty} (1-t^d)^{-B_d}$.

$$\begin{aligned}
\ln \prod_{d=1}^{\infty} (1-t^d)^{-B_d} &= -\sum_{d=1}^{\infty} B_d \cdot \ln(1-t^d) \\
&= \sum_{d=1}^{\infty} B_d \Big(\sum_{r=1}^{\infty} \frac{t^{rd}}{r} \Big) \\
&= \sum_{r=1}^{\infty} \Big(\sum_{d|r} B_d \tfrac{d}{r} \Big) t^r = \sum_{r=1}^{\infty} \tfrac{N_r}{r} t^r = z(t)
\end{aligned}$$

luego

$$e^{z(t)} = \prod_{d=1}^{\infty} (1-t^d)^{-B_d}$$

(2) Ahora

$$\begin{aligned}\prod_{d=1}^{\infty}\frac{1}{(1-t^d)^{B_d}} &= \prod_{P\in\mathcal{L}_F}\frac{1}{(1-t^{\deg P})}\\ &= \prod_{P\in\mathcal{L}_F}\Big(\sum_{n=0}^{\infty}t^{\deg nP}\Big)\\ &= \sum_{D\in\mathcal{D}_F^+}t^{\deg D}=\sum_{n=0}^{\infty}A_nt^n=Z(t)\end{aligned}$$

y listo.

3c. Zeta de Pellikaan

- Queremos Z en 2 variables. Lo más natural sería definir

$$Z(t,v) = \sum_{n=0}^{\infty} \sum_{k=1}^{\infty} A_{n,k}\, t^n v^k$$

donde

$$A_{n,k} = \#\{A \in \mathcal{D}_F^+ \,:\, \deg A = n,\, \dim A = k\}$$

- Notar que,

$$Z(t,1) = \sum_{n=0}^{\infty} \Big(\sum_{k=1}^{\infty} A_{n,k} \Big)\, t^n = \sum_{n=0}^{\infty} A_n\, t^n = Z(t).$$

- $Z(t,v)$ define una función racional, pero no es obvio como obtener una ecuación funcional.

3c. Zeta de Pellikaan

- Mejor es definir

$$Z(t,u) = \sum_{n=0}^{\infty} \sum_{k=1}^{\infty} a_{n,k} \, \frac{u^k - 1}{u - 1} \, t^n$$

donde

$$a_{n,k} = \#\{[A] \in \mathcal{C}_F \, : \, \deg[A] = n, \, \dim[A] = k\}$$

- Recordemos que para cada $A \in \mathcal{D}_F$ con $\dim A = k$ hay $\frac{q^k - 1}{q - 1}$ divisores en la clase $[A]$ y así

$$A_n = a_{n,k} \, \frac{q^k - 1}{q - 1}$$

- Luego,

$$Z(t,q) = \sum_{n=0}^{\infty} \sum_{k=1}^{\infty} a_{n,k} \, \frac{q^k - 1}{q-1} \, t^n = \sum_{n=0}^{\infty} A_n \, t^n = Z(t)$$

- $Z(t,u)$ tiene propiedades análogas a $Z(t)$ por lo que es la generalización correcta.

Por ejemplo

Proposición (Ecuación funcional)

$$Z(t,u) = u^{g-1} \, t^{2g-2} \, Z(\tfrac{1}{ut}, u)$$

Proposición

La función $Z(t,u)$ define una función racional. Más aún,

1. *Si $g = 0$ entonces*

$$Z(t,u) = \frac{1}{(1-t)(1-ut)}$$

2. *Si $g \geq 1$, entonces $Z(t,u) = F(t,u) + G(t,u)$, donde*

$$F(t,u) = \frac{1}{u-1} \sum_{\deg[C]=0}^{2g-2} u^{\dim[C]} t^{\deg[C]}$$

$$G(t,u) = \frac{h}{u-1}\left(\frac{u^g t^{2g-1}}{1-ut} - \frac{1}{1-t}\right)$$

Proposición (L-polinomio)

$Z(t,u)$ es de la forma

$$Z(t,u) = \frac{L(t,u)}{(1-t)(1-ut)}$$

donde $L(t,u) \in \mathbb{Z}[t,u]$ *con* $\deg_t L = 2g$ *y* $\deg_u L = g$.

1. $L(1,u) = h$.
2. *Si* $L(t,u) = a_0(u) + a_1(u)t + \cdots + a_{2g}(u)t^{2g}$ *entonces*
   1. $a_0(u) = 1, \qquad a_{2g}(u) = u^g$.
   2. $\deg a_i(u) \leq i/2, \qquad 1 \leq i \leq 2g$.
   3. $a_{2g-i}(u) = u^{g-i}a_i(u), \qquad 1 \leq i \leq g$.

Ejemplo

Si F es un cuerpo elíptico con N lugares racionales (curva elíptica con N puntos racionales) Entonces

$$Z(t,u) = \frac{1 + (N - 1 - u)t + ut^2}{(1-t)(1-ut)}$$

4. HASSE-WEIL Y LA HIPÓTESIS DE RIEMANN

(a) El Teorema de Hasse-Weil.

(b) La Hipótesis de Riemann para cuerpos de funciones.

Teorema (Hasse-Weil)

Los recíprocos de las raíces de $L(t)$ satisfacen

$$|\alpha_i| = q^{1/2} \qquad 1 \leq i \leq 2g.$$

Corolario

Sea $r \geq 1$. El Teorema de Hasse-Weil vale para $F/\mathbb{F}_q$ si y sólo si vale para la extensión constante $F_r/\mathbb{F}_{q^r}$. En particular,

$$|\alpha_i^r| = q^{r/2} \qquad 1 \leq i \leq 2g.$$

Prueba del corolario. Los recíprocos de las raíces de $L_r(t)$ son $\alpha_1^r, \ldots, \alpha_{2g}^r$, $r \geq 1$. El resultado sigue de

$$|\alpha_i| = q^{1/2} \qquad \Leftrightarrow \qquad |\alpha_i^r| = |\alpha_i|^r = q^{r/2}$$

Corolario (Cota de Hasse-Weil)

Para $F_r/\mathbb{F}_{q^r}$ de género g con $r \geq 1$ vale

$$|N_r - (q^r + 1)| \leq 2gq^{r/2}$$

Prueba.

$$|N_r - (q^r + 1)| = |\sum_{i=1}^{2g} \alpha_i^r| \leq \sum_{i=1}^{2g} |\alpha_i^r| = 2gq^{r/2}$$

Existe una mejora para el caso en que $r = 1$.

Teorema (Cota de Serre)

Para $F/\mathbb{F}_q$ de género g se tiene

$$|N - (q + 1)| \leq g[2q^{1/2}]$$

$F/\mathbb{F}_q$ se dice **maximal** si se alcanza la igualdad en la Cota de Hasse-Weil, i.e., $N = q + 1 + 2g\sqrt{q}$. En particular, $q = p^{2m}$.

Proposición

Si $F/\mathbb{F}_q$ es maximal entonces $g \leq \frac{q-\sqrt{q}}{2}$

Prueba. Tenemos $N = q + 1 - \sum \alpha_i$ y $|\alpha_i| = \sqrt{q}$. Como $N = q + 1 + 2g\sqrt{q}$ se tiene $\alpha_i = -\sqrt{q}$, $1 \leq i \leq 2g$. Ahora

$$N_2 = q^2 + 1 - \sum \alpha_i^2 = q^2 + 1 - 2g\sqrt{q}$$

y $N \leq N_2$ implica

$$q + 1 + 2g\sqrt{q} \leq q^2 + 1 - 2gq$$

de donde $g \leq \frac{1}{2}(q - \sqrt{q})$. □

Ejemplo (Cuerpos Hermitianos)

- El cuerpo de funciones Hermitiano $H = \mathbb{F}_{q^2}(x, y)$ se puede definir mediante la ecuación

$$y^q + y = x^{q+1}$$

- Se puede ver que

$$g = \tfrac{1}{2}q(q-1) \qquad N = q^3 + 1$$

- La cota de Hasse-Weil es:

$$N \leq q^2 + 1 + 2g\sqrt{q^2} = q^2 + 1 + q(q-1)q = q^3 + 1$$

- Luego H es maximal.

asintóticas

- Definimos los números
  - $N_g(F) = \text{máx}\{N(F) : F/\mathbb{F}_q \text{ de género } g\}$
  - $A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{g}$
- Por la cota de Serre y Hasse-Weil tenemos

$$A(q) \leq [2\sqrt{q}] \leq 2\sqrt{q}$$

Estas versiones asintóticas pueden ser mejoradas.

Teorema (Cota de Drinfeld-Vladut)

$$A(q) \leq \sqrt{q} - 1$$

4b. La Hipótesis de Riemann

El teorema de Hasse-Weil suele llamarse la *hipótesis de Riemann para cuerpos de funciones algebraicas*.

- La función *zeta de Riemann* clásica

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}, \qquad Re(s) > 1$$

tiene ceros triviales en $s = -2, -4, -6 \ldots$

Conjetura (Hipótesis de Riemann)

Los ceros no triviales de $\zeta(s)$ están todos en la recta $Re(s) = \frac{1}{2}$.

- La **norma absoluta** de $A \in \mathcal{D}_F$ es

$$\mathcal{N}(A) = q^{\deg A}$$

y cumple

$$\mathcal{N}(A+B) = q^{\deg(A+B)} = q^{\deg A} q^{\deg B} = \mathcal{N}(A)\mathcal{N}(B)$$

- Notar que

$$Z_F(q^{-s}) = \sum_{n=0}^{\infty} A_n q^{-sn} = \sum_{A \in \mathcal{D}_F^+} (q^{\deg A})^{-s} = \sum_{A \in \mathcal{D}_F^+} \mathcal{N}(A)^{-s}$$

Definición

La función **zeta de Riemann para cuerpos de funciones** es

$$\zeta_F(s) := Z_F(q^{-s}) = \sum_{A \in \mathcal{D}_F^+} \mathcal{N}(A)^{-s}$$

y resulta un análogo de $\zeta(s)$.

4b. La Hipótesis de Riemann

Supongamos que $\zeta_F(s) = Z_F(q^{-s}) = 0$. Como

$$Z_F(t) = \frac{L_F(t)}{(1-t)(1-qt)}$$

entonces

$$Z_F(q^{-s}) = 0 \quad \Rightarrow \quad L_F(q^{-s}) = 0 \quad \Rightarrow \quad q^{-s} = \alpha_i^{-1}$$

$$\text{Hasse-Weil} \quad \Rightarrow \quad q^{-Re(s)} = |q^{-s}| = |\alpha_i^{-1}| = q^{-1/2}.$$

Luego,

$$\zeta_F(s) = 0 \quad \Rightarrow \quad Re(s) = \tfrac{1}{2}$$

o sea, vale la HR para cuerpos de funciones sobre cuerpos finitos.