LA COTA DE WEIL Y CURVAS CON MUCHOS PUNTOS RACIONALES

ADRIANA ALEXANDRA ALBARRACÍN MANTILLA

Universidad del Valle

Facultad de ciencias

Departamento de Matemáticas

Santiago de Cali

2006

LA COTA DE WEIL Y CURVAS CON MUCHOS PUNTOS RACIONALES

ADRIANA ALEXANDRA ALBARRACÍN MANTILLA

Trabajo de grado presentado como requisito parcial para optar al título de magister en matemáticas

ALVARO GARZÓN ROJAS, Doctor
Director

Universidad del Valle
Facultad de ciencias
Departamento de Matemáticas
Santiago de Cali
2006

Nota de Aceptación

Doctor Álvaro Garzón Rojas
Director

Doctor Roberto Ruíz Salguero
Jurado

Doctor Carlos Trujillo
Jurado

Santiago de Cali, FEBRERO de 2006

A mis padres Maria E. y Marco A., por su apoyo incondicional.

Agradecimientos

En primera instancia quiero agradecer a Dios por ser el motor de mi vida, al profesor Álvaro Garzón Rojas por haber aceptado dirigir este trabajo, por su tiempo, y dedicación y a todos los profesores del Departamento de matemáticas que me colaboraron durante la maestría.

ADRIANA ALEXANDRA ALBARRACÍN MANTILLA

Universidad del Valle
FEBRERO 2006

Tabla de Contenido

Resumen

En este trabajo se construyen curvas con "muchos"puntos racionales desde el punto de vista de la construcción de cubrimientos duplos del cuerpo de funciones racionales $F_q(x)$ vía extensiones de Kummer y Arthin-Schreier con "muchos"lugares de grado uno, entendiéndose por esto que el número de lugares de grado uno del cuerpo de funciones algebraicas está cercano a la cota de Weil. Para esto, se hace un estudio detallado de la cota de Weil desarrollado por Stichtenoth[1], con el objetivo de complementar y ejemplificar los principales resultados expuestos en ([12]-V).

[1] Ver[12]

Introducción

Sea $\mathbb{F}_q$ un cuerpo finito con $q = p^n$ elementos y $\overline{\mathbb{F}_q}$ la clausura algebraica de $\mathbb{F}_q$. Dado un polinomio $f(x, y) \in \mathbb{F}_q[x, y]$ irreducible sobre $\overline{\mathbb{F}_q}$, el conjunto:

$$C_f = \{(\alpha, \beta) \in \overline{\mathbb{F}_q} \times \overline{\mathbb{F}_q} : f(\alpha, \beta) = 0\}$$

es una curva algebraica afín (sobre el cuerpo finito $\mathbb{F}_q$) y los puntos $P = (\alpha, \beta) \in C_f$ tal que $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q$ se llaman puntos racionales de C_f sobre ${\mathbb{F}_q}^2$.

Durante muchos años la pregunta sobre cuántos puntos racionales puede tener una curva de género g mantuvo el interés de los matemáticos hasta que en 1940 Andre Weil [3] probó la hipótesis de Riemman para curvas sobre cuerpos finitos obteniendo, como consecuencia de este resultado una cota superior para el número de puntos racionales de una curva C de género g sobre un cuerpo finito de cardinalidad q, a saber:

$$|C(\mathbb{F}_q)| \leq q + 1 + 2g\sqrt{q},$$

donde $C(\mathbb{F}_q)$ denota el conjunto de puntos racionales de la curva C. El resultado de Weil se mantuvo intocable hasta que en 1980 Goppa [4] introdujo códigos asociados a curvas algebraicas conocidos como códigos geométricos de Goppa. En tal construcción se destacan dos propiedades que debe tener una curva de tal forma que el código inducido tenga buenos parámetros:

1 . La curva debe ser explícita, es decir debe obtenerse mediante una ecuación de la forma $f(x, y) = 0$.

2 . El número de puntos racionales de dicha curva debe estar cercano a la cota de Weil.

[2]Existe una correspondencia biunívoca entre las curvas algebraicas y los cuerpos de funciones algebraicas, esta correspondencia permite trasladar definiciones y resultados de curvas algebraicas a cuerpos de funciones algebraicas y vicerversa, Ver [1], [7].

[3]H. Stichtenoth, Ver [12].

[4]Goppa, Ver [6].

A partir de este hecho algunos matemáticos empezaron a trabajar en el mejoramiento de la cota de Weil y muchos otros encaminaron esfuerzos hacia la construcción de curvas con muchos puntos racionales.

En 1981 Ihara [5]mostró que si detonamos por N_q el máximo número de puntos racionales que una curva C de género g puede tener, entonces

$$N_q \leq q + 1 + \left[\frac{\left(\sqrt{(8q+1)^2 g + 4(q^2 - q)g} - g \right)}{2} \right]$$

donde $[x]$ es la parte entera de $x \in \mathbb{R}$. La importancia de este resultado radica en el hecho de que para curvas cuyo género satisface $g > \frac{q-\sqrt{q}}{2}$ esta cota es mejor que la cota de Weil. Posteriormente en 1993 Serre [6] mostró que la cota de Weil puede mejorarse:

$$N_q \leq q + 1 + 2[g\sqrt{q}].$$

En cuanto a la construcción explícita de curvas se han diseñado diferentes métodos que conducen a obtener "buenas curvas"(curvas con muchos puntos racionales), la mayoría de ellas vía extensiones de Kummer o extensiones de Artin-Schreier de $\mathbb{F}_q(x)$.

Este trabajo consta de tres capítulos, en el primer capítulo se hace un breve recorrido por los conceptos básicos de la teoría de Cuerpos Finitos ilustrados con algunos ejemplos para una mejor comprensión de los capítulos siguientes. El segundo capítulo es una revisión bibliográfica acerca de la Cota de Weil y sus diferentes mejoramientos (Cota de Serre, Cota de Ihara y Cota de Drinfeld Vladut) con aportes en cuanto a ejemplos y aclaraciones en algunas pruebas y en el tercer capítulo se construyen curvas (cuerpos de funciones algebraicas) con muchos puntos racionales (lugares de grado uno) entendiendo por esto, que el número $N(F/\mathbb{F}_q)$ de puntos racionales satisface $a \leq N(F/\mathbb{F}_q) \leq b$, donde b es la cota de Weil, Ihara o Serre para un cuerpo de funciones de género g y $a = b/\sqrt{2}$. Dichas curvas se obtienen por medio de cubrimientos duplos de la recta proyectiva $\mathbb{F}_q(x)$ vía extensiones de Kummer y Artin-Schreier, es decir torres de cuerpos de funciones del tipo $\mathbb{F}_q(x) \subset \mathbb{F}_q(x,y) \subset \mathbb{F}_q(x,y,z)$ donde la extensión $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ es una extensión de Kummer y $\mathbb{F}_q(x,y,z)/\mathbb{F}_q(x,y)$ una extensión de Artin-Schreier.

[5]Ihara, Ver [8].
[6]Serre, Ver [11].

Capítulo 1

Preliminares

El objetivo de este capítulo es hacer una presentación de las definiciones y resultados de la teoría de cuerpos de funciones algebraicas, esenciales para la comprensión de los capítulos siguientes. Todos ellos se presentan sin pruebas puesto que aparecen en [12] y algunas proposiciones se ilustran con ejemplos.

1.1. Anillos de valuación, lugares, ceros y polos

Sea F/K un cuerpo de funciones algebraicas sobre K, es decir $F \supseteq K$ es una extensión finita de $K(x)$, con $x \in F$ trascendente sobre K.

Se dice que $O \subseteq F$ es un *Anillo de Valuación* de F/K si:

i) $K \subsetneq O \subsetneq F$.

ii) Para cualquier $z \in F$, $z \in O$ ó $z^{-1} \in O$.

Puede probarse que todo anillo de valuación O es un *Anillo de Valuación Discreta*, es decir, un anillo de ideales principales con un único ideal máximal $P := O - O^*$. Puesto que P es principal, entonces existe un $t \in O$ el cual llamaremos *uniformizante local* para P tal que $P = tO$ y cada $0 \neq z \in F$ tiene una única expresión de la forma $z = t^n u$ con $u \in O^*$ y $n \in \mathbb{Z}$.

Si denotamos por F_P al cuerpo residual O/P, entonces existe una aplicación

$$\begin{array}{rcl} F & \longrightarrow & O/P := F_P \\ x & \longmapsto & \begin{cases} x(P) = x + P, & \text{si } x \in O \\ \infty, & \text{si } x \notin O \end{cases} \end{array}$$

Decimos que P es un *lugar de* F/K, si P es el ideal máximal de algún anillo de valuación de F/K. Denotaremos por $\mathbb{P}_F$ al conjunto de lugares del cuerpo de funciones F/K y ν_P la valuación discreta de F/K asociada al lugar P definida como $\nu_P(z) = n$, *si* $z = t^n \cdot u$. Si $z \in F$ y $P \in \mathbb{P}_F$, decimos que P es un *cero* de z si y sólo si $\nu_P(z) > 0$; P es un *polo* de z si y sólo si $\nu_P(z) < 0$. Si $\nu_P(z) = m > 0$, P es un cero de z de orden m; si $\nu_P(z) = -m < 0$, P es un polo de z de orden m.

1.2. El cuerpo de funciones racionales

El ejemplo clásico de cuerpo de funciones algebraicas es el cuerpo de funciones racionales. Todos los conceptos de anillos de valuación, lugares, ceros y polos de la sección anterior que se utilizarán a lo largo de este trabajo se pueden precisar en este cuerpo de funciones.

Definición 1.1 *Sea F/K un cuerpo de funciones algebraicas, decimos que F/K es un cuerpo de funciones racionales si existe $x \in F$ trascendente sobre K tal que $F = K(x)$.*

Notemos que de acuerdo a la definición, cada $z \in F - \{0\}$ tiene representación única en la forma

$$z = a \prod_i p_i(x)^{n_i}, \tag{1.1}$$

donde $a \in K - \{0\}$, los $p_i(x) \in K[x]$ son mónicos e irreducibles y cada $n_i \in \mathbb{Z}$.
Dado un polinomio mónico irreducible $p(x) \in K[x]$, entonces el conjunto

$$O_{p(x)} := \left\{ \frac{f(x)}{g(x)} : \ f(x), g(x) \in K[x] \ \text{ y } p(x) \nmid g(x) \right\}, \tag{1.2}$$

es un anillo de valuación de $K(x)/K$. En este caso su ideal máximal viene dado por

$$P_{p(x)} := \left\{ \frac{f(x)}{g(x)} : \ f(x), g(x) \in K[x] \ \text{ y } p(x) \mid f(x) \ \text{ y } \ p(x) \nmid g(x) \right\}. \tag{1.3}$$

En el caso particular de $p(x) = x - \alpha$ con $\alpha \in K$ escribimos $P_{x-\alpha} := P_\alpha$.
Otro anillo de valuación de $K(x)/K$ es el conjunto

$$O_\infty := \left\{ \frac{f(x)}{g(x)} : \ f(x), g(x) \in K[x] \ \text{ y } grad(f(x)) \leq grad(g(x)) \right\}, \tag{1.4}$$

cuyo ideal máximal es

$$P_\infty := \left\{ \frac{f(x)}{g(x)} : \ f(x), g(x) \in K[x] \ \text{ y } grad(f(x)) < grad(g(x)) \right\}, \tag{1.5}$$

el cual se llama el *lugar infinito de* $K(x)$.

Teorema 1.1 *Sea* $F = K(x)$ *el cuerpo de funciones racionales sobre* K.

i) *Si* $P = P_{p(x)}$ *es el lugar definido en (1.3), donde* $p(x) \in K[x]$ *es un polinomio mónico irreducible, entonces* $p(x)$ *es un uniformizante local para* P *y la correspondiente valuación discreta* ν_P *puede ser descrita en la siguiente forma. Si* $z \in F - \{0\}$ *tenemos que* z *admite la escritura* $z = p(x)^n \dfrac{f(x)}{g(x)}$, *donde* $p(x) \nmid f(x), p(x) \nmid g(x)$ *y* $n \in \mathbb{Z}$, *entonces* $\nu_P(z) := n$. *El cuerpo de clases residuales* $F_P = O_P/P$ *es isomorfo al cuerpo* $K[x]/(p(x))$ *y en consecuencia,* $grad(P) = grad(p(x))$.

ii) *En el caso especial* $p(x) = x - \alpha$, *con* $\alpha \in K$, *el grado de* P_α *es uno y la aplicación de clases residuales se dá en la siguiente forma, para* $z \in F : z(P_\alpha) = z(\alpha)$, *donde* $z(\alpha)$ *se define como sigue. Si* $z = \dfrac{f(x)}{g(x)}$, *donde* $f(x), g(x)$ *son polinomios en* $K[x]$ *primos relativos entre sí, entonces*

$$z(\alpha) = \begin{cases} \dfrac{f(\alpha)}{g(\alpha)}, & si\ g(\alpha) \neq 0, \\ \\ \infty, & si\ g(\alpha) = 0\ . \end{cases}$$

iii) *Sea* P_∞ *el lugar definido en (1.5), entonces* $grad(P_\infty) = 1$ *y un uniformizante local de* P_∞ *es* $t = \dfrac{1}{x}$. *La correspondiente valuación discreta es dada por*

$$\nu_{p_\infty}\left(\frac{f(x)}{g(x)}\right) = grad(g(x)) - grad(f(x)),$$

donde $f(x), g(x) \in K[x]$.

iv) K *es el cuerpo de constantes de* $K(x)/K$.

v) *Los únicos lugares de* $K(x)/K$ *son* P_∞ *y* $P_{p(x)}$ *definidos en (1.3) y (1.5), por lo tanto los lugares de grado uno de* $K(x)/K$ *están en correspondencia uno a uno con* $K \cup \{\infty\}$.

1.3. Divisores

A partir de esta sección F/K denotará un cuerpo de funciones algebraicas de una variable tal que K es el cuerpo de constantes de F/K.

La suma formal

$$D = \sum_{P \in \mathbb{P}_F} n_P(D)P,$$

con $n_P \in \mathbb{Z}$ y $n_P = 0$, para casi todo $P \in \mathbb{P}_F$ se llama *un divisor de* F/K.

El soporte de D está definido por :

$$Sop(D) := \{P \in \mathbb{P}_F, n_P(D) \neq 0\},$$

así

$$D = \sum_{P \in Sop(D)} n_P(D)P.$$

Un divisor de la forma $D = P$ con $P \in \mathbb{P}_F$, se llama *divisor primo.*

Un divisor $D = \sum_{P \in \mathbb{P}_F} \nu_P(D) \cdot P$, se dice *positivo* si todo $\nu_P(D) \geq 0$ y se escribe $D \geq 0$, así un divisor positivo es la suma de divisores primos.

Dados dos divisores $D = \sum_{P \in \mathbb{P}_F} n_P(D)P$ y $E = \sum_{P \in \mathbb{P}_F} n_P(E)P$, definimos el divisor suma de la siguiente forma

$$D + E = \sum_{P \in \mathbb{P}_F} (n_P(D) + n_P(E)) \cdot P.$$

Es fácil verificar que el conjunto de divisores con la suma definida anteriormente forma un grupo abeliano el cual denotaremos por $\mathcal{D}_F$.

El *cero* en $\mathcal{D}_F$ es $0 := \sum_{P \in \mathbb{P}_F} n_P \cdot P$, con $n_P = 0$, para cada $P \in \mathbb{P}_F$.

Para un divisor D y $Q \in \mathbb{P}_F$ se define $\nu_Q(D) := n_Q$.

Se define el grado de $P \in \mathbb{P}_F$ como $grad(P) = [F_P : K]$. La aplicación

$$grad : \mathcal{D}_F \longrightarrow \mathbb{Z},$$

define un homomorfismo de grupos con

$$grad(D) = \sum_{P \in \mathbb{P}_F} \nu_P(D) \cdot grad(P).$$

Si $0 \neq x \in F$ definimos el *Divisor Cero de* x como

$$(x)_0 := \sum_{P \in Z} (\nu_P(x))P,$$

donde Z denota el conjunto de ceros de x en $\mathbb{P}_F$ y el *Divisor Polar de x* como

$$(x)_\infty := \sum_{P \in N} -(\nu_P(x))P,$$

donde N el conjunto de polos de x en $\mathbb{P}_F$. A cada elemento no nulo x de F/K le asociamos un divisor el cual llamaremos el *Divisor Principal de x* dado por

$$(x) := (x)_0 - (x)_\infty.$$

En otras palabras $(x) := \sum_{P \in \mathbb{P}_F} (\nu_P(x))P$.

Cualquier divisor principal tiene grado cero. Además si $x \in F \setminus K$ entonces

$$grad(x)_0 = grad(x)_\infty = [F : K(x)].$$

Sea $\mathcal{P}_F := \{(x) | 0 \neq x \in F\}$ el grupo de divisores principales de F/K. Claramente este conjunto es un subgrupo de $\mathcal{D}_F$. Observe que para $0 \neq x \in F$, entonces $(xy) = (x)+(y)$.

Llamaremos *Grupo de Clase de Divisores* al grupo cociente $C_F := \mathcal{D}_F/\mathcal{P}_F$, y diremos que los divisores D_1 y $D_2 \in \mathcal{D}_F$ son equivalentes ($D_1 \sim D_2$), si $D_1 = D_2 + (x)$ para algún $x \in F \setminus 0$.

La clase de $A \in \mathcal{D}_F$ en C_F es denotado por $[A]$ y $grad([A]) := grad(A)$.

Para un divisor $A \in \mathcal{D}_F$, se define $\mathcal{L}(A) := \{x \in F | (x) \geq -A\} \cup \{0\}$. Observemos que si $A \in \mathcal{D}_F$ se tiene que:

i) $x \in \mathcal{L}(A)$ si y sólo si $\nu_P(x) \geq -\nu_P(A)$ para todo $P \in \mathbb{P}_F$.

ii) $\mathcal{L}(A) \neq \{0\}$ si y sólo si existe un divisor $A' \sim A$ con $A' \geq 0$.

Lema 1.1 *Si $A \in \mathcal{D}_F$ entonces*

i) $\mathcal{L}(A)$ es un espacio vectorial sobre K.

ii) $\mathcal{L}(0) = K$.

iii) Si $A < 0$ entonces $\mathcal{L}(A) = \{0\}$.

Se define ahora *la dimensión* del divisor A como $dim(A) := dim(\mathcal{L}(A))$.

Corolario 1.1 *i) Sean A, A' divisores tales que $A \sim A'$. Entonces*

$$dim(A) = dim(A') \text{ y } grad(A) = grad(A').$$

ii) Si $grad(A) < 0$ *entonces* $dim(A) = 0$.

iii) Para cualquier divisor A *de grado cero, las siguientes afirmaciones son equivalentes:*

a) A *es principal.*

b) $dim(A) \geq 1$.

c) $dim(A) = 1$.

Definición 1.2 *El género de* F/K *está definido por*

$$g := máx\{grad(A) - dim(A) + 1 \mid A \in \mathcal{D}_F\}.$$

El género de F/K *es un entero no negativo.*

Un *Adele* de F/K es una función $\alpha : \begin{cases} \mathbb{P}_F & \longrightarrow F, \\ P & \longmapsto \alpha_P, \end{cases}$
tal que $\alpha_P \in O_P$ para casi todo $P \in \mathbb{P}_F$. Un adele es como un elemento del producto directo $\prod_{P \in \mathbb{P}_F} F$ y además se usa la notación $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$.
El conjunto $\mathcal{A}_F := \{\alpha | \alpha$ es un adele de $F/K\}$, se llama *el espacio adele* de F/K y se considera como un espacio vectorial sobre K. *El adele principal* de un elemento $x \in F$ es el adele constante y de valor x. Para un divisor $A \in \mathcal{D}_F$ se define

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F | \nu_P(\alpha) \geq -\nu_P(A) \text{ para todo } P \in \mathbb{P}_F\},$$

con $\nu_P(\alpha) := \nu_P(\alpha_P)$.
Un diferencial de Weil de F/K es una aplicación K-lineal

$$\omega : \mathcal{A}_F \longrightarrow K$$

tal que ω se anula sobre $\mathcal{A}_F(A) + F$ para algún divisor $A \in \mathcal{D}_F$. *El módulo* de los diferenciales de Weil de F/K se define por

$$\Omega_F := \{\omega | \omega \text{ es un diferencial de Weil de } F/K\}.$$

Para un divisor $A \in \mathcal{D}_F$, $\Omega_F(A) := \{\omega \in \Omega_F | \omega$ se anula en $\mathcal{A}_F(A) + F\}$.

Definición 1.3 *i) El divisor* (ω) *de un diferencial de Weil* $w \neq 0$*, es un divisor unívocamente determinado por las siguientes condiciones:*

a) ω *se anula en* $\mathcal{A}_F((\omega)) + F$.

b) Si ω se anula en $\mathcal{A}_F(A) + F$ con $A \in \mathcal{D}_F$ entonces $A \leq (\omega)$.

ii) Para $0 \neq \omega \in \Omega_F$ y $P \in \mathbb{P}_F$ definimos $\nu_P(\omega) := \nu_P((\omega))$.

iii) Se dice que un lugar P es un cero (polo) de ω, si $\nu_P(\omega) > 0$ ($\nu_P(\omega) < 0$).

iv) Un divisor W se llama un divisor canónico de F/K si $W = (\omega)$ para algún $\omega \in \Omega_F$.

El siguiente teorema es uno de los teoremas más importantes en la teoría de Cuerpos de Funciones Algebraicas.

Teorema 1.2 *(Teorema de Riemann-Roch): Sea W un divisor canónico de F/K, entonces, para cualquier $A \in \mathcal{D}_F$,*

$$dim(A) = grad(A) + 1 - g + dim(W - A).$$

1.4. Extensiones de Cuerpos de Funciones Algebraicas

Sea F/K un cuerpo de funciones algebraicas en una variable con cuerpo de constantes K. A lo largo de este trabajo supondremos que el cuerpo K es perfecto.

Definición 1.4 *i) Un cuerpo de funciones algebraicas F'/K' es una extensión algebraica de F/K, si $F' \supset F$ es una extensión algebraica de cuerpos y $K' \supset K$.*

ii) Una extensión algebraica F'/K' de F/K se llama extensión por constantes si $F' = FK'$ es el cuerpo composición de F y K'.

iii) Una extensión algebraica F'/K' de F/K es una extensión finita si

$$[F' : F] < \infty.$$

Definición 1.5 *Sea F'/K' una extensión algebraica de F/K. Se dice que un lugar $P' \in \mathbb{P}_{F'}$ cae sobre $P \in \mathbb{P}_F$ si $P \subseteq P'$. También decimos que P' es una extensión de P, y escribimos $P'|P$.*

Proposición 1.1 *Sea F'/K' una extensión algebraica de F/K. Supongamos que P (P') es un lugar de F/K (F'/K'), y sea $O_P \subseteq F$ ($O_{P'} \subseteq F'$) el correspondiente anillo de valuación. Entonces las siguientes afirmaciones son equivalentes:*

i) $P'|P$.

ii) $O_P \subseteq O_{P'}$.

iii) *Existe un entero* $e \geq 1$ *tal que* $\nu_{P'}(x) = e \cdot \nu_P(x)$ *para todo* $x \in F$. *Más aún, si* $P'|P$ *entonces* $P = P' \cap F$ *y* $O_P = O_{P'} \cap F$.

Por esta razón, P *se llama la restricción de* P' *a* F.

Definición 1.6 *Sea* F'/K' *una extensión algebraica de* F/K *y sea* $P' \in \mathbb{P}_{F'}$ *un lugar de* F'/K' *que cae sobre* $P \in \mathbb{P}_F$.

i) *El entero* $e(P'|P) := e$ *con* $\nu_{P'}(x) = e \cdot \nu_P(x)$ *para cualquier* $x \in F$ *se llama índice de ramificación de* P' *sobre* P.

Decimos que $P'|P$ *es ramificado si* $e(P'|P) > 1$, *y* $P'|P$ *es no ramificado si* $e(P'|P) = 1$.

ii) $f(P'|P) := [F'_{P'} : F_P]$ *se llama el grado relativo de* P' *sobre* P.

Note que $f(P'|P)$ *puede ser finito o infinito; sin embargo el índice de ramificación siempre es un número natural.*

En particular si $[F' : F] < \infty, P \in \mathbb{P}_F$ *y* $P_1, P_2, ..., P_m \in \mathbb{P}_{F'}$ *son todos los lugares de* F'/K' *que caen sobre* P *entonces* $[F' : F] = \sum_{i=1}^{m} e(P_i|P) \cdot f(P_i|P)$.

Definición 1.7 *Sea* F'/F *una extensión finita y separable del cuerpo de funciones, entonces el diferente de* F'/F, *denotado por* $\mathcal{D}(F'/F)$, *es el divisor de* F' *dado por*

$$\mathcal{D}(F'/F) = \sum_{P \in \mathbb{P}(F)} \sum_{P'|P} d(P'|P)P'.$$

Proposición 1.2 *(Fórmula de Hurwitz):*

Sea F/K *un cuerpo de funciones algebraicas de género* g *y* F'/F *una extensión finita separable. Sea* K' *el cuerpo de constantes de* F' *y sea* g' *el género de* F'/K'. *Entonces tenemos que:*

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + grad((D(F'/F))).$$

Puesto que uno de los objetivos de este trabajo es el de construir cuerpos de funciones cuyo número de lugares de grado uno, sea "grande", es necesario obtener un mecanismo que nos ayude a calcular este número, el siguiente resultado nos proporciona una técnica para acercarnos a dicho valor.

Proposición 1.3 *Sea* $\varphi(T) = T^n + f_{n-1}(x)T^{n-1} + ... + f_0(x) \in K(x)[T]$ *un polinomio irreducible sobre el cuerpo de funciones racionales* $K(x)$.

Consideremos el cuerpo de funciones $K(x,y)/K$ donde y satisface la ecuación $\varphi(y)=0$ y un elemento $\alpha \in K$ tal que $f_j(\alpha) \neq \infty$ para cualquier $0 \leq j \leq n-1$. Denotemos por $P_\alpha \in \mathbb{P}_{K(x)}$ el cero de $x-\alpha$ en $K(x)$. Supongamos que el polinomio

$$\varphi_\alpha(T) := T^n + f_{n-1}(\alpha)T^{n-1} + ... + f_0(\alpha) \in K[T],$$

se descompone en el anillo de polinomios $K[T]$ de la siguiente forma:

$$\varphi_\alpha(T) = \prod_{i=1}^{r} \psi_i(T),$$

donde $\psi_i(T) \in K[T]$ corresponden a polinomios irreducibles, mónicos y distintos. Entonces tenemos que:

i) Para cualquier $i = 1, ..., r$ existe un único lugar determinado por el lugar $P_i \in \mathbb{P}_{K(x,y)}$ tal que $x-\alpha \in P_i$ y $\psi_i(y) \in P_i$. Además $e(P_i|P_\alpha) = 1$ y el cuerpo de clase residual de P_i es isomorfo a $K[T]/(\psi_i(T))$.

De aquí $f(P_i|P_\alpha) = grad(\psi_i(T))$.

ii) Si $grad(\psi_i(T)) = 1$ a lo más para $i \in 1, ..., r$, entonces K es el cuerpo de constantes de $K(x,y)$.

iii) Si $\varphi_\alpha(T)$ tiene n raíces distintas en K, donde $n = grad(\varphi(T))$, entonces existe para cualquier β con $\varphi_\alpha(\beta) = 0$ un único lugar $P_{\alpha,\beta} \in \mathbb{P}_{K(x,y)}$, tal que $x-\alpha \in P_{\alpha,\beta}$ y, $y-\beta \in P_{\alpha,\beta}$. $P_{\alpha,\beta}$ es un lugar de $K(x,y)$ de grado 1.

Como una ilustración del anterior resultado tenemos

Ejemplo 1.1 Sean $\varphi(T) = T^2 + T + x^3 + x \in \mathbb{F}_2(x)[T]$ y $E = \mathbb{F}_2(x,y)$ con $\varphi(y) = 0$. Observe que en este caso $f_1(x) = 1$ y $f_0(x) = x^3 + x$, además para cada $\alpha \in \mathbb{F}_2$ se tiene que $f_1(\alpha) = 1$ y $f_0(\alpha) = 0$.

De otro lado, los polinomios $\varphi_0(T) = \varphi_1(T) = T^2 + T \in \mathbb{F}_2[T]$ se factorizan como $\varphi_0(T) = \varphi_1(T) = T(T+1)$ con T y $T+1$ polinomios irreducibles sobre $\mathbb{F}_2[T]$.

Ahora, para cada $\alpha \in \mathbb{F}_2$, el polinomio $\varphi_\alpha(T) = T^2 + T$ tiene $2 = grad(\varphi(T))$ raices distintas (en $\mathbb{F}_2$), luego por cada β que satisfaga $\varphi_\alpha(\beta) = 0$ tenemos un lugar de grado uno en E a saber $P_{(\alpha,\beta)}$; es decir, tenemos además de P_∞ (el polo de x), 4 lugares de grado uno que simbolizaremos por $P_{(0,0)}$,$P_{(0,1)}$,$P_{(1,0)}$ y $P_{(1,1)}$. □

Observación 1.1 i) El ejemplo anterior es un caso muy particular de la Proposición 1.3. De hecho los ejemplos que consideraremos en este trabajo serán dados por polinomios $\varphi(T) = T^n + f_{n-1}(x)T^{n-1} + ... + f_0(x) \in K(x)[T]$ para los cuales $f_j(x) = 0$, para $1 \leq j \leq n-1$, este hecho se justificará a lo largo del trabajo.

ii) Los lugares racionales que hemos " contado.[en] este ejemplo corresponden a los llamados "Puntos de Rama", es decir son aquellos lugares obtenidos después de analizar el conjunto de ceros y polos de la función racional $f_0(x) = x^3 + x$. Posteriormente precisaremos cómo calcular el número exacto de lugares de grado uno.

Hasta el momento hemos presentado resultados que nos permiten, por un lado, calcular el género de un cuerpo de funciones (Fórmula de Hurwitz) y por otro, un acercamiento al número de lugares de grado uno (Proposición 1.3). No obstante, debe observarse que la fórmula de Hurwitz requiere del cálculo del diferente de la extensión en consideración. Afortunadamente y aún cuando en general este cálculo es muy díficil, los dos teoremas siguientes indican como calcularlo en un tipo particular de extensiones.

Proposición 1.4 *(Extensiones de Kummer). Sea F/K un cuerpo de funciones algebraicas, ζ una raíz r-ésima primitiva de la unidad contenida en K (con $r > 1$ y r primo relativo con la característica de K) y $u \in F$ que satisface:*

$$u \neq w^d, \quad \forall w \in F \quad y\ d|r, \qquad d > 1.$$

La extensión

$$F' = F(y) \ con \ \ y^r = u,$$

se llama una extensión de Kummer de F, y tiene las siguientes propiedades:

i) El polinomio $\phi(T) = T^r - u$, es el polinomio minimal de y sobre F (en particular éste es irreducible sobre F.) F'/F es una extensión de Galois de grado r, cuyo grupo de Galois es cíclico y todos los automorfismos de F'/F están dados por $\sigma(y) = \zeta y$, donde $\zeta \in K$ es una raíz r-ésima de la unidad.

ii) Sea $P \in \mathbb{P}_F$ y sea $P' \in \mathbb{P}_{F'}$ una extensión de P. Entonces

$$e(P'|P) = \frac{r}{m_P} \quad y\ d(P'|P) = \frac{r}{m_P} - 1,$$

donde

$$m_P := mcd(r, \nu_P(u)) > 0,$$

iii) Si K' denota el cuerpo de constantes de F', g y g' denotan el género de F/K y F'/K' respectivamente, entonces:

$$g' = 1 + \frac{r}{[K' : K]} \left(g - 1 + \frac{1}{2} \sum_{P \in \mathbb{P}_F} \left(1 - \frac{m_P}{r}\right) grad(P) \right).$$

Ejemplo 1.2 Sea $F = \mathbb{F}_{25}(x)$ el cuerpo de funciones racionales y

$$\mu(x) := \frac{x^5(x+1)^5}{(x+3)(x^2+2x+3)^4} \in F = \mathbb{F}_{25}(x).$$

Tomando $r = 12$, afirmamos que μ no es una d-ésima potencia para cualquier divisor d de 12. Definamos $F' = \mathbb{F}_{25}(x, y)$ dado por la ecuación de Kummer

$$y^{12} = \frac{x^5(x+1)^5}{(x+3)(x^2+2x+3)^4} = \mu(x).$$

Observe que los únicos lugares $P \in \mathbb{P}_F$ que pertenecen al soporte de (μ) son

$$P_0, P_{-1}, P_{-3}, P_\infty, P_{\zeta_1} \text{ y } P_{\zeta_2},$$

con $\zeta_i^2 + 2\zeta + 3 = 0$. A manera de ilustración analizaremos la ramificación de P_0, P_∞ y P_{ζ_1}.

$$m_{P_0} = 1, \quad e(P_0'|P_0) = \frac{12}{1} = 12 \quad \text{y } d(P_0'|P_0) = \frac{12}{1} - 1 = 11.$$

$$m_{P_\infty} = 1, \quad e(P_\infty'|P_\infty) = \frac{12}{1} = 12 \quad \text{y } d(P_\infty'|P_\infty) = \frac{12}{1} - 1 = 11.$$

$$m_{P_{\zeta_1}} = 4, \quad e(P_{\zeta_1}'|P_{\zeta_1}) = \frac{12}{4} = 3 \quad \text{y } d(P_{\zeta_1}'|P_{\zeta_1}) = \frac{12}{4} - 1 = 2.$$

en consecuencia los lugares P_0, P_{-1}, P_{-3} y P_∞ son totalmente ramificados, mientras que P_{ζ_1} y P_{ζ_2} son débilmente ramificados en $F'/\mathbb{F}_{25}$.

Finalmente, para calcular el género del cuerpo de funciones $F'/\mathbb{F}_{25}$ usamos la parte c) del teorema y obtenemos

$$g' = \ 1 + 12\left(-1 + \tfrac{1}{2}\left(4\left(\tfrac{11}{12}\right) + 2\left(\tfrac{2}{3}\right)\right)\right) = 19. \square$$

Proposición 1.5 *(Extensiones de Artin-Schreier).*

Sea F/K un cuerpo de funciones algebraicas de característica $p > 0$. Supongamos que $u \in F$ es un elemento que satisface la siguiente condición:

$$u \neq w^p - w, \ \forall \ w \in F.$$

Sea

$$F' = F(y) \text{ con } y^p - y = u,$$

de F. Para $P \in P_F$ se define el entero m_P así:

$$m_P := \begin{cases} m, & \text{si existe } z \in F \text{ tal que } \nu_P(u - (z^p - z) = -m < 0 \text{ y } m \equiv 0 \bmod p, \\ -1, & \text{si } \nu_P(u - (z^p - z)) \geq 0 \text{ para algún } z \in F. \end{cases}$$

Entonces tenemos que:

i) *F'/F es una extensión cíclica de Galois de grado p. Los automorfismos de F'/F son dados por $\sigma(y) = y + \zeta$, con $\zeta \in F_p$.*

ii) *P es no ramificado en F'/F si y solo si $m_P = -1$.*

iii) *P es totalmente ramificado en F'/F si y solo si $m_P > 0$. Se denota por P' el único lugar de F' que cae sobre P. Entonces el exponente diferente $d(P'|P)$ está dado por*

$$d(P'|P) = (p-1)(m_P + 1).$$

iv) *Si al menos un lugar $Q \in \mathbb{P}_F$ satisface $m_Q > 0$, entonces K es algebraicamente cerrado en F', y*

$$g' = p \cdot g + \frac{p-1}{2}\left(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) grad(P)\right), \tag{1.6}$$

donde g y g' son los géneros de F/K y F'/K' respectivamente.

Observación 1.2 Debe notarse que de acuerdo con la definición de m_P (cuya existencia esta garantizada por ([12]-III.7.7)) y del exponente diferente, en este tipo de extensiones solamente ocurre ramificación total, lo cual hace que el género se vea altamente afectado cuando un lugar se ramifica. Por lo tanto para construir cuerpos de funciones con un género pequeño el conjunto de polos del divisor (u) así como sus órdenes deben ser pequeños.

Ejemplo 1.3 Sea E el cuerpo de funciones definido en el ejemplo 1.1. En este caso $u = x^3 + x$ y no es difícil probar que $f(T) = T^2 + T - u$ no tiene ceros en $\mathbb{F}_{25}(x)$. Observe que los únicos lugares $P \in \mathbb{P}_F$ que pertenecen al soporte de (u) son P_0, P_1 y P_∞. Además tomando $z = 0$ tenemos que

$$\nu_{P_0}(u(x)) > 0, \nu_{P_1}(u(x)) > 0 \text{ y } \nu_{P_\infty}(u(x)) < 0.$$

es decir, P_∞ es totalmente ramificado mientras los lugares P_0 y P_1 no se ramifican en $F'/\mathbb{F}_2$. Finalmente, para calcular el género del cuerpo de funciones $F'/\mathbb{F}_2$ utilizamos (1.6) y obtenemos

$$g' = 2 \cdot 0 + \frac{1}{2}(-2 + (3+1)) = 1. \square$$

Resumiendo los ejemplos 1.1 y 1.3, tenemos que el cuerpo de funciones algebraicas E definido por la ecuación de Artin-Shreirer $y^2 + y = x^3 + x$ tiene género 1 y por lo menos 5 lugares de grado 1. Para este caso $(q, g) = (2, 1)$ la cota de Weil, Ihara y Serre es 5, es decir E tiene exactamente 5 lugares de grado 1 y es un ejemplo de un cuerpo de funciones sobre $\mathbb{F}_2$ de género 1 con el mayor número de lugares racionales que se puede obtener.

Capítulo 2

Función Zeta asociada a un Cuerpo de Funciones

En esta sección asociamos al cuerpo de funciones $F/\mathbb{F}_q$ una cierta función $Z(t)$ semejante a la función Zeta de Riemman en variable compleja:

$$\zeta(s) = \sum_{n=0}^{\infty} n^{-s}.$$

Es conocido que sobre la función Zeta se conjetura que si $\zeta(x) = 0$ entonces $Re(x) = 1/2$. Aún cuando no ha sido posible probar esta conjetura, veremos que, para el caso de nuestra función $Z(t)$ asociada al Cuerpo de Funciones $F/\mathbb{F}_q$, se tiene un resultado similar al de la conjetura de Riemman.
Este resultado obtenido por A.Weil, tiene como consecuencia un hecho trascendental en el estudio de los cuerpos de funciones algebraicas con cuerpo de constantes finito, como es el de establecer una cota superior para el número de lugares de grado 1. Esta cota, conocida como cota de Weil dependerá únicamente del género del cuerpo de funciones y de la cardinalidad del cuerpo de constantes.

Como en los Preliminares, en este capítulo $\mathcal{D}_F$ denota el grupo de divisores de $F/\mathbb{F}_q$ y $A \in D_F$ con $A \geq 0$ un divisor positivo.

Lema 2.1 *Para cualquier $n \geq 0$ existe sólo un número finito de divisores positivos de grado n.*

Demostración: Dado que un divisor positivo es la suma de divisores primos, es suficiente probar que el conjunto $S := \{P \in \mathbb{P}_F |\ grad(P) \leq n\} \neq \emptyset$ es finito.

Tomemos un $x \in F \setminus \mathbb{F}_q$ y consideremos el conjunto

$$S_0 = \{P_0 \in P_{\mathbb{F}_q(x)} |\ grad(P_0) \leq n\}.$$

Para cualquier $P \in S$ tenemos que $P \cap \mathbb{F}_{q(x)} \in S_0$ en efecto:

$$P \cap \mathbb{F}_q(x) = P_0 \text{ y } grad(P) = [\mathbb{F}_P : \mathbb{F}_q] = [\mathbb{F}_P : \mathbb{F}_{P_0}][\mathbb{F}_{P_0} : \mathbb{F}_q] \leq n,$$

entonces

$$grad(P_0) = [\mathbb{F}_{P_0} : \mathbb{F}_q] \leq n,$$

y en consecuencia $P_0 \in S_0$. Ahora bien, dado que para cualquier $P_0 \in S_0$ existe un número finito de extensiones en F, sólo debemos mostrar que S_0 es finito. La finitud de S_0 se tiene puesto que los lugares de $F_q(x)$ (excepto el polo de x) corresponden a polinomios mónicos e irreducibles $p(x) \in \mathbb{F}_q(x)$ de algún grado menor o igual a n. □

Definición 2.1 *Sea $F/\mathbb{F}_q$ un cuerpo de funciones algebraicas. Denotaremos por $\mathcal{D}_F^0 = \{A \in \mathcal{D}_F | grad(A) = 0\}$, al conjunto de divisores de grado cero, por C_F^0 al conjunto $\{[A] \in C_F | grad([A]) = 0\}$, al cual llamaremos el grupo clase de divisores de grado cero.*

Proposición 2.1 *C_F^0 es un grupo finito.*

Demostración: Sean $B \in \mathcal{D}_F$ con $grad(B) = n \geq g$ y

$$C_F^n = \{[C] \in C_F \ | grad[C] = n\}.$$

Consideremos la función

$$\varphi : C_F^0 \to C_F^n,$$

definida por

$$\varphi([A]) = [A + B],$$

afirmamos que φ es una biyección, en efecto:

$$[A + B] = [C + B] \Leftrightarrow [A] + [B] = [C] + [B] \Leftrightarrow [A] = [C].$$

De otro lado, sea $[C] \in C_F^n$ entonces el divisor

$$A := C - B,$$

satisface que $grad([A]) = 0$, de aquí $\varphi([A]) = [C]$. En consecuencia todas las clases de divisores de cualquier grado de $F/\mathbb{F}_q$ tienen el mismo cardinal h.

Ahora veamos que C_F^n es finito. Por el Teorema de Riemann-Roch, para todo $[C] \in C_F^n$ tenemos que

$$\delta[C] = n + 1 - g \geq 1,$$

entonces existe $A \in [C]$ con $A \geq 0$; es decir, cualquier clase de divisores de grado n tiene representante positivo. Además existe sólo un número finito de divisores positivos de grado n, lo cual implica que C_F^n es finito. □

El número $h := h_F := |C_F^0|$ es llamado el número de clase del Cuerpo de funciones algebraicas $F/\mathbb{F}_q$.

Definamos

$$\partial := min\{grad(A)|A \in \mathcal{D}_F \text{ y } grad(A) > 0\}.$$

La imagen de la función grado

$$grad : \mathcal{D}_F \to \mathbb{Z},$$

es un subgrupo de $\mathbb{Z}$ generado por ∂ y el grado de cualquier divisor de $F/\mathbb{F}_q$ es un múltiplo de ∂. Más adelante mostraremos que $\partial = 1$, es decir que la función $grad$ es un homomorfismo sobreyectivo.

En lo que sigue estudiaremos los números

$$A_n = |\{A \in \mathcal{D}_F \text{ tal que } A \geq 0 \text{ y } grad(A) = n\}|.$$

Por conveniencia $A_0 := 1$ y A_1 corresponde al número de lugares de grado 1.

Más aún observe que si $\partial \nmid n$ entonces $A_n = 0$ en efecto: Supongamos que existe $A \in \mathcal{D}_F$ con $grad(A) = n$ y puesto que $grad(A) \in \partial\mathbb{Z}$ entonces $\partial | n$, en consecuencia $A_n = 0$.

Lema 2.2 *i) Para una clase de divisores fija $[C] \in C_F$ se tiene*

$$|\{A \in [C] \ | A \geq 0\}| = \frac{1}{q-1}\left(q^{\delta[C]} - 1\right).$$

ii) Para cualquier $n > 2g - 2$ con $\partial | n$

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

Demostración:

i) Puesto que $A \in [C]$ entonces existe $0 \neq x \in F$ tal que $A = C + (x)$ y como $A \geq 0$ entonces $x \in \mathcal{L}(C) \setminus \{0\}$.

De otro lado $\delta([C]) := dim_{\mathbb{F}_q}\mathcal{L}(C)$, en consecuencia existen exactamente $q^{\delta[C]} - 1$ elementos no nulos en $\mathcal{L}(C)$ y dado que dos elementos de $\mathcal{L}(C) \setminus \{0\}$ tienen el mismo divisor si y sólo si difieren por una constante entonces

$$|\{A \in [C]; A \geq 0\}| = \frac{q^{\delta[C]} - 1}{q-1}.$$

ii) Dado que existen $h = h_F$ clases de divisores de grado n digamos: $[C_1], [C_2], ..., [C_h]$. entonces por parte i) y por Teorema de Riemman-Roch tenemos

$$|\{A \in [C_j] | A \geq 0\}| = \frac{1}{q-1}\left(q^{\delta[C_j]} - 1\right) = \frac{q^{n+1-g}-1}{q-1}, 1 \leq j \leq h$$

y puesto que cualquier divisor de grado n pertenece a una de las clases $[C_1], [C_2], ..., [C_h]$, entonces

$$A_n = \sum_{j=1}^{h} |\{A \in [C_j]; A \geq 0\}| = \frac{h}{q-1}\left(q^{n+1-g} - 1\right). \square$$

Definición 2.2 *La serie de potencias*

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

se llama la función Zeta de $F/\mathbb{F}_q$.

Si consideramos a t como una variable compleja, observemos que $Z(t)$ es una serie de potencias sobre el Cuerpo de los números complejos. Debemos mostrar ahora que esta serie de potencias converge en una vecindad de 0.

Proposición 2.2 *La serie de potencias* $Z(t) = \sum_{n=0}^{\infty} A_n t^n$ *es convergente para* $|t| < q^{-1}$. *Más precisamente para* $|t| < q^{-1}$ *tenemos:*

i) Si $F/\mathbb{F}_q$ *tiene género* $g = 0$ *entonces* $Z(t) = \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right)$.

ii) Si $g \geq 1$ *entonces* $Z(t) = F(t) + G(t)$ *con*

$$F(t) = \frac{1}{q-1} \sum_{0 \leq grad[C] \leq 2g-2} q^{\delta[C]} \cdot t^{grad[C]},$$

(donde $[C]$ *recorre todas las clases de divisores* $[C] \in C_F$ *con*

$$0 \leq grad([C]) \leq 2g-2).$$

y

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

Demostración: Ver ([12]-V.I.6).

Corolario 2.1 $Z(t)$ *puede extenderse a una función racional sobre* $\mathbb{C}$ *que tiene un polo simple en* $t = 1$.

Demostración: Observemos que en la proposición anterior $\dfrac{1}{1-t^{\partial}}$, es un término de $Z(t)$ y como $\dfrac{1}{1-t^{\partial}}$ tiene un polo simple en $t=1$ de orden ∂ entonces $Z(t)$ puede extenderse a una función racional sobre $\mathbb{C}$. $\square$

Al estudiar el comportamiento de la función Zeta de $F/\mathbb{F}_q$ bajo extensiones por constantes es conveniente tener una segunda representación de $Z(t)$ como un producto infinito.

Recordemos que un producto infinito $\prod_{i=1}^{\infty}(1+a_i)$ (con números complejos $a_i \neq -1$) es convergente con límite $a \in \mathbb{C}$, si $lim_{n\longrightarrow\infty}\prod_{i=1}^{n}(1+a_i) = a \neq 0$. Este producto es absolutamente convergente si $\sum_{i=1}^{\infty}|a_i| < \infty$. Es bien conocido que la convergencia absoluta implica la convergencia del producto y que el límite de un producto absolutamente convergente es independiente del orden de los factores.

Además, si el producto de $\prod_{i=1}^{\infty}(1+a_i) = a$ es absolutamente convergente, entonces $\prod_{i=1}^{\infty}(1+a_i)^{-1}$ también converge absolutamente y $\prod_{i=1}^{\infty}(1+a_i)^{-1} = a^{-1}$.

Proposición 2.3 *(Producto de Euler). Para $|t| < q^{-1}$, la función Zeta puede representarse como un producto absolutamente convergente*

$$Z(t) = \prod_{P\in\mathbb{P}_F}\left(1-t^{grad(P)}\right)^{-1}. \tag{2.1}$$

En paticular $Z(t) \neq 0$ para $|t| < q^{-1}$.

Demostración: Por la proposición 2.2, tenemos que $\sum A_n t^n < \infty$ para $|t| < q^{-1}$ y puesto que $\sum_{P\in\mathbb{P}_F}|t|^{grad(P)} \leq \sum_{n=0}^{\infty}A_n|t|^n$ entonces tenemos que $\prod_{P\in\mathbb{P}_F}(1-t^{grad(P)})^{-1}$ es absolutamente convergente. De otro lado cada factor de (2.1) lo podemos escribir como una serie geométrica y así obtenemos

$$\prod_{P\in\mathbb{P}_F}\left(1-t^{grad(P)}\right)^{-1} = \prod_{P\in\mathbb{P}_F}\sum_{n=0}^{\infty}t^{grad(nP)}$$

$$= \sum_{A\in D_F, A\geq 0}t^{grad(A)} = \sum_{n=0}^{\infty}A_n t^n = Z(t). \ \square$$

En lo que sigue, fijamos una clausura algebraica $\overline{\mathbb{F}}_q$ de $\mathbb{F}_q$ y consideramos la extensión por constantes $\overline{F} = F\overline{\mathbb{F}}_q$ de $F/\mathbb{F}_q$.

Para cualquier $r \geq 1$ existe exactamente una extensión $\mathbb{F}_{q^r}/\mathbb{F}_q$ de grado r con $\mathbb{F}_{q^r} \subseteq \overline{\mathbb{F}}_q$ y $F_r := F\mathbb{F}_{q^r} \subseteq \overline{F}$.

Lema 2.3 *i) F_r/F es una extensión ciclíca de grado r y $Gal(F_r/F)$ es generado por el automorfismo de Frobenius σ que actúa sobre $\mathbb{F}_{q^r}$ así: $\sigma(\alpha) = \alpha^q$.*

ii) $\mathbb{F}_{q^r}$ es el cuerpo de constantes de F_r.

iii) $F_r/\mathbb{F}_{q^r}$ tiene el mismo género de $F/\mathbb{F}_q$.

iv) Sea $P \in \mathbb{P}_F$,un lugar de grado m. Entonces

$$Con_{F_r/F}(P) = P_1 + P_2 + ... + P_d,$$

con $d = m.c.d(m, r), P_i \in \mathbb{P}_{F_r}$ y $grad(P_i) = m/d$.

Demostración:

i) Es conocido que la extensión $\mathbb{F}_{q^r}/\mathbb{F}_q$ es cíclica de grado r y que $Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$ es generado por la función de Frobenius $\alpha \to \alpha^q$.

Dado que $F_r/\mathbb{F}_{q^r}$ es una extensión por constantes de $F/\mathbb{F}_q$, se puede ver que $[F_r : F] = r = [\mathbb{F}_{q^r} : \mathbb{F}_q]$ por ([12]-III.6.3), así la afirmación (i) se tiene inmediatamente.

ii) y iii) se tienen por ([12]-III.6.1-III.6.3).

iv) P es no ramificado en F_r/F por ([12]-III.6.3). Consideremos $P' \in \mathbb{P}_{F_r}$ tal que $P'|P$. Por ([12]-III.6.3 (g)) el cuerpo de clase residual de P' es la composición de $\mathbb{F}_{q^r}$ con el cuerpo de clase residual F_P de P así:

$$F_{r_{P'}} = F_P \cdot \mathbb{F}_{q^r}.$$

Sea $l = m.c.m.(m, r)$, dado que $F_P = \mathbb{F}_{q^m}$, tal composición es:

$$\mathbb{F}_{q^l} = \mathbb{F}_{q^m} \cdot \mathbb{F}_{q^r},$$

y puesto que $l = \dfrac{m \cdot r}{d}$, entonces

$$grad(P') = [\mathbb{F}_{r_{P'}} : \mathbb{F}_{q^r}] = [\mathbb{F}_{q^l} : \mathbb{F}_{q^r}] = \frac{m}{d}.$$

De otro lado, por ([12]-III.6.3.(c)) tenemos que

$$grad(Con_{F_r/F}(P)) = grad(P) = m,$$

y dado que

$$grad(Con_{F_r/F}(P)) = \sum_{P' \in \mathbb{P}_{F_r}} e(P'|P) grad(P'),$$

entonces

$$Con_{F_r/F}(P)) = P_1 + P_2 + ... + P_d,$$

con lugares $P_i \in \mathbb{P}_{F_r}$ de grado $\dfrac{m}{d}$. □

La siguiente proposición relaciona la función Zeta de un cuerpo de funciones algebraicas $F/\mathbb{F}_q$ con la del cuerpo de funciones $F_r/\mathbb{F}_{q^r}$, para ello necesitamos el siguiente resultado.

Lema 2.4 *Si $m \geq 1$ y $r \geq 1$ son enteros y $d = m.c.d.(m, r)$, entonces*

$$(X^{r/d} - 1)^d = \prod_{\zeta^r=1} (X - \zeta^m), \tag{2.2}$$

Demostración: Ambos lados de (2.2) son polinomios mónicos del mismo grado, y cada raíz (r/d)-ésima de la unidad tiene multiplicidad d, en efecto, si $\zeta^r = 1$ entonces $\zeta = Exp\left(\frac{2\pi ik}{r}\right)$ para algún $k = 0, 1, 2, ..., r-1$, elevando a la m obtenemos que $\zeta^m = Exp\left(\frac{2\pi ikm}{r}\right), m \in \mathbb{Z}$, ahora dado que d divide a m existe $t \in \mathbb{Z}^+$ tal que $m = dt$ y al reemplazar tenemos que $\zeta^m = Exp\left(\frac{2\pi ikdt}{r}\right) = Exp\left(\frac{2\pi ikt}{\frac{r}{d}}\right)$, así que $\zeta^m = Exp\left(\frac{2\pi ik}{\frac{r}{d}}\right)^t$. Observe que cuando k recorre el conjunto $0, 1, ..., \frac{r}{d} - 1$, obtenemos las diferentes raices r-ésimas de la unidad, luego para $k = \frac{r}{d}$, tenemos que

$$Exp\left(\frac{2\pi ik}{\frac{r}{d}}\right)^t = 1,$$

a partir de este valor las raices se repiten, es decir cada $\frac{r}{d}$ enteros tenemos el conjunto de raices $\frac{r}{d}$-ésimas de 1 y puesto que hay d grupos, tendremos la igualdad polinomial deseada.

Ahora, si sustituimos $X = t^{-m}$ en (2.2) y multiplicamos por t^{mr}, tenemos

$$\begin{aligned}
(t^{-mr/d} - 1)^d \cdot (t^{mr/d})^d &= \left(\prod_{\zeta^r=1} (t^{-m} - \zeta^m)\right) \cdot (t^{mr}), \\
\left[\left(t^{-mr/d} - 1\right)\left(t^{mr/d}\right)\right]^d &= \prod_{\zeta^r=1} \left((t^{-m} - \zeta^m) \cdot (t^m)\right), \\
\left(1 - t^{mr/d}\right)^d &= \prod_{\zeta^r=1} \left(1 - (\zeta t)^m\right).
\end{aligned} \tag{2.3}$$

Proposición 2.4 *Sean $Z(t)$ y $Z_r(t)$ las funciones Zeta de F y F_r respectivamente, entonces*

$$Z_r(t^r) = \prod_{\zeta^r=1} Z(\zeta t), \tag{2.4}$$

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

Demostración: Es suficiente probar (2.4) para $|t| < q^{-1}$. En esta región la representación del producto de Euler nos conduce a:

$$Z_r(t^r) = \prod_{P\in\mathbb{P}_F} \prod_{P'|P} \left(1 - t^{r\cdot grad(P')}\right)^{-1}. \tag{2.5}$$

Para un lugar fijo $P \in \mathbb{P}_F$, definimos $m := grad(P)$ y $d := m.c.d.(m, r)$, entonces

$$\begin{aligned} \prod_{P'|P} \left(1 - t^{r\cdot grad(P')}\right) &= \left(1 - t^{m\cdot r/d}\right)^d, \\ = \prod_{\zeta^r=1} \left(1 - (\zeta t)^m\right) &= \prod_{\zeta^r=1} \left(1 - (\zeta t)^{grad(P)}\right), \end{aligned}$$

por (2.3) y Lema 2.3(d). Ahora de (2.5) obtenemos:

$$Z_r(t^r) = \prod_{\zeta^r=1} \prod_{P\in\mathbb{P}_F} \left(1 - (\zeta t)^{grad(P)}\right)^{-1} = \prod_{\zeta^r=1} Z(\zeta t).\square$$

Corolario 2.2 $\partial = 1$.

Demostración: Si $\zeta^\partial = 1$ entonces

$$\begin{aligned} Z(\zeta t) &= \prod_{P\in\mathbb{P}_F} (1 - (\zeta t)^{grad(P)})^{-1} \\ = \prod_{P\in\mathbb{P}_F} (1 - \zeta^{grad(P)} t^{grad(P)})^{-1} &= \prod_{P\in\mathbb{P}_F} (1 - \zeta^{\partial n} t^{grad(P)})^{-1} \\ = \prod_{P\in\mathbb{P}_F} (1 - t^{grad(P)})^{-1} &= Z(t), \end{aligned}$$

con $n \in \mathbb{Z}$ y para cualquier $P \in \mathbb{P}_F$.

Además por la Proposición 2.4 tenemos que

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

Puesto que $Z(t)$ tiene un polo simple en $t = 1$, podemos afirmar que $Z_\partial(t^\partial)$ tiene un polo simple en $t = 1$ y $Z(t)^\partial$ tiene un polo en $t = 1$ de orden ∂. En consecuencia $\partial = 1.\square$

Observe que el anterior resultado no establece que siempre existan lugares de grado 1, sólo que existen divisores de cualquier grado.

Corolario 2.3 *i) Cualquier cuerpo de funciones $F/\mathbb{F}_q$ de género 0 es racional, y su función Zeta es*

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

ii) Si $F/\mathbb{F}_q$ tiene género $g \geq 1$, su función $Z(t)$ puede escribirse en la forma

$$Z(t) = F(t) + G(t),$$

con

$$F(t) = \frac{1}{q-1} \sum_{0 \leq grad([C]) \leq 2g-2} q^{\delta[C]} \cdot t^{grad([C])}$$

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

Demostración: Puesto que un cuerpo de funciones de género 0, es racional si tiene un divisor de grado 1, ([12]-(I.6.3.)), entonces por proposición 2.2 y dado que $\partial = 1$ tenemos las afirmaciones a) y b). □

Proposición 2.5 *(Ecuación Funcional de la Función Zeta): La función Zeta de $F/\mathbb{F}_q$ satisface la ecuación funcional*

$$Z(t) = q^{g-1} t^{2g-2} Z(1/qt).$$

Demostración:

a) Para $g = 0$,

$$Z\left(\frac{1}{qt}\right) = \frac{1}{\left(1 - \frac{1}{qt}\right)\left(1 - q\frac{1}{qt}\right)} = \frac{q^2t^2}{(qt-1)(qt-q)}.$$

Entonces

$$q^{g-1}t^{2g-2} Z\left(\frac{1}{qt}\right) = q^{-1}t^{-2}\left(\frac{q^2t^2}{(qt-1)(qt-q)}\right) = \frac{1}{(qt-1)(t-1)} = Z(t).$$

b) Para $g \geq 1$, tenemos que $Z(t) = F(t) + G(t)$ como en el corolario 2.3. Sea W un divisor canónico de F, entonces

$$(q-1)F(t) = \sum_{0 \leq grad([C]) \leq 2g-2} q^{\delta[C]} \cdot t^{grad([C])},$$

$$= \sum_{0 \leq grad([C]) \leq 2g-2} q^{grad([C])+1-g+dim[W-C]} \cdot t^{grad([C])}.$$

Multiplicando y dividiendo por $q^{g-1}t^{2g-2}$, obtenemos

$$\begin{aligned}(q-1)F(t) &= q^{g-1}t^{2g-2}\sum_{0\leq grad([C])\leq 2g-2} q^{grad([C])-(2g-2)+dim[W-C]}\cdot t^{grad([C])-(2g-2)},\\ &= q^{g-1}t^{2g-2}\sum_{0\leq grad([C])\leq 2g-2} q^{dim[W-C]}(qt)^{grad([C])-grad([W])},\\ &= q^{g-1}t^{2g-2}\sum_{0\leq grad([C])\leq 2g-2} q^{dim[W-C]}\left(\frac{1}{qt}\right)^{grad([W-C])},\\ &= q^{g-1}t^{2g-2}\,(q-1)\,F\left(\frac{1}{qt}\right).\end{aligned} \tag{2.6}$$

Observe que hemos usado el grado del divisor canónico ($grad(W) = 2g-2$) y si la clase de divisor $[C]$ recorre todas las clases de divisores con $0 \leq grad([C]) \leq 2g-2$, tiene sentido la clase $[W-C]$. Ahora para $G(t)$, obtenemos:

$$\begin{aligned}(q-1)t^{2g-2}G\left(\frac{1}{qt}\right) &= \frac{h}{q-1}\left(q^{g-1}t^{2g-2}\right)\left(q^g\left(\frac{1}{qt}\right)^{2g-1}\frac{1}{1-q\dfrac{1}{qt}}-\frac{1}{1-\dfrac{1}{qt}}\right),\\ &= \frac{h}{q-1}\left(t^{-1}\frac{1}{\dfrac{t-1}{t}}-\frac{q^{g-1}t^{2g-2}}{\dfrac{qt-1}{qt}}\right),\\ &= \frac{h}{q-1}\left(\frac{1}{t-1}-\frac{q^gt^{2g-1}}{qt-1}\right),\\ &= \frac{h}{q-1}\left(\frac{q^gt^{2g-1}}{1-qt}-\frac{1}{1-t}\right),\\ &= G(t).\end{aligned} \tag{2.7}$$

Sumando (2.6) y (2.7) obtenemos

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

Definición 2.3 *El polinomio* $L(t) := L_F(t) := (1-t)(1-qt)Z(t)$ *se llama el L-polinomio de* $F/\mathbb{F}_q$.

Por Corolario 2.3 es claro que $L(t)$ es un polinomio de grado menor o igual a $2g$. Observemos que $L(t)$ contiene toda la información acerca de los números A_n (con $n \geq 0$), puesto que

$$L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n. \tag{2.8}$$

Teorema 2.1 *i)* $L(t) \in \mathbb{Z}[t]$ *y* $grad\,(L(t)) = 2g$.

ii) $L(t) = q^g t^2 g L(1/qt)$ *(Ecuación Funcional).*

iii) $L(1) = h$.

iv) si $L(t) = a_0 + a_1 t + ... + a_{2g} t^{2g}$ *entonces:*

a) $a_0 = 1$ *y* $a_{2g} = q^g$.

b) $a_{2g-i} = q^{g-i} a_i$, *para* $0 \leq i \leq g$.

c) $a_1 = N - (q+1)$, *donde* N *es el número de lugares* $P \in \mathbb{P}_F$ *de grado 1.*

v) $L(t)$ *se factoriza en* $\mathbb{C}[t]$ *en la forma:*

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

Además los α_i, *con* $i = 1, 2, ..., 2g$ *son enteros algebraicos y pueden ser reordenados de tal forma que:* $\alpha_j \alpha_{g+j} = q$, *para* $j = 1, 2, .., g$.

vi) si $L_r(t) := (1-t)(1-q^r t)Z_r(t)$ *denota el L-polinomio de la extensión por constantes* $F_r = F\mathbb{F}_{q^r}$ *entonces*

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

donde $\alpha_i \in \mathbb{C}$.

Demostración:

i) a) Para $g = 0$, la función Zeta de $F/\mathbb{F}_q$ satisface la ecuación funcional

$$Z(t) = q^{-1}t^{-2}Z\left(\frac{1}{qt}\right) = q^{-1}t^{-2}\frac{q^2t^2}{(qt-1)q(t-1)} = \frac{1}{(qt-1)(t-1)}.$$

Y dado que $L(t) = (1-t)(1-q)Z(t)$, tenemos que

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

además $grad(L(t)) = 0$.

b) Si $g \geq 1$,

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

entonces

$$L(t) = (1-t)(1-qt)\frac{q^gt^{2g}}{(1-qt)(1-t)} = q^gt^{2g},$$

y $grad(L(t)) = 2g$.

ii) Para $g = 0$ todas las afirmaciones son inmediatas. Veamos para $g \geq 1$.
$L(t) = (1-t)(1-qt)Z(t) = q^gt^{2g}$ y

$$\begin{aligned} L\left(\frac{1}{qt}\right) &= \left(1-\frac{1}{qt}\right)\left(1-q\frac{1}{qt}\right)q^{g-1}\left(\frac{1}{qt}\right)^{2g-2}Z\left(\frac{1}{q\left(\frac{1}{qt}\right)}\right), \\ &= \left(\frac{qt-1}{qt}\right)\left(\frac{t-1}{t}\right)\frac{qt^2}{(1-qt)(1-t)}, \\ &= 1. \end{aligned}$$

iii) Dado que $L(t) = (1-t)(1-qt)Z(t)$, reemplazamos $Z(t) = F(t) + G(t)$ definido en el corolario 2.3(b) y obtenemos

$$\begin{aligned} L(t) &= (1-t)(1-qt)\left[F(t) + \frac{h}{q-1}\left(q^gt^{2g-1}\frac{1}{1-qt} - \frac{1}{1-t}\right)\right], \\ &= (1-t)(1-qt)F(t) + \frac{h}{q-1}\left(q^gt^{2g-1}(1-t) - (1-qt)\right). \end{aligned}$$

Evaluando para $t = 1$ tenemos que $L(1) = h$.

iv) Sea $L(t) = a_0 + a_1 t + ... + a_{2g} t^{2g}$. Por parte b) tenemos que

$$\begin{aligned} L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right) &= q^g t^{2g} \left(a_0 + a_1 \left(\frac{1}{qt}\right) + ... + a_{2g} \left(\frac{1}{qt}\right)^{2g} \right). \\ &= \frac{a_{2g}}{q^g} + \frac{a_{2g-1}}{q^{g-1}} t + ... + q^g a_0 t^{2g}. \end{aligned}$$

Por consiguiente $a_{2g-i} = q^{g-i}$, para $i = 0, ..., g$ y así hemos probado b).

Ahora comparando los coeficientes de t^0 y t^1 en (2.8), se observa que $a_0 = A_0$ y $a_1 = A_1 - (q+1)A_0$ y puesto que $A_0 = 1$ y $A_1 = N$, por definición de A_n obtenemos que $a_0 = 1$ y $a_1 = N - (q+1)$. Finalmente, $a_{2g} = q^g a_0 = q^g$ por b).

v)

$$\begin{aligned} L^{\perp}(t) := t^{2g} L\left(\frac{1}{t}\right) &= a_0 t^{2g} + a_1 t^{2g-1} + ... + a_{2g} \\ &= t^{2g} + a_1 t^{2g-1} + ... + q^g. \end{aligned} \tag{2.9}$$

$L^{\perp}(t)$ es un polinomio mónico con coeficientes en $\mathbb{Z}$, así sus ceros $\alpha_1, ..., \alpha_{2g} \in \mathbb{C}$ son enteros algebraicos y $L^{\perp}(t) = \prod_{i=1}^{2g} (t - \alpha_i)$. De aquí que

$$\begin{aligned} L(t) = t^{2g} L^{\perp}\left(\frac{1}{t}\right) \qquad &= t^{2g} \prod_{i=1}^{2g} \left(\frac{1 - \alpha_i t}{t}\right) \\ = \prod_{i=1}^{2g} t \left(\frac{1 - \alpha_i t}{t}\right) &= \prod_{i=1}^{2g} (1 - \alpha_i t). \end{aligned}$$

Observe que las raices α_i de $L^{\perp}(t)$ son los recíprocos de las raices de $L(t)$ puesto que $L(\alpha_i^{-1}) = 0$.

La ecuación funcional ii) implica que $L^{\perp}(\alpha) = 0$ si y sólo si $L^{\perp}(q/\alpha) = 0$, en efecto, $L^{\perp}(\alpha) = 0$ si y sólo si $\alpha^{2g} L\left(\frac{1}{\alpha}\right) = 0$ entonces $L\left(\frac{1}{\alpha}\right) = 0$. Por otro lado

$$\begin{aligned} L^{\perp}(q/\alpha) &= \frac{q^{2g}}{\alpha^{2g}} L\left(\frac{\alpha}{q}\right), \\ &= \frac{q^{2g}}{\alpha^{2g}} q^g \left(\frac{\alpha}{q}\right)^{2g} L\left(\frac{1}{q\left(\frac{\alpha}{q}\right)}\right), \\ &= q^g L\left(\frac{1}{\alpha}\right) = 0. \end{aligned}$$

Y los ceros de $L^{\perp}(t)$ los arreglamos como

$$\alpha_1, \frac{q}{\alpha_1}, ..., \alpha_k, \frac{q}{\alpha_k}, q^{1/2}, ..., q^{1/2}, q^{-1/2}, ...q^{-1/2}.$$

vi) Si $L_r(t) := (1-t)(1-q^r t)Z_r(t)$, donde $Z_r(t)$ denota la función Zeta de F_r entonces

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

$$= (1-t^r)(1-q^r t^r)\prod_{\zeta^r=1} Z(\zeta t),$$

$$= (1-t^r)(1-q^r t^r)\prod_{\zeta^r=1} \frac{L(\zeta t)}{(1-\zeta t)(1-q\zeta t)},$$

$$= \prod_{\zeta^r=1} L(\zeta t),$$

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

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

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

Ejemplo 2.1 *: Consideremos $F = \mathbb{F}_{64}(x,y)$ con $y^3 = (x+1)^3(x^2+x+1)^8$; entonces $g(F_{64}(x,y)/\mathbb{F}_{64}) = 1$ y $N = 81$. En efecto, dado que $L(x) = 64x^2+16x+1$, corresponde al L-polinomio de $F_{64}(x,y)/\mathbb{F}_{64}$ entonces $g = 1$ por teorema 2.1(i), el número de clase h está dado por $L(1) = 81$ por teorema 2.1(iii) y dado que $a_1 = 16$ tenemos que $N = a_1 + q + 1 = 81$ por teorema 2.1(iv).*

Observación 2.1 *i) En el teorema 2.1 se muestra que*

$$N(F) := N = |P \in \mathbb{P}_F; grad(P) = 1| = q + 1 - \sum_{i=1}^{2g}\alpha_i,$$

el cual se puede calcular fácilmente si conocemos $L(t)$.

ii) Si $r \geq 1, N_r := N(F_r) = |P \in \mathbb{P}_{F_r}; grad(P) = 1| = q^r + 1 - \sum_{i=1}^{2g}\alpha_i^r$, donde F_r es la extensión por constantes de $F/\mathbb{F}_q$ de grado r, entonces si conocemos N_r para $r \geq 1$ podemos encontrar el polinomio $L(t)$. Los siguientes resultados nos dan alguna información al respecto.

Corolario 2.4 *Para cualquier $r \geq 1$,*

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

donde $\alpha_i, ..., \alpha_{2g} \in \mathbb{C}$ son los recíprocos de las raíces de $L(t)$. En particular puesto que $N_1 = N(F)$, tenemos que

$$N(F) = q + 1 - \sum_{i=1}^{2g}\alpha_i.$$

Corolario 2.5 *Si* $L(t) = \sum_{i=0}^{2g} a_i t^i$ *es el L-polinomio de* $F/\mathbb{F}_q$, *y*

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

Entonces tenemos que:

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

b) $a_0 = 1$, *y*

$$ia_i = S_i a_0 + S_{i-1} a_1 + ... + S_1 a_{i-1}; \text{ con } i = 1, ..., g. \tag{2.10}$$

De aquí que dados $N_1, ..., N_g$ *podemos determinar* $L(t)$ *por (2.10) y las ecuaciones* $a_{2g-i} = q^{g-i} a_i$, *para* $i = 0, ..., g$; *por teorema 2.1(iv).*

2.1. Teorema de Hasse-Weil

En esta sección mantendremos la misma notación anterior. $F/\mathbb{F}_q$ es un cuerpo de funciones de género $g(F) = g$ sobre el cuerpo finito $\mathbb{F}_q$,

$Z_F(t) = \dfrac{L_F(t)}{(1-t)(1-qt)}$ *su función Zeta*;
$\alpha_1, ..., \alpha_{2g}$ *son los recíprocos de las raíces de* $L_F(t)$,
$N(F) = |P \in \mathbb{P}_F; grad(P) = 1|$, $F_r = F\mathbb{F}_{q^r}$, *es la extensión por constantes de grado* r,
y $N_r = N(F_r)$.

El principal resultado de esta sección es el siguiente teorema.

Teorema 2.2 Teorema de Hasse-Weil.

Los recíprocos de la raíces de $L(t)$ *satisface*

$$|\alpha_i| = q^{1/2},$$

para $i = 1, 2, ..., 2g$

Demostración: Ver ([12]-V.2.1).

Utilizando este resultado observemos cómo se puede ver la función Zeta, $Z_F(t)$ como un análogo de la función ζ de Riemman

$$\zeta(s) := \sum_{n=1}^{\infty} n^{-s}, \tag{2.11}$$

donde $s \in \mathbb{C}$ y $Re(s) > 1$.

Recordemos que la hipótesis clásica de Riemman establece que si $\zeta(s) = 0$ entonces $Re(s) = 1/2$.

Se define la norma absoluta de un divisor $A \in D_F$ como

$$N(A) := q^{grad(A)}.$$

Por ejemplo, la norma absoluta $N(P)$ de un divisor primo $P \in \mathbb{P}_F$ es la cardinalidad del cuerpo de clase residual F_P. Así la función

$$\zeta_F(s) := Z_F(q^{-s}),$$

puede escribirse como

$$\zeta_F(s) = \sum_{n=0}^{\infty} A_n q^{-sn} = \sum_{A \in D_F, A \geq 0} N(A)^{-s},$$

la cual es la análoga de (2.11).

En el caso de cuerpo de funciones algebraicas,

$$\zeta_F(s) = 0, \ \textit{implica que} \ \ Z_F(q^{-s}) = 0,$$

entonces q^{-s} es un cero del polinomio $L(t)$ y por el teorema de Hasse-Weil tenemos que

$$|q^{-s}| = q^{-1/2}.$$

Ahora, si $s = a + ib$ entonces

$$q^{-s} = e^{-slogq} = e^{(-a-ib)logq},$$

lo cual implica que $|q^{-s}| = q^{-a} = q^{-Re(s)}$; esto significa que si $\zeta_F(s) = 0$, entonces $Re(s) = 1/2$. Este es el análogo de la conjetura para cuerpos de funciones algebraicas.

Teorema 2.3 Cota de Hasse-Weil

El número $N = N(F)$ de lugares de grado 1, puede estimarse por

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

Demostración: Por Corolario 2.4 tenemos que

$$N - (q+1) = -\sum_{i=1}^{2g} \alpha_i,$$

entonces

$$|N - (q+1)| = \left| -\sum_{i=1}^{2g} \alpha_i \right| \leq \sum_{i=1}^{2g} |\alpha_i| = 2gq^{1/2},$$

por Teorema 2.2, es decir, la cota de Weil es una consecuencia del teorema de Weil. □

Si aplicamos el Teorema 2.3 al cuerpo de funciones $F_r/\mathbb{F}_{q^r}$, obtenemos

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

para $r \geq 1$.

2.2. Mejoramientos de la Cota de Hasse-Weil

Si denotamos por N al número de puntos racionales que una curva de género g puede tener sobre $\mathbb{F}_q$, la cota de Hasse-Weil implica que

$$|N - (q+1)| \leq 2g\sqrt{q},$$

pero si q no es un cuadrado entonces $|N - (q+1)| \leq \left[2g\sqrt{q}\right]$, donde [x] es la parte entera de $x \in \mathbb{R}$.
Sin embargo esta cota puede ser mejorada como sigue:

Teorema 2.4 Cota de Serre: *El número de lugares de grado uno del cuerpo de funciones $F/\mathbb{F}_q$ de género g, es acotado por*

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

Demostración: Para la prueba suponemos que $g > 0$. Sea $A \subseteq \mathbb{C}$ el conjunto de enteros algebraicos, es decir un número complejo $\alpha \in A$ si y solo si α satisface la ecuación

$$\alpha^m + b_{m-1}\alpha^{m-1} + ... + b_1\alpha + b_0 = 0$$

con $b_i \in \mathbb{Z}$. Es conocido que

$$A \text{ es un subanillo de } \mathbb{C} \text{ y } A \cap \mathbb{Q} = \mathbb{Z}. \tag{2.12}$$

Consideremos el L-polinomio $L(t) = \prod_{i=1}^{2g}(1-\alpha_i t)$ de $F/\mathbb{F}_q$, donde los α_i para $i = 1, 2..., 2g$ son enteros algebraicos con $|\alpha_i| = q^{1/2}$ por Teorema 2.2, y por Teorema 2.1 estos pueden ordenarse de tal forma que $\alpha_i\alpha_{g+i} = q$, lo cual implica que $\overline{\alpha_i} = \alpha_{g+i} = q/\alpha_i$ para $1 \leq i \leq g$.

Sean

$$\begin{aligned} \gamma_i &:= \alpha_i + \overline{\alpha_i} + [2q^{1/2}] + 1 \qquad y \\ \delta_i &:= -(\alpha_i + \overline{\alpha_i}) + [2q^{1/2}] + 1, \end{aligned}$$

por (2.12) γ_i y δ_i son enteros algebraicos reales y puesto que

$$\alpha_i + \overline{\alpha_i} = 2Re(\alpha_i) \leq 2|\alpha_i| = 2q^{1/2} \leq \left[2q^{1/2}\right] + 1,$$

se tiene que

$$\gamma_i > 0 \text{ y } \delta_i > 0. \tag{2.13}$$

Cualquier inmersión $\sigma : \mathbb{Q}(\alpha_1, ...\alpha_{2g}) \to \mathbb{C}$ permuta $\alpha_1, ..., \alpha_{2g}$ puesto que

$$\prod_{i=1}^{2g}(t - \alpha_i) \quad = L^{\perp}(t) \in \mathbb{Z}[t],$$

donde

$$L^{\perp}(t) \quad := t^{2g} L\left(\frac{1}{t}\right).$$

Más aún si $\sigma(\alpha_i) = \alpha_j$ entonces

$$\sigma(\overline{\alpha_i}) = \sigma(q/\alpha_i) = q/\sigma(\alpha_i) = \overline{\sigma(\alpha_i)} = \overline{\alpha_j}.$$

Por tanto σ actúa como una permutación sobre los conjuntos $\{\gamma_1, ..., \gamma_g\}$ y $\{\delta_1, ..., \delta_g\}$.

Ahora, sean

$$\gamma := \prod_{i=1}^{g} \gamma_i$$

y

$$\delta := \prod_{i=1}^{g} \delta_i,$$

entonces γ y δ son enteros algebraicos los cuales son invariantes bajo todas las inmersiones de $\mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_{2g})$ en $\mathbb{C}$; de aquí que γ y $\delta \in \mathbb{Q} \cap A = \mathbb{Z}$.

Dado que $\gamma_i > 0$ y $\delta_i > 0$ por (2.13), entonces tenemos que

$$\prod_{i=1}^{g} \gamma_i \geq 1 \text{ y } \prod_{i=1}^{g} \delta_i \geq 1.$$

La conocida desigualdad entre la media aritmética y media geométrica afirma que :

$$\frac{1}{g}\sum_{i=1}^{g}\gamma_i \;\geq \left(\prod_{i=1}^{g}\gamma_i\right)^{1/g} \geq 1,$$

entonces

$$g \;\leq \left(\sum_{i=1}^{g}\alpha_i+\overline{\alpha_i}\right)+g[2q^{1/2}]+g \;=\sum_{i=1}^{2g}\alpha_i+g[2q^{1/2}]+g,$$

en consecuencia

$$0 \;\leq \sum_{i=1}^{2g}\alpha_i+g[2q^{1/2}],$$

y puesto que $\sum_{i=1}^{2g}\alpha_i=(q+1)-N$ tenemos que

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

De igual forma, la desigualdad $\frac{1}{g}\sum_{i=1}^{g}\delta_i \;\geq \left(\prod_{i=1}^{g}\delta_i\right)^{1/g} \geq 1,$ implica

$$g \;\leq \left(\sum_{i=1}^{g}-(\alpha_i+\overline{\alpha_i})\right)+g[2q^{1/2}]+g \;=-\sum_{i=1}^{2g}\alpha_i+g[2q^{1/2}]+g,$$

por tanto

$$0\leq -\sum_{i=1}^{2g}\alpha_i+g[2q^{1/2}],$$

y puesto que

$$-\sum_{i=1}^{2g}\alpha_i=N-(q+1),$$

entonces

$$N-(q+1)\geq -g[2q^{1/2}].\square$$

Teorema 2.5 Cota de Ihara: *Para un cuerpo de funciones $F/\mathbb{F}_q$ de género g, el número de lugares de grado uno es acotado por*

$$|N-(q+1)|\leq \left[\frac{\left(\sqrt{(8q+1)g^2+4(q^2-g)g}-g\right)}{2}\right].$$

Demostración: Sea $F/\mathbb{F}_q$ un cuerpo de funciones algebraicas con género g, $\overline{\alpha_i}$ el conjugado complejo de α_i para $i = 1, ..., g$ con $\alpha_i\overline{\alpha_i} = q$ y $a_i = \alpha_i + \overline{\alpha_i}$. Para cada entero positivo $m \geq 1$, se define

$$N_m = \quad q^m + 1 - \textstyle\sum_{i=1}^{g} \left(\alpha_i^m + \overline{\alpha_i}^m\right).$$

como el número de lugares de grado 1 de $F\mathbb{F}_{q^m}/F_{q^m}$, entonces

$$\begin{aligned} q + 1 - \sum_{i=1}^{g} \alpha_i = \quad N_1 \leq N_2 \quad &= q^2 + 1 - \sum_{i=1}^{g} \left(\alpha_i^2 + \overline{\alpha_i}^2\right), \\ &= q^2 + 1 - \sum_{i=1}^{g} \left(\alpha_i^2 + 2\alpha_i\overline{\alpha_i} + \alpha_i^2\right) + 2gq, \\ &= q^2 + 1 + 2gq - \sum_{i=1}^{g} \left(\alpha_i + \overline{\alpha_i}\right)^2, \\ &= q^2 + 1 + 2gq - \sum_{i=1}^{g} a_i^2. \end{aligned}$$

Puesto que

$$\left(\sum_{i=1}^{g} a_i\right)^2 \leq g \sum_{i=1}^{g} a_i^2,$$

entonces

$$\begin{aligned} N_1 \quad &\leq q^2 + 1 + 2gq - \frac{1}{g}\left(\sum_{i=1}^{g} a_i\right)^2, \\ &\leq q^2 + 1 + 2gq - \frac{1}{g}\left(N_1 - q - 1\right)^2, \end{aligned}$$

equivale a: $\dfrac{1}{g}\left(N_1^2 - 2N_1q + q^2 - 2N_1 + 2q + 1\right) - q^2 - 1 - 2qg + N_1 \quad \leq 0.$

Por consiguiente,

$$N_1^2 - (2q + 2 - g)\, N_1 + (q+1)^2 - \left(q^2 + 1\right) g - 2qg^2 \quad \leq 0.$$

De aquí que,

$$N_1 \quad \leq \quad \frac{\sqrt{(8q+1)\, g^2 + (4q^2 - 4q)\, g} - (g - 2q - 2)}{2},$$

$$|N_1 - (q+1)| \leq \quad \left[\frac{\left(\sqrt{(8q+1)g^2 + 4(q^2 - g)g} - g\right)}{2}\right]. \qquad \square$$

Definición 2.4 *Un cuerpo de funciones $F/\mathbb{F}_q$ de género g se dice Maximal si*

$$N = q + 1 + 2gq^{1/2}. \tag{2.14}$$

Ejemplo 2.2 *: El cuerpo de funciones hermitianas $F_{q^2}(x,y)/\mathbb{F}_{q^2}$ definido por la ecuación $y^q + y = x^{q+1}$ con $g(C) = q(q-1)/2$ y $N = 1 + q^3$ es maximal, puesto que al sustituir g en (2.14) se obtiene*

$$N = q^2 + 1 + 2\,(q(q-1)/2)\,q = q^3 + 1.\square$$

Un cuerpo de funciones maximal sobre $\mathbb{F}_q$ puede existir sólo si q es un cuadrado.

El siguiente resultado muestra que $F/\mathbb{F}_q$ no puede ser maximal si el género es mayor con respecto a q.

Proposición 2.6 *Si $F/\mathbb{F}_q$ es maximal entonces $g \leq (q - q^{1/2})/2$.*

Demostración: Sean $\alpha_1, \alpha_2, ..., \alpha_{2g}$ las raíces recíprocas de $L(t)$.

Puesto que $N = q+1-\sum_{i=1}^{2g} \alpha_i$ y $|\alpha_i| = q^{1/2}$ por Corolario 2.4 y Teorema 2.2, el supuesto

$$N = q + 1 + 2gq^{1/2},$$

implica que $\alpha_i = -q^{1/2}$ para $i = 1, 2, ..., 2g$. Ahora, si consideramos N_2 el número de lugares de grado 1 en $F\mathbb{F}_{q^2}/\mathbb{F}_{q^2}$, tenemos que

$$N_2 = (q^2 + 1) - \sum_{i=1}^{2g} \alpha_i^2 = q^2 + 1 - 2gq,$$

y puesto que $N \leq N_2$ entonces

$$\begin{aligned} & q + 1 + 2gq^{1/2} && \leq q^2 + 1 - 2gq, \\ \Leftrightarrow \quad & g(2q^{1/2} + 2q) && \leq q^2 - q, \\ \Leftrightarrow \quad & g && \leq \frac{q^2 - q}{2(q^{1/2} + q)}, \\ = \quad & \frac{q - q^{1/2}}{2}. \quad \square \end{aligned}$$

Se puede refinar la prueba de la Proposición 2,6 con el fin de obtener otras cotas para el número de lugares de grado 1, para ello se procede como sigue.

Sea $N_r = N(F_r) = |\{P \in \mathbb{P}_{F_r}; grad(P) = 1\}|$, donde $F_r = F\mathbb{F}_{q^r}$ es la extensión por constantes de grado r y consideremos para $i = 1, ..., 2g$,

$$w_i := \alpha_i q^{1/2},$$

donde $\alpha_1,\ \alpha_2,\ ...\alpha_{2g}$ son los recíprocos de las raíces de $L(t)$, entonces

$$|w_i| = |\alpha_i q^{-1/2}| = |\alpha_i||q^{-1/2}| = 1,$$

(por el Teorema de Hasse-Weil) y podemos suponer que $w_{g+i} = \overline{w_i} = w_i^{-1}$, para $i = 1, ..., g$, (por Teorema 2.1(v)). Puesto que $w_i^{-1} = w_{g+i}$, tenemos que

$$\sum_{i=1}^{2g} w_i^r = \sum_{i=1}^{g} (w_i^r + w_i^{-r}),$$

entonces por el Corolario 2.4

$$N_r = q + 1 - \sum_{i=1}^{g} (w_i^r + w_i^{-r}),$$

multiplicando por $q^{-r/2}$, obtenemos:

$$N_r q^{-r/2} = q^{r/2} + q^{-r/2} - \sum_{i=1}^{g} (w_i^r + w_i^{-r}). \tag{2.15}$$

Dados $c_1, c_2, ...$ números reales, multiplicamos (2.15) por c_r y tenemos que:

$$N_r c_r q^{-r/2} = c_r q^{r/2} + c_r q^{-r/2} - \sum_{i=1}^{g} c_r (w_i^r + w_i^{-r}),$$

ahora sumamos y restamos $N_1 c_r q^{-r/2}$ y obtenemos:

$$N_1 c_r q^{-r/2} = c_r q^{r/2} + c_r q^{-r/2} - \sum_{i=1}^{g} c_r (w_i^r + w_i^{-r}) - (N_r c_r q^{-r/2} - N_1 c_r q^{-r/2},)$$

sumando la ecuación para $r = 1, ..., m$ tenemos:

$$\begin{aligned} N_1\lambda_m(q^{-1/2}) = \ & \lambda_m(q^{1/2}) + \lambda_m(q^{-1/2}) - \sum_{i=1}^{g} \left(\lambda_m(w_i) + \lambda_m(w_i^{-1})\right), \\ & - \left(N_r\lambda_m(q^{-1/2}) - N_1\lambda_m(q^{-1/2})\right), \\ N_1\lambda_m(q^{-1/2}) = \ & \lambda_m(q^{1/2}) + \lambda_m(q^{-1/2}) - \sum_{i=1}^{g} (f_m(w_i) - 1) - \sum_{r=1}^{m} (N_r - N_1) c_r q^{-r/2}, \end{aligned}$$

$$N_1\lambda_m(q^{-1/2}) = \lambda_m(q^{1/2}) + \lambda_m(q^{-1/2}) + g - \sum_{i=1}^{g} f_m(w_i) - \sum_{r=1}^{m} (N_r - N_1) c_r q^{-r/2}, \tag{2.16}$$

donde

$$\lambda_m(t) = \sum_{r=1}^{m} c_r t^r,$$

y

$$f_m(t) = 1 + \lambda_m(t) + \lambda_m(t^{-1}). \tag{2.17}$$

para $0 \neq t \in \mathbb{C}$.

Note que $f_m(t) \in \mathbb{R}$ para $|t| = 1$. Más precisamente si $t = cos(\theta) + isen(\theta)$, tenemos que $t^r = cos(r\theta) + isen(r\theta)$ y $t^{-r} = cos(r\theta) - isen(r\theta)$ entonces

$$\lambda_m(t) = \sum_{r=1}^{m} c_r \left(cos(r\theta) + isen(r\theta)\right),$$

y

$$\lambda_m(t^{-1}) = \sum_{r=1}^{m} c_r \left(cos(r\theta) - isen(r\theta)\right),$$

por (2.17),

$$f_m(\theta) = 1 + 2\sum_{r=1}^{m} c_r cos(r\theta).$$

La ecuación (2.16) se llama *fórmula explícita.*, ver ([11]) . La selección de las constantes c_r producen una buena estimación para N.

Proposición 2.7 *Supongamos que $c_1, ..., c_m \in \mathbb{R}$ satisface las siguientes condiciones:*

i) $c_r \geq 0$ para $r = 1, .., m$ y no toda $c_r = 0$.

ii) $f_m(t) \geq 0$, para toda $t \in \mathbb{C}$ con $|t| = 1$ (donde $f_m(t)$ está definido por (2.17). Entonces el número de lugares de grado 1 está acotado por

$$N \leq \frac{g}{\lambda_m(q^{-1/2})} + \frac{\lambda_m(q^{1/2})}{\lambda_m(q^{-1/2})} + 1.$$

Demostración: Por (2.16) y puesto que $c_r \geq 0$ y $f_m(t) \geq 0$ para $t \in \mathbb{C}$, con $|t| = 1$ tenemos que:

$$N_1\lambda_m(q^{-1/2}) \leq \lambda_m(q^{1/2}) + \lambda_m(q^{-1/2}) + g.$$

Por parte *i)* $\lambda_m(q^{-1/2}) > 0$, entonces si dividimos por $\lambda_m(q^{-1/2})$ obtenemos:

$$\begin{aligned} N_1 \leq & \frac{\lambda_m(q^{1/2})}{\lambda_m(q^{-1/2})} + \frac{\lambda_m(q^{-1/2})}{\lambda_m(q^{-1/2})} + \frac{g}{\lambda_m(q^{-1/2})}, \\ N_1 \leq & \frac{g}{\lambda_m(q^{-1/2})} + \frac{\lambda_m(q^{1/2})}{\lambda_m(q^{-1/2})} + 1. \end{aligned}$$ □

Ilustramos con un ejemplo el anterior resultado.

Ejemplo 2.3 *Sean* $q = 2, r = 6$ *y* $c_1 = \frac{184}{203}, c_2 = \frac{20}{29}, c_3 = \frac{90}{203}, c_4 = \frac{89}{406}$, $c_5 = \frac{2}{29}, c_6 = \frac{2}{203}$. *Por (2.17) tenemos que* $\lambda_6(\sqrt{2}) = 4,34,\ \lambda_6(\sqrt{2})^{-1} = 1,21$,

$$f_6(t) = \frac{406 + 368t + 280t^2 + 180t^3 + 89t^4 + 28t^5 + 4t^6}{406} +$$

$$+\frac{368t^{-1} + 280t^{-2} + 180t^{-3} + 89t^{-4} + 28t^{-5} + 4t^{-6}}{406},$$

puesto que $|t| = 1, f_6(t) \geq 0$ *y por proposición 2.7*

$$N_2(g) \leq \ \frac{g}{1,21} + \frac{4,34}{1,21} + 1 = 0,83g + 5,35.$$

Definición 2.5 *i)* $N_q(g) := máx\{N(F)|F/\mathbb{F}_q tiene\ género\ g\}$.

ii) $A(q) := LimSup_{g\to\infty} N_q(g)/g$.

La cota de Serre afirma que $A_q \leq [2q^{1/2}]$. Mostraremos a continuación que existe una cota más refinada para $A(q)$.

Teorema 2.6 Cota de Drinfeld-Vladut:

$$A(q) \leq q^{1/2} - 1.$$

Demostración: Fijemos $m \geq 1$ y definamos $c_r := 1 - \frac{r}{m}, (r = 1, .., m)$.

Para $t \neq 1$ sea $\lambda_m(t) = \sum_{r=1}^{m} \left(1 - \frac{r}{m}\right) t^r = \sum_{r=1}^{m} t^r - \sum_{r=1}^{m} \frac{rt^r}{m}$,

donde

$$\sum_{r=1}^{m} t^r = \frac{1 - t^{m+1}}{1 - t} - 1 = \frac{t - t^{m+1}}{1 - t}, \tag{2.18}$$

y derivando $\sum_{r=1}^{m} t^r$, obtenemos que:

$$D_t\left(\sum_{r=1}^{m} t^r\right) = \sum_{r=1}^{m} rt^{r-1} = \frac{1}{t}\sum_{r=1}^{m} rt^r,$$

ahora al derivar el lado derecho de la igualdad (2.18) tenemos que:

$$D_t\left(\frac{t - t^{m+1}}{1 - t}\right) = \frac{t - mt^m - t^m + mt^{m+1}}{(1 - t)^2},$$

entonces

$$\frac{1}{t}\sum_{r=1}^{m} rt^r = \frac{t - mt^m - t^m + mt^{m+1}}{(1-t)^2},$$

lo cual implica

$$\sum_{r=1}^{m} \frac{rt^r}{m} = \frac{t}{m}\left(\frac{t - mt^m - t^m + mt^{m+1}}{(1-t)^2}\right).$$

entonces

$$\lambda_m(t) = \frac{t - t^{m+1}}{1-t} - \frac{t^2 - mt^{m+1} - t^{m+1} + mt^{m+2}}{m(1-t)^2} = \frac{t}{(1-t)^2}\left(\frac{t^m - 1 + m - mt}{m}\right)$$

$$= \frac{t}{(1-t)^2}\left(\frac{t^m - 1}{m} + 1 - t\right).$$

y

$$\begin{aligned} f_m(t) &= 1 + \lambda_m(t) + \lambda_m(t^{-1}) = 1 + \frac{t}{(1-t)^2}\left(\frac{t^m - 1}{m} + 1 - t\right) \\ &+ \frac{t^{-1}}{(1-t^{-1})^2}\left(\frac{t^{-m} - 1}{m} + 1 - t^{-1}\right) \\ &= \frac{m - 2mt + mt^2 + t^{m+1} - t + mt - mt^2}{m(1-t)^2} + \frac{t^{1-m} - t + mt - m}{m(1-t)^2} \qquad (2.19) \\ &= \frac{t^{m+1} - t}{m(1-t)^2} + \frac{t^{m-1} - t}{m(t-1)^2} \\ &= \frac{2 - t^m - t^{-m}}{m(t-1)(t^{-1}-1)}. \end{aligned}$$

Puesto que $t^{-1} = \bar{t}$ para $|t| = 1$, la ecuación (2.19) afirma que $f_m(t) \geq 0$ para todo $t \in \mathbb{C}$ con $|t| = 1$ entonces dividimos por g la inecuación dada por proposición 4.2 y obtenemos:

$$\frac{N}{g} \leq \frac{1}{\lambda_m(q^{-1/2})} + \frac{1}{g}\left(1 + \frac{\lambda_m(q^{1/2})}{\lambda_m(q^{1/2})}\right).$$

Si $m \to \infty$ entonces

$$\lambda_m(q^{-1/2}) \to \frac{q^{-1/2}}{(1-q^{-1/2})^2}\left(1 - q^{-1/2}\right) = \frac{q^{-1/2}}{1 - q^{-1/2}} = \frac{1}{q^{1/2} - 1};$$

entonces para cualquier $\varepsilon > 0$ existe m_0 tal que $\lambda_{m_0}(q^{-1/2})^{-1} < q^{1/2} - 1 + \varepsilon/2$, ahora si escogemos g_0 tal que

$$\frac{1}{g_0}\left(1 + \frac{\lambda_{m_0}(q^{1/2})}{\lambda_{m_0}(q^{1/2})}\right) < \varepsilon/2,$$

entonces para cualquier $g \geq g_0$ se tiene que

$$\frac{N}{g} < q^{1/2} - 1 + \varepsilon.$$

Por lo tanto

$$A(q) = limSup_{g\to\infty}\,(N/g) \leq q^{1/2} - 1.\square$$

Observación 2.2 *Si q es un cuadrado, existen secuencias de cuerpos de funciones $F^{(v)}/\mathbb{F}_q$ con género $g\left(F^{(v)}\right) \to \infty$ tal que $N\left(F^{(v)}/g(F^{(v)})\right) \to q^{1/2} - 1$ para $\nu \to \infty$. De aquí $A(q) = q^{1/2} - 1$ si q es un cuadrado.*

Capítulo 3

Cubrimientos Duplos

En esta sección construiremos cuerpos de funciones algebracias $E = E_1E_2$ con cuerpo de constantes el cuerpo finito $\mathbb{F}_q$ donde E_1 está definido por una ecuación de Kummer y E_2 por una de Artin-Shreier, tales cuerpos de funciones serán construidos de forma tal que el número de lugares de grado 1 esté cercano bien sea a la Cota de Weil, Serre o Ihara.

Por tratarse de extensiones duplas, el cálculo del género de E no obedece a una fórmula específica, no obstante usaremos las Proposiciones 1.4 y 1.5 para calcular este invariante, así mismo para el conteo del número de lugares de grado uno será necesario hacer un análisis más detallado que en la Proposición 1.3. Este proceso se desarrollará en las siguientes secciones.

3.1. Construcciones vía extensiones de Kummer.

En esta sección haremos un análisis detallado de cierto tipo de extensiones de Kummer introducidas en [2] y usaremos dicha técnica para construir nuevas curvas.

Sea r un divisor de $q-1$ y $\mu(x) \in \mathbb{F}_q(x)$. Por la Proposición 1.3, el polinomio $\varphi(T) = T^r - \mu(x) \in \mathbb{F}_q(x)[T]$ es irreducible sobre el cuerpo de funciones racionales $\mathbb{F}_q(x)$, siempre y cuando $\mu(x) \neq w(x)^d$ para todo $w \in \mathbb{F}_q(x)$ y todo $d|r$, es decir $\mu(x)$ no es una d - ésima potencia para todo $d|r$.

Supondremos entonces que $\varphi(T)$ es irreducible y que $E_1 = \mathbb{F}_q(x, y)$ con $\varphi(y) = 0$.

Como en la Proposición 1.3, para cada $\alpha \in \mathbb{F}_q$ definimos

$$\varphi_\alpha(T) := T^r - \mu(\alpha) \in \mathbb{F}_q[T],$$

el cual se factoriza como

$$\varphi_\alpha(T) = \prod_{i=1}^{r} \psi_i(T), \tag{3.1}$$

con $\psi_i(T)$ irreducible en $\mathbb{F}_q[T]$, puesto que nuestro objetivo es el estudio de lugares de grado 1, desearíamos que $\varphi_\alpha(T)$ se factorice como un producto de r factores, es decir que cada $\psi_i(T)$ sea un polinomio de grado 1, así las cosas por cada $\alpha \in \mathbb{F}_q$ tal que $\varphi_\alpha(T) = \prod_{i=1}^{r} \psi_i(T)$, existirán r lugares de grado 1 en el cuerpo de funciones E_1.

Surge ahora la pregunta ¿Cómo debe ser $\mu(x) \in \mathbb{F}_q(x)$ de tal forma que $\varphi_\alpha(T)$ se factorice como un producto de r factores?

Una primera respuesta a este interrogante es que para un α fijo, $\mu(\alpha)$ debe ser una r-ésima potencia, es decir debe existir $w_\alpha \in \mathbb{F}_q$ tal que $w_\alpha^r = \mu(\alpha)$, ahora, por la elección de r el cuerpo $\mathbb{F}_q$ contiene todos las raíces r-ésimas de la unidad y por lo tanto tenemos que

$$\varphi_\alpha(T) = (T - w_\alpha)(T - \zeta w_\alpha)...(T - \zeta^{r-1} w_\alpha).$$

Si denotamos por $N(E) = \{P \in \mathbb{P}_{E_1}; grad(P) = 1\}$, entonces por lo anterior tenemos que

$$\#N(E) \geq r\{\alpha \in \mathbb{F}_q; \mu(\alpha) \text{ es una } r\text{-ésima potencia en } \mathbb{F}_q\}.$$

Otros lugares de grado uno pueden obtenerse analizando los puntos de rama de $\mu(x)$.

Construcción de un $\mu(x) \in \mathbb{F}_q(x)$ apropiado.

Nuestro objetivo ahora es construir un $\mu(x) \in \mathbb{F}_q(x)$ tal que para "muchos"$\alpha \in \mathbb{F}_q$, $\mu(\alpha)$ sea una r-ésima potencia. Un primer (y natural) intento es hacer que $\mu(\alpha) = 1$ con $\alpha \in \mathbb{F}_q$, para ello procederemos como sigue.

Sean $f(x)$ y $\ell(x) \in \mathbb{F}_q[x]$ polinomios tales que mcd $(f(x), \ell(x)) = 1$, $\ell(x)$ tiene todas (o casi todas) sus raíces en $\mathbb{F}_q$ y $grad(f(x)) \geq grad(\ell(x))$.

Por el algoritmo de la división existe $h(x) \in \mathbb{F}_q[x]$ tal que

$$f(x) = \ell(x)h(x) + \mathcal{R}_\ell(f(x)), \tag{3.2}$$

donde $\mathcal{R}_\ell(f(x))$ es el residuo de la división de $f(x)$ por $\ell(x)$. Ahora, si definimos

$$\mu(x) := \frac{f(x)}{\mathcal{R}_\ell(f(x))}, \tag{3.3}$$

tenemos que todo $\alpha \in \vartheta_l := \{\alpha \in \mathbb{F}_q; \ell(\alpha) = 0\}$, satisface

$$\mu(\alpha) = \frac{f(\alpha)}{\mathcal{R}_\ell(f(x))(\alpha)} = 1.$$

Observe que en este proceso hemos transformado el problema de obtener "muchos"lugares de grado 1 a obtener polinomios $\ell(x) \in \mathbb{F}_q[x]$ con "muchosçeros en $\mathbb{F}_q$.

Es conocido ([10]-8.2) que, si $q = p^n$ y $g(x)$ es un polinomio irreducible de grado n con coeficientes en $\mathbb{F}_p$ entonces $g(x)$ tiene todos sus ceros en $\mathbb{F}_{q=p^n}$, además para todo m el número de polinomios irreducibles sobre $\mathbb{F}_q$ de grado m es

$$N_q(m) = \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) q^d,$$

donde μ es la función de Möbius [7] definida por

$$\mu(x) = \begin{cases} 1, & \text{si } x = 1. \\ (-1)^k, & \text{si } x = p_1 p_2 \cdots p_k \text{ para distintos primos } p_i. \\ 0, & \text{en otro caso.} \end{cases}$$

Esto implica que siempre es posible encontrar polinomios con coeficientes en $\mathbb{F}_p$ que se descompongan completamente en $\mathbb{F}_q$, más aún bajo ciertas condiciones (que precisaremos luego) casi siempre podremos construir polinomios $p(x)$ de cualquier grado con un número considerable de ceros en $\mathbb{F}_q$.

De otro lado, el producto de todos los polinomios irreducibles de grado m sobre $\mathbb{F}_p$ está dado por

$$I(p, m, x) = \prod_{d|m} \left(x^{p^d} - x\right)^{\mu(m/d)},$$

y en consecuencia una factorización de $I(p, m, x)$ dará como resultado una lista de polinomios irreducibles sobre $\mathbb{F}_p$ de grado m. Como ilustración de lo anterior tenemos.

Ejemplo 3.1 1) Sean $p = 2, n = 1$ y $m = 4$. Por un lado tenemos que existen $N_2(4) = 3$ polinomios irreducibles de grado 4 cuyos ceros están en $\mathbb{F}_{16}$, y $I(2, 4, x) = (x^{16} - x)^{\mu(1)}(x^4 - x)^{\mu(2)}(x^2 - x)^{\mu(4)} = x^{12} + x^9 + x^6 + x^3 + 1$.

De otro lado, factorizando $I(2, 4, x)$ obtenemos la lista completa de polinomios irreducibles de grado 4 sobre $\mathbb{F}_2$ a saber

$$\{x^4 + x^3 + x^2 + x + 1, x^4 + x^3 + 1, x^4 + x + 1\}.$$

[7] Ver [9], Teorema 3.25

Ahora, observe que además de los 3 polinomios de grado 4 citados en el párrafo anterior, los polinomios x, $x+1$ y x^2+x+1 también tienen sus ceros en $\mathbb{F}_{16}$, esto posibilita la construcción de polinomios $p(x)$ de grados $1 \leq grad(p(x)) \leq 16$ con todos sus ceros en $\mathbb{F}_{16}$.

2) Para $p=3, n=1$ y $m=3$ tenemos $N_3(3)=8$ y $I(3,3,x)=\dfrac{x^{27}-x}{x^3-x}$.

La lista de polinomios irreducibles de grado 3 sobre $\mathbb{F}_3$ está dada por

$\{(x^3+2x+1),(x^3+2x+2),(x^3+x^2+2),(x^3+x^2+x+2),(x^3+x^2+2x+1),$
$(x^3+2x^2+1),(x^3+2x^2+x+1),(x^3+2x^2+2x+2)\}$.

3) Si $p=2$ y $m=5$ tenemos que existen 6 polinomios irreducibles sobre $\mathbb{F}_2$ de grado 5, estos son $\{(x^5+x^2+1),(x^5+x^3+1),(x^5+x^3+x^2+x+1),$
$(x^5+x^4+x^2+x+1),(x^5+x^4+x^3+x+1),(x^5+x^4+x^3+x^2+1)\}$, en este caso no es posible encontrar polinomios de grados 3,4,8,9 etc. con todos sus ceros en $\mathbb{F}_{32}$. □

Proposición 3.1 Sean $r, f(x)$ y $\ell(x)$ como antes, entonces el cuerpo de funciones algebraicas $E_1=\mathbb{F}_q(x,y)$ definido por la ecuación de Kummer

$$y^r=\frac{f(x)}{\mathcal{R}_\ell(f(x))}, \tag{3.4}$$

satisface

$$\#N(\mathbb{F}_q(x,y)/\mathbb{F}_q) \geq r \cdot grad(\ell(x)).$$

Además, si $D=\sum_{i=1}^n d_iP_i$, es el divisor de $\mu(x)$ y existe un i tal que $m.c.d.(r,|d_i|)=1$, entonces el género de $\mathbb{F}_q(x,y)/\mathbb{F}_q$ está dado por

$$g(\mathbb{F}_q(x,y)/\mathbb{F}_q)=\frac{2+r(n-2)-\sum_{i=1}^n m.c.d.(r,|d_i|)}{2}.\square$$

Observe que en el proceso de cálculo del número de lugares de grado 1 en el cuerpo de funciones $\mathbb{F}_q(x,y)/\mathbb{F}_q$ definido por la ecuación (3.4) sólo hemos considerado los ceros del polinomio $\ell(x)$ en $\mathbb{F}_q$, es decir aquellos $\alpha \in \mathbb{F}_q$ tales que $\mu(\alpha)=1$, otros lugares de grado 1 pueden obtenerse de los puntos de rama y además del conjunto

$$\{\alpha \in \mathbb{F}_q; \mu(\alpha)=\zeta^r\},$$

con $\zeta^r \neq 1$ y $\zeta \in \mathbb{F}_q$, esto es, para los elementos $\alpha \in \mathbb{F}_q$ tales que $\mu(\alpha)$ sea una r-ésima potencia en $\mathbb{F}_q$ distinta de 1.

El número exacto de lugares de grado uno está dado por el siguiente resultado.

Proposición 3.2 Sean p un número primo, $q = p^n$ y $\alpha \in \mathbb{F}_q$.

La congruencia $x^r \equiv \mu(\alpha) \pmod{q}$ tiene $\kappa = m.c.d.(r, q-1)$ soluciones si y solamente si

$$\mu(\alpha)^{\frac{q-1}{\kappa}} \equiv 1 \pmod{q}. \tag{3.5}$$

Demostración: Ver ([10]). □

Observación 3.1 Por 3.2, $\mu(\alpha)$ será una r-ésima potencia en $\mathbb{F}_q$ siempre y cuando el máximo común divisor $d(x)$ entre $x^q - x$ y el numerador de la función racional $\mu(x)^{\frac{q-1}{r}} - 1$ sea diferente de 1, pero de acuerdo a nuestra definición de $\mu(x)$ esto siempre ocurre, más aún $\ell(x)$ es un factor de $d(x)$. Ahora, observe que el conjunto de ceros del polinomio $d(x)$ contiene a todos los α de $\mathbb{F}_q$ que son enviados por la función μ a r-ésimas potencias, esto claramente incluye los ceros de $\ell(x)$.

En consecuencia

$$\#N(\mathbb{F}_q(x,y)/\mathbb{F}_q) = r \cdot grad(d(x)) + \rho.$$

donde ρ es el número de lugares de grado uno obtenido de la ramificación de $\mu(x)$.

3.2. Construcción vía extensiones de Artin-Schreier.

El objetivo de esta sección es el de construir un cubrimiento E_2 del Cuerpo de Funciones $E_1/\mathbb{F}_q = \mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ definido en la sección anterior, por medio de una extensión de Artin-Schreier,

$$y^p - y = g(x), \tag{3.6}$$

con $g(x) \in \mathbb{F}_q(x)$, de tal forma que $E = E_1E_2$ tenga "muchos"lugares de grado 1.

De acuerdo con las Proposiciones 1.3 y 1.5, el problema de contar lugares de grado 1 en este tipo de extensiones está estrechamente relacionado con el siguiente teorema.

Teorema 3.1 Teorema 99 de Hilbert. Sea F una extensión finita de $K = \mathbb{F}_p$. Entonces para $\alpha \in F$ se tiene que

$$Tr_{F/K}(\alpha) = 0 \Longleftrightarrow \alpha = \beta^p - \beta,$$

para algún $\beta \in F$.

Demostración: Ver ([9], Tma. 2.25). □

Haciendo $F = \mathbb{F}_{q=p^n}$ tendremos que un punto de coordenadas (α, β) en $\mathbb{F}_q \times \mathbb{F}_q$ induce un lugar de grado 1, $P_{(\alpha,\beta)}$ en el cuerpo de funciones E_2 si y solamente si $Tr_{\mathbb{F}_q/\mathbb{F}_p}(g(\alpha)) = 0$.

Luego para determinar aproximadamente el número de lugares de grado 1 de E_2, es necesario analizar el polinomio $\delta(x) = \text{m.c.d.}(Tr_{\mathbb{F}_q/\mathbb{F}_p}(g(x)), x^q - x)$, puesto que si α es un cero de $\delta(x)$, entonces existirá un $\beta \in \mathbb{F}_q$ tal que $P_{(\alpha,\beta)}$ es un lugar de grado 1 de E_2.

Ahora dado que estamos interesados en construir cubrimientos duplos, es claro que debe haber una relación entre los polinomios $d(x)$ de la sección anterior y $\delta(x)$, pues por cada cero común tendremos $p \cdot r$ lugares racionales en la composición $E = E_1E_2$. Precisando lo anterior tenemos la siguiente proposición.

Proposición 3.3 Sean E, E_1 y E_2 como antes y si $\tau(x) = \text{m.c.d.}(d(x), \delta(x))$, entonces el número de lugares de grado uno del cuerpo de funciones E satisface

$$\#N(E/\mathbb{F}_q) \geq p \cdot r(grad(\tau)).$$

Demostración: Sea $E := E_1E_2$ un cuerpo de funciones algebraicas con $E_1 := \mathbb{F}_q(x, y)/\mathbb{F}_q(x)$ definido por la ecuación de Kummer $y^r = \mu(x)$ y $E_2 := \mathbb{F}_q(x, y, z)/\mathbb{F}_q(x, y)$ definido por la ecuación de Arthin-Schreier $z^p - z = g(x)$, por la Observación 3.1 tenemos que

$$\#N(\mathbb{F}_q(x, y)/\mathbb{F}_q) = r \cdot grad(d(x)) + \rho,$$

donde ρ es el número de lugares de grado uno obtenidos de la ramificación de $\mu(x)$ y $d(x) = \text{m.c.d}(\mu(x)^{\frac{q-1}{r}} - 1, x^q - x)$.

Puesto que $\delta(x) = \text{m.c.d.}(Tr_{\mathbb{F}_q/\mathbb{F}_p}(g(x)), x^q - x)$ entonces por cada cero de $\delta(x)$ tenemos p lugares de grado uno en $\mathbb{F}_q(x, y, z)$, dado que

$$\tau(x) = \text{m.c.d.}(d(x), \delta(x)) \neq 1,$$

existen por cada cero de $\tau(x)$, por lo menos $p \cdot r$ lugares de grado uno en E. Otros lugares racionales pueden obtenerse de la ramificación de $\mu(x)$ y $g(x)$.

□

En este trabajo desarrollaremos dos métodos que posibilitan la escogencia de un $g(x)$ apropiado.

Método 1.

Sea $\ell(x)$ como en la sección anterior, es decir $\ell(x) \in \mathbb{F}_q[x]$ con todos sus ceros en $\mathbb{F}_q$.

Si $t(x)$ y $\gamma(x) \in \mathbb{F}_q[x]$ son tales que $t(x)$ es un divisor de $\ell(x)$ y

$$\text{m.c.d}(\gamma(x)^p - \gamma(x), t(x)) = 1,$$

entonces existen polinomios $v(x)$ y $\omega(x)$ tales que

$$t(x)v(x) + (\gamma(x)^p - \gamma(x))\omega(x) = 1,$$

dividiendo por $\omega(x)$ obtenemos:

$$\frac{t(x)v(x)}{\omega(x)} + (\gamma(x)^p - \gamma(x)) = \frac{1}{\omega(x)}. \tag{3.7}$$

Ahora, si $\alpha \in \mathbb{F}_q$ es un cero de $t(x)$, entonces

$$0 = Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{t(\alpha)v(\alpha)}{\omega(\alpha)}\right) = Tr_{\mathbb{F}_q/\mathbb{F}_p}\left((\gamma(\alpha)^p - \gamma(\alpha)) + \frac{1}{\omega(\alpha)}\right),$$

por la linealidad de la traza y puesto que $Tr_{\mathbb{F}_q/\mathbb{F}_p}(\gamma(\alpha)^p - \gamma(\alpha)) = 0$, tenemos que $Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{1}{\omega(\alpha)}\right) = 0$ y en consecuencia por Teorema 3.1 existe $\zeta \in \mathbb{F}_{p^n}$ tal que

$$\zeta^p - \zeta = \frac{1}{\omega(\alpha)}. \tag{3.8}$$

Resumimos nuestro análisis en el siguiente resultado.

Proposición 3.4 Sean $\ell(x), t(x), \gamma(x)$ y $\omega(x)$ como antes, entonces el cuerpo de funciones algebraicas E_2 dado por la ecuación de Artin-Shreier

$$z^p - z = \frac{1}{\omega(x)} \tag{3.9}$$

tiene por lo menos $p \cdot \text{grad}(t(x))$ lugares de grado uno.

Observe que aún de acuerdo con la hipótesis de 3.4 debemos garantizar la existencia de un $\gamma(x) \in \mathbb{F}_q[x]$ tal que m.c.d. $(\gamma(x)^p - \gamma(x), t(x)) = 1$, esta existencia será justificada en el siguiente resultado.

Lema 3.1 Con las hipótesis de la Proposición 3.4, si $\gamma(x) = (x - \alpha)$ con $\alpha \in \mathbb{F}_q$, entonces

$$\text{m.c.d}\,(t(x), \gamma(x)^p - \gamma(x)) = 1.$$

Demostración. : Dado que $\gamma(x) = (x - \alpha)$ con $\alpha \in \mathbb{F}_q$ entonces

$$\gamma(x)^p - \gamma(x) = (x - \alpha)^p - (x - \alpha) = x^p - x.$$

Si suponemos que $mcd\,(t(x), \gamma(x)^p - \gamma(x)) \neq 1$ entonces $(x^p - x)|t(x)$ y puesto que $t(x)$ es un factor de $\ell(x)$, tenemos que $(x^p - x)|\ell(x)$, pero $\ell(x)$ es un polinomio irreducible

o producto de irreducibles sobre $\mathbb{F}_p$, con todos sus ceros en $\mathbb{F}_q \setminus \mathbb{F}_p$, entonces $x^p - x$ no puede dividir a $\ell(x)$ y en consecuencia

$$\text{m.c.d}\,(t(x), \gamma(x)^p - \gamma(x)) = 1.\square$$

En el siguiente ejemplo construiremos un cuerpo de funciones algebraicas sobre el cuerpo finito $\mathbb{F}_{16}$, con género 20 y 127 lugares racionales utilizando el método 1. No se conoce aún una curva (o su equivalente un cuerpo de funciones) sobre $\mathbb{F}_{16}$ de género 20 con más de 127 puntos racionales. [8]

Ejemplo 3.2 Sean $p = 2$, $n = 4$ y $f(x) = (x^2 + x + 1)^4 \in \mathbb{F}_{16}[x]$.

Si $\ell(x) = x^8 + x^7 + x^6 + x^4 + 1 = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) \in \mathbb{F}_{16}[x]$, entonces tenemos que $\mathcal{R}_\ell(f(x)) = x^6(x + 1)$.

Consideremos la Extensión de Kummer $E_1 = \mathbb{F}_{16}(x, y)$ de $\mathbb{F}_{16}(x)$ dada por la ecuación:

$$y^5 = \frac{f(x)}{\mathcal{R}_\ell(f(x))} = \frac{(x^2 + x + 1)^4}{x^6(x + 1)}.$$

Afirmamos que $E_1/\mathbb{F}_{16}$ tiene género 6 y 65 lugares de grado uno, es decir E_1 es un cuerpo de funciones maximal.

En efecto, dado que la extensión es de grado primo sólo ocurrirá ramificación total y por 1.4 los lugares correspondientes a $x = 0, x = 1, x = \infty$ y $x = \zeta_i$ con $\zeta_i^2 + \zeta_i + 1 = 0$ e $i = 1, 2$ (los cuales denotaremos por p_0, p_1, p_∞ y p_{ζ_i} respectivamente) son totalmente ramificados, luego el género está dado por

$$g(\mathbb{F}_{16}(x, y)/\mathbb{F}_{16}(x)) = 1 + 5(-1) + \frac{1}{2}\,(5(4)) = -4 + 10 = 6.$$

Para hallar el número de lugares de grado 1, resolvemos la congruencia (3.5) y obtenemos $d(x) = x^{12} + x^9 + x^6 + x^3 + 1$.

Observemos que $\ell(x) \cdot (x^4 + x^3 + 1) = d(x)$, donde los ceros del polinomio $x^4 + x^3 + 1$ aportan quintas potencias diferentes de 1.

Entonces tenemos que

$$\#N(\mathbb{F}_{16}(x, y)) = 12 \times 5 + 5 = 65.$$

Este Cuerpo de Funciones es Maximal puesto que

$$\#N(\mathbb{F}_{16}(x, y)) = q + 1 + 2g\sqrt{q} = 16 + 1 + 2(6)(4) = 65.$$

[8] Ver [5] y [13].

Ahora si $t(x) = x^4 + x + 1$ un factor de $\ell(x)$ y $\gamma(x) = x(x+1)^5$, es fácil comprobar que $t(x) \cdot ((x^3 + x + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)) + \Gamma(x) \cdot x(x^2 + x + 1) = 1$, donde hemos denotado por $\Gamma(x)$ al polinomio $\gamma(x)^p - \gamma(x)$. Ahora, tomemos $\omega(x) = x(x^2+x+1)$ y consideremos la extensión E_2 de E_1 dada por la ecuación de Artin-Schreier

$$z^2 + z = \frac{1}{\omega(x)} = \frac{1}{x(x^2 + x + 1)}.$$

De acuerdo con la Proposición 1.5 los únicos lugares que se ramifican son P_0 y P_{ζ_i}, los lugares correspondientes a P_∞ y P_1 son no ramificados. Veamos a manera de ilustración algunos cálculos:

$\nu_{P_0}\left(\frac{1}{\omega(x)}\right) = e(P_0|p_0) \cdot \nu_{p_0}\left(\frac{1}{\omega(x)}\right) = (5)(-1) = -5,$ luego $m_{P_0} = 5$

$\nu_{P_\infty}\left(\frac{1}{\omega(x)}\right) = e(P_\infty|p_\infty) \cdot \nu_{p_\infty}\left(\frac{1}{\omega(x)}\right) = (5)(3) = 15 \geq 0,$ luego $m_{P_\infty} = -1$

y por lo tanto, el género está dado por

$$g(\mathbb{F}_{16}(x, y, z)/\mathbb{F}_{16}(x)) = 2 \cdot 6 + \frac{1}{2}(-2 + 18) = 20.$$

Para el cálculo de lugares de grado uno, observe que existen 2 lugares que caen sobre P_∞ y P_1,(los cuales denotaremos por $\mathcal{P}_\infty$ y $\mathcal{P}_1$ respectivamente), estos lugares son de grado 1, así como también $\mathcal{P}_0$ y $\mathcal{P}_{\zeta_i}, i = 1, 2$ (por ser totalmente ramificados) por lo tanto tenemos 7 lugares de grado uno provenientes de los puntos de rama.

De otro lado,

$$\text{grad}(\delta(x)) = \text{grad}\left(\text{m.c.d}\left(Tr_{\mathbb{F}_{16}/\mathbb{F}_2}\left(\frac{1}{x(x^2 + x + 1)}\right), x^{16} + x\right)\right) = 13,$$

más precisamente

$$\delta(x) = x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^3 + x + 1,$$

y por lo tanto $\tau(x) := \text{m.c.d}\,(d(x), \delta(x)) = x^{12} + x^9 + x^6 + x^3 + 1$.

Ahora, puesto que el polinomio $\tau(x)$ coincide con el polinomio $d(x)$, tenemos que

$$\#N(E/\mathbb{F}_{16}(x)) = 5 \cdot 2 \cdot 12 + 7 = 127.\square$$

Ahora construiremos un cuerpo de funciones algebraicas sobre el cuerpo finito $\mathbb{F}_8$, con género 25 y 86 lugares de grado 1 utilizando el Método 1. No se conoce aún una curva (o su equivalente un cuerpo de funciones) sobre $\mathbb{F}_8$ de género 25 con más de 86 lugares de grado uno.

Ejemplo 3.3 Sean $p = 2,\ n = 3,$ y $f(x) = x^3(x+1)^3 \in \mathbb{F}_8[x]$.

Si $\ell(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x^2 + 1)(x^3 + x + 1) \in \mathbb{F}_8[x]$, entonces tenemos que $\mathcal{R}_\ell(x^3(x+1)^3) = x^2 + x + 1$.

Consideremos la Extensión de Kummer $E_1 = \mathbb{F}_8(x, y)$ de $\mathbb{F}_8(x)$ dada por la ecuación:

$$y^7 = \frac{x^3(x+1)^3}{x^2 + x + 1}.$$

Puesto que la extensión es de grado primo, sólo se presentará ramificación total, y por la Proposición 1.4 los lugares correspondientes a $x = 0, x = 1, x = \infty$ y $x = \zeta_i$ con $\zeta_i^2 + \zeta_i + 1 = 0$ e $i = 1, 2$ (denotados por p_0, p_1, p_∞ y p_{ζ_i}) son totalmente ramificados, luego el género está dado por

$$g(\mathbb{F}_8(x, y)/\mathbb{F}_8(x)) = 1 + 7(-1) + \frac{1}{2}(4(6)) = -6 + 12 = 6.$$

Para hallar el número de lugares de grado 1, resolvemos la congruencia (3.5) y obtenemos $d(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

Observemos que $\ell(x) = d(x)$, por lo tanto los ceros de $\ell(x)$ son los únicos lugares que aportan séptimas potencias.

Entonces tenemos que

$$\#N(\mathbb{F}_8(x, y)) = 6 \cdot 7 + 3 = 45.$$

Ahora si $\gamma(x) = x + 1$, se puede probar que

$$\ell(x) \cdot 1 + \Gamma(x) \cdot (x^2 + x + 1)^2 = 1,$$

donde $\Gamma(x)$ corresponde al polinomio $\gamma(x)^p - \gamma(x)$, ahora tomemos

$$\omega(x) = (x^2 + x + 1)^2$$

y consideremos la extensión E_2 de E_1 dada por la ecuación de Artin-Schreier

$$z^2 + z = \frac{1}{\omega(x)} = \frac{1}{(x^2 + x + 1)^2}.$$

De acuerdo con la Proposición 1.5 el único lugar totalmente ramificado es $P_{\zeta_i}, i = 1, 2$, los lugares correspondientes a P_∞, P_0 y a P_1 son no ramificados. Veamos a manera de ilustración algunos cálculos:

$$\nu_{P_0}\left(\frac{1}{\omega(x)}\right) = e(P_0|p_0) \cdot \nu_{p_0}\left(\tfrac{1}{\omega(x)}\right) = (7)(0) = 0, \qquad \text{luego } m_{P_0} = -1,$$

$$\nu_{P_\infty}\left(\frac{1}{\omega(x)}\right) = e(P_\infty|p_\infty) \cdot \nu_{p_\infty}\left(\tfrac{1}{\omega(x)}\right) = (7)(4) = 28, \quad \text{luego } m_{P_\infty} = -1.$$

Si tomamos $\eta = \dfrac{1}{\omega(x)}$, tenemos que

$\nu_{P_{\zeta_1}}\left(\dfrac{1}{\omega(x)} + \eta^2 + \eta\right) = e(P_{\zeta_1}|p_{\zeta_1}) \cdot \nu_{p_{\zeta_1}}\left(\frac{1}{\omega(x)} + \eta^2 + \eta\right) = (7)(-1) = -7.$

Luego $m_{P_{\zeta_1}} = 7$ y por lo tanto el género está dado por

$$g(\mathbb{F}_8(x,y,z)/\mathbb{F}_8(x)) = 2 \cdot 9 + \frac{1}{2}(-2+16) = 25.$$

Para el cálculo de lugares de grado uno, observemos que existen 2 lugares que caen sobre P_∞, P_1 y P_0 respectivamente y únicamente los lugares que caen sobre P_∞ son de grado 1 y sobre $P_{\zeta_i}, i = 1, 2$ cae un lugar que no es de grado 1, por lo tanto tenemos sólo 2 lugares de grado uno provenientes de los puntos de rama.

De otro lado $\text{grad}(\delta(x)) = \text{grad}\left(\text{m.c.d}\left(Tr_{\mathbb{F}_8/\mathbb{F}_2}\left(\dfrac{1}{(x^2+x+1)^2}\right), x^8 + x\right)\right)$, más precisamente

$$\delta(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

y por lo tanto $\tau(x) := \text{m.c.d}\,(d(x), \delta(x)) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

Puesto que el polinomio $\tau(x)$ coincide con el polinomio $d(x)$, tenemos que

$$\#N(E/\mathbb{F}_8(x)) = 6 \cdot 2 \cdot 7 + 2 = 86.\square$$

Método 2.

A lo largo de esta sección supondremos que $g(x) \in \mathbb{F}_q[x]$ con

$$Tr_{\mathbb{F}_q/\mathbb{F}_p}(g(\alpha)) = 0, \alpha \in \mathbb{F}_q,$$

$f(x)$ y $\ell_1(x) \in \mathbb{F}_q[x]$, tales que m.c.d $(\ell_1(x), f(x)) = 1$, con

$$\text{grad}(\ell_1(x)) \leq \text{grad}(f(x)),$$

y $\ell_1(x)$ un divisor de m.c.d $(Tr(g(x)), x^q - x)$ el cual denotaremos por $\ell(x)$, entonces por el algoritmo de la división existe $h(x) \in \mathbb{F}_q[x]$ tal que

$$f(x) = \ell_1(x) \cdot h(x) + \mathcal{R}_{\ell_1}(f(x)),$$

donde $\mathcal{R}_{\ell_1}(f(x))$ es el residuo de la división de $f(x)$ por $\ell_1(x)$.

Si definimos

$$\mu(x) = \frac{f(x)}{\mathcal{R}_{\ell_1}(f(x))}, \tag{3.10}$$

tenemos que todo $\alpha \in \vartheta_{\ell_1} := \{\alpha \in \mathbb{F}_q; \ell_1(\alpha) = 0\}$, satisface

$$\mu(\alpha) = \frac{f(\alpha)}{\mathcal{R}_{\ell_1}(f(x))(\alpha)} = 1.$$

Ahora consideremos

$$\delta(x) = \text{m.c.d.}(Tr_{\mathbb{F}_q/\mathbb{F}_p}(g(x)), x^q - x), d(x) = \text{m.c.d}(\mu(x)^{\frac{q-1}{r}} - 1, x^q - x),$$

y $\tau(x) = \text{m.c.d.}(d(x), \delta(x))$, como antes y observemos que $\ell(x) = \delta(x)$ y $\ell_1(x)$ es factor de $\delta(x), d(x)$ y $\tau(x)$ respectivamente, en consecuencia tenemos el siguiente resultado.

Proposición 3.5 Con las hipótesis establecidas en esta sección, tenemos que el cuerpo de funciones algebraicas $E = E_1E_2$ donde E_1 está dado por la ecuación de Kummer $y^r = \mu(x)$ y E_2 dado por la ecuación de Artin-Shreier $z^p - z = g(x)$ tendrá por lo menos $p \cdot r \cdot \text{grad}(\tau(x))$ lugares de grado 1, donde $\tau(x) = \text{m.c.d}(d(x), \delta(x))$.

A manera de ilustración tenemos:

Ejemplo 3.4 Sean $p = 2, n = 3, g(x) = x \in \mathbb{F}_8[x]$ con $Tr(g(x)) = x^4 + x^2 + x \in \mathbb{F}_8[x]$ y $\ell(x) = x^4 + x^2 + x = x(x^3 + x + 1) \in \mathbb{F}_8[x]$. Si $\ell_1(x) = x^3 + x + 1$ y $f(x) = (x^2 + x + 1)^2$ entonces $\mathcal{R}_{\ell_1}(f(x)) = x + 1$.

Consideremos la Extensión de Kummer $E_1 = \mathbb{F}_8(x, y)$ de $\mathbb{F}_8(x)$ dada por la ecuación:

$$y^7 = \frac{f(x)}{\mathcal{R}_\ell(f(x))} = \frac{(x^2 + x + 1)^2}{(x + 1)}.$$

Afirmamos que $E_1/\mathbb{F}_8$ tiene género 6 y 31 lugares de grado uno.

Puesto que la extensión es de grado primo, sólo se presentará ramificación total, y por la Proposición 1.4 los lugares correspondientes a $x = 1, x = \infty$ y $x = \zeta_i$ con $\zeta_i^2 + \zeta_i + 1 = 0$ e $i = 1, 2$ (denotados por p_1, p_∞ y p_{ζ_i}) son totalmente ramificados, luego el género está dado por

$$g(\mathbb{F}_8(x, y)/\mathbb{F}_8(x)) = 1 + 7(-1) + \frac{1}{2}(4(6)) = -6 + 12 = 6.$$

Para hallar el número de lugares de grado 1, resolvemos la congruencia (3.5) y obtenemos $d(x) = x^4 + x^2 + x$.

Observemos que $\ell(x) = d(x)$ por lo tanto los ceros de $\ell(x)$ son los únicos lugares que aportan séptimas potencias en $\mathbb{F}_8$.

Entonces tenemos que

$$\#N(\mathbb{F}_8(x, y)) = 4 \cdot 7 + 4 = 31.$$

Ahora consideremos la extensión E_2 de E_1 dada por la ecuación de Artin-Schreirer

$$z^2 + z = x.$$

De acuerdo con la Proposición 1.5 el único lugar totalmente ramificado es P_∞ y los lugares correspondientes a P_0, P_1 y a P_{ζ_i} para $i = 1, 2$ son no ramificados. Veamos a manera de ilustración algunos cálculos:

$\nu_{P_0}(g(x)) = e(P_0|p_0) \cdot \nu_{p_0}(g(x)) = (1)(1) = 1$, luego $m_{P_0} = -1$
$\nu_{P_\infty}(g(x)) = e(P_\infty|p_\infty) \cdot \nu_{p_\infty}(g(x)) = (7)(-1) = -7$, luego $m_{P_\infty} = 7$.

y por lo tanto el género está dado por

$$g(\mathbb{F}_8(x, y, z)/\mathbb{F}_8(x)) = 2 \cdot 6 + \frac{1}{2}(-2 + 8) = 15.$$

Para el cálculo de lugares de grado uno, observemos que existen 2 lugares que caen sobre cada uno de los 7 lugares que caen sobre p_0, 2 lugares que caen sobre P_1 y $P_{\zeta_i}, i = 1, 2$ respectivamente y solamente un lugar que cae sobre P_∞ que además es el único de grado 1, por lo tanto tenemos sólo un lugar de grado uno proveniente de los puntos de rama.

De otro lado, por la escogencia de $g(x)$ tenemos que $\delta(x) = \ell(x)$ y por lo tanto

$$\tau(x) = x^4 + x^2 + x.$$

Puesto que el polinomio $\tau(x)$ coincide con el polinomio $\ell(x)$, tenemos que

$$\#N(E/\mathbb{F}_8(x)) = 4 \cdot 2 \cdot 7 + 1 = 57.$$

No se conoce aún una curva (o su equivalente un cuerpo de funciones) sobre $\mathbb{F}_8$ de género 15 con más de 57 lugares de grado uno.

Ejemplo 3.5 Sean $p = 2, n = 6, g(x) = \dfrac{x+1}{x} \in \mathbb{F}_{64}[x]$ con

$$Tr(g(x)) = \frac{1}{x^{32}} + \frac{1}{x^{16}} + \frac{1}{x^8} + \frac{1}{x^4} + \frac{1}{x^2} + \frac{1}{x} \in \mathbb{F}_{64}[x] \text{ y}$$

$$\begin{aligned} \ell(x) &= x(x+1)(x^3+x+1)(x^3+x^2+1)(x^6+x^3+1)(x^6+x^5+1) \\ &\quad (x^6+x^5+x^3+x^2+1)(x^6+x^5+x^4+x^2+1) \in \mathbb{F}_2[x]. \end{aligned}$$

Si $\ell_1(x) = x^6 + x^5 + 1$ y $f(x) = (x^2 + x)^6$ entonces $\mathcal{R}_{\ell_1}(f(x)) = 1$.

Consideremos la Extensión de Kummer $E_1 = \mathbb{F}_{64}(x, y)$ de $\mathbb{F}_{64}(x)$ dada por la ecuación:

$$y^9 = \frac{f(x)}{\mathcal{R}_{\ell_1}(f(x))} = x^5(x+1).$$

Afirmamos que $E_1/\mathbb{F}_{64}$ es maximal puesto que tiene género 3 y 113 lugares de grado uno.

Puesto que la extensión no es de grado primo, se presentará ramificación débil y total, y por la Proposición 1.4 los lugares correspondientes a $x = 0, x = 1$ (denotados por p_0 y p_1) son totalmente ramificados y el lugar correspondiente a $x = \infty$ denotado por p_∞ es débilmente ramificado, luego el género está dado por

$$g(\mathbb{F}_{64}(x, y)/\mathbb{F}_{64}(x)) = 1 + 9(-1) + \frac{1}{2}(2(8) + 3(2)) = 3.$$

Para hallar el número de lugares de grado 1, resolvemos la congruencia (3.5) y obtenemos

$$d(x) = x^{12} + x^6 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x + 1)(x^3 + x^2 + 1)(x^6 + x^5 + 1).$$

Observemos que $\ell_1(x)$ es un factor de $d(x)$.

Entonces tenemos que

$$\#N(\mathbb{F}_{64}(x, y)) = 12 \cdot 9 + 5 = 113.$$

Ahora consideremos la extensión E_2 de E_1 dada por la ecuación de Artin-Schreirer

$$z^2 + z = \frac{x+1}{x}.$$

De acuerdo con la Proposición 1.5 el único lugar totalmente ramificado es P_0 y los lugares correspondientes a P_∞ y P_1 son no ramificados. Veamos a manera de ilustración algunos cálculos:

$\nu_{P_0}(g(x)) = e(P_0|p_0) \cdot \nu_{p_0}(g(x)) = (9)(-1) = -9$, luego $m_{P_0} = 9$.
$\nu_{P_\infty}(g(x)) = e(P_\infty|p_\infty) \cdot \nu_{p_\infty}(g(x)) = (3)(0) = 0$, luego $m_{P_\infty} = -1$.

y por lo tanto el género está dado por

$$g(\mathbb{F}_{64}(x, y, z)/\mathbb{F}_{64}(x)) = 2 \cdot 3 + \frac{1}{2}(-2 + 10) = 10.$$

Para el cálculo de lugares de grado uno, observemos que existen 2 lugares que caen sobre cada uno de los 3 lugares correspondientes a P_∞, 2 lugares que caen sobre P_1 y únicamente un lugar que cae sobre P_0 y todos son de grado 1, por lo tanto tenemos 9 lugares de grado uno provenientes de los puntos de rama.

De otro lado, por la escogencia de $\ell(x)$ tenemos que $\ell_1(x)|\delta(x)$ y $d(x)|\delta(x)$ por lo tanto $\tau(x) = (x^3+x+1)(x^3+x^2+1)(x^6+x^5+1)$ y el número de lugares de grado 1 está dado por

$$\#N(E/\mathbb{F}_{64}(x)) = 12 \cdot 2 \cdot 9 + 9 = 225.$$

Este Cuerpo de Funciones es Maximal puesto que

$$\#N(\mathbb{F}_{64}(x,y,z)) = q + 1 + 2g\sqrt{q} = 64 + 1 + 2(10)(8) = 65.$$

□

Bibliografía

[1] Fulton W., *Algebraics curves, Benjamin,1969.*

[2] Garzón A., *A Construction of Curves over Finite Fields with many rational points, Tesse de Doutorado, IMPA Agosto 2001.*

[3] A. Garcia and H. Stichtenoth , *A Class of Polynomials over Finite Fields*, Finite Fields and their Appl. 5 (1999), 424-435.

[4] G van der Geer and M. van der Vlugt, *Kummer Covers with many Rational Points*, Finite Fields and their Appl. 6 (2000), 327-341.

[5] Van der Geer G. and Van der Vlugt M., *Tables for the function* $N_q(g)$, available at http://www.wins.uva.nl/ geer.

[6] Goppa V. D., *Codes on algebraic curves.* Sov. Math. Dokl.24 (1981), p 170-172.

[7] Hartshorne R., *Algebraic geometry* Graduate text in mathematics, vol 52, Springer-Verlag,1977.

[8] Ihara Y.,*Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Tokyo 28 (1981), p 721-724.

[9] Lild R. and Niederreiter H., *Finite Fields and Applications*, Cambridge Univ. Press, Cambridge, 1994.

[10] Roman S. , *Field Theory* , Springer-Verlag, 1995.

[11] Serre J-P., *Sur le nombre de points rationnels dúne courbe alge'brique sur un cops fini.* C.R.Sci. Paris 296, Serie I (1993) p. 397-402.

[12] Stichtenoth H. , *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.

[13] Shabat V., *Tables of curves with many points*, available at http://www.wins.uva.nl/ shabat/tables.html.