Universidad Nacional Autónoma de México

Facultad de Ciencias

Algunas propiedades de una curva sobre un campo finito

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
MATEMÁTICO

PRESENTA:
ERIK MARTIN HESS FRIELING

DIRECTOR DE TESIS:
RODOLFO SAN AGUSTÍN CHI

2013

1.Datos del alumno

Apellido paterno	Hess
Apellido materno	Frieling
Nombre(s)	Erik Martin
Teléfono	55 55 55 76 57
Universidad	Universidad Nacional Autónoma de México
Facultad o escuela	Facultad de Ciencias
Carrera	Matemáticas
Número de cuenta	304500219

2. Datos del tutor

Grado	Dr.
Nombre(s)	Rodolfo
Apellido paterno	San Agustín
Apellido materno	Chi

3. Datos del sinodal 1

Grado	Dr.
Nombre(s)	Felipe de Jesús
Apellido paterno	Zaldivar
Apellido materno	Cruz

4. Datos del sinodal 2

Grado	Dr.
Nombre(s)	Alberto León
Apellido paterno	Kushner
Apellido materno	Schnur

5. Datos del sinodal 3

Grado	M. en C
Nombre(s)	Rolando
Apellido paterno	Gómez
Apellido materno	Macedo

6. Datos del sinodal 4

Grado	Dra.
Nombre(s)	Adriana
Apellido paterno	Ortiz
Apellido materno	Rodríguez

7.Datos del trabajo escrito.

Título	Algunas propiedades de una curva sobre un campo finito
Número de páginas	32 p.
Año	2013

Quisiera dedicarle esta tesis a
mi mamá Andrea Hess,
mi papá Peter Hess,
mis hermanos Kristopher y Steffen,
mis abuelos Ria y Heinz Frieling
mis abuelos Anna y Anton Hess
y mi novia Andrea Muñoz.
Gracias por su apoyo y amor que me han brindado.

Quisiera agradezerle a:
Octavio Páez
por ayudarme a encontrar mi camino académico
y mis sinodales por sus consejos.

También quisiera agradecerle a
toda mi familia
y mis amigos
en especial a:
Jasmin, Raul, Arturo y Fernanda
por los buenos tiempos.

Índice general

Introducción

En este trabajo describiremos algunas propiedades de la familia de curvas $y^{q^2} - y = x^N$ sobre el campo finito $\mathbb{F}_{q^{2n}}$ con $N := \dfrac{q^n + 1}{q + 1}$, q una potencia de un primo y $n \geq 3$ impar. Esta es una familia de curvas se puede encontrar en [1] donde se demuestra quee ésta es máximas. El interés de estudiar curvas con esta propiedad viene de la teoría de códigos correctores de errores. Ésto se debe a que con éstas curvas se pueden construir códigos de gran longitud, respecto al tamaño del alfabeto. Éstos códigos asociados a las curvas máximas, tendrán buenos parámetros, como una distancia mínima grande. Una distancia mínima grande permite corregir una mayor cantidad de errores.

Tomamos esta curva, ya que se ve en [1], que esta es máxima. Esta propiedad es importante, ya que una curva máxima alcanza la cota de Hasse-Weil. Eso quiere decir que la curva va a tener el mayor número de puntos posible sobre un campo finito.

En este trabajo definiremos una forma de construir diseños partiendo de una curva dada. Aplicar este método en la curva y la vamos a comparar con otros dos diseños que corresponden a la curva hermitiana y la curva de Fermat.

En el capítulo 1 enunciaremos los teoremas que usaremos en este trabajo. Antes de eso daremos las definiciones, teoremas y proposiciones para poder entender la herramienta que nos será útil. Los resultado aqui vistos, se pueden consultar principalmente en [4]. El teorema 1.62 se podra consultar en cualquier libro de teoría de números.

En el capítulo 2 calcularemos el género de la curva con la ayuda de los divisores principales de x y y. Estos también los encontraremos en ese capítulo. En [1] el género se calcula usando extensiones de Kummer, a diferencia de como lo calcularemos nosotros.

En el capítulo 3 daremos una forma de construir un diseño a partir de una curva. De esta forma construiremos el diseño correspondiente a la curva mencionada. También construiremos los diseños correspondientes a la curva hermitiana, que se menciaona el la introducción de [1] y a una curva de tipo Fermat, que se puede encontrar en [5]. Éstas dos curvas las definiremos en el momento que las necesitemos. Estas curvas también se pueden consultar en [1]. Los diseños combinatorios también sirven para poder construir códigos correctores de errores, usando la matriz de incidencia del diseño como matriz generadora o matriz de verificación del código.

En el capítulo 4 compararemos los tres diseños construídos en el capítulo anterior.

En el capítulo 5 buscaremos los automorfismos sobre esta curva. Los automorfismos de una curva también son interesantes en la teoría de códigos correctores de errores, ya que éstos se pueden traducir a los automorfismos del código asociado a la curva.

Capítulo 1

Generalidades de campos de funciones

En este capítulo enunciaremos los resultados que vamos a necesitar en este trabajo. Sólo demostraremos los resultados que usaremos y consideramos importantes para este trabajo. Las demostraciones de los resultados que no demostramos aquí, se pueden consultar principalmente en las secciones 1 a 7 del primer capítulo y la sección 1 del tercer capítulo de [4]. El teorema 1.62 se puede encontrar en varios cualquier libro de teoría de números y a demostración del teorema 1.63 se puede encontrar en la segunda sección del quinto capítulo. El lema 1.64, se puede encontrar en el apéndice A de [4] y el teorema de Kummer que aquí usamos, es el corolario III.3.8. del mismo libro.

Suponemos que el lector tiene un conocimiento de la teoría de campos. A lo largo de este capítulo, K será un campo arbitrario y A^* denotará en grupo de unidades del anillo A.

Definición 1.1. *Un campo de funciones algebraicas F/K en una variable es una extensión F del campo K tal que F es una extensión finita de $K(x)$ para algún $x \in F$ trascendente sobre K.*

Si F es una extensión de K, entonces $\tilde{K} := \{x \in F | x \text{ es algebraico en } K\}$ se llama el campo de constantes de F/K. El campo K será algebraicamente cerrado en F si $K = \tilde{K}$.

Definición 1.2. *Un anillo de valuación del campo de funciones F/K es un anillo $\mathcal{O}$ que cumple:*

1. *$K \subset \mathcal{O} \subset F$.*
2. *Para todo $x \in F$, $x \in \mathcal{O}$ o bien $x^{-1} \in \mathcal{O}$.*

Proposición 1.3. *Sea $\mathcal{O}$ un anillo de valuación del campo de funciones F/K. Entonces se tiene que:*

1. *$\mathcal{O}$ tiene un único ideal máximo $P = \mathcal{O} \setminus \mathcal{O}^*$.*
2. *Para $x \in F$ y $x \neq 0$ se cumple que $x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$.*
3. *Para $\tilde{K}$ de F/K se tiene que $\tilde{K} \subseteq \mathcal{O}$ y $\tilde{K} \cap P = \{0\}$.*

Teorema 1.4. *Sea $\mathcal{O}$ un anillo de valuación del campo de funciones F/K y sea P su ideal máximo. Entonces se tiene que:*

1. *P es un ideal principal.*
2. *Si $P = t\mathcal{O}$ entonces cualquier $x \in F \setminus \{0\}$ tiene una representación única de la forma $x = t^n u$ para algún $n \in \mathbb{Z}$, $u \in \mathcal{O}^*$.*
3. *$\mathcal{O}$ es un dominio de ideales principales. En particular, si $P = t\mathcal{O}$ y $\{0\} \neq I \subseteq \mathcal{O}$ es un ideal, entonces $I = t^n\mathcal{O}$ para algún $n \in \mathbb{N}$.*

Definición 1.5. *Se tienen las siguientes definiciones:*

1. *Un lugar P del campo de funciones F/K es el ideal máximo de algún anillo de valuación $\mathcal{O}$ de F/K. Cualquier elemento $t \in P$ tal que $P = t\mathcal{O}$ se llama elemento primo o parámetro uniformizador de P.*

2. *$\mathbb{P}_F$ es el conjunto de todos los lugares de F/K.*

Si $\mathcal{O}$ es un anillo de valuación con ideal máximo P, entonces $\mathcal{O}$ está determinado únicamente por P, de la forma $\mathcal{O} = \{x \in F | x^{-1} \notin P\}$. Entonces llamamos a $\mathcal{O}_P := \mathcal{O}$ el anillo de valuación de P.

Definición 1.6. *Una valuación discreta de F/K es una función $v : F \to \mathbb{Z} \cup \{\infty\}$ que cumple las siguientes propiedades:*

1. $v(x) = \infty \Leftrightarrow x = 0$.

2. $v(xy) = v(x) + v(y)$ *para todo* $x, y \in F$.

3. $v(x + y) \geq \text{mín}\{v(x), v(y)\}$ *para todo* $x, y \in F$.

4. $\exists z \in F$ *tal que* $v(z) = 1$.

5. $v(k) = 0 \quad k \in K \setminus \{0\}$.

A la propiedad 3 de esta definición se le llama "desigualdad ultramétrica".

Lema 1.7. *Sea v una valuación discreta de F/K y $x, y \in F$ tales que $v(x) \neq v(y)$. Entonces $v(x + y) = \text{mín}\{v(x), v(y)\}$.*

Definición 1.8. *Se le asocia a todo lugar $P \in \mathbb{P}_F$ una función $v_P : F \to \mathbb{Z} \cup \{\infty\}$, de la siguiente forma:*

Sea t un elemento primo de P, entonces todo $x \in F \setminus \{0\}$ tiene una representación única $x = t^n u$ con $u \in \mathcal{O}_P^*$ y $n \in \mathbb{Z}$. Se define $v_P(x) := n$ y $v_P(0) := \infty$. Es fácil de ver que esta definición solo depende de la elección de P y no de t.

Lema 1.9. *La función de la definición anterior es una valuación de F/K.*

Teorema 1.10. *Sea F/K un campo de funciones.*

1. *Para todo lugar $P \in \mathbb{P}_F$ se tiene:*

   - $\mathcal{O}_P = \{x \in F | v_P(x) \geq 0\}$.
   - $\mathcal{O}_P^* = \{x \in F | v_P(x) = 0\}$.
   - $P = \{x \in F | v_P(x) > 0\}$.

2. *Un elemento $x \in F$ es un elemento primo de P si y sólo si $v_P(x) = 1$.*

3. *Si v es una valuación de F/K, entonces el conjunto $P := \{x \in F | v(x) > 0\}$ es un lugar en F/K y $\mathcal{O}_P = \{x \in F | v_P(x) \geq 0\}$ es su anillo de valuación correspondiente.*

4. *Un anillo de valuación $\mathcal{O}$ de F/K es un subanillo máximo de F.*

Definición 1.11. *Sea $P \in \mathbb{P}_F$.*

1. *$F_P := \mathcal{O}_P/P$ es el campo residual de P. La función $F \to F_P \cup \{\infty\}$ con $x \mapsto x(P)$, se llama el morfismo residual respecto a P. También se usa la notación $x + P := x(P)$, para $x \in \mathcal{O}_P$.*

2. *$degP := [F_P : K]$ se llama grado de P.*

Como $K \subseteq \tilde{K} \subseteq \mathcal{O}_P$, esta última definición tiene sentido ya que F_P es extensión de K.

Proposición 1.12. *Si P es un lugar de F/K y $0 \neq x \in P$, entonces se tiene que*

$$degP \leq [F : K(x)] < \infty$$

.

Corolario 1.13. *El campo de constantes de F/K es una extensión finita de K.*

Definición 1.14. *Sean $x \in F$ y $P \in \mathbb{P}_F$. Se dice que P:*

1. *es un cero de orden m de x si $v_P(x) = m > 0$,*
2. *es un polo de orden m de x si $v_P(x) = -m > 0$.*

Teorema 1.15. *Sean F/K un campo de funciones y A un subanillo de F tal que $K \subseteq A \subseteq F$. Si $\{0\} \neq I \subset A$ es un ideal propio de A, entonces existe un lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ y $A \subseteq \mathcal{O}_P$.*

Corolario 1.16. *Sean F/K un campo de funciones, $x \in F$ trascendente sobre K, entonces x tiene al menos un cero y un polo. En particular $\mathbb{P}_F \neq \emptyset$.*

Teorema 1.17. ***(Aproximación débil)*** *Sean F/K un campo de funciones, $P_1, \ldots, P_n \in \mathbb{P}_F$ lugares distintos de F/K, $x_1, \ldots, x_n \in F$ y $r_1, \ldots, r_n \in \mathbb{Z}$. Entonces existe $x \in F$ tal que*

$$v_{P_i}(x - x_i) = r_i \quad para\ i = 1, \ldots n$$

.

Demostración. Sea $v_i := v_{P_i}$. Para demostrar este teorema es necesario demostrar 3 afirmaciones.

Afirmación 1 Existe $u \in F$ con $v_1(u) > 0$ y $v_i(u) < 0$ para $i = 2, \ldots, n$.

La demostración de esta afirmación es por inducción sobre n. Para $n = 2$ se puede observar que $\mathcal{O}_{P_1} \nsubseteq \mathcal{O}_{P_2}$ y viceversa ya que los anillos de valuación son subanillos máximos propios de F. Por lo tanto se pueden encontrar $y_1 \in \mathcal{O}_{P_1} \backslash \mathcal{O}_{P_2}$ y $y_2 \in \mathcal{O}_{P_2} \backslash \mathcal{O}_{P_1}$. Entonces $v_1(y_1) \geq 0$, $v_2(y_1) < 0$, $v_1(y_2) < 0$ y $v_2(y_2) \geq 0$. La función $u := y_1/y_2$ es tal que $v_1(u) \geq 0$ y $v_2(u) < 0$ como se quería.

Para $n > 2$ se tiene, por hipótesis de inducción, un elemento $y \in F$ con $v_1(y) > 0$, $v_2(y) < 0, \ldots, v_{n-1}(y) < 0$. Si sucede que $v_n(y) \geq 0$ se escoge z con $v_1(z) > 0$ y $v_n(z) \geq 0$ y se hace $u := y + z^r$. Aquí $r \geq 1$ se escoge de tal manera que $rv_i(z) \neq v_i(y)$ para $i = 1, \ldots, n-1$. Se sigue que $v_1(u) \geq min\{v_1(y), r \cdot v_1(z)\} > 0$ y $v_i(u) \geq min\{v_i(y), r \cdot v_i(z)\} < 0$ para $i = 2, \ldots, n$. Esto demuestra la primera afirmación.

Afirmación 2 Existe una función $w \in F$ tal que $v_1(w-1) > r_1$ y $v_i(w) > r_i$ para $i = 2, \ldots, n$.

Para demostrar esta afirmación, se escoge $u \in F$ como en la primera afirmación y se hace $w := (1 + u^s)^{-1}$. Se tiene que, para una $s \in \mathbb{N}$ suficientemente grande,

$$v_1(w - 1) = v_1(-u^s(1 + u^s)^{-1}) = sv_1(u) > r_1$$

y

$$v_i(w) = -v_i(1 + u^s) = -s \cdot v_i(u) > r_i \text{ para } i = 2, \ldots, n$$

.

Afirmación 3 Dadas $y_1, \ldots, y_n \in F$ existe un elemento $z \in F$ tal que $v_i(z - y_i) > r_i$ para $i = 1, \ldots, n$. Escogiendo $s \in \mathbb{Z}$ tal que $v_i(y_j) \geq s$ para todas $i, j \in \{1, \ldots, n\}$. Por la afirmación 2 (aplicada n veces) existen $w_1, \ldots, w_n \in F$ con

$$v_i(w_i - 1)) > r_i - s \text{ y } v_i(w_j) > r_i - s \text{ para } j \neq i.$$

Entonces la función $z := \sum_{j=1}^{n} y_j w_j$ es la buscada.

Con la tercera afirmación demostrada, se puede demostrar el teorema: Por la tercera afirmación se puede encontrar $z \in F$ con $v_i(z - x_i) > r_i$, $i = 1, \ldots, n$. Se escogen funciones z_i con $v_i(z_i) = r_i$. De nuevo por la afirmación 3 existe $z' \in F$ con $v_i(z' - z_i) > r_i$ para $i = 1, \ldots, n$. Se sigue que

$$v_i(z') = v_i((z' - z_i) + z_i) = min\{v_i(z' - z_i), v_i(z_i)\} = r_i.$$

Sea $x := z + z'$. Entonces

$$v_i(x - x_i) = v_i((z - x_i) + z') = min\{v_i(z - x_i), v_i(z')\} = r_i.$$

q.e.d

Corolario 1.18. *Todo campo de funciones tiene un número infinito de lugares.*

Proposición 1.19. *Sea F/K un campo de funciones y $P_1, \ldots, P_n \in \mathbb{P}_F$ ceros de un elemento $x \in F$, entonces*

$$\sum_{i=1}^{n} v_{P_i} \cdot \deg P_i \leq [F : K(x)].$$

Corolario 1.20. *Cualquier elemento distinto de cero del campo de funciones F/K, tiene un número finito de ceros y polos.*

A partir de ahora F/K denotará a un campo de funciones algebraicas en una variable tal que K es el campo de constantes de F/K; i.e. K será algebraicamente cerrado en F.

Definición 1.21. *Se define $\mathcal{D}_F$ como el grupo libre abeliano generado por los lugares de F/K y se le llama grupo de divisores de F/K. Los elementos de $\mathcal{D}_F$ se llaman divisores de F/K.*

Usaermos la siguiente notación para los elementos de $\mathcal{D}_F$:

$$D = \sum_{P \in \mathbb{P}_F} n_P P \text{ con } n_P \in \mathbb{Z} \text{ y casi todos los } n_P = 0.$$

Definición 1.22. *Dos divisores de suman coeficiente a coeficiente, i.e. si $D = \sum_{P \in \mathbb{P}_F} n_P P$ y $D' = \sum_{P \in \mathbb{P}_F} n'_P P$, entonces*

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P.$$

Los divisores cumplen lo siguiente:

1. El inverso de $D = \sum_{P \in \mathbb{P}_F} n_P P$ se denota $-D$ y es de la forma $-D = \sum_{P \in \mathbb{P}_F} -n_P P$.
2. El elemento cero es el divisor $0 := \sum_{P \in \mathbb{P}_F} r_P P$ con $r_P = 0$.
3. Se extiende la definición de valoración a $\mathcal{D}_F$ de la siguiente manera: $v_Q(D) := n_Q$ con $Q \in \mathbb{P}_F$. Se puede escribir cualquier divisor de la siguiente forma:

   $$D = \sum_{P \in suppD} v_P(D) \cdot P$$

   donde $suppD := \{P \in \mathbb{P}_F | n_P \neq 0\}$ es el soporte del divisor.
4. Se define un orden parcial en el grupo $\mathcal{D}_F$ de la siguiente forma:

   $$D_1 \leq D_2 \Leftrightarrow v_P(D_1) \leq v_P(D_2) \quad \textit{para todo } P \in \mathbb{P}_F.$$

5. Un divisor que cumpla $D \geq 0$ se llama divisor efectivo (o positivo).

6. El grado de un divisor se define de la siguiente manera:

$$\deg D := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot \deg P.$$

7. Al divisior $D = P$ con $P \in \mathbb{P}_F$ se le llama divisor primo.

Definición 1.23. *Sea $x \in F$ distinto de cero. Se denota al conjunto de ceros de x por Z y al conjunto de polos de x por N. Entonces se define:*

- $(x)_0 := \sum_{P \in Z} v_P(x)P$ *el divisor de ceros de x.*
- $(x)_\infty := \sum_{P \in N} (-v_P(x))P$ *el divisor de polos de x.*
- $(x) := (x)_0 - (x)_\infty$ *el divisor principal de x.*

Estas tres definiciones tienen sentido, por el corolario 1.20.

Definición 1.24. *$\mathcal{P}_F := \{(x) | 0 \neq x \in F\}$ se llama el grupo de divisores principales de F/K.*

Se tiene lo siguiente:

- Se sigue que $\mathcal{P}_F$ es subgrupo normal de $\mathcal{D}_F$, ya que $\mathcal{D}_F$ es abeliano. Con esto definimos

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

  y se llamará el grupo de clases de divisores.

- Si $[D] \in \mathcal{C}_F$ ($[D]$ es la clase del divisior D), entonces dos divisores $D, D' \in \mathcal{D}_F$ son equivalentes ($D \sim D'$) si y sólo si $[D] = [D']$, i.e. $D = D' + (x)$ para algún $x \in F$ distinto de cero.

La relación dada en el punto anterior es una relación de equivalencia y motiva la siguiente definición:

Definición 1.25. *Para un divisor D de F se define el conjunto:*

$$\mathcal{L}(D) := \{x \in F | (x) \geq -D\} \cup \{0\}.$$

Comentarios:

- Si el divisor D tiene la forma:

$$D = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$$

  con $n_i > 0$ y $m_j > 0$, entonces $\mathcal{L}(D)$ consiste de los elementos $x \in F$ tales que:

  1. x tiene ceros de orden mayor o igual a m_j en Q_j para $j = 1, \ldots s$.
  2. x solo puede tener polos en los lugares $P_1, \ldots, P_r$ con orden no mayor a n_i en P_i.

- Si $D \in \mathcal{D}_F$, entonces:

  1. $x \in \mathcal{L}(D) \Leftrightarrow v_P(x) \geq -v_P(D)$ para todo $P \in \mathbb{P}_F$.
  2. $\mathcal{L}(D) \neq \{0\} \Leftrightarrow$ existe un divisor $D' \sim D$, con $D' \geq 0$.

Lema 1.26. *Sea $D \in \mathcal{D}_F$, entonces se tiene que:*

1. *$\mathcal{L}(D)$ es un espacio vectorial sobre K.*

2. *Si D' es un divisor equivalente a D, entonces $\mathcal{L}(D)$ y $\mathcal{L}(D')$ son isomorfos como espacios vectoriales sobre K.*

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

4. *Si $D < 0$, entonces $\mathcal{L}(D) = \{0\}$.*

Lema 1.27. *Sean D y D' divisores de F/K con $D \leq D'$. Entonces se tiene que $\mathcal{L}(D) \subseteq \mathcal{L}(D')$ y $\dim(\mathcal{L}(D')/\mathcal{L}(D)) \leq \deg D' - \deg D$.*

Proposición 1.28. *Para cualquier divisor $D \in \mathcal{D}_F$, el espacio $\mathcal{L}(D)$ es un espacio vectorial sobre K de dimensión finita. Más aún si $D = D_1 - D_2$, con D_1 y D_2 divisores positivos, entonces*

$$dim\mathcal{L}(D) \leq degD_1 + 1.$$

Definición 1.29. *Para $D \in \mathcal{D}_F$, $dimD := dim\mathcal{L}(D)$ se llama la dimensión del divisor D.*

Con esta definición se puede hablar de la dimensión de la clase de D.

Teorema 1.30. *Sea $x \in F$ pero $x \notin K$. Sean $(x)_0$ y $(x)_\infty$ el divisor de ceros de x y el divisor de polos de x respectivamente. Entonces:*

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

Corolario 1.31.

1. *Sean D y D' con $D \sim D'$. Entonces se tiene $dimD = dimD'$ y $degD = degD'$.*

2. *Si $degD < 0$, entonces $dimD = 0$.*

3. *Para un divisor D de grado cero las siguientes afirmaciones son equivalentes:*

   a) *D es principal.*
   b) *$dimD \geq 1$.*
   c) *$dimD = 1$.*

Proposición 1.32. *Existe una constante $\gamma \in \mathbb{Z}$ tal que para todo divisor $D \in \mathcal{D}_F$ se tiene que*

$$degD - dimD \leq \gamma.$$

Es necesario mencionar en este punto que la constante γ, mencionada en la propocision anterior, no depende del divisor que se tome. Depende únicamente del campo de funciones. Con ayuda de esta constante, la siguiente definición tiene sentido.

Definición 1.33. *El género g de F/K se define de la siguiente forma:*

$$g := max\{degD - dimD + 1 | D \in \mathcal{D}_F\}.$$

El género es un número entero no negativo.

Teorema 1.34. ***(Riemann)***
Sea F/K un campo de funciones con género g.

1. *Para todo divisor $D \in \mathcal{D}_F$*
$$dimD \geq degD + 1 - g$$
.

2. *Existe un entero c tal que*
$$dimD = degD + 1 - g \text{ para todo divisor } D \text{ que cumple } degD \geq c$$
.

Demostración. 1. Esto sigue de la definición de género.

2. Sea D_0 un divisor tal que $g = degD_0 - dimD_0 + 1$ y sea $c := degD_0 + g$. Si $degD \geq c$, se tiene que
$$dim(D - D_0) \geq deg(D - D_0) + 1 - g \geq c - degD_0 + 1 - g \geq 1$$
Por lo tanto existe un elemento $x \in \mathcal{L}(D - D_0)$, distinto de cero. Se considera ahora el divisor $D' := D + (x)$, que es $\geq D_0$. Ahora se tiene:
$$\begin{aligned} degD - dimD &= degD' - dimD' \\ &\geq degD_0 - dimD_0 \\ &= g - 1. \end{aligned} \tag{1.1}$$

q.e.d

Definición 1.35. *Se tienen las siguientes definiciones:*

1. *Para $D \in \mathcal{D}_F$, el índice de especialidad se define como:*
$$i(D) = dimD - degD + g - 1.$$
2. *Un adele de F/K es una función $\alpha : \mathbb{P}_F \to F$ con $P \mapsto \alpha_P$ tal que $\alpha_P \in \mathcal{O}_P$ para casi todo $P \in \mathbb{P}_F$. Un adele se puede ver como un elemento del producto directo $\prod_{P \in \mathbb{P}_F} F$.*
3. *$\mathcal{A}_F := \{\alpha | \alpha$ es un adele de $F/K\}$ que será un K-espacio vectorial.*
4. *Sea $x \in F$. El adele α tal que $\alpha_P = x$ para todo $P \in \mathbb{P}_F$, se llama adele principal de x.*

Esta última definición tiene sentido, ya que sabemos que por el corolario 1.20 sólo hay un número finito de lugares P que cumplen que $v_P(x) < 0$. Esto implica, por el teorema 1.10, que sólo hay un número finito de entradas del adele que cumplen que $x \notin \mathcal{O}_P$. Esto nos da una inclusión de F en $\mathcal{A}_F$. Las valuaciones en F se pueden extender a $\mathcal{A}_F$ definiendo $v_P(\alpha) := v_P(\alpha_P)$

Definición 1.36. *Sea $D \in \mathcal{D}_F$. Se define*
$$\mathcal{A}_F(D) := \{\alpha \in \mathcal{A}_F | v_P(\alpha) \geq -v_P(D) \text{ para todo } P \in \mathbb{P}_F\}.$$

Lema 1.37. *Sean $D_1, D_2 \in \mathcal{D}_F$ con $D_1 \leq D_2$. Entonces $\mathcal{A}_F(D_1) \subseteq \mathcal{A}_F(D_2)$ y*
$$dim(\mathcal{A}_F(D_2)/\mathcal{A}_F(D_1)) = grado(D_2) - grado(D_1).$$

Los siguiente, nos ayudará a demostrar el siguiente teorema.
Vemos que la sucesión
$$\begin{aligned} 0 \to \mathcal{L}(D_2)/\mathcal{L}(D_1) &\to \mathcal{A}_F(D_2)/\mathcal{A}_F(D_1) \\ &\to (\mathcal{A}_F(D_2) + F)/(\mathcal{A}_F(D_1) + F) \to 0 \end{aligned}$$
es exacta para cualquier par de divisores, por lo que
$$\begin{aligned} dim((\mathcal{A}_F(D_2) + F) &/ (\mathcal{A}_F(D_1) + F)) \\ &= dim(\mathcal{A}_F(D_2)/\mathcal{A}_F(D_1)) - dim(\mathcal{L}(D_2)/\mathcal{L}(D_1)) \\ &= (grado(D_2) - grado(D_1)) - (dim(D_2) - dim(D_1)). \end{aligned}$$

Supongamos ahora que $D \in \mathcal{D}_F$ es tal que $dim(D) = grado(D) + 1 - g$. Si $D_1 \geq D$ entonces
$$dim(D_1) \leq grado(D_1) + dim(D) - grado(D) = grado(D_1) + 1 - g.$$

El teorema de Riemann (Teoremos 1.34) dice que

$$dim(D_1) \geq grado(D_1) + 1 - g$$

por lo que

$$dim(D_1) = grado(D_1) + 1 - g \text{ para todo } D_1 \geq D.$$

Dado $\alpha \in \mathcal{A}_F$ se puede encontrar $D_1 \geq D$ tal que $\alpha \in \mathcal{A}_F(D_1)$.
Se tiene que

$$\begin{array}{rcl} dim((\mathcal{A}_F(D_1) + F) & / & ((\mathcal{A}_F(D) + F) \\ & = & (grado(D_1) - dim(D_1)) - (grado(D) - dim(D)) \\ & = & (g-1) - (g-1) = 0. \end{array}$$

Es decir, $\mathcal{A}_F(D_1) + F = \mathcal{A}_F(D) + F$. Como $\alpha \in \mathcal{A}_F(D_1)$ se tiene que:

$$\mathcal{A}_F = \mathcal{A}_F(D) + F.$$

Ahora tenemos el siguiente teorema.

Teorema 1.38. *Para un divisor D, el índice de especialidad es:*

$$i(D) = dim(\mathcal{A}_F/(\mathcal{A}_F(D) + F)).$$

Demostración. Sea $D \in \mathcal{D}_F$. Por el teorema de Riemann existe un divisor $D_1 \geq D$ tal que $dim(D_1) = grado(D_1) + 1 - g$. Se tiene que $\mathcal{A}_F = \mathcal{A}_F(D_1) + F$ y implica que:

$$\begin{array}{rcl} dim(\mathcal{A}_F/(\mathcal{A}_F(D) + F)) & = & dim((\mathcal{A}_F(D_1) + F)/(\mathcal{A}_F(D) + F)) \\ & = & (grado(D_1) - dim(D_1)) - (grado(D) - dim(D)) \\ & = & g - 1 + dim(D) - grado(D) = i(D). \end{array}$$

q.e.d

Corolario 1.39.

$$g = dim(\mathcal{A}_F/(\mathcal{A}_F(0) + F)).$$

Demostración. Por definición:
$i(0) = dim(0) - grado(0) + g - 1 = 1 - 0 + g - 1 = g.$

q.e.d

Definición 1.40. *Se tienen las siguientes definiciones:*

1. *Una diferencial de Weil de F/K es una función K-lineal $\omega : \mathcal{A}_F \to K$ tal que se anula en $\mathcal{A}_F(D) + F$ para algún divisor $D \in \mathcal{D}_F$.*

2. *$\Omega_F := \{\omega | \omega$ es una diferencial de Weil de $F/K\}$ se llama el módulo de las diferenciales de Weil.*

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

Se puede ver que Ω_F es un K-espacio vectorial y que $\Omega_F(D)$ es un subespacio de Ω_F. También se puede ver que es claro que $\Omega_F = \bigcup_{D \in \mathcal{D}_F} \Omega_F(D)$.

Corolario 1.41. *Para $D \in \mathcal{D}_F$, se tiene que $dim\Omega_F(D) = i(D)$.*

Demostración. El espacio $\Omega_F(D)$ es el espacio de formas lineales en $\mathcal{A}_F/(\mathcal{A}_F(D)+F)$. El corolario se sigue pues la dimensión de $\mathcal{A}_F/(\mathcal{A}_F(D)+F)$ es finita e igual a $i(D)$ por el teorema 1.38.

q.e.d

Definición 1.42. *Para $x \in F$ y $\omega \in \Omega_F$ se define $x\omega : \mathcal{A}_F \to K$ mediante:*

$$(x\omega)(\alpha) := \omega(x\alpha).$$

Se puede ver que si ω se anula en $\mathcal{A}_F(D)+F$ entonces $x\omega$ se anula en $\mathcal{A}_F(D+(x))+F$. Esto queire decir que $x\omega$ es una diferencial de Weil y esta definición inspira lo siguiente:

Proposición 1.43. *Ω_F es un espacio vectorial de dimensión uno sobre F.*

A cada diferencial de Weil ω se le puede asociar un divisor de la siguiente manera:
Se considera el conjunto

$$M(\omega) := \{D \in \mathcal{D}_F | \omega \text{ se anula en } \mathcal{A}_F(D)+F\}.$$

Lema 1.44. *Sea $0 \neq \omega \in \Omega_F$. Entonces existe un único divisor, $W \in M(\omega)$ tal que $D \leq W$ para todo divisor $D \in M(\omega)$.*

Un divisor W de una diferencial de Weil ω también se denota por (ω).
El lema anterior motiva lo siguiente:

Definición 1.45. *Tenemos las siguientes definiciones:*

1. *El divisor (ω) de una diferencial de Weil $\omega \neq 0$ se define como el único divisor de F/K que cumple las siguientes dos propiedades:*
   a) *ω se anula en $\mathcal{A}_F((\omega))+F$.*
   b) *Si ω se anula en $\mathcal{A}_F(D)+F$ entonces $D \leq (\omega)$.*
2. *Dado $0 \neq \omega \in \Omega_F$ y $P \in \mathbb{P}_F$ se define $v_P(\omega) := v_p((\omega))$.*
3. *Se dice que un lugar P es un cero (resp. polo) de ω si $v_P((\omega)) > 0$ (resp. $v_P((\omega)) < 0$). La diferencial ω se dice que es regular en P si $v_P((\omega)) \geq 0$. La diferencial ω se llama regular si es regular en todo $P \in \mathbb{P}_F$.*
4. *Un divisor W se llama divisor canónico de F/K si $W = (\omega)$ para algún $\omega \in \Omega_F$.*

Lema 1.46. *Para un capo de funciones F/K se tiene que:*

$$dim\Omega_F(0) = g.$$

Proposición 1.47. *Se tiene que:*

1. *Para $0 \neq x \in F$ y $0 \neq \omega \in \Omega_F$, se tiene que $(x\omega) = (x) + (\omega)$.*
2. *Cualquiera dos divisores canónicos de F/K son equivalentes.*

Demostración. Si ω se anula en $\mathcal{A}_F(D)+F$, entonces $x\omega$ se anula en $\mathcal{A}_F(D+(x))+F$, por lo tanto $(\omega)+(x) \leq (x\omega)$. Tambien se tiene que $(x\omega)+(x^{-1}) \leq (x^{-1}x\omega) = (\omega)$. Combinando esta desigualdad con la anterior, se obtiene que $(\omega)+(x) \leq (x\omega) \leq -(x^{-1})+(\omega) = (\omega)+(x)$.

Una parte de segunda parte de la proposición se obtiene automaticamente de la primera parte y del hecho que Ω_F es espacio vectorial de dimensión uno sobre F. Si ahora se tiene que $D \sim (\omega)$ para $D \in \mathcal{D}_F$ y ω es una diferencial de Weil, entonces $D = (\omega)+(x)$. Por la proposición 1.47, se tiene que $D = (\omega x)$ y sabemos que ωx es una diferencial de Weil, lo que implica que D es un divisor canónico. Con esto podemos concluir que los divisores canónicos forman una clase de equivalencia de $\mathcal{C}_F$. A esta clase de equivalencia se le llama clase canónica de F/K.

q.e.d

Teorema 1.48. *Sean A un divisor cualquiera y $W = (\omega)$ un divisor canónico de F/K. La función $\mu : \mathcal{L}(W - D) \to \Omega_F(D)$; $x \mapsto x\omega$ es un isomorfismo de K-espacios vectoriales. En particular,*

$$i(D) = dim(W - D).$$

Demostración. Dada $x \in \mathcal{L}(W - D)$ se tiene que

$$(x\omega) = (x) + (\omega) \geq -(W - D) + W = D,$$

por lo que $x\omega \in \Omega_F(D)$. Entonces μ es una función de $\mathcal{L}(W - D)$ a $\Omega_F(D)$. La función μ es lineal. También es inyectiva, ya que si $x \in Ker(\mu)$, tenemos que $x\omega = 0$, lo que implica que $x = 0$. Falta demostrar que μ es sobre. Para demostrar esto, sea $\omega_1 \in \Omega_F(D)$ una diferencial de Weil. Entonces $\omega_1 = x\omega$ para $x \in F$. Ya que $(x) + W = (x) + (\omega) = (x\omega) = (\omega_1) \geq D$ se obtiene que

$$(x) \geq D - W = -(W - D),$$

entonces $x \in \mathcal{L}(W - D)$ y $w_1 = \mu(x)$. Por lo tanto $i(D) = dim(\Omega_F(D)) = dim(W - D)$.

q.e.d

Teorema 1.49. ***(Riemann-Roch)***
Sea W un divisor canónico de F/K. Entonces para todo $D \in \mathcal{D}_F$,

$$dimD = degD + 1 - g + dim(W - D)$$

Demostración. Esto se sigue directamente de la definición de $i(D)$ y del teorema anterior.

q.e.d

Corolario 1.50. *Para un divisor canónico W, se tiene*

$$degW = 2g - 2 \text{ y } dimW = g.$$

Demostración. Para $0 = D \in \mathcal{D}_F$ se tiene, por el teorema de Riemann-Roch (teorema 1.49) que

$$1 = dim(0) = deg(0) + 1 - g + dim(W - 0).$$

Entonces $dim(W) = g$. Para $D = W$ tenemos que

$$g = dim(W) = deg(W) + 1 - g + dim(W - W) = deg(W) + 2 - g.$$

Por lo tanto $deg(W) = 2g - 2$.

q.e.d

Teorema 1.51. *Si D es un divisor de F/K de grado mayor o igual a $2g - 1$, entonces $dimD = degD + 1 - g$.*

Definición 1.52. *Se tienen las siguientes definiciones:*

1. *Un campo de funciones F'/K' se llama extensión algebraica de F/K si $F' \supseteq F$ es una extensión de campos de funciones y $K' \supseteq K$. Note que una extensión alegbraica satisface que F'/F es algebraica, finitamente generada y por lo tanto finita.*
2. *Sea F'/K' una extensión algebraica de F/K. Un lugar $P' \in \mathbb{P}_{F'}$ está arriba de $P \in \mathbb{P}_F$ si $P \subseteq P'$. También se dice que P' es una extensión de P o bien que P está debajo de P'. Se escribe $P'|P$.*

Teorema 1.53. *Sea F'/K' una extensión algebraica de F/K. Sea ahora P un lugar de F/K y P' un lugar de F'/K'. Sean $\mathcal{O}_P$ y $\mathcal{O}_{P'}$ los anillos de valuación y v_P y $v_{P'}$ las valuaciones discretas correspondientes. Entonces las siguientes afirmaciónes son equivalentes:*

1. *$P'|P$.*

2. $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.

3. *Existe un entero* $e \geq 1$ *tal que* $v_{P'}(x) = e \cdot v_P(x)$ *para todo* $x \in F$.

Más si $P'|P$, *entonces*

$$P = P' \cap F \quad y \quad \mathcal{O}_P = \mathcal{O}_{P'} \cap F.$$

Definición 1.54. *Sea* F'/K' *una extensión algebraica de* F/K *y sea* $P' \in \mathbb{P}_F$ *un lugar de* F'/K' *arriba de* $P \in \mathbb{P}_F$. *Entonces:*

1. *El entero* $e(P'|P) := e$ *tal que* $v_{P'}(x) = e \cdot v_P(x)$ *para todo* $x \in F$, *se llama índice de ramificación de* P' *sobre* P.

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

Teorema 1.55. *Sea* F'/K' *una extensión finita de* F/K, P *un lugar de* F/K *y* $P_1, \ldots, P_m$ *todos los lugares de* F'/K' *que están arriba de* P. *Sea* $e_i := e(P_i|P)$ *el índice de ramificación y* $f_i := f(P_i|P)$ *el grado relativo de* $P_i|P$. *Entonces*

$$\sum_{i=1}^{m} e_i f_i = [F' : F].$$

Para finalizar este capítulo enunciaremos los teoremas, que son importantes para este trabajo. Los que consideramos más importantes, serán los que demostraremos.

Proposición 1.56. *Sea* $P \in \mathbb{P}_F$. *Para cualquier* $n \geq 2g$, *existe un elemento* $x \in F$ *con divisor de polos* $(x)_\infty = nP$.

Por el teorema 1.51 se puede notar que el entero c que existe por el teorema 1.34 es igual a $2g - 1$. Entonces la n de la proposición anterior cumple $n > c$.

Definición 1.57. *Sea* $P \in \mathbb{P}_F$. *Un entero* $n \geq 0$ *se llama orden de polo de* P *si y solo si existe un elemento* $x \in F$ *con* $(x)_\infty = nP$. *En otro caso se llama laguna de* P.

Teorema 1.58. ***(de las lagunas de Weierstrass)*** *Sea* F/K *con género* $g > 0$ *y* P *un lugar de grado uno. Entonces hay exactamente* g *lagunas* $i_1 < \ldots < i_g$ *de* P. *Además se tiene que*

$$i_1 = 1 \quad e \quad i_g \leq 2g - 1.$$

Demostración. Cualquier laguna de P es menor a $2g-1$, por la proposición anterior. Es claro que 0 es un orden de polo. Se tiene esta caracterización de las lagunas:

$$i \text{ es laguna de } P \Leftrightarrow \mathcal{L}((i-1)P) = \mathcal{L}(iP).$$

Ahora se considera la siguiente cadena:

$$K = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq \cdots \subseteq \mathcal{L}((2g-1)P),$$

con $dim\mathcal{L}(0) = 1$ y $dim\mathcal{L}((2g-1)P) = g$. Se ve que

$$dim\mathcal{L}(iP) \leq dim\mathcal{L}((i-1)P) + 1$$

para cualquier i. Así se tienen exactamente $g-1$ números con $1 \leq i \leq 2g-1$ con $\mathcal{L}((i-1)P) \subsetneq \mathcal{L}(iP)$. Los g números que sobran son lagunas de P.

q.e.d

Teorema 1.59. ***(Clifford)*** *Para cualquier divisor* D *con* $0 \leq degD \leq 2g - 2$ *se tiene que*

$$dimD \leq 1 + \frac{1}{2} degD.$$

Para demostrar el teorema de Clifford se necesita el siguiente lema y el teorema de Riemann.

Lema 1.60. *Si A y B son dos divisores tales que $dimA > 0$ y $dimB > 0$, entonces*

$$dimA + dimB \leq 1 + dim(A + B).$$

Demostración. (del teorema de Clifford)
El caso $dimD = 0$ es trivial. Si $dim(W - D) = 0$ con W canónico, entonces

$$dimD = degD + 1 - g = 1 + \frac{1}{2}degD + \frac{1}{2}(degD - 2g) < 1 + \frac{1}{2}degD$$

ya que $degD \leq 2g - 2$. Falta ver el caso en el que $dimD > 0$ y $dim(W - D) > 0$. Se tiene, por el lema anterior, que

$$dimD + dim(W - D) \leq 1 + dimW = 1 + g$$

Por otro lado, según el teorema de Riemann-Roch (teorema 1.49) se tiene que

$$dimD - dim(W - D) = degD + 1 - g$$

Si se suman estas dos ecuaciones se obtiene lo que se quería demostrar.

q.e.d

Proposición 1.61. ***(Criterio de Eisenstein)*** *Sea F/K un campo de funciones y*

$$\varphi(T) = a_n T^n + \cdots + a_1 T + a_0$$

un polinomio con $a_i \in F$. Sea $P \in \mathbb{P}_F$ un lugar que cumpla una de las dos siguientes condiciones:

1. *$v_P(a_n) = 0$, $v_P(a_i) \geq v_P(a_0) > 0$ para $i = 1, \ldots, n-1$ y $mcd(n, v_P(a_0)) = 1$.*
2. *$v_P(a_n) = 0$, $v_P(a_i) \geq 0$ para $i = 1, \ldots, n-1$, $v_P(a_0) < 0$ y $mcd(n, v_P(a_0)) = 1$.*

Entonces $\varphi(T)$ es irreducible en $F[T]$. Si $F' = F(y)$ con y una raiz del polinomio, entonces P tiene una extensión única $P' \in \mathbb{P}_{F'}$ y se tiene que $e(P'|P) = n$ y $f(P'|P) = 1$.

Demostración. Sea $F' = F(y)$ una extensión de campo con $\varphi(y) = 0$. El grado de F'/F es $[F' : F] \leq deg\varphi(T) = n$, donde se cumple la igualdad si y solo si $\varphi(T)$ es irreducible en $F[T]$. Se toma una extensión $P' \in \mathbb{P}_{F'}$ de P. Como $\varphi(y) = 0$ se tiene que

$$-a_n y^n = a_0 + a_1 y + \cdots + a_{n-1} y^{n-1}. \tag{1.2}$$

Primero se asume que la condición 1 se cumpla. Como $v_{P'}(a_n) = 0$ y $v_{P'}(a_i) > 0$ para $i = 1, \ldots, n-1$, se tiene que $v_{P'}(y) > 0$. Poniendo $e := e(P'|P)$ se tiene que $v_{P'}(a_0) = e \cdot v_P(a_0)$ y $v_{P'}(a_i y^i) = e \cdot v_P(a_i) + i \cdot v_{P'}(y) > e \cdot v_P(a_0)$ para $i = 1, \ldots, n-1$. Por la desigualdad del triangulo estricta, la ecuación 1.2 implica

$$n \cdot v_{P'}(y) = e \cdot v_P(a_0).$$

Como $mcd(n, v_P(a_0)) = 1$, se tiene que $n|e$ y por lo tanto $n \leq e$. Por otro lado $n \geq [F' : F] \geq e$. Asi se obtiene que

$$n = e = [F' : F]$$

Con lo que se cumple todo lo que se quería demostrar. Para la condición 2 la demostración es similar.

q.e.d

El teorema aquí demostrado es un resultado que vamos a necesitar solamente una vez, pero que aún así es importante.

Teorema 1.62. *Si $a, b \in \mathbb{N}$, $a, b \neq 1$ y $mcd(a, b) = 1$, entonces todo natural mayor que $ab - a - b$ se puede escribir como combinación lineal positiva de a y b.*

Demostración. Esto será demostrado por inducción. Primero se demostrará que $ax + by = ab - a - b + 1$ tiene soluciones nonegativas.
Como $mcd(a, b) = 1$ se tiene que $ax_0 + by_0 = 1$ para algunos enteron x_0 y y_0 con $0 < x_0 < b$ ya que $b \neq 1$. Entonces se ve que $ab - a - b + 1 = ab - a - b + ax_0 + by_0 = a(x_0 - 1) + (y_0 + a - 1)$. Se ve con esto que lo que se tiene que demostrar es que $x_0 - 1 \geq 0$ y que $y_0 + a - 1 \geq 0$. Como $x_0 > 0$ se tiene que $x_0 - 1 \geq 0$. Sea ahora $y_0 + a - 1 < 0$, entonces $y_0 + a \leq 0 \Rightarrow y_0 \leq -a \Rightarrow by_0 \leq -ab$. Sustituyendo esto se tiene que $ax_0 + by_0 \leq ax_0 - ab = a(x_0 - b) < 0$. Con esto se obtiene una contradicción $(1 < 0)$. Por lo tanto se debe cumplir que $y_0 + a - 1 \geq 0$.
Para el paso de inducción, sea $ax + by = n$ con $n \geq ab - a - b + 1$ y $x, y \geq 0$. Como $mcd(a, b) = 1$ se tiene como en el caso base que $ax_0 + by_0 = 1$ para algunos enteron x_0 y y_0 con $0 < x_0 < b$. Con eso tenemos que $n + 1 = ax + by + ax_0 + by_0 = a(x + x_0) + b(y + y_0)$. Se tiene que $x + x_0 > 0$. Si $y + y_0 \geq 0$, la demostración ha terminado. Sea ahora $y + y_0 < 0$. Como $ab - a - b + 1 \leq n$, se tiene que:

$$\begin{aligned}
ab - a - b + 1 &< n + 1 \\
ab - a - b + 1 - b(y + y_0) &< n + 1 - b(y + y_0) \\
ab - a - b + 1 - b(y + y_0) &< a(x + x_0) \\
b - 1 - \frac{b}{a} + \frac{1}{a} - \frac{b}{a}(y + y_0) &< x + x_0 \text{ (ya que } a > 1) \\
b - 1 + \frac{1}{a} - \frac{b}{a}(y + y_0 + 1) &< x + x_0
\end{aligned}$$

Por suposición se tiene que $y + y_0 < 0$, por lo tanto $y + y_0 + 1 \leq 0$ y por eso se tiene que $\frac{b}{a}(y + y_0 + 1) \leq 0$. Con eso se obtiene que $b - 1 + \frac{1}{a} < x + x_0$ y por lo tanto $b < x + x_0$. Ahora como $0 \leq a + y_0 - 1$, se tiene que $y + 1 \leq a + y_0 + y$. Como $y \geq 0$ se tiene que $a + y_0 + y \geq 0$.
Con eso se obtiene la combinación lineal no negativa que se estaba buscando. Esta es $a(x + x_0 - b) + b(a + y_0 + y) = n + 1$.

q.e.d

Por último quisieramos enunciar la cota de Hasse-Weil, ya que la curva en este trabajo alcanza la cota.

Teorema 1.63. ***(Cota de Hasse-Weil)***
El número de lugares de grado uno de $F/\mathbb{F}_q$, que denotaremos por M, cumple:

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

donde g es el género de la extensión.

Lema 1.64. *Sea F un campo de característica p primo, entonces $\sigma(x) = x^q$, donde q es una potencia de p, es un automorfismo de $\mathbb{F}_{q^n}$ en $\mathbb{F}_{q^n}$ que cumple que*

$$x_0 \in \mathbb{F}_q \Leftrightarrow \sigma(x_0) = x_0.$$

Observación: Hay una correspondencia biyectiva entre el conjunto de campos de funciones de grado de trascendencia uno y el conjunto de las curvas algebraicas sobre un campo dado.

Para ver esto supondremos que la extensión $F/K(x)$ es finita y que $K(x)/K$ es de grado de trascendencia uno, porque ese es el caso que nos interesa.

Si tenemos que $F/K(x)$ es separable, podemos ver que por el teorema del elemento primitivo la extensión es simple. Por lo tanto hay un elemento $y \in F$ tal que $F = K(x)(y)$. Como el grado de la extensión es finita, hay un polinomio con coeficientes en $K(x)$ tal que y es raíz de dicho polinomio.

Eso nos da una curva de la forma $F(x, y) = 0$. Si ahora tomamos una curva $\mathcal{C}$ en K podemos ver que el campo de funciones racionales en $\mathcal{C}$ es $K(\mathcal{C})$. Este campo es un álgebra de tipo finito. Esto quiere decir que todo elemento k de $K(\mathcal{C})$ se puede escribir de la forma $k = f(t_1, \ldots, t_n)$, donde $f(t_1, \ldots, t_n)$ es un polinomio en n variables. Es claro que $K \subseteq K(\mathcal{C})$. Como $\mathcal{C}$ es una curva, es de dimensión uno. Esto nos dice que el grado de trascendencia de $K(\mathcal{C})/K$ es uno. Esto quiere decir que existe $i \in \{1, \ldots, n\}$ tal que $K(t_i)/K$ tiene grado de trascendencia uno. Por lo tanto la extensión ascociada a la curva sería $K(\mathcal{C})/K(t_i)$.

Para el caso de característica cero se puede ver esto en [6].

El caso de que la extensión $F/K(x)$ sea inseparable, encontrar esta correspondencia es más complicado. Aqui es necesario mencionar que se deben excluir del lenguaje geométrico las extensiones inseparables en las que género decrece bajo extensiones del campo base. Este caso se puede ver en [3].

Este último teorema, da una relación entre los lugares de grado uno de una extensión de campos y los puntos que cumplen la ecuación que se obtiene en la extensión.

Teorema 1.65. ***(Kummer)***
Sea $\varphi(T) = T^n + f_{n-1}(x)T^{n-1} + \cdots + f_0(x) \in K(x)[T]$ un polinomio irreducible sobre un campo de funciones racionales $K(x)$. Se considera el campo de funciones $K(x, y)/K$ donde y satisface la ecuación $\varphi(y) = 0$. También se considera un elemento $\alpha \in K$ tal que $f_j(\alpha) \neq \infty$ para toda j, $0 \leq j \leq n-1$. Se denota por $P_\alpha \in \mathbb{P}_{K(x)}$ el cero de $x - \alpha$ en $K(x)$. Si

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

tiene la siguiente descomposición en $K[T]$:

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

con $\psi_i(T) \in K[T]$ irreducibles, mónicos y distintos por pares, entonces se tiene:

1. *Para toda $i = 1, \ldots, r$, existe un lugar único $P_i \in \mathbb{P}_{K(x,y)}$, tal que $x - \alpha \in P_i$ y $\psi_i(y) \in P_i$. El elemento $x - \alpha$ es elemento primo de P_i (i.e. $e(P_i|P_\alpha) = 1$) y el campo de clases residuales de P_i es isomorfo a $K[T]/ < \psi_i(T) >$. Por lo tanto $f(P_i|P_\alpha) = deg(\psi_i(T))$.*

2. *Si $deg(\psi_i(T)) = 1$ para al menos una $i \in \{1, \ldots, r\}$, entonces K es campo de constantes del campo $K(x, y)$.*

3. *Si $\varphi_\alpha(T)$ tiene $n = deg\varphi(T)$ raíces distintas en K, entonces existe, para toda β con $\varphi_\alpha(\beta) = 0$, un lugar único $P_{\alpha,\beta} \in \mathbb{P}_{K(x,y)}$ tal que*

   $$x - \alpha \in P_{\alpha,\beta} \text{ y } y - \beta \in P_{\alpha,\beta}$$

   $P_{\alpha,\beta}$ es un lugar de $K(x, y)$ de grado uno.

En este teorema se puede ver que que hay una relación entre los lugares $P_{\alpha,\beta}$ de grado uno de $K(x, y)$ y los puntos (α, β) que cumplen con la ecuación que da la extensión.

Teniendo la relación entre curavs y extensiones de campos, que mencionamos arriba y el teorema 1.65, usaremos ambas notaciones indistintamente.

Con ésto tenemos la herramienta necesaria para poder trabajar con la extensión y obtener las propiedades necesarias para poder definir el diseño correspondiente, que compararemos con otros diseños construidos de la misma forma.

Capítulo 2

La familia de extensiones

En este capítulo vamos a calcular el género de los integrantes de la familia de extensiones. En el articulo donde encontramos esta curva, se calcula usando extensiónes de Kummer. Nosotros vamos a calcularlo de una forma distinta. Primero buscaremos los divisores principales de x y y. Después con ayuda del teorema de las lagunas de Weierstrass (teorema 1.58), el teorema de Clifford (teorema 1.59) y el teorema de Riemann (teorema 1.34) acotaremos al género por arriba y por abajo y obtendremos el mismo resultado que en el artículo [1]. El género nos servirá para poder calcular el número de lugares de grado uno de ésta familia. Como la familia de extensiones es máxima, alcanza la cota de Hasse-Weil. Eso quiere decir que si M es el número de lugares de grado uno de la extensión, $M = q^{2n} + 2gq^n + 1$, donde g es el género. Esto nos ayudará a poder definir el diseño en el próximo capítulo.

Consideremos el polinomio:

$$\varphi(T) = T^N - y^{q^2} + y \in \mathbb{F}_{q^{2n}}(y)[T]$$

donde $N := \frac{q^n+1}{q+1}$, $n \geq 3$ impar y q una potencia de un primo. Éste polinomio φ es irreducible sobre $\mathbb{F}_{q^{2n}}(y)$. Para ver eso usaremos el criterio de Eisenstein (Proposición 1.61):
Sean y un elemento primo y Q un polo simple de y en $\mathbb{F}_{q^{2n}}(y)$. Vemos que:

- $a_N = 1$,
- $a_i = 0 \ \forall \ i \in \{1, ..., N-1\}$,
- $a_0 = -y^{q^2} + y$.

Entonces tenemos que:

- $v_Q(a_N) = 0$,
- $v_Q(a_i) = \infty \ \forall \ i \in \{1, ..., N-1\}$,
- $v_Q(a_0) = v_Q(-y^{q^2} + y) \geq min\{v_Q(-y^{q^2}), v_Q(y)\}$.

Vemos que $v_Q(y) = -1$ por como escogimos a Q, lo que nos da que $v_Q(-y^{q^2}) = v_Q(y^{q^2}) = q^2 v_Q(y) = -q^2$ ya que $q \geq 2$. Ahora como $v_Q(-y^{q^2}) \neq v_Q(y)$ tenemos que se cumple la igualdad en la desigualdad ultramétrica. Por lo que tenemos que

$$v_Q(-y^{q^2} + y) = min\{v_Q(-y^{q^2}), v_Q(y)\} = min\{-q^2, -1\} = -q^2.$$

También vemos, con la ayuda del algoritmo de Euclides, que $mcd(N, -q^2) = 1$. Tenemos que:

$$N = \frac{q^n + 1}{q + 1} = q^{n-1} - q^{n-2} + \cdots - q + 1.$$

Por el algoritmo de Euclides, obtenemos las siguientes igualdades:

$$q^{n-1} - q^{n-2} + \cdots - q + 1 = q^2(q^{n-3} - q^{n-4} + \cdots - q + 1) + (-q + 1)$$

$$q^2 = (-q + 1)(-q) + q$$

$$-q + 1 = -1(q) + 1$$

$$q = q(1) + 0$$

Con esto vemos que $m.c.d.(N, -q^2) = m.c.d.(N, q^2) = 1$

Si ahora x es raíz de $\varphi(T)$, podemos concluir, por el criterio de Eisenstein (proposición 1.61), que:

- $\varphi(T)$ es irreducible sobre $\mathbb{F}_{q^{2n}}(y)[T]$,
- Q tiene una extensión única Q_∞ sobre $\mathbb{F}_{q^{2n}}(x, y)$,
- Se tiene que $e(Q_\infty|Q) = N$ y $f(Q_\infty|Q) = 1$.

Como tenemos que $f(Q_\infty|Q) = 1$, tenemos por definición que $[F'_{P'} : F_P] = 1$. Ahora como $\mathbb{F}_{q^{2n}}(y) = \tilde{\mathbb{F}}_{q^{2n}}(y) \subseteq \mathbb{F}_{q^{2n}}(y)(x)$, tenemos que $degP = [F_P : K] = 1$ para todo $P \in \mathbb{P}_F$. Eso implica que $[F'_{P'} : K] = [F'_{P'} : F_P][F_P : K] = 1$. Con esto podemos concluir que $F'_{P'} = K$ y por lo tanto $\mathbb{F}_{q^{2n}}$ es el campo de constantes.

Ahora falta calcular el género de la extensión. Para esto necesitamos los divisores principales de x y de y. Primero buscaremos al divisor principal (y). Para esto tenemos que encontrar $(y)_\infty$ y $(y)_0$. Como Q_∞ es la única extensión de Q y es de grado N tenemos que por 1.54

$$v_{Q_\infty}(y) = e(Q_\infty|Q)v_Q(y) = Nv_Q(y) = -N.$$

La última igualdad se debe a que $v_Q(y) = -1$, ya que Q es un polo simple de y. Con esto podemos concluir que $(y)_\infty = NQ_\infty$.

Ahora nos fijamos en los lugares de grado uno que son ceros de y y vemos qué más tiene que cumplir uno de estos lugares de grado uno P_0. Queremos ver cuando P_0 es cero de $x^N - y^{q^2} + y$:

$$\begin{aligned}(x^N - y^{q^2} + y)(P_0) &= (x^N)(P_0) - (y^{q^2})(P_0) + y(P_0) \\ &= x(P_0)^N - y(P_0)^{q^2} + y(P_0).\end{aligned}$$

Ahora como P_0 es cero de y, también tiene que ser cero de x. Ahora por 1.30 tenemos que $N = deg(y)_\infty = deg(y)_0$ y por lo tanto

$$(y) = NP_0 - NQ_\infty.$$

Ahora falta encontrar (x). Para ésto vemos que lugares son ceros de x. Aquí usaremos la relación que hay entre los lugares de grado uno de $\mathbb{F}_{q^{2n}}(x, y)$ y los puntos con coordenadas en $\mathbb{F}_{q^{2n}}$, que cumplen la ecuación $x^N - y^{q^2} + y = 0$.

Esto quiere decir que basta ver los valores que toma y si $x = 0$. i.e.

$$x^N - y^{q^2} + y = 0.$$

Vemos que esto se puede expresar de la siguiente forma:

$$y^{q^2} = y.$$

Vemos ahora el automorfismo de Frobenius (Lema 1.64)

$$\sigma : \mathbb{F}_{(q^2)^n} \to \mathbb{F}_{(q^2)^n}$$

definido por $\sigma(a) = a^{q^2}$. Lo que dice que si queremos encontrar los valores que cumplen la ecuación de arriba, tenemos que ver qué elementos de $\mathbb{F}_{(q^2)^n}$ quedan fijos por el automorfismo σ. Como σ es automorfismo de Frobenius, este fija los elementos del campo base. En este caso el campo base es $\mathbb{F}_{q^2}$. Con esto concluimos que:

$$(x)_0 = \sum_{z \in \mathbb{F}_{q^2}} P_{0,z}.$$

Por último falta ver a $(x)_\infty$. Para eso calculamos la valuación de x^N en Q_∞:

$$v_{Q_\infty}(x^N) = v_{Q_\infty}(y^{q^2} - y) \geq min\{v_{Q_\infty}(y^{q^2}), v_{Q_\infty}(-y)\}.$$

Ahora vemos que $v_{Q_\infty}(y^{q^2}) = q^2 v_{Q_\infty}(y) = -Nq^2$ y $v_{Q_\infty}(-y) = v_{Q_\infty}(y) = -N$. Como éstas dos valuaciones son distintas, tenemos que se cumple la igualdad en la desigualdad de arriba. Como $-Nq^2 \leq -N$ obtenemos que

$$N v_{Q_\infty}(x) = v_{Q_\infty}(x^N) = -Nq^2.$$

Resolviendo la ecuación llegamos a que $v_{Q_\infty}(x) = -q^2$ y por lo tanto $(x)_\infty = q^2 Q_\infty$. Con esto concluimos que:

$$(x) = \sum_{z \in \mathbb{F}_{q^2}} P_{0,z} - q^2 Q_\infty$$

y

$$(y) = N P_{0,0} - N Q_\infty.$$

Teniendo esto, podemos calcular ahora el género de la curva. Si observamos los divisores de polos de x y y, vemos que N y q^2 son órdenes de polos en Q_∞. Como el conjunto de ordenes de polos es un subsemigrupo de $\mathbb{N}$, entonces cualquier combinación lineal positiva de N y q^2 también es orden de polo. Ahora, consideramos la cadena:

$$\mathcal{L}(0) \leq \mathcal{L}(Q_\infty) \leq \mathcal{L}(2Q_\infty) \leq \cdots \leq \mathcal{L}(iQ_\infty) \leq \ldots \mathcal{L}((r-1)Q_\infty) \leq \mathcal{L}(rQ_\infty).$$

Por el teorema de las lagunas de Weierstrass (teorema 1.58) existen g valores de i, para los cuales se tiene la igualdad. Por el teorema 1.62 todo número mayor a $Nq^2 - N - q^2$ se puede escribir como combinacion lineal positiva de N y q^2. Por eso definimos $r := Nq^2 - N - q^2 + 1 = (q-1)(q^n - q)$. Ahora como $r = \deg(rQ)$ y por los teoremas de Clifford y de Riemann-Roch (teoremas 1.59 y 1.49, respectivamente), obtenemos la desigualdad

$$1 + \frac{r}{2} \geq \dim(rQ) \geq r + 1 - g.$$

Resolviendo esta desigualdad obtenemos que

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

Por otro lado el teorema de Weierstrass (teoremos 1.58) afirma que la última laguna cumple que $i_g \leq 2g-1$, pero como a partir de $Nq^2 - N - q^2 + 1$ ya no hay lagunas, necesariamente tenemos que $i_g \leq 2g - 1 \leq Nq^2 - N - q^2$. Con eso obtenemos que $2g \leq Nq^2 - N - q^2 + 1 = (q^n - q)(q-1)$ y por lo tanto

$$g \leq \frac{r}{2} = \frac{(q^n - q)(q-1)}{2}$$

Así llegamos a la conclusión de que el género de la curva es

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

lo que coincide con el resultado de [1].

Con lo visto en este capítulo tenemos lo necesario para trabajar en los siguientes capítulos.

Capítulo 3

Diseño

A lo largo de este capítulo denotaremos por $\mathcal{X}$ a la curva $y^{q^2} - y = x^N$ con $N = \dfrac{q^n+1}{q+1}$, $n \geq 3$ impar y q una potencia de primos. El interés en esta curva viene del hecho de que la curva es máxima. Eso quiere decir que esta va a alcanzar la cota de Hasse-Weil, i.e. tiene el mayor número de puntos posible. En el caso de esta curva, éste será:

$$\begin{aligned} |\mathcal{X}| &= q^{2n} + 2gq^n + 1 \\ &= q^{2n} + q^n(q^n - q)(q-1) + 1. \end{aligned}$$

En esta sección vamos a construir un diseño con ayuda de esta curva. Graficando $f(q) = q^2$ y $g(q) = \dfrac{q^n+1}{q+1}$ en la misma gráfica (para distintos valores de n) observamos que si $n = 3 \Rightarrow f(q) > g(q)$ para $q \geq 2$. Es claro que $f(q)$ y $g(q)$ son crecientes si $q \geq 2$. Si ahora tomamos $n \geq 5$, veo que obtenemos que $f(q) < g(q)$ para $n \geq 2$. Estas dos afirmaciones se pueden ver facilmente si se observan las gráficas de f y g, que se verán en figura 3.1 y figura 3.2.

En estas figuras de pueden comparar las funciones f y g dependiendo del valor de n. Para valores de n mayores a 5 las dos funciones ya no se pueden comparar bien en la gráfica, ya que la función g crece rapidamente comparada con la función f. La gráfica de f ya no se puede distinguir del eje x.

Eso quiere decir que tendremos que fijarnos en dos casos:

- **Caso 1:** $n = 3$
- **Caso 2:** $n \geq 5$, n impar

3.1. Caso 1 $(n = 3)$

Con ayuda de un prigrama en GAP, buscamos los puntos en la curva, para q pequeña. El programa usado se puede ver en el apéndice A. Notamos que los puntos se pueden juntar en bloques de tamaño q^2, donde los puntos de un bloque tienen las primeras coordenadas iguales.

También se pueden juntar en bloques de tamaño N, donde las segundas coordenadas de los puntos son iguales y distintos de los elementos de $\mathbb{F}_{q^2}$. Para cada elemento $c \in \mathbb{F}_{q^2}$, se puede ver que la clase de equivalencia de los puntos con segunda coordenada c es de tamaño 1.

Antes de construir el diseño, demostraremos los siguientes dos lemas, que resumen las observaciones anteriores. Estos dos lemas los podemos construir intentando generalizar para cualquier potencia de primos q con $N = \dfrac{q^n+1}{q+1}$ y $n = 3$.

Definición 3.1. *Sea $F(x, y) = x^N - y^{q^2} + y$. Se define:*

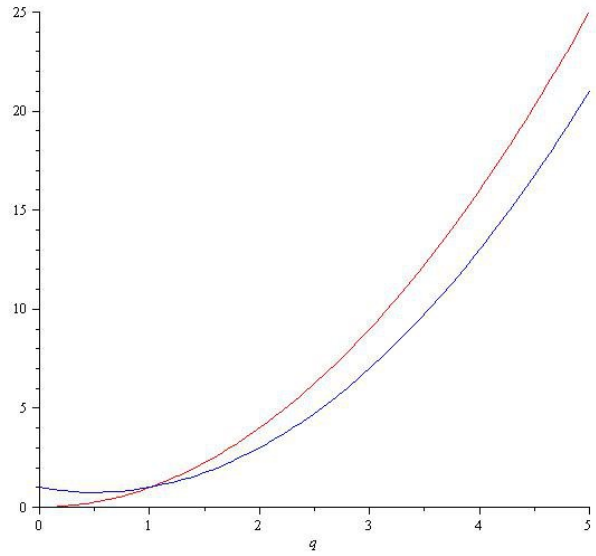

Figura 3.1: Aquí se está tomando el valor $n = 3$. La gráfica azul es g y la roja es f

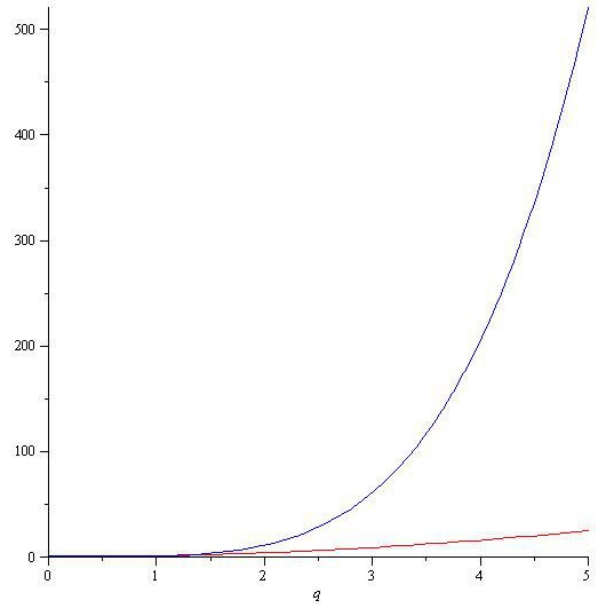

Figura 3.2: En esta figura se está tomando el valor $n = 5$. La gráfica azul es g y la roja es f

1. *La relación X tal que $aXb \Leftrightarrow F(a,c) = F(b,c) = 0$ para alguna $c \in \mathbb{F}_{q^{2n}}$.*

2. *La relación Y tal que $cYd \Leftrightarrow F(a,c) = F(a,d) = 0$ para alguna $a \in \mathbb{F}_{q^{2n}}$.*

Lema 3.2. *La relación X es de equivalencia y sus clases de equivalencia son de tamaño $N := \dfrac{q^n+1}{q+1}$, con excepción de q^2 clases de equivalencia que son de tamaño 1.*

Demostración. Es claro que es reflexiva, ya que $F(a,c) = F(a,c) = 0$ para algunos $a, c \in \mathbb{F}_{q^{2n}}$, por lo que aXa.

La simetría también es clara, ya que si $F(a,c) = F(b,c) = 0$ con $a, b, c \in \mathbb{F}_{q^{2n}}$, entonces se tiene que $F(b,c) = F(a,c) = 0$, por lo que si aXb, se tiene que bXa.

Se tiene también la transitividad por la siguiente cadena de igualdades:
$F(a_0,c) = F(a_1,c) = F(a_2,c) = 0$ con $a_0, a_1, a_2, c \in \mathbb{F}_{q^{2n}}$, por lo que se tiene que a_0Xa_2 si a_0Xa_1 y a_1Xa_2.

Ahora falta ver que las clases de equivalencia son de tamaño N. Para esto vemos que si fijamos un elemento $b \in \mathbb{F}_{q^{2n}}$ tal que $F(a,b) = 0$ para alguna $a \in \mathbb{F}_{q^{2n}}$, se tiene que

$$F(a) = a^N - b^{q^2} + b = 0.$$

Si tenemos que $b \in \mathbb{F}_{q^2}$, entonces obtenemos que $a^N = b^{q^2} - b = 0$. Pero esto implica que $a = 0$, por el automorfismo de Frobenius. Por lo tanto obtenemos q^2 clases de equivalencia de tamaño 1.

Si ahora $b \notin \mathbb{F}_{q^2}$, entonces obtenemos un polinomio de grado N. Para ver el número de soluciones de este polinomio podemos ver su derivada y ver cual es el máximo común divisor de ellos. La derivada de $F(a) = a^N - b^{q^2} + b$, es $F'(a) = Na^{N-1}$. Podemos reescribir al polinomio F de la siguiente forma:

$$a^N - b^{q^2} + b = Na^{N-1}(q+1)a + (-b^{q^2} + b).$$

Ahora por el algoritmmo de euclides se puede ver que

$$m.c.d.(a^N - b^{q^2} + b, Na^{N-1}) = -b^{q^2} + b \neq 0$$

lo que nos dice que el polinomio F y su derivada son primos relativos. Con esto podemos concluir que F tiene N raices distintas.

Por lo que por cada $b \in \mathbb{F}_{q^{2n}}/\mathbb{F}_{q^2}$ existen N elementos $a \in \mathbb{F}_{q^{2n}}$ tal que $F(a,b) = 0$.

q.e.d

Lema 3.3. *La relación Y es de equivalencia y sus clases de equivalencia son de tamaño q^2.*

Demostración. La demostración de que la relación Y es de equivalencia es análoga a la demostración de que la relación X es de equivalencia. Lo que quiere decir que basta ver que las clases de equivalencia sean de tamaño q^2.

Para ver esto fijamos un elemento $a \in \mathbb{F}_{q^{2n}}$ tal que $F(a,b) = 0$ para alguna $b \in \mathbb{F}_{q^{2n}}$. Con esto obtenemos un polinomio en b de grado q^2, que se ve de la siguiente forma:

$$F(b) = -b^{q^2} + b + a^N = 0.$$

Este polinomio tiene q^2 raices, ya que $F'(b) = -q^2 b^{q^2-1} + 1 = 1$ y por lo tanto

$$m.c.d.(F(b), F'(b)) = 1.$$

Con esto tenemos que por cada $a \in \mathbb{F}_{q^{2n}}$ existen q^2 elementos $b \in \mathbb{F}_{q^{2n}}$ tal que $F(a,b) = 0$.

q.e.d

Con estas dos demostraciones, obtenemos entonces dos relaciones de equivalencia que nos serán útiles en el momento de construir los diseños.

3.2. Caso 2 ($n \geq 5$)

Para este caso también buscamos los puntos de casos pequeños con ayuda de GAP (A). Estos casos fueron:

1. $n = 5; q = 2$,
2. $n = 5; q = 3$,
3. $n = 7; q = 2$.

Aquí podemos ver que también se pueden definir relaciones de equivalencia iguales a las del caso $n = 3$. También aquí se cumplen los lemas 3.2 y 3.3. Nótese que ninguna de las demostraciones necesitaron la distinción de los valores de n.

Esto quiere decir que a pesar de la diferencia en la relación entre las funciones f y g según el valor n, dicho valor n no influye en nada más a la curva.

3.3. Construcción del diseño

Primero daremos unas definiciones que nos ayudarán en la construcción de los diseños.

Definición 3.4. *Una estructura de incidencia es una tripleta $D = (V, B, I)$, con V y B conjuntos y una relación I en $V \times B$. A V se le llama el conjunto de vértices y a B se le llama el conjunto de bloques.*
Si $p \in V$ y $b \in B$ estan relacionados se escribe pIb. Si ese es el caso, se dirá una de estas expresiones:

- *El vértice p está en el bloque b,*
- *b pasa por p,*
- *p y b son incidentes.*

Definición 3.5. *Sea $D = (V, B, I)$ una estructura de incidencia. Se etiquetan los vértices $p_1, \ldots, p_{|V|}$ y los bloques $b_1, \ldots, b_{|B|}$. Tomamos la matriz $M = (m_{ij})$ con $i = 1, \ldots, |V|$ y $j = 1, \ldots, |B|$,*

$$m_{ij} := \begin{cases} 1 & \text{si } p_i I b_j \\ 0 & \text{en otros casos} \end{cases}$$

y se le llama matriz de incidencia para la estructura de incidencia D.

Definición 3.6. *Una estructura de incidencia $D = (V, B, I)$ se llama diseño con parámetros v, K, λ, $t \in \mathbb{N}$, si cumple con las siguientes condiciones:*

1. *$|V| = v$,*
2. *$\lambda = \{\lambda_1, ..., \lambda_j\}$ es un subconjunto finito de $\mathbb{N}$,*
3. *cada t vértices distintos están en exactamente λ_i bloques para $i \in \{1, ..., j\}$,*
4. *$K = \{k_1, ..., k_j\}$ es un subconjunto finito de $\mathbb{N}$,*
5. *$|b| = k_i$ para cualquier bloque b en B y alguna $i \in \{1, ..., j\}$.*

Un diseño se denotará $t - (v, K, \lambda)$.

Definición 3.7. *Sea $D = (V, B, I)$ un diseño. El diseño dual de D está definido por la estructura de incidencia $D' = (B, V, I^*)$ donde bI^*p si y sólo si pIb con $p \in V$ y $b \in B$. Esta estructura de incidencia tiene al conjunto de vértices de D como su conjunto de bloques y el conjunto de bloques de D como su conjunto de vértices.*

Sea ahora

$$F(x, y) = x^N - y^{q^2} + y.$$

Tomamos

$$V = B = \mathbb{F}_{q^{2n}}$$

y definimos que

$$pIB_\alpha \Leftrightarrow F(p, \alpha) = 0$$

como la relación de la estructura de incidencia. Teniendo esto, se tienen que encontrar los parámetros del diseño. Está claro que el diseño tiene q^{2n} vértices. Para encontrar el tamaño de los bloques, fijamos a $\alpha \in \mathbb{F}_{q^{2n}}$. Entonces

$$\begin{aligned} |B_\alpha| &= |\{p \in V | F(p, \alpha) = 0\}| \\ &= |\{p \in V | p^N - \alpha^{q^2} + \alpha = 0\}|. \end{aligned}$$

Por el lema 3.2, se ve que si $\alpha \in \mathbb{F}_{q^2}$, entonces $|B_\alpha| = 1$. Si ahora $\alpha \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^2}$, entonces $|B_\alpha| = N$. Para cualquier punto del diseño, se puede ver por el lema 3.3 que van a pasar q^2 bloques.

Con esta información puedo ver que el diseño correspondiente a la curva tiene los parámetros siguientes:

$$1 - (q^{2n}, \{1, N\}, q^2)$$

con un diseño dual

$$1 - (q^{2n}, q^2, \{1, N\}).$$

En el apéndice A se podrá ver un programa en GAP, con el que se pueden encontrar los bloques de un diseño dado.

Capítulo 4

Comparación con otros dos diseños

En esta sección vamos a comparar el diseño que acabamos de construir con los diseños que se pueden construir con la curva hermitiana y la curva de tipo Fermat, usando la misma idea con la relación de incidencia, como en el capítulo anterior. La curva hermitiana y la curva de tipo Fermat, se pueden encontrar en [4].

4.1. El diseño de la curva hermitiana

Aquí daremos a conocer la curva hermitiana y construiremos su diseño correspondiente.

La curva hermitiana es la siguiente:

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

en $\mathbb{F}_{q^2}$. Usando otra vez GAP, obtenemos que si los puntos se juntan según la coordenada x, se hacen grupos de q puntos. Si se juntan según la coordenada y se hacen grupos de $q+1$ puntos, excepto un grupo que es de q puntos, que es cuando $y \in \mathbb{F}_q$. Esto es parecido a lo que pasa con la curva $F(x, y)$, lo que se vio en los lemas 3.2 y 3.3.

4.1.1. El diseño

Teniendo esta información, se puede encontrar un diseño con esta curva.
Sea

$$G(x, y) = x^{q+1} - y^q - y,$$

entonces definimos a

$$V = B = \mathbb{F}_{q^2}$$

y

$$pIB_\alpha \Leftrightarrow G(p, \alpha) = 0.$$

Usando la misma argumentación que con la otra curva, obtenemos el diseño

$$1 - (q^2, \{1, q+1\}, q)$$

con su dual

$$1 - (q^2, q, \{1, q+1\}).$$

Si ahora tomamos al campo $\mathbb{F}_{(q^n)^2} = \mathbb{F}_{q^{2n}}$, obtenemos el diseño

$$1 - (q^{2n}, \{1, q^n + 1\}, q^n).$$

con su dual

$$1 - (q^{2n}, q^n, \{1, q^n + 1\}).$$

4.2. El diseño de la curva de tipo Fermat

Aqui definiremos la curva tipo Fermat y construiremos su diseño correspondiente que compararemos con el diseño construido en el capítulo 3. Sea $q = p^k$.

Definición 4.1. *A una curva de la forma $x^m + y^m = 1$ en un campo K y tal que la característica de K no divide a m, se le dice de tipo Fermat.*

Si ahora tomamos $K = \mathbb{F}_{q^{2n}}$, vemos que nos conviene tomar $m = N := \frac{q^n+1}{q+1}$, ya que la característica de $\mathbb{F}_{q^{2n}}$ divide a q^2, pero no a N.

En [5] se puede ver que si $m.c.d(p, m) = 1$. Se tiene que la curva $x^m + y^m = 1$ sobre $\mathbb{F}_{q^{2n}}$ es máxima si y sólo si m divide a $q^n + 1$.

Ya que $N = \dfrac{q^n + 1}{q + 1}$, es claro que $m.c.d(p, N) = 1$ y que N es un divisor de $q^n + 1$.

Con esto podemos tomar a la curva de tipo Fermat:

$$x^N + y^N = 1$$

sobre $\mathbb{F}_{q^{2n}}$. Y también esta curva será maximal, por lo visto arriba.

Usando un programa para GAP, como los que están en el apéndice A, pero usando la curva tipo Fermat, obtenemos otra vez listas de puntos para distintos valores de q y n. En ellas podemos observar que las relaciones X y Y tambien son de equivalencia y las clases de equivalencia son de tamaño N, con excepción de N clases de equivalencia que son de tamaño 1.

Eso lo vemos tomando la relación de equivalencia X (La relación de equivalencia Y es igual, por la forma de la función tipo Fermat). Si fijamos un elemento $\alpha \in \mathbb{F}_{q^{2n}}$, entonces el polinomio $y^N + \alpha^N - 1 = 0$ es de grado N. En este polinomio hay por cada α, N raices. Esto es porque p no divide a N y por lo tanto el polinomio es separable. Pero también hay N elementos $\beta \in \mathbb{F}_{q^{2n}}$ que cumplen que $\beta^N = 1$, por lo que hay N valores que puede tomar x que van a forzar $y = 0$.

Teniendo esto se ve que los tamaños de las clases de equivalencia que mencionamos más arriba son los correctos.

4.2.1. El diseño

Ahora podremos definir el diseño que corresponde a la curva tipo Fermat.

Sea

$$H(x, y) = x^N + y^N - 1.$$

Entonces, como lo hicimos en la sección pasada, definimos a

$$V = B = \mathbb{F}_{q^{2n}}$$

y

$$pIB_\alpha \Leftrightarrow H(p, \alpha) = 0.$$

Con esto obtenemos un diseño de la forma

$$1 - (q^{2n}, \{1, N\}, N)$$

con su dual

$$1 - (q^{2n}, N, \{1, N\}).$$

4.3. Comparaciones

Tenemos tres diseños con los parámetros siguientes:

$$1 - (q^{2n}, \{1, N\}, q^2), \tag{4.1}$$

$$1 - (q^{2n}, \{1, q^n + 1\}, q^n), \tag{4.2}$$

$$1 - (q^{2n}, \{1, N\}, N). \tag{4.3}$$

Donde el primer diseño se obtiene de la curva

$$y^{q^2} - y = x^N,$$

el segundo diseño se obtiene de la curva hermitiana

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

y el tercer diseño se obtiene de la curva tipo Fermat

$$x^N + y^N = 1.$$

En los tres casos tenemos que $n \geq 3$ impar, q potencia de un primo y $N = \dfrac{q^n + 1}{q + 1}$. Las tres curvas están definidas sobre el campo $\mathbb{F}_{q^{2n}}$.

Viendo estos tres diseños se puede ver que, por definición, tienen la misma cantidad de vértices y bloques. También se puede observar que los tres diseños tienen al menos un bloque incidente en un sólo vértice. Con mayor cuidado se puede ver que los bloques de tamaño uno, son así porque ya sea $x = 0$ o $y = 0$. Esto último lo pudimos observar cuando construimos los diseños correspondientes a las tres curvas.

Los bloques del diseño 4.2 van a ser más grandes que los bloques de los otros dos diseños, ya que $N|q^n + 1$, por como está definido N. Pero se puede notar que, por como fueron construidos, el diseño 4.3 va a tener una cantidad mayor de bloques de tamaño 1 que el diseño 4.1. De hecho 4.3 tiene N bloques de tamaño 1 y 4.1 solo tiene q^2.

Por como esta definida la matríz de incidencia de un diseño, las entradas van a ser sólo unos y ceros. Podemos observar que entre más grande k_i con $i \in \{1, \ldots, n\}$ más entradas iguales a uno va a tener la matríz de incidencia. Más aún podemos observar que entre mas grande sea $\sum_{k=1}^{n} k_i$, más entradas iguales a uno va a tener la matríz de incidencia.

Viendo las matrices de incidencia de los tres diseños se puede ver que el diseño 4.2 tendrá más unos que las matrices de los otros dos diseños. Viendo las matrices de incidencia de los otros dos diseños, se puede ver que la matriz de incidencia del diseño 4.1 va a tener más unos que la del diseño 4.3, porque 4.3 tiene más bloques de tamaño uno que 4.1.

Esto último de las matrices de incidencia es importante, porque el rango de la matríz de incidencia nos va a decir cual es la dimensión de un código. Si la matríz de incidencia tiene muy pocas entradas iguales a uno, puede que la dimensión se reduzca.

Capítulo 5

Algunos automorfismos

Un automorfismo de una curva es una función biregular con dominio y codominio a la curva. En este capitulo buscaremos los automorfismos de la curva F. Nos quedaremos con la forma de ver a la curva dada por el polinomio $F(x,y) = x^N - y^{q^2} + y$ que hemos usado. Aquí también tenemos que $N := \dfrac{q^n+1}{q+1}$, $n \geq 3$ impar y q una potencia de un primo. Aqui encontramos algunos automorfismos, pero no sabemos si son todos o si existen más automorfismos.

Para eso definiremos el siguiente conjunto:

Definición 5.1. $C_\alpha := \{\beta | F(\alpha,\beta) = 0\}$.

Se puede notar que $C_0 = \mathbb{F}_{q^2}$.

Sea ahora $b \in C_\alpha$ y $c \in C_0$. Se tiene que $b + c \in C_\alpha$, ya que:

$$\begin{aligned} \alpha^N - (b+c)^{q^2} + (b+c) &= \alpha^N - b^{q^2} - c^{q^2} + (b+c) \\ &= \alpha^N - b^{q^2} - c^{q^2} + b + c \\ &= \alpha^N - b^{q^2} + b + (-c^{q^2} + c) \\ &= \alpha^N - b^{q^2} + b + 0 = 0. \end{aligned}$$

Aquí usamos el hecho de que q es potencia de un primo, que es la caracteristica del campo $\mathbb{F}_{q^{2n}}$

Con eso encontramos q^2 automorfismos. Estos son:

$$\begin{aligned} \sigma_c \quad : \quad & \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^{2n}} \\ & b \longmapsto b + c \end{aligned}$$

Sea ahora $c \in C_0$ y $b \in C_\alpha$. Ahora veremos las condiciones que se tienen que cumplir para que $cb \in C_\alpha$. Sea ahora:

$$\begin{aligned} \alpha^N - (cb)^{q^2} + cb &= \alpha^N - b^{q^2}c^{q^2} + cb + cb^{q^2} - cb^{q^2} \\ &= \alpha^N + b^{q^2}(-c^{q^2} + c) + c(-b^{q^2} + b) \\ &= \alpha^N + c\alpha^N \\ &= \alpha^N(c+1) = 0. \end{aligned}$$

Con esto se ve que las condiciones para que $cb \in C_\alpha$, $c+1$ tiene que ser cero.

Esto me da por cada σ_c dos automorfismos, para un total de $2q^2$ automorfismos.

Apéndice A

Programas de GAP

En este apéndice están los programas de GAP que fueron hechos para este trabajo y que utilizamos para apoyarnos a hacer este trabajo. Con ellos encontremos las listas de puntos que me ayudaron a deducir los automorfismos y otras cosas.

Modificando la definición de F y cambiando la ecuación después del "if" en los primeros dos programas, estos se pueden usar para encontrar los puntos que cumplen cualquier curva definida sobre algún campo finito.

Con las mismas modificaciones, el tercer programa se podría usar para encontrar los bloques del diseño correspondiente a la curva deseada.

El primer programa fue para encontrar los puntos de las curvas con distintos valores de n y q. Los puntos aquí salen juntos según la coordenada x.

```
puntosx:=function(q,n)
local F, x, y, N;
F:=GF(q^(2*n));
N:=((q^n)+1)/(q+1);
for x in F do
for y in F do
if y^(q^2)-y=x^N then AppendTo("puntosx.dat", "(",x,",",y,")\n"); fi;
od;
od;
end;
```

El siguiente programa es el mismo de arriba, pero se le hicieron dos pequeños cambios, que están marcados con (*). Aqui los puntos estan juntos según la coordenada y.

```
puntosy:=function(q,n)
local F, x, y, N;
F:=GF(q^(2*n));
N:=((q^n)+1)/(q+1);
for y in F do (*)
for x in F do (*)
if y^(q^2)-y=x^N then AppendTo("puntosy.dat", "(",x,",",y,")\n"); fi;
od;
od;
end;
```

En el siguiente programa se encuentran los bloques de un diseño usando la curva $F(x, y)$.

```
bloques:=function(q,n)
local N, F,x,y,B;
```

```
F:=GF(q^(2*n));
N:=((q^n)+1)/(q+1);
for x in F do
B:=[];
for y in F do
if y^(q^2)-y=x^N then Append(B,[y]); fi;
od;
AppendTo("bloques.dat","B_",x,"=",B,"\n");
od;
end;
```

Bibliografía

[1] M. Abdón, J. Bezerra, L. Quoos, "Further examples of maximal curves", *J. Pure and Applied Algebra*, **213**, pp. 1192 a 1196

[2] T. Beth, D. Jungnickel, H. Lenz, *Design Theory, Volume I*, Cambridge University Press, Cambridge, 1999

[3] C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, American Matematical Society, E.U.A, 1951

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

[5] S. Tafazolian, F. Torres, "On maximal curves of Fermat type", *J. Advances in Geometry*, **13**, pp. 613 a 617

[6] F. Zaldivar, *Funciones algebraicas de una variable compleja*, Universidad Autónoma Metropolitana, Mexico D.F., 1995