Publicaciones Matemáticas del Uruguay
Volumen 18, Diciembre 2023, Páginas 1–57
S 0797-1443

CURVAS SOBRE CUERPOS FINITOS

MIRIAM ABDÓN, CÍCERO CARVALHO, Y DANIEL PANARIO

Resumen. El objetivo principal de estas notas es presentar resultados de la teoría de curvas algebraicas definidas sobre cuerpos finitos, con énfasis en el estudio de curvas maximales. Iniciamos con una exposición de resultados de la teoría de cuerpos finitos que serán necesarios en el estudio de curvas. En seguida pasamos al estudio de cuerpos de funciones algebraicas en una variable, que corresponde al estudio de la geometría intrínseca de las curvas algebraicas, y presentamos también una aplicación de resultados de cuerpos de funciones a la teoría de códigos. Finalmente pasamos a algunos de los principales resultados de la teoría de curvas algebraicas, especialmente a los que se refieren al número de puntos racionales de la curva.

Índice

Versión final: 18 de mayo de 2019.
Cicero Carvalho: trabajo parcialmente financiado por Fapemig (proc. CEX-APQ-01645-16) y CNPq.
Daniel Panario: trabajo parcialmente financiado por NSERC de Canada.
Estas notas corresponden al curso dictado por los autores en la escuela AGRA III, Aritmética, Grupos y Análisis, del 9 al 20 de Julio de 2018 en Córdoba, Argentina.

1. Introducción

El origen de los cuerpos finitos se remonta a los siglos XVII y XVIII. Los primeros en estudiarlos fueron: Fermat (1601-1665), Euler(1707-1783), Lagrange (1736-1813) y Legendre (1752-1833). Todos ellos trabajaron sobre determinados cuerpos finitos: $\mathbb{F}_p$, donde p es un número primo. Más adelante se verá que existe otro tipo de cuerpos finitos.

La teoría de cuerpos finitos tal y como se conoce hoy en día fue construida a finales del siglo XVIII y principios del XIX. Los principales investigadores en el área fueron: Carl Friedrich Gauss (1777-1855) y Évariste Galois (1811-1832). El artículo de Galois *Sur la théorie des nombres* marcó el inicio de los *cuerpos finitos*.

El siguiente gran paso en la construcción de cuerpos finitos fue dado por Richard Dedekind en 1857. Él caracterizó a los cuerpos finitos de orden p^n como anillos de clases residuales

$$\mathbb{F}_p[x]/(f)$$

donde f es un polinomio irreducible de grado n sobre $\mathbb{F}_p$. También introdujo la fórmula de inversión de Möbius en cuerpos finitos para estudiar el número de polinomios irreducibles de cierto grado.

Finalmente, Eliakim H. Moore en 1893, demostró que los cuerpos finitos deben tener p^n elementos si p es un número primo.

A finales del siglo XIX, toda la estructura de los cuerpos finitos era conocida. El libro de Dickson (1901) ya tenía todos los elementos importantes de tal estructura.

1.1. Resultados fundamentales.

1. En cualquier cuerpo finito, el número de elementos es potencia de un número primo, este último es la característica del cuerpo.
2. Si p es un primo y m un número positivo, entonces existe un cuerpo finito de orden p^m, el cual es único salvo isomorfismos.
3. El grupo multiplicativo de elementos no nulos de $\mathbb{F}_q$, $\mathbb{F}_q^\times$, es cíclico. Cualquier elemento generador es un elemento primitivo de $\mathbb{F}_q$.
4. Si $q = p^m$ entonces cada subcuerpo de $\mathbb{F}_q$ tiene orden p^d, donde d es un divisor positivo de m. Recíprocamente, si $d|m$ entonces existe exactamente un subcuerpo de $\mathbb{F}_q$ de orden p^d.
5. Cada elemento $a \in \mathbb{F}_q$ cumple $a^q = a$.
6. Un cuerpo finito $\mathbb{F}_q$ es isomorfo al cuerpo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$, donde p es la característica de $\mathbb{F}_q$.

El siglo XX fue la época en la que se desarrollaron aplicaciones de cuerpos finitos, debido mayormente a la aparición de las computadoras.

Las áreas de aplicación más importantes son: criptografía y teoría de códigos. Sin embargo, hoy en día el uso de los cuerpos finitos se ha expandido.

El principal libro para ahondarse en la teoría de cuerpos finitos es de Lidl y Niederreiter [40]; para una colección actualizada de temas de investigación en cuerpos finitos ver el manual de cuerpos finitos de Mullen y Panario [41].

1.2. Anillos y cuerpos.

Definición 1.1. Un *anillo* $(R, +, \cdot)$ es un conjunto R junto con dos operaciones "$+$" y "$\cdot$", tal que:

1. $(R, +)$ es un grupo abeliano;
2. $\cdot$ es asociativo, es decir, para todo $a, b, c \in R, a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

3. las leyes distributivas se cumplen: para todo $a, b, c \in R$, $a \cdot (b+c) = a \cdot b + a \cdot c$ y $(b + c) \cdot a = b \cdot a + c \cdot a$.

Definición 1.2. Sea R un anillo.

1. Un anillo se denomina **anillo con identidad**, si el anillo tiene identidad multiplicativa.
2. Un anillo es **conmutativo** si bajo "$\cdot$" es conmutativo.
3. Un anillo se denomina **anillo de división** si los elementos distintos de cero forman un grupo bajo "$\cdot$".
4. Un anillo se denomina **cuerpo** si es un anillo de división conmutativo con identidad.

Dicho de otra manera, un cuerpo $(F, +, \cdot)$ es un conjunto F junto con operaciones $+$ y $\cdot$ tal que:

1. $(F, +)$ es un grupo abeliano con identidad 0;
2. $(F \setminus \{0\}, \cdot)$ es un grupo abeliano con identidad 1;
3. las leyes distributivas se cumplen, i.e., para todo $a, b, c \in F$ se cumple

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$
$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

Si $|F|$ es finito, entonces se dice que F es un *cuerpo finito*. El número de elementos en F es el *orden* del cuerpo finito.

La definición anterior implica que, excepto el 0, todos los elementos de F tienen inverso.

Es bien conocido que $\mathbb{Z}/(p)$ es un cuerpo si y sólo si p es un número primo. Por ejemplo, $\mathbb{Z}/(6)$ no es un cuerpo finito puesto que $2 \cdot 3 \equiv 0 \pmod 6$. Dicho de otra forma, 2 no tiene inverso multiplicativo en $\mathbb{Z}/(6)$.

Definición 1.3. Sea p un número primo, $\mathbb{F}_p$ el conjunto $\{0, 1, \ldots, p-1\}$ de enteros y $\phi : \mathbb{Z}/(p) \to \mathbb{F}_p$, la aplicación: $\phi([a]) = a$ para $a = 0, 1, \ldots, p-1$. Entonces, $\mathbb{F}_p$ posee la estructura de cuerpo inducida por $\mathbb{Z}/(p)$, por lo tanto es un cuerpo finito de orden p.

Se denotará a un cuerpo finito con q elementos por $\mathbb{F}_q$. Más adelante se verá que q debe ser una potencia de un primo y que salvo isomorfismos hay solamente un cuerpo finito con q elementos.

En $\mathbb{Z}$, para un entero $a \neq 0$, $an = 0$ (donde $n \in \mathbb{N}$) implica que $n = 0$.

Ahora consideremos $\mathbb{Z}/(p)$ y nuevamente tomemos $a \neq 0$. Entonces se puede demostrar que $ap = 0$ y p es el entero positivo más pequeño con esta propiedad.

Definición 1.4. Si R es un anillo arbitrario y existe un entero positivo n tal que $nr = 0$ para todo $r \in R$, entonces el entero positivo más pequeño n es la *característica* del anillo y se dice que R tiene *característica positiva*. De no ser así, se dice que R es de *característica cero*.

Teorema 1.5. *Un anillo $R \neq \{0\}$ con característica positiva que tiene una identidad y ningún divisor de cero trivial, debe tener característica prima.*

Corolario 1.6. *Un cuerpo finito tiene característica prima.*

1.3. Propiedades básicas.

Teorema 1.7. *Si $\mathbb{F}_q$ es un cuerpo de característica prima p y $n \geq 1$, entonces*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \text{ y } (a-b)^{p^n} = a^{p^n} - b^{p^n}.$$

Demostración. (Esbozo.) Usamos inducción sobre n:

1. Base (cuando $n = 1$): $(a+b)^p = a^p + b^p$. Se desarrolla el binomio y se verifica que cada coeficiente $0 < i < p$ es cero, puesto que
$$\left(\begin{array}{c} p \\ i \end{array} \right) = \frac{p(p-1)\dots(p-i+1)}{i \dots 2\,1} \equiv 0 \mod p.$$
2. De $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ se deduce que $(a-b)^{p^n} = a^{p^n} - b^{p^n}$ puesto que
$$a^{p^n} = ((a-b)+b)^{p^n} = (a-b)^{p^n} + b^{p^n}.$$

□

Teorema 1.8. *El grupo multiplicativo de elementos distintos de cero en $\mathbb{F}_q$, denotado por $\mathbb{F}_q^\times$, es cíclico.*

Demostración. (Esbozo.) Si $q = 2$ es fácil ver que el resultado es cierto. Suponga que $q \geq 3$. El orden de $\mathbb{F}_q^\times$ es $q-1$. Ahora considere la factorización en primos de $h = q-1$

$$h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m},$$

donde $p_1, p_2, \dots, p_m$ son números primos distintos y $r_1, r_2, \dots, r_m$ son enteros positivos.

Para cada $i, 1 \leq i \leq m$, considere el polinomio $x^{h/p_i} - 1$. Puesto que el grado de este es h/p_i, tiene como máximo h/p_i raíces. Ahora bien, $h/p_i < h = q-1$, por lo tanto hay elementos en $\mathbb{F}_q^\times$ que no son raíces de $x^{h/p_i} - 1$.

Sea a_i un elemento de $\mathbb{F}_q^\times$ que no es una raíz de $x^{h/p_i} - 1$. Definamos el elemento

$$b_i = a_i^{h/(p_i)^{r_i}}.$$

Dejamos como ejercicio probar que el orden de b_i es $p_i^{r_i}$ y que si $b = b_1, b_2, \dots b_m$, entonces el orden de b es $q-1$ y por lo tanto es un generador de $\mathbb{F}_q^\times$. □

Ejemplo 1.9. Consideremos $\mathbb{F}_7$ y su grupo multiplicativo $\mathbb{F}_7^\times = \{1,2,3,4,5,6\}$. Es fácil verificar que 2 no es un elemento primitivo, pero en el caso de 3 se tiene que:

$$3^1 = 3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 4,\ 3^5 = 5,\ 3^6 = 1,$$

de donde se concluye que 3 es un elemento primitivo.

Existen algoritmos para encontrar elementos primitivos, pero ninguno de ellos se ejecuta en un tiempo polinomial en el tamaño de la entrada. Encontrar un tal algoritmo es un problema abierto difícil.

El siguiente teorema caracteriza los elementos que pertenecen a un cuerpo finito.

Teorema 1.10. *Si $\mathbb{F}_q$ es un cuerpo finito de q elementos, entonces cada $a \in \mathbb{F}_q$ satisface $a^q = a$.*

Demostración. Si $a = 0$, entonces es claro que $a^q = a$. Si $a \neq 0$, entonces $a^{q-1} = 1$, puesto que $q-1$ es el orden del grupo multiplicativo in $\mathbb{F}_q$. □

1.4. Polinomios sobre cuerpos finitos. Un polinomio sobre un anillo R es una expresión de la forma

$$p(x) = \sum_{i=0}^{n} a_i x^i,$$

donde n es un entero no negativo y $a_i \in R$, para todo $i = 0, 1, \ldots n$. Un polinomio es *mónico* si el término líder tiene coeficiente 1.

Definición 1.11. El anillo formado por los polinomios sobre R con operaciones suma y producto de polinomios, se denomina **anillo de polinomios sobre** R y se denota como $R[x]$.

Un polinomio $f(x) = a_n x^n + \cdots + a_0$ tiene grado n si $a_n \neq 0$. Por convención, el polinomio $f(x) = 0$ tiene grado $-\infty$.

Teorema 1.12. *Si $f, g \in R[x]$, entonces*

$$\begin{aligned} grado(f+g) &\leq max(grado(f), grado(g)) \\ grado(fg) &\leq grado(f) + grado(g). \end{aligned}$$

Sea F un cuerpo. Un polinomio $g \in F[x]$ *divide a* un polinomio $f \in F[x]$, si existe un polinomio $h \in F[x]$ tal que $f = gh$. Se dice entonces que g es un *divisor* de f.

Teorema 1.13 (Algoritmo de la división)**.** *Si $g \in F[x], g \neq 0$ y F es un cuerpo, entonces para cualquier $f \in F[x]$ existen polinomios únicos $q, r \in F[x]$ tales que $f = qg + r$ y $grado(r) < grado(g)$.*

Algunas clases importantes de polinomios sobre cuerpos finitos incluyen:

- Un polinomio $f \in \mathbb{F}_q[x]$ es *irreducible* sobre $\mathbb{F}_q$ si f tiene grado positivo y $f = gh$ con $g, h \in \mathbb{F}_q[x]$ implica que g o h es una constante. De otra forma f es reducible.
- Sea $f \in \mathbb{F}_q[x]$ un polinomio distinto del polinomio idénticamente nulo. Si $f(0) \neq 0$, entonces al entero positivo más pequeño e para el cual $f(x)$ divide a $x^e - 1$, se le denomina el *orden* de f y se denota como $\text{ord}(f)$. Si $f(x) = x^h g(x)$ con $g(0) \neq 0$, entonces $\text{ord}(f) = \text{ord}(g)$. Un polinomio mónico $f \in \mathbb{F}_q[x]$ de grado m es *primitivo* sobre $\mathbb{F}_q$ si $f(0) \neq 0$ y $\text{ord}(f) = q^m - 1$.
- Un polinomio $f \in \mathbb{F}_q[x]$ es una *permutación polinomial* sobre $\mathbb{F}_q$ si la función polinomial asociada $f : c \mapsto f(c)$ de $\mathbb{F}_q$ en $\mathbb{F}_q$ es una permutación de $\mathbb{F}_q$.

En las presentes notas no nos adentraremos en aplicaciones de estos polinomios, pero existen innumerables aplicaciones de ellos en criptografía, sucesiones sobre cuerpos finitos, combinatoria y geometría finita, entre otras áreas de investigación.

Cada aplicación de $\mathbb{F}_q$ en sí mismo puede expresarse como un polinomio. Es claro que si $\phi : \mathbb{F}_q \to \mathbb{F}_q$ es una función arbitraria de $\mathbb{F}_q$ en $\mathbb{F}_q$, entonces existe un polinomio único $g \in \mathbb{F}_q$ con $\text{grado}(g) < q$ representando a ϕ, es decir, $g(c) = \phi(c)$ para toda $c \in \mathbb{F}_q$. Es posible hallar al polinomio g usando algún método de interpolación (como el de Lagrange) para la función ϕ.

Los polinomios irreducibles son los elementos "primos" de los polinomios. Al igual que los números primos para los números enteros, los polinomios irreducibles tienen un papel preponderante para los cuerpos finitos. En el caso de los enteros, se tiene que

$$\mathbb{Z}/(p) \text{ es un cuerpo si y sólo si } p \text{ es un número primo.}$$

Los siguientes teoremas garantizan que lo mismo se cumple para los polinomios sobre cuerpos finitos.

Teorema 1.14. *Para $f \in \mathbb{F}_q[x]$, el anillo de clases residuales $\mathbb{F}_q[x]/(f)$ es un cuerpo si y sólo si f es irreducible.*

Por lo tanto, un problema de suma importancia es hallar polinomios irreducibles en cuerpos finitos. En aplicaciones, como criptografía por ejemplo, la elección del polinomio irreducible para la construcción de una extensión de un cuerpo finito juega un papel muy importante en la eficiencia de los métodos considerados.

El teorema anterior garantiza que se obtendrá un cuerpo si y solamente si, el polinomio que define la estructura es irreducible. Observamos que si f es un polinomio mónico irreducible sobre $\mathbb{F}_p$ y grado $(f) = n$, entonces el número de elementos de $\mathbb{F}_p/(f)$ es p^n. Así que $\mathbb{F}_p/(f)$ es un cuerpo finito con p^n elementos.

Ejemplos: Consideremos primero $x^2 + 1 \in \mathbb{F}_2[x]$ como el polinomio que define al "cuerpo" $\mathbb{F}_4$. Usándolo se genera la tabla para el producto que se muestra a continuación:

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

.

Como se podrá observar no se obtuvo un cuerpo finito, esto se debe a que $(x + 1)(x + 1) = 0$ en $\mathbb{F}_2[x]/(x^2 + 1)$ y $x + 1 \neq 0$, es decir, se tienen divisores de cero diferentes de cero y por tanto no puede ser un cuerpo (finito). Adicionalmente, $x + 1$ no tiene inverso ya que no existe un elemento que multiplicado por $x + 1$ dé 1 como resultado y los elementos en un cuerpo que son distintos de cero, deben tener un inverso.

Ahora dado $x^2 + x + 1 \in \mathbb{F}_2[x]$, se tiene que

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

.

En este caso sí se obtiene un cuerpo. La diferencia está en el polinomio que se usó. En el primer ejemplo, el polinomio usado $x^2 + 1$ era *reducible* sobre $\mathbb{F}_2$, mientras que en el segundo ejemplo, $x^2 + x + 1$ es *irreducible* sobre $\mathbb{F}_2$. (Ejercicio: verificar que $x^2 + x + 1$ es irreducible sobre $\mathbb{F}_2$.)

Terminamos esta sección con un teorema fundamental para polinomios sobre cuerpos finitos.

Teorema 1.15 (Factorización única en $\mathbb{F}_q[x]$.)**.** *Cualquier polinomio $f \in \mathbb{F}_q[x]$ de grado positivo se puede expresar como*

$$f = a f_1^{e_1} f_2^{e_2} \dots f_k^{e_k}$$

donde $a \in \mathbb{F}_q$, $f_1, f_2, \dots, f_k$ son polinomios mónicos irreducibles distintos y $e_1, e_2, \dots, e_k$ son enteros positivos. Además esta factorización es única independientemente del orden en el que aparezcan los factores.

La demostración de este teorema no es constructiva. En otras palabras, no ofrece ningún algoritmo para factorizar polinomios. Sin embargo, hoy en día existen métodos muy eficientes para factorizar polinomios sobre cuerpos finitos; ver, por ejemplo [23].

1.5. Estructura de los cuerpos finitos. Sea p un número primo. Es sabido que:

1. $\mathbb{Z}/(p)$ es un cuerpo finito;
2. $\mathbb{F}_p[x]/(f)$ es un cuerpo finito si f es irreducible sobre $\mathbb{F}_p$;
3. si grado $(f) = n$ y f es irreducible entonces $\mathbb{F}_p[x]/(f)$ tiene p^n elementos.

¿Son las anteriores las únicas posibles opciones para construir cuerpos finitos? Lo que se desea, es justamente caracterizar a todos los cuerpos finitos posibles.

Definición 1.16. Sea F un cuerpo y $K \subseteq F$. Si K es en sí mismo un cuerpo bajo las operaciones de F, a K se le denomina *subcuerpo* de F y a F se le llama una *extensión* de K. Si $K \neq F$, se dice que K es un *subcuerpo propio* de F.

Observe que $\mathbb{F}_p$ no tiene subcuerpos propios. Es claro que si $K \subset \mathbb{F}_p$ y K es un cuerpo, entonces 0 y 1 son elementos de K. Puesto que K es un cuerpo, debe ser cerrado bajo la suma, así que cada elemento en $\mathbb{F}_p$ está en K. En consecuencia $K = \mathbb{F}_p$.

Definición 1.17. Un cuerpo que no tiene subcuerpos propios se llama un **cuerpo primo**.

Los cuerpos primos se obtienen considerando la intersección de todas las colecciones distintas de cero, de subcuerpos de un cuerpo dado. El siguiente teorema caracteriza a los cuerpos primos.

Teorema 1.18. *El subcuerpo primo de un cuerpo F es isomorfo a $\mathbb{F}_p$ o bien a $\mathbb{Q}$, dependiendo de si la característica de F es prima o cero.*

Definición 1.19. Si K es un subcuerpo de F y M cualquier subconjunto de F. Entonces el cuerpo $K(M)$ está definido como la intersección de todos los subcuerpos de F que contienen tanto a K como a M y se le denomina extensión del cuerpo K, obtenida adjuntando los elementos de M.

Para un conjunto finito $M = \{\theta_1, \theta_2, \ldots, \theta_n\}$, se escribe $K(M) = K(\theta_1, \theta_2, \ldots, \theta_n)$. Si M tiene sólo un elemento $\theta \in F$, entonces $L = K(\theta)$ se llama una *extensión simple de K* y θ será el *elemento de definición* de L sobre K.

Si L es una extensión del cuerpo K, entonces es posible ver a L como un espacio vectorial sobre K, puesto que los elementos de L forman un grupo abeliano bajo la suma (L es un cuerpo) y la multiplicación escalar de un elemento $\alpha \in L$ por un elemento $r \in K$ da como resultado $r\alpha \in L$, el cual cumple que:

$$\begin{aligned} r(\alpha + \beta) &= r\alpha + r\beta \\ (r + s)\alpha &= r\alpha + s\alpha \\ (rs)\alpha &= r(s\alpha) \\ 1 \cdot \alpha &= \alpha \end{aligned}$$

para todas $r, s \in K$ y $\alpha, \beta \in L$. La dimensión de este espacio vectorial es el grado de la extensión, si se tiene un espacio de dimensión finita.

Definición 1.20. Sea L una extensión de un cuerpo K. Si L, considerado como un espacio vectorial sobre K, tiene dimensión finita, entonces a L se le denomina una *extensión finita de K*. A la dimensión del espacio vectorial se le llama el *grado* de L sobre K y se denota por $[L : K]$

Teorema 1.21. *Si L es una extensión finita de K y M es una extensión finita de L, entonces M es una extensión finita de K y $[M : K] = [M : L][L : K]$.*

Definición 1.22. Si $f \in K[x]$ de grado positivo y F es una extensión de K, entonces se dice que f descompone en F, si f puede escribirse como el producto de factores lineales en $F[x]$. Es decir, f descompone en F si existen $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ tales que

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

donde $a \in K$ es el coeficiente líder de f. Al cuerpo F se le llama *cuerpo de descomposición* de f sobre K si f se descompone en F y si $F = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

El siguiente teorema caracteriza a los cuerpos de descomposición.

Teorema 1.23 (Existencia y unicidad de los cuerpos de descomposición.)**.** *Si K es un cuerpo y f es cualquier polinomio de grado positivo en $K[x]$, entonces existe un cuerpo de descomposición de f sobre K. Cualesquiera dos cuerpos de descomposición de f sobre K son isomorfos bajo un isomorfismo que mantiene a los elementos de K fijos y lleva las raíces de f entre sí.*

Teorema 1.24. *Si F es un cuerpo finito. Entonces F tiene p^n elementos donde p es la característica de F y n es el grado de extensión de F sobre su cuerpo primo.*

Demostración. Puesto que F es finito, la característica de F es un número primo, y esto implica que el subcuerpo primo K de F es isomorfo a $\mathbb{F}_p$. Por lo tanto contiene p elementos.

Es posible ver a los elementos en F como elementos de un espacio vectorial de F sobre K. Por lo tanto, existe una base para F sobre K formada por $\beta_1, \beta_2, \ldots, \beta_n$. Entonces cualquier elemento en F se puede escribir como

$$a_1\beta_1 + a_2\beta_2 + \cdots + a_n\beta_n$$

con $a_1, a_2, \ldots a_n \in K$. Puesto que $a_i \in K$ para todo $i = 1, \ldots, n$, se tienen p posibles valores, el número total de elementos en F es p^n. □

Ahora estamos listos para dar uno de los resultados más importantes de cuerpos finitos.

Teorema 1.25 (Existencia y unicidad de los cuerpos finitos.)**.** *Para cada primo p y cada entero positivo n, existe un cuerpo finito con p^n elementos. Cualquier cuerpo finito con p^n elementos es isomorfo al cuerpo de descomposición de $x^{p^n} - x$ sobre $\mathbb{F}_p$.*

Por ejemplo, este teorema garantiza que existe un cuerpo finito con 8 elementos, puesto que $8 = 2^3$ y 2 es primo. Sin embargo, este cuerpo con 8 elementos no es $\mathbb{Z}/(8)$, puesto que $\mathbb{Z}/(8)$ no es un cuerpo; por ejemplo, 4 no tiene inverso. Para encontrar $\mathbb{F}_{2^3}$ hay que hallar un polinomio irreducible de grado 3 sobre $\mathbb{F}_2$. (Ejercicio: hallar un polinomio irreducible de grado 3 sobre $\mathbb{F}_2$ y construir $\mathbb{F}_{2^3}$.)

Teorema 1.26. *Si $\mathbb{F}_q$ es un cuerpo finito con $q = p^n$ elementos. Entonces cada subcuerpo de $\mathbb{F}_q$ tiene orden p^m, donde m es un divisor positivo de n. Recíprocamente, si m es un divisor positivo de n, entonces existe exactamente un subcuerpo de $\mathbb{F}_q$ con p^m elementos.*

Ejemplos:

1. $\mathbb{F}_{2^{10}}$ tiene subcuerpos $\mathbb{F}_{2^2}$ y $\mathbb{F}_{2^5}$, cada uno de los cuales tiene a $\mathbb{F}_2$ como subcuerpo.

2. $\mathbb{F}_{3^{18}}$ tiene subcuerpos $\mathbb{F}_{3^6}$ y $\mathbb{F}_{3^9}$; $\mathbb{F}_{3^6}$ tiene subcuerpos $\mathbb{F}_{3^2}$ y $\mathbb{F}_{3^3}$, mientras que $\mathbb{F}_{3^9}$ tiene como subcuerpo a $\mathbb{F}_{3^3}$; finalmente, cada uno de ellos, tiene como subcuerpo a $\mathbb{F}_3$.
3. $\mathbb{F}_8$ no es un subcuerpo de $\mathbb{F}_{16}$, aunque $8|16$. Como 3 no divide a 4, por lo tanto $\mathbb{F}_8$ no es un subcuerpo de $\mathbb{F}_{16}$.

Los ejemplos anteriores están ilustrados en la Figura 1.

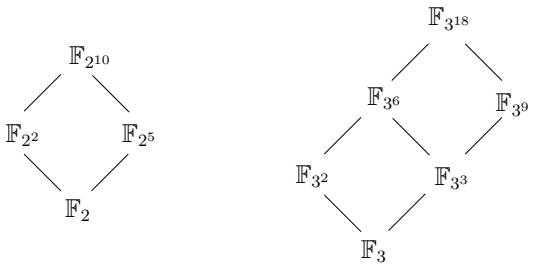


FIGURA 1. Subcuerpos de $\mathbb{F}_{2^{10}}$ e $\mathbb{F}_{3^{18}}$.

Nuestro próximo paso es definir los *conjugados* de un elemento de un cuerpo finito.

Definición 1.27. Sean $\mathbb{F}_{q^m}$ una extensión de $\mathbb{F}_q$ y α un elemento en $\mathbb{F}_{q^m}$. Los elementos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ son los *conjugados* de α con respecto a $\mathbb{F}_q$.

Sea $\alpha \in \mathbb{F}_{q^n}$ con polinomio minimal sobre $\mathbb{F}_q$ de grado d. Consideremos el conjunto $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ de conjugados de α. Los elementos de este conjunto son distintos si $n = d$; sino, cada conjugado distinto aparece repetido n/d veces.

Teorema 1.28. *Los automorfismos distintos de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ son las funciones $\sigma_0, \sigma_1, \ldots, \sigma_{n-1}$, donde $\sigma_j \colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ definida como $\sigma_j(\alpha) = \alpha^{q^j}$ para cada $\alpha \in \mathbb{F}_{q^n}$.*

El conjunto de automorfismos de $\mathbb{F}_q$ forma un grupo con la operación de composición funcional llamado *grupo de Galois de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$*. Es un grupo cíclico con generador $\sigma_1 \colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ que lleva $\alpha \in \mathbb{F}_{q^n}$ a α^q llamado *automorfismo de Frobenius*. Los conjugados de α son, entonces, los elementos a los cuales α es enviado aplicando iterativamente el automorfismo de Frobenius.

La suma y el producto de los conjugados de α producen dos funciones especiales muy usadas en aplicaciones.

Definición 1.29. Para cada $\alpha \in \mathbb{F}_{q^m}$, la *traza* de α sobre $\mathbb{F}_q$ es definida por

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}.$$

La próxima proposición, que dejamos como ejercicio, contiene algunas propiedades de la traza.

Proposición 1.30. *Sean $\mathbb{F}_{q^m}$ una extensión de $\mathbb{F}_q$, $\alpha, \beta \in \mathbb{F}_{q^m}$ y $a, b \in \mathbb{F}_q$. Entonces,*

1. $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$;
2. $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a\alpha + b\beta) = a\,\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) + b\,\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)$;

3. $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ *es una transformación linear de* $\mathbb{F}_{q^m}$ *en* $\mathbb{F}_q$*, donde* $\mathbb{F}_{q^m}$ *y* $\mathbb{F}_q$ *son vistos como espacios vectoriales sobre* $\mathbb{F}_q$*;*
4. $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) = ma$*;*
5. $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^q) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$.

Observamos que

$$\begin{aligned} f(x) &= (x-\alpha)(x-\alpha^q)\dots(x-\alpha^{q^{n-1}}) \\ &= x^n - (\alpha+\alpha^q+\dots+\alpha^{q^{n-1}})x^{n-1} + \dots + (-1)^n \alpha\alpha^q\dots\alpha^{q^{n-1}}, \end{aligned}$$

entonces $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = -a_{n-1}$.

Podemos definir la traza de $\mathbb{F}_{q^n}$ sobre un subcuerpo $\mathbb{F}_{q^m}$:

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^m}}(x) = x + x^{q^m} + \dots + \left(x^{q^m}\right)^{\frac{n-1}{m}}.$$

Cuando tenemos una cadena de extensiones de cuerpos, podemos calcular la composición de trazas.

Teorema 1.31. *Sea* K *un cuerpo finito,* F *una extensión de* K *y* E *una extensión de* F*. Entonces, para* $\alpha \in E$*,*

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_{F/K}\left(\mathrm{Tr}_{E/F}(\alpha)\right).$$

Demostración. Sea $K = \mathbb{F}_q$, $[F:K] = n$, $[E:F] = m$ y entonces $[E:K] = mn$. Para $\alpha \in E$ tenemos

$$\begin{aligned} \mathrm{Tr}_{F/K}\left(\mathrm{Tr}_{E/F}(\alpha)\right) &= \sum_{i=0}^{n-1} \left(\mathrm{Tr}_{E/K}(\alpha)\right)^{q^i} = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{m-1} \alpha^{(q^n)^j} \right)^{q^i} \\ &= \sum_{i=0}^{n-1}\sum_{j=0}^{m-1} \alpha^{q^{nj+i}} = \sum_{k=0}^{mn-1} \alpha^{q^k} = \mathrm{Tr}_{E/K}(\alpha). \end{aligned}$$

□

La función traza $\mathrm{Tr}_{F/K}$ para una extensión F de K es una transformación linear de F en K que describe todas las posibles transformaciones de F en K (*funcionales lineales* de F).

Teorema 1.32. *Sea* F *un cuerpo, extensión finita del cuerpo finito* K*, donde ambos son considerados como espacios vectoriales sobre* K*. Las transformaciones lineales de* F *en* K *son exactamente las funciones* L_β*,* $\beta \in F$*, donde* $L_\beta(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha)$ *para todo* $\alpha \in F$*. Además, tenemos* $L_\beta \neq L_\gamma$ *cuando* β *y* γ *son elementos distintos de* F*.*

Otra función interesante de un cuerpo finito a un subcuerpo es la *norma*.

Definición 1.33. Para $\alpha \in \mathbb{F}_{q^n}$, la *norma* $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ sobre $\mathbb{F}_q$ es definida como

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha\alpha^q\dots\alpha^{q^{n-1}} = \alpha^{\frac{q^n-1}{q-1}}.$$

Si $f(x) = (x-\alpha)\dots(x-\alpha^{q^{n-1}}) = \sum_{i=0}^n \alpha_i x^i$, entonces $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = (-1)^n a_0$.

Teorema 1.34. *La función norma de* $\mathbb{F}_{q^n}$ *sobre* $\mathbb{F}_q$ *verifica*

(a) $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha\beta) = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta)$ *para todo* $\alpha, \beta \in \mathbb{F}_{q^n}$*;*
(b) $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ *lleva* $\mathbb{F}_{q^n}$ *en* $\mathbb{F}_q$ *y* $\mathbb{F}_q^*$ *en* $\mathbb{F}_q^*$*;*

(c) $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha^n$, *para todo* $\alpha \in \mathbb{F}_q$;
(d) $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^q) = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$, *para todo* $\alpha \in \mathbb{F}_{q^n}$.
(e) Transitividad de la norma: *Si* K *es una extensión de un cuerpo finito* K *y* E *es una extensión de un cuerpo finito* F, *entonces* $\mathrm{N}_{E/K}(\alpha) = \mathrm{N}_{F/K}\left(\mathrm{N}_{E/F}(\alpha)\right)$, *para todo* $\alpha \in E$.

Ejercicio: probar el Teorema 1.34.

2. Cuerpos de funciones, semigrupos de Weierstrass y códigos de Goppa

2.1. Cuerpos de funciones de una variable. Sean K y F cuerpos tales que $K \subset F$. Como se ha visto anteriormente, se dice que F es una *extensión* de K y escribimos $F \,|\, K$. También se ha visto que podemos pensar a F como un K-espacio vectorial. Si F es de dimensión finita, con $\dim_K F = d$, entonces decimos que la extensión $F \,|\, K$ es *finita, de grado* d. Si $y \in F$ es tal que para un polinomio distinto de cero $p(X) \in K[X]$ tenemos $p(y) = 0$, entonces decimos que y es un elemento *algebraico* sobre K, de lo contrario, decimos que y es *trascendente* sobre K. Observamos que si $F \,|\, K$ es una extensión finita, entonces cada elemento $y \in F$ es algebraico sobre K: de hecho, digamos que $\dim_K F = n$, tenemos que $\{1, y, \ldots, y^n\}$ es un conjunto linealmente dependiente, por lo tanto, existen $a_0, \ldots, a_n \in K$, no todos iguales a cero, tal que $a_0 + a_1 y + \cdots + a_n y^n = 0$, es decir, y es una raíz de $p(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$. Si $y \in F$ es trascendente sobre K, entonces es fácil comprobar que la intersección de todos los subcuerpos de F que contienen K e y es el subcuerpo $K(y) := \{p(y)/q(y) \in F \,|\, p(X), q(X) \in K[X], q(X) \neq 0\}$, que es isomorfo al cuerpo de fracciones de polinomios $K(X) = \{p(X)/q(X) \,|\, p(X), q(X) \in K[X], q(X) \neq 0\}$. Esto refleja el hecho de que si y es trascendente sobre K, entonces se comporta como "una variable" sobre K, ya que para cualquier $a_0, \ldots, a_n \in K$ tenemos $\sum_{i=0}^{n} a_i y^i = 0$ si y sólo si $a_i = 0$ para todo $i = 0, \ldots, n$. Decimos que $F \,|K$ es una *extensión algebraica* si cada elemento de F es una raíz de algún polinomio distinto de cero en $K[X]$, de lo contrario, decimos que $F \,|\, K$ es una extensión *trascendente*.

En lo que sigue vamos a trabajar con un objeto básico: *un cuerpo de funciones algebraicas* $F \,|\, K$ *de una variable*. Esta es una extensión $F \,|\, K$ con la propiedad de que existe un elemento $x \in F$, trascendente sobre K y tal que la extensión $F \,|\, K(x)$ es finita.

$$\begin{array}{ll} F & \\ \big| \big) & \text{extensión finita} \\ K(x) & \\ \big| \big) & \text{extensión trascendente} \\ K & \end{array}$$

Siempre asumiremos que K *es algebraicamente cerrado en* F, lo que significa que si $f \in F$ es un elemento algebraico sobre K, entonces $f \in K$ (en otras palabras, excepto los elementos de $K \subset F$, que obviamente son algebraicos sobre K, no hay otros elementos de F que sean algebraicos sobre K). Nuestra referencia, en esta sección, es el primer capítulo del libro de H. Stichtenoth ([47]). No tenemos tiempo para demostrar la mayor parte de lo que necesitaremos, por lo que solo indicaremos los resultados y el lector podrá ver las pruebas en ese libro.

El ejemplo más básico de un cuerpo de funciones se obtiene al tomar $F = K(X)$: claramente X es trascendente sobre K y la extensión $F \mid K(X)$ es finita de grado uno (que es solo una forma elaborada de decir que $F = K(X)$).

Definición 2.1. Un *anillo de valoración* del cuerpo de funciones $F \mid K$ es un anillo $\mathcal{O}$ tal que:

(1) $K \subsetneq \mathcal{O} \subsetneq F$;
(2) para cualquier $f \in F$ tenemos $f \in \mathcal{O}$ o $f^{-1} \in \mathcal{O}$.

Lema 2.2. *Sea $\mathcal{O}$ un anillo de valoración de $F \mid K$. Entonces $\mathcal{O}$ es un anillo local, es decir, $\mathcal{O}$ tiene un único ideal maximal, que es el conjunto $P := \mathcal{O} \setminus \mathcal{O}^*$ (donde $\mathcal{O}^*$ denota el conjunto de elementos invertibles de $\mathcal{O}$).*

Demostración. Veamos que P es un ideal, y comenzamos por observar que $0 \in P$. Sea $z \in P$ y $f \in \mathcal{O}$, si $zf =: u \in \mathcal{O}^*$ tenemos $(zu^{-1})f = 1$ y $f \in \mathcal{O}^*$, luego $z = uf^{-1} \in \mathcal{O}^*$ lo cual es absurdo, por lo tanto, $zf \in P$. Dado $f, g \in P \setminus \{0\}$ tenemos que $f/g \in \mathcal{O}$ o $g/f \in \mathcal{O}$, digamos $f/g \in \mathcal{O}$. Luego $1 + f/g \in \mathcal{O}$ y $f + g = g(1 + f/g) \in P$ por lo que acabamos de probar que P es un ideal de $\mathcal{O}$. Obviamente es un ideal maximal porque si $J \subset \mathcal{O}$ es un ideal tal que $P \subsetneq J \subsetneq \mathcal{O}$, entonces J debe contener un elemento de $\mathcal{O}^*$, de modo que $J = \mathcal{O}$. □

Definición 2.3. Un subconjunto $P \subset F$ que es un ideal maximal de algún anillo de valoración de $F \mid K$ se llama *lugar* de $F \mid K$.

El teorema a continuación enumera las propiedades importantes de los lugares.

Teorema 2.4. *Sea $\mathcal{O}$ un anillo de valoración de $F \mid K$ y sea $P \subset \mathcal{O}$ su ideal maximal. Entonces:*

(1) *P es un ideal principal;*
(2) *sea $t \in P$ tal que $P = t\mathcal{O}$, luego cualquier elemento distinto de cero $z \in F$ se escribe de manera única como $z = t^n u$, con $n \in \mathbb{Z}$ y $u \in \mathcal{O}^*$;*
(3) *$z \in \mathcal{O}$ si y sólo si $z = t^n u$, con $n \in \mathbb{Z}$, $n \geq 0$ y $u \in \mathcal{O}^*$;*
(4) *el número entero n es el mismo para cualquier generador de P.*

Demostración. (1) Véase [47, Teorema 1.1.6].
(2) Véase [47, Teorema 1.1.6]. Aunque no probaremos la existencia, la parte de unicidad del elemento es fácil de verificar. De hecho, suponga que $z = t^{n_1}u_1 = t^{n_2}u_2$ para $n_1, n_2 \in \mathbb{Z}$ y $u_1, u_2 \in \mathcal{O}^*$. Supongamos que $n_1 \geq n_2$, lo que implica que $1 = t^{n_1 - n_2}u_1u_2^{-1}$ y como $1 \notin P$ debemos tener $n_1 = n_2$, y luego $u_1 = u_2$.
(3) Si $z = t^n u$ con $u \in \mathcal{O}^*$ y $n < 0$, entonces no podemos tener $z \in \mathcal{O}$ porque en este caso $1 = zt^{-n}u^{-1} \in P$, lo cual es absurdo. La recíproca es obvia.
(4) Supongamos ahora que $P = t\mathcal{O} = z\mathcal{O}$, sabemos que existen $n \in \mathbb{Z}$ y $u \in \mathcal{O}$ únicos tales que $z = t^n u$, y como $z \in P \subset \mathcal{O}$ debemos tener $n \geq 0$. No podemos tener $n = 0$ ya que esto implicaría $z \in \mathcal{O}^*$ (y luego $1 \in \mathcal{O}$) por lo que $n > 0$. Como $P = z\mathcal{O} = t^n\mathcal{O}$ debemos tener $n = 1$ (porque $t \in \mathcal{O}$ y debido a la unicidad probada en el ítem (2)). Así $z = tu$ y dado $f \in F$, $f \neq 0$ tenemos $f = t^m v$ con $m \in \mathbb{Z}$ y $v \in \mathcal{O}$, entonces $f = z^m(u^m v)$ y así el entero m es el mismo, independientemente si usamos t o z. □

En la definición siguiente, ∞ denota un elemento tal que $\infty + \infty = n + \infty = \infty + n = \infty$ y $\infty > n$ para cualquier $n \in \mathbb{Z}$.

Definición 2.5. Una *valoración (discreta)* de $F \mid K$ es una función $v : F \to \mathbb{Z} \cup \{\infty\}$ con las siguientes propiedades:

(1) $v(f) = \infty \Leftrightarrow f = 0$;
(2) $v(fh) = v(f) + v(h)$ para cualquier $f, h \in F$;
(3) $v(f + h) \geq \text{mín}\{v(f), v(h)\}$ para cualquier $f, h \in F$;
(4) existe $t \in F$ tal que $v(t) = 1$;
(5) $v(a) = 0$ para cualquier $a \in K$, $a \neq 0$.

Observe que si $a \in K^*$ y $f \in F$ tenemos $v(af) = v(a)+v(f) = v(f)$, en particular $v(-f) = v(f)$. Una propiedad importante de las valoraciones discretas es la llamada *desigualdad triangular estricta*, que enunciamos a continuación.

Lema 2.6. *Sea v una valoración discreta de $F \mid K$ y sean $f, h \in F$. Si $v(f) \neq v(h)$, entonces $v(f + h) = \text{mín}\{v(f), v(h)\}$.*

Demostración. Supongamos que $v(f) < v(h)$ y supongamos también que $v(f+h) \neq \text{mín}\{v(f), v(h)\} = v(f)$. De (3) obtenemos $v(f+h) > v(f)$ y $v(f) = v((f+h)-h) \geq \text{mín}\{v(f + h), v(-h)\} > v(f)$, una contradicción. □

Definición 2.7. Sea P un lugar de $F \mid K$ y definamos una función $v_P : F \to \mathbb{Z} \cup \{\infty\}$ de la siguiente manera: $v(0) = \infty$; si $f \neq 0$ sea $t \in P$ tal que $P = t\mathcal{O}$ y escribamos $f = t^n u$, con $u \in \mathcal{O}^*$; luego tomamos $v(f) := n$. Esta función se llama la *valoración asociada a P*. Del Teorema 2.4 esta función está bien definida, es decir, no depende de la elección del generador para P y para cualquier generador t tenemos $v_P(t) = 1$. Un generador para P también se llama *parámetro local en P*.

Dejamos al lector, como ejercicio, la prueba de que v_P es de hecho una valoración discreta de $F \mid K$. El resultado a continuación puede ayudar a probar que v_P tiene la propiedad (3) en la definición de valoraciones.

Lema 2.8. *Sea P un lugar de $F \mid K$, $\mathcal{O}$ su anillo de valoración y sea v_P la valoración asociada. Entonces:*

(1) $\mathcal{O} = \{f \in F \mid v_P(f) \geq 0\}$;
(2) $\mathcal{O}^* = \{f \in F \mid v_P(f) = 0\}$;
(3) $P = \{f \in F \mid v_P(f) > 0\}$.

Demostración. Sea $t \in P$ tal que $P = t\mathcal{O}$.
(1) Claramente, $t^n u \in \mathcal{O}$ siempre que $n \geq 0$ y $u \in \mathcal{O}^*$. Por otro lado, del Teorema 2.4 (3) tenemos $\mathcal{O} \subset \{f \in F \mid v_P(f) \geq 0\}$.
(2) Sea $f = t^n u \in \mathcal{O}^*$. Como $f^{-1} = t^{-n}u^{-1} \in \mathcal{O}$, debemos tener $n \geq 0$ y $-n \geq 0$. Por lo tanto $n = 0$.
(3) Esto es claro ya que $P = \mathcal{O} \setminus \mathcal{O}^*$. □

Por lo tanto, un lugar determina una valoración de $F \mid K$, y del ítem (1) del Lema anterior vemos que hay un único anillo de valoración que contiene un lugar dado. Es fácil probar el siguiente resultado, que es una especie de implicación inversa a la del lema: sea $v : F \to \mathbb{Z} \cup \{\infty\}$ una valoración de $F \mid K$ y sea $\mathcal{O} := \{f \in F \mid K \mid v(f) \geq 0\}$; entonces $\mathcal{O}$ es un anillo de valoración de $F \mid K$, que tiene como ideal maximal el conjunto $P := \{f \in F \mid v(f) > 0\}$. Uno incluso puede probar que hay una biyección entre los conjuntos de funciones de valoraciones discretas de $F \mid K$ y los lugares de $F \mid K$. Además, hay una biyección entre el conjunto de anillos de valoración de $F \mid K$ y el conjunto de lugares de $F \mid K$ (es decir, el conjunto de subconjuntos de f que son ideales maximales para anillos de valoración de $F \mid K$).

Dado que P es un ideal maximal de $\mathcal{O}$, obtenemos que $\mathcal{O}/P$ es un cuerpo. Además, como $K \subset \mathcal{O}$ podemos escribir $K \subset \mathcal{O}/P$, es decir, tenemos una extensión $(\mathcal{O}/P) \,|\, K$. Uno puede mostrar que esta es una extensión finita, y su grado se llama *grado de* P (notación: $\deg P$). Sea $z \in \mathcal{O}$, es habitual escribir $z(P)$, en lugar de $\overline{z}$, para denotar la clase de z en el cuerpo $\mathcal{O}/P$; esta notación se usará libremente en las secciones 3 y 4 a continuación.

Cuando $\deg P = 1$ decimos que P es un *lugar racional de* $F \,|\, K$.

Ejemplo 2.9. Veamos dos ejemplos de cuerpos de funciones y examinemos sus anillos de valoración, lugares y valoraciones discretas.
1) Sea K un cuerpo (que, en una primera lectura, se puede pensar que sea el cuerpo de números complejos $\mathbb{C}$) y considere el cuerpo de funciones $F \,|\, K$ donde $F = K(X) = \{f(X)/g(X) \,|\, f(X), g(X) \in K[X], g(X) \neq 0\}$. Esto cuerpo se llama *cuerpo de funciones racionales*). Sea $p(X) \in K[X]$ un polinomio irreducible (entonces, si $K = \mathbb{C}$ debemos tener $p(X) = X - \alpha$, para determinado $\alpha \in \mathbb{C}$). Recordamos que $K[X]$ es un dominio euclidiano, en particular es un dominio de factorización única. Luego, dado $f(X)/g(X) \in K(X)$, podemos encontrar un único $n \in \mathbb{Z}$ tal que $f(X)/g(X) = p(X)^n \tilde{f}(X)/\tilde{g}(X)$, donde $\tilde{f}(X), \tilde{g}(X) \in K[X]$ y ni $\tilde{f}(X)$ ni $\tilde{g}(X)$ son múltiplos de $p(X)$. Definiendo $v_P(f(X)/g(X)) = n$ y $v_P(0) = \infty$ obtenemos una función $v_P : F \to \mathbb{Z} \cup \{\infty\}$. No es difícil probar que v_P es una valoración de $K(x)$. El anillo de valoración correspondiente es

$$\mathcal{O}_{p(X)} = \{f(X)/g(X) \in K(X) \,|\, g(X) \text{ no es un múltiplo de } p(X)\},$$

y el lugar correspondiente es el conjunto

$$P_{p(X)} = \{f(X)/g(X) \in K(X) \,|\, f(X) \text{ es un múltiplo de } p(X) \text{ pero } g(X) \text{ no es un múltiplo de } p(X)\} = p(X)\mathcal{O}_{p(X)};$$

entonces, por supuesto,

$$\mathcal{O}^*_{p(X)} = \{f(X)/g(X) \in K(X) \,|\, f(X) \text{ y } g(X) \text{ no son múltiplos de } p(X)\}.$$

Vamos a demostrar ahora que $\deg P_{p(X)} = \deg\, p(X)$. Sea $f(X)/g(X) \in \mathcal{O}_{p(X)}$. En $K[X]$ tenemos $\operatorname{mcd}(p(X), g(X)) = 1$ (ya que $p(X) \nmid g(X)$) por lo tanto, existen $t(X), s(X) \in K[X]$ tales que $t(X)p(X) + s(X)g(X) = 1$, luego $s(X)g(X) - 1 \in (p(X))$ y en $\mathcal{O}_{p(X)}/P_{p(X)}$ tenemos $\overline{s(X)/1} = \overline{1/g(X)}$; esto muestra que $\overline{f(X)/g(X)} = \overline{f(X)s(X)/1}$ en $\mathcal{O}_{p(X)}/P_{p(X)}$. Ahora sea $r(X)$ el resto en la división (euclidiana) de $f(X)s(X)$ por $p(X)$, luego obtenemos $\overline{f(X)s(X)/1} = \overline{r(X)/1}$ con $r(X) = 0$ o $\deg\, r(X) < \deg\, p(X)$. De aquí es fácil concluir que $\mathcal{O}_{p(X)}/P_{p(X)}$ se genera, como un K-espacio vectorial, por $\overline{1/1}$, $\overline{X/1}$, …, $\overline{X^{\deg(p(X))-1}/1}$.

Otra valoración de $K(x)$, generalmente denotada por v_∞ es la función definida por $v_\infty(0) = \infty$ y $v_\infty(f(X)/g(X)) = \deg g(X) - \deg f(X)$ para todo $f(X)/g(X) \in K(X) \setminus \{0\}$. El anillo de valoración correspondiente es

$$\mathcal{O}_\infty = \{f(X)/g(X) \in K(X) \,|\, \deg f(X) \leq \deg g(X)\},$$

el lugar correspondiente es

$$P_\infty = \{f(X)/g(X) \in K(X) \,|\, \deg f(X) < \deg g(X)\} = (1/X)\mathcal{O}_\infty$$

y luego $\mathcal{O}^*_\infty = \{f(X)/g(X) \in K(X) \,|\, \deg f(X) = \deg g(X)\}$. Vamos a demostrar ahora que $\deg P_\infty = 1$. De hecho, en $\mathcal{O}_\infty/P_\infty$ tenemos $\overline{f(X)/g(X)} \neq \overline{0}$ si y solo

si $\deg f(X) = \deg g(X)$. Suponga que $\overline{f(X)/g(X)} \neq \overline{0}$ y sean a y b, respectivamente, los coeficientes líderes de $f(X)$ y $g(X)$. Tenemos $\overline{f(X)/g(X)} - \overline{ab^{-1}/1} = \overline{(f(X) - ab^{-1}g(X))/g(X)} = \overline{0}$, y por lo tanto $\mathcal{O}_\infty/P_\infty = K$.

Se puede mostrar que estas son todas las valoraciones de $K(X)\,|\,K$ (ver [47, Proposition 1.2.1]).

Supongamos ahora que $K = \mathbb{C}$ y sea $p(X) = X - \alpha$, para algún $\alpha \in \mathbb{C}$ (observe que todos los polinomios irreducibles de $\mathbb{C}[X]$ son de esta forma). Entonces $\deg P_{x-\alpha} = 1$ y puede escribir $\mathcal{O}_{X-\alpha}/P_{X-\alpha} = \mathbb{C}$. De lo que hicimos arriba, sabemos que los elementos de $\mathcal{O}_{X-\alpha}/P_{X-\alpha}$ son de la forma $\overline{z(X)/1}$, donde $z(X) \in \mathbb{C}[X]$. Está claro que $\overline{X/1} = \alpha$ así que $\overline{z(X)/1} = z(\alpha)$. Esta es la motivación para la notación $z(P)$ presentada justo antes de este ejemplo.

2) Sea $f(X, Y) = Y^2 - X(X-1)(X-2)(X-3)(X-4)(X-5)(X-6) \in \mathbb{C}(X)[Y]$; no es difícil ver que $f(X, Y)$ (como un polinomio en la variable Y) es irreducible, luego $\mathbb{C}(X)[Y]/(f(X, Y))$ es un cuerpo. Escribimos

$$x := \overline{X},\ y := \overline{Y} \text{ y } \mathbb{C}(x, y) := \mathbb{C}(X)[Y]/(f(X, Y)).$$

Como $y^2 = \prod_{i=0}^{6}(x - i)$ vemos que cualquier elemento de f puede escribirse como $f(x) + g(x)y$. Observe que $\mathbb{C}(x, y)\,|\,\mathbb{C}$ es un cuerpo de funciones.

$$\begin{array}{ll} \mathbb{C}(x,y) & \\ \big| \big) & \text{extensión finita de grado 2: } \mathbb{C}(x,y) = \mathbb{C}(x) \oplus \mathbb{C}(x)y \\ \mathbb{C}(x) & \\ \big| \big) & \text{extensión trascendente} \\ \mathbb{C} & \end{array}$$

Damos ahora alguna información sobre las valoraciones de $\mathbb{C}(x, y)$. Sea v_∞ la valoración de $\mathbb{C}(x)$ que describimos antes, entonces la función $w_\infty : \mathbb{C}(x, y) \to \mathbb{Z} \cup \{\infty\}$ definida en un elemento no nulo por

$$w_\infty(f(x) + g(x)y) = \text{mín}\{2v_\infty(f(x)), 2v_\infty(g(x)) - 7\}$$

(y $w_\infty(0) = \infty$) es una valoración de $\mathbb{C}(x, y)\,|\,\mathbb{C}$. Para $i \in \{0, 1, 2, 3, 4, 5, 6\}$ tenemos que

$$w_i(f(x) + g(x)y) := \text{mín}\{2v_{x-i}(f(x)), 2v_{x-i}(g(x)) + 1\}$$

(y $w_i(0) = \infty$) también es una valoración (aquí v_{x-i} es la valoración de $\mathbb{C}(x)$ asociada con el polinomio irreducible $x - i$, como se vio anteriormente), cuyo anillo de valoración (observe que $\mathbb{C}(x, y)$ es el cuerpo de fracciones de $\mathbb{C}[x, y] := \mathbb{C}[X, Y]/(f(X, Y))$) es ahora

$$\mathcal{O}_i = \left\{ \frac{p(x) + q(x)y}{m(x) + n(x)y} \in \mathbb{C}(x, y)\,|\,p(x), q(x), m(x), n(x) \in \mathbb{C}[x] \text{ y } m(i) \neq 0 \right\}.$$

Además, para $a \in \mathbb{C} \setminus \{0, 1, 2, 3, 4, 5, 6\}$, sea $b \in \mathbb{C}$ tal que $b^2 = \prod_{i=0}^{6}(a - i)$; luego $b \neq 0$ y existen dos valoraciones distintas de $\mathbb{C}(x, y)$, digamos $w_{a,b}$ y $w_{a,-b}$, con

anillos de valoración iguales a

$$\mathcal{O}_{a,b} = \left\{ \frac{p(x)+q(x)y}{m(x)+n(x)y} \in \mathbb{C}(x,y) \,|\, p(x), q(x), m(x), n(x) \in \mathbb{C}[x] \right. \\ \left. \text{y } m(a)+n(a)b \neq 0 \right\}$$

y

$$\mathcal{O}_{a,-b} = \left\{ \frac{p(x)+q(x)y}{m(x)+n(x)y} \in \mathbb{C}(x,y) \,|\, p(x), q(x), m(x), n(x) \in \mathbb{C}[x] \right. \\ \left. \text{y } m(a)-n(a)b \neq 0 \right\}.$$

Estos son todos los anillos de valoración de $\mathbb{C}(x,y)$. Además, todos los lugares son racionales. Esto es cierto porque, como se observó justo antes de estos ejemplos, para un lugar P en un cuerpo de funciones $F \,|\, K$ la extensión $(\mathcal{O}_P/P) \,|\, K$ es finita, por lo tanto es una extensión algebraica, pero en nuestro caso $K = \mathbb{C}$, un cuerpo algebraicamente cerrado, entonces debemos tener $\mathcal{O}_P/P = \mathbb{C}$ para todos los lugares P de $\mathbb{C}(x,y) \,|\, \mathbb{C}$.

Definición 2.10. Sea $\mathcal{P}$ el conjunto de lugares de $F \,|\, K$. Una suma formal de lugares $\sum_{P\in\mathcal{P}} n_P P$, donde $n_P \in \mathbb{Z}$ para todo $P \in \mathcal{P}$ y $n_P \neq 0$ solo para un número finito de lugares P, se llama *divisor* de $F \,|\, K$. El conjunto $\mathcal{D}$ de divisores es un grupo abeliano con la suma $\sum_{P\in\mathcal{P}} n_P P + \sum_{P\in\mathcal{P}} s_P P := \sum_{P\in\mathcal{P}} (n_P + s_P)P$. Definimos un orden parcial en el conjunto de divisores $\mathcal{D}$ como $\sum_{P\in\mathcal{P}} n_P P \leq \sum_{P\in\mathcal{P}} s_P P$ si y sólo si $n_P \leq s_P$ para todo $P \in \mathcal{P}$. El *grado* de un divisor es el número entero $\sum_{P\in\mathcal{P}} n_P \deg P$. El *soporte* de un divisor $\sum_{P\in\mathcal{P}} n_P P$ es el conjunto (finito) de lugares P tal que $n_P \neq 0$.

Sea $f \in F$ con $f \neq 0$. Podemos mostrar que $v_P(f) \neq 0$ sólo para un número finito de lugares P (ver [47, Corollary 1.3.4]). Si P es tal que $v_P(f) > 0$, entonces se dice que P es un *cero* de f; si $v_P(f) < 0$, entonces se dice que P es un *polo* de f. Definimos el *divisor de* f como $\operatorname{div}(f) := \sum_{P\in\mathcal{P}} v_P(f)P$. Observe que si $f, h \in F \setminus \{0\}$, a partir de las propiedades de las valoraciones, obtenemos $\operatorname{div}(fh) = \operatorname{div}(f) + \operatorname{div}(h)$; en particular, ya que $\operatorname{div}(1) = 0$, obtenemos $\operatorname{div}(f^{-1}) = -\operatorname{div}(f)$. Los divisores del tipo $\operatorname{div}(f)$, con $f \in F$, $f \neq 0$, se llaman *divisores principales* y el siguiente lema enumera algunas propiedades relacionadas con estos divisores (ver [47, Corollary 1.1.20 y Theorem 1.4.11]).

Lema 2.11. *Sea $f \in F \setminus K$. Entonces f tiene al menos un cero y un polo. Además,* $\deg(\operatorname{div}(f)) = 0$.

Ejemplo 2.12. Sea $\mathbb{R}(X)$ el cuerpo de funciones racionales sobre los números reales $\mathbb{R}$, y sea $f = (X^2+1)(X^2+2)^3(X-1)^2/((X-3)(X-5)^4)$. Luego, del Ejemplo 2.9 (1) (utilizamos la notación de ese ejemplo) y las propiedades de las valoraciones vemos que $v_{X^2+1}(f) = 1$, $v_{X^2+2}(f) = 3$, $v_{X-1}(f) = 2$, $v_{X-3}(f) = -1$, $v_{X-5}(f) = -4$ y $v_\infty(f) = -5$, además $v_P(f) = 0$ para cualquier $P \notin \{P_{X^2+1}, P_{X^2+2}, P_{X-1}, P_{X-3}, P_{X-5}, P_\infty(f)\}$. Así $\operatorname{div}(f) = P_{X^2+1} + 3P_{X^2+2} + 2P_{X-1} - P_{X-3} - 4P_{X-5} - 5P_\infty(f)$, los ceros de f son $\{P_{X^2+1}, P_{X^2+2}, P_{X-1}\}$, los polos de f son $\{P_{X-3}, P_{X-5}, P_\infty(f)\}$ y, recordando que $\deg P_{X^2+1} = \deg P_{X^2+2} = 2$, es fácil comprobar que $\deg(\operatorname{div}(f)) = 0$.

Definición 2.13. Sea D un divisor de $F \mid K$. Denotamos como $L(D)$ el conjunto $L(D) = \{f \in F \setminus \{0\} \mid \operatorname{div}(f) + D \geq 0\} \cup \{0\}$ (de manera equivalente, si $D = \sum_{P \in \mathcal{P}} n_P P$ entonces $L(D)$ es el conjunto de funciones f tal que $v_P(f) + n_P \geq 0$ para todo $P \in \mathcal{P}$). De las propiedades (3) y (5) de las valoraciones vemos que $L(D)$ es un K-espacio vectorial, generalmente llamado *espacio de Riemann-Roch asociado a* D; denotaremos su dimensión por $\ell(D)$.

No es trivial, pero uno puede mostrar que $\ell(D)$ es finito para cualquier divisor D de $F \mid K$.

Definición 2.14. Decimos que los divisores D y E son *linealmente equivalentes* si existe una función $f \in F$ tal que $E = D + \operatorname{div}(f)$.

La equivalencia lineal es una relación de equivalencia en el conjunto de divisores de $F \mid K$. A continuación, enumeramos algunos resultados relacionados con el espacio $L(D)$.

Lema 2.15. *Sean D un divisor de $F \mid K$ y $f \in F$, $f \neq 0$. Sea $E := \operatorname{div}(f) + D$, entonces $L(D) \cong L(E)$.*

Demostración. Mostraremos que $\psi : L(D) \to L(E)$ definido por $\psi(h) = h/f$ es un isomorfismo de K-espacios vectoriales. Sea $h \in L(D)$, luego $\operatorname{div}(h) + D \geq 0$, por lo tanto $\operatorname{div}(h/f) + \operatorname{div}(f) + D \geq 0$, es decir $\operatorname{div}(h/f) + E \geq 0$; esto muestra que ψ está bien definida. Está claro que ψ es lineal e inyectiva, veamos que es suryectiva. Si $z \in L(E)$, entonces $\operatorname{div}(z) + E \geq 0$ por lo tanto $\operatorname{div}(z) + \operatorname{div}(f) + D \geq 0$, por lo tanto $zf \in L(D)$ y por supuesto $\psi(zf) = z$. □

Lema 2.16. *Sea D un divisor de $F \mid K$ tal que $\deg D < 0$, entonces $\ell(D) = 0$ (i.e., $L(D) = \{0\}$).*

Demostración. Suponga que existe $f \in L(D)$, $f \neq 0$, luego $\operatorname{div}(f) + D \geq 0$. Observe que $\deg(\operatorname{div}(f) + D) = \deg(\operatorname{div}(f)) + \deg D = \deg D$ y tomando el grado en ambos lados de esta desigualdad obtenemos $\deg D \geq 0$, una contradicción con la hipótesis. □

Lema 2.17. *Si $D \geq 0$ tenemos $K \subset L(D)$ y si $D = 0$, entonces $L(D) = K$ (y tenemos $\ell(D) = 1$).*

Demostración. Suponga que $D \geq 0$ y sea $a \in K \setminus \{0\}$. Como $v_P(a) = 0$ para todos los lugares P de $F \mid K$ obtenemos $\operatorname{div}(a) = 0$, por lo tanto $\operatorname{div}(a) + D \geq 0$ y tenemos $K \subset L(D)$. Ahora suponga $D = 0$; si $f \in L(D) \cap (F \setminus K)$ entonces del Lema 2.11 existe un lugar P tal que $v_P(f) < 0$ por lo que no podemos tener $\operatorname{div}(f) + 0 \geq 0$ y luego $L(D) = K$. □

Lema 2.18. *Si $D \leq E$, entonces $L(D) \subset L(E)$ y $\dim(L(E)/L(D)) \leq \deg(E - D)$.*

Demostración. Si $h \in L(D)$ entonces $\operatorname{div}(h) + D \geq 0$, por lo tanto $\operatorname{div}(h) + E = \operatorname{div}(h) + D + (E - D) \geq E - D \geq 0$ y tenemos $h \in L(E)$. Supongamos ahora que $E = D + P$ y sea n_P el coeficiente de P en el divisor D; si $h \in L(D + P)$ tenemos $v_P(h) + n_p + 1 \geq 0$. Sea t un parámetro local en P y sea $\psi : L(D + P) \to \mathcal{O}_P/P$ la transformación K-lineal definida por $\psi(h) = \overline{ht^{n_P+1}}$, es fácil verificar que el núcleo de ψ es exactamente $L(D)$ y por lo tanto $\dim(L(D + P)/L(D)) \leq \dim \mathcal{O}_P/P = \deg P$. Ahora el lema sigue por inducción y del hecho que si $U \subset W \subset V$ son espacios vectoriales K de dimensión finita, entonces $\dim V/U = \dim V/W + \dim W/U$. □

El principal teorema sobre los espacios $L(D)$ es el llamado *Teorema de Riemann-Roch* (ver [47, Section I.5]) que indicamos a continuación.

Teorema 2.19. *Sea $F \mid K$ un cuerpo de funciones y sea D un divisor de $F \mid K$. Existe un entero no negativo g y un divisor C tal que*

$$\ell(D) = \deg\, D + 1 - g + \ell(C - D).$$

Además, C puede ser reemplazado por cualquier divisor en su clase de equivalencia lineal.

Este teorema presenta el invariante más importante de $F \mid K$, el entero g, que se llama el *género* de $F \mid K$. La clase de equivalencia de C se llama *clase canónica* de divisores de $F \mid K$ y cualquier divisor en ella se llama *divisor canónico*.

Corolario 2.20. *Sea C un divisor de $F \mid K$. Entonces C es un divisor canónico si y sólo si* $\deg\, C = 2g - 2$ *y* $\ell(C) = g$.

Demostración. Supongamos que C sea un divisor canónico; aplicando el teorema de Riemann-Roch a $D = 0$ y recordando del Lema 2.17 que $\ell(0) = 1$ obtenemos $1 = 0 + 1 - g + \ell(C)$, luego $\ell(C) = g$. Ahora aplicamos el teorema de Riemann-Roch a $D = C$ y usamos $\ell(C) = g$ y $\ell(C - C) = \ell(0) = 1$, así $g = \deg\, C + 1 - g + 1$ para que $\deg\, C = 2g - 2$. Para probar la recíproca, sea C' un divisor canónico y suponga que $\deg\, C = 2g - 2$ y $\ell(C) = g$. Del teorema de Riemann-Roch aplicado a $D = C$ obtenemos $g = 2g - 2 + 1 - g + \ell(C' - C)$ y $\ell(C' - C) = 1$. Esto significa que existe $z \in F \setminus \{0\}$ tal que $\mathrm{div}(z) + (C' - C) \geq 0$, es decir, $\mathrm{div}(z) + C' \geq C$. Observe que ambos lados tienen el mismo grado, por lo tanto, debemos tener $\mathrm{div}(z) + C' = C$, por lo que C es linealmente equivalente a C' y, por lo tanto, es un divisor canónico. □

Corolario 2.21. *Sea D un divisor de $F \mid K$ tal que* $\deg D > 2g - 2$. *Entonces* $\ell(D) = \deg D + 1 - g$.

Demostración. Sea C un divisor canónico, luego $\deg C = 2g - 2$ y obtenemos $deg(C - D) = \deg C - \deg D < 0$. Así, del Lema 2.16 obtenemos $\ell(C - D) = 0$ y del teorema de Riemann-Roch tenemos $\ell(D) = \deg D + 1 - g$. □

Ejemplo 2.22. El corolario anterior proporciona un método para calcular el género de un cuerpo de funciones, aunque generalmente no sea práctico. La idea es calcular $\deg(D) + 1 - \ell(D)$ para divisores cuyos grados crecen hasta el infinito, obteniendo así una secuencia de enteros que debe ser constante después de que el grado "sea lo suficientemente grande".
1) Usaremos este método para calcular el género de $K(x)$. Sea

$$P_\infty = \{f(X)/g(X) \in K(X) \mid \deg f(X) < \deg g(X)\}$$

(consulte el Ejemplo 2.9 (1) para recordar las definiciones y la notación que usaremos aquí) y sea n un entero positivo. Entonces

$$L(nP_\infty) = \{z \in K(X) \mid v_\infty(z) + n \geq 0 \text{ y } v_{p(X)}(z) \geq 0 \text{ para todo irreducible } p(X) \in K[X]\}.$$

Vamos a escribir $z \in K(X)$ como $z = \prod_{p(X)} p(X)^{n_{p(X)}}$, donde $p(X)$ recorre el conjunto de polinomios irreducibles en $K[X]$ y $n_{p(X)}$ es un número entero (por supuesto, $n_{p(X)} = 0$ excepto por un número finito de $p(X)$). Al recordar la definición de v_∞ vemos que $L(nP_\infty) = \{f(X) \in K[X] \mid \deg\, f(X) \leq n\} \cup \{0\}$, luego $\ell(nP_\infty) = n+1 = \deg\, nP_\infty + 1$. Esto muestra que $K(x)$ tiene género cero. Uno puede demostrar

la recíproca: si $F \mid K$ tiene género cero y un lugar racional, entonces $F = K(X)$ (vea [47, Proposition 1.6.3]).

2) También aplicaremos el método anterior para calcular el género del cuerpo de funciones $\mathbb{C}(x, y)$ descrito en el Ejemplo 2.9 (2) (consulte este ejemplo para las definiciones y la notación). Es un poco más elaborado, pero vamos a delinear el razonamiento. Para n un entero positivo, queremos determinar $L(nP_\infty)$ para calcular $\ell(nP_\infty)$. Tenemos

$$L(nP_\infty) = \{z \in \mathbb{C}(x, y) \mid w_\infty(z) + n \geq 0 \text{ y } w(z) \geq 0 \text{ siempre que } w \neq w_\infty\}.$$

Para $L' := \{z \in \mathbb{C}(x, y) \mid w(z) \geq 0 \text{ siempre que } w \neq w_\infty\}$, vamos a mostrar que

$$L' = \{p(x) + q(x)y \in \mathbb{C}(x, y) \mid p(x), q(x) \in \mathbb{C}[x]\}.$$

Sabemos que los elementos de $\mathbb{C}(x, y)$ pueden escribirse como $p(x) + q(x)y$ con $p(x), q(x) \in \mathbb{C}(x)$ y sea $\sigma : \mathbb{C}(x, y) \to \mathbb{C}(x, y)$ el automorfismo de $\mathbb{C}(x, y)$ definido por $\sigma(p(x) + q(x)y) = p(x) - q(x)y$ (en otras palabras, σ es el automorfismo de $\mathbb{C}(x, y)$ definido por $\sigma(x) = x$ y $\sigma(y) = -y$). Sea w una valoración de $\mathbb{C}(x, y)$. No es difícil comprobar que la composición $w \circ \sigma$ es también una valoración de $\mathbb{C}(x, y)$; además, si $P \neq P_\infty$ tenemos $w_P \circ \sigma \neq w_\infty$. De hecho, $(w_P \circ \sigma)(x) = w_P(\sigma(x)) = w_P(x) \geq 0$ ya que $x \in \mathcal{O}_P$, mientras que $w_\infty(x) = \text{mín}\{2 \cdot (-1), \infty\} = -2$. De esto podemos concluir que $\sigma(L') \subset L'$ porque si $z \in L'$ entonces $w(\sigma(z)) = (w \circ \sigma)(z) \geq 0$ para todos $w \neq w_\infty$. Por lo tanto, si $p(x) + q(x)y \in L'$ entones $p(x) - q(x)y \in L'$ y luego $p(x), q(x)y \in L'$. Ahora $L' \cap \mathbb{C}(x) = \{a(x) \in \mathbb{C}(x) \mid w(a(x)) \geq 0 \text{ siempre que } w \neq w_\infty\} = \{a(x) \in K(x) \mid a(x) \in \mathcal{O}_P \text{ para todos los lugares } P \neq P_\infty\}$ y de la descripción de los anillos de valoración en el Ejemplo 2.9 (2) obtenemos $L' \cap \mathbb{C}(x) = \mathbb{C}[x]$. Por lo tanto, $p(x) \in \mathbb{C}[x]$ y $(q(x)y)^2 = q(x)^2 \prod_{i=0}^{6}(x - i) \in \mathbb{C}[x]$; escribiendo $q(x)$ como el cociente de dos polinomios vemos que debemos tener $q(x) \in \mathbb{C}[x]$. Así $L' = \{p(x) + q(x)y \in \mathbb{C}(x, y) \mid p(x), q(x) \in \mathbb{C}[x]\}$ y como $L(nP_\infty) = L' \cap \{z \in F \mid w_\infty(z) + n \geq 0\}$ obtenemos

$$\begin{aligned} L(nP_\infty) &= \{p(x) + q(x)y \mid p(x), q(x) \in \mathbb{C}[x] \text{ y } w_\infty(p(x) + q(x)y) \geq -n\} \\ &= \{p(x) + q(x)y \mid p(x), q(x) \in \mathbb{C}[x],\ 2v_\infty(p(x)) \geq -n \\ &\qquad\qquad \text{y } 2v_\infty(q(x)) - 7 \geq -n\} \\ &= \{p(x) + q(x)y \mid p(x), q(x) \in \mathbb{C}[x],\ \deg(p(x)) \leq n/2 \\ &\qquad\qquad \text{y } \deg(q(x)) \leq (n-7)/2\}. \end{aligned}$$

De esto concluimos que

$$L(nP_\infty) = \begin{cases} [n/2] + 1 & \text{si } 1 \leq n \leq 6, \\ n + 1 - 3 & \text{si } n \geq 7, \end{cases}$$

y luego el género de $\mathbb{C}(x, y)$ es 3.

Necesitaremos, en una demostración en la próxima sección, el resultado a continuación (ver [47], sección 4.2, y especialmente el Teorema 4.2.6, para obtener resultados más generales). Recordemos que el anillo *de la serie formal de Laurent* sobre un cuerpo K, en la variable t, es el anillo $K((t)) := \{\sum_{i=n}^{\infty} a_i t^i \mid n \in \mathbb{Z}, a_i \in K \text{ para todo } i \geq n\}$ (este conjunto es un anillo con la suma y el producto habituales de la serie). Recuerde también que un *cuerpo perfecto* K es un cuerpo de característica cero o, si la característica es $p > 0$, entonces cada elemento tiene una raíz p-ésima en K. Por lo tanto, los cuerpos finitos son ejemplos de cuerpos perfectos (este es el ejemplo que nos interesará, especialmente en las dos últimas secciones).

Teorema 2.23. *Sea $F \mid K$ un cuerpo de funciones donde K es un cuerpo perfecto. Sea t un parámetro local en un lugar racional Q. Luego, existe un monomorfismo de anillos $\Phi : F \to K((t))$ que asocia a cada elemento $z \in F \setminus \{0\}$ una serie $\Phi(z) = \sum_{i=n}^{\infty} a_i t^i$, donde $a_n \neq 0$ y $n = v_P(z)$. La serie $\Phi(z)$ se denomina* expansión local de z en Q.

2.2. Semigrupos de Weierstrass de varios puntos. En lo que sigue, denotaremos el conjunto de enteros no negativos como $\mathbb{N}_0$. Sea $F \mid K$ un cuerpo de funciones de una variable y sea $f \in F$, $f \neq 0$. Ya vimos que f tiene un número finito de ceros y polos.

Definición 2.24. Llamamos al divisor $\mathrm{div}_0(f) := \sum_{P \in \mathcal{P} \text{ y } v_p(f)>0} v_P(f)P$ *divisor de ceros* de f, mientras que el divisor $\mathrm{div}_\infty(f) := \sum_{P \in \mathcal{P} \text{ y } v_p(f)<0} (-v_P(f))P$ se llamará *divisor de polos* de f.

Observe que $\mathrm{div}_0(f) \geq 0$, $\mathrm{div}_\infty(f) \geq 0$, $\mathrm{div}(f) = \mathrm{div}_0(f) - \mathrm{div}_\infty(f)$ y que $\deg(\mathrm{div}_0(f)) = \deg(\mathrm{div}_\infty(f))$.

Definición 2.25. El conjunto $H(Q) = \{n \in \mathbb{N}_0 \mid \exists f \in F \text{ tal que } \mathrm{div}_\infty(f) = nQ\}$ se denomina *semigrupo de Weierstrass asociado a Q*, o el *semigrupo de Weierstrass en Q*.

Recordamos que un *semigrupo* es una estructura algebraica que consiste en un conjunto no vacío H sobre el cual está definida una operación binaria asociativa y un *monoide* es un semigrupo que tiene un elemento neutro relativo a la operación (es decir, existe $0 \in H$ tal que $h + 0 = 0 + h = h$ para todos los $h \in H$). Observe que el conjunto $H(Q)$ es un subsemigrupo de $\mathbb{N}_0$, ya que si $n_1, n_2 \in H(Q)$ entonces existen $f_1, f_2 \in F$ tales que $\mathrm{div}_\infty(f_1) = n_1 Q$ y $\mathrm{div}_\infty(f_2) = n_2 Q$ y tomando $f := f_1 f_2$ obtenemos $\mathrm{div}_\infty(f) = (n_1 + n_2)Q$, es decir $n_1 + n_2 \in H(Q)$. En realidad, como $0 \in H(Q)$ (porque $\mathrm{div}_\infty(1) = 0Q$) tenemos que $H(Q)$ es un submonoide de $\mathbb{N}_0$, pero llamar a $H(Q)$ un semigrupo ya es un procedimiento estándar.

Un resultado muy útil al estudiar $H(Q)$ es el siguiente.

Lema 2.26. *Existe $f \in F \setminus \{0\}$ tal que $\mathrm{div}_\infty(f) = nQ$ si y sólo si $L((n-1)Q) \subsetneqq L(nQ)$.*

Demostración. Tenemos: $\mathrm{div}_\infty(f) = nQ$ para algún $f \in F \Leftrightarrow \mathrm{div}(f) + nQ \geq 0$ pero $\mathrm{div}(f) + (n-1)Q \not\geq 0 \Leftrightarrow f \in L(nQ) \setminus L((n-1)Q)$. □

Sea g el género de $F \mid K$. Si $n \geq 2g$, entonces del teorema de Riemann-Roch obtenemos $\ell(nQ) = n + 1 - g$, $\ell((n-1)Q) = (n-1) + 1 - g$, por lo tanto $\ell(nQ) - \ell((n-1)Q) = 1$, así que $L((n-1)Q) \subsetneqq L(nQ)$. Por lo tanto $\{n \in \mathbb{N}_0 \mid n \geq 2g\} \subset H(Q)$ y en particular, si $g = 0$, entonces $H(Q) = \mathbb{N}_0$. Supongamos que $g = 1$. Luego de Corolario 2.21 obtenemos $\ell(Q) = 1$ y como $\ell(0) = 1$ debemos tener $H(Q) = \{n \in \mathbb{N}_0 \mid n = 0 \text{ o } n \geq 2\}$. Entonces, asumimos que $g \geq 2$ y analizamos el caso donde $n \in \{1, \ldots, 2g-1\}$. Observe que $\ell(0Q) = 1$ y $\ell((2g-1)Q) = g$ y del Lema 2.18 obtenemos $0 \leq \ell(nQ) - \ell((n-1)Q) \leq 1$, por lo tanto, cuando n va de 0 a $2g-1$ existen $2g-1$ "saltos", mientras que la dimensión $\ell(nQ)$ salta $g-1$ veces, de 1 a g. Por lo tanto, podemos concluir que hay exactamente $g-1$ elementos $n \in \{1, \ldots, 2g-1\}$ satisfaciendo $L((n-1)Q) \subsetneqq L(nQ)$ y de lo que se hizo arriba obtenemos

$$H(Q) = \{n \in \mathbb{N}_0 \mid \exists f \in K \text{ tal que } \mathrm{div}_\infty(f) = nQ\} = \{0, \gamma_1, \ldots, \gamma_{g-1}\} \cup \{n \in \mathbb{N}_0 \mid n \geq 2g\}$$

donde $0 < \gamma_1 < \ldots < \gamma_{g-1} \leq 2g-1$, y luego $\#(\mathbb{N}_0 \setminus H(Q)) = g$, para cualquier $g \geq 0$.

Definición 2.27. El conjunto $\mathbb{N}_0 \setminus H(Q)$ se llama *conjunto de lagunas* o *secuencia de lagunas* en Q y sus g elementos se llaman *lagunas de Weierstrass en* Q; los elementos de $H(Q)$ a menudo se denominan *no-lagunas en* Q.

El semigrupo $H(Q)$ es un objeto clásico y muy estudiado, de enorme importancia en el estudio de los cuerpos de funciones y de las curvas algebraicas. En la Sección 2.4 daremos algunas aplicaciones de estos semigrupos a la teoría de codificación, pero su importancia va mucho más allá. Suponiendo que K es un cuerpo algebraicamente cerrado, se puede probar que para casi todos los lugares de $F \,|\, K$ (es decir, todos los lugares, excepto un número finito) la secuencia de lagunas es la misma (y si $K = \mathbb{C}$, entonces esta secuencia de lagunas es $\{1, \ldots, g\}$) y los lugares que tienen una secuencia de lagunas diferente se llaman *lugares de Weierstrass*. El lector interesado puede encontrar más información sobre los semigrupos y lugares de Weierstrass en [26, Sección 4.4], [29, Section 7.6] y [49]. Por ahora, demostramos un resultado simple que usaremos más tarde.

Lema 2.28. *Sea Q un lugar racional de un cuerpo de funciones $F \,|\, K$, sea α una laguna en Q, y sea C un divisor canónico de $F \,|\, K$. Entonces existe un elemento $h \in F$ tal que* $\operatorname{div}(h) + C = (\alpha - 1)Q + E$, *con $E \geq 0$ y $Q \notin \operatorname{supp} E$.*

Demostración. Si α es una laguna en Q, entonces $\ell(\alpha Q) = \ell((\alpha-1)Q)$. Del teorema de Riemann-Roch obtenemos $\alpha+1-g+\ell(C-\alpha Q) = (\alpha-1)+1-g+\ell(C-(\alpha-1)Q)$ y, por lo tanto, $\ell(C-(\alpha-1)Q) = \ell(C-\alpha Q)+1$. Entonces existe $h \in F$ tal que $\operatorname{div}(h) + C - (\alpha-1)Q \geq 0$ pero $\operatorname{div}(h) + C - \alpha Q \not\geq 0$. Así, tomando $E := \operatorname{div}(h)+C-(\alpha-1)Q$ tenemos $E \geq 0$, $\operatorname{div}(h)+C = (\alpha-1)Q+E$ y $Q \notin \operatorname{supp} E$. $\square$

Presentamos ahora una generalización directa del concepto de semigrupo de Weierstrass en un punto, a un conjunto de varios puntos. Por lo que sabemos, apareció por primera vez en [7, p. 366], pero su estudio sistemático comenzó con Kim ([36]) y Homma ([30]). Sea m un entero positivo. Observe que $\mathbb{N}_0^m$ es un semigrupo con la adición coordenada a coordenada de m-tuplas.

Definición 2.29. Sea m un entero positivo y sea $Q_1, \ldots, Q_m$ lugares de $F \,|\, K$ de grado uno. El subsemigrupo de $\mathbb{N}_0^m$ dado por

$$H(Q_1, \ldots, Q_m) := \{(\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m : \\ \exists f \in F \text{ con } \operatorname{div}_\infty(f) = \alpha_1 Q_1 + \ldots + \alpha_m Q_m\}$$

se llama *semigrupo de Weierstrass en* $Q_1, \ldots, Q_m$. A partir de las propiedades de las valoraciones, es fácil comprobar que se trata de un subsemigrupo de $\mathbb{N}_0^m$.

El conjunto complementario $G(Q_1, \ldots, Q_m) := \mathbb{N}_0^m \setminus H(Q_1, \ldots, Q_m)$ se llama el *conjunto de lagunas en* $Q_1, \ldots, Q_m$, y los elementos de $H(Q_1, \ldots, Q_m)$ se llaman *no-lagunas*.

De nuevo, observamos que $H(Q_1, \ldots, Q_m)$ es en realidad un monoide conmutativo, ya que, por ejemplo, $\operatorname{div}_\infty(1) = 0 = \sum_{i=1}^m 0Q_i$ y así $(0, \ldots, 0) \in H(Q_1, \ldots, Q_m)$.

En lo que sigue, usaremos la siguiente notación. Denotamos por $\mathbf{0}$ la m-tupla de $\mathbb{N}_0^m$ teniendo todas las entradas igual a cero; cuando escribimos $\boldsymbol{\alpha} \in \mathbb{N}_0^m$ debe entenderse que las entradas de esta m-tupla son $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_m)$ (de manera similar para $\boldsymbol{\beta}, \boldsymbol{\gamma} \in \mathbb{N}_0^m$). Además, para $i \in \{1, \ldots, m\}$ denotamos por $\boldsymbol{e}_i$ la m-tupla

que tiene todas las entradas iguales a cero, excepto la i-ésima entrada, que es igual a 1 y por v_i nos referimos a la valoración asociada a Q_i. Si $\boldsymbol{\alpha} \in \mathbb{N}_0^m$ anotamos como $L(\boldsymbol{\alpha})$ al espacio vectorial de Riemann-Roch $L(\alpha_1 Q_1 + \cdots + \alpha_m Q_m)$ y por $\ell(\boldsymbol{\alpha})$ nos referimos a $\dim L(\boldsymbol{\alpha})$. Sumamos m-tuplas de $\mathbb{N}_0^m$ y las multiplicamos por enteros de la manera habitual. Denotamos la m-tupla de los puntos $(Q_1, \ldots, Q_m)$ por $\mathbf{Q}_m$ y generalmente escribiremos $H(\mathbf{Q}_m)$ en lugar de $H(Q_1, \ldots, Q_m)$ y $G(\mathbf{Q}_m)$ en lugar de $G(Q_1, \ldots, Q_m)$.

Siempre asumiremos que $\#K \geq m$, si K es un cuerpo finito.

Lema 2.30. *Sea $\boldsymbol{\alpha} \in \mathbb{N}_0^m \backslash \{\mathbf{0}\}$. Entonces las siguientes afirmaciones son equivalentes*:

(1) $\boldsymbol{\alpha} \in H(\mathbf{Q}_m)$;
(2) $\ell(\boldsymbol{\alpha}) = \ell(\boldsymbol{\alpha} - \boldsymbol{e}_i) + 1$, *para todo $i \in \{1, \ldots, m\}$ tal que $\alpha_i > 0$.*

Demostración. Tenemos que (1) implica (2) simplemente porque si $\boldsymbol{\alpha} \in H(\mathbf{Q}_m)$ entonces existe $f \in F$ tal que $\mathrm{div}_\infty(f) = \alpha_1 Q_1 + \cdots + \alpha_m Q_m$, luego $f \in L(\boldsymbol{\alpha}) \setminus L(\boldsymbol{\alpha} - \boldsymbol{e}_i)$ para todo $i \in \{1, \ldots, m\}$ tal que $\alpha_i > 0$. Para ver que (2) implica (1), suponga que $\alpha_i > 0$ para algún $i \in \{1, \ldots, m\}$ y sean $f_1, \ldots, f_m \in F$ tales que $v_i(f_i) = -\alpha_i$ y $v_j(f_i) \geq -\alpha_j$ para todo $j \in \{1, \ldots, m\}$. Vamos a mostrar que existen elementos $\alpha_1, \ldots, \alpha_m \in K$ tales que el divisor de polos de $\sum_{i=1}^m \alpha_i f_i$ es precisamente $\sum_{i=1}^m \alpha_i Q_i$. Para cada $i = 1, \ldots, m$, sea t_i un parámetro local en Q_i. Sea

$$f_i = a_{i,j} t_j^{v_j(f_i)} + \cdots \in K((t_j))$$

la expansión local de f_i en Q_j (cf. Teorema 2.23). Luego, $\mathrm{div}_\infty(\sum_{i=1}^m \alpha_i f_i) \neq \sum_{i=1}^m \alpha_i Q_i$ si y sólo si existe $j \in \{1, \ldots, m\}$ tal que $\alpha_j > 0$ (es decir, $v_j(f_j) = -\alpha_j < 0$) y $v_j(\sum_{i=1}^m \alpha_i f_i) > -\alpha_j$), es decir, $\sum_{i=1}^m \alpha_i a_{i,j} = 0$; por lo tanto, para tener $\mathrm{div}_\infty(\sum_{i=1}^m \alpha_i f_i) = \sum_{i=1}^m \alpha_i Q_i$ es suficiente elegir una m-tupla $(\alpha_1, \ldots, \alpha_m) \in K^m$ fuera de la unión de (como máximo) m subespacios lineales de dimensión $m-1$. Cada uno de estos subespacios lineales tiene $(\#K)^{m-1}$ elementos y el origen es un elemento común a todos estos subespacios. Por lo tanto, debemos evitar como máximo un total de $m((\#K)^{m-1} - 1) + 1$ elementos y esto es posible porque $\#K \geq m$, luego $\#K^m > m(\#K)^{m-1} - m + 1$; y la prueba está completa. □

Lema 2.31. *Sea $\boldsymbol{\alpha} \in \mathbb{N}_0^m$ tal que $\alpha_i > 0$ para algún $i \in \{1, \ldots, m\}$. Las siguientes afirmaciones son equivalentes.*

(1) $\ell(\boldsymbol{\alpha}) = \ell(\boldsymbol{\alpha} - \boldsymbol{e}_i) + 1$;
(2) $\{\boldsymbol{\beta} \in H(\mathbf{Q}_m) \,|\, \beta_i = \alpha_i \text{ y } \beta_j \leq \alpha_j \text{ para todo } j = 1, \ldots, m\} \neq \emptyset$.

Demostración. Si $\ell(\boldsymbol{\alpha}) = \ell(\boldsymbol{\alpha} - \boldsymbol{e}_i) + 1$ entonces existe $f \in F$ tal que $\mathrm{div}_\infty(f) \leq \sum_{j=1}^m \alpha_j Q_j$ y $v_i(f) = -\alpha_i$. Así, escribiendo $\mathrm{div}_\infty(f) = \sum_{j=1}^m \beta_j P_j$ tenemos que $\boldsymbol{\beta} \in H(\mathbf{Q}_m)$, con $\beta_i = \alpha_i$ y $\beta_j \leq \alpha_j$ para todo $j = 1, \ldots, m$.

La implicación (2) $\Rightarrow$ (1) es fácil. □

En lo que sigue vamos a denotar el conjunto

$$\{\boldsymbol{\beta} \in H(\mathbf{Q}_m) \,|\, \beta_i = \alpha_i \text{ y } \beta_j \leq \alpha_j \text{ para todo } j = 1, \ldots, m\} \neq \emptyset$$

por $\nabla_i(\boldsymbol{\alpha})$, $i \in \{1, \ldots, m\}$.

Nos gustaría llamar la atención del lector sobre dos observaciones importantes: 1) El número de lagunas es siempre finito. De hecho, dado $\boldsymbol{\alpha} \in \mathbb{N}_0^m$, si $\sum_{j=1}^m \alpha_j \geq 2g$ entonces, del teorema de Riemann-Roch tenemos que $\ell(\boldsymbol{\alpha}) = \sum_{j=1}^n \alpha_j + 1 - g$ y para todo $i \in \{1, \ldots, m\}$ tales que $\alpha_i > 0$ obtenemos $\ell(\boldsymbol{\alpha} - \boldsymbol{e}_i) = (\sum_{j=1}^n \alpha_j - 1) + 1 - g = \ell(\boldsymbol{\alpha}) - 1$ y por lo tanto $\boldsymbol{\alpha} \in H(\mathbf{Q}_m)$.

2) Sea $i \in \{1, \ldots, m\}$, existe una biyección entre el semigrupo de Weierstrass (habitual) $H(Q_i)$ y el conjunto $\{\boldsymbol{\beta} \in H(\mathbf{Q}_m) \mid \boldsymbol{\beta} = a\boldsymbol{e}_i \text{ para algún } a \in \mathbb{N}_0\}$, definida por $a \mapsto a\boldsymbol{e}_i$ para todos los $a \in H(Q_i)$.

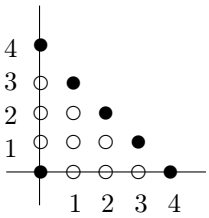
Como consecuencia de los lemas anteriores, tenemos el siguiente resultado.

Corolario 2.32. *Sea $\boldsymbol{\alpha} \in \mathbb{N}_0^m$ y supongamos que $\#K \geq m$. Entonces las siguientes afirmaciones son equivalentes:*

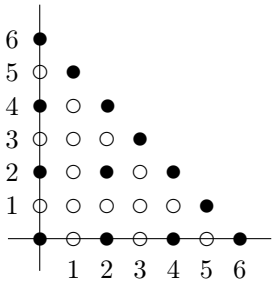
(1) $\boldsymbol{\alpha} \in G(\mathbf{Q}_m)$;
(2) *existe* $i \in \{1, \ldots, m\}$ *tal que* $\alpha_i > 0$ *y* $\ell(\boldsymbol{\alpha}) = \ell(\boldsymbol{\alpha} - \boldsymbol{e}_i)$;
(3) *existe* $i \in \{1, \ldots, m\}$ *tal que* $\alpha_i > 0$ *y* $\nabla_i(\boldsymbol{\alpha}) = \emptyset$.

En [36], Kim comenzó el estudio de $H(\mathbf{Q}_m)$ tratando el caso $m = 2$ (aunque él trabajó bajo las hipótesis de que K es algebraicamente cerrado y char$K = 0$, sus resultados son válidos para cuerpos perfectos de cualquier característica). Presentamos a continuación dos ejemplos de semigrupos de Weierstrass, basados en ejemplos de su trabajo.

Ejemplo 2.33. Sea $F = \mathbb{C}[x, y]$, donde $y^2 = \prod_{j=0}^{6}(x - j)$.
(i) Sean Q_1 y Q_2 los lugares tales que $\ell(Q_1 + Q_2) = 1$ (y luego no existe una función $f \in F \setminus K$ tal que $Q_1 + Q_2 \geq \text{div}_\infty(f)$). Tome, por ejemplo, los lugares asociados a los puntos $(7!, \sqrt{7!})$ y $(8!, \sqrt{8!})$. Se puede mostrar que en este caso $H(Q_1, Q_2)$ es el subsemigrupo de $\mathbb{N}_0^2$ cuyas lagunas se indican abajo como círculos vacíos:



Por otro lado, si consideramos que Q_1 y Q_2 son puntos de Weierstrass (por ejemplo, $(0, 0)$ y $(1, 0)$), entonces $H(Q_1, Q_2)$ es el subsemigrupo de $\mathbb{N}_0^2$ que tiene las siguientes lagunas:



Como podemos observar a partir de estos ejemplos, el número de lagunas puede variar con la elección de $Q_1, \ldots, Q_m$. Uno puede mostrar que

$$\#G(\mathbf{Q}_m) \geq \binom{m+g}{g}$$

(ver [36] para el caso $m = 2$, [33] para el caso $m \geq 2$ y [9] para una prueba de este hecho en una situación más general).

Como señalan Homma y Kim (véase [31]), para las aplicaciones de la teoría de la codificación, el siguiente concepto es importante.

Definición 2.34. Una *laguna de Weierstrass pura* de $H(\mathbf{Q}_m)$ es una laguna $\boldsymbol{\alpha}$ tal que, para todo $i \in \{1, \ldots, m\}$, tenemos $\alpha_i > 0$ y $\ell(\boldsymbol{\alpha}) = \ell(\boldsymbol{\alpha} - \boldsymbol{e}_i)$ (o, de manera equivalente, $\nabla_i(\boldsymbol{\alpha}) = \emptyset$). El conjunto de lagunas puras se denotará por $G_0(\mathbf{Q}_m)$.

De la equivalencia de (2) y (3) en el Corolario 2.32 obtenemos que $(1, 1)$, $(1, 2)$ y $(2, 1)$ son lagunas puras del semigrupo de Weierstrass del Ejemplo 2.33 (i), mientras que en el Ejemplo 2.33 (ii) las lagunas puras son los puntos (a, b) con $a, b \in \{1, 3, 5\}$.

Lema 2.35. *Si $\boldsymbol{\alpha} \in G_0(\mathbf{Q}_m)$, entonces α_i es una laguna de Weierstrass en Q_i, para todo $i \in \{1, \ldots, m\}$.*

Demostración. Sea $i \in \{1, \ldots, m\}$. De $\nabla_i(\boldsymbol{\alpha}) = \emptyset$ tenemos $\alpha_i \boldsymbol{e}_i \notin H(\mathbf{Q}_m)$, luego $\alpha_i \notin H(Q_i)$. □

Lema 2.36. *Las siguientes afirmaciones son equivalentes:*

(i) $\boldsymbol{\alpha} \in G_0(\mathbf{Q}_m)$;
(ii) $\ell(\boldsymbol{\alpha}) = \ell(\boldsymbol{\alpha} - \mathbf{1})$.

Demostración. Para demostrar que (i) implica (ii) supongamos que existe $f \in L(\boldsymbol{\alpha}) \setminus L(\boldsymbol{\alpha} - \mathbf{1})$, entonces debemos tener $v_i(f) = -\alpha_i$ para $i \in \{1, \ldots, m\}$, luego $\nabla_i(\boldsymbol{\alpha}) \neq \emptyset$ y $\boldsymbol{\alpha} \notin G_0(\mathbf{Q}_m)$. Para demostrar la recíproca, observamos que para cualquier $i \in \{1, \ldots, m\}$ tenemos $\ell(\boldsymbol{\alpha}) \geq \ell(\boldsymbol{\alpha} - \boldsymbol{e}_i) \geq \ell(\boldsymbol{\alpha} - \mathbf{1})$, luego las hipótesis implican $\ell(\boldsymbol{\alpha}) = \ell(\boldsymbol{\alpha} - \boldsymbol{e}_i)$ para todo $i \in \{1, \ldots, m\}$. □

2.3. Códigos de Goppa. Un *código* es un conjunto formado por combinaciones de un conjunto de símbolos que se llama el *alfabeto* del código. Una combinación del alfabeto que pertenece al código se llama *palabra* del código. Los códigos se utilizan para transmitir información, generalmente a través de un medio que puede manipular las palabras del código, transformándolas en otras palabras o en combinaciones que no están en el código. Los llamados *códigos correctores de errores* tienen la propiedad de que, si el medio no cambia "demasiado" una palabra, la palabra original puede recuperarse de la palabra recibida. Esta propiedad se deriva del hecho de que cada palabra, en dichos códigos, transporta no solo información, sino también cierta "redundancia de información" que se utiliza para recuperar palabras que han sido cambiadas.

Uno de los tipos más comunes de códigos correctores de errores es el *código lineal*.

Definición 2.37. Un *código lineal de longitud n* sobre un cuerpo finito K es simplemente un subespacio vectorial de K^n. Sea $\mathcal{C} \subset K^n$ un código lineal y sean $v, w \in \mathcal{C}$. La *distancia de Hamming* entre $v = (v_1, \ldots, v_n)$ y $w = (w_1, \ldots, w_n)$ se define como $d(v, w) := \#\{i \mid v_i \neq w_i\}$. La *distancia mínima de un código* es el número $\min\{d(v, w) \mid v, w \in \mathcal{C}, v \neq w\}$, o equivalentemente, $\min\{d(v, 0) \mid v \in \mathcal{C}, v \neq 0\}$.

Siempre trabajaremos con códigos lineales y por eso omitiremos la palabra lineal. Un *código* $[n, k, d]$ es un código de longitud n, dimensión k y distancia mínima d. Para aplicaciones, generalmente queremos códigos con una distancia mínima d grande, ya que no es difícil mostrar que si un medio de transmisión cambia como máximo $(d - 1)/2$ entradas en una palabra w, convirtiéndola en una n-tupla w',

entonces w será la única palabra del código cuya distancia para w' es como máximo $(d-1)/2$ y decodificaremos la n-tupla w' recibida como w. También es deseable tener una gran dimensión k, ya que esto significa que el código puede transmitir grandes cantidades de información. Sin embargo, para un n de longitud fija, no podemos tener grandes d y k, debido a la cota de Singleton.

Lema 2.38 (Cota de Singleton)**.** *Sea C un código $[n,k,d]$. Entonces*

$$k+d \leq n+1.$$

Demostración. Sea w el subespacio de K^n definido por $W = \{(a_1,\ldots,a_n) \in K^n \mid a_i = 0 \text{ para todo } i \geq d\}$. Como $d(w,0) \leq d-1$ para todo $w \in W$, tenemos $W \cap C = \{0\}$. De $\dim W = d-1$ obtenemos $k+(d-1) \leq n$, que prueba el lema. □

Definición 2.39. Si $\mathcal{C} \subset K^n$ es un código, entonces

$$\mathcal{C}^{\perp} := \{w \in K^n \mid \langle w, v\rangle = 0 \text{ para todo } v \in \mathcal{C}\}$$

se llama *código dual* de $\mathcal{C}$ (aquí $\langle\ ,\ \rangle$ denota el producto interno habitual en K^n).

Presentamos ahora la construcción, debido a V.D. Goppa, que usa material de las secciones anteriores, para obtener los llamados *códigos (geométricos) de Goppa.*

Sea $F \mid K$ un cuerpo de funciones de una variable. Sean G y D divisores de $F \mid K$ con soporte disjunto, con D de la forma $D = P_1 + \cdots + P_n$, donde $P_1,\ldots,P_n$ son lugares racionales de $F \mid K$. Sea $\varphi : L(G) \to K^n$ la función definida por $\varphi(f) = (f(P_1),\ldots,f(P_n))$ (recuerde que $f(P)$ es la clase de $f \in \mathcal{O}_P$ en $\mathcal{O}_p/P$, cf. pág. 14); luego, φ es una transformación lineal de K-espacios vectoriales y $\varphi(L(G))$ es un código de longitud n; denotaremos este código como $\mathcal{C}(D,G)$. Una ventaja de esta construcción es que de inmediato podemos calcular o encontrar una estimación de los principales parámetros del código.

Teorema 2.40. *$\mathcal{C}(D,G)$ es un código $[n,k,d]$, donde $k = \dim L(G) - \dim L(G-D)$ y $d \geq n - \deg G$.*

Demostración. Observe que φ es una transformación lineal suryectiva sobre $\mathcal{C}(D,G)$ y

$$\begin{aligned}
\operatorname{Ker}(\varphi) &= \{f \in L(G) \mid f(P_i) = 0 \text{ para todo } i = 1,\ldots,n\}\\
&= \{f \in L(G) \mid v_{P_i}(f) > 0 \text{ para todo } i = 1,\ldots,n\}\\
&= \{f \in L(G) \mid \operatorname{div}_0(f) \geq D\}\\
&= \{f \in F \mid \operatorname{div}_0(f) \geq D \text{ y } \operatorname{div}_0(f) - \operatorname{div}_\infty(f) + G \geq 0\}\\
&= \{f \in F \mid \operatorname{div}(f) + G - D \geq 0\} = L(D-G).
\end{aligned}$$

La definición de distancia mínima tiene sentido sólo si el código tiene un elemento distinto de cero, lo que asumimos ahora. Sea $x \in L(G)$ tal que $\varphi(x) \neq 0$ (en particular $x \neq 0$) y tal que $d = d(\varphi(x),0)$. Luego, existe un subconjunto $\Lambda \subset \{1,\ldots,n\}$ de cardinalidad $n-d$ tal que si $i \in \Lambda$ entonces $v_{P_i}(x) > 0$ (y $v_{P_j}(x) \neq 0$ si $j \notin \Lambda$). Por lo tanto $x \in L(G - \sum_{i\in\Lambda} P_i)$, luego $\deg(G - \sum_{i\in\Lambda} P_i) \geq 0$ y tenemos $d \geq n - \deg G$. □

En lo que sigue, denotamos por g el género de $F \mid K$.

Corolario 2.41. *Supongamos que $\deg G < \deg D = n$. Entonces $\varphi : L(G) \to \mathcal{C}(D,G)$ es inyectiva y:*

(1) $\mathcal{C}(D,G)$ *es un código* $[n,k,d]$ *con* $d \geq n - \deg G$ *y* $k = \dim G \geq \deg G + 1 - g$ *(luego* $k + d \geq n + 1 - g$*);*
(2) *suponiendo además que* $2g - 2 < \deg G < n$*, tenemos* $k = \deg G + 1 - g$.

Demostración. Si $\deg(G-D) < 0$ entonces $\dim L(G-D) = 0$ y del teorema anterior tenemos $k = \dim L(G)$, por lo tanto, φ es inyectiva. Del teorema de Riemann-Roch obtenemos $\dim L(G) = \deg G + 1 - g + \dim L(C - G) \geq \deg G + 1 - g$, donde C es un divisor canónico; si $\deg G < \deg C = 2g - 2$ entonces $\dim L(C - G) = 0$, luego $k = \deg G + 1 - g$. □

En estas notas llamamos al número $n - \deg G$ la *cota de Goppa para la distancia mínima de* $\mathcal{C}(D,G)$.

Se puede probar [47, Proposition 2.2.10] que el código que es el dual de $\mathcal{C}(D,G)$ es el código $\mathcal{C}(D, D - G + C)$, donde C es un divisor canónico tal que $D - G + C$ es un divisor cuyo soporte es disjunto del soporte de D (en el curso de la determinación de $\mathcal{C}(D,G)^\perp$ uno ve que de hecho existe tal divisor canónico). No lo probaremos, pero demostramos al menos que $\mathcal{C}(D, D - G + C)$ tiene la dimensión correcta. Pero primero, presentamos algunos hechos sobre los parámetros de $\mathcal{C}(D,G)^\perp$.

Corolario 2.42. $\mathcal{C}(D,G)^\perp$ *es un código* $[n,k',d']$*, con* $k' = \ell(C-(G-D))-\ell(C-G)$ *y* $d' \geq \deg G - (2g-2)$*. Si* $\deg G > 2g - 2$ *entonces* $k' = \ell(C - (G - D)) \geq n + g - 1 - \deg G$ *y si* $2g - 2 < \deg G < n$*, entonces* $k' = n + g - 1 - \deg G$.

Demostración. La primera afirmación es una consecuencia del Teorema 2.40 y del hecho de que $\mathcal{C}(D,G)^\perp = \mathcal{C}(D, D - G + C)$. Las otras afirmaciones se obtienen de la primera y del teorema de Riemann-Roch. □

Observe que $\dim \mathcal{C}(D,G) + \dim \mathcal{C}(D, D - G + C) = \ell(G) - \ell(G - D) + \ell(D - G + C) - \ell(C - G) = \ell(G) - \ell(C - G) - (\ell(G - D) - \ell(C - (G - D))) = \deg G + 1 - g - (\deg G - \deg D + 1 - g) = \deg D = n$, que es el resultado esperado.

En estas notas llamaremos al número $\deg G - (2g - 2)$ *la cota de Goppa para la distancia mínima de* $\mathcal{C}(D,G)^\perp$.

2.4. Semigrupos de Weierstrass y códigos de Goppa. En esta sección pretendemos mostrar cómo utilizar la información de los semigrupos de Weierstrass en varios puntos para construir códigos de Goppa que tengan cotas para la distancia mínima mejor que la cota de Goppa.

Sea $F \mid K$ un cuerpo de funciones de una variable; en esta sección, K es siempre un cuerpo finito. Comenzamos con una aplicación del semigrupo de Weierstrass habitual para construir códigos con una distancia mínima "grande" y que apareció en un trabajo de García, Kim y Lax (ver [18]).

Teorema 2.43. *Sean* $Q, P_1, \ldots, P_n$ *lugares racionales distintos de* $F \mid K$*. Supongamos que hay un conjunto de* $t + 1$ *lagunas consecutivas en* $H(Q)$*, digamos* $\gamma - t, \ldots, \gamma - 1, \gamma$ *(donde* t *es un entero no negativo). Para* $G := \gamma Q$*, si el código* $\mathcal{C}(D,G)$ *tiene una dimensión positiva, entonces* $n - \deg G + t + 1$ *es una cota inferior para su distancia mínima.*

Demostración. Supongamos que existe $f \in L(G)$ tal que $w := d(\varphi(f), 0) \leq n - \deg G + t$ (recuerde que φ es la función que aparece en la construcción de $\mathcal{C}(D,G)$ —vea la página 25); esto significa que existe un subconjunto $\Lambda \subset \{1, \ldots, n\}$ tal que $\#\Lambda = n - w$ y $v_{P_i}(f) > 0$ para todo $i \in \Lambda$ (y por supuesto, $v_{P_j}(f) = 0$ para $j \in \{1, \ldots, n\} \setminus \Lambda$). Luego $\operatorname{div}(f) + G > \sum_{i \in \Lambda} P_i$ por lo tanto $E := \operatorname{div}(f) +$

$G - \sum_{i\in\Lambda} P_i \geq 0$, además $\deg E = \deg G - n + w \leq t$, entonces escribimos $E = \lambda Q + E'$, donde $E' \geq 0$ y $Q \notin \operatorname{supp} E'$; observe que $0 \leq \lambda \leq t$. Por lo tanto, $\operatorname{div}(f) = \lambda Q + E' - G + \sum_{i=1}^{n-w} P_i = -(\gamma - \lambda)Q + E' + \sum_{i\in\Lambda} P_i$, de modo que $\gamma - \lambda \in H(Q)$. □

El teorema anterior muestra que la existencia de $t+1$ lagunas de Weierstrass consecutivas en el semigrupo $H(Q)$ de un lugar racional Q permite la construcción de un código de Goppa cuya cota para la distancia mínima puede mejorarse mediante $t+1$ en comparación con la cota de Goppa. El caso $t = 0$ de este teorema fue probado por Janwa (ver [34]).

Presentamos ahora un teorema de García y Lax que muestra cómo construir un código dual con una cota inferior mejor que la cota de Goppa para la distancia mínima (ver [19]).

Teorema 2.44. *Sean $Q, P_1, \ldots, P_n$ lugares racionales distintos de $F \mid K$ y sean α y β lagunas de Weierstrass en Q. Sean $D := P_1 + \cdots + P_n$ y $G := (\alpha + \beta - 1)Q$. Si $\dim \mathcal{C}(D,G)^\perp > 0$, entonces $\deg G - (2g-2) + 1$ es una cota inferior para la distancia mínima de $\mathcal{C}(D,G)^\perp$.*

Demostración. Recordemos que $\mathcal{C}(D,G)^\perp = \mathcal{C}(D, D-G+C)$, donde C es un divisor canónico tal que $\operatorname{supp}(D-G+C) \cap \operatorname{supp}(D) = \emptyset$. Sea $\varphi : L(G) \to \mathcal{C}(D, D-G+C)$ como en la sección anterior. Suponga que hay un elemento $f \in L(G)$ tal que $w := d(\varphi(f), 0) \leq \deg G - (2g-2)$. Como $\deg G - (2g-2)$ es una cota inferior para la distancia mínima, debemos tener $w = \deg G - (2g-2)$. Entonces existe $\Gamma \subset \{1, \ldots, n\}$ tal que $\#\Gamma = w$ y $v_{P_i}(f) = 0$ para todo $i \in \Gamma$ (y $v_{P_j}(f) > 0$ para todo $j \in \{1, \ldots, n\} \setminus \Gamma$). Por lo tanto, $\operatorname{div}(f) + C + D - G \geq \sum_{j\in\{1,\ldots,n\}\setminus\Gamma} P_j$ y así $\operatorname{div}(f) + C \geq G - \sum_{j\in\Gamma} P_j$. Observe que ambos lados de esta desigualdad tienen el mismo grado, luego $\operatorname{div}(f) + C = G - \sum_{j\in\Gamma} P_j$. Dado que α es una laguna en Q tenemos, del Lema 2.28, que existe $h \in F$ tal que $\operatorname{div}(h) + C = (\alpha - 1)Q + E$, con $E \geq 0$ y $Q \notin \operatorname{supp} E$. Por lo tanto, $\operatorname{div}(h/f) = \operatorname{div}(h) - \operatorname{div}(f) = \sum_{j\in\Gamma} P_j + E - \beta Q$ y tenemos $\beta \in H(Q)$, contradiciendo una hipótesis. □

En [18] los autores presentan la siguiente generalización del resultado anterior (que no demostraremos aquí).

Teorema 2.45. *Sean $Q, P_1, \ldots, P_n$ lugares racionales distintos de $F \mid K$. Supongamos que $\alpha, \ldots, \alpha + t, \beta - (t-1), \ldots, \beta - 1, \beta$ son lagunas de Weierstrass en Q, con $\alpha + t \leq \beta$ y $t \geq 1$. Sean $D := P - 1 + \cdots + P_n$ y $G := (\alpha + \beta - 1)Q$; si $\dim \mathcal{C}(D,G)^\perp > 0$, entonces $\deg G - (2g-2) + t + 1$ es una cota inferior para la distancia mínima de $\mathcal{C}(D,G)^\perp$.*

Corolario 2.46. *Sean $Q, P_1, \ldots, P_n$ lugares racionales distintos de $F \mid K$. Supongamos que $\alpha, \ldots, \alpha + t$ son $t+1$ lagunas de Weierstrass consecutivas en Q. Sean $D := P_1 + \cdots + P_n$ y $G := (2\alpha + t - 1)Q$; si $\dim \mathcal{C}(D,G)^\perp > 0$, entonces $\deg G - (2g-2) + t + 1$ es una cota inferior para la distancia mínima de $\mathcal{C}(D,G)^\perp$.*

En 2001, en su tesis doctoral, escrita bajo la supervisión de R.F. Lax, Gretchen Matthews dio la primera aplicación de los semigrupos de Weierstrass en más de un punto a la teoría de codificación (ver [27]). Uno de sus principales resultados en ese trabajo es el siguiente.

Teorema 2.47. *Sean $Q_1, Q_2, P_1, \ldots, P_n$ lugares racionales distintos de $F \mid K$. Suponga que $(\alpha_1, \alpha_2) \in G(Q_1, Q_2)$ con $\alpha_1 > 1$ y $\ell(\alpha_1 Q_1 + \alpha_2 Q_2) = \ell((\alpha_1 -$*

$1)Q_1 + \alpha_2 Q_2)$. *Suponga además que* $(\gamma_1, \gamma_2 - t - 1) \in G(Q_1, Q_2)$ *para todo* t, $0 \leq t \leq min\{\gamma_2 - 1, 2g - 1 - (\alpha_1 + \alpha_2)\}$. *Sean* $G = (\alpha_1 + \gamma_1 - 1)Q_1 + (\alpha_2 + \gamma_2 - 1)Q_2$, *y* $D = P_1 + \cdots + P_n$. *Si la dimensión de* $\mathcal{C}(D, G)^\perp$ *es positiva, entonces la distancia mínima de este código es al menos* $\deg G - (2g - 2) + 1$.

Poco después de la publicación del trabajo de Matthews, un trabajo de Homma y Kim introdujo el concepto de "lagunas puras", que vimos en la Sección 2.2 y lo usaron para obtener códigos con cotas inferiores mejores para la distancia mínima. Homma y Kim trabajaron con el semigrupo de Weierstrass en dos puntos, y sus resultados han sido generalizados al caso de los semigrupos de Weierstrass en m puntos, m cualquier entero positivo, por C. Carvalho y F. Torres (ver [10]). Para presentar los principales resultados de [10], comenzamos con un resultado de Homma y Kim (ver [31]), ligeramente modificado para estas notas.

Lema 2.48. *Sean* B, E, N *y* M *divisores de* $F \,|\, K$, *con* $B \geq 0$. *Si*

(1) $N + M + E$ *es un divisor canónico;*
(2) $\ell(M - B) = \ell(M)$;
(3) $\ell(N) \leq \ell(N + E)$;
(4) $\ell(N) = \ell(N + B)$;

entonces $\deg B \leq \deg E$.

Demostración. Por supuesto, tenemos que $N + M + E = (N + B + E) + (M - B)$ es un divisor canónico, por lo tanto, del teorema de Riemann-Roch obtenemos $\ell(N + B + E) = \deg N + \deg B + \deg E + 1 - g + \ell(M - B)$ y $\ell(N + E) = \deg N + \deg E + 1 - g + \ell(M)$, donde g es el género de $F \,|\, K$. Usando (2) obtenemos $\ell(N + B + E) - \ell(N + E) = \deg B$. Ahora, de (3), (4) y el teorema de Riemann-Roch, obtenemos $\deg B = \ell(N + B + E) - \ell(N + E) \leq \ell(N + B + E) - \ell(N) = \ell(N + B + E) - \ell(N + B) \leq \deg E$. □

Lema 2.49. [31, Lema 3.1] *Sean* M *y* B *divisores de* $F \,|\, K$ *con* $B \geq 0$ *y* $\ell(M) = \ell(M - B)$. *Si* $R \geq 0$ *es un divisor que satisface* $\operatorname{supp} R \cap \operatorname{supp} B = \emptyset$, *entonces* $\ell(M - R) = \ell(M - R - B)$.

Demostración. Observe que $L(M - B) \subset L(M)$ y $L(M - R) \subset L(M)$; de $\operatorname{supp} R \cap \operatorname{supp} B = \emptyset$ obtenemos $L(M - B) \cap L(M - R) = L(M - R - B)$, por lo tanto debemos tener $L(M - R) = L(M - R - B)$ ya que $L(M) = L(M - B)$. □

Uno de los principales resultados de [10] es el siguiente.

Teorema 2.50. [10, Teorema 3.3] *Sean* $Q_1, \ldots, Q_m, P_1, \ldots, P_n$ *lugares racionales distintos de* $F \,|\, K$. *Supongamos que* $(\alpha_1, \ldots, \alpha_m)$ *y* $(\beta_1, \ldots, \beta_m)$ *son lagunas puras en* $Q_1, \ldots, Q_m$. *Sea* $G = \sum_{i=1}^{m} (\alpha_i + \beta_i - 1)Q_i$ *y* $D = P_1 + \cdots + P_n$. *Si la dimensión de* $\mathcal{C}(D, G)^\perp$ *es positiva, entonces a distancia mínima de este código es al menos* $\deg G - (2g - 2) + m$.

Demostración. Recuerde que $\mathcal{C}(D, G)^\perp = \mathcal{C}(D, D - G + C)$, donde C es un divisor canónico tal que $\operatorname{supp}(D - G + C) \cap \operatorname{supp}(D) = \emptyset$ y sea $\varphi : L(D - G + C) \to \mathcal{C}(D, D - G + C)$ la función definida en la página 25 (es decir, $\varphi(h) = (h(P_1), \ldots, h(P_n))$ para todo $h \in L(D - G + C)$). Sea $f \in L(G)$ y sea $w = d(\varphi(f), 0)$, luego existe un subconjunto $\Lambda \subset \{1, \ldots, n\}$ tal que $\#\Lambda = w$, $v_{P_i}(f) = 0$ si $i \in \Lambda$ y $v_{P_i}(f) > 0$ si $i \in \{1, \ldots, n\} \setminus \Lambda$. Por lo tanto, $\operatorname{div}(f) + D - G + C \geq \sum_{i \in \{1, \ldots, n\} \setminus \Lambda} P_i$ (aquí estamos usando que $\operatorname{supp}(D - G + C) \cap \operatorname{supp}(D) = \emptyset$ y que $\operatorname{supp}(G) \cap \operatorname{supp}(D) = \emptyset$) por lo

tanto $\operatorname{div}(f) + C - G + \sum_{i\in\Lambda} P_i \geq 0$. Sean $B := \sum_{i=1}^{m} Q_i$, $E := C - G + \sum_{i\in\Lambda} P_i$, $N := \sum_{i=1}^{m}(\alpha_i - 1)Q_i$ y $M := \sum_{i=1}^{m} \beta_i Q_i - \sum_{i\in\Lambda} P_i$. Entonces $E + N + M$ es el divisor canónico C, $\ell(N) = \ell(N + B)$ por Lema 2.36 y $\ell(M - B) = \ell(M)$ por Lema 2.36 y el lema anterior. También tenemos $\ell(N) \leq \ell(N + \operatorname{div}(f) + E)$, porque $\operatorname{div}(f) + E \geq 0$; de $N \geq 0$ tenemos $\operatorname{div}(f) + E + N \geq 0$, por lo tanto, $f \in L(E + N)$ y $\ell(\operatorname{div}(f) + E + N) = \ell(E + N)$, luego $\ell(N) \leq \ell(N + E)$. Por lo tanto, del Lema 2.48 obtenemos $\deg B \leq \deg E$, es decir, $m \leq 2g - 2 - \deg G + w$, de modo que $w \geq \deg G - (2g - 2) + m$. □

Otro resultado principal de [10] es el siguiente.

Teorema 2.51. [10, Teorema 3.4] *Sean $Q_1, \ldots, Q_m, P_1, \ldots, P_n$ lugares racionales distintos de $F \mid K$. Sean $(\alpha_1, \ldots, \alpha_m), (\beta_1, \ldots, \beta_m) \in \mathbb{N}_0^m$ tales que $\alpha_i \leq \beta_i$ para todo $i \in \{1, \ldots, m\}$ y asuma que cada m-tupla $(\gamma_1, \ldots, \gamma_m) \in \mathbb{N}_0^m$ con $\alpha_i \leq \gamma_i \leq \beta_i$ para todo $i \in \{1, \ldots, m\}$ es una laguna pura en $Q_1, \ldots, Q_m$. Sea $G = \sum_{i=1}^{m}(\alpha_i + \beta_i - 1)Q_i$ y $D = P_1 + \cdots + P_n$. Si la dimensión de $\mathcal{C}(D, G)^{\perp}$ es positiva, entonces la distancia mínima de este código es al menos* $\deg G - (2g - 2) + m + \sum_{i=1}^{m}(\beta_i - \alpha_i)$.

Demostración. Sean φ, f, w y Λ como en el comienzo de la prueba anterior. Entonces, como arriba, tenemos $\operatorname{div}(f) + C - G + \sum_{i\in\Lambda} P_i \geq 0$. Ahora sea $B := \sum_{i=1}^{m}(\beta_i - \alpha_i + 1)Q_i$ y como arriba, tome $E := C - G + \sum_{i\in\Lambda} P_i$, $N := \sum_{i=1}^{m}(\alpha_i - 1)Q_i$ y $M := \sum_{i=1}^{m} \beta_i Q_i - \sum_{i\in\Lambda} P_i$. Entonces $E + N + M$ es un divisor canónico y $N + B = \sum_{i=1}^{m} \beta_i Q_i$. Así, a partir de la definición de lagunas puras y del Lema 2.36, obtenemos $\ell(N + B) = \ell(N)$. Además, como $\ell(\sum_{i=1} \beta_i Q_i) = \ell(\sum_{i=1}(\alpha_i - 1)Q_i) = \ell(\sum_{i=1} \beta_i Q_i - B)$ y $\operatorname{supp} B \cap \operatorname{supp}(\sum_{i\in\Lambda} P_i) = \emptyset$ obtenemos del Lema 2.49 que $\ell(\sum_{i=1}^{m} \beta_i Q_i - \sum_{i\in\Lambda} P_i) = \ell(\sum_{i=1} \beta_i Q_i - B - \sum_{i\in\Lambda} P_i)$, es decir, $\ell(M) = \ell(M - B)$. Como en la prueba anterior, tenemos $\ell(N) \leq \ell(N + E)$, así que del Lema 2.48 obtenemos $\deg B \leq \deg E$, es decir, $\sum_{i=1}^{m}(\beta_i - \alpha_i + 1) \leq 2g - 2 - \deg G + w$, luego $w \geq \deg G - (2g - 2) + m + \sum_{i=1}^{m}(\beta_i - \alpha_i)$. □

Observe que, de alguna manera, este resultado extiende los resultados 2.43 y 2.44, si pensamos que todos las lagunas puras en la hipótesis son "¡lagunas consecutivas!".

3. Curvas maximales

Al escribir el material de esta sección, intentamos presentar algunos de los problemas que se estudian hoy en esta área. La selección de los temas es algo personal y solo muestra una pequeña parte del panorama completo. Esperamos que sea un buen punto de partida para aquellos estudiantes interesados en este tema.

El propósito de esta sección es estudiar curvas definidas sobre cuerpos finitos, interesados particularmente en curvas con "muchos" puntos racionales. Tales curvas resultan muy útiles en Teoría de Códigos ya que para códigos fabricados a partir de tales curvas, la distancia mínima es grande.

Algunas veces, para probar los resultados es más fácil usar el lenguaje de cuerpos de funciones y a veces, para trabajar con ejemplos concretos es más fácil usar el lenguaje de curvas, así que comenzaremos mostrando que existe un diccionario que nos permite pasar de un lenguaje al otro sin problemas.

3.1. Definiciones básicas. Los detalles y pruebas de la parte de curvas pueden ser encontrados en [28], [15], [45] y [46], mientras que los detalles sobre cuerpos de funciones en [47].

Sea $\mathbb{F}_q$ un cuerpo finito con q elementos, denotamos por $\bar{\mathbb{F}}_q$ el cierre galoisiano. Podemos pensar que el espacio proyectivo puede ser obtenido a partir del espacio afín, agregando puntos en el infinito.

Definición 3.1. El conjunto $\mathbb{A}^n(\bar{\mathbb{F}}_q) = \{(a_1, \ldots, a_n) : a_i \in \bar{\mathbb{F}}_q \ \forall i\}$ es llamado de *n-espacio afín.*

El *espacio proyectivo*, que denotaremos por $\mathbb{P}^n(\bar{\mathbb{F}}_q)$ es el conjunto formado por las clases de equivalencia cuando consideramos la siguiente relación definida sobre $\mathbb{A}^{n+1}$:

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) \Leftrightarrow \exists \lambda \in \bar{\mathbb{F}}_q^* \text{ tal que } a_i = \lambda b_i \ \forall i.$$

Así, un punto $P \in \mathbb{P}^n(\bar{\mathbb{F}}_q)$ será denotado por $P = (a_0 : \cdots : a_n)$.

Note que si $\sigma \in G = Gal(\bar{\mathbb{F}}_q, \mathbb{F}_q)$ entonces σ actúa sobre $\mathbb{P}^n(\bar{\mathbb{F}}_q)$ como sigue:

$$\sigma((a_0 : \cdots : a_n)) = (\sigma(a_0) : \cdots : \sigma(a_n)).$$

En particular, el automorfismo de Frobenius nos permite caracterizar el conjunto $\mathbb{P}^n(\mathbb{F}_q)$ de puntos $\mathbb{F}_q$-racionales (o sea, puntos cuyas coordenadas pertenecen a $\mathbb{F}_q$) ya que estos puntos son dejados fijos por este automorfismo.

Otra consecuencia de este hecho es que el número de puntos racionales de $\mathbb{P}^n(\bar{\mathbb{F}}_q)$ es $q^{n+1}/(q-1)$.

Definición 3.2. Considere $P \in \mathbb{P}^n(\bar{\mathbb{F}}_q)$, entonces

1. El conjunto $\mathbf{P} = \{\sigma(P) : \sigma \in G\}$ es un *punto cerrado* sobre $\mathbb{F}_q$.
2. La cardinalidad del conjunto $\{\sigma(P) : \sigma \in G\}$ es el *grado* de $\mathbf{P}$.

Si $P = (a_0 : \cdots : a_n)$ es un elemento de $\mathbf{P}$ con $a_i \neq 0$ entonces

$$\mathbf{P} = \{\sigma(P) : \sigma \in G\} = \{\sigma(P) : \sigma \in Gal(\mathbb{F}_q(a_0/a_i, \ldots, a_n/a_i); \mathbb{F}_q)\}$$

y el grado de $\mathbf{P}$ es igual al grado de la extensión $\mathbb{F}_q(a_0/a_i, \ldots, a_n/a_i)|\mathbb{F}_q)$.

Vamos a definir qué es una variedad afín. Sea S un subconjunto de $\bar{\mathbb{F}}_q[x_1, \ldots, x_n] = \bar{\mathbb{F}}_q[X]$. Definimos el conjunto $V(S)$ de ceros de S por

$$V(S) := \{P \in \mathbb{A}^n(\bar{\mathbb{F}}_q) : f(P) = 0 \ \forall f \in S\}.$$

Definición 3.3. Un *conjunto algebraico afín* es cualquier conjunto de la forma $V(S)$ para algún $S \subseteq \bar{\mathbb{F}}_q[X]$.

Diremos que el conjunto $V(S)$ está definido sobre $\mathbb{F}_q$ si $S \subseteq \mathbb{F}_q[X]$ y será denotado en este caso por $V|\mathbb{F}_q$.

El conjunto de puntos racionales de $V|\mathbb{F}_q$ es

$$V(\mathbb{F}_q) = V \cap \mathbb{A}^n(\mathbb{F}_q).$$

Definición 3.4. Un conjunto algebraico afín V es *reducible* si existen dos conjuntos algebraicos afines V_1 y V_2 tales que $V_i \neq V$ para $i = 1, 2$ y $V = V_1 \cup V_2$. Si V es no vacío y no reducible, diremos en este caso que V es *irreducible.*

Un conjunto afín $V|\mathbb{F}_q$ tiene asociado los ideales

$$I(V) = \{f \in \bar{\mathbb{F}}_q[X] : f(P) = 0 \ \forall P \in V\},$$
$$I(V|\mathbb{F}_q) = I(V) \cap \mathbb{F}_q[X].$$

Observación 3.5. Un conjunto algebraico afín es irreducible si y solamente si $I(V)$ es un ideal primo de $\bar{\mathbb{F}}_q[X]$.

Definición 3.6. Un conjunto algebraico afín $V|\mathbb{F}_q$ es una *variedad afín* si $I(V|\mathbb{F}_q)$ es un ideal primo de $\mathbb{F}_q[X]$.

Para una variedad afín $V|\mathbb{F}_q$ definimos:

1. El *anillo de coordenadas* de $V|\mathbb{F}_q$ como $\mathbb{F}_q[V] = \mathbb{F}_q[X]/I(V|\mathbb{F}_q)$;
2. El *anillo de coordenadas absoluto* de V como $\bar{\mathbb{F}}_q[V] = \bar{\mathbb{F}}_q[X]/I(V)$;
3. El *cuerpo de funciones* $\mathbb{F}_q(V)$ de $V|\mathbb{F}_q$ como el cuerpo de fracciones de $\mathbb{F}_q[V]$;
4. El *cuerpo de funciones absoluto* $\bar{\mathbb{F}}_q(V)$ como el cuerpo de fracciones de $\bar{\mathbb{F}}_q[V]$.

Definición 3.7. Sean $V|\mathbb{F}_q$ una variedad afín y $P \in V$. El *anillo local* de V en P es

$$\bar{\mathbb{F}}_q(V)_P = \{h \in \bar{\mathbb{F}}_q(V) : \ h \text{ está bien definida en } P\}.$$

El único ideal maximal de este anillo está dado por

$$\bar{M}_P = \{h \in \bar{\mathbb{F}}_q(V) : h(P) = 0\}.$$

Observación 3.8. Si P es un punto $\mathbb{F}_q$-racional, entonces

$$\mathbb{F}_q(V)_P = \bar{\mathbb{F}}_q(V)_P \cap \mathbb{F}_q(V) \quad \text{y} \quad M_P = \bar{M}_P \cap \mathbb{F}_q(V).$$

Definición 3.9. La *dimensión* de una variedad afín $V|\mathbb{F}_q$ es el grado de trascendencia de la extensión $\bar{\mathbb{F}}_q(V)$ sobre $\bar{\mathbb{F}}_q$.

Definición 3.10. Sea $V|\mathbb{F}_q$ una variedad afín y sea $\{f_1, \ldots, f_m\} \subseteq \mathbb{F}_q[X]$ un conjunto que genera $I(V)$, entonces V será una variedad *suave* en $P \in V$ si la matriz $m \times n$

$$\left(\frac{\partial f_i}{\partial x_j}(P)\right)_{1 \le i \le m, 1 \le j \le n}$$

tiene rango igual a $n - \dim(V)$.

En el caso proyectivo los conceptos son definidos de manera análoga.

Definición 3.11. $V \subseteq \bar{\mathbb{F}}_q$ es un *conjunto algebraico proyectivo* si existe un conjunto de polinomios homogéneos $S \subseteq \bar{\mathbb{F}}_q[X_0, X_1, \ldots, X_n] = \bar{\mathbb{F}}_q[X]$ tales que $V = V(S) = \{P \in \mathbb{P}^n(\bar{\mathbb{F}}_q) : f(P) = 0 \ \forall f \in S\}$.

Como antes, diremos que V está definido sobre $\mathbb{F}_q$ si $S \subseteq \mathbb{F}_q[X]$.

Definición 3.12. Un conjunto algebraico proyectivo V es *reducible* se existen dos conjuntos algebraicos proyectivos V_1 y V_2 tales que $V_i \neq V$ para $i = 1, 2$ y $V = V_1 \cup V_2$. Si V es no vacío y no reducible, diremos en este caso que V es *irreducible*.

También podemos asociarle los ideales

$$I(V) = \langle \{f \in \bar{\mathbb{F}}_q[X] : f \text{ es homogéneo y } f(P) = 0 \ \forall P \in V\} \rangle,$$
$$I(V|\mathbb{F}_q) = I(V) \cap \mathbb{F}_q[X].$$

Observación 3.13. Un conjunto algebraico proyectivo es irreducible si y solamente si $I(V)$ es un ideal primo de $\bar{\mathbb{F}}_q[X]$.

Definición 3.14. Un conjunto algebraico proyectivo es una *variedad proyectiva* cuando $I(V)$ es un ideal primo homogéneo de $\bar{\mathbb{F}}_q[X]$.

Para cada $i = 1, \ldots, n$ considere las aplicaciones

$$\begin{aligned} \varphi_i : \mathbb{A}^n(\bar{\mathbb{F}}_q) &\to \mathbb{P}^n(\bar{\mathbb{F}}_q) \\ (a_1 \ldots, a_n) &\mapsto (a_1 : \cdots : a_{i-1} : 1 : a_i : \cdots : a_n) \end{aligned}$$

Definición 3.15. Sea $V|\mathbb{F}_q$ una variedad proyectiva y sea i tal que $\varphi_i^{-1}(V \cap U_i) \neq \emptyset$ donde $U_i = \varphi_i(\mathbb{A}^n(\bar{\mathbb{F}}_q))$. Entonces definimos:

1. La *dimensión* de V como la dimensión de $\varphi_i^{-1}(V \cap U_i)$.
2. El *cuerpo de funciones* $\mathbb{F}_q(V)$ de V como el cuerpo de funciones $\mathbb{F}_q(\varphi_i^{-1}(V \cap U_i))$.
3. El *cuerpo de funciones absoluto* $\bar{\mathbb{F}}_q(V)$ de V como el cuerpo de funciones absoluto $\bar{\mathbb{F}}_q(\varphi_i^{-1}(V \cap U_i))$.

Definición 3.16. Sea $P = (a_0 : \cdots : a_n) \in V$ tal que $a_i \neq 0$, entonces diremos que V es *suave* en P si $\varphi_i^{-1}(V \cap U_i)$ es suave en $(a_0/a_i, \ldots, a_{i-1}/a_i, a_{i+1}/a_i, \ldots, a_n/a_i)$.

Definición 3.17. Una variedad proyectiva de dimensión uno, definida sobre $\mathbb{F}_q$ será una *curva proyectiva* sobre $\mathbb{F}_q$.

Sea $f(X,Y) \in \mathbb{F}_q[X,Y]$ un polinomio absolutamente irreducible de grado d, o sea, es irreducible sobre $\bar{\mathbb{F}}_q$ y sea $F(X,Y,Z)$ su homogeneización. Considere la curva proyectiva asociada $\mathcal{C} = \{(x : y : z) \in \mathbb{P}^2(\bar{\mathbb{F}}_q) : F(x,y,z) = 0\}$; entonces el género de $\mathcal{C}$ satisface

$$g \leq \frac{(d-1)(d-2)}{2},$$

donde la igualdad vale si $\mathcal{C}$ es suave.

Proposición 3.18. *Sea $f(X,Y) \in \mathbb{F}_q[X,Y]$ un polinomio del siguiente tipo:*

$$f(X,Y) = a_0 Y^n + a_1(X)Y^{n-1} + \cdots + a_n(X)$$

donde $a_0 \in \mathbb{F}_q^*$ y $a_1(X), \ldots, a_n(X) \in \mathbb{F}_q[X]$. Suponga que $\deg(a_n) = m$ con $\mathrm{mcd}(n,m) = 1$ y que

$$\frac{m}{n} > \frac{\deg(a_i)}{i} \qquad \text{para cada } i \text{ tal que } a_i(X) \neq 0.$$

Entonces $f(X,Y)$ es absolutamente irreducible sobre $\mathbb{F}_q$.

Dada una curva proyectiva, no singular e irreducible $\mathcal{C}$, podemos asociarle su cuerpo de funciones $\mathbb{F}_q(\mathcal{C})$ definido anteriormente.

Ahora, si comenzamos con un cuerpo de funciones $F = \mathbb{F}_q(x,y)|\mathbb{F}_q(x)$ sabemos que existe un polinomio irreducible $g(X,Y) \in \mathbb{F}_q[X,Y]$ tal que $g(x,y) = 0$. Así, podemos asociar a F la curva proyectiva no singular cuyo modelo plano está dado por $g(X,Y) = 0$.

Teorema 3.19. *Sea $\mathcal{C}$ sobre $\mathbb{F}_q$ una curva proyectiva, no singular y sea F su cuerpo de funciones, entonces existe una correspondencia biunívoca entre los puntos $P \in \mathcal{C}$ y los lugares de $F|\mathbb{F}_q$ dada por*

$$P \mapsto M_P,$$

donde M_P es el ideal maximal del anillo local de $\mathcal{C}$ en P.

3.1.1. Extensiones de cuerpos de funciones. Antes de adentrarnos en el problema de contar puntos racionales, vamos a echarle una mirada rápida a algunas extensiones de cuerpos de funciones que serán útiles en lo que sigue.

Definición 3.20. Un cuerpo de funciones $F'|K'$ es una extensión *algebraica finita* del cuerpo de funciones $F|K$ si $F' \supseteq F$, $K' \supseteq K$ y $[F' : F] < \infty$.

Definición 3.21. Un lugar $P' \in \mathbb{P}_{F'}$ está sobre un lugar $P \in \mathbb{P}_F$ si $P \subseteq P'$ o, equivalentemente, si existe un número entero $e \geq 1$ tal que $v_{P'}(x) = e \cdot v_P(x)$ para todo $x \in F$.

En este caso denotaremos por $P'|P$ y diremos que el lugar P' es una *extensión* del lugar P.

• El número entero e, que pasaremos a denotar por $e(P'|P)$, es llamado *índice de ramificación* de P' sobre P.

• La extensión $P'|P$ es ramificada si $e > 1$.

• Para $P'|P$, el número entero $f(P'|P) := [F'_{P'} : F_P]$ es llamado de *grado relativo* de P' sobre P.

Proposición 3.22. *Sea $F'|F$ una extensión algebraica finita de cuerpos de funciones, entonces:*

1. *Para todo lugar $P' \in \mathbb{P}_{F'}$, existe un único lugar $P \in \mathbb{P}_F$ tal que $P'|P$.*
2. *Para todo lugar $P \in \mathbb{P}_F$, existe por lo menos una extensión $P' \in \mathbb{P}_{F'}$. Más aún, el número de tales extensiones es finito.*
3. *Si $P \in \mathbb{P}_F$ y $P_1, \ldots, P_m$ son todas las extensiones de P en $\mathbb{P}_{F'}$, entonces*

$$\sum_{i=1}^{m} e(P_i|P) f(P_i|P) = [F' : F] = n.$$

Definición 3.23. Sea $F'|F$ una extensión algebraica de cuerpos de funciones y sean $P \in \mathbb{P}_F$ y $P' \in \mathbb{P}_{F'}$. Entonces

1. P es *ramificada* si existe $P' \in \mathbb{P}_{F'}$ tal que $P'|P$ y $e(P'|P) > 1$.
2. $P'|P$ es de *ramificación moderada* si $e(P'|P) > 1$ y $e(P'|P)$ no es divisible por la característica del cuerpo de constantes.
3. $P'|P$ es de *ramificación salvaje* si $e(P'|P) > 1$ y $e(P'|P)$ es divisible por la característica del cuerpo de constantes.
4. P es de *ramificación moderada* si para todo lugar $P' \in \mathbb{P}_{F'}$ con $P'|P$, la extensión $P'|P$ es de ramificación moderada.
5. P es de *ramificación salvaje* si existe un lugar $P' \in \mathbb{P}_{F'}$ con $P'|P$ tal que la extensión $P'|P$ es de ramificación salvaje.
6. P *se descompone totalmente* si para todo lugar $P' \in \mathbb{P}_{F'}$ con $P'|P$, vale que $e(P'|P) = f(P'|P) = 1$.
7. P es *totalmente ramificado* si existe un único lugar $P' \in \mathbb{P}_{F'}$ con $P'|P$ y $e(P'|P) = [F' : F]$.

A partir de ahora, vamos a suponer que el cuerpo de constantes K es un cuerpo perfecto, el cual es el caso de un cuerpo finito por ejemplo.

Consideremos $F'|F$ una extensión separable de cuerpos de funciones. Para $P \in \mathbb{P}_F$ definimos $\mathcal{O}'_P$ el cierre integral en F' del anillo de valoración $\mathcal{O}_P$. El módulo complementar $\mathcal{C}_P$ sobre $\mathcal{O}_P$ es dado por

$$\mathcal{C}_P = \{z \in F' : \mathcal{T}_{F'|F}(z \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P\},$$

donde $\mathcal{T}_{F'|F}$ es la función traza asociada a la extensión separable $F'|F$.

Observación 3.24. Existe un elemento $t \in F'$ que depende de P tal que $\mathcal{C}_P = t \cdot \mathcal{O}'_P$. Más aún, $v_{P'}(t) \leq 0$ para todo $P'|P$.

Definición 3.25. Considere un lugar $P \in \mathbb{P}_F$ y sea $\mathcal{C}_P = t \cdot \mathcal{O}'_P$ el módulo complementar. Para $P'|P$ definimos el *exponente de la diferente* por $d(P'|P) = -v_{P'}(t)$.

Definición 3.26. La *diferente* de $F'|F$ es el divisor dado por

$$\mathrm{Diff}(F'|F) := \sum_{P\in\mathbb{P}_F}\sum_{P'|P} d(P'|P)\cdot P'.$$

Proposición 3.27. *(Fórmula del género de Hurwitz) Sea $F|K$ un cuerpo de funciones de género g y sea $F'|F$ una extensión separable finita. Denotamos por K' el cuerpo de constantes de F' y por g' el género de $F'|K'$. Entonces*

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) - \deg(\mathrm{Diff}(F'|F)).$$

Proposición 3.28. *(Teorema de la Diferente de Dedekind) Con las notaciones anteriores, para $P'|P$ vale que*

1. *$d(P'|P) \geq e(P'|P) - 1$.*
2. *$d(P'|P) = e(P'|P) - 1$ si y solamente si la característica de K no divide $e(P'|P)$.*

En general, es difícil calcular el género de un cuerpo de funciones. Vamos a enunciar dos resultados que suelen ser útiles a la hora de calcularlo.

Teorema 3.29. *Suponga que $F' = F(y)$ es una extensión de grado n, separable del cuerpo de funciones F. Sea $P \in \mathbb{P}_F$ tal que el polinomio mínimo $\varphi(T)$ de y sobre F tiene sus coeficientes en $\mathcal{O}_P$ y sean $P_1, \ldots, P_r$ todos los lugares de F' sobre P. Entonces*

1. *$d(P_i|P) \leq v_{P_i}(\varphi'(y))$;*
2. *$\{1, y, \ldots, y^{n-1}\}$ es una base entera de $F'|F$ en el lugar P si y solamente si $d(P_i|P) = v_{P_i}(\varphi'(y))$ para todo $i = 1, \ldots, r$,*

donde $(\varphi'(T))$ denota la derivada usual del polinomio $\varphi(T)$.

Proposición 3.30. *Sean $F'|F$ una extensión separable de cuerpos de funciones, $P \in \mathbb{P}_F$ y $P' \in \mathbb{P}_{F'}$ con $P'|P$. Suponga que $P'|P$ sea totalmente ramificada y sea $t \in F'$ un elemento P'-primo (o sea, $P' = t\mathcal{O}_{P'}$). Considere $\varphi(T) \in F[T]$ el polinomio mínimo de t sobre F. Entonces $d(P'|P) = v_{P'}(\varphi'(t))$ y $\{1, t, \ldots, t^{n-1}\}$ es una base entera de $F'|F$ en el lugar P.*

3.1.2. Extensiones de Kummer y Artin-Schreier.

Definición 3.31. $F'|F$ es una *extensión de Galois* de cuerpos de funciones si $F'|F$ es una extensión de Galois de cuerpos.

Tenemos dos clases importantes de extensiones galoisianas: extensiones de Kummer y de Artin-Schreier. Estas extensiones tienen dos ventajas importantes: podemos explicitar las ecuaciones que las definen y el género puede ser calculado fácilmente.

Definición 3.32. Sea $F|K$ un cuerpo de funciones en donde K contiene una raíz primitiva de orden $n \geq 1$ de la unidad y tal que $\mathrm{mcd}(n, \mathrm{char}\, K) = 1$. Suponga que existe un elemento $u \in F$ tal que $u \neq w^d$ para todo $w \in F$ y para todo $d > 1$ con $d|n$. Entonces el cuerpo de funciones dado por

$$F' := F(y), \quad \text{con } y^n = u,$$

es una *extensión de Kummer* de F.

Observación 3.33. Una extensión de Kummer $F'|F$ satisface las siguientes propiedades:

1. $F'|F$ es una extensión cíclica y su grupo de Galois está generado por $\sigma(y) = \zeta y$ donde $\zeta \in K$ es una raíz primitiva de la unidad de orden n.
2. Sea $P \in \mathbb{P}_F$ y sea $P' \in \mathbb{P}_{F'}$ una extensión de P, entonces
$$e(P'|P) = \frac{n}{r_P} \quad \text{y} \quad d(P'|P) = e(P'|P) - 1,$$
donde $r_P := \text{mcd}(n, v_P(u)) > 0$.
3. Si K' es el cuerpo de constantes de F' y g' es el género de F', entonces
$$g' = 1 + \frac{n}{[K' : K]}\left(g - 1 + \frac{1}{2}\sum_{P \in \mathbb{P}_F}\Big(1 - \frac{r_P}{n}\Big)\deg(P)\right).$$

Observación 3.34. Sea $F|K$ un cuerpo de funciones de género g y sea F' dado por $F' := F(y)$ con $y^n = u \in F$, donde $n \not\equiv 0 \mod \text{char(K)}$. Suponga que K contiene una raíz primitiva de orden n de la unidad y que existe un lugar $Q \in \mathbb{P}_F$ tal que $\text{mcd}(v_Q(u), n) = 1$. Entonces K es el cuerpo de constantes de F' y la extensión $F'|F$ es cíclica de grado n. El género g' está dado por
$$g' = 1 + n(g-1) + \frac{1}{2}\sum_{P \in \mathbb{P}_F}\Big(n - r_P\Big)\deg(P).$$

Ejemplo 3.35. Considere un cuerpo K de característica diferente de 2. Sea
$$F := K(x, y) \quad \text{con } y^2 = f(x) = \prod_{i=1}^{s} p_i(x) \in K[x],$$
donde $p_i(x)$ son polinomios mónicos, irreducibles distintos y $s \geq 1$.

Denotando por m el grado del polinomio $f(x)$ tenemos que K es el cuerpo de constantes de F y que el género está dado por
$$g = \begin{cases} (m-1)/2 \text{ si } m \equiv 1 \mod 2, \\ (m-2)/2 \text{ si } m \equiv 0 \mod 2. \end{cases}$$

De hecho, considere $F = F_0(y)$ donde $F_0 := K(x)$ es el cuerpo de funciones racionales. Denotando por $P_i \in \mathbb{P}_{K(x)}$ el cero de $p_i(x)$ y P_∞ el polo de x en $K(x)$, entonces $v_{P_i}(f(x)) = 1$ y $v_{P_\infty}(f(x)) = -m$. Así $F|F_0$ es una extensión cíclica de grado 2. Vale también que

1. $r_{P_j} = 1$ para $j = 1, \ldots, s$;
2. $r_{P_\infty} = 1$ si $m \equiv 1 \mod 2$;
3. $r_{P_\infty} = 2$ si $m \equiv 0 \mod 2$.

Definición 3.36. Sea $F|K$ un cuerpo de funciones de característica $p > 0$. Suponga que $u \in F$ es tal que $u \neq w^p - w$ para todo $w \in F$. El cuerpo de funciones F' dado por
$$F' := F(y), \quad \text{con } y^p - y = u$$
es una *extensión de Artin-Schreier* de F.

Observación 3.37. Una extensión de Artin-Schreier satisface las siguientes propiedades:

1. $F'|F$ es una extensión cíclica de grado p y los automorfismos de $F'|F$ están dados por $\sigma(y) = y + \nu$ donde $\nu = 0, 1, \ldots, p-1$.

2. Para $P \in \mathbb{P}_F$ y P' una extensión de P, el número a continuación está bien definido

$$m_P := \begin{cases} m & \text{si existe } z \in F \text{ tal que } v_P(u-(z^p-z)) = -m \text{ y } m \not\equiv 0 \mod p, \\ -1 & \text{si } v_P(u-(z^p-z)) \geq 0 \text{ para algún } z \in F. \end{cases}$$

3. P es no ramificado si y solamente si $m_P = -1$.
4. P es totalmente ramificado si y solamente si $m_P \geq 0$. En este caso tenemos que

$$d(P'|P) = (p-1)(m_P+1), \quad \text{donde } P' \text{ es el único lugar sobre } P.$$

5. Si por lo menos un lugar $Q \in \mathbb{P}_F$ es totalmente ramificado, entonces K es el cuerpo de constantes de F' y el género g' de F' está dado por

$$g' = p \cdot g + \frac{p-1}{2}\left(-2 + \sum_{P \in \mathbb{P}_F} \Big(m_P + 1\Big) \cdot \deg(P) \right).$$

Definición 3.38. Un polinomio $a(x) \in K[x]$ del tipo $a(x) = a_n x^{p^n} + a_{n-1}x^{p^{n-1}} + \cdots + a_1 x^p + a_0 x$ donde p es la característica del cuerpo K, es llamado polinomio aditivo sobre K.

Proposición 3.39. *Sean $F|K$ un cuerpo de funciones de característica $p \geq 0$, $a(x)$ un polinomio aditivo de grado p^n que tiene todas sus raíces en K y $u \in F$. Suponga que para todo lugar $P \in \mathbb{P}_F$ existe un elemento $z \in F$ (z depende de P) tal que*

$$\begin{cases} v_P(u-a(z)) \geq 0 & o \\ v_P(u-a(z)) = -m & \text{con } m > 0 \text{ y } m \not\equiv 0 \mod p. \end{cases}$$

Definimos $m_P = -1$ en el primer caso y $m_p = -m$ en el segundo caso.

Consideremos ahora la extensión

$$F' := F(y) \quad \text{con } a(y) = u.$$

Si existe un lugar $Q \in \mathbb{P}_F$ con $m_Q > 0$, entonces

1. *$F'|F$ es una extensión de Galois de grado p^n, cuyo grupo de Galois es isomorfo a $(\mathbb{Z}/p\mathbb{Z})^n$.*
2. *K es algebraicamente cerrado en F'.*
3. *Si $P \in \mathbb{P}_F$ es tal que $m_P = -1$, entonces P es no ramificado en $F'|F$.*
4. *Si $P \in \mathbb{P}_F$ es tal que $m_P > 0$, entonces P es totalmente ramificado en $F'|F$. En este caso*

$$d(P'|P) = (p^n-1)(m_P+1), \quad \text{donde } P' \text{ es el único lugar sobre } P.$$

5. *El género g' de F' está dado por*

$$g' = p^n \cdot g + \frac{p^n-1}{2}\left(-2 + \sum_{P \in \mathbb{P}_F} \Big(m_P + 1\Big) \cdot \deg(P) \right).$$

3.2. ¿Cuántos puntos podemos esperar? Nuestro objetivo es establecer un límite superior para el número de puntos racionales de una curva definida sobre un cuerpo finito $\mathbb{F}_q$, o lo que es equivalente, para el número de lugares racionales de un cuerpo de funciones $F|\mathbb{F}_q$. Vamos a hacer una serie de afirmaciones, la mayor parte sin demostraciones. Las pruebas se encuentran en [47] o [42]

Afirmación 3.40. *Para todo $n \geq 0$ existe únicamente un número finito de divisores positivos de grado n*

Consideremos los conjuntos

$$\mathcal{D}_F^0 := \{A \in \mathcal{D}_F; \deg(A) = 0\},$$
$$\mathcal{C}_F^0 := \{[A] \in \mathcal{C}_F; \deg([A]) = 0\},$$

donde $\mathcal{P}_F$ es el grupo de divisores principales (vea pág. 16) y $\mathcal{C}_F := \mathcal{D}_F/\mathcal{P}_F$ es llamado de grupo de clases de divisores de $F|\mathbb{F}_q$.

Afirmación 3.41. *$\mathcal{C}_F^0$ es un grupo finito de orden h.*

Definimos $\partial > 0$ por

$$\partial = \text{mín}\{\deg(A) : A \in \mathcal{D}_F \text{ y } \deg(A) > 0\}.$$

Observación 3.42. No es verdad en general que para un cuerpo de constantes arbitrario exista un divisor positivo de grado ∂.

Vamos ahora a estimar los números $A_n := \#\{A \in \mathcal{D}_F : A \geq 0 \text{ y } \deg(A) = n\}$.

Por ejemplo $A_0 = 1$ y A_1 es precisamente el número de lugares de grado uno que queremos limitar.

Proposición 3.43. *Con las notaciones anteriores vale que:*

1. *$A_n = 0$ si $\partial \nmid n$.*
2. *Para una clase de divisores fija $[C] \in \mathcal{C}_F$ tenemos*
$$\#\{A \in [C] : A \geq 0\} = \frac{h}{q-1}\Big(q^{\dim[C]} - 1\Big).$$
3. *Para cualquier entero $n > 2g - 2$ con $\partial | n$, tenemos*
$$A_n = \frac{h}{q-1}\Big(q^{n+1-g} - 1\Big).$$

Definición 3.44. La serie de potencias definida por

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

es llamada la *Función Zeta* de $F|\mathbb{F}_q$.

Proposición 3.45. *La serie de potencias $Z(t) = Z_F(t)$ es convergente para $|t| < q^{-1}$ y en este caso tenemos que*

1. *Si $F|\mathbb{F}_q$ tiene género cero, entonces*
$$Z(t) = \frac{1}{q-1}\Big(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\Big).$$
2. *Si $g \geq 1$, entonces $Z(t)$ puede ser escrita como $Z(t) = F(t) + G(t)$ donde*
$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg[C] \leq 2g-2} q^{\dim[C]} \cdot t^{\deg[C]},$$
$$G(t) = \frac{h}{q-1}\Big(q^{1-g}(qt)^{2g-2+\partial}\frac{1}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\Big).$$

Corolario 3.46. *La función $Z(t)$ puede ser extendida a una función racional definida sobre $\mathbb{C}$ con polo simple en $t = 1$.*

La función Zeta también puede ser escrita para $|t| < q^{-1}$ como un producto (conocido como producto de Euler) de la forma

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

En particular, $Z(t) \neq 0$ para $|t| < q^{-1}$ y $Z(t)$ satisface la ecuación funcional

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

Vamos a estudiar ahora el comportamiento de la función Zeta cuando hacemos extensiones del cuerpo F por constantes.

Consideremos la siguiente extensión por constantes $F_r := F \cdot \mathbb{F}_{q^r}$ del cuerpo $F|\mathbb{F}_q$ y denotemos por $Z_r(t)$ la función Zeta asociada. Vale que

$$Z_r(t) = \prod_{\zeta^r = 1} Z(\zeta t) \quad \forall t \in \mathbb{C}, \qquad \text{y } \zeta \in \mathbb{C} \text{ tal que } \zeta^r = 1.$$

Observación 3.47. Usando la igualdad anterior, F.K. Schmidt mostró que $\partial = 1$.

Podemos asociar a $Z(t)$ un polinomio que va a jugar un papel importante para determinar un límite superior para el número de lugares racionales.

Definición 3.48. El polinomio $L(t) := (1-t)(1-qt)Z(t)$ es llamado el *L-polinomio* de $F|\mathbb{F}_q$ y tiene grado como máximo $2g$.

Como $L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n$, este polinomio guarda toda la información sobre los $A_n'^s$ para todo $n \geq 0$. Este hecho nos motiva a estudiarlo un poco más. Algunas de sus propiedades están resumidas en el siguiente teorema.

Teorema 3.49. *Sea $L(t)$ como antes. Entonces:*

1. *$L(t) \in \mathbb{Z}[t]$ y tiene grado $2g$;*
2. *$L(t) = q^g\, t^{2g} L(1/qt)$;*
3. *$L(1) = h$;*
4. *si $L(t) = \sum_{i=0}^{2g} a_i t^i$, entonces:*
   a) *$a_0 = 1$ y $a_{2g} = q^{2g}$;*
   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 de grado uno;*
5. *$L(t)$ se factoriza en $\mathbb{C}[t]$ como:*

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

y $\alpha_1, \ldots, \alpha_{2g}$ pueden ser ordenados tal que $\alpha_i\, \alpha_{g+i} = q$ para $i = 1, \ldots, g$.

Definición 3.50. Los números $\alpha_1, \ldots, \alpha_{2g}$ son llamados las *raíces recíprocas* de $L(t)$.

Corolario 3.51. *Para cada $r \geq 1$ tenemos*

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

donde $\alpha_1, \ldots, \alpha_{2g}$ son las raíces recíprocas de $L(t)$.

Así, para estimar N basta estimar $|\alpha_i|$.

Teorema 3.52. *(Hasse-Weil) Los números α_i satisfacen*

$$|\alpha_i| = \sqrt{q}, \quad \forall i = 1, \ldots, 2g.$$

Teorema 3.53. *(Cota de Hasse-Weil) El número N de lugares de grado uno puede ser estimado por*

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

Esta desigualdad es equivalente a la validez de la hipótesis de Riemann para la función Zeta asociada al cuerpo de funciones $F|\mathbb{F}_q$. De hecho, si definimos la *norma absoluta* de un divisor A como $\mathcal{N}(A) = q^{\deg A}$ y consideramos la función dada por

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

entonces esta función puede ser escrita como

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

que es análoga a la función Zeta de Riemann clásica $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$.

La hipótesis de Riemann para la función clásica afirma que, además de los ceros triviales, todos los ceros se encuentran localizados en la recta $Re(s) = 1/2$. En el caso de cuerpo de funciones, el teorema de Hasse-Weil muestra que

$$\zeta_F(s) = 0 \Rightarrow Z_F(q^{-s}) = 0 \Rightarrow |q^{-s}| = q^{1/2},$$

ya que $|q^{-s}| = q^{Re(s)}$, lo que implica trivialmente que $Re(s) = 1/2$.

Históricamente, los primeros estudios sobre ecuaciones sobre cuerpos finitos se centraban en las congruencias del tipo

$$Y^2 \equiv f(X) \mod p \quad (*)$$

donde p es un número primo y $f(X)$ un polinomio (o una función racional) definido sobre $\mathbb{Z}$.

Artin introdujo la función Zeta para extensiones cuadráticas del cuerpo racional $\mathbb{F}_p(x)$ obtenido por la adjunción de las raíces de la congruencia anterior, basado en la función Zeta de Dedekind para extensiones cuadráticas de $\mathbb{Q}$.

Asumiendo como verdadera la hipótesis de Riemann para la función clásica, Artin llegó a conjeturar una cota superior para el número de soluciones de la congruencia (*). Esta conjetura fue probada por Hasse para polinomios de grado 3 o 4 definidos sobre un cuerpo finito arbitrario y después generalizada por Weil como vimos en el teorema anterior.

Observación 3.54. Ihara mostró en [32] que si $F|\mathbb{F}_q$ es un cuerpo de funciones de género g, entonces el número de lugares racionales N satisface

$$N \leq q + 1 + \left\lfloor \frac{\sqrt{(8q+1)g^2 + 4(q^2-q)g} - g}{2} \right\rfloor,$$

donde $\lfloor x \rfloor$ denota la parte entera de x.

Note que si $g > (q - \sqrt{q})/2$, esta cota es mejor que la de Hasse-Weil.

Ejemplo 3.55. (Hermitiana) Considere la curva $\mathcal{H}$ definida sobre $\mathbb{F}_{q^2}$ asociada al polinomio $f(X,Y) = Y^q + Y - X^{q+1}$. Esta curva es no singular y tiene género $g = q(q-1)/2$.

Vamos a calcular el número de puntos racionales, o sea

$$\#\{(x:y:z)\,|\,x,y,z\in\mathbb{F}_{q^2}\text{ tales que }F(x,y,z)=0\},$$

donde $F(X,Y,Z)=ZY^q+Z^qY-X^{q+1}$ es la homogeneización de $f(X,Y)$.

Vamos a comenzar por la parte afín, o sea, cuando $z=1$, en este caso tenemos que calcular las soluciones de $f(x,y)$ en $\mathbb{F}_{q^2}\times\mathbb{F}_{q^2}$. Podemos pensar en calcular el número N_a de elementos del conjunto

$$N_a=\#\{(x,y)\in\mathbb{F}_{q^2}\times\mathbb{F}_{q^2}:Tr_{\mathbb{F}_{q^2}|\mathbb{F}_q}(y)=N_{\mathbb{F}_{q^2}|\mathbb{F}_q}(x)\}$$

donde $Tr_{\mathbb{F}_{q^2}|\mathbb{F}_q}$ y $N_{\mathbb{F}_{q^2}|\mathbb{F}_q}$ son las funciones Traza y Norma de la extensión galoisiana $\mathbb{F}_{q^2}|\mathbb{F}_q$.

Como $\mathcal{T}$ es suryectiva, tenemos que $\#\mathcal{T}^{-1}(y)=q$ para todo $y\in\mathbb{F}_{q^2}$, obtenemos así

$$\begin{aligned}N_a &= \sum_{x\in\mathbb{F}_{q^2}}\#\{y\in\mathbb{F}_{q^2}:Tr_{\mathbb{F}_{q^2}|\mathbb{F}_q}(y)=x^{q+1}\}\\ &= \sum_{x\in\mathbb{F}_{q^2}}\#Tr^{-1}_{\mathbb{F}_{q^2}|\mathbb{F}_q}(x^{q+1})\\ &= \sum_{x\in\mathbb{F}_{q^2}}q\\ &= q^3.\end{aligned}$$

Falta calcular el número de puntos racionales en el infinito (en este caso $z=0$). Así se $(x:y:0)$ es una solución de $F(X,Y,Z)=0$, entonces $x=0$ lo que implica que $y=1$. Tenemos, por lo tanto, un único punto racional en el infinito. Finalmente tenemos que la curva $\mathcal{H}$ tiene q^3+1 puntos racionales alcanzando la cota de Hasse-Weil.

Definición 3.56. Un cuerpo de funciones $F|\mathbb{F}_q$ es llamada *maximal* sobre $\mathbb{F}_q$ si el número de lugares racionales de grado uno alcanza la cota de Hasse-Weil.

Observación 3.57. Si $F|\mathbb{F}_q$ es maximal, como $N(F|\mathbb{F}_q)=q+1+2g\sqrt{q}$ es un número entero, tenemos necesariamente que q debe ser un cuadrado.

3.3. Mejoras de la cota de Hasse-Weil. Como vimos en la subsección anterior, la cota de Hasse-Weil sólo es alcanzada si la cardinalidad del cuerpo finito es un cuadrado, así una mejora trivial para la cota es

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

Serre dio en [44] la siguiente mejora.

Teorema 3.58. *(Cota de Serre) Sea $F|\mathbb{F}_q$ un cuerpo de funciones de género g, entonces el número N de lugares de grado uno está limitado por*

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

La idea de la prueba es bastante simple, así que vamos hacer un esbozo.

Demostración. Sabemos que el L-polinomio puede ser escrito como

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

y que los α_i pueden ser ordenados de tal forma que $\bar{\alpha}_i = \alpha_{g+i}$ para $i = 1, \ldots, g$, donde $\bar{\alpha}_i$ denota el complejo conjugado de α_i. De hecho, como $|\alpha_i| = \sqrt{q}$ y $\alpha_i \alpha_{g+i} = q$, debemos tener que $\bar{\alpha}_i = \alpha_{g+i}$ para $i = 1, \ldots, g$.

Vamos a comenzar mostrando que

$$N - (q+1) \leq g\lfloor 2\sqrt{q} \rfloor.$$

Para cada $i = 1, \ldots, g$, definimos $\beta_i := \alpha_i + \bar{\alpha}_i + \lfloor 2\sqrt{q} \rfloor$. Los números así definidos son números reales positivos y son enteros algebraicos.

Sea $E = \mathbb{Q}(\alpha_1, \ldots, \alpha_{2g})$ una extensión $E|\mathbb{Q}$ galoisiana. Todo $\sigma \in Gal(E|\mathbb{Q})$ induce una permutación del conjunto $\{\beta_1, \ldots, \beta_g\}$, lo que implica que

$$\beta = \prod_{i=1}^{g} \beta_i$$

es dejado fijo por todos los automorfismos y como β es un entero algebraico debemos tener que $\beta \in \mathbb{Z}$ y $\beta \geq 1$.

Tenemos entonces que

$$\begin{aligned} g \ \leq \ \sum_{i=1}^{g} \beta_i &= \sum_{i=1}^{g} (\alpha_i + \bar{\alpha}_i) + g\lfloor 2\sqrt{q} \rfloor + g \\ &= \Big(\sum_{i=1}^{2g} \alpha_i \Big) + g\lfloor 2\sqrt{q} \rfloor + g. \end{aligned}$$

Como $N = q + 1 - \sum_{i=1}^{2g} \alpha_i$ y usando la desigualdad entre la media aritmética y la geométrica, tenemos que

$$\frac{1}{g} \sum_{i=1}^{g} \beta_i \geq \Big(\prod_{i=1}^{g} \beta_i \Big)^{1/g},$$

lo que concluye la prueba de la desigualdad.

La prueba de que $N - (q+1) \geq -(g\lfloor 2\sqrt{q} \rfloor)$ es análoga y será dejada como ejercicio para el lector. □

Ejemplo 3.59. (La cuártica de Klein) Considere la curva $\mathcal{C}$ definida sobre $\mathbb{F}_8$ por el polinomio

$$f(X, Y) = Y^3 + X^3 Y + X$$

y sea $F(X, Y, Z) = ZY^3 + X^3 Y + Z^3 X \in \mathbb{F}_8[X, Y, Z]$ la homogeneización de f. La curva $\mathcal{C}$ es no singular y tiene género $3 = (d-1)(d-2)/2$, donde $d = 4$ es el grado de f.

Vamos a calcular los puntos racionales afines, o sea, cuando $z = 1$ y para los cuales $x \neq 0$ y $y \neq 0$.

Multiplicando $f(X, Y)$ por X^6 obtenemos la ecuación

$$W^3 + X^7 W + X^7,$$

donde $W = X^2 Y$.

Olvidándonos del origen, tenemos que

$$\begin{aligned} \#N_a - 1 &= \#\left\{ (x, w) \in \mathbb{F}_8^* \times \mathbb{F}_8 : x^7 = \frac{w^3}{w+1} \right\} \\ &= \#\Big\{ (x, w) \in \mathbb{F}_8^* \times \mathbb{F}_8 ; w^3 + w + 1 = 0 \Big\}. \end{aligned}$$

El polinomio $W^3 + W + 1$ es irreducible sobre $\mathbb{F}_2[W]$, así tiene todas sus raíces en $\mathbb{F}_8$. Por lo tanto $N_a - 1 = 7 \cdot 3 = 21$ y la cuártica de Klein tiene $N = 21 + 3 = 24$ puntos racionales alcanzando así la cota de Serre. Los 3 puntos que faltan son puntos en el infinito y la caracterización de los mismos es dejada para el lector.

Es lógico esperar que si tenemos un cuerpo de funciones F definido sobre $\mathbb{F}_q$ y extendemos el cuerpo de constantes para algún $\mathbb{F}_{q^r}$, el número de lugares de grado uno de $F|\mathbb{F}_{q^r}$ sólo puede aumentar. Usando esta idea, Serre mostró el siguiente teorema.

Teorema 3.60. *Sea $\Psi(t) = \sum_{r=1}^{m} c_r t^r \in \mathbb{R}[t] \setminus \{0\}$ un polinomio con coeficientes no negativos. Considere la función racional dada por $f(t) = 1 + \Psi(t) + \Psi(t^{-1})$. Suponga que $f(\gamma) \geq 0$ para todo $\gamma \in \mathcal{C}$ con $|\gamma| = 1$. Entonces para F un cuerpo de funciones de género g definido sobre $\mathbb{F}_q$ vale que*

$$N_1 := N \leq \frac{g}{\Psi\left(q^{-\frac{1}{2}}\right)} + \frac{\Psi\left(q^{\frac{1}{2}}\right)}{\Psi\left(q^{-\frac{1}{2}}\right)} + 1.$$

Demostración. Claramente tenemos que $\Psi\left(q^{-\frac{1}{2}}\right) \geq 0$ y $\Psi\left(q^{\frac{1}{2}}\right) \geq 0$.

Reordenando $\alpha_1, \ldots, \alpha_{2g}$ tal que $\bar{\alpha}_i = \alpha_{g+i}$ para todo $i = 1, \ldots, g$ tenemos que

$$N_r = q^r + 1 - \sum_{i=1}^{g} (\alpha_i^r + \bar{\alpha}_i^r),$$

donde N_r denota el número de lugares de grado uno de $F|\mathbb{F}_{q^r}$. Multiplicando la igualdad anterior por $q^{-r/2}$ obtenemos

$$q^{-r/2} N_r = q^{r/2} + q^{-r/2} - \sum_{i=1}^{g} [(\alpha_i q^{-1/2})^r + (\bar{\alpha}_i q^{-1/2})^r].$$

Por Hasse-Weil, sabemos que los números $\gamma_i := \alpha_i q^{-1/2}$ son complejos de norma uno para $i = 1, \ldots, g$. Así,

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

Multiplicando esta igualdad por c_r para cada $r = 1, \ldots, m$ y sumando, tenemos

$$0 = \Psi(q^{1/2}) + \Psi(q^{-1/2}) + g - \sum_{i=1}^{g} f(\gamma_i) - \sum_{r=1}^{m} N_r c_r q^{-r/2}.$$

Por lo tanto

$$N_1 \Psi(q^{1/2}) = \Psi(q^{1/2}) + \Psi(q^{-1/2}) + g - R,$$

donde $R = \sum_{i=1}^{g} f(\gamma_i) + \sum_{r=1}^{m} (N_r - N_1) c_r q^{-r/2}$.

Como $f(\gamma_i) \geq 0$ para todo i y $c_r \geq 0$ para todo r, tenemos que $R \geq 0$ y el teorema sigue a partir de ahí. □

Ejemplo 3.61. Considere la curva no singular definida sobre $\mathbb{F}_q$ cuyo modelo plano está dado por

$$f(X, Y) = Y^q - Y - X^{q_0}(X^q - X)$$

donde $q = 2^{2e+1}$ y $q_0 = 2^{2e}$. Esta curva es llamada la Curva de Suzuki y tiene género $g = q_0(q - 1)$.

Tomando $\Psi(t) = \frac{1}{\sqrt{2}}t + \frac{1}{4}t^2$ y aplicando el teorema anterior, vemos que el número de puntos racionales es $1 + q^2$, y por lo tanto esta curva alcanza la cota de Serre.

Otra herramienta que podemos usar para mejorar la cota de Hasse-Weil es conocido como Método de Stöhr-Voloch [49]. Este método consiste en construir una función auxiliar que tenga ceros de orden alto en los puntos racionales de la curva y es una herramienta fundamental en el estudio de curvas maximales.

Vamos a ilustrar su funcionamiento en el caso de curvas no singulares planas. En este caso alto va a significar mayor o igual a dos.

Sea $\mathcal{C}$ la curva afín dada por el polinomio

$$f(X,Y) = \sum_{i,j} a_{ij} X^i Y^j \in \mathbb{F}_q[X,Y].$$

Para un punto de la curva $(x,y) \in \bar{\mathbb{F}}_q \times \bar{\mathbb{F}}_q$ podemos definir la recta tangente como

$$(X-x)f_X(x,y) + (Y-y)f_Y(x,y) = 0,$$

donde f_X, f_Y son las derivadas parciales usuales.

Vamos ahora a definir un polinomio auxiliar $h(X,Y)$ dado por

$$h(X,Y) = (X - X^q)f_X(X,Y) + (Y^q - Y)f_Y(X,Y),$$

el grado del polinomio satisface $\deg(h) \leq \deg(f) + q - 1$.

Proposición 3.62. *Si* $h(X,Y) \equiv 0 \mod f$, *entonces*

$$f_{XX}f_Y^2 - 2f_{XY}f_Xf_Y + f_{YY}f_X^2 \equiv 0 \mod f.$$

Demostración. Si $h(X,Y) \equiv 0 \mod f$, implica que

$$(X - X^q)f_X(X,Y) \equiv -(Y^q - Y)F_Y(X,Y) \mod f.$$

Multiplicando $f_{XX}f_Y^2 - 2f_{XY}f_Xf_Y + f_{YY}f_X^2$ por $(X - X^q)^2$ tenemos que

$$\begin{aligned}&(X - X^q)^2(f_{XX}f_Y^2 - 2f_{XY}f_Xf_Y + f_{YY}f_X^2)\\ &\equiv \left[(X - X^q)^2(f_{XX} + 2(X - X^q)(Y - Y^q)f_{XY} + (Y - Y^q)f_{YY}\right]f_Y^2 \mod f.\end{aligned}$$

Sabemos también que existe un polinomio $g = g(X,Y)$ tal que $h = f \cdot g$, o sea

$$h(X,Y) = (X - X^q)f_X(X,Y) + (Y^q - Y)f_Y(X,Y) = f(X,Y)g(X,Y).$$

Derivando con respecto a X la igualdad anterior y multiplicando el resultado por $X - X^q$, obtenemos que

$$(X - X^q)^2 f_{XX} + (X - X^q)(Y - y^q)f_{YX} \equiv (X - X^q)f_X(g-1) \mod f.$$

Haciendo lo mismo con Y tenemos

$$(Y - Y^q)^2 f_{YY} + (X - X^q)(Y - y^q)f_{XY} \equiv (Y - Y^q)f_Y(g-1) \mod f.$$

Sumando estas dos congruencias se obtiene que

$$(X - X^q)^2 f_{XX} + 2(X - X^q)(Y - y^q)f_{XY} + (Y - Y^q)^2 f_{YY} \equiv h(g-1)0 \mod f.$$

El resultado sigue a partir de aquí ya que $(X - X^q)^2 \not\equiv 0 \mod f$. □

Observación 3.63.

1. Si la característica del cuerpo es dos, entonces $f_{XX}f_Y^2 - 2f_{XY}f_Xf_Y + f_{YY}f_X^2$ es idénticamente cero.
2. Si $h \equiv 0 \mod f$, entonces para cualquier punto (x,y) que pertenezca a la parte afín de $\mathcal{C}$ tenemos que (x^q, y^q) pertenece a la recta tangente en (x,y).

Teorema 3.64. *Sea $\mathbb{F}_q$ un cuerpo finito de característica impar y sea $f(X,Y) \in \mathbb{F}_q[X,Y]$ un polinomio absolutamente irreducible de grado d. Suponga que f no divide al polinomio $f_{XX}f_Y^2 - 2f_{XY}f_Xf_Y + f_{YY}f_X^2$, entonces*

$$\#\mathcal{C}(\mathbb{F}_q) \leq \frac{d(d+q-1)}{2},$$

donde $\mathcal{C}$ es la curva proyectiva asociada a $f(X,Y)$.

Demostración. Para simplificar, vamos a hacer la prueba para el caso afín.

Como f no divide a $f_{XX}f_Y^2 - 2f_{XY}f_Xf_Y + f_{YY}f_X^2$, eso implica que tampoco divide a $h(X,Y)$ y por lo tanto no tiene ningún factor de grado positivo en común.

Si $P = (x,y) \in \mathbb{F}_q \times \mathbb{F}_q$ pertenece a $\mathcal{C}$, entonces (x,y) es un cero de $h(X,Y)$ por definición. Más aún, como $\mathcal{C}$ y la curva asociada a $h(X,Y)$ comparten la misma recta tangente por P, concluimos que el índice de intersección $I(P;f,h)$ entre las dos curvas en P es de por lo menos 2. Así,

$$\#\mathcal{C}(\mathbb{F}_q) = \#\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q : f(x,y) = 0\} \leq \frac{1}{2}\sum_P \mathcal{I}(P;f,h),$$

donde P se mueve sobre todos los puntos de $\mathbb{F}_q \times \mathbb{F}_q$. Por el Teorema de Bezout, tenemos que

$$\frac{1}{2}\sum_P \mathcal{I}(P;f,h) \leq \frac{1}{2}\deg(f)\cdot\deg(h) \leq \frac{d(d+q-1)}{2}.$$

□

Ejemplo 3.65. Considere la curva de Fermat sobre $\mathbb{F}_{13}$ cuyo modelo plano está dado por

$$f(X,Y) = w^2X^4 + Y^4 + w,$$

donde $w \in \mathbb{F}_{13} \setminus \{1\}$ es una raíz tercera de la unidad. La curva asociada a este polinomio tiene género $g = 3$. Esta curva no tiene ningún punto racional en el infinito y tampoco tiene puntos racionales afines donde una de las coordenadas sea cero.

Vamos a calcular los puntos racionales afines. Sea $H = \{1, w, w^2\}$ el único subgrupo de $\mathbb{F}_{13}^*$ de orden 3. Considere el homomorfismo suryectivo

$$\begin{aligned} \phi : \mathbb{F}_{13}^* &\to H \\ x &\mapsto x^4. \end{aligned}$$

El núcleo es el único subgrupo de $\mathbb{F}_{13}^*$ de orden 4, así $\phi^{-1}(z) = 4$ para todo $z \in H$ $(*)$.

Sea $(x,y) \in \mathcal{C}_a(\mathbb{F}_{13})$ un punto racional afín. Como $x \in \mathbb{F}_{13}^*$, entonces $x^4 \in H$.

1. Si $x^4 = w^2$, entonces

   $$f(x,Y) = w^4 + Y^4 + w = Y^4 + 2w.$$

   Como $y \in H$ y $1 + w + w^2 = 0$, tenemos que no existen puntos racionales afines con primera coordenada satisfaciendo $x^4 = w^2$.
2. Si $x^4 = 1$ entonces $y^4 = 1$.
3. Si $x^4 = w$ entonces $y^4 = w^2$.

Resumiendo, tenemos que

$$\mathcal{C}(\mathbb{F}_{13}) = \underbrace{\{(x,y) : x^4 = y^4 = 1\}}_{\mathcal{C}_1} \cup \underbrace{\{(x,y) : x^4 = w, y^4 = w^2\}}_{\mathcal{C}_w}.$$

Por lo tanto

$$\#\mathcal{C}(\mathbb{F}_{13}) = \#\mathcal{C}_1 + \#\mathcal{C}_w.$$

Ahora, por $(*)$, tenemos que $\#\mathcal{C}_1 = \#\mathcal{C}_w = 16$.

Falta mostrar que las hipótesis del teorema son satisfechas y dejamos esto para el lector.

3.4. Algunas construcciones de curvas con muchos puntos racionales. Curvas con muchos puntos racionales son importantes desde el punto de vista de las aplicaciones. Los tres métodos descritos aquí tienen como objetivo construir curvas de manera que el número de puntos racionales se aproxime a los mejores registros existentes.

3.4.1. Primer método. Este método apareció en [35]. Sea H un subgrupo de orden v del grupo multiplicativo $\mathbb{F}_{q^r}^*$ y considere un polinomio separable $f_1(t) \in \mathbb{F}_{q^r}[t]$ tal que $\{\alpha \in \mathbb{F}_q : f_1(\alpha) = 0\} \subseteq H$.

Dado un par $(k,l) \in \mathbb{N} \times N$, definimos el polinomio

$$f(X,Y) = X^k \cdot f_1(X^l \cdot Y).$$

Podemos reducir el grado de la variable X haciendo $X^v = 1$ y vamos a denotar por $\tilde{f}(X,Y)$ el polinomio reducido. El grado de X del nuevo polinomio es como máximo $v-1$.

Las principales ventajas de la reducción son:

1. El género de la curva $\tilde{\mathcal{C}}$ asociada a $\tilde{f}$ es menor que el género de la curva $\mathcal{C}$ asociada a f.
2. La probabilidad de $\tilde{f}$ de ser absolutamente irreducible es mayor.

Dado un punto $(a,b) \in \bar{\mathbb{F}}_q \times \bar{\mathbb{F}}_q$ con $a \in H$, por construcción de $\tilde{f}$, tenemos que $\tilde{f}(a,b) = f(a,b)$. Así, los puntos racionales de $\mathcal{C}$ sobre $\mathbb{F}_{q^r}$ cuya primera coordenada pertenece a H, son puntos racionales de la curva $\tilde{\mathcal{C}}$.

Entonces, tenemos claramente que

$$\#\tilde{\mathcal{C}}(\mathbb{F}_{q^r}) \geq v \cdot \deg(f_1).$$

De hecho, sea $d = \deg(f_1)$ y sean $\alpha_1, \ldots, \alpha_d \in H$ todas las raíces de f_1. Dado $a \in H$ considere $b_j = \alpha_j / a^l$ para $j = 1, \ldots, d$. Entonces $\tilde{f}(a, b_j) = f(a, b_j) = a^k f_1(a^l b_j) = a^k f_1(\alpha_j) = 0$.

Ejemplo 3.66. Tome $f_1(t) = t^5 + t^2 + 1 \in \mathbb{F}_{32}[t]$. Este polinomio tiene 5 raíces en $\mathbb{F}_{32}^*$, así podemos tomar $v = 31$. Considerando

$$f(X,Y) = X^7 f_1(X^{12}Y) = X^{67}Y^5 + X^{31}Y^2 + X^7,$$

tenemos que

$$\tilde{f}(X,Y) = X^5Y^5 + Y^2 + X^7$$

es absolutamente irreducible y así

$$\#\tilde{\mathcal{C}}(\mathbb{F}_{32}) \geq 5 \cdot 31 = 155.$$

En realidad faltan solo 3 puntos racionales: el origen y dos puntos en el infinito, así $\tilde{g} = 15$ y $\#\tilde{\mathcal{C}}(\mathbb{F}_{32}) = 158$.

3.4.2. Segundo método. Este método creado por van der Geer-van der Vlugt está descrito en [24].

Sea $R(X) \in \mathbb{F}_q[X]$ un polinomio separable que tiene todas sus raíces en $\mathbb{F}_q$. Consideremos ahora dos polinomios $R_1(X), R_2(X) \in \mathbb{F}_q[X]$ tales que

$$R(X) = R_1(X) + R_2(X).$$

La curva $\mathcal{C}$ asociada al polinomio

$$f(X,Y) = Y^{q-1} + \frac{R_1(X)}{R_2(X)}$$

tiene muchos puntos racionales ya que

$$\{(a,b) : R(a) = 0, R_1(a) \neq 0 \text{ y } b \in \mathbb{F}_q^*\} \subseteq \mathcal{C}(\mathbb{F}_q),$$

lo que nos da

$$\#\mathcal{C}(\mathbb{F}_q) \geq (q-1)\#\{a \in \mathbb{F}_q : R(a) = 0, R_1(a) \neq 0\}.$$

Para mantener el género bajo, es deseable que el producto $R_1(X) \cdot R_2(X)$ sea altamente inseparable. Vamos a ver un ejemplo.

Ejemplo 3.67. Sea $R(X) = X^{16} + X \in \mathbb{F}_{16}[X]$ y tomemos $R_1(X) = X^{16} + X^2$ y $R_2(X) = X^2 + X$. Con esta elección tenemos que

$$f(X,Y) = Y^{15} + \frac{(X^8 + X)^2}{X^2 + X} \quad \text{y} \quad \#\mathcal{C}(\mathbb{F}_{16}) = 213.$$

De hecho

$$\#\{a \in \mathbb{F}_{16} : R(a) = 0, R_1(a) \neq 0\} = 14,$$

luego $\#\mathcal{C}(\mathbb{F}_{16}) \geq 15 \cdot 14 = 210$. Los tres puntos que faltan son $(0,0), (0,1)$ y un punto en el infinito. La parte difícil aquí es mostrar que el género es 49.

Para calcular el género necesitamos introducir algunas propiedades de las extensiones de Kummer. Vamos a comenzar concentrándonos en extensiones del tipo

$$Y^m = f(X) \in \mathbb{F}_q(X), \quad \text{donde } m \text{ divide } q-1.$$

Suponga que la función racional $f(X)$ pueda ser escrita como $f(X) = \frac{g(X)}{h(X)}$ donde g y h son polinomios primos entre sí y definidos sobre $\mathbb{F}_q$. Digamos, para fijar la notación, que

$$g(X) = \prod_{i=1}^{r} (X - \alpha_i)^{m_i} \quad \text{y} \quad h(X) = \prod_{j=1}^{s} (X - \beta_j)^{n_j}$$

donde $\alpha_i, \beta_j \in \bar{\mathbb{F}}_q$ son distintos.

La fórmula de Riemann-Hurwitz afirma que

$$2g(\mathcal{C}) - 2 = m(-2) + D_{\text{ceros}} + D_{\text{polos}} + D_\infty$$

donde $\mathcal{D}_{\text{ceros}}, \mathcal{D}_{\text{polos}}$ y $\mathcal{D}_\infty$ son ciertos divisores y $D_{\text{ceros}}, D_{\text{polos}}, D_\infty$ son los grados respectivos. Hasse mostró que, si denotamos

$$\begin{cases} m_\infty = |\deg(g) - \deg(h)|, \\ d_\infty = \text{mcd}(m_\infty, m), \end{cases}$$

entonces

$$D_\infty = d_\infty(e_\infty - 1) = m - d_\infty, \quad \text{donde } e_\infty = \frac{m}{d_\infty}.$$

El conjunto $\{\alpha_i, i = 1, \ldots, r\}$ contribuirá con D_{ceros} con

$$D_{\text{ceros}} = \sum_{i=1}^{r} d(\alpha_i)(e(\alpha_i) - 1) = rm - \sum_{i=1}^{r} d(\alpha_i),$$

ya que

$$\begin{cases} d(\alpha_i) = \text{mcd}(m_i, m), \\ e(\alpha_i) = \frac{m}{d(\alpha_i)}. \end{cases}$$

Análogamente, el conjunto $\{\beta_j : j = 1, \ldots, s\}$ contribuirá con D_{polos} con

$$D_{\text{polos}} = \sum_{j=1}^{s} d(\beta_j)(e(\beta_j) - 1) = sm - \sum_{j=1}^{s} d(\beta_j).$$

Así, en el ejemplo anterior reescribiendo las ecuaciones como

$$Y^{15} = \left(\frac{X^8 + X}{X^2 + X}\right)^2 (X^2 + X),$$

donde $\frac{X^8+X}{X^2+X}$ es un polinomio mónico de grado 6 cuyas seis raíces son exactamente los elementos de $\mathbb{F}_8 \setminus \mathbb{F}_2$. Tenemos que f tiene seis raíces duplas y dos raíces simples (las raíces de $X^2 + X$). Con las notaciones anteriores

$$\begin{cases} m_\infty = 15, \\ D_\infty = 14, \\ D_{\text{ceros}} = 112. \end{cases}$$

Lo que nos da que el género es igual a 49 como fue afirmado.

3.4.3. Tercer método. Este método fue inspirado por el método anterior, así que continuaremos trabajando con extensiones de Kummer. Fue propuesto por [17] como una generalización de la idea de [16].

Considere dos polinomios $f(X), \ell(X) \in \mathbb{F}_q[X]$ tales que

1. $\deg(f) \geq \deg(\ell)$
2. $\ell(X) \nmid f(X)$.

Así, existe un polinomio $r(X) \in \mathbb{F}_q[X]$ tal que $f(X) = h(X)\ell(X) + r(X)$ y $\deg(r) < \deg(\ell)$.

Sea $\mathcal{C}$ la curva proyectiva no singular asociada a

$$Y^m = \frac{f(X)}{r(X)}, \quad \text{donde } m \text{ divide } q - 1.$$

La idea es nuevamente que $f(X)r(X)$ sea altamente inseparable para garantizar un género bajo y que $\ell(X)$ tenga todas sus raíces en $\mathbb{F}_q$ para que tengamos muchos puntos racionales. De hecho, considere el conjunto

$$S = \{\alpha \in \mathbb{F}_q : h(\alpha)\ell(\alpha) = 0 \text{ y } f(\alpha) \neq 0\}.$$

Así, para todo $\alpha \in S$ tenemos que $f(\alpha)/r(\alpha) = 1$. Esto nos da la siguiente cota para el número de puntos racionales:

$$\#\mathcal{C}(\mathbb{F}_q) \geq m \cdot \#S.$$

Ahora, el género puede ser calculado sabiendo que la extensión es de Kummer.

Ejemplo 3.68. Sean $f(X) = (X^3 + X^2 + 1)^4$ y $\ell(X) = \frac{X^{16}+X}{X^4+X}$ definidos sobre $\mathbb{F}_{16}$. En este caso $r(X) = X^3(X+1)^3(X^3+X+1)$. La curva proyectiva asociada a

$$Y^3 = \frac{f(X)}{r(X)}$$

tiene género 4 y 45 puntos racionales sobre $\mathbb{F}_{16}$.

3.5. Curvas maximales. Como definimos antes, una curva $\mathcal{C}$ proyectiva, geométricamente irreducible, no singular de género g definida sobre $\mathbb{F}_{q^2}$ es maximal cuando el número de puntos racionales alcanza la cota de Hasse-Weil, o sea

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = q^2 + 1 + 2gq.$$

Así, tenemos un número finito de posibilidades para el género de una curva maximal ya que Ihara mostró en [32] que

$$g \leq \frac{q(q-1)}{2}.$$

De hecho, si $\mathcal{C}$ es maximal sobre $\mathbb{F}_{q^2}$, entonces $\alpha_i = -q$ para todo $i = 1, \ldots, 2g$.

Como $N_2 \geq N_1$, tenemos que

$$N_2 := q^2 + 1 - \sum_{i=1}^{2g} \alpha_i^2 \leq N_1 = q + 1 - \sum_{i=1}^{2g} \alpha_i,$$

lo que es equivalente a

$$q^2 - 2gq^2 \geq q + 2gq,$$

y a partir de esta desigualdad podemos mostrar la cota de Ihara.

La curva Hermitiana del Ejemplo 3.55 definida sobre $\mathbb{F}_{q^2}$ es una curva de género máximo y es la única curva, a menos de isomorfismo, con esta propiedad. Este resultado fue probado por [43].

Vamos a considerar dos problemas sobre curvas $\mathbb{F}_{q^2}$-maximales:

1. Determinar todos los géneros posibles para una curva maximal.
2. Clasificar las curvas maximales de un dado género.

3.5.1. Géneros posibles. Stichtenoth y Xing conjeturaron en [48] que el género de una curva maximal sobre $\mathbb{F}_{q^2}$ debe satisfacer

$$g = g_1 = \frac{q(q-1)}{2} \quad \text{o} \quad g \leq \frac{(q-1)^2}{4}.$$

Esta conjetura fue mostrada por Fuhrmann y Torres en [14] usando un caso particular de la Teoría de ordenes de Frobenius asociada a un sistema linear. Tal herramienta fue creada por Stöhr-Voloch en [49].

El punto clave de la prueba de Fuhrmann-Torres es el hecho que existe un punto $\mathbb{F}_{q^2}$-racional $P_0 \in \mathcal{C}$ tal que q y $q+1$ son no lagunas en P, o sea, existen funciones x, y tales que $\mathrm{div}_\infty(x) = qP_0$ y $\mathrm{div}_\infty(y) = (q+1)P_0$.

La conjetura fue probada aplicando las técnicas de Stöhr-Voloch al sistema linear definido por $\mathcal{D} := |(Q+1)P_0|$ Así, existe un segundo mayor género g_2 dado por

$$g_2 := \begin{cases} \frac{(q-1)^2}{4} & \text{si } q \text{ es impar,} \\ \frac{q(q-2)}{4} & \text{si } q \text{ es par.} \end{cases}$$

Nuevamente existe una única curva maximal, a menos de isomorfismo, de género g_2.

En el caso de característica impar, fue mostrado en [13] que la curva maximal de g_2 es isomorfa a la curva cuyo modelo plano está dado por

$$Y^q + Y = X^{(q+1)/2}.$$

Esta curva es maximal ya que está cubierta por la curva Hermitiana y todo cubrimiento de una curva maximal es maximal también [39].

En el caso de característica par, en [5] fue mostrado que la curva cuyo modelo plano está dado por

$$Y^{q/2} + Y^{q/4} + \cdots + Y = X^{q+1}$$

es maximal y tiene género g_2, y es única si $q/2$ es una no laguna en algún punto. Finalmente la unicidad fue mostrada en [38], ya que $q/2$ es siempre una no laguna en algún punto. Más aún, ellos mostraron que existe un tercer mayor género g_3 dado por

$$g_3 = \lfloor (q^2 - q + 4)/6 \rfloor.$$

Resumiendo, tenemos el siguiente teorema.

Teorema 3.69. *Si $\mathcal{C}$ es una curva maximal definida sobre $\mathbb{F}_{q^2}$ de género g, entonces*

$$g = g_1, \quad g = g_2 \quad o \quad g \leq g_3.$$

Observación 3.70. El resultado es el mejor posible ya que existe una curva maximal de género g_3.

Observación 3.71. Si $q \equiv 2 \mod 3$, entonces $g_4 = g_3 - 1$.

Existen solamente 12 ejemplos de curvas maximales salvo isomorfismos, cuyo género satisface

$$\lfloor (q-1)(q-3)/8 \rfloor \leq g < \lfloor (q-1)^2/4 \rfloor,$$

a saber:

1. $g = \lfloor (q^2 - q + 4)/6 \rfloor$ para $q \equiv 0, 1, 2 \mod 3$ [38];
2. $g = \lfloor (q^2 - q - 2)/6 \rfloor$ para $q \equiv 2 \mod 3$ [22], [12];
3. $g = \lfloor (q-1)(q-2)/6 \rfloor$ para $q \equiv 0, 2 \mod 3$ [38];
4. $g = \lfloor (q^2 - 2q + 5)/8 \rfloor$ para $q \equiv 0, 1, 3 \mod 4$ [38];
5. $g = \lfloor (q-1)(q-3)/8 \rfloor$ para $q \equiv 0, 1, 3 \mod 4$ [38].

El objetivo de todas las investigaciones realizadas inicialmente (vea [22], [11], [4], [2]) para encontrar nuevos valores para el género de un cuerpo de funciones maximal $F|\mathbb{F}_{q^2}$ se concentraba en estudiar subcuerpos del cuerpo de funciones Hermitiano $H = \mathbb{F}_{q^2}(x, y)$ donde $y^q + y = x^{q+1}$. Giulietti y Korchmáros construyeron el primer ejemplo de un cuerpo de funciones maximal que no puede ser obtenido como subcuerpo del Hermitiano [25]. Otros ejemplos pueden ser vistos en [50].

En general, en [22] y [4], los autores consideran $H|\mathbb{F}_{q^2}$ como una extensión galoisiana de $\mathbb{F}_{q^2}(x)$ y para algunos subgrupos no moderados del grupo de automorfismos de la Hermitiana computan el género del cuerpo fijo por ese subgrupo.

A menos de conjugación por $PGU(3, \mathbb{F}_{q^2})$ los grupos no moderados están contenidos en el grupo de descomposición $\mathcal{A}(P_\infty)$ del único lugar P_∞ sobre el polo de la función x.

En nuestro caso, el grupo de descomposición $\mathcal{A}(P_\infty)$ consiste en todos los automorfismos que satisfacen

$$\begin{cases} \sigma(x) = ax + b, \\ \sigma(y) = a^{q+1}y + ab^q x + c, \end{cases}$$

donde $a \in \mathbb{F}_{q^2}^*, b \in \mathbb{F}_{q^2}$ y $c^q + c = b^{q+1}$.

El grupo $\mathcal{A}(P_\infty)$ tiene orden $q^3(q^2-1)$ y contiene un número grande de subgrupos.

Observación 3.72. Suponga que la característica es impar. Sean $\mathcal{G}$ un subgrupo de $\mathcal{A}(P_\infty)$,

$$V = \{b \in \mathbb{F}_{q^2} : \text{ existe } c \in \mathbb{F}_{q^2} \text{ tal que } [1, b, b^{q+1}/2] \in \mathcal{G}\}$$

un subgrupo de $\mathbb{F}_{q^2}$ de orden p^v y

$$W = \{c \in \mathbb{F}_{q^2} : \text{ tal que } [1, 0, c] \in \mathcal{G}\}$$

un subgrupo de $\mathbb{F}_{q^2}$ de orden p^w.

Con estas notaciones tenemos que

$$ord(\mathcal{G}) = mp^{v+w} \quad \text{con } m \mid q^2 - 1.$$

Ahora, el género del cuerpo fijo por $\mathcal{G}$ está dado por ([22])

$$g(H^{\mathcal{G}}) = (p^{n-w} - 1)(p^{n-v} + 1 - d)/2m, \quad \text{donde } d = \text{mcd}(m, q+1).$$

Ahora, para m un divisor de $q-1$, definimos

$$s = \text{orden de } p \text{ en el grupo multiplicativo } (\mathbb{Z}/m\mathbb{Z})^*,$$

$$r = \begin{cases} \text{orden de } p \text{ en } (\mathbb{Z}/\frac{m}{2}\mathbb{Z})^* \text{ si } m \equiv 0 \mod 2, \\ s \text{ caso contrario.} \end{cases}$$

Teorema 3.73. [4] *Con las notaciones anteriores, para cada divisor m de $q-1$, para todos los múltiplos v de s satisfaciendo $0 \le n \le s$ y para todos los múltiplos w de r satisfaciendo $0 \le w \le n-1$, existe un subgrupo $\mathcal{G}$ de $\mathcal{A}(P_\infty)$ de orden mp^{v+w} tal que el género del cuerpo fijo por $H^{\mathcal{G}}$ es*

$$g = \begin{cases} (p^{n-w} - 1)(p^{n-v} - 1)/2m, & m \equiv 0 \mod 2, \\ (p^{n-w} - 1)p^{n-v}/2m, & m \equiv 1 \mod 2. \end{cases}$$

Corolario 3.74. [4] *Para $m = 1$ y para todo $0 \le v \le n$ y $0 \le w \le n-1$, existe un p-subgrupo de $\mathcal{A}(P_\infty)$ tal que el género del cuerpo fijo por ese subgrupo es*

$$g = p^{n-v}(p^{n-w} - 1)/2.$$

Sea m un divisor de $q^2 - 1$ tal que m no divide $q-1$. Definimos

$$d = \text{mcd}(m, q+1),$$
$$s = \text{el orden de } p \text{ en } (\mathbb{Z}/m\mathbb{Z})^*,$$
$$r = \text{el orden de } p \ (\mathbb{Z}/\frac{m}{d}\mathbb{Z})^*.$$

Teorema 3.75. [4] *Para cada m divisor de $q^2 - 1$ tal que m no divide a $q-1$ y para cada v y w satisfaciendo*

1. $0 \le v \le n, v \mid 2n, v \nmid n$ *y v es divisible por s,*
2. $v/2 \le w \le n$, *y w es divisible por r,*

existe un subgrupo $\mathcal{G}$ de $\mathcal{A}(P_\infty)$ de orden mp^{v+w} tal que el género del cuerpo fijo por $H^{\mathcal{G}}$ es

$$g = \frac{(p^{n-w} - 1)(p^{n-v} - d + 1)}{2m}.$$

Identificamos $\sigma \in \mathcal{A}(P_\infty)$ con el par $[b, c]$ si

$$\begin{cases} \sigma(x) = x + b, \\ \sigma(y) = y + b^q x + c, \end{cases}$$

donde $b \in \mathbb{F}_{q^2}$ y $c^q + c = b^{q+1}$.

Definimos $\phi : \mathcal{G} \to \mathbb{F}_{q^2}$ por

$$\phi(\sigma) = b \quad \text{si } \sigma \text{ está identificado con el par } [b, c].$$

Esta aplicación es un morfismo suryectivo en un subgrupo aditivo de $\mathbb{F}_{q^2}$. Definimos

$$V := Im(\phi) \quad \text{y} \quad W = \{c \in \mathbb{F}_{q^2} : [0, c] \in \mathcal{G}\}.$$

Tenemos que V y W son subgrupos aditivos de $\mathbb{F}_{q^2}$ de ordenes

$$ord(V) = 2^v, \quad ord(W) = 2^w \quad \text{y} \quad ord(\mathcal{G}) = 2^{v+w}.$$

Teorema 3.76. [22] *Sea $q = 2^n$ y $g \geq 1$ un entero. Entonces son equivalentes:*

1. *Existe un 2-subgrupo $\mathcal{G} \subseteq \mathcal{A}$ tal que $g = g(H^{\mathcal{G}})$;*
2. *$g = 2^{n-v-1}(2^{n-w} - 1)$ con $0 \leq v, w \leq n - 1$ y existen $\mathbb{F}_2$-espacios vectoriales $V \subseteq \mathbb{F}_{q^2}$ y $W \subseteq \mathbb{F}_q$ de ordenes 2^v y 2^w respectivamente, tales que $V^{q+1} = \{b^{q+1} : b \in V\}$ está contenido en W.*

Teorema 3.77. *Para cada $1 \leq v \leq n-1$ tal que $v = s+k$ con $s|n$, $0 \leq k \leq s$ y para cada w satisfaciendo $s \leq w \leq n - 1$, las siguientes afirmaciones son equivalentes:*

1. *Existe un 2-subgrupo $\mathcal{G} \subseteq \mathcal{A}$ tal que $g = g(H^{\mathcal{G}})$;*
2. *$g = 2^{n-v-1}(2^{n-w} - 1)$.*

Observación 3.78. En [11] los autores consideraron subgrupos de orden p y dieron ecuaciones explícitas para los subcuerpos que obtuvieron.

3.5.2. Problema de clasificación. Para el problema de clasificación vamos a estudiar dos tipos:

1. Existe un punto racional $P_0 \in \mathcal{C}$ tal que m es una no laguna en P_0 con $m \cdot n = q + 1$ y $2g = (q - 1)(m - 1)$.
2. Existe un punto racional $P_0 \in \mathcal{C}$ tal que m es una no laguna en P_0 con $m \cdot n = q$ y $2g = q(m - 1)$ con una hipótesis extra.

Estos dos tipos aparecen naturalmente ya que si $\mathcal{C}$ es una curva maximal, entonces q y $q + 1$ son no lagunas en cualquier punto racional.

El primer caso, fue estudiado en [13] donde mostraron que existe una única curva maximal, a menos de isomorfismo y que está dada por

$$Y^q + Y = X^m.$$

Ahora, no podemos esperar tener unicidad en el segundo caso, como muestra el siguiente ejemplo.

Ejemplo 3.79. Sea $q = 2^6$ y considere las curvas $\mathcal{C}_1$ y $\mathcal{C}_2$ definidas sobre $\mathbb{F}_{q^2}$ como

$$\mathcal{C}_1 = (X^{65} + Z^{16} + Z^4 + Z = 0),$$
$$\mathcal{C}_2 = (X^{65} + W^{16} + W^8 + W^2 + W = 0).$$

Son curvas maximales, ya que son cubiertas por la Hermitiana (basta hacer $Z = Y^4 + Y$ y $W = Y^4 + Y^2 + Y$). Ambas tienen el mismo género y no son isomorfas (vea [1], [3]).

Observación 3.80. En [1] fue mostrado que en característica 2, para todo $n \in \mathbb{N}$ existen 2^{n-1} curvas maximales no isomorfas con el mismo género. En el segundo caso, Fuhrmann conjeturó que las curvas deberían ser isomorfas a

$$F(Y) = X^{q+1}, \quad \text{donde } F(Y) \text{ es un polinomio aditivo de grado } m.$$

De hecho, los ejemplos mencionados antes, son todos de este tipo.

Teorema 3.81. [3] *Sea $\mathcal{C}$ una curva maximal definida sobre $\mathbb{F}_{q^2}$ de género $g = (m-1)q/2$ donde m es una no laguna en $P_0 \in \mathcal{C}$ tal que $nm = q$. Suponga que la extensión $\mathbb{F}_{q^2}(\mathcal{C})|\mathbb{F}_{q^2}(x)$ es una extensión de Galois donde $x \in \mathbb{F}_{q^2}(\mathcal{C})$ es una función tal que $\mathrm{div}_\infty(x) = mP_0$. Entonces la curva $\mathcal{C}$ es isomorfa a la curva dada por*

$$P(z) = A(x),$$

donde $P(z) \in \mathbb{F}_{q^2}[z]$ es un polinomio aditivo separable de grado m y $A(x) \in \mathbb{F}_{q^2}[x]$ es un polinomio de grado $q+1$.

Para el caso $m = p$ (donde p es la característica del cuerpo), sin ninguna otra hipótesis, fue mostrado que la curva $\mathcal{C}$ es $\mathbb{F}_{q^2}$-isomorfa a la curva dada por

$$\sum_{i=1}^{t} z^{p^{t-i}} = cx^{p^t+1},$$

donde $c \in \mathbb{F}_{q^2}^*$ es tal que $c^q + c = 0$ y $q = p^t$.

Este resultado generaliza algunos resultados de [5] y [6].

3.6. Comportamiento asintótico. El objetivo de esta sección es el de presentar la cota de Drinfeld-Vladut y dar algunos ejemplos de cuando la cota es alcanzada.

Definimos

$$N_q(g) := \text{máx}\{N(F) : F|\mathbb{F}_q \text{ es un cuerpo de funciones de género } g\}$$

y

$$A(q) := \limsup_{g\to\infty} \frac{N_q(g)}{g}.$$

La cantidad $A(q)$ fue introducida por Ihara y satisface

$$A(q) \leq \sqrt{2q + \frac{1}{4}} - \frac{1}{2}.$$

Esta cota fue mejorada por Drinfeld-Vladut [51].

Teorema 3.82. *(Cota de Drinfeld-Vladut)*

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

La prueba del teorema usa el método de Serre de fórmulas explícitas.

Demostración. Para todo $m \in \mathbb{N}$, considere el polinomio $\Psi_m(t)$ dado por

$$\Psi_m(t) = \sum_{r=1}^{m} c_r t^r = \sum_{r=1}^{m} \big(1 - \frac{r}{m}\big) t^r,$$

así el grado es $m-1$. Para $|t| \neq 1$, podemos escribir $\Psi_m(t)$ como

$$\Psi_m(t) = \frac{t}{(t-1)^2} \cdot \Big(\frac{t^m - 1}{m} + 1 - t\Big).$$

Definiendo $f_m(t) := 1 + \Psi_m(t) + \Psi_m(t^{-1})$, tenemos que

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

Si $\gamma \in \mathcal{C}$ es tal que $|\gamma| = 1$, entonces $(\gamma - 1) \cdot (\gamma^{-1} - 1)$ es un número real positivo y $|\gamma^m + \bar{\gamma}^{-m}| \leq 2$. Esto implica que

$$f_m(t) = \frac{2 - (\gamma^m + \bar{\gamma}^{-m})}{m|\gamma - 1|^2} \geq 0,$$

para todo $\gamma \in \mathcal{C}$ con $|\gamma| = 1$. Así, tenemos

$$\frac{N_q(g)}{g} \leq \frac{1}{\Psi_m(q^{-1/2})} + \frac{1}{g}\Big(\frac{\Psi_m(q^{1/2})}{\Psi_m(q^{-1/2})} + 1\Big).$$

Si $m \to \infty$ entonces

$$\Psi_m(q^{-1/2}) \to \frac{1}{q^{1/2} - 1}.$$

Entonces para todo $\epsilon > 0$ existe g_0 tal que para todo $g > g_0$ vale

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

El teorema sigue de la desigualdad anterior. □

El valor exacto de $A(q)$ es desconocido para casi todos los valores de q. Serre mostró que $A(q) > 0$ para todo q. Cuando q es un cuadrado, Ihara mostró que $A(q) > \sqrt{q} - 1$ usando técnicas profundas de curvas modulares de Shimura y su argumento no es constructivo.

En particular, Ihara nos dice que

$$A(q) = \sqrt{q} - 1 \quad \text{cuando } q \text{ es un cuadrado.}$$

El primer ejemplo de una construcción explícita sobre $\mathbb{F}_{q^2}$ que alcanza la cota de Drinfeld-Vladut se debe a García y Stichtenoth en [20]. Desde entonces otras construcciones explícitas fueron apareciendo.

Vamos introducir algunos conceptos nuevos (vea [21]).

Definición 3.83. Una *torre* $\mathcal{F}$ sobre $\mathbb{F}_q$ es una familia infinita de cuerpos

$$F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n \subseteq F_{n+1} \subseteq \cdots$$

donde

1. $F_n|\mathbb{F}_q$ es un cuerpo de funciones para todo n;
2. $F_{n+1}|F_n$ es una extensión finita y separable para todo n;
3. $g_n := g(F_n)$ va para infinito cuando n va para infinito.

El *límite de la torre* $\mathcal{F}$ está definido por

$$\lambda_q(\mathcal{F}) := \lim_{n\to\infty} \frac{N(F_n)}{g(F_n)}.$$

Observación 3.84. El número $\lambda_q(\mathcal{F})$ existe. De hecho, si $E|F$ es una extensión separable de cuerpos de funciones definidos sobre $\mathbb{F}_q$, entonces

$$\frac{N(E)}{g(E) - 1} \leq \frac{N(F)}{g(F) - 1}.$$

Así, la sucesión $\{N(F_n)/g(F_n)\}$ es no creciente y por lo tanto es convergente.

Definición 3.85. Sea $\mathcal{F} = (F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n \subseteq F_{n+1} \subseteq \cdots)$ una torre sobre $\mathbb{F}_q$ y suponga que existan un polinomio $\Phi(X,Y) \in \mathbb{F}_q[X,Y]$ y elementos $x_r \in F_r$ para todo $r \geq 0$ tales que

1. $F_0 = \mathbb{F}_q(x_0)$;
2. $F_n = F_{n-1}(x_n)$ y $\Phi(x_{n-1}, x_n) = 0$ para todo $n \geq 1$;
3. $\Phi(x_{n-1}, Y) \in F_{n-1}[Y]$ es absolutamente irreducible sobre F_{n-1},

entonces decimos que la torre $\mathcal{F}$ está *definida recursivamente* por $\Phi(X,Y)$.

Observación 3.86. Si $\mathcal{F}$ está definida recursivamente por $\Phi(X,Y)$ y $\lambda_q(\mathcal{F}) > 0$, entonces $\deg_X(\Phi) = \deg_Y(\Phi)$.

Definición 3.87. Una torre $\mathcal{F}$ es *moderada* si y solamente si existe $F \in \mathcal{F}$ tal que la extensión $E|F$ es moderada para toda extensión $E|F$ y $E \in \mathcal{F}$.

Para cada $F \in \mathcal{F}$, definimos el conjunto de ramificación sobre F como

$V_F = \{P \in \mathbb{P}_{F \cdot \bar{\mathbb{F}}_q} : P \text{ es ramificado en alguna extensión finita } E|F \text{ y } E \in \mathcal{F}\}$.

Definición 3.88. La torre $\mathcal{F}$ es del *tipo de ramificación finita* si existe $F \in \mathcal{F}$ tal que $\#V_F < \infty$.

Definición 3.89. Una torre $\mathcal{F}$ es de *descomposición completa* si existe $F \in \mathcal{F}$ y un lugar racional $P \in \mathbb{P}_F$ tal que P se descompone totalmente en toda extensión $E|F$ con $E \in \mathcal{F}$.

Para $F \in \mathcal{F}$ definimos

$\mathcal{T}_F(\mathcal{F}) = \{P \in \mathbb{P}_F : P \text{ es racional y se descompone totalmente } \forall E|F \text{ con } E \in \mathcal{F}\}$.

Así, $\mathcal{F}$ se descompone totalmente si y solamente si existe $F \in \mathcal{F}$ tal que $\mathcal{T}_F(\mathcal{F}) \neq \emptyset$.

Observación 3.90. Para todo $F \in \mathcal{F}$ tenemos

$$0 \leq \#\mathcal{T}_F(\mathcal{F}) \leq N(F).$$

Proposición 3.91. *Sea $\mathcal{F}$ una torre moderada con ramificación de tipo finito y que se descomponga completamente, definida sobre $\mathbb{F}_q$. Sea $F \in \mathcal{F}$ tal que $\#V_F < \infty$; $\#T_F(\mathcal{F}) \geq 1$, y tal que $E|F$ es moderada para todo $E \in \mathcal{F}$. Entonces*

$$\lambda_q(\mathcal{F}) \geq \frac{2\#\mathcal{T}_F(\mathcal{F})}{2g(F) - 2 + \#V_F}.$$

Ahora, volviendo a la cota de Drinfeld-Vladut, la torre de García-Stichtenoth [20] fue la primera construcción explícita que alcanzó la cota. La torre fue definida como

1. $F_0 = \mathbb{F}_{q^2}(x_0)$;
2. $F_1 = F_0(z)$ donde $z_1^q + z_1 = x_0^{q+1}$, definiendo $x_1 = z_1/x_0$;
3. $F_2 = F_1(z_2)$ donde $z_1^q + z_1 = x_1^{q+1}$, y así sucesivamente.

Cada extensión es de Artin-Schreier y usando las propiedades de este tipo de extensión, se puede controlar la ramificación en cada paso de la torre, calcular los géneros y estimar el número de puntos racionales.

3.7. Ejercicios.

1. Complete la prueba del Teorema 3.58: Muestre que $N-(q+1) \geq -(g\lfloor 2\sqrt{q} \rfloor)$ usando $\gamma_i := -(\alpha_i + \bar{\alpha}_i) + \lfloor 2\sqrt{q} \rfloor + 1$ en lugar de β_i para $i = 1, \ldots, g$.
2. Considere la cuártica de Klein del Ejemplo 3.59.
   a) Muestre que tiene exactamente dos puntos en el infinito.
   b) Analice los puntos racionales de la forma $(x, 0, 1), (0, y, 1) \in \mathbb{F}_8^3$ y deduzca que pertenecen a la curva si y solamente si $x = y = 0$.
3. Muestre que la curva de Suzuki del Ejemplo 3.61 tiene q^2+1 puntos racionales.
4. Considere la curva de Fermat del Ejemplo 3.65.
   a) Muestre que la curva no tiene puntos racionales en el infinito.
   b) Muestre que la curva no tiene puntos racionales afines donde una de las coordenadas sea cero.
5. Muestre que σ es un automorfismo del cuerpo de funciones Hermitiano, donde
$$\begin{cases} \sigma(x) = ax + b, \\ \sigma(y) = a^{+1}y + ab^q x + c, \end{cases}$$
$a \in \mathbb{F}_{q^2}^*, b \in \mathbb{F}_{q^2}$ y $c^q + c = b^{q+1}$.
6. Considere la curva proyectiva asociada al polinomio
$$f(X, Y) = X^3Y + Y^3 + X + X^2Y^2 + Y^2 + X^2 + X^2Y + XY^2.$$
   a) Muestre que la curva es no singular y tiene género 3.
   b) Muestre que tiene 3 puntos en el infinito.
   c) Muestre que $f(x, y) = 0$ para todo $x, y \in \mathbb{F}_2$.
   d) Deduzca que $\#\mathcal{C}(\mathbb{F}_2) = 7$.

Referencias

[1] M. Abdón *On maximal curves in characteristic two*, Ph.D. dissertation, IMPA **F-121**, 1–50 (2000).

[2] M. Abdón, J. Bezerra y L. Quoos, *Further examples of maximal curves*, J. Pure Appl. Algebra **213(6)**, 1192–1196 (2009). DOI 10.1016/j.jpaa.2008.11.037.

[3] M. Abdón y A. Garcia, *On a characterization of certain maximal curves*, Finite Fields Appl. **10 (2)**, 133–158 (2004). DOI 10.1016/j.ffa.2003.06.002.

[4] M. Abdón y L. Quoos, *On the genera of subfields of the Hermitian function field*, Finite Fields and Appl **10 (3)**, 271–284 (2004). DOI 10.1016/j.ffa.2003.08.003.

[5] M. Abdón y F. Torres, On maximal curves in characteristic two, Manuscripta Math. **99**, 39–53 (1999). DOI 10.1007/s002290050161.

[6] M. Abdón y F. Torres, *On $\mathbb{F}_{q^2}$-maximal curves of genus $q(q-3) = 6$*, Beitr. Algebra Geom. **46 (1)**, 241–260 (2005).

[7] E. Arbarello; M. Cornalba, M.; P.A. Griffiths y J. Harris, Geometry of Algebraic Curves, Springer-Verlag, New York, 1985. DOI:10.1007/978-1-4757-5323-3

[8] D. Bartoli, M. Montanucci y F. Torres *$\mathbb{F}_p$-maximal curves with many automorphisms are Galois covered by the Hermitian curve*, arXiv:1708.03933v2 [math.AG]

[9] C. Carvalho, On $\mathcal{V}$-Weierstrass sets and gaps, Journal of Algebra **312**:2, 956–962 (2007). DOI:10.1016/j.jalgebra.2006.11.016.

[10] C. Carvalho y F. Torres, On Goppa codes and Weierstrass gaps at several points, Des. Codes Cryptogr. **35**:2, 211–225 (2005). DOI:10.1007/s10623-005-6403-4

[11] A. Cossidente, G. Korchmáros y F. Torres, *Curves of large genus covered by the Hermitian curve*, Comm. Algebra **28 (1)**, 4707–4728 (2000). DOI 10.1080/00927870008827115.

[12] A. Cossidente, G. Korchmáros y F. Torres, *On curves covered by the Hermitian curve*, Composition Math **216**, 56–76 (1999). DOI 10.1006/jabr.1998.7768.

[13] R. Fuhrmann, A. Garcia y F. Torres, *On maximal curves*, J. Number Theory **67(1)**, 29–51 (1997). DOI 10.1006/jnth.1997.2148.

[14] R. Fuhrman y F. Torres, *The genus of curves over finite fields with many rational points*, Manuscripta Mathematica **89(1)**, 103–106 (1996). DOI 10.1007/BF02567508.
[15] W. Fulton, *Algebraic Curves: An Introduction to Algebraic Geometry*, Addison-Wesley, 245 páginas (1989).
[16] A. Garcia y A. Garzón, *On Kummer covers with many rational points over finite fields*, Journal of Pure and Applied Algebra 185, 177–192 (2003). DOI 10.1016/S0022-4049(03)00110-5.
[17] A. Garcia y L. Quoos, *A construction of curves over finite fields*, Acta Arith. **98**, 181–195 (2001).
[18] A. Garcia, S.J. Kim y R.F. Lax, Consecutive Weierstrass gaps and minimum distance of Goppa codes, J. Pure Appl. Algebra **84**:2, 199–207 (1993). DOI:10.1016/0022-4049(93)90039-V
[19] A. Garcia y R.F. Lax, Goppa codes and Weierstrass gaps, Coding theory and algebraic geometry (Luminy, 1991), 33–42, Lecture Notes in Math., 1518, Springer, Berlin, 1992. DOI:10.1007/BFb0087991
[20] A. Garcia y H. Stichtenoth, *A tower of Artin-Schreier extensions of functions fields attaining the Drinfeld-Vladut¸ bound*, Inventiones Math. **121**, 211–222 (1995). DOI 10.1007/BF01884295.
[21] A. Garcia y H. Stichtenoth, *On towers over finite fields*, J. Reine Angew. **557**, 53–80 (1995).
[22] A. Garcia, H. Stichtenoth y C.P. Xing, *On subfields of the Hermitian function field* Compositio Math **120**, 137–170 (2000) DOI 10.1023/A:1001736016924.
[23] J. von zur Gathen y D. Panario, *A survey on factoring polynomials over finite fields*, Journal of Symbolic Computation **31**, 3-17 (2001).
[24] G van der Geer y M. van der Vlugt, *Kummer covers with many points*, Finite Fields Appl. **6(4)**, 327–341 (2000). DOI 10.1006/ffta.2000.0286.
[25] M. Giulietti y G. Korchmáros, *A new family of maximal curves over a finite field*, Math. Ann. **343**, 229–245 (2009). DOI 10.1007/s00208-008-0270-z.
[26] D.M. Goldschmidt, Algebraic functions and projective curves, Graduate Texts in Mathematics, 215. Springer-Verlag, New York, 2003. DOI:10.1007/b97844
[27] G.L. Matthews, Weierstrass pairs and minimum distance of Goppa codes, Des. Codes Cryptogr. **22**:2, 107–121 (2001). DOI:10.1023/A:1008311518095
[28] R. Hartshorne, Algebraic Geometry, Graduate Texts in Math. **52**, 496 páginas (1997).
[29] J.W.P. Hirschfeld, G. Korchmáros y F. Torres, Algebraic curves over a finite field. Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008 DOI:10.1515/9781400847419
[30] M. Homma, The Weierstrass semigroup of a pair of points on a curve, Arch. Math. **67**:4, 337–348 (1996). DOI:10.1007/BF01197599
[31] M. Homma y S.J. Kim, Goppa codes with Weierstrass pairs, J. Pure Appl. Algebra **162**:2-3, 273–290 (2001). DOI:S0022-4049(00)00134-1
[32] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Tokio **28**, 721–724 (1981).
[33] N. Ishii, A certain graph obtained from a set of several points on a Riemann surface, Tsukuba J. Math. **23**:1, 55–89 (1999). DOI:10.21099/tkbjm/1496163776
[34] H. Janwa, On the parameters of algebraic geometric codes, Applied algebra, algebraic algorithms and error-correcting codes (New Orleans, LA, 1991), 19–28, Lecture Notes in Comput. Sci., 539, Springer, Berlin, 1991 DOI:10.1007/3-540-54522-0_92
[35] J. Justesen, K. Larsen, H. Jensen, H. Elbrnd, A. Havemose y T. Holdt, *Constructing ans decoding of a class of algebraic geometry codes*, IEEE Trans. Infor. Theory **35(4)**, 811–821 (1989). DOI 10.1109/18.32157.
[36] S.J. Kim, On the index of the Weierstrass semigroup of a pair of points on a curve, Arch. Math. **62**:1, 73–82 (1994). DOI:10.1007/BF01200442.
[37] G. Korchmáros y F. Torres, *Embedding of a maximal curve in a Hermitian variety*, Composition Math. **128**, 95–113 (2001). DOI 10.1023/A:1017553432375.
[38] G. Korchmáros y F. Torres, *On the genus of a maximal curve*, Math. Ann. **323(3)**, 589–608 (2002). DOI 10.1007/s002080200316.
[39] G. Lachaud, *Sommes d'Eisenstein e nombre de points de certaines curves algébriques sur les corps finis*, C. R. Acd. Sci. Paris **305** Série I, 729–732 (1987).
[40] R. Lidl y H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, second edition, 755 páginas (1997).
[41] G. Mullen y D. Panario, *Handbook of Finite Fields*, Discrete Mathematics and Its Applications Series, CRC Press, 1068 páginas (2013).

[42] H. Niederreiter y C. P. Xing, *Rational Points on Curves over Finite Fields*, London Mathematical Society, Lecture Notes Series **288**, 256 páginas (2001).
[43] H. G Rück y H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. **457**, 185–188 (1994).
[44] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini.*, C. R. Acad. Sci. Paris **296**, 397–402 (1983).
[45] I. R. Shafarevich, *Basic Algebraic Geometry I*, Springer, 310 páginas (2013).
[46] J. H. Silverman, *The Arithmetic of Elliptic Curves over Finite Fields*, Undergraduate Texts in Mathematics, Springer New York, 281 páginas (1994).
[47] H. Stichtenoth, *Algebraic Function Fields and Codes*, Graduate Texts in Mathematics **254**, 360 páginas (2008).
[48] H. Stichtenoth y C. P. Xing, *The genus of maximal function fields*, Manuscripta Math. **86**, 217–224 (1995). DOI 10.1007/BF02567990.
[49] K.O. Stöhr y J. F. Voloch, *Weierstrass points and curves over finite fields* Proc. London Math. Soc. 52, 1–19 (1986). DOI 10.1112/plms/s3-52.1.1..
[50] S. Tafazolian, A. Teherán-Herrera y F. Torres, *Further examples of maximal curves which cannot be covered by the Hermitian curve*, J. Pure Appl. Algebra **220(3)**, 1122–1132 (2016). DOI 10.1016/j.jpaa.2015.08.010.
[51] S.G. Vladut y V.G. Drinfeld, *Number of points of an algebraic curve*, Funct. Anal. **17(1)**, 68–69 (1983). DOI 10.1007/BF01083182.

Universidade Federal Fluminense, Instituto de Matemática e Estatística. Rua Professor Marcos Waldemar de Freitas Reis, s/n, Blocos G e H - Campus do Gragoatá, Niterói - RJ, CEP: 24210-201 - Brasil
Email address: miriam_abdon@id.uff.br

Universidade Federal de Uberlândia, Faculdade de Matemática, Av. J.N. de Ávila 2121, 38400-902 Uberlândia - MG, Brasil
Email address: cicero@ufu.br

Carleton University, School of Mathematics and Statistics, 1125 Colonel By Dr., K1S 5B6 Ottawa - Ontario, Canada
Email address: daniel@math.carleton.ca