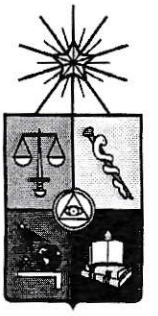


Buscando parámetros óptimos para la calidad de Códigos Goppa sobre curvas Hermitianas y su decodificación.

Tesis

entregada a la

Universidad de Chile

en cumplimiento parcial de los requisitos

para optar al grado de

Magíster en Ciencias con mención en Matemáticas

Facultad de Ciencias

por

Victoria Fernández Bascuñán

Enero, 2013

Director de Tesis: **Dr. Antonio Behn.**

FACULTAD DE CIENCIAS
UNIVERSIDAD DE CHILE

INFORME DE APROBACIÓN
TESIS MAGÍSTER

Se informa a la Escuela de Postgrado de la Facultad de Ciencias que la Tesis de Magíster presentada por la candidata

Victoria Fernández Bascuñán

ha sido aprobada por la Comisión de Evaluación de la Tesis como requisito para optar al grado de Magíster en Ciencias con mención en Matemáticas, en el examen de Defensa de Tesis rendido el día 28 de Diciembre del 2012.

Director de Tesis

Dr. Antonio Behn

Comisión de Evaluación de la Tesis

Dra. Anita Rojas

Dr. Luis Arenas

Dedicado a

mi amorcito

AGRADECIMIENTOS

Quiero agradecer a todos aquellos que me acompañaron en este difícil proceso, que empezó el año 2005 con mi ingreso a la licenciatura y que culmina hoy con la entrega de esta tesis.

Para comenzar quiero agradecer enormente a mi amorcito lindo, por confiar siempre en mi, por apoyarme, ayudarme y contenerme en los momentos complicados. Tu compañia, apoyo y amor han sido fundamentales en todo este proceso, de verdad muchas gracias.

También quiero agradecer a mi mamá, papá, hermanita y amigos, que apesar de no entender mucho lo que hago, se que apoyan y confían 100 % en mi.

No puedo dejar de agradecer a mis pilares desde la licenciatura, con quienes pasé los mejores y peores momentos, y por lo cual son muy importantes para mi, me refiero a mi chanchita linda, al Ale, la Tere y la Roxana.

Finalmente, agradecer a todos los profesores que participaron en mi formación, por estar siempre dispuestos para nosotros, en especial a mi tutor, el profesor Antonio Behn, quien accedio a ayudarme y guiarme a lo largo de esta tesis.

¡Muchas gracias a todos!

Índice general

RESUMEN

En esta tesis analizaremos los parámetros de un código Goppa $C_{D,G}$, para definir e imponer ciertas condiciones a los divisores D y G que harán a nuestros códigos óptimos al momento de corregir errores de transmisión. Aprovecharemos la correspondencia que existe entre curvas algebraicas y cuerpos de funciones, para definir estos códigos Goppa y analizar sus parámetros. En particular, consideraremos el cuerpo de funciones Hermitianas $\mathcal{H}$ y algunos de sus subcuerpos, elegidos por tener muchos lugares racionales. Apartir de ellos generaremos códigos Goppa para luego comparar sus parámetros. Se crean algunas herramientas para calcular los cuerpos fijos $\mathcal{H}^{\mathcal{G}}$ para algunos subgrupos $\mathcal{G}$ del grupo de automorfismos de $\mathcal{H}$ y sus correspondientes códigos.

ABSTRACT

In this thesis we analyze the Goppa code's $(C_{D,G})$ parameters to acquire certain conditions over the divisors D and G such that our codes become optimal in the sense of error correction. We will use the correspondence between algebraic curves and function fields to define these Goppa codes and analyze their parameters. In particular, we will consider Hermitian function fields and some of its subfields, chosen for having many rational points. With these fields we will construct Goppa codes to compare its parameters. We created some tools to compute the fixed fields $\mathcal{H}^{\mathcal{G}}$ for some subgroups $\mathcal{G}$ of the automorphism group of $\mathcal{H}$ and its corresponding codes.

Capítulo 1

Preliminares

Comenzaremos con una breve introdución a la teoría de códigos, pasando desde sus orígenes a su modelo general, mostrando también una cota para sus parámetros. Seguiremos con una descripción más detallada de cuerpos de funciones algebraicas, incluyendo extensiones de Galois de cuerpo de funciones. Finalmente recordaremos algunas definiciones básicas de Geometría Algebraica y aprovecharemos la correspondecia que existe entre curvas algebraicas y cuerpos de funciones para entender (en el siguiente capítulo) los llamados códigos Geométrico-Algebraicos o códigos Goppa.

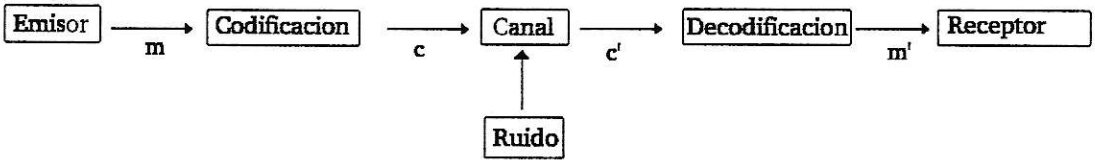
1.1. Introducción a la Teoría de Códigos.

En mas de alguna ocasión nos hemos encontrado con textos que tienen palabras mal escritas o le faltan algunas letras y aún así somos capaces de leerlos y entenderlos sin problemas. Esto se debe a que el lenguaje es un código y sus palabras son lo suficientemente distintas como para detectar o corregir una gran cantidad de errores de escritura.

Pero el lenguaje es un código muy conocido, por lo que no goza de mucha seguridad. Esto ha llevado al hombre, desde hace miles de años, a construir distintos

códigos dependiendo de sus necesidades. En un principio, luego de ser codificados, los mensajes eran transportados por personas y por lo tanto, una vez entregados satisfactoriamente sólo bastaba conocer el código para descifrarlos. Sin embargo, el auge de las comunicaciones a partir de la segunda mitad del siglo XX motivó la necesidad de transmitir información a través de ciertos canales, los que no necesariamente eran personas y esto generó bastantes problemas, ya que la información enviada a través de estos canales podía sufrir algunas alteraciones en el camino y generar mensajes distintos a los enviados, dependiendo de las perturbaciones que tuviera el canal y por lo tanto ya no bastaba sólo conocer el código para decifrar el mensaje.

Para ejemplificar la situación, supongamos que nosotros "los emisores" queremos enviar cierto mensaje m. Entonces el proceso comienza transformando el mensaje m en el mensaje encriptado c, el cual será enviado a través de un canal de comunicación. Las características del canal dependen de la naturaleza del mensaje a ser enviado (por ejemplo, si el mensaje son transmisiones desde un satélite, el canal es el espacio). Nuestro intermediario recibirá un mensaje codificado c' posiblemente erróneo, ya que en todo proceso de comunicación hay ruido e interferencias. Finalmente, se intentan corregir o detectar los errores de transmisión del mensaje c', para luego decodificarlo generando un mensaje desencriptado m' que es entregado al "el receptor". Todo el proceso se resume en el siguiente esquema:



Con el tiempo las formas de encriptar información fueron mejorando, y los problemas al enviar y luego tratar de desencriptar esta información se estudiaron en profundidad, dando nacimiento a la rama de la matemática llamada Teoría de Códigos. El problema principal de la teoría de códigos es el cómo poder transmitir información

de manera segura y fiable a través de un canal que sea poco seguro y poco fiable (con ruido). Como ejemplos que todos conocemos podemos pensar en:

- Conversaciones telefónicas convencionales, donde el canal es el cable.
- Transmisiones desde un satélite o telefonía móvil. Aquí el canal es el espacio.
- Grabación y recuperación de datos en el disco duro de un ordenador o en un disco compacto (de música por ejemplo). El canal a través del que transmitimos los datos es en este caso el propio disco.

1.1.1. Códigos Lineales.

Definición 1.1. *Sea $A = \{a_1, a_2, \ldots, a_q\}$ un conjunto finito de q elementos distintos. A este conjunto le llamaremos alfabeto (ó alfabeto del código).*

En muchas aplicaciones se considera al conjunto A como un cuerpo finito.

Definición 1.2. *Sea $A = \{a_1, a_2, \ldots, a_q\}$ un alfabeto. Entonces*
(i) Todo subconjunto no vacío C de A^n es llamado un código (o código q-ario). Cada $c \in C$ será llamada palabra del código, n el largo del código y la cantidad de palabras en C será el tamaño del código.
(ii) Si el alfabeto A es un espacio vectorial sobre algún cuerpo K y C es un subespacio de A^n, entonces el código C será llamado lineal.

Definición 1.3. *En A^n se define d, la llamada distancia de Hamming mediante*

$$d(\vec{x}, \vec{y}) := \#\{i : x_i \neq y_i\},$$

donde $\vec{x} = (x_1, ..., x_n)$ e $\vec{y} = (y_1, ..., y_n)$. Definimos el peso de $\vec{x}$ por

$$w(\vec{x}) := d(\vec{x}, \vec{0}),$$

donde $\vec{0} = (0, ..., 0)$.

De aquí en adelante siempre que hablemos de distancia estaremos hablando de la distancia de Hamming.

Definición 1.4. *Para cada código C definimos la distancia mínima como*

$$d(C):=min\{d(\vec{x},\vec{y}) : \vec{x},\vec{y} \in C, \vec{x} \neq \vec{y}\}.$$

Notemos que si C es un código lineal la anterior definición es equivalente a

$$d(C):=\min\{w(\vec{x}) : \vec{x} \in C, \vec{x} \neq \vec{0}\}.$$

Diremos que C es un $[n,k,d]_q$-*código lineal* si es un subespacio vectorial de $\mathbb{F}_q^n$ de dimensión k y distancia mínima d.

La distancia mínima será de vital importancia en la detección y corrección de errores de transmisión, como veremos en el próxima sección.

1.1.2. Modelo General.

El modelo general de un sistema de protección contra los errores producidos en el almacenamiento o la transmisión de información a través de un canal discreto (sin memoria)[1] sometido a ruido comprende los siguientes elementos:

Emisión.

Para el proceso de emisión necesitamos definir un alfabeto al que llamaremos *alfabeto fuente* y denotaremos por A. También debemos definir el largo de las palabras del mensaje, al cual llamaremos k, es decir, una palabra cualquiera m será de la forma

$$m = a_1 a_2 \cdots a_k \quad \text{donde } a_i \in A \text{ para todo } 1 \leq i \leq k.$$

[1] Con esto nos referimos a un canal cuyo alfabeto de entrada y salida es un conjunto finito, y que además no guarda la información transmitida.

Codificación.

Una vez definido el alfabeto fuente se construye un código $C \subset A^n$ $(k < n)$ que ocuparemos para encriptar nuestros mensajes. Pero antes de encriptar nuestros mensajes definiremos algunos elementos que nos serán de gran utilidad, en el caso en que A sea un cuerpo finito.

Definición 1.5. *Dado $\mathbb{F}_q$ un alfabeto fuente y C un $[n,k,d]_q-$ código lineal, se llamará codificador a una función lineal $f : \mathbb{F}_q^k \longrightarrow C$.*

Esta función puede ser representada una matriz Γ de rango k, la cual no está únicamente determinada, ya que depende de la base en la que trabajemos.

Definición 1.6. *Sea C un $[n,k,d]_q-$ código lineal, llamamos matriz generadora de C a una $(k \times n)-$ matriz Γ, tal que*

$$C = \{v\Gamma \mid v \in \mathbb{F}_q^k\}$$

Observación 1.1. Si $C \subseteq \mathbb{F}_q^n$ un código lineal de dimensión k, entonces una matriz generadora de C es una matriz de $k \times n$ cuyas filas formen una base de C sobre $\mathbb{F}_q$.

En conclusión, una vez definido un código $C \subset \mathbb{F}_q^n$, encontramos una matriz generadora Γ de C. Así, nuestro proceso de codificación consistirá en tomar una palabra $m \in \mathbb{F}_q^k$ y convertirla en la palabra $c = m\Gamma$ perteneciente al código C.

Canal.

Una vez codificado el mensaje, el paso siguiente es atravesar un canal de comunicación, pero ¿qué es un canal de comunicación?.

Un *canal de comunicación* es el medio de transmisión por el que viajan las señales portadoras de la información de emisor a receptor. Éste puede ser desde al aire, hasta señales electomagnéticas o un disco compacto (CD).

Lo importante de un canal de comunicación es que si recibe una palabra $c \in A^n$,

devuelve una palabra $c' \in A^n$, donde la distancia entre c de c' depende del ruido del canal.

Si A tiene estructura algebraica entonces $c' = c + r$, donde $r \in A^n$. La distancia entre r y 0 es llamada la cantidad de *errores de transmisión* de la palabra c.

Para nuestro propósito, el mensaje enviado, luego de pasar por el canal de transmisión, será $c' = c + r$ y quisieramos corregir estos errores para recuperar el mensaje c.

Decodificación.

No es una tarea fácil, a partir de c' recuperar el mensaje c, de hecho si la palabra recibida es otra palabra del código no hay manera de saber cual fue la palabra enviada, ni siquiera detectar que hubo un error. Es en este caso que un código con distancia mínima grande se vuelve muy útil, ya que si la cantidad de errores que trae c' es menor que $d(C)$, es decir, $d(c, c') < d(C)$, entonces c' no es una palabra del código y por lo tanto a mayor distancia mínima (como veremos más adelante) mayor es la cantidad de errores podemos corregir o detectar.

La siguiente definición y el posterior lema, nos entregarán una manera fácil de verificar si c' es o no una palabra del código.

Definición 1.7. *Sea $C \subseteq \mathbb{F}_q^n$ un código. El código dual de C es el código $C^\perp$ definido por*

$$C^\perp := \{x \in \mathbb{F}_q^n \,:\, \langle x, y\rangle = 0 \,\forall\, y \in C\},$$

donde para cada $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)$, $\langle x, y\rangle := \sum x_i y_i$ es la forma bilineal usual de $\mathbb{F}_q^n \times \mathbb{F}_q^n$.

Notar que $C^\perp$ es de hecho un código lineal.

Lema 1.1. *Sea $C \subset \mathbb{F}_q^n$ un código lineal de dimensión k y matriz generadora Γ. Entonces*

(1) $C^\perp = \{x \in \mathbb{F}_q^n \,:\, \Gamma x^t = 0\}$.

(2) $C^{\perp}$ *tiene dimensión* $n-k$.

Donde x^t, *denotará la traspuesta de* x. *Para una demostración ver [4] pag. 2.*

Corolario 1.1. *Sea* C *un código lineal y sea* H *una matriz generadora de* $C^{\perp}$. *Entonces*

(1) $C = (C^{\perp})^{\perp}$.

(2) $C = \{x \in \mathbb{F}_q^n \ : \ Hx^t = 0\}$.

Para una demostración ver [4] pag. 3

Por lo tanto, c' pertenece a C si y sólo si $Hc' = 0$, o sea, tenemos una forma fácil de verificar si la palabra recibida, luego de pasar por el canal de transmisión, pertenece o no al código C.

Ahora veremos dos teoremas que nos dirán cuando es posible detectar que la palabra c' contiene errores y cuando es posible recuperar la palabra enviada c.

Teorema 1.1. *Un código con distancia mínima* $d(C)$ *nos permite detectar* s *errores si* $d(C) \geq s+1$.

Demostración: Supongamos que $d(C) \geq s+1$ y que enviamos la palabra $c \in C$ y recibimos la palabra $c' \in A^n$ con s errores. Lo que afirmamos es que $c' \notin C$ pues $d(c,c') = s < d(C)$ y esto no puede ocurrir entre palabras de código por definición de distancia mínima, por lo tanto, los s errores son detectados. □

Teorema 1.2. *Un código con distancia mínima* $d(C)$ *nos permite corregir* t *errores si* $d(C) \geq 2t+1$.

Demostración: Supongamos que $d(C) \geq 2t+1$ y que enviamos la palabra $c \in C$ y recibimos la palabra $c' \in A^n$ con t errores. Lo que afirmamos es que c es la única palabra del código a distancia menor o igual a t de c'. Esto se debe a que si existiese otra palabra de C, digamos c_1 con $d(c_1,c') \leq t$ entonces $d(c,c_1) \leq d(c,c') + d(c',c_1) \leq 2t$, lo que contradice que la distancia mínima entre dos palabras del código es mayor o igual a $d(C)$. □

Observación 1.2. Notar que si $d \geq s+1$ y $d \geq 2t+1$, no podemos detectar s errores y corregir t simultáneamente.

Observación 1.3. Con los teoremas anteriores podemos concluir que los mejores códigos tendrán una distancia mínima lo más grande posible.

Definición 1.8. *Se llamarán parámetros relativos de C al par $[R, \delta]$, donde $R := k/n$ se llama tasa de transmisión y representa simultáneamente el costo y la velocidad de transmisión, y donde $\delta := d/n$ se llama distancia relativa y mide la capacidad correctora en relación a su longitud.*

Observación 1.4. Con la definición anterior es natural querer que tanto R como δ estén lo más cerca de 1 posible. Lamentablemente estos parámetros dependen uno del otro, como veremos a continuación, y por lo tanto nos conformaremos con que su suma sea lo más grande posible.

1.1.3. Cota de Singleton

Proposición 1.1. *(Cota de Singleton [1]) Si C es un $[n,k,d]_q$-código lineal sobre $\mathbb{F}_q$, se cumple que:* $$d - 1 \leq n - k$$

La cota de Singleton es equivalente a $\delta + R \leq 1 + 1/n$, lo que significa que la suma de los parámetros relativos de un código no pueden exceder al valor $1 + 1/n$. Nuestro trabajo se enfocará en conseguir códigos donde la suma de los parámetros relativos se acerquen los que más posible a esta cota.

Definición 1.9. *Un $[n,k,d]_q$-código lineal sobre $\mathbb{F}_q$ se llamará MDS (maximum distance separable) si $d - 1 = n - k$.*

1.2. Cuerpos de Funciones Algebraicas.

En la sección anterior conocimos la cota de Singleton, como una cota superior para la suma de los parámetros relativos del código, sería ideal contar también

con una cota inferior. Cotas de este tipo existen, pero en general no son óptimas. Sin embargo, existen cierto tipos de códigos, los llamados códigos Goppa ó códigos Geométrico-Algebraicos (que conoceremos en el siguiente capítulo) que poseen una cota inferior bastante buena. Para definir estos códigos primero necesitamos introducir el concepto de cuerpos de funciones algebraicas.

1.2.1. Definiciones.

Definición 1.10. *Un cuerpo de funciones algebraicas F/K de una variable sobre K es una extensión de cuerpos $F \supseteq K$ tal que F es una extensión algebraica finita de $K(x)$ para algún elemento $x \in F$ el cual es trascendente sobre K.*

Definición 1.11. *Un anillo de valuación de un cuerpo de funciones F/K es un anillo $\mathcal{O} \subseteq F$ con las siguientes propiedades:*
(1) $K \subsetneq \mathcal{O} \subsetneq F$.
(2) para cada $z \in F$ tenemos que $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$.

Para la demostración de la siguiente propiedad y posterior teorema ver [1], pag. 2 y 3.

Proposición 1.2. *Sea $\mathcal{O}$ un anillo de valuación de un cuerpo de funciones F/K. Entonces se cumplen las siguientes afirmaciones:*
(a) $\mathcal{O}$ es un anillo local, es decir, $\mathcal{O}$ tiene un único ideal maximal $P = \mathcal{O} \backslash \mathcal{O}^{\times}$, donde $\mathcal{O}^{\times} = \{z \in \mathcal{O} |$ existe un elemento $w \in \mathcal{O}$ con $zw = 1\}$ es el subgrupo de unidades de $\mathcal{O}$.
(b) Sea $0 \neq x \in F$. Entonces $x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$

Teorema 1.3. *Sea $\mathcal{O}$ un anillo de valuación del cuerpo de funciones F/K y sea P su único ideal maximal. Entonces tenemos,*
(a) P es un ideal principal.
(b) Si $P = t\mathcal{O}$ entonces cada $0 \neq z \in F$ tiene una representación única de la forma

$z = t^n u$ para algún $n \in \mathbb{Z}$ y $u \in \mathcal{O}^\times$.

(c) $\mathcal{O}$ es un dominio de ideales principales. Mas aún, si $P = t\mathcal{O}$ y $\{0\} \neq I \subseteq \mathcal{O}$ es un ideal entonces $I = t^n\mathcal{O}$ para algún $n \in \mathbb{N}$.

Un anillo que tiene las propiedades anteriores es llamado un anillo de valuación discreta.

1.2.2. Lugares.

Definición 1.12. *Para F/K un cuerpo de funciones algebraicas definimos:*

(a) Un lugar P de un cuerpo de funciones es el ideal maximal de algún anillo de valuación $\mathcal{O}$ de F/K. Cada elemento $t \in P$ tal que $P = t\mathcal{O}$ es llamado un parámetro uniformizante de P (también es llamado parámetro local o elemento primo).

(b) $\mathbb{P}(F) := \{P : P$ es un lugar de $F/K\}$.

Si $\mathcal{O}$ es un anillo de valuación de F/K y P es su ideal maximal, entonces $\mathcal{O}$ está únicamente determinado por P, a saber, $\mathcal{O} = \{z \in F : z^{-1} \notin P\}$. Luego $\mathcal{O}_P := \mathcal{O}$ es llamado *anillo de valuación del lugar P.*

Una segunda descripción útil del conjunto de lugares está dada en términos de valuaciones.

Definición 1.13. *Una valuación discreta de F/K es una función $v : F \to \mathbb{Z} \cup \{\infty\}$ con las siguientes propiedades:*

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

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

(3) $v(x + y) \geq min\{v(x), v(y)\}$ para todo $x, y \in F$

(4) Existe un elemento $z \in F$ con $v(z) = 1$

(5) $v(a) = 0$ para todo $0 \neq a \in K$

Para las demostraciones del Lema 1.2 y Teorema 1.4 ver [1] pag. 5.

Lema 1.2. *Sea v una valuación discreta de F/K y sean $x, y \in F$ con $v(x) \neq v(y)$. Entonces $v(x + y) = min\{v(x), v(y)\}$.*

Para cada lugar $P \in \mathbb{P}(F)$ definiremos la función $v_P : F \to \mathbb{Z} \cup \{\infty\}$ como sigue: Escogemos un parámetro uniformizante t de P, luego cada $0 \neq z \in F$ tiene una única representación $z = t^n u$, donde $u \in \mathcal{O}_P^\times$ y $n \in \mathbb{Z}$. Así definimos,

$$v_P(z) := n \text{ y } v_P(0) := \infty.$$

Observemos que esta definición sólo depende de P, no de la elección de t.

Teorema 1.4. *Sea F/K un cuerpo de funciones.*
(a) Para un lugar $P \in \mathbb{P}_F$, la función v_P definida anteriormente es una valuación discreta de F/K. Mas aún tenemos

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

(b) Un elemento $t \in F$ es un parámetro uniformizante de P si y sólo si $v_P(t) = 1$.
(c) Inversamente, suponemos que v es una valuación discreta de F/K. Entonces el conjunto $P := \{z \in F : v(z) > 0\}$ es un lugar de F/K, y $\mathcal{O}_P := \{z \in F : v(z) \geq 0\}$ es su correspondiente anillo de valuación.
(d) Cada anillo de valuación $\mathcal{O}$ de F/K es un subanillo propio maximal de F.

Sea P un lugar de F/K y sea $\mathcal{O}_P$ su anillo de valuación. Como P es un ideal maximal, $\mathcal{O}_P/P$ es un cuerpo. Para cada $x \in \mathcal{O}_P$ definimos $x(P) \in \mathcal{O}_P/P$ como la clase residual de x módulo P, para $x \in F \backslash \mathcal{O}_P$ ponemos $x(P) := \infty$. Es fácil comprobar que $K \subset \mathcal{O}_P$ y $K \cap P = \{0\}$, luego la función residual $\mathcal{O}_P \to \mathcal{O}_P/P$ induce una inscrustación canónica de K en $\mathcal{O}_P/P$. A partir de ahora siempre consideraremos K como un subcuerpo de $\mathcal{O}_P/P$ via esta incrustación.

Definición 1.14. *Sea $P \in \mathbb{P}(F)$.*
(a) $F_P := \mathcal{O}_P/P$ es el cuerpo residual de P. La función $x \mapsto x(P)$ de F a $F_P \cup \{\infty\}$ es llamado la función residual con respecto de P.

(b) $deg(P) := [F_P : K]$ *es llamado el grado de* P. *Un lugar de grado 1 es llamado un lugar racional de* F/K.

(c) Denotaremos por $\mathcal{N}(F)$ *al conjunto de todos los lugares racionales de* F.

Es un resultado conocido que el grado de un lugar es siempre finito, pero si desea una demostración puede ver [1] pag. 6.

Definición 1.15. *Sea* $z \in F$ *y* $P \in \mathbb{P}(F)$. *Diremos que* P *es un cero de* z *si* $v_P(z) > 0$; P *es un polo de* z *si* $v_P(z) < 0$. *Si* $v_P(z) = m > 0$, P *es un cero de* z *de orden* m; *si* $v_P(z) = -m < 0$, P *es un polo de* z *de oden* m.

1.2.3. Divisores.

Definición 1.16. *El grupo de divisores de* F/K, *denotado por* $Div(F)$, *es un grupo abeliano libre generado por los lugares de* F/K. *Los elementos de este grupo son llamados divisores de* F/K.

En otras palabras, un *divisor* D es una suma formal finita de lugares de $\mathbb{P}(F)$, esto es $D = \sum_{P\in\mathbb{P}(F)}(n_P P)$, donde n_P es un entero igual a 0 para casi todos los lugares de $\mathbb{P}(F)$.

Definición 1.17. *Para cada* $D \in Div(F)$ *definimos su soporte por,*

$$supp(D) := \{P \in \mathbb{P}(F) : n_P \neq 0\}$$

Definición 1.18. *Dos divisores* $D = \sum_{P\in\mathbb{P}(F)}(n_P P)$ *y* $D' = \sum_{P\in\mathbb{P}(F)}(n'_P P)$ *se suman de manera natural como sigue,*

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

Definición 1.19. *El elemento cero de el grupo de divisores es* $D = \sum_{P\in\mathbb{P}(F)} n_P P$ *con* $n_P = 0$ *para todo* $P \in \mathbb{P}(F)$.

Definición 1.20. *Si* $n_P \geq 0$ *para todo* $P \in \mathbb{P}(F)$ *llamaremos a* D *positivo o efectivo.*

Definición 1.21. *Sea $D = \sum_{P \in \mathbb{P}(F)} n_P P$ un divisor de F, definimos el grado de D como sigue*

$$deg(D) = \sum_{P \in \mathbb{P}(F)} n_P \cdot deg(P).$$

Definición 1.22. *Llamaremos divisores de un punto a los divisores $D = mP$ donde P es un lugar racional de F y $m > 0$.*

1.2.4. El teorema de Riemann-Roch.

Antes de enunciar el teorema de Riemann-Roch, debemos definir el concepto de divisor asociado a una función y el espacio de Riemann-Roch asociado a un divisor.

Definición 1.23. *Sea $f \in F$, como f tiene una valuación para cada lugar en $\mathbb{P}(F)$, es natural asociar a f con un divisor, que llamaremos divisor de f como sigue:*

$$(f) := \sum_{P \in \mathbb{P}(F)} v_P(f)P.$$

Notemos que tal divisor es el divisor cero si y sólo si $f \in K$.
Si $f \notin K$, (f) puede ser escrito como diferencia de dos divisores efectivos

$$(f) = (f)_0 - (f)_\infty,$$

donde $(f)_0 = \sum_{v_P > 0} v_P(f)P$ es el *divisor de los ceros de f* y $(f)_\infty = \sum_{v_P < 0} v_P(f)P$ es el *divisor de los polos de f*.
Para la construcción de códigos lineales, el siguiente concepto jugará un rol fundamental.

Definición 1.24. *Dado un divisor $D = \sum n_P P$, el conjunto de todas las funciones que satisfacen $v_P(f) \geq -n_P$ para todo lugar P, junto con la función cero, es llamado el espacio de Riemann-Roch asociado a D y es denotado por $\mathcal{L}(D)$.*

Es sencillo chequear que $\mathcal{L}(D)$ es un espacio vectorial sobre K. Un poco mas complicado es verificar que además su dimensión es finita (ver [1] pag. 18). A esta dimensión la denotaremos por $l(D)$.

Observación 1.5. Para un divisor efectivo D, $\mathcal{L}(D)$ consiste en todas las funciones que cumplen con que todos sus polos se encuentran en el supp(D), y la multiplicidad de cada uno de ellos no es mayor que n_P.

Observación 1.6. Si D es un divisor de un punto, es decir $D = mP$, entonces

$$\mathcal{L}(D) = \{f \in K : (f)_\infty = lP, \text{ con } l \leq m\} \cup \{0\}.$$

Además si $f_1, \ldots, f_r \in \mathcal{L}(D)$ son tales que $v_P(f_i) \neq v_P(f_j)$ $\forall\, i \neq j$, $1 \leq i, j \leq r$. Entonces $f_1, \ldots, f_r$ son linealmente independientes sobre K (ver [4] pag. 12).

Observación 1.7. No es difícil verificar que para todo $D \in Div(F)$ con $deg(D) < 0$ se tiene que $\mathcal{L}(D) = \{0\}$ y que además $\mathcal{L}(0) = K$.

En general, calcular la dimensión del espacio $\mathcal{L}(D)$ es complicado. Para solucionar este problema contamos con el teorema de Riemann-Roch, el cual nos da una fórmula para calcular tal dimensión. Pero antes de esto necesitamos un par de definiciones.

Definición 1.25. *El género g de F/K está definido por*

$$g := max\{deg(A) - l(A) + 1 : A \in Div(F)\}.$$

Considerando $A = 0$ se puede concluir que $g \geq 0$.

Definición 1.26. *Un divisor canónico de F es un divisor W que cumple con:*

$$deg(W) = 2g - 2 \quad y \quad l(W) = g,$$

donde g es el género de F.

Teorema 1.5. ***(Teorema de Riemann-Roch** [1]) Dado un divisor D,*

$$l(D) = deg(D) + 1 - g + l(W - D),$$

donde W es algún divisor canonico.

Aún con esta fórmula calcular $l(D)$ puede resultar complicado, ya que debemos conocer $l(W - D)$. Para liberarnos de este problema, podemos restringuir el grado del divisor D y recurrir al siguiente corolario [1].

Corolario 1.2. *Para todo divisor D tal que $deg(D) \geq 2g - 1$,*

$$l(D) = deg(D) + 1 - g$$

1.3. Extensiones de Cuerpos de Funciones.

Nos interesa estudiar extensiones de cuerpos de funciones, por la relación que existe entre los lugares de un cuerpo de funciones F y los lugares de una extensión de F, cuando esta extensión también es un cuerpo de funciones.

1.3.1. Definiciones.

Definición 1.27. *a) Un cuerpo de funciones algebraicas F'/K' es llamada una extensión algebraica de F/K si $F' \supseteq F$ es una extensión de cuerpos algebraica y $K' \supseteq K$.*
b) La extensión algebraica F'/K' de F/K es llamada finita si $[F' : F] < \infty$

Definición 1.28. *Consideremos la extensión algebraica F'/K' de F/K. Se dice que un lugar de $P' \in \mathbb{P}(F')$ se encuentra sobre $P \in \mathbb{P}(F)$ si $P \subseteq P'$. También diremos que P' es una extensión de P o que P se encuentra bajo P', y escribiremos $P'|P$.*

Para las demostraciones de la Proposiciones 1.3 y 1.4, Lema 1.3 y Teoremas 1.6, 1.7 y 1.8 ver [1] en las pag. 69, 111, 98, 74, 100 y 99 respectivamente.

Proposición 1.3. *Sea F'/K' una extensión algebraica de F/K. Supongamos que P (resp. P') es un lugar de F/K (resp. F'/K'), $\mathcal{O}_P \subseteq F$ (resp. $\mathcal{O}_{P'} \subseteq F'$) el*

correspondiente anillo de valuación y v_P *(resp.* $v_{P'}$*) la correspondiente valuación discreta. Entonces las siguientes afirmaciones son equivalentes:*

1) $P'|P$.

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

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

Mas aún, si $P'|P$ *entonces,*

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

Por esta razón, P *es también llamada la restricción de* P' *en* F.

Una consecuencia de la anterior proposición es que para $P'|P$ existe una inyección canonica del cuerpo residual $F_P = \mathcal{O}_P/P$ en el cuerpo residual $F_{P'} = \mathcal{O}_{P'}/P'$, dada por

$$x(P) \mapsto x(P') \quad \text{para} \quad x \in \mathcal{O}_P$$

Por lo tanto podemos considerar F_P como un subcuerpo de $F_{P'}$.

Definición 1.29. *Sea* F'/K' *una extensión algebraica de* F/K, *y sea* $P' \in \mathbb{P}(F')$ *un lugar de* F'/K' *que se encuentra sobre* $P \in \mathbb{P}(F)$.

a) El entero $e(P'|P) := e$ *con*

$$v_{P'}(x) = e \cdot v_P(x) \quad \textit{para todo} \quad x \in F$$

es llamado el índice de ramificación de P' *sobre* P.

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

b) $f(P'|P) := [F_{P'} : F_P]$ *es llamado el grado relativo de* P' *sobre* P.

Notemos que $f(P'|P)$ puede ser finito o infinito; mientras que el índice de ramificación siempre es un número natural, ya que si $x \in P$ entonces $v_P(x) > 0$ y como $P \subset P'$ entonces $v_{P'}(x) > 0$.

Teorema 1.6. *(Igualdad Fundamental) Sea F'/K' una extensión finita de F/K, sea P un lugar de F/K y sean $P_1, \cdots, P_r$ todos los lugares de F'/K' que se encuentran sobre P. Denotemos por $e_i := e(P_i|P)$ a los índices de ramificación y por $f_i := f(P_i|P)$ a los grados relativos de $P_i|P$. Entonces*

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

Definición 1.30. *Sea F'/K' una extensión de F/K de grado $[F' : F] = n$ y sea $P \in \mathbb{P}(F)$.*

a) P se descompone completamente en F'/F si existen exactamente n distintos lugares $P' \in \mathbb{P}(F')$ con $P'|P$.

b) P es totalmente ramificado en F'/F si existe un lugar $P' \in \mathbb{P}(F')$ con $P'|P$ y $e(P'|P) = n$.

Por la Igualdad Fundamental es claro que un lugar $P \in \mathbb{P}(F)$ se descompone completamente en F'/F si y sólo si $e(P'|P) = f(P'|P) = 1$ para todos los lugares $P'|P$ en F'. Si P está totalmente ramificado en F'/F entonces existe exactamente un lugar $P' \in \mathbb{P}(F')$ con $P'|P$.

La siguiente definición contiene varios términos que no definiremos, dado que sólo nos interesa introducir el diferente de una extensión de cuerpos de funciones F'/F.

Definición 1.31. *Consideremos un lugar $P \in \mathbb{P}(F)$ y la clausura integral[2] $\mathcal{O}'_P$ de $\mathcal{O}_P$ en F'. Sea $\mathcal{C}_P = t \cdot \mathcal{O}'_P$ el módulo complementario[3] sobre $\mathcal{O}_P$. Entonces definimos para cada $P'|P$ el exponente diferencial de P' sobre P por*

$$d(P'|P) := -v_{P'}(t).$$

[2]Para conocer esta definición ver [1] pag. 78

[3]Para conocer esta definición ver [1] pag. 91

Sabemos que $d(P'|P)$ está bien definido y $d(P'|P) \geq 0$. Mas aún $d(P'|P) = 0$ se mantiene para casi todo $P \in \mathbb{P}_F$ y $P'|P$, ya que $\mathcal{C}_P = 1 \cdot \mathcal{O}'_P$ para casi todo P. Por lo tanto podemos definir el divisor

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

Este divisor es llamado el diferente de F'/F.

Calcular directamente el diferente de una extensión de cuerpos es complicado, pero los siguientes lemas y teoremas nos ayudarán en esta tarea.

Lema 1.3. ***(Transitividad del diferente).*** *Si $F'' \supseteq F' \supseteq F$ son extensiones finitas separables, entonces tendremos*

$$d(P''|P) = e(P''|P) \cdot d(P'|P) + d(P''|P),$$

donde P'' (resp. P', P) son lugares de F'' (resp. F', F) con $P'' \supseteq P' \supseteq P$.

Teorema 1.7. ***(Teorema del diferente de Dedekind)*** *Sea $P \in \mathbb{P}_F$ y $P' \in \mathbb{P}_{F'}$ una extensión de P, entonces:*
a) $d(P'|P) \geq e(P'|P) - 1$.
b) $d(P'|P) = e(P'|P) - 1 \Leftrightarrow e(P'|P)$ no es divisible por la característica de K.

Proposición 1.4. *Sea F'/F una extensión separable de cuerpos de funciones, $P \in \mathbb{P}_F$ y $P' \in \mathbb{P}'_F$ con $P'|P$. Supongamos que $P'|P$ es totalmente ramificado; es decir, $e(P'|P) = [F' : F] = n$. Sea $t \in F'$ un parámetro uniformizante de P', y consideremos el polinimio minimal $\varphi(T) \in F[T]$ de t sobre F. Entonces $d(P'|P) = v_{P'}(\varphi'(t))$.*

Conocer Diff(F'/F) nos será de gran utilidad en el cálculo de los géneros $g(F')$ y $g(F)$, ya que ellos están relacionados por el siguiente teorema.

Teorema 1.8. ***(Fórmula del género de Hurwitz)*** *Sea F/K un cuerpo de funciones algebraico de género g y sea F'/F una extensión separable finita. Denotaremos*

K' al cuerpo de contantes de F' y g' al género de F'/K'. Entonces tenemos

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

1.3.2. Extensiones de Galois.

Las demostraciones del Lema 1.4, Teoremas 1.9 y 1.10 y Corolario 1.3 se pueden encontrar en [1], pag. 100, 121, 131 y 121 respectivamente.

Lema 1.4. *Sea F'/F una extensión algebraica de cuerpos de funciones, $P \in \mathbb{P}(F)$ y $P' \in \mathbb{P}(F')$ con $P'|P$. Si σ es un automorfismo de F'/F, entonces*
a) $\sigma(P') := \{\sigma(z) : z \in P'\}$ es un lugar de F'.
b) $v_{\sigma(P')}(y) = v_{P'}(\sigma^{-1}(y))$ para todo $y \in F'$.
c) $\sigma(P')|P$.
d) $e(\sigma(P')|P) = e(P'|P)$ y $f(\sigma(P')|P) = f(P'|P)$.

Recordemos que una extensión de cuerpos finita M/L es llamada una extensión de Galois si el grupo de automorfismos

$$Aut(M/L) = \{\sigma : M \longrightarrow M : \text{ es un isomorfismo con } \sigma(a) = a \text{ para todo } a \in L\}$$

tiene orden $[M : L]$. En tal caso llamaremos a $Aut(M/L)$, el grupo de Galois de M/L y lo denotaremos por $Gal(M/L) := Aut(M/L)$.

Definición 1.32. *Una extensión F'/K' de un cuerpo de funciones F/K es llamada de Galois si F'/F es una extensión de Galois de grado finito.*

Sea P un lugar de F/K. Entonces $Gal(F'/F)$ actúa en el conjunto de todas las extensiones $\{P' \in \mathbb{P}(F') : P'|P\}$ via $\sigma(P') = \{\sigma(x) : x \in P'\}$, y donde por el lema anterior la correspondiente valuación $v_{\sigma(P')}$ está dada por

$$v_{\sigma(P')}(y) = v_{P'}(\sigma^{-1}(y)) \text{ para todo } y \in F' \tag{1.1}$$

Teorema 1.9. *Sean F'/K' una extensión de Galois de F/K y $P_1, P_2 \in \mathbb{P}(F')$ extensiones de $P \in \mathbb{P}_F$. Entonces $P_2 = \sigma(P_1)$ para algún $\sigma \in Gal(F'/F)$. En otras palabras, el grupo de Galois actúa transitivamente en el conjunto de extensiones de P.*

Corolario 1.3. *Sean $P_1, \ldots, P_r$ todos los lugares de F' que extienden a P. Entonces tenemos:*

a) $e(P_i|P) = e(P_j|P)$ y $f(P_i|P) = f(P_j|P)$ para todo i, j. Por lo tanto podemos definir

$$e(P) := e(P_i|P) \text{ y } f(P) := f(P_i|P),$$

y llamaremos $e(P)$ (resp. $f(P)$) el índice de ramificación (resp. grado relativo) de P en F'/F.

b) $e(P) \cdot f(P) \cdot r = [F' : F]$. En particular $e(P), f(P)$ y r dividen a el grado $[F' : F]$.

c) Los exponentes diferentes $d(P_i|P)$ y $d(P_i|P)$ son los mismos para todo i, j.

d) $deg(P_i) = deg(P_j)$ para todo $i, j \in \{1, \ldots, r\}$.

e) $deg(P) = ([K' : K]/f(P))deg(P_i)$.

Definición 1.33. *Sea F'/F una extensión de Galois de cuerpos de funciones algebraicas con grupo de Galois $G = Gal(F'/F)$. Considere un lugar $P \in \mathbb{P}(F)$ y una extensión P' de P en F', entonces definimos.*

a) $G_Z(P'|P) := \{\sigma \in G : \sigma(P') = P'\}$ es llamdo el grupo de descomposición de P' sobre P.

b) $G_T(P'|P) := \{\sigma \in G : v_{P'}(\sigma z - z) > 0 \text{ para todo } z \in \mathcal{O}_{P'}\}$ es llamado el grupo de inercia de $P'|P$.

c) El cuepo fijo $Z := Z(P'|P)$ de $G_Z(P'|P)$ es llamado el cuerpo de descomposición, el cuepo fijo $T := T(P'|P)$ de $G_T(P'|P)$ es llamado el cuerpo de inercia de P' sobre P.

Claramente $G_T(P'|P) \subseteq G_Z(P'|P)$, y ambos son subgrupos de G.

Teorema 1.10. *Con la notación anterior.*

a) El grupo de descomposición $G_Z(P'|P)$ tiene orden $e(P'|P) \cdot f(P'|P)$.

b) El grupo de inercia $G_T(P'|P)$ es un subgrupo normal de $G_Z(P'|P)$ y tiene orden $e(P'|P)$.

c) Denotemos por P_Z (resp. P_T) la restricción de P' en el cuerpo de descomposición $Z = Z(P'|P)$ (resp. en el cuerpo de inercia $T = T(P'|P)$). Entonces los indices de ramificación y grados residuales de los lugares $P|P_T$, $P_T|P_Z$ y $P_Z|P$ se muestran en la siguiente figura

$$
\begin{array}{ll}
F' & P' \\
| & | \qquad e(P'|P_T) = e(P'|P) = [F' : T] \\
| & | \qquad y\ f(P'|P_T) = 1 \\
T & P_T \\
| & | \qquad f(P_T|P_Z) = f(P'|P) = [T : Z] \\
| & | \qquad y\ e(P_T|P_Z) = 1 \\
Z & P_Z \\
| & | \qquad e(P_Z|P) = f(P_Z|P) = 1 \\
| & | \\
F & P
\end{array}
$$

Proposición 1.5. *Consideremos una extensión de Galois F'/F de cuerpos de funciones algebraicas, un lugar $P \in \mathbb{P}(F)$, un lugar $P' \in \mathbb{P}(F')$ que extiende a P y un elemento $u \in \mathcal{O}_{P'}$ tal que $\mathcal{O}_{P'} = \mathcal{O}_P[u]$[4]. Entonces el exponente diferente $d(P'|P)$ es*

$$d(P'|P) = \sum_{\substack{\sigma \in G_T \\ \sigma \neq Id}} v_{P'}(\sigma(u) - u).$$

[4]Si $P'|P$ es ramificada basta tomar u como un parámetro uniformizante de P'.

1.4. Geometría Algebraica y Cuerpos de Funciones.

1.4.1. Definiciones y Propiedades Básicas.

Sea K un cuerpo cualquiera. Definimos $A^n(\overline{K})$ el n- *espacio afín sobre* $\overline{K}$ por

$$A^n(\overline{K}) := \{(a_1, \ldots, a_n) : a_i \in \overline{K}\},$$

y $\mathbb{P}^n(\overline{K})$ el n- *espacio proyectivo sobre* $\overline{K}$ por

$$P^n(\overline{K}) := \{(a_1; \ldots; a_n; 1) : a_i \in \overline{K}\} \cup H_\infty,$$

donde $(a_1; \ldots; a_n; 1)$ representa a la clase de todos los puntos $\lambda(a_1, \ldots, a_n, 1)$ con $\lambda \in K - \{0\}$, y $H_\infty = \{(a_1; \ldots; a_n; 0) : a_i \in \overline{K}\}$.

Para simplificar notación supondremos que K es un cuerpo algebraicamente cerrado, pero si ésto no ocurriese, como es el caso de $K = \mathbb{F}_p$, cambiamos K por $\overline{K}$. A continuación entregaremos algunas definiciones y proposiciones que se pueden ver en profundidad en [2] .

1. Sea $p \in A^n(K)$ (resp. en $\mathbb{P}^n(K)$) y $f \in K[x_1, \ldots, x_n]$ (resp. $f \in K[x_1, \ldots, x_{n+1}]$). Diremos que f *se anula* en p si $f(p) = 0$ (resp. si $f(a_1, \ldots, a_{n+1}) = 0$ para todo $(a_1, \ldots, a_{n+1})$ en la clase de p).

2. Para todo $S \subseteq K[x_1, \ldots, x_n]$ (resp. $S \subseteq K[x_1, \ldots, x_{n+1}]$) definimos

$$V(S) := \{p \in A^n(K) \text{ (resp. } p \in \mathbb{P}^n(K)) : \ f(p) = 0 \text{ para todo } f \in S\}.$$

3. Un conjunto $X \subseteq A^n(K)$ (resp. $X \subseteq \mathbb{P}^n(K)$) es llamado un *conjunto algebraico afín (resp. proyectivo)* si $X = V(S)$ para algún $S \subseteq K[x_1, \ldots, x_n]$ (resp. $S \subseteq K[x_1, \ldots, x_{n+1}]$). Todo conjunto algebraico afín (resp. proyectivo) propio e infinito de $A^2(K)$ (resp. de $\mathbb{P}^2(K)$) es llamado una *curva afín plana* (resp. *curva proyectiva plana*).

4. Para todo $X \subseteq A^n(K)$ (resp. $X \subseteq \mathbb{P}^n(K)$) definimos el *ideal de* X por

   $$I(X) := \{f \in K[x_1, \ldots, x_n] (\text{ resp. } f \in K[x_1, \ldots, x_{n+1}]) : f(p) = 0 \text{ para todo } p \in X\}.$$

   Si $X \subseteq \mathbb{P}^n(K)$, entonces $I(X)$ es un ideal homogéneo, es decir, contiene las partes homogéneas de todos sus elementos.

5. Un conjunto algebraico afín (resp. proyectivo) se dice *irreducible* si no es la unión de dos conjuntos algebraicos más pequeños. Todo conjunto algebraico irreducible es llamado una *variedad afín (resp. proyectiva).*

6. Existe una correspondencia uno a uno entre los conjunto algebraicos afínes de $A^n(K)$ (resp. proyectivos de $\mathbb{P}^n(K)$) y los ideales de $K[x_1, \ldots, x_n]$ (resp. los ideales homogéneos de $K[x_1, \ldots, x_{n+1}]$) dada por

   $$\left\{ \begin{array}{c} \text{Ideales rad.} \\ \text{(resp. Ideales rad. homogéneos)} \end{array} \right\} \begin{array}{c} \xrightarrow{V} \\ \xleftarrow{I} \end{array} \left\{ \begin{array}{c} \text{Conjuntos alg. afines} \\ \text{(resp. Conj. alg. proyectivos)} \end{array} \right\}$$

   Esto induce una correspondencia uno a uno entre variedades afínes (resp. proyectivas) e ideales primos (resp. ideales primos homogéneos: generados por una forma irreducible), como también entre puntos e ideales maximales.

7. Si V es una variedad afín (resp. proyectiva), entonces $I(V)$ es un ideal primo (resp. ideal primo homogéneo). Luego $\Gamma(V) := K[x_1, \ldots, x_n]/I(V)$ (resp. $\Gamma_h(V) := K[x_1, \ldots, x_{n+1}]/I(V)$) es un dominio, llamado *anillo de coordenadas (resp. homogéneo)* de V.

8. Sea $K(V)$ (resp. $K_h(V)$) el cuerpo cuociente de $\Gamma(V)$ (resp. $\Gamma_h(V)$); este es llamado el *cuerpo de funciones (resp. homogéneas) de* V.

9. Sea V es una variedad algebraica proyectiva. Definimos el *cuerpo de funciones de* V, que denotaremos por $K(V)$, por

   $$K(V) := \{w \in K_h(V) : \exists g, h \in \Gamma_h(V) \text{ formas del mismo grado con } w = g/h\}.$$

10. Si $V = V(f)$ una variedad afín, entonces llamaremos a $V^* = V(f^*)$ su *clausura proyectiva*, donde f^* denotará al homogeneizado de f. Además, si $f \in \Gamma_h(V^*)$ es una forma de grado d, es decir, $f = F + I(V^*)$ donde $F \in K[x_1, \cdots, x_{n+1}]$ es una forma de grado d, definimos $f_* := F_* + I(V)$ (esta definición es independiente de la elección de F).

    Con las anteriores definiciones es fácil comprobar que el siguientes homomorfismos es biyectivo

$$\begin{array}{rccc} \alpha : & K(V^*) & \longrightarrow & K(V) \\ & \dfrac{f}{g} & \mapsto & \dfrac{f_*}{g_*} \end{array}$$

    donde f, g son formas del mismo grado en $\Gamma_h(V^*)$.

1.4.2. Correspondencia entre Cuerpos de Funciones y Curvas Planas.

Sea K un cuerpo cualquiera y $\mathcal{X} \subsetneq A^2(\overline{K})$ una curva afín, es decir, existe $f \in K[x, y]$ un polinimio irreducible, tal que

$$\mathcal{X} = V(f).$$

Luego $\mathcal{X}^* \subseteq \mathbb{P}^2(\overline{K})$, la clausura proyectiva de $\mathcal{X}$, estará dada por $\mathcal{X}^* = V(f^*)$.
No es difícil verificar que f es irreducible como polinomio en $K(x)[y]$, por lo tanto

$$K(\mathcal{X}) := Quot\left(\frac{K[x,y]}{(f)}\right) = \frac{K(x)[y]}{(f)},$$

es decir, se comprueba que $K(\mathcal{X})/K$ efectivamente es un cuerpo de funciones en el sentido de la Definición 1.10.
Además, por el punto (10) de la sección anterior sabemos que $K(\mathcal{X}) \cong K(\mathcal{X}^*)$, es decir, $K(\mathcal{X}^*)/K$ también es un cuerpo de funciones.
Otra consecuencia del punto (10) es que si $(a; b; 1) \in \mathcal{X}^*$, entonces $(a, b) \in \mathcal{X}$. Luego

α induce un isomorfismo entre los anillos de valuación

$$\mathcal{O}_{p_{(a;b;1)}} := \{w \in K(\mathcal{X}^*) : \ w \text{ está bien definido en } (a;b;1)\} \subseteq K(\mathcal{X}^*)$$

y

$$\mathcal{O}_{p_{(a,b)}} := \{w \in K(\mathcal{X}) : \ w \text{ está bien definido en } (a,b)\} \subseteq K(\mathcal{X}).$$

Además, si $(c;d;0) \in \mathcal{X}^*$ entonces los siguientes anillos de valuación también son isomorfos

$$\mathcal{O}_{p_{(c;d;0)}} := \{w \in K(\mathcal{X}^*) : \ w \text{ está bien definido en } (c;d;0)\} \subseteq K(\mathcal{X}^*).$$

y

$$\mathcal{O}_{p_\infty} := \{w \in K(\mathcal{X}) : \ w^* \text{ está bien definido en } (c;d;0)\} \subseteq K(\mathcal{X}),$$

donde si $w = \frac{g}{h} \in K(\mathcal{X})$, entonces $w^* := \frac{g^*}{h^*} \cdot z^{gr(h)-gr(g)}$.

Esta correspondencia 1 a 1 entre los anillos de valuación de $K(\mathcal{X}^*)$ y $K(\mathcal{X})$, nos induce una correspodencia 1 a 1 entre sus respectivos lugares. De esta forma podremos simplificar nuestro trabajo y trabajar sólo con curvas afines $\mathcal{X}$ y sus correspondentes cuerpos de funciones $K(\mathcal{X})$.
A continuación entregaremos algunas definiciones importantes acerca de curvas planas, que serán útiles en el capítulo 3.

Definición 1.34. *Diremos que $(a,b) \in \mathcal{X}$ (resp. $(a;b;c) \in \mathcal{X}^*$)) es un punto racional de $\mathcal{X}$ (resp. $\mathcal{X}^*$) si $a,b \in K$ (resp. si $a,b,c \in K$ para algún representante de la clase $(a;b;c)$).*

Definición 1.35. *La curva $\mathcal{X} = V(f)$ (resp. $\mathcal{X}^* = V(f^*)$), se dirá singular si contiene puntos p (resp. p^*) tales que[5] $\partial_x(f)(p) = 0 = \partial_y(f)(p))$ (resp. además $\partial_z(f)(p^*) \neq 0$). En el caso contrario se dirá no singular.*

[5] Donde $\partial_x(f)$, $\partial_y(f)$ y $\partial_z(f)$ denotan las derivadas parciales formales del polinomio $f(x,y,z)$.

Capítulo 2

Cuerpos de funciones y códigos.

En este capítulo aprenderemos cómo, a partir de un cuerpo de funciones algebraicas de una variable, podemos generar un tipo muy especial de códigos, los llamados Geométrico-Algebraicos o códigos Goppa, para los cuales existe una cota inferior bastante buena para $\delta + R$. También estableceremos un tipo de códigos Goppa, en los cuales se basará nuestro trabajo, pues para ellos conocemos más información.

2.1. Condiciones para poder generar códigos Goppa.

Consideraremos $K = \mathbb{F}_q$ y $F = K(x)(y)$ un cuerpo de funciones sobre K, donde y es un elemento algebraico sobre $K(x)$. Para este tipo de cuerpos podemos decir que

$$F = Quot(K[x, y]/J),$$

donde J es el ideal primo de $K[x, y]$ generado por $f(y)$ (el polinimio minimal de y). Sea $\mathcal{X}_F := V(J)$ la curva afín definida por J. Por Sección 1.4.2 sabemos que

$$F = K(\mathcal{X}_F)$$

Luego por el punto (6) de la Sección 1.4.1, existe una correspondencia 1 a 1 entre los lugares de F y los elementos de la curva $\mathcal{X}_F$, dada por el isomorfismo.

$$\begin{aligned} \phi : \mathcal{X}_F &\Longrightarrow \mathbb{P}(F) \\ p &\rightarrow P, \end{aligned}$$

donde $P := I(\{p\})$.

Observación 2.1. El isomorfismo anterior está bien definido puesto que si $p \in \mathcal{X}_F$, entonces $J \subseteq I(\{p\})$.

Dada esta correspondencia, nos será útil la siguiente notación: Si "P" es un lugar de $\mathbb{P}(F)$, denotaremos por "p" al correspondiente punto en la curva $\mathcal{X}_F$. Inversamente si "m" es un punto de $\mathcal{X}_F$, denotaremos por "M" al correspondiente lugar en $\mathbb{P}(F)$".

2.2. Construcción de un código Goppa.

Siguiendo con la notación de la sección anterior. Sean $p_1, p_2, \ldots, p_n$, puntos racionales distintos de $\mathcal{X}_F$ y sea $G \in Div(F)$ tal que $v_{P_i}(G) = 0$ para todo $i = 1, 2, \ldots, n$. Luego

$$\begin{aligned} e : \mathcal{L}(G) &\longrightarrow K^n \\ f &\rightarrow (f(p_1), \ldots, f(p_n)) \end{aligned}$$

es una función $\mathbb{F}_q$- lineal y por lo tanto $e(\mathcal{L}(G))$ es un subespacio vectorial de K^n. Denotaremos $D := P_1 + \cdots + P_n$.

Definición 2.1. *La imagen de $\mathcal{L}(G)$ bajo la anterior función, es el denominado código Geométrico-Algebraico o Goppa asociado con D y G que denotaremos por $C_{D,G}$.*

La demostración del siguiente lema y la posterior proposición se puede encontrar en [4], pag. 13 y 14.

Lema 2.1. *Sea $k := dim(C_{D,G})$ y d la distancia mínima del código $C_{D,G}$. Entonces*
1) $k = l(G) - l(G - D)$;
2) $d \geq n - deg(G)$.

Proposición 2.1. *Sea $C_{D,G}$ un código Goppa con parámetros k y d como arriba y sea g el género de F.*
1) Si $n > deg(G)$, entonces $k = l(G)$. En particular, $k \geq deg(G) + 1 - g$ y también $d + k \geq n + 1 - g$. Mas aún, una matriz generedora de $C_{D,G}$ está dada por

$$M := \begin{pmatrix} f_1(p_1) & \dots & f_1(p_n) \\ \vdots & & \vdots \\ f_k(p_1) & \dots & f_k(p_n) \end{pmatrix}$$

donde $f_1, \dots, f_k$ son una base de $L(G)$.
2) Si $n > deg(G) > 2g - 2$, entonces $k = deg(G) + 1 - g$.

Definición 2.2. *Llamaremos códigos Goppa de un punto a aquellos códigos $C_{D,G}$ donde G es un divisor de un punto, es decir, $G = \gamma P$, $\gamma \geq 0$ y P es un lugar racional de F.*
Recordemos que en este caso $\mathcal{L}(G) = \{f \in F : v_P(f) \geq -\gamma\}$.

2.3. Un tipo de Códigos Goppa interesantes.

Si queremos generar código Goppa asociado con D y G, a partir de un cuerpo de funciones F, nos encontramos con algunas dificultades, como por ejemplo:

1. En general calcular $l(G)$ no es fácil

2. Tampoco es fácil encontrar generadores de $\mathcal{L}(G)$.

3. La dimensión k del código depende de $l(G)$ y de $l(G-D)$.

Pero hay ciertas proposiciones que nos ayudarán a solucionar estos problemas.

1. El Corolario de Riemann-Roch (1.2) nos dice como calcular $l(G)$ si $deg(G) \geq 2g-1$.

2. La Observación 1.6 nos dice como son los elementos lineamente independientes (una posible base) en $L(G)$ si $G = mP$, P es un lugar $K-$ racional y $m > 0$.

3. La Proposición 2.1 nos dice que si $n > deg(G)$ entonces $k = l(G)$.

Por lo tanto algunas condiciones que impondremos a los códigos Goppa $C_{D,G}$ que trataremos en nuestro trabajo serán:

a) $G = mP$, donde P es un lugar racional de F y $m > 0$.

b) $n > deg(G) > 2g-2$.

Observación 2.2. Bajo las condiciones anteriores, usando Lema 2.1 y Proposición 2.1, tendremos que los parámetros de los código $C_{D,G}$ cumplirán:

$$d \geq n - deg(G) \qquad k = deg(G) + 1 - g, \tag{2.1}$$

Uniendo estas ecuaciones tendremos

$$n + 1 - g \leq d + k. \tag{2.2}$$

Por otro lado, sabemos que todo código cumple la Cota de Singleton (1.1), luego

$$n + 1 - g \leq d + k \leq n + 1. \tag{2.3}$$

Observación 2.3. La Observación 2.2 nos entregó una condición muy importante que cumplen los parámetros de los códigos que trataremos en nuestro trabajo, pero aún podemos obtener más información.

Por ejemplo, si dividimos la inecuación 2.3 por n tendremos

$$1+\frac{1}{n}-\frac{g}{n} \leq \delta + R \leq 1+\frac{1}{n}. \tag{2.4}$$

Lo que nos dice, que a menor cuociente "g/n", mayor será la suma de los parámetros asintóticos (1.8) ($\delta + R$). Una forma de disminuir este cuociente es aumentar n, es decir, considerar más lugares racionales al momento de generar el código. De esta manera dejaremos sólo un lugar racional para definir G y el resto para definir D, en otras palabras, $n = \#\mathcal{N}(F) - 1$.

En donde $\mathcal{N}(F)$ representa al conjunto de todos los lugares racionales de F. Recordemos que dado un género g el mayor número de puntos racionales lo obtendremos considerenado el cuerpo de funciones maximales de tal género (siempre que exista), es por esto que nos enfocaremos en el cuerpo Hermitiano y algunos subcuerpos, cuerpos de funciones maximales que conoceremos en los siguientes capítulos.

En resumen, los *códigos Goppa* $C_{D,G}$ *que trataremos en nuestro trabajo serán códigos con las siguientes condiciones*:

a) $G = mP$, donde P es un lugar racional de F y $m > 0$.

b) $n > deg(G) > 2g - 2$.

c) $n = \#\mathcal{N}(F) - 1$,

Además, consideraremos F como el cuerpo de funciones Hermitianas y algunos subcuerpos de este, elegidos por su gran cantidad de lugares racionales. Bajo estas condiciones analizaremos los correspondientes cuocientes "g/n" para encontrar en que casos se obtienen los menores cuocientes.

Capítulo 3

El Cuerpo de Funciones Hermitianas ($\mathcal{H}$).

En el capítulo anterior vimos la importancia de que un cuerpo de funciones tenga la mayor cantidad de lugares racionales posibles. Una cota superior para la cantidad de números racionales fue introducida por Hesse y Weil ($\sim$ 40'), y mejorada por Serre (83'), la cual nos dice que si $F/\mathbb{F}_{q^r}$ es un un cuerpo de funciones de gérero $g(F)$, entonces la cantidad de números racionales ($\mathcal{N}(F)$) esta acotado por[1]

$$|\#\mathcal{N}(F) - (q^r + 1)| \leq g(F)\lfloor 2\sqrt{q^r} \rfloor \tag{3.1}$$

Los cuerpos que alcanzan esta cota son llamados *cuerpos maximales.*
A continuación les presentaremos el cuerpo de funciones *Hermitianas* o simplemente cuerpo *Hermitiano*, un cuerpo maximal que será el cuerpo base de nuestro trabajo.

3.1. Propiedades.

Sea $K = \mathbb{F}_{q^2}$ el cuerpo finito de q^2 elementos, donde $q = p^l$ y p es un número primo.

[1]Para conocer más acerca de esta cota ver [5] pag. 6

Definición 3.1. *Llamaremos cuerpo de funciones Hermitianas al cuerpo de funciones algebraicas $\mathcal{H}/K$, donde $K := \mathbb{F}_{q^2}$ y $\mathcal{H} := Quot\left(K[x,y]/(y^q + y - x^{q+1})\right)$.*

Observación 3.1. *El cuerpo Hermitiano $\mathcal{H}$ corresponde al cuerpo de funciones $K(\mathcal{X}_{\mathcal{H}})$ asociado a la curva $\mathcal{X}_{\mathcal{H}} = V(y^q + y - x^{q+1})$. Este a su vez es isomorfo al cuerpo de funciones $K(\mathcal{X}^*_{\mathcal{H}})$, donde $\mathcal{X}^*_{\mathcal{H}} = V(zy^q + z^q y - x^{q+1})$ (ver Def. 1.4.1).*

A continuación entregaremos una serie de propiedades que nos ayudarán a demostrar que efectivamente $\mathcal{H}$ es un cuerpo maximal.

Proposición 3.1. *El Cuerpo de Funciones Hermitianas tiene género $g(\mathcal{H}) = q(q-1)/2$.*

Demostración: Usando $\mu = 1$, $f(x) = x^{q+1}$ y $m := deg(f)$ en Proposición 6.4.1 (pág. 232) en [1] obtenemos $g = (q-1)(m-1)/2 = q(q-1)/2$. □

Proposición 3.2. *Si $(\alpha,\beta) \in \mathcal{X}_{\mathcal{H}}$, entonces los siguientes conjuntos son anillos de valuación (1.11) de $\mathcal{H}$.*

$$\begin{aligned} \mathcal{O}_{P'_{\alpha,\beta}} &:= \{(f/g) \in \mathcal{H} : (f/g)(\alpha,\beta) \text{ está bien definido}\} \\ \mathcal{O}_{P'_{\infty}} &:= \{(f/g) \in \mathcal{H} : (f/g)^*(0;1;0) \text{ está bien definido}\}, \end{aligned}$$

Demostración: ver Sección 1.4.2. □

Proposición 3.3. *Los ideales principales (1.12) de $\mathcal{O}_{P'_{\alpha,\beta}}$ y $\mathcal{O}_{P'_{\infty}}$ respectivamente son:*

$$\begin{aligned} P'_{\alpha,\beta} &:= \{(f/g) \in \mathcal{O}_{P'_{\alpha,\beta}} : (f/g)(\alpha,\beta) = 0\} \\ P'_{\infty} &:= \{(f/g) \in \mathcal{O}_{P'_{\infty}} : (f/g)^*(0,1,0) = 0\}, \end{aligned}$$

Proposición 3.4. *Si $\alpha,\beta \in \mathbb{F}_{q^2}$, entonces existen q^3 lugares distintos del tipos $P'_{\alpha,\beta}$.*

Demostración: Es fácil verificar que $\alpha^{q+1} \in \mathbb{F}_q$ para todo $\alpha \in \mathbb{F}_{q^2}$. Con esto tendremos que el polinomio $h(t) = t^q + t - \alpha^{q+1} \in \mathbb{F}_q$ tiene todas sus raices en $\mathbb{F}_{q^2}$, ya que si β es una raiz de h entonces

$$\beta^{q^2} = (\alpha^{q+1} - \beta)^q = (\alpha^{q+1})^q - \beta^q = \alpha^{q+1} - \beta^q = \beta.$$

Además, dado que la derivada formal $h'(t) = 1$, todas las raices de h son distintas. En conlución, para cada $\alpha \in \mathbb{F}_{q^2}$ existen q distintos $\beta \in \mathbb{F}_{q^2}$ que cumplen con $\beta^q + \beta = \alpha^{q+1}$, es decir, hay q^3 pares (α, β) distintos que cumplen con esta ecuación. También es fácil verificar que por cada par distinto (α, β), los anillos de valuación $\mathcal{O}_{P'_{\alpha,\beta}}$ son distintos. Así, concluimos que existen q^3 anillos de valorarión distintos $\mathcal{O}_{P'_{\alpha,\beta}}$ y por lo tanto q^3 lugares distintos $P'_{\alpha,\beta}$, cuando $\alpha, \beta \in \mathbb{F}_{q^2}$. □

Proposición 3.5. *Todos los lugares del tipo $P'_{\alpha,\beta}$, con $\alpha, \beta \in \mathbb{F}_{q^2}$, más el lugar P'_∞ son lugares racionales.*

Demostración: Consideremos el homomorfismo epiyectivo,

$$\begin{aligned} \varphi : \mathcal{O}_{P'_{\alpha,\beta}} &\longrightarrow K \\ (f/g) &\rightarrow (f/g)(\alpha, \beta) \end{aligned}$$

y notemos que $Ker(\varphi) = P'_{\alpha,\beta}$. De aquí podemos concluir que :

$$\mathcal{H}_{P'_{\alpha,\beta}} := \mathcal{O}_{P'_{\alpha,\beta}}/P'_{\alpha,\beta} \approx K,$$

por lo tanto $deg(P'_{\alpha,\beta}) = [\mathcal{H}_{P'_{\alpha,\beta}} : K] = 1$. La misma idea demuestra que $deg(P_\infty) = 1$. □

Observación 3.2. *Con la propiedad anterior podemos concluir que $\mathcal{H}$ tiene por lo menos $q^3 + 1$ lugares racionales. Pero además la desigualdad (3.1) nos dice que:*

$$|\#\mathcal{N}(\mathcal{H}) - (q^2 + 1)| \leq g(\mathcal{H})\lfloor 2\sqrt{q^2} \rfloor = q^3 - q^2 \Rightarrow \#\mathcal{N}(\mathcal{H}) = q^3 + 1.$$

Así, $\mathcal{H}$ tiene exactamente $q^3 + 1$ lugares racionales y por lo tanto $\mathcal{H}$ es un cuerpo maximal.

Algunas propiedades importantes acerca de $\mathcal{H}/\mathbb{F}_{q^2}$ son presentadas a continuación[2]

(i) El cuerpo de funciones Hermitiano es el único cuerpo de funciones maximal de género $g = q(q-1)/2$.

(ii) Todo subcuerpo $E \subsetneq F$ de un cuerpo de funciones maximal F/K (con $K \subsetneq E$) es maximal. Así, los subcuerpos del cuerpo de funciones Hermitiana $\mathcal{H}$ nos dan ejemplos de cuerpos de funciones maximales sobre K.

(iii) Ningún cuerpo de funciones sobre K de género $g > q(q-1)/2$ es maximal.

3.2. Los Lugares racionales de $K(x)$.

En esta sección conoceremos un poco más acerca de los lugares racionales de $K(x)$. Todo esto para ver a $\mathcal{H}$ como una extensión (de cuerpos de funciones) de $K(x)$ y luego conocer un poco más acerca de las propiedades de $\mathcal{H}$.
Para comenzar notemos que

$$K(x) = Quot(K[x,y]/I),$$

donde $I \subseteq K[x,y]$ es el ideal generado por $f(x,y) = y$.

Observación 3.3. El cuerpo $K(x)$ corresponde al cuerpo de funciones $K(\mathcal{X}_{K(x)})$ asociado a la curva $\mathcal{X}_{K(x)} = V_{\overline{K}}(f) = \overline{K} \times \{0\}$, definida sobre la clausura algebraica de K.

Proposición 3.6. *Si $\alpha \in \overline{K}$, es fácil de verificar que los siguientes conjuntos son*

[2] Para mayor información ver [3], pag. 138.

anillos de valuación de $K(x)$.

$$\mathcal{O}_{Q_\alpha} := \left\{ \frac{f(x)}{g(x)} \in K(x) \,:\, g(\alpha) \neq 0 \right\}$$
$$\mathcal{O}_{Q_\infty} := \left\{ \frac{f(x)}{g(x)} \in K(x) \,:\, \partial(f) \leq \partial(g) \right\}.$$

Cuyos lugares son respectivamente

$$Q_\alpha := \left\{ \frac{f(x)}{g(x)} \in \mathcal{O}_{Q_\alpha} \,:\, f(\alpha) = 0 \right\}$$
$$Q_\infty := \left\{ \frac{f(x)}{g(x)} \in \mathcal{O}_{Q_\infty} \,:\, \partial(f) < \partial(g) \right\}$$

Observación 3.4. Es inmediato verificar que para cada $w \in Q_\infty$ existen $f, g \in K(x)$ tales que

$$w = \left(\frac{1}{x}\right)^i \frac{f}{g},$$

donde $i \in \mathbb{N}$ y $gr(f) = gr(g)$, es decir, que $(1/x)$ es un parámetro uniformizante de Q_∞.

Análogamente si $\alpha \in K$ y $w \in Q_\alpha$ existen $f, g \in K(x)$ tales que

$$w = (x - \alpha)^i \frac{f}{g},$$

donde $i \in \mathbb{N}$ y $f(\alpha) \neq 0$, es decir, $(x - \alpha)$ es un parámetro uniformizante de Q_α.

Observación 3.5. *El cuerpo* $K(x)$ *tiene género* $g(K(x)) = 0$. *Esto se obtiene considerando el lugar infinito de* $K(x)$, *los elementos linealmente independientes* $1, x, x^2, \ldots, x^r$ *de* $\mathcal{L}(rP_\infty)$ *y el corolario de Riemann-Roch, que para un* r *suficientemente grande nos dice:*

$$r + 1 \leq l(rP_\infty) = deg(rP'_\infty) + 1 - g = r + 1 - g.$$

Así $g \leq 0$, *pero sabemos que para todo cuerpo de funciones* $g \geq 0$, *con lo cual obtenemos* $g = 0$.

Proposición 3.7. *Si* $\alpha \in K$, *entonces todos los lugares del tipo* Q_α *más el lugar* Q_∞ *son lugares racionales de* $K(x)$.

Demostración: Usando la misma idea que usamos para demostrar que los lugares $P'_{\alpha,\beta}$ eran lugares racionales, se demuestra que los grados de Q_α y Q_∞ son 1. □

Observación 3.6. *Con la propiedad anterior podemos concluir que $K(x)$ tiene por lo menos q^2+1 lugares racionales, pero además la desigualdad (3.1) nos dice que:*

$$|\#\mathcal{N}(K(x)) - (q^2+1)| \leq g(K(x))\lfloor 2\sqrt{q^2}\rfloor = 0 \Rightarrow \#\mathcal{N}(K(x)) = q^2+1.$$

Así, $K(x)$ tiene exactamente q^2+1 lugares racionales y por lo tanto $K(x)$ es también un cuerpo maximal.

3.3. $\mathcal{H}$, una extensión de $K(x)$.

Sabemos que $\mathcal{H}$ es una extensión de $K(x)$ al ser $\mathcal{H}/K$ un cuerpo de funciones. Pero no es obvio que los lugares P'_∞ y $P'_{\alpha,\beta}$ de $\mathcal{H}$ sean respectivamente extensiones de los lugares de Q_∞ y Q_α de $K(x)$. En esta sección nos encargaremos de demostrar esta afirmación y de ella derivaran algunas propiedades importantes acerca de los lugares de $\mathcal{H}$.

Lema 3.1. *El lugar P'_∞ de $\mathcal{H}$ es una extensión del lugar Q_∞ en $K(x)$.*

Demostración: Sea $w \in Q_\infty$, sabemos por Observación 3.4 que existen $f, g \in K(x)$ tales que

$$w = \left(\frac{1}{x}\right)^i \frac{f}{g},$$

donde $i \in \mathbb{N}$ y $gr(f) = gr(g)$. Luego

$$w^* = \left(\frac{z}{x}\right)^i \frac{f^*}{g^*},$$

donde si $f/g = (a_n x^n + \cdots + a_0)/(b_n x^n + \cdots + b_0)$, entonces

$$\frac{f^*}{g^*} = \frac{a_n + a_{n-1}(z/x) + \cdots + a_0(z/x)^n}{b_n + b_{n-1}(z/x) + \cdots + b_0(z/x)^n}.$$

Finalmente usando que $z/x = x^q/(y^q + z^{q-1}y)$, tendremos que $(z/x)(0;1;0) = 0$ y por lo tanto también $w^*(0;1;0) = 0$, es decir $w \in P_\infty$. □

Lema 3.2. *Los lugares $P'_{\alpha,\beta}$ de $\mathcal{H}$ son extensiones de los lugares Q_α en $K(x)$.*

Demostración: Si $w \in Q_\alpha$, en particular $w \in \mathcal{H}$ y obviamente $w(\alpha,\beta) = 0$. Luego $w \in P'_{\alpha,\beta}$. □

Lema 3.3. *$(x/y) \in \mathcal{H}$ es un parámetro uniformizante de P'_∞, es decir,*

$$P'_\infty = \left\langle \frac{x}{y} \right\rangle \text{ en } \mathcal{O}_{P'_\infty}.$$

Demostración: Partiremos notando de $1/y \in P'_\infty$ y por lo tanto $v_{P'_\infty}(y) < 0$. Usaremos esto más el hecho que $y^q + y = x^{q+1}$ en la siguiente ecuación.

$$\begin{aligned} v_{P'_\infty}(x^{q+1}) &= v_{P'_\infty}(y^q + y) \\ (q+1)v_{P'_\infty}(x) &= min\{v_{P'_\infty}(y^q), v_{P'_\infty}(y)\} \\ (q+1)v_{P'_\infty}(x) &= min\{qv_{P'_\infty}(y), v_{P'_\infty}(y)\} \\ (q+1)v_{P'_\infty}(x) &= qv_{P'_\infty}(y) \end{aligned}$$

De la cual concluimos que $v_{P'_\infty}(y) = v_{P'_\infty}(x) + (1/q)v_{P'_\infty}(x)$.
Por otro lado, dado que P'_∞ es una extensión de Q_∞ y $(1/x)$ es uniformizante de Q_∞, tendremos

$$v_{P'_\infty}(x) = e(P'_\infty|Q_\infty)v_{Q_\infty}(x) = -e(P'_\infty|Q_\infty).$$

En conclusión,

$$v_{P'_\infty}(x/y) = v_{P'_\infty}(x) - v_{P'_\infty}(y) = -(1/q)v_{P'_\infty}(x) = e(P'_\infty|Q_\infty)/q = 1,$$

ya que por igualdad fundamental (1.6) $e(P'_\infty|Q_\infty) \leq q$ y la valuación es un entero. □
Una consecuencia inmediata del lema anterior es que $e(P'_\infty|Q_\infty) = q$, lo que nos da paso los siguientes corolarios.

Corolario 3.1. *Las valoraciones de $x, y \in \mathcal{H}$ con respecto a P'_∞ son respectivamente,*

$$v_{P'_\infty}(x) = -q \quad y \quad v_{P'_\infty}(y) = -(q+1)$$

Corolario 3.2. *El lugar Q_∞ está totalmente ramificado en $\mathcal{H}$ y P'_∞ es el único lugar de $\mathcal{H}$ extiende a Q_∞.*

Lema 3.4. *Si $\alpha, \beta \in \mathbb{F}_{q^2}$, entonces $(x - \alpha z)/z \in \mathcal{H}$ es un parámetro uniformizante de $P'_{\alpha,\beta}$, es decir,*

$$P'_{\alpha,\beta} = \left\langle \frac{x - \alpha z}{z} \right\rangle \text{ en } \mathcal{O}_{P'_{\alpha,\beta}}.$$

Demostración: En la página 7 de [4] podemos encontrar la Proposición 3.7 que nos dice: "Sea $p = (a; b; c)$ un punto en la curva $\mathcal{X}$ definida por $f(x, y, z)$. Asumamos $c \neq 0$, sea $t = L_1(x, y, z)/L_2(x, y, z)$ una función en M_p tal que $gr(L_1) = gr(L_2) = 1$, $L_2(p) \neq 0$ y L_1 no es un múltiplo (constante) de $\partial_x f(p)x + \partial_y f(p)y + \partial_z f(p)z$. Entonces t es un parámetro uniformizante de P."

En nuestro caso $p = (\alpha; \beta; 1)$ y $\partial_x f(p)x + \partial_y f(p)y + \partial_x f(p)z = -\alpha x + y + \beta z$. Por lo tanto $t = (x - \alpha z)/z$ es un parámetro uniformizante de $P'_{\alpha,\beta}$. □

Proposición 3.8. *Los lugares Q_α se descomponen completamente en $\mathcal{H}$. Además para cada $\alpha \in K$, los q lugares distintos $P'_{\alpha,\beta} \in \mathbb{P}(\mathcal{H})$ son los únicos lugares de $\mathcal{H}$ que extienden a $Q_\alpha \in \mathbb{P}(K(x))$.*

Demostración: Por Proposición 3.4 sabemos que si $\alpha \in K$, entonces existen $\beta_1, \beta_2, \ldots, \beta_q$ elementos distintos en $\mathbb{F}_{q^2}$ tales que $\beta_i^q + \beta_i = \alpha^{q+1}$, es decir, $(\alpha, \beta_i) \in \mathcal{X}_\mathcal{H}$. Además sabemos por Lema 3.2 que los q lugares P'_{α,β_i} de $\mathcal{H}$ extienden al lugar Q_α de $K(x)$.

Finalmente, por la Igualdad Fundamental (1.6) sabemos que se debe cumplir

$$[\mathcal{H} : K(x)] = q = \sum_{Q|Q_\alpha} e(Q|Q_\alpha) f(Q|Q_\alpha) \geq \sum_{i=1}^{q} e(P'_{\alpha,\beta_i}|Q_\alpha),$$

por lo tanto $e(P'_{\alpha,\beta_i}|Q_\alpha) = 1$ para todo $1 \leq i \leq q$ y $P_{\alpha,\beta_1}, P_{\alpha,\beta_2}, \ldots, P_{\alpha,\beta_q}$ son los únicos lugares de $\mathcal{H}$ que extienden a Q_α. □

3.4. Automorfismos de $\mathcal{H}$.

Al final de la sección 3.1 vimos que al ser $\mathcal{H}/K$ un cuerpo de funciones maximal, los subcuerpos de $\mathcal{H}$ nos entregan ejemplos de cuerpos maximales. Sabemos que los subcuerpos de $\mathcal{H}$ son cuerpos fijos bajo algún subgrupo del grupo de automorfimo de $\mathcal{H}$. Por lo tanto debemos describir en más detalles este grupo.

$$\mathcal{A} = Aut(\mathcal{H}) := \{\sigma : \mathcal{H} \to \mathcal{H} \ / \ \sigma \text{ es un automorfismo y } \sigma|_K = id_K\}$$

El grupo de automorfismos de $\mathcal{H}$ es extremadamente grande, de hecho tiene orden $q^3(q^2-1)(q^3-1)$. Por lo que para estudiarlo en profundidad definiremos algunos de sus subgrupos.

Definición 3.2. *Llamaremos $\mathcal{A}(P'_\infty)$ al subgrupo de $\mathcal{A}$ definido por:*

$$\mathcal{A}(P'_\infty) := \{\sigma \in \mathcal{A} \ / \ \sigma(P'_\infty) = P'_\infty\}$$

que consiste en todos los automorfismos σ con: $\sigma(x) = ax+b$, $\sigma(y) = a^{q+1}y+ab^qx+c$, donde $a \in K^*$, $b \in K$ y $c^q + c = b^{q+1}$, es decir, $(b,c) \in \mathcal{X}_\mathcal{H}$.

Lema 3.5. *El orden de $\mathcal{A}(P'_\infty)$ es $q^3(q^2-1)$.*

Definición 3.3. *Llamaremos $\mathcal{A}_1(P'_\infty)$ al subgrupo de $\mathcal{A}$ definido por:*

$$\mathcal{A}_1(P'_\infty) = \{\sigma \in \mathcal{A}(P'_\infty) \ / \ \sigma(x) = x + b \ \ \textit{algún } b \in K\} \subseteq \mathcal{A}(P'_\infty)$$

Lema 3.6. *El orden de $\mathcal{A}_1(P'_\infty)$ es q^3.*

El grupo cuociente $\mathcal{A}(P'_\infty)/\mathcal{A}_1(P'_\infty)$ es cíclico de orden q^2-1; este es generado por el automorfismo $\varepsilon \in \mathcal{A}(P'_\infty)$ con

$$\varepsilon(x) = ax \qquad \varepsilon(y) = a^{q+1}y,$$

donde $a \in K^*$.

Otro automorfismo $\omega \in \mathcal{A}$ está dado por

$$\omega(x) = \frac{x}{y} \qquad \omega(y) = \frac{1}{y},$$

este elemento ω es una involución (e.d, ord(ω)=2).

Observación 3.7. Si denotamos por $\mathcal{H}^{\mathcal{G}}$ al *cuerpo fijo* de $\mathcal{H}$ bajo la acción del subgrupo $\mathcal{G}$, es decir,

$$\mathcal{H}^{\mathcal{G}} := \{z \in \mathcal{H} \,/\, \sigma(z) = z \quad \forall \sigma \in \mathcal{G}\}.$$

entonces se cumplirá que $\mathcal{H}/\mathcal{H}^{\mathcal{G}}$ es una extensión de Galois de grado $[\mathcal{H} : \mathcal{H}^{\mathcal{G}}] = \text{ord}(\mathcal{G})$ y $\mathcal{G}$ es el grupo de Galois de $\mathcal{H}/\mathcal{H}^{\mathcal{G}}$.

Capítulo 4

Posibles géneros de $\mathcal{H}^{\mathcal{G}}$

Para llegar a generar códigos $C_{D,G}$ del tipo especificado en la Sección 2.3, a partir de cuerpos fijos $\mathcal{H}^{\mathcal{G}}$, es de vital importancia conocer el género $g(\mathcal{H}^{\mathcal{G}})$. Pero este cálculo es bastante difícil en general, es por esto que en este capítulo sólo nos encargaremos de encontrar los posibles géneros de $\mathcal{H}^{\mathcal{G}}$ cuando $\mathcal{G}$ es un subgrupo de $\mathcal{A}_1(P'_\infty)$.

4.1. Idea Principal

Para calcular $g(\mathcal{H}^{\mathcal{G}})$, recurrimos a la fórmula del género de Hurwitz (Teorema 1.8), que para nuestro caso quedaría

$$2g(\mathcal{H}) - 2 = \frac{[\mathcal{H} : \mathcal{H}^{\mathcal{G}}]}{[K : K]}(2g(\mathcal{H}^{\mathcal{G}}) - 2) + deg\ \text{Diff}(\mathcal{H}/\mathcal{H}^{\mathcal{G}}).$$

Por la Observación 3.7 sabemos que $\mathcal{H}/\mathcal{H}^{\mathcal{G}}$ es una extensión de Galois con

$$[\mathcal{H} : \mathcal{H}^{\mathcal{G}}] = ord(\mathcal{G}) = q \quad \text{y} \quad Gal(\mathcal{H}/\mathcal{H}^{\mathcal{G}}) = \mathcal{G}.$$

Luego para tener $g(\mathcal{H}^{\mathcal{G}})$ nos faltaría conocer el grado del divisor $\text{Diff}(\mathcal{H}/\mathcal{H}^{\mathcal{G}})$, pero conocer tal grado no es para nada trivial. De hecho para llegar a conocer tal divisor necesitaremos primero saber:

1. Los índices de ramificación $e(P|P')$ para todo P' lugar racional de $\mathcal{H}$ y $P = P' \cap \mathcal{H}^{\mathcal{G}}$.

2. Los grados de $P = P' \cap \mathcal{H}^{\mathcal{G}}$, para los lugares $P' \in \mathbb{P}(\mathcal{H})$ con $e(P|P') \neq 1$.

Realizar estos cálculos para cualquier $\mathcal{G}$ subgrupo del grupo de automorfismo $\mathcal{A}$ es un gran problema, ya que el grupo de automorfismos de $\mathcal{H}$ es un grupo muy extenso. Así que en este cápitulo sólo nos enfocaremos calcular los posibles géreros de $\mathcal{H}^{\mathcal{G}}$ cuando $\mathcal{G}$ es un subgrupo de $\mathcal{A}_1(P'_\infty)$.

Recordemos que $\mathcal{A}_1(P'_\infty)$ es el subgrupo de $\mathcal{A}$, dado por

$$\mathcal{A}_1(P'_\infty) = \{\sigma \in \mathcal{A}(P'_\infty) \,/\, \sigma(x) = x + b \ , \sigma(y) = y + b^q x + c\} \subset \mathcal{A}(P'_\infty),$$

donde $b \in K$ y $c^q + c = b^{q+1}$.

4.2. Indices de ramificación.

Como sabemos, los lugares de $\mathcal{H}^{\mathcal{G}}$ son de la forma $P = P' \cap \mathcal{H}^{\mathcal{G}}$, donde P' es un lugar de $\mathcal{H}$. En lo que sigue demostraremos que si $\mathcal{G} < \mathcal{A}_1(P'_\infty)$ se cumplirá:

$$e(P'_\infty|P_\infty) = ord(\mathcal{G}) \quad \text{y} \quad e(P'|P) = 1 \ \ \forall\, P' \neq P'_\infty \ (P' \text{ racional}) \tag{4.1}$$

Comenzaremos con el lugar P_∞ de $\mathcal{H}^{\mathcal{G}}$, la demostración se dividira en varias partes, pero la idea principal es demostrar que $G_T(P'_\infty|P_\infty) = \mathcal{G}$ (ver Definición 1.33) y dado que este grupo de inercia tiene orden $e(P'_\infty|P_\infty)$ tendremos lo que buscamos. Partiremos con una proposición que nos será muy útil.

Proposición 4.1. *Si $w \in \mathcal{H}$ entonces $v_{P'_\infty}(w) = v_{P'_\infty}(\sigma(w))$ para todo $\sigma \in \mathcal{A}(P'_\infty)$.*

Demostración: Recordemos que $\sigma(P'_\infty) = P_{\infty'}$ para todo $\sigma \in \mathcal{A}(P'_\infty)$, luego reemplazando $y = \sigma(w)$ y $P' = P'_\infty$ en la ecuación (1.1) tendremos que:

$$\begin{aligned} v_{\sigma(P'_\infty)}(\sigma(w)) &= v_{P'_\infty}(w) \\ v_{P'_\infty}(\sigma(w)) &= v_{P'_\infty}(w) \end{aligned}$$

□

Proposición 4.2. *Para P'_∞, el lugar infinito de $\mathcal{H}$, y $\mathcal{G} < \mathcal{A}(P'_\infty)$ se tiene*

$$v_{P'_\infty}(\sigma(z) - z) > 0 \quad \forall\, z \in \mathcal{O}_{P'_\infty} \ y \ \forall\, \sigma \in \mathcal{G}.$$

Demostración: En toda la demostración σ será un elemento cualquierea de $\mathcal{G}$, pero dividiremos la demostración en dos partes.

1) ($z \in P'_\infty$): Sabemos por definición que $v_{P_{\infty'}}(z) > 0$ y por proposición anterior podemos concluir también que $v_{P_{\infty'}}(\sigma(z)) > 0$. Así, tendremos

$$\begin{aligned} v_{P'_\infty}(\sigma(z) - z) &\geq min\{v_{P'_\infty}(\sigma(z)), v_{P'_\infty}(z)\} \\ &> 0 \end{aligned}$$

2) ($z \in \mathcal{O}_{P'_\infty} - P'_\infty$): Como $z^*(0:1:0) \neq 0$ existe una representación de z de la forma

$$z = \frac{f_0(x,y) + \cdots + f_N(x,y)}{g_0(x,y) + \cdots + g_N(x,y)},$$

donde $f_i, g_i \in K[x,y]$ son formas de grado i. Además con esta representación observamos que,

$$z - z^*(0:1:0) = \frac{(f_0(x,y) + \cdots + f_N(x,y)) - z^*(0:1:0)(g_0(x,y) + \cdots + g_N(x,y))}{g_0(x,y) + \cdots + g_N(x,y)},$$

donde el grado del numerador es menor o igual a N. Luego no es difícil verificar, que en ambos casos, $(z - z^*(0:1:0))^*(0:1:0) = 0$, y por lo tanto $z - z^*(0:1:0) \in P'_\infty$. Finalmente, si denotamos $k := z^*(0:1:0) \in K$ y usamos es resultado anterior, tendremos

$$\begin{aligned} v_{P'_\infty}(\sigma(z) - z) &= v_{P'_\infty}[\sigma(z - k + k) - (z - k + k)] \\ &= v_{P'_\infty}[\sigma(z - k) - (z - k)] \\ &\geq min\{v_{P'_\infty}(\sigma(z - k)), v_{P'_\infty}(z - k)\} \quad > 0 \end{aligned}$$

□

Observación 4.1. De la proposición anterior se concluye que si $\mathcal{G} < \mathcal{A}(P'_\infty)$ entonces $G_T(P'_\infty|P_\infty) = \mathcal{G}$, luego por el Teorema 1.10 se tiene que $e(P'_\infty|P_\infty) = ord(\mathcal{G})$.

Ahora que tenemos resuelto el caso P_∞ consideraremos los lugares de $\mathcal{H}^{\mathcal{G}}$ de la forma $P = P' \cap \mathcal{H}^{\mathcal{G}}$ donde P' es un lugar racional de $\mathcal{H}$ distinto de P'_∞. Al igual que en el caso anterior la idea de la demostración será encontrar $G_T(P'|P)$.

Proposición 4.3. *Para todo lugar racional $P' \neq P'_\infty$, $\mathcal{G} < \mathcal{A}_1(P'_\infty)$ y $P = P' \cap \mathcal{H}^{\mathcal{G}}$ se tiene $G_T(P'|P) = \{Id\}$.*

Demostración: Sabemos que si P es un lugar racional de $\mathcal{H}$ distinto de P'_∞ entonces $P' = P'_{\alpha,\beta}$ con $\alpha, \beta \in \mathbb{F}_{q^2}$. Además si $\sigma \in \mathcal{G}$ entonces σ es de la forma $\sigma(x) = x + b$ y $\sigma(y) = y + b^q x + c$.
La idea de la demostración será que para todo $\sigma \in \mathcal{G}$ existe un $w \in \mathcal{O}_{P'_{\alpha,\beta}}$ que cumple $v_{P'_{\alpha,\beta}}(\sigma(w) - w) \leq 0$.
Para esto consideremos los siguientes casos:

(*i*) ($b \neq 0$): En este caso consideremos $w = (x - \alpha)$, con lo que $\sigma(w) = x + b - \alpha$. Luego $v_{P'_{\alpha,\beta}}(w) > 0$, $v_{P'_{\alpha,\beta}}(\sigma(w)) = 0$ y por lo tanto $v_{P'_{\alpha,\beta}}(\sigma(w) - w) = 0$.

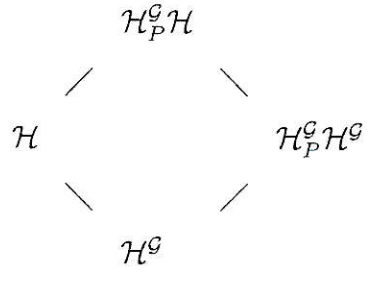
(*ii*) ($b = 0$ y $c \neq 0$): En este caso consideremos $w = (y - \beta)$, con lo que $\sigma(w) = y + c - \beta$. Luego $v_{P'_{\alpha,\beta}}(w) > 0$, $v_{P'_{\alpha,\beta}}(\sigma(w)) = 0$ y por lo tanto $v_{P'_{\alpha,\beta}}(\sigma(w) - w) = 0$.

En conclusión, el único automorfismo que cumple $v_{P'_{\alpha,\beta}}(\sigma(z) - z) > 0$ para todo $z \in \mathcal{O}_{P'_{\alpha,\beta}}$ es la identidad. □

Observación 4.2. De la proposición anterior más el Teorema 1.10, se concluye que si $\mathcal{G} < \mathcal{A}_1(P'_\infty)$ entonces $e(P'|P) = 1$ para todo lugar racional $P' \neq P'_\infty$ de $\mathcal{H}$.

Proposición 4.4. *Si $\mathcal{G} < \mathcal{A}_1(P'_\infty)$ y $P \in \mathbb{P}(\mathcal{H}^{\mathcal{G}})$ es un lugar de grado $d \neq 1$, entonces para todo $P' \in \mathbb{P}(\mathcal{H})$ con $P'|P$ se tiene $e(P'|P) = 1$.*

Demostración: Si P es un lugar de grado d tendremos que $[\mathcal{H}_P^{\mathcal{G}} : K] = d$, es decir, el cuerpo residual $\mathcal{H}_P^{\mathcal{G}} \cong F_{q^{2d}}$. Así P es no ramificado en el cuerpo de funciones[1] $\mathcal{H}_P^{\mathcal{G}}\mathcal{H}^{\mathcal{G}}/\mathcal{H}^{\mathcal{G}}$, de hecho existen d lugares de grado 1 en $\mathcal{H}_P^{\mathcal{G}}\mathcal{H}^{\mathcal{G}}$ que extienden a P. Además como ya hemos demostrado que los lugares de grado 1 en $\mathcal{H}^{\mathcal{G}}/\mathbb{F}_{q^2}$ no son ramificados en $\mathcal{H}$, para todo q potencia de un primo, podemos concluir que los anteriores d lugares de grado 1 en $\mathcal{H}_P^{\mathcal{G}}\mathcal{H}^{\mathcal{G}}$ son no ramificados en $\mathcal{H}_P^{\mathcal{G}}\mathcal{H}$.
Finalmente, ya que se cumple el siguente diagrama de cuerpos.



Concluimos que P es no ramificado en $\mathcal{H}_P^{\mathcal{G}}\mathcal{H}$ y por lo tanto tampoco en $\mathcal{H}$. □

4.3. Lugares racionales de $\mathcal{H}^{\mathcal{G}}$.

En esta sección describiremos los lugares racionales de $\mathcal{H}^{\mathcal{G}}$ y veremos por qué tipo de lugares en $\mathcal{H}$ son extendidos.
Recordemos que si $P_1', \ldots, P_r'$ son todos los lugares de $\mathcal{H}$ que extiende a P, entonces por Corolario 1.3

$$e(P) \cdot f(P) \cdot r = [\mathcal{H} : \mathcal{H}^{\mathcal{G}}] = ord(\mathcal{G}), \tag{4.2}$$

donde $e(P) := e(P_i'|P)$ y $f(P) := f(P_i'|P)$ para todo $1 \leq i \leq r$.
También por Corolario 1.3 sabemos que para calcular el grado de un lugar basta con conocer los grados de su extensiones y que además todas sus extensiones tienen el

[1] El cuerpo de funciones $\mathcal{H}_P^{\mathcal{G}}\mathcal{H}^{\mathcal{G}}/\mathcal{H}_P^{\mathcal{G}}$ corresponde al cuerpo de funciones asociado a la curva $\mathcal{X}_{\mathcal{H}^{\mathcal{G}}}$, definida sobre $\mathcal{H}_P^{\mathcal{G}}$

mismo grado. De hecho, la fórmula del grado de un lugar en nuestro caso quedará

$$deg(P) = \frac{deg(P')}{f(P)}, \tag{4.3}$$

donde $P \in \mathbb{P}(\mathcal{H}^{\mathcal{G}})$ y $P' \in \mathbb{P}(\mathcal{H})$ es una extensión cualquiera de P.

Observación 4.3. Si $P \in \mathbb{P}(\mathcal{H}^{\mathcal{G}})$ es un lugar de grado 1 y P' es un lugar de $\mathcal{H}$ que lo extiende, entonces se debe cumplir que

$$1 = \frac{deg(P')}{f(P)}$$

Por lo tanto, los lugares de $\mathcal{H}$ que extienden a lugares racionales de $\mathcal{H}^{\mathcal{G}}$ son lugares que tienen grado igual al grado relativo entre ellos.

Observación 4.4. En la sección anterior demostramos que $e(P_\infty) = ord(\mathcal{G})$, luego de la ecuación (4.2) se concluye que $r = f(P_\infty) = 1$, es decir, existe un único lugar en $\mathcal{H}$ que extiende a P_∞, a saber P'_∞.
Además de la ecuación (4.3) tendremos que

$$deg(P_\infty) = \frac{deg(P'_\infty)}{f(P_\infty)} = 1.$$

Observación 4.5. En la sección anterior demostramos que si $P' \neq P'_\infty$ es un lugar racional de $\mathcal{H}$ y $P = P' \cap \mathcal{H}^{\mathcal{G}}$, entonces $e(P'|P) = 1$. Luego de la ecuación (4.2) se concluye que $f(P_\infty) \cdot r = ord(\mathcal{G})$, y reemplazando esto en la ecuación (4.3) tendremos

$$deg(P) = \frac{deg(P')}{f(P)} = \frac{r}{ord(\mathcal{G})}.$$

Pero por ecuación 4.2, sabemos que también r divide a $ord(\mathcal{G})$. Luego $r = ord(\mathcal{G})$ y con esto obtenemos que $deg(P) = 1$.
Por lo tanto, los q^3 lugares racionales afines de $\mathcal{H}$ se tranforman en $q^3/ord(\mathcal{G})$ lugares racionales de $\mathcal{H}^{\mathcal{G}}$.

El siguente lema nos ayudará a encontrar lugares de grado m primo en $\mathcal{H}$, aunque no lo usaremos hasta el capítulo 5.

Lema 4.1. *Sea $K' = \mathbb{F}_{q^{2m}}$ y $K = \mathbb{F}_{q^2}$ como siempre. Si $p_1 = (a, b) \in \mathcal{X}_{\mathcal{H}}$ con $a, b \in (K' - K)$, entonces P_1 es un lugar de grado m en $\mathcal{H}$.*

Demostración: Consideremos el homomorfismo epiyectivo

$$\begin{aligned} \phi: \ \mathcal{O}_{P_1} &\longrightarrow K' \\ z &\mapsto z(p_1) \end{aligned}$$

y notemos que $Ker(\phi) = P_1$. Luego, $\mathcal{H}_{P_1} = \mathcal{O}_{P_1}/P_1 \cong K'$ y por lo tanto

$$deg(P_1) = [\mathcal{H}_{P_1} : K] = [\mathcal{H}_{P_1} : K'][K' : K] = [K' : K] = m.$$

□

4.4. Calculando el grado de $\mathcal{H}^{\mathcal{G}}$.

Con los resultados de la sección anterior tenemos la información necesaria para conocer $\text{Diff}(\mathcal{H}/\mathcal{H}^{\mathcal{G}})$ y finalmente calcular $g(\mathcal{H}^{\mathcal{G}})$.

Proposición 4.5. *Si $\mathcal{G} < \mathcal{A}_1(P'_\infty)$ entonces, $Diff(\mathcal{H}/\mathcal{H}^{\mathcal{G}}) = d(P'_\infty|P_\infty)P_\infty$.*

Demostración: Sabemos por Definición 1.31 que,

$$\text{Diff}(\mathcal{H}/\mathcal{H}^{\mathcal{G}}) := \sum_{P \in \mathbb{P}_{\mathcal{H}^{\mathcal{G}}}} \sum_{P'|P} \text{d}(P'|P)P'.$$

Además como para todo $P \neq P_\infty$ sabemos que $e(P'|P) = 1$, por el Teorema 1.7 podemos concluir que $d(P'|P) = 0$. Por lo tanto

$$\begin{aligned} \text{Diff}(\mathcal{H}/\mathcal{H}^{\mathcal{G}}) &= \sum_{P \neq P_\infty} \sum_{P'|P} \text{d}(P'|P).P' + \sum_{P_\infty} \sum_{P'|P} \text{d}(P'|P).P' \\ &= \sum_{P_\infty} \sum_{P'|P} \text{d}(P'|P).P' \\ &= \text{d}(P'_\infty|P_\infty).P'_\infty \end{aligned}$$

□

Recordemos que el lugar P_∞ de $\mathcal{H}^{\mathcal{G}}$ es un lugar de grado 1, por lo tanto usando el resultado anterior tendremos que

$$deg(\text{Diff}(\mathcal{H}/\mathcal{H}^{\mathcal{G}})) = d(P'_\infty|P_\infty). \tag{4.4}$$

Luego sólo restaría encontrar este diferente y para hacerlo usaremos la siguiente idea[2].

Si $\sigma \in \mathcal{A}_1(P_\infty)$ entonces $\sigma(x) = x + b$ y $\sigma(y) = y + b^q x + c$. Luego, σ queda totalmente determinado por b, c y lo podemos identificar con el par $[b, c]$.

Con esta notación, para cada $\mathcal{G} < \mathcal{A}_1(P_\infty)$, consideremos el siguiente homomorfismo,

$$\begin{aligned} \varphi: \quad \mathcal{G} \quad &\longrightarrow K \\ [b,c] \quad &\to b \end{aligned}$$

y los siguientes conjuntos:

$$\mathcal{V}_{\mathcal{G}} := Im(\varphi) \quad \text{y} \quad \mathcal{W}_{\mathcal{G}} := Ker(\varphi). \tag{4.5}$$

No es difícil verificar $ord(\mathcal{V}_{\mathcal{G}}) = p^v$, $ord(\mathcal{W}_{\mathcal{G}}) = p^w$ y por lo tanto $ord(\mathcal{G}) = p^{v+w}$.

Proposición 4.6. *Si $\mathcal{G} < \mathcal{A}_1(P'_\infty)$ entonces,*

$$deg(Diff(\mathcal{H}/\mathcal{H}^{\mathcal{G}})) = 2(p^{v+w} - p^w) + (q+2)(p^w - 1).$$

[2] Esta idea es usada por García, Henning, Stichtenoth y Xing en [3].

Demostración: Recordemos la Proposición 1.5, que para $P = P_\infty$ quedará

$$\begin{aligned}
d(P'_\infty|P_\infty) &= \sum_{\substack{\delta\in\mathcal{G}\\ \delta\neq Id}} v_{P'_\infty}(\delta(x/y) - x/y) \\
&= \sum_{\substack{[n,m]\in\mathcal{G}\\ n\neq 0}} v_{P'_\infty}(\delta(x/y) - x/y) + \sum_{\substack{[n,m]\in\mathcal{G}\\ n=0,m\neq 0}} v_{P'_\infty}(\delta(x/y) - x/y) \\
&= \sum_{\substack{[n,m]\in\mathcal{G}\\ n\neq 0}} 2 + \sum_{\substack{[n,m]\in\mathcal{G}\\ n=0,m\neq 0}} (q+2) \\
&= \sum_{\delta\in(\mathcal{G}-\mathcal{W}_\mathcal{G})} 2 + \sum_{\delta\in(\mathcal{W}_\mathcal{G}-[0,0])} (q+2) \\
&= 2ord(\mathcal{G}-\mathcal{W}_\mathcal{G}) + (q+2)ord(\mathcal{W}_\mathcal{G} - [0,0]) \\
&= 2(p^{v+w} - p^w) + (q+2)(p^w - 1)
\end{aligned}$$

□

Proposición 4.7. *Si* $\mathcal{G} < \mathcal{A}_1(P'_\infty)$ *entonces,* $g(\mathcal{H}^{\mathcal{G}}) = \frac{1}{2}p^{l-v}(p^{l-w} - 1)$.

Demostración: Evaluando todo lo que ya conocemos la fórmula del género de Hurwitz (1.8) tendremos

$$\begin{aligned}
2g(\mathcal{H}) - 2 &= \frac{[\mathcal{H}:\mathcal{H}^{\mathcal{G}}]}{[K:K]}(2g(\mathcal{H}^{\mathcal{G}}) - 2) + deg\mathrm{Diff}(\mathcal{H}/\mathcal{H}^{\mathcal{G}}) \\
2\frac{q(q-1)}{2} - 2 &= ord(\mathcal{G})(2g(\mathcal{H}^{\mathcal{G}}) - 2) + 2(p^{v+w} - p^w) + (q+2)(p^w - 1) \\
q^2 - q - 2 &= p^{v+w}(2g(\mathcal{H}^{\mathcal{G}}) - 2) + 2p^{v+w} - 2p^w + qp^w - q + 2p^w - 2 \\
q^2 &= 2p^{v+w}g(\mathcal{H}^{\mathcal{G}}) + qp^w \\
q^2 - qp^w &= 2p^{v+w}g(\mathcal{H}^{\mathcal{G}}) \\
p^{2l} - p^{l+w} &= 2p^{v+w}g(\mathcal{H}^{\mathcal{G}}).
\end{aligned}$$

Así, despejando $g(\mathcal{H}^{\mathcal{G}})$ y factorizando obtenemos los que buscamos. □

Observación 4.6. Para todo v, w tales que el resultado de la fórmula en la Proposición 4.7 sea un número natural, existe un cuerpo fijo $\mathcal{H}^{\mathcal{G}}$ con tal género[3].

[3] Para más información acerca de esta afirmación ver [3] pag. 145.

Observación 4.7. No existen subgrupos de $\mathcal{A}_1(P'_\infty)$ con $ord(\mathcal{W}_\mathcal{G}) = p^w$ y $w > l$, ni $ord((\mathcal{V}_\mathcal{G}) = p^v$ y $v > l$. Esto se debe a que si ocurriese alguna de estas dos condiciones tendriamos un género no natural.
Por lo tanto en la fórmula del género de $\mathcal{H}^{\mathcal{G}}$ tendremos que $0 \leq v, w \leq l$.

La siguiente propiedad nos será de mucha utilidad para determinar cuando un cuerpo fijo $\mathcal{H}^{\mathcal{G}}$ sea isomorfo a $K(x)$.

Proposición 4.8. *Si $\mathcal{G} < \mathcal{A}_1(P_\infty)$, entonces $\mathcal{H}^{\mathcal{G}}$ es el cuerpo de funciones racionales si y sólo si alguna de las siguientes condiciones se cumplen,*

a) $ord(\mathcal{W}_\mathcal{G}) = q$.

b) $\mathcal{G} \supseteq \{[0, c] : c^q + c = 0\}$.

c) $\mathcal{H}^{\mathcal{G}} \subseteq K(x)$.

Observación 4.8. Si $\mathcal{G} < \mathcal{A}_1(P_\infty)$, entonces $g(\mathcal{H}^{\mathcal{G}}) = 0 \Leftrightarrow w = l$. En tal caso $\mathcal{H}^{\mathcal{G}} = K(x)$.
La equivalencia es fácil de verificar por la fórmula que determina el género en la Propiedad 4.7. Ahora si $g(\mathcal{H}^{\mathcal{G}}) = 0$, entonces $\mathcal{W}_\mathcal{G} = \{[0, c] : c^q + c = 0\}$, dado que $|\mathcal{W}_\mathcal{G}| = q$, luego por Propiedad 4.8 tendremos que $\mathcal{H}^{\mathcal{G}} = K(x)$.

Observación 4.9. Notemos que el menor cuociente "g/n" se obtiene al tener $g(\mathcal{H}^{\mathcal{G}}) = 0$ o lo que es equivalente $\mathcal{H}^{\mathcal{G}} = K(x)$, independiente del valor de n. En tal caso los códigos Goppas detallados en la Sección 2.3 son códigos (MDS). Esto se obtiene reemplazando $g = 0$ en la ecuación (2.3).

Con la observación anterior tenemos completamente determinados los códigos Goppa especificados en la Sección 2.3, sobre el cuerpo de funciones $K(x)$ de género cero. Es por esto que en la siguiente sección analizaremos los cuocientes "g/n" cuando $g(\mathcal{H}^{\mathcal{G}}) \neq 0$.

4.5. Analizando los cuocientes g/n.

Recordemos que en la Observación 2.3 vimos que fijando un género g, el menor cuociente "g/n" se obtiene al considerar $n = \#\mathcal{N}(F) - 1$ y F un cuerpo de funciones maximal de género g. Pero que pasará con estos cuocientes si hacemos variar el género. En esta sección compararemos los distintos cuocientes "g/n" cuando g varia entre todos los géneros $g(\mathcal{H}^{\mathcal{G}}) \neq 0$.

Dado que $\mathcal{H}^{\mathcal{G}}$ es un cuerpo maximal, no es difícil verificar que la cantidad de lugares racionales de $\mathcal{H}^{\mathcal{G}}$ es

$$\#\mathcal{N}(\mathcal{H}^{\mathcal{G}}) = q^2 + 1 + 2g(\mathcal{H}^{\mathcal{G}})q.$$

y por lo tanto,

$$n = q^2 + 2gq \qquad \text{y} \qquad \frac{n}{g} = \frac{q^2}{g} + 2q = \frac{2p^{l+v}}{p^{l-w}-1} + 2p^l = 2p^l\left(\frac{p^v}{p^{l-w}-1} + 1\right).$$

Nótese que, g/n decrece si y solo si n/g crece. A continuación analizaremos caso a caso.

Observación 4.10. Es fácil verificar que dados l, p y w fijos "n/g" crece al crecer v, es decir, g/n decrece al crecer v.

Análogamente, dados l, p y v fijos "n/g" crece al crecer w, es decir, g/n decrece al crecer w.

Recordemos que en la Observación 4.8 analizamos el caso en que $w = l$ y en la Observación 4.7 vimos que $1 \leq v, w \leq l$. Por lo tanto, de entre todos los cuerpos fijo $\mathcal{H}^{\mathcal{G}}$, el menor cuociente "$g/n \neq 0$" que podemos obtener es:

$$\left[2p^l\left(\frac{p^l}{p-1} + 1\right)\right]^{-1}, \tag{4.6}$$

que corresponde a $v = l$ y $w = l - 1$.

Observación 4.11. Para $q = p^l$ fijo y $\mathcal{G} < \mathcal{A}_1(P_\infty)/\mathbb{F}_{q^2}$ un subgrupo con parámetros v y w asociados, siempre existe p' un primo y $\mathcal{G}' < \mathcal{A}_1(P_\infty)/\mathbb{F}_{p'^2}$ un subgrupo con

parámetros $v' = 1$ y $w' = 0$ asociados que cumplen

$$\frac{g}{n} > \frac{g'}{n'}.$$

Esto se debe a que siempre podemos encontar p' primo con $p^l < p'(*)$. Luego

$$p^{l-w} < p^l < p' \quad \Rightarrow \quad 0 < \frac{p^{l-w}-1}{p'-1} < 1.$$

Además, también siempre existe p' primo con

$$p^v < p'\left(\frac{p^{l-w}-1}{p'-1}\right). \quad (**)$$

Por lo tanto, si p' es un primo que cumple $(*)$ y $(**)$ (siempre existe) tendremos

$$2p^l\left(\frac{p^v}{p^{l-w}-1}+1\right) < 2p'\left(\frac{p'}{p'-1}+1\right),$$

es decir, $g'/n' < g/n$.

La observación anterior nos dice dado $q = p^l$, siempre podemos encontrar un primo p' y $\mathcal{G}' < \mathcal{A}_1(P'_\infty)/\mathbb{F}_{p'^2}$ con parámetros asociados $v = 1$ y $w = 0$ que cumplen con

$$\left[2p'\left(\frac{p'}{p'-1}+1\right)\right]^{-1} < \left[2p^l\left(\frac{p^l}{p-1}+1\right)\right]^{-1}.$$

Por lo tanto, de aquí en adelante podemos considerar $q = p$, es decir $l = 1$, ya que aumentando p siempre conseguiremos cuocientes "g/n" tan pequeños como queramos.

4.6. Trabajando con $\mathcal{H}^{\mathcal{G}}$ sobre $K = \mathbb{F}_{q^2}$ y $q = p$.

En la sección anterior concluimos que bastaba con conocer los distintos cuocientes "g/n" considerando $q = p$, es decir, con $l = 1$.

Bajo estas condiciones sea $\mathcal{G} < \mathcal{A}_1(P'_\infty)$ y $\mathcal{V}_\mathcal{G}$, $\mathcal{W}_\mathcal{G}$ como en la ecuación (4.5). Seguiremos denotando los órdenes de $\mathcal{G}$, $\mathcal{V}_\mathcal{G}$ y $\mathcal{W}_\mathcal{G}$ respectivamente por p^{v+w}, p^v y p^w, donde $0 \leq v, w \leq 1$.

Sabemos que $ord(\mathcal{A}_1(P_\infty)) = q^3 = p^3$, luego si $\mathcal{G} < \mathcal{A}_1(P_\infty)$, sus posibles órdenes serán p^0, p^1, p^2 y p^3. Analizaremos caso a caso que sucede con $\mathcal{H}^{\mathcal{G}}$ y su género.

Lema 4.2. *Si $\mathcal{G} < \mathcal{A}_1(P_\infty)$ con $ord(G) = p^0$ entonces $\mathcal{H}^{\mathcal{G}} = \mathcal{H}$ y $g(\mathcal{H}^{\mathcal{G}}) = p(p-1)/2$.*

Demostración: Si $ord(\mathcal{G}) = 1$, entonces $\mathcal{G} = \{Id\}$. Luego $\mathcal{H}^G = \mathcal{H}$ y por lo tanto $g(\mathcal{H}^{\mathcal{G}}) = p(p-1)/2$. □

El análisis del caso $ord(\mathcal{G}) = p$ lo dejaremos para el final. Por ahora seguiremos con $ord(\mathcal{G}) = p^2$ y p^3.

Lema 4.3. *Si $\mathcal{G} < \mathcal{A}_1(P_\infty)$ con $ord(\mathcal{G}) = p^2$ entonces $\mathcal{H}^{\mathcal{G}} \cong K(x)$ y $g(\mathcal{H}^{\mathcal{G}}) = 0$.*

Demostración: Si $ord(\mathcal{G}) = p^2$, entonces el único caso posible, dado que $0 \leq v, w \leq 1$, es:

$$ord(\mathcal{V}_{\mathcal{G}}) = p^1 \quad \text{y} \quad ord(\mathcal{W}_{\mathcal{G}}) = p^1.$$

Luego por Propiedad 4.8 tendremos que $\mathcal{H}^{\mathcal{G}} = K(x)$ y por lo tanto $g(\mathcal{H}^{\mathcal{G}}) = 0$. □

Lema 4.4. *Si $\mathcal{G} < \mathcal{A}_1(P_\infty)$ con $ord(\mathcal{G}) = p^3$ entonces $\mathcal{H}^{\mathcal{G}} \cong K(x)$ y $g(\mathcal{H}^{\mathcal{G}}) = 0$.*

Demostración: Si $ord(\mathcal{G}) = p^3$, entonces $\mathcal{G} = \mathcal{A}_1(P'_\infty)$, luego $\mathcal{G} \supseteq \{[0, c] : c^q + c = 0\}$ y por Propiedad 4.8 podemos concluir que $\mathcal{H}^{\mathcal{G}} = K(x)$ y por lo tanto $g(\mathcal{H}^G) = 0$. □ Sólo nos queda pendiente el caso $\mathcal{G} < \mathcal{A}_1(P_\infty)$ y $ord(\mathcal{G}) = p$. Pero esto significa que $\mathcal{G}$ es un grupo cíclico, digamos generado por

$$\sigma(x) = x + b \qquad \sigma(y) = y + b^q x + c,$$

donde (b, c) es un punto racional de $\mathcal{H}$.

Una observación no muy difícil de probar (por inducción) es que

$$\sigma^i(x) = x + ib \qquad \sigma^i(y) = y + ib^q x + ic + \frac{(i-1)i}{2} b^{q+1}. \tag{4.7}$$

Además, como $\sigma \in \mathcal{A}_1(P_\infty)$ su orden divide a p^3, luego para que σ efectivamente genere un grupo de orden p sólo debemos comprobar que $\sigma^p(x) = x$ y $\sigma^p(y) = y$.

Dividiremos el análisis en dos caso: $p = 2$ y $p \neq 2$.

Lema 4.5. *Si $p = 2$, entonces σ genera un subgrupo de orden p si y solo si $b = 0$ y $c \neq 0$.*

Demostración: Notemos que por la observación anterior

$$\sigma^2(x) = x \qquad \sigma^2(y) = y + b^3.$$

Luego si $b \neq 0$, entonces $ord(\mathcal{G}) > 2$, además si $b = 0$ y $c \in K$ con $c^2 + c = 0$, entonces $ord(\mathcal{G}) = 2$. □

Lema 4.6. *Si $p \neq 2$, entonces σ genera un subgrupo de orden p para todo $b \in K$.*

Demostración: Notemos que por la ecuación (4.7)

$$\sigma^p(x) = x \qquad \sigma^p(y) = y + \frac{(p-1)p}{2}b^3 = y,$$

ya que $p - 1$ es par y por lo tanto $(p-1)/2 \in \mathbb{Z}$. □

Usando los Lemas 4.5 y 4.6, ya estamos en condiciones de determinar los géneros de $\mathcal{H}^{\mathcal{G}}$ cuando $ord(\mathcal{G}) = p$.

Lema 4.7. *Si $p = 2$ y $\mathcal{G} < \mathcal{A}_1(P_\infty)$ con $ord(\mathcal{G}) = p$, entonces $g(\mathcal{H}^{\mathcal{G}}) = 0$.*

Demostración: Por lema anterior sabemos que $\mathcal{G} = \langle\sigma\rangle$ tiene orden $p \Leftrightarrow \sigma = [0, c]$. Luego $\mathcal{V}_{\mathcal{G}} = \{0\}$ y $\mathcal{W}_{\mathcal{G}} = \mathcal{G}$, por lo tanto $g(\mathcal{H}^{\mathcal{G}}) = \frac{1}{2}p^{1-0}(p^{1-1} - 1) = 0$. □
Con esto hemos completado el caso $p = 2$, por lo que pasaremos al caso $p \neq 2$.

Lema 4.8. *Si $p \neq 2$ y $\mathcal{G} < \mathcal{A}_1(P_\infty)$ con $ord(\mathcal{G}) = p$, entonces $g(\mathcal{H}^{\mathcal{G}}) = 0$ ó $(p-1)/2$.*

Demostración: Por lema anterior sabemos que $\mathcal{G} = \langle\sigma\rangle$ tiene orden p para todo $b \in K$. Luego tenemos dos casos:

- $b = 0 \Rightarrow \mathcal{V}_{\mathcal{G}} = \{0\}$ y $\mathcal{W}_{\mathcal{G}} = \mathcal{G}$, por lo tanto $g(\mathcal{H}^{\mathcal{G}}) = \frac{1}{2}p^{1-0}(p^{1-1} - 1) = 0$.

- $b \neq 0 \Rightarrow \mathcal{V}_{\mathcal{G}} = \{b, 2b, \ldots, pb\}$ y $\mathcal{W}_{\mathcal{G}} = \{[0,0]\}$, por lo tanto $g(\mathcal{H}^{\mathcal{G}}) = \frac{1}{2}p^{1-1}(p^{1-0}-1) = (p-1)/2$.

□

En resumen, usando el hecho que $g(\mathcal{H}^{\mathcal{G}}) = 0$ implica $\mathcal{H}^{\mathcal{G}} = K(x)$ tendremos: Si $\mathcal{G} < \mathcal{A}_1(P_\infty)$ con $ord(\mathcal{G}) = p$, entonces

$$g(\mathcal{H}^{\mathcal{G}}) = \begin{cases} 0 & \text{si } p = 2 \\ 0 & \text{si } p \neq 2 \text{ y } b = 0 \\ (p-1)/2 & \text{si } p \neq 2 \text{ y } b \neq 0 \end{cases} \qquad \mathcal{H}^{\mathcal{G}} = \begin{cases} K(x) & \text{si } p = 2 \\ K(x) & \text{si } p \neq 2 \text{ y } b = 0 \\ ? & \text{si } p \neq 2 \text{ y } b \neq 0 \end{cases}$$

Por lo tanto, solo nos faltaría conocer en un caso el cuerpo fijo $\mathcal{H}^{\mathcal{G}}$, pero para esto diseñamos un programa al cual le entregamos valores de p y b y éste nos calcula el cuerpo fijo correspondiente. Pero de esto hablaremos más en detalle en el siguiente capítulo.

Capítulo 5

Ejemplos

En la sección anterior concluimos que si $\mathcal{G} < \mathcal{A}_1(P_\infty)$, $ord(\mathcal{G}) = p \neq 2$, $\mathcal{G} =< [b,c] >$ y $b \neq 0$, entonces $g(\mathcal{H}^{\mathcal{G}}) = (p-1)/2$. Pero no pudimos concluir cuál era el cuerpo fijo $\mathcal{H}^{\mathcal{G}}$ correspondiente. Para solucionar este problema construimos un programa, que explicaremos en el capítulo 6, al cual se le entregan los valores de p, b y c nos devuelve el cuerpo fijo correspondiente. A modo de ejemplo les presentaremos la idea para $p = 3$ y como anexo aparecerá el programa en el que se podrá reemplazar por un primo cualquiera.

5.1. Conociendo $\mathcal{H}^{\mathcal{G}}$ cuando $ord(\mathcal{G}) = 3$

Sea $\mathcal{G} =< [b,c] >$ el subgrupo de orden 3 de $\mathcal{A}_1(P_\infty)$, cuyos elementos son de la forma.

$$\begin{aligned} \sigma_1(x) &= x+1 & \sigma_1(y) &= y+x+2 \\ \sigma_2(x) &= x+2 & \sigma_2(y) &= y+2x+2 \\ \sigma_3(x) &= x & \sigma_3(y) &= y \end{aligned}$$

Luego, si f es un elemento de $\mathcal{H}^{\mathcal{G}}$ de la forma

$$f(x,y) = a_0(x) + a_1(x)y + a_2(x)y^2.$$

Entonces, aplicando σ_1 a f tendremos,

$$\begin{aligned}
* \ \sigma_1(a_0(x)) &= a_0(x+1) \\
* \ \sigma_1(a_1(x)y) &= a_1(x+1)(y+x+2) \\
&= a_1(x+1)(x+2) + a_2(x+1)y \\
* \ \sigma_1(a_2(x)y^2) &= a_2(x+1)(y+x+2)^2 \\
&= a_2(x+1)(y^2+x^2+1+2xy+x+y) \\
&= a_2(x+1)(x^2+x+1) + a_2(x+1)(2x+1)y + a_2(x+1)y^2
\end{aligned}$$

Luego como $f \in \mathcal{H}^{\mathcal{G}}$ se debe cumplir

$$a_0(x) = a_0(x+1) + a_1(x+1)(x+2) + a_2(x+1)(x^2+x+1) \quad (5.1)$$

$$a_1(x) = a_1(x+1) + a_2(x+1)(2x+1) \quad (5.2)$$

$$a_2(x) = a_2(x+1) \quad (5.3)$$

lo que es equivalente a,

$$a_0(x+1) - a_0(x) = -a_1(x+1)(x+2) - a_2(x+1)(x^2+x+1) \quad (5.4)$$

$$a_1(x+1) - a_1(x) = -a_2(x+1)(2x+1) \quad (5.5)$$

$$a_2(x+1) - a_2(x) = 0 \quad (5.6)$$

Para encontrar la solución de estas ecuaciones vamos a definir un operador sobre $K[x]$ que denotaremos por

$$\triangle(p(x)) = p(x+1) - p(x)$$

Este operador cumple las siguientes propiedades:

$$\begin{aligned} \circ\ \triangle\left((pq)(x)\right) &= pq(x+1) - pq(x) \\ &= p(x+1)\cdot q(x+1) - p(x)\cdot q(x) + p(x+1)\cdot q(x) - p(x+1)\cdot q(x) \\ &= p(x+1)\,\triangle\left(q(x)\right) - q(x)\,\triangle\left(p(x)\right) \end{aligned}$$

$\circ$ Si $\triangle(p(x)) = 0$, entonces $\triangle((pq)(x)) = p(x)\,\triangle\left(q(x)\right)$, es decir, para este operador las funciones que cumplen con $\triangle(p(x)) = 0$ son tratadas como contantes.

$$\begin{aligned} \circ\ \triangle\left((p+q)(x)\right) &= (p+q)(x+1) - (p+q)(x) \\ &= p(x+1) + q(x+1) - p(x) - q(x) \\ &= \triangle(p(x)) + \triangle(q(x)) \end{aligned}$$

Luego, reemplazando las ecuaciones (5.6) con nuestro operador Δ tendremos,

$$\triangle\left(a_0(x)\right) = -a_1(x+1)(x+2) - a_2(x+1)(x^2+x+1) \tag{5.7}$$

$$\triangle(a_1(x)) = -a_2(x+1)(2x+1) \tag{5.8}$$

$$\triangle(a_2(x)) = 0 \tag{5.9}$$

Para resolver este sistema nos será de gran utilidad las siguiente proposición.

Proposición 5.1. $\{p(x) \in K(x) \,/\, \triangle\left(p(x)\right) = 0\} = K(x^3 - x)$.

Demostración: Primero notemos que $\{p(x) \in K(x)/\triangle(p(x)) = 0\} = K(x)^{\mathcal{M}}$, donde $\mathcal{M} \in Aut(K(x))$ es el subgrupo generado por $\tau(x) = x + 1$, así $[K(x)^{\mathcal{M}} : K(x)] = |\mathcal{G}| = 3$.

Ademas notemos que:

$\triangle(x^3 - x) = (x+1)^3 - (x+1) - (x^3 - x) = 0$,

y como $\triangle(p(x))$ es un operador lineal, podemos concluir que $K(x^3 - x) \subset \{p(x) \in K(x) \,/\, \triangle\left(p(x)\right) = 0\}$.

Ahora sólo nos restaría demostrar que $[K(x^3 - x) : K(x)] = 3$. Para esto consideremos $m(t) = t^3 - t - (x^3 - x) \in K(x^3 - x)[t]$ en cual es un polinomio irreducible

en $K(x)[t]$ ya que no tiene raices en $K(x^3 - x)$ (todo elemento en $K(x^3 - x)$ tiene grado mayor o igual a 3, por lo tanto no pouede ser raiz). Así,

$$\frac{K(x^3 - x)[t]}{m(t)} = K(x^3 - x)(x) = K(x)$$

Por lo tanto, $[K(x^3-x) : K(x)] = \deg(m) = 3$ y con ello la proposición es cierta. □

Con esta propiedad podemos escribir las ecuaciones (5.9) de la siguiente forma

$$\begin{aligned} \triangle(a_0(x)) &= -a_1(x+1)(x+2) - a_2(x+1)(x^2+x+1) && (5.10)\\ \triangle(a_1(x)) &= -b_0(x)(2x+1) && (5.11)\\ a_2(x) &= b_0(x), && (5.12) \end{aligned}$$

donde $b_0(x) \in K(x^3 - x)$.

También creamos un programa que encuentra soluciones particulares para el operador Δ, como por ejemplo:

$$\begin{aligned} \triangle(x^2) &= 2x+1\\ \triangle(2x^2) &= x+2\\ \triangle(x^4) &= x^3+x+1 \end{aligned}$$

lo que implicará que:

$$\begin{aligned} a_2(x) &= b_0(x) && (5.13)\\ a_1(x) &= -b_0(x)x^2 + b_1(x) && (5.14) \end{aligned}$$

donde $b_0(x), b_1(x) \in K(x^3 - x)$. Luego

$$\begin{aligned} a_1(x+1) &= -b_0(x+1)(x+1)^2 + b_1(x+1)\\ a_1(x+1) &= -b_0(x)(x^2+2x+1) + b_1(x) \end{aligned}$$

Reemplazando esto en la ecuación (5.11) nos queda:

$$\begin{aligned}
\triangle(a_0(x)) &= -(-b_0(x)(x^2+2x+1)+b_1(x))(x+2) - b_0(x)(x^2+x+1) \\
\triangle(a_0(x)) &= b_0(x)(x^3+x^2-x-1) - b_1(x)(x+2) - b_0(x)(x^2+x+1) \\
\triangle(a_0(x)) &= b_0(x)(x^3+x+1) - b_1(x)(x+2)
\end{aligned}$$

lo que implica que:

$$a_0(x) = b_0(x)x^4 + b_1(x)x^2 + b_2(x), \tag{5.15}$$

donde $b_0(x), b_1(x), b_2(x) \in K(x^3 - x)$.

Finalmente, de (5.13), (5.14) y (5.15) podemos concluir que:

$$\begin{aligned}
f(x,y) &= [b_0(x)x^4 + b_1(x)x^2 + b_2(x)] + [-b_0(x)x^2 + b_1(x)]y + [b_0(x)]y^2 \\
&= b_0(x)(x^4 - x^2y + y^2) + b_1(x)(x^2+y) + b_2(x) \\
&= b_0(x)(x^2+y)^2 + b_1(x)(x^2+y) + b_2(x)
\end{aligned}$$

$$\therefore \mathcal{H}^{\mathcal{G}} = K(x^2+y)(x^3-x), \text{ con } y^3 + y - x^4 = 0.$$

5.2. Construyendo códigos Goppa sobre $\mathcal{H}^{\mathcal{G}}$.

En la Sección 2.3 vimos que los códigos Goppa que generaremos son códigos $C_{D,G}$ con $D = p_1 + p_2 + \cdots + p_n$, donde p_i son todos los puntos racionales de $\mathcal{H}^{\mathcal{G}}$ distintos de p_∞, $G = mP_\infty$ y $2g - 2 < m < n$. Por lo tanto nuestra primera tarea será encontrar los puntos racionales de $\mathcal{H}^{\mathcal{G}}$.

Para esto recordemos que en la Observación 4.3 vimos que si P es un lugar racional finito de $\mathcal{H}^{\mathcal{G}}$, entonces los lugares P' de $\mathcal{H}$ que lo extienden tienen grado $f(P)$.

Por otro lado, la ecuación (4.2) nos dice que en nuestro caso

$$e(P) \cdot f(P) \cdot r = p.$$

Esto significa que $f(P)$ sólo puede tomar los valores 1 y p.

Observación 5.1. Si $f(P) = 1$ de la ecuación (4.3) se concluye que $deg(P') = 1$. Además, de las Observaciones 4.5 y 4.4 se deduce que la candidad de lugares racionales de $\mathcal{H}^{\mathcal{G}}$ que son extendidos por lugares racionales en $\mathcal{H}$, son $p^3/ord(\mathcal{G})+1 = p^2+1$.

Observación 5.2. Si $f(P) = p$ de la ecuación (4.2) se concluye que $r = 1$, es decir, cada lugar en $\mathcal{H}$ de grado $f(p) = p$ extiende a un solo lugar racional en $\mathcal{H}^{\mathcal{G}}$.
Además sabemos que $\mathcal{H}^{\mathcal{G}}$ un cuerpo maximal, por lo tanto cumple

$$\#\mathcal{N}(\mathcal{H}^{\mathcal{G}}) = p^2 + 1 + 2g(\mathcal{H}^{\mathcal{G}})p = p^2 + 1 + p^2 - p. \tag{5.16}$$

Por lo tanto $p^2 - p$ lugares racionales en $\mathcal{H}^{\mathcal{G}}$ son extendidos por lugares de grado p en $\mathcal{H}$, a saber, lugares de grado p con $f(P) = p$.

Observación 5.3. Por Lema 4.1, sabemos que los puntos de grado p en $\mathcal{X}_{\mathcal{H}}$ son los puntos cuyas coordenadas se encuentran en $\mathbb{F}_{p^{2p}} - \mathbb{F}_{p^2}$. Estos son todos los puntos $\mathbb{F}_{p^{2p}}-$ racionales[1] de $\mathcal{X}_{\mathcal{H}}$, menos los puntos racionales de $\mathcal{X}_{\mathcal{H}}$. Los que son respectivamente $(p^p)^2 + 1 + 2g(p^p)$ y $p^3 + 1$.

Observación 5.4. Usando la observación anterior podemos concluir que en $\mathcal{X}_{\mathcal{H}}$ hay $(3^3)^2 + 1 + 2 \cdot 3(3^3) - (3^3 + 1) = 864$ puntos de grado 3.

Observación 5.5. Si $f \in \mathcal{H}^{\mathcal{G}}$, entonces

$$f(x, y) = f(x + 1, y + x + 2) = f(x + 2, y + 2x + 2).$$

Por lo tanto, los puntos (α, β), $(\alpha + 1, \beta + \alpha + 2)$ y $(\alpha + 2, \beta + 2\alpha + 2)$ de $\mathcal{X}_{\mathcal{H}}$ son equivalentes en $\mathcal{X}_{\mathcal{H}^{\mathcal{G}}}$, es decir, los puntos de $\mathcal{X}_{\mathcal{H}^{\mathcal{G}}}$ son clases de puntos de $\mathcal{X}_{\mathcal{H}}$.

Así, los $27 = 3^3$ puntos (afines) de grado 1 de $\mathcal{X}_{\mathcal{H}}$ y 864 puntos de grado 3 en $\mathcal{X}_{\mathcal{H}}$ se tranforman en 9 y 288 clases respectivamente en $\mathcal{X}_{\mathcal{H}^{\mathcal{G}}}$. Además el punto infinito

[1] Los puntos $\mathbb{F}_{p^{2p}}-$ racionales de $\mathcal{X}_{\mathcal{H}}$ son los puntos cuyas coordenadas entán en $\mathbb{F}_{p^{2p}} - \mathbb{F}_{p^2}$

de $\mathcal{X}_{\mathcal{H}}$ queda fijo bajo la acción de $\mathcal{G}$, por lo que su clases solo lo contiene al él. Por Observaciones 4.3, 4.4 y 4.5 sabemos que las 8 clases (afines) más la clases del punto infinito son efectivamente puntos racionales de $\mathcal{X}_{\mathcal{H}^{\mathcal{G}}}$, pero de las 288 sólo 6 los son.

Para solucionar este problema y efectivamente encontrar los lugares racionales de $\mathcal{H}^{\mathcal{G}}$ diseñamos un programa que mostraremos y explicaremos en el siguiente capítulo y por ahora sólo mostraremos resultados.

La siguiente tabla nos muestra los 16 representantes de los puntos racionales de $\mathcal{H}^{\mathcal{G}}$ calculados con nuestro programa.

p_1	$(0, 0)$
p_2	$(0, b^5 + b^3 + 2b^2 + b)$
p_3	$(0, 2b^5 + 2b^3 + b^2 + 2b)$
p_4	$(b^5 + b^3 + 2b^2 + b, 2)$
p_5	$(b^5 + b^3 + 2b^2 + b, b^5 + b^3 + 2b^2 + b + 2)$
p_6	$(b^5 + b^3 + 2b^2 + b, 2b^5 + 2b^3 + b^2 + 2b + 2)$
p_7	$(b^5 + b^4, b^4 + 2b^3 + 2b^2 + b + 1)$
p_8	$(b^5 + b^4, b^5 + b^4 + b^2 + 2b + 1)$
p_9	$(b^5 + b^4, 2b^5 + b^4 + b^3 + 1)$
p_{10}	$(2b^5 + 2b^3 + b^2 + 2b, 2)$
p_{11}	$(2b^5 + 2b^3 + b^2 + 2b, b^5 + b^3 + 2b^2 + b + 2)$
p_{12}	$(2b^5 + 2b^3 + b^2 + 2b, 2b^5 + 2b^3 + b^2 + 2b + 2)$
p_{13}	$(2b^5 + 2b^4, b^4 + 2b^3 + 2b^2 + b + 1)$
p_{14}	$(2b^5 + 2b^4, b^5 + b^4 + b^2 + 2b + 1)$
p_{15}	$(2b^5 + 2b^4, 2b^5 + b^4 + b^3 + 1)$
p_∞	$(0 : 1 : 0)$

Una vez resuelto el problema de los puntos racionales de $\mathcal{H}^{\mathcal{G}}$, sólo nos restaría

encontrar los generadores de $\mathcal{L}(G)$ y con esto encontrar la matriz generadora del código $C_{D,G}$ donde $D = p_1, \ldots, p_{15}$ y $G = mP_\infty$.

Recordemos que en el capítulo anterior demostramos que el índice de ramificación $e = e(P'_\infty|P_\infty)$ es 3, con esto más Definición 1.29 tendremos

$$v_{P_\infty}(m(x)) = \frac{v_{P'_\infty}(m(x))}{3} \qquad \forall\, m(x) \in \mathcal{H}^{\mathcal{G}}. \tag{5.17}$$

Con esta igualdad es fácil calcular las valoraciones de las siguientes funciones.

$$\begin{aligned} v_{P_\infty}(x^3 - x) &= v_{P'_\infty}(x^3 - x)/3 = -9/3 = -3 \\ v_{P_\infty}(x^2 + y) &= v_{P'_\infty}(x^2 + y)/3 = -6/3 = -2. \end{aligned}$$

Además, dado que el único polo de $x^3 - x$ y $x^2 + y$ es P_∞, concluimos que:

$$(x^3 - x)_\infty = -3P_\infty \text{ y } (x^2 + y)_\infty = -2P_\infty.$$

Observación 5.6. Usando la Proposición 1.6 se comprueba que el conjunto

$$\{\underbrace{(x^2+y)^i}_{f_{2i}}, \underbrace{(x^2+y)^j(x^3-x)}_{f_{2j+1}} : 0 \leq i, j \leq \lambda\}$$

es linealmente independiente para todo $\lambda \in \mathbb{N}$, ya que

$$v_{P'_\infty}(f_{2i}) = -2i \neq -2j - 3 = v_{P'_\infty}(f_{2j+1}).$$

En particular, el conjunto

$$\{f_{2i}, f_{2j+1} : 2i \leq \lambda, 2j + 3 \leq \lambda\}$$

es una base de $\mathcal{L}(\lambda P'_\infty)$, dado que su cardinalidad es $\lambda = l(\lambda P'_\infty)$.

A modo de ejemplo y por efectos gráficos, sólo mostraremos la matriz generadora del código $C_{D,G}$ para $D = p_1 + \cdots + p_4$ y $G = 3P_\infty$. La observación anterior nos dice que el conjunto $\{1, (x^2 + y), (x^3 - x)\}$ es una base de $\mathcal{G}$, luego la matriz generadora del codigo Goppa $C_{D,G}$ será:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & d^5 + d^3 + 2d^2 + d + 1 & 2d^5 + 2d^3 + d^2 + 2d + 1 \\ 0 & d^5 + d^3 + 2d^2 + d & d^5 + d^3 + 2d^2 + d & d^5 + d^3 + 2d^2 + d \end{pmatrix}$$

5.3. Observación

Consideremos nuevamente el cuerpo de funciones $\mathcal{H}/\mathbb{F}_{q^2}$ $(q \neq 2)$ y $\mathcal{G} = \langle\sigma\rangle$, donde

$$\sigma(x) = x + b,\ b \neq 0,\ \sigma(y) = y + b^q x + c.$$

Es decir, el caso en que no pudimos encontrar específicamente el cuerpo fijo $\mathcal{H}^{\mathcal{G}}$. Después de usar muchas veces el programa para calcular cuerpos fijos, nos dimos cuenta de una cierta relación. Si consideramos $\alpha = \frac{-b^{q-1}}{2}$ y $\beta = \frac{-2c+b^{q+1}}{2b}$, entonces los siguientes dos polinomios en $\mathcal{H}$ quedan fijos bajo la acción de sigma.

$$(x^q - x) \quad (\alpha x^2 + \beta x + y).$$

Comprobemos nuestra afirmación.

- $\sigma(x^q - b^{q-1}x) = (x+b)^q - b^{q-1}(x+b) = (x^q + b^q) - b^{q-1}(x-b) = x^q - b^{q-1}x$
- $\sigma(\alpha x^2 + \beta x + y) = \alpha(x+b)^2 + \beta(x+b) + (y + b^q x + c)$
  $= \alpha x^2 + 2\alpha b x + \alpha b^2 + \beta x + \beta b + y + b^q x + c$
  $= (\alpha x^2 + \beta x + y) + (2\alpha b + b^q)x + (\alpha b^2 + b\beta + c)$
  $= (\alpha x^2 + \beta x + y) + (-b^q + b^q)x + (-b^{q+1}/2 + -c + b^{q+1}/2 + c)$
  $= (\alpha x^2 + \beta x + y)$

Con lo que tendremos la siguiente proposición.

Proposición 5.2. *Si consideramos σ como antes y $\mathcal{G} = \langle\sigma\rangle$, entonces*

$$\mathcal{H}^{\mathcal{G}} = K(x^q - b^{q-1}x, \alpha x^2 + \beta x + y),$$

donde $(\alpha x^2 + \beta x + y)^q + (\alpha x^2 + \beta x + y) = -\frac{b^{1-q}}{2}(x^q - b^{q-1}x)^2 + \beta^q(x^q - b^{q-1}x)$.

Demostración: Primero notemos que

$$(\alpha x^2 + \beta x + y)^q + (\alpha x^2 + \beta x + y) + \tfrac{b^{1-q}}{2}(x^q - b^{q-1}x)^2 - \beta^q(x^q - b^{q-1}x)$$
$$= (\alpha^q x^{2q} + \beta^q x^q + y^q) + (\alpha x^2 + \beta x + y) + \tfrac{b^{1-q}}{2}(x^{2q} - 2b^{q-1}x^{q+1} + b^{2q-2}x^2) - \beta^q(x^q - b^{q-1}x)$$

$= (y^q + y - x^{q+1}) + (\alpha^q + \frac{b^{1-q}}{2})x^{2q} + (\alpha + \frac{b^{q-1}}{2})x^2 + \beta^q(x^q + \beta^{1-q}x) - \beta^q(x^q + -b^{q-1}x)$
$= (y^q + y - x^{q+1})$.

Esta última igualdad se tiene ya que es fácil comprobar que:

$$\left(\alpha^q + \frac{b^{1-q}}{2}\right) = 0, \quad \left(\alpha + \frac{b^{q-1}}{2}\right) = 0 \ y \ \beta^{1-q} = b^{q-1}$$

Por lo tanto,

$$\underset{\sim}{K(x^q - b^{q-1}x, \alpha x^2 + \beta x + y)} \subset \mathcal{H}^{\mathcal{G}} \subset \mathcal{H}.$$

Por otra parte, se cumple que

$$K(x^q - b^{q-1}x, \alpha x^2 + \beta x + y)(x) = K(x, y).$$

Luego, si $n(t)$ denota al polinomio irreducible de x en $K(x^q - b^{q-1}x, \alpha x^2 + \beta x + y)[t]$ tendremos

$$[\mathcal{H} : K(x^q - b^{q-1}x, \alpha x^2 + \beta x + y)] = deg(n(t)),$$

donde $deg(n(t)) \geq q$, pues $[\mathcal{H} : K(x^q - b^{q-1}x, \alpha x^2 + \beta x + y)] \geq [\mathcal{H} : \mathcal{H}^{\mathcal{G}}] = ord(\mathcal{G}) = q$.

Finalmente, usando que el polinomio $m(t) = t^q - b^{q-1}t - (x^q - b^{q-1}x) \in K(x^q - b^{q-1}x, \alpha x^2 + \beta x + y)[t]$ se anula en x concluimos que $[\mathcal{H} : K(x^q - b^{q-1}x, \alpha x^2 + \beta x + y)] = q$ que es lo que queríamos. □

Apéndice A

Sage

A continuación presentaremos el programa realizado para calcular los cuerpos fijos $\mathcal{H}^{\mathcal{G}}$ cuando $\mathcal{G} < \mathcal{A}_1(P'_\infty)$ es un subgrupo cíclico y los lugares racionales de $\mathcal{H}^{\mathcal{G}}$. Continuaremos usando la notación de capítulo 4, en donde denotamos por P' a lugares de $\mathcal{H}$ y por $P = P' \cap \mathcal{H}^{\mathcal{G}}$ a los lugares de $\mathcal{H}^{\mathcal{G}}$.
Dividiremos el programa en dos partes: la primera calculará los representantes de los puntos racionales de $\mathcal{H}^{\mathcal{G}}$ y la segunda encontrará especificamente $\mathcal{H}^{\mathcal{G}}$ para luego encontrar el código Goppa $C_{D,G}$, donde $D = P_1 + \cdots + P_{\mathcal{N}(\mathcal{H}^{\mathcal{G}})-1}$ y $G = \lambda P_\infty$.

A modo de ejemplo mostraremos el programa para $q = 3$.

A.1. Encontrando los puntos racionales de $\mathcal{H}^{\mathcal{G}}$.

Recordemos que en la Observación 4.3 concluimos que si P es un lugar racional de $\mathcal{H}^{\mathcal{G}}$, entonces los lugares P' de $\mathcal{H}$ que lo extienden tienen grado $f(P)$. Además, en el capítulo anterior vimo que si $q = p$, entonces $f(P)$ sólo puede tomar los valores 1 y p.
Por otra parte, en la Observación 5.3 vimos que los puntos de grado p en $\mathcal{X}_{\mathcal{H}}$ son puntos cuyas coordenadas se encuentran en $\mathbb{F}_{q^{2p}} - \mathbb{F}_{q^2}$, es decir, los puntos $\mathbb{F}_{q^{2p}}-$

racionales de $\mathcal{X}_{\mathcal{H}}$, que no son puntos racionales $\mathcal{X}_{\mathcal{H}}$. Esta idea es fundamental para la obtención de puntos racionales de $\mathcal{H}^{\mathcal{G}}$.

1. Definiciones básicas

```
Sage : q=3, l=2*q
Sage : # q es la característica del cuerpo.
Sage : F.<d>=GF(q^l)
Sage : # F:= cuerpo de q^l elementos.
Sage : R.<x, y, z>=F[]
Sage : # R:=F[x,y,z].
```

2. Encontrando los puntos racionales de $\mathcal{H}/K$.

```
Sage : f=y^q*z+y*z^q -x^(q+1)
Sage : # f es el polinomio generador de X_H.
Sage : C=Curve(f)
Sage : # C=X_H definida sobre F_q.
Sage : L=C.rational_points()
```

La lista L *contiene a todos los puntos racionales afines de* $\mathcal{X}_{\mathcal{H}}$ *definida sobre* $\mathbb{F}_{q^{2p}}$.

3. Definiendo los valores b, c del automorfismo $\sigma(x) = x + b$ y $\sigma(y) = y + b^q x + c$, donde $c^q + c = b^{q+1}$.

```
Sage : b=1
Sage : # Le asignamos un valor a b.
Sage : c=F((q+1)/2)
Sage : # Damos un valor a c, de manera que: c^q+c=b^q+1.
```

Consideramos $b = 1$, *ya que si* $b \neq 1$, *entonces el cuerpo fijo resultante será isomorfo al con* $b = 1$.

4. Definiendo la acción σ para los puntos de $\mathcal{X}_{\mathcal{H}}$.

```
Sage : def g(x):
return C(([x[0]+b*x[2],x[1]+b^q*x[0]+c*x[2],x[2]]))
Sage : def frob(x):
return C(([x[0]^3,x[1]^3,x[2]^3]))
```

La primera función es la acción el grupo $\mathcal{G}$ y la segunda es la acción de automorfismo de Frobenius sobre $\mathbb{F}_q$.

5. Definiendo los elementos de $\mathcal{X}_{\mathcal{H}^{\mathcal{G}}}$.

```
Sage : L1=[]
Sage : for k in L:
P=[k,g(k),g(g(k))]
P.sort()
if not P in L1:
L1.append(P)
```

La lista `L1` *contiene las clases de puntos afines de $\mathcal{X}_{\mathcal{H}^{\mathcal{G}}}$ provenientes de los puntos racionales afines definidos en la lista* `L`.

6. Encontrando las clases de todos los puntos racionales de $\mathcal{X}_{\mathcal{H}^{\mathcal{G}}}$.

```
Sage : L2=[]
Sage : for P in L1:
Q=[frob(frob(k)) for k in P]
Q.sort()
if P==Q:
L2.append(P)
```

La lista `L2` *contiene a todas las clases de puntos racionales de $\mathcal{X}_{\mathcal{H}^{\mathcal{G}}}$.*

7. Encontrando los representantes de las clases de puntos racionales de $\mathcal{X}_{\mathcal{H}^{\mathcal{G}}}$.

```
Sage : L3=[L2[i][0] for i in range(0,2*q^2+1-q)]
```

La lista L3 *contiene a todos los representantes de las clases de puntos racionales de* $\mathcal{X}_{\mathcal{H}^{\mathcal{G}}}$*, es decir a los* $2q^2 - q + 1$ *puntos racionales de* $\mathcal{X}_{\mathcal{H}^{\mathcal{G}}}$.

A.2. Encontrando $\mathcal{H}^{\mathcal{G}}$.

Para encontrar $\mathcal{H}^{\mathcal{G}}$ consideremos $f \in \mathcal{H}$ de la forma

$$f(x,y) = a_0(x) + a_1(x) + \cdots + a_{q-1}(x)y^{q-1}.$$

Luego para que f pertenezca a $\mathcal{H}^{\mathcal{G}}$ se debe cumplir que $\sigma(f) = f$, donde si denotamos $a_i(\sigma(x)) = a_i'(x)$ tendremos

$$\sigma(f) = a_0'(x) + a_1'(x)\sigma(y) + \cdots + a_{q-1}'(x)(\sigma(y))^{q-1}.$$

Observemos que $gr_y(\sigma(y)^i) = i$, por lo que podemos reordenar $\sigma(f)$ como

$$\sigma(f) = p_0(x) + p_1(x)y + \cdots + p_{q-1}(x)y^{q-1},$$

donde p_i depende de x, pero también se puede hacer depender de $a_0'(x), \ldots, a_{q-1}'(x)$ y no es difícil comprobar que

$$\begin{aligned}
p_0(x) &= a_0'(x) + a_1'(x)m_{0,1}(x) + \cdots + a_{q-1}'(x)m_{0,q-1}(x) \\
p_1(x) &= a_1'(x) + a_1'(x)m_{1,2}(x) + \cdots + a_{q-1}'(x)m_{1,q-1}(x) \\
&\vdots \\
p_{q-2}(x) &= a_{q-2}'(x) + a_{q-1}'(x)m_{q-2,q-1} \\
p_{q-1}(x) &= a_{q-1}'(x)
\end{aligned}$$

Luego, como queremos $\sigma(f) = f$ nos quedará

$$\begin{aligned}
a_0(x) &= a_0'(x) + a_1'(x)m_{0,1}(x) + \cdots + a_{q-1}'(x)m_{0,q-1}(x) \\
a_1(x) &= a_1'(x) + a_1'(x)m_{1,2}(x) + \cdots + a_{q-1}'(x)m_{1,q-1}(x) \\
&\vdots \\
a_{q-2}(x) &= a_{q-2}'(x) + a_{q-1}'(x)m_{q-2,q-1} \\
a_{q-1}(x) &= a_{q-1}'(x)
\end{aligned}$$

Lo que es equivalente a

$$\begin{aligned}
\triangle(a_0(x)) &= -[a'_1(x)m_{0,1}(x) + \cdots + a'_{q-1}(x)m_{0,q-1}(x)] \\
\triangle(a_1(x))- &= -[a'_1(x)m_{1,2}(x) + \cdots + a'_{q-1}(x)m_{1,q-1}(x)] \\
&\vdots \\
\triangle(a_{q-2}(x)) &= -[a'_{q-1}(x)m_{q-2,q-1}] \\
\triangle(a_{q-1}(x)) &= 0
\end{aligned}$$

Para simplificar un poco los calculos (al programarlos) definiremos

$$M = \begin{pmatrix}
1 & m_{0,1} & \cdots & \cdots & m_{0,q-1} \\
0 & 1 & m_{1,2} & \cdots & m_{1,q-1} \\
\vdots & 0 & \ddots & \ddots & \vdots \\
\vdots & & \ddots & 1 & m_{q-2,q-1} \\
0 & \cdots & \cdots & 0 & 1
\end{pmatrix}$$

Luego si $M[i]$ es la fila $i-$ésima de M, tendremos que

$$\triangle(a_{q-i}(x)) = -M[-i](a'_1, \ldots, a'_{q-1}) \quad \forall\, i = 0, \ldots q-1$$

Con este argumento revisemos el programa

1. Definiciones básicas

```
Sage : q=3
Sage : # q es la caracteristica del cuerpo
Sage : F.<aa>=GF(q^2)
Sage : # F es el cuerpo de q^2 elementos.
Sage : b=1
Sage : c=F((q+1)/2)
```

La variables `b` *y* `c` *cumplen con* `c^q +c^- b^(q+1)=0`.

2. Definiciones de variables

```
Sage : bes=['x','y','a']+['b'+str(k)for k in range(q)]
Sage : K=PolynomialRing(F,bes)
Sage : for k in range(q+3):
Sage : bes[k]=K.gen(n=k)
Sage : a=K.gen(n=2)
Sage : y=K.gen(n=1)
Sage : x=K.gen(n=0)
```

3. Definiendo la función AntiD=$\triangle^{-1}$.

```
Sage : def D(p): return p.subs(x=x+1)-p
Sage : # Usaremos B=x^0,..,x^r como bases de F[x^0,..,x^r]
Sage : def AntiD(p):
r=q^2
dd=[D(x^k) for k in range(r)]
m=matrix([[d.coefficient(x:k)for k in range(r)]for d in
dd])
v=vector([p.coefficient(x:k)for k in range(r)])
w=m.solve_left(v)
return sum(K(w[k])*x^k for k in range(r))
```

dd contiene los coeficientes de $D(x^i)$, m es la matriz de la función D de B en B y v contiene los coeficientes de p en la base B. Luego, encontrando los coeficientes de z tal que D(z)=v, obtenemos z.

4. Definiendo la matriz M.

```
Sage : h = sum(a^(i+1)*y^i for i in range(q))
Sage : # h es un polinomio cualquiera en H
Sage : f=h.subs(y=y+b^q*x+c)
Sage : # aplico σ(y) a h
Sage : a1=[f.coefficient(y:i) for i in range(q)]
Sage : # Encuentro los coef (dependiendo de a^k) de cada
y^i
Sage : M=[[d.coefficient(a^(j+1)) for
j in range(q)]for d in a1]
Sage : matrix(M)
```

5. Encontrando las soluciones

```
Sage : def Mult(p,r): return sum(p[i]*r[i] for i in
range(q))
Sage : B=[K.gen(n=k) for k in range(3,q+3)]
Sage : bb=[B[k] for k in range(q)]
Sage : a_sol=[0 for i in range(q)]
Sage : a_sol[q-1]=bb[0]
# a nuestra última solución la llamamos a_0(x)=b0
Sage : A=[0 for i in range(q)]
a=[0 for i in range(q)]
Sage : a[q-1]=a_sol[q-1]
Sage : A[q-1]=a_sol[q-1].subs(x=x+b)
Sage : for k in range(2,q+1):
a_sol[q-k]=-AntiD(Mult(A,M[-k]))+bb[k-1]
a[q-k]=a_sol[q-k]
A[q-k]=a[q-k].subs(x=x+1)
```

La lista a_sol contendrá las soluciones a_0(x),..,a_q-1(x)

6. Definiendo los generadores de $\mathcal{L}(G)$, para $G = \lambda P'_\infty$.

El paso anterior nos entrega los generadores de $\mathcal{H}^G$, que en el caso de $p = 3$ son $(x^3 - x)$ y $(x^2 + y)$. Esta información es suficiente para encontrar los generadores de $\mathcal{L}(G)$ si $G = \lambda P'_\infty$, ya que estos son combinaciones de los anteriores polinomios (ver Observación 5.6).

Además, recordemos si $\lambda \geq 2g - 1$, entonces $l(G) = deg(G) + 1 - g$.

A continuación encontraremos los generadores de $\mathcal{L}(G)$ cuando $G = 3P_\infty$.

```
Sage : def e1(x,y): return x^2+y
Sage : def e2(x,y): return x^q-x
Sage : # e1 y e2 son los generadores de H^G.
Sage : genus= (q-1)/2
Sage : # genus es el género de H^G.
Sage : # Sea G=sP_infty, s>=2genus-1 y l(D)=s+1-(q-1)/2
Sage : s=3
Sage : lD=s+1-(q-1)/2
Sage : s1=integer_floor(lD/2)
Sage : s2=[]
Sage : for i in range(s):
if 2*i+3<=lD:
s2=s2+[i]
Sage : I1=[e2(x,y)^i for i in range(s1+1)]
Sage : I2=[e1(x,y)*e2(x,y)^j for j in s2]
Sage : I=[e2(x,y)^0]
Sage : for i in range(1,s1+1):
if i-1 in s2:
I=I+[I1[i], I2[i-1]]
if len(I1)-len(I2)>1:
I=I+[I1[s1]]
```

La lista I contiene a todos los generadores de `L(sP_infty)`.

7. Creando los código Goppa $C_{D,G}$ para $G = \lambda P_\infty$ y $D = p_1 + \cdots + p_n$.

```
Sage : infty= L3[1]
Sage : L3.remove(infty)
Sage : # Sacamos al punto infinito de la lista L3
Sage : n=4
Sage : Definimos el largo del codigo
Sage : L4=[L3[i] for i in range(n)]
Sage : # Definiendo D=p1+...+pn
Sage : m=matrix(F1,[[f(k[0],k[1],1) for k in L4] for f in
I3])
Sage : C=m.row_space()
Sage : C=LinearCode(m)
Sage : C.length(), C.dimension()
```

`C` es el código Goppa asociado a $D = p_1 + \cdots + p_4$ y $G = 3P_\infty$, y `m` es su matriz generadora.

Bibliografía

[1] HENNING STICHTENOTH, *Algebraic Function Fields and Codes*, 2 ed., Springe, Berlin, 2009.

[2] WILLIAM FULTON, *Curvas algebraicas*, Reverté, España, 2005.

[3] ARNALDO GARCIA, HENNING STICHTENOTH AND CHAO-PING XING, *On Subfields of the Hermitian Function Field*, Compositio Mathematica (2000), no. 120, 137–170.

[4] MASSIMO GIULIETTI, *Notes on Algebraic-Geometric codes*, Dipartimento di Matematica, Universita degli Studi di Perugia, Perugia, Italy.

[5] CARLOS MUNUERA GÓMEZ Y FERNANDO TORRES, *Sobre curvas algebraicas y códigos correctores*, Gaceta de la Real Sociedad Matematica Espaõla, ISSN 1138-8927 (2006), no. 1, 203–222.