UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN CIENCIAS MATEMÁTICAS Y DE LA ESPECIALIZACIÓN EN ESTADÍSTICA APLICADA.

CONSTRUCCIÓN Y DECODIFICACIÓN DE CÓDIGOS HERMITIANOS

TESIS
QUE PARA OPTAR POR EL GRADO DE:
MAESTRA EN CIENCIAS

PRESENTA:
ANAYANZI DELIA MARTÍNEZ HERNÁNDEZ

DIRECTOR DE LA TESIS
DR. OCTAVIO PÁEZ OSUNA
Posgrado en Ciencias Matemáticas

MÉXICO, D. F. NOVIEMBRE 2015

Índice general

Introducción

La teoría de Códigos Correctores de Errores tiene como uno de sus objetivos la creación de listas finitas de *palabras* a partir de un *alfabeto* finito de tal forma que al ser *transmitidas* sea posible la detección y corrección de errores. Debido al avance de la tecnología se requieren códigos que nos permitan detectar y corregir la mayor cantidad de errores pero a su vez, que no sean costosos en términos de almacenamiento o cálculos.

A la lista finita de palabras mencionada arriba la reconocemos como *código*. Específicamente, llaremos *código* a un subespacio no trivial del espacio vectorial de dimensión n, $\mathbb{F}_q^n$, donde $\mathbb{F}_q$ representa al campo finito con q elemento. Debido a la naturaleza de esta definición se utilizan herramientas del álgebra para la creación y el manejo de estas estructuras. A través de las últimas cinco décadas y aprovechando diferentes propiedades algebraicas, se ha logrado la clasificación de algunos códigos. En este trabajo trataremos con un tipo de códigos llamados *Códigos Geométricos*.

El punto de partida de este trabajo son los campos algebraicos de funciones. Estos campos contienen un tipo de ideales llamados *lugares* con los cuales se define un grupo abeliano llamado *grupo de divisores*. A cada divisor le podemos asociar un espacio en particular llamado *Espacio de Riemann Roch*. Estos espacios son fundamentales en la construcción de los códigos geométricos.

Por otro lado, la corrección y detección de errores en un código serán posibles sólo si existe un algoritmo establecido para ello. La estructura de dichos algoritmos (llamados *algoritmos de decodificación*) dependen de las propiedades de cada código. Se desea que dicho algoritmo nos permita corregir la mayor cantidad posible de errores.

El principal punto de interés de este trabajo es el de estudiar los resultados presentados en *On a decoding algorithm for codes on maximal curves* [11], los cuales refieren a un algoritmo de decodificación establecido por Alexei N. Skorobogatov que se utiliza para corrección y detección de errores en los códigos geométricos.

El primer capítulo contiene una breve referencia acerca de los principales conceptos y resultados utilizados para comprender las ideas desarrolladas en [11]. Se omiten algunas demostraciones pero pueden ser consultadas en el primer y tercer capítulo de [15].

En la segunda parte de este trabajo se presentan conceptos básicos en la Teoría de Códigos Correctores de Errores, se dan algunos ejemplos y se expone explícitamente la construcción de los Códigos Geométricos. Para finalizar, se trata el proceso de la decodificación de estos códigos y se presentan problemas abiertos asociados a éstos.

Notación

A menos que se indique algo diferente, se utilizará la siguiente notación:

- K denotará un campo aribitrario.
- H^n será el n-producto cartesiano de H.
- $\mathbb{F}_q$ se utilizará para referirse al campo finito de q elementos tal que $q = p^r$ con p un elemento primo y r un entero positivo.
- $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ será el grupo multiplicativo de $\mathbb{F}_q$.
- $[K : F]$ representa el grado de la extensión K/F.

Capítulo 1

Preliminares

El objetivo de este capítulo es presentar las definiciones y resultados fundamentales para la construcción de Códigos Geométricos utilizados en este trabajo. Si se requiere mayor profundidad de éstos, la referencia base es [15]. Comenzaremos con el concepto de Campo de funciones algebraico y a partir de este, obtendremos algunos espacios con estructuras interesantes, por ejemplo, el grupo de divisores o los espacios de Riemann-Roch.

Definición 1.0.1. *Sea K un campo arbitrario y sea $F \supseteq K$ una extensión algebraica finita de $K(x)$, para algún elemento $x \in F$ trascendente sobre K. A dicha extensión F la denotaremos como F/K y la llamaremos* ***campo de funciones algebraico de una variable sobre*** *K. Por brevedad haremos referencia a F/K como* ***campo de funciones****.*

Observación 1.0.1. Hacemos las siguientes observaciones acerca de los elementos de F:

- Elementos algebraicos: al conjunto $\tilde{K} := \{z \in F | z \text{ es algebraico sobre } K\}$ lo llamaremos el **campo de constantes** de F/K. Se tiene que $K \subseteq \tilde{K} \subseteq F$ y $F/\tilde{K}$ es a su vez un campo de funciones sobre $\tilde{K}$.

- Elementos trascendentes: un elemento $z \in F$ es trascendente sobre K si y solamente si $[F : K(z)] < \infty$.

1.1. Anillos de valoración y lugares

Definición 1.1.1. *Diremos que el anillo $\mathcal{O} \subset F/K$ es de **valoración** (o de valuación) si cumple que:*

(1) $K \subsetneq \mathcal{O} \subsetneq F$ y

(2) para cualquier elemento $z \in F, z \in \mathcal{O}$ ó $z^{-1} \in \mathcal{O}$.

Observación 1.1.1. Si $\mathcal{O}$ es de valoración de F/K el **anillo de unidades de $\mathcal{O}$** será el conjunto: $\mathcal{O}^* = \{z \in \mathcal{O} \mid \text{existe } w \in \mathcal{O} \text{ tal que } zw = 1\}$.

Proposición 1.1.1. *(Propiedades de los anillos de valoración.) Si $\mathcal{O}$ es un anillo de valoración de F/K, entonces:*

(a) El anillo $\mathcal{O}$ es local, es decir $\mathcal{O}$ tiene un único ideal máximal $P := \mathcal{O} \backslash \mathcal{O}^*$;

(b) para $x \in F$, $x \neq 0$, $x \in P$ si y solamente si $x^{-1} \notin \mathcal{O}$;

(c) para el campo $\tilde{K}$ de constantes de F/K tenemos que $\tilde{K} \subseteq \mathcal{O}$ y $\tilde{K} \cap P = \{0\}$.

Demostración.

(a) Primero veremos que $P := \mathcal{O}\backslash\mathcal{O}^*$ es un ideal de $\mathcal{O}$. Sea $x \in P$ y $z \in \mathcal{O}$. Si $xz \in \mathcal{O}^*$ entonces x sería una unidad contradiciendo la hipótesis de que $x \in P$, por lo tanto $xz \notin \mathcal{O}^*$ de donde $xz \in P$. Sean $x, y \in P$ y $a = xy^{-1}$. Sabemos que $a \in F$ y que se cumple alguna de las siguientes condiciones: $a \in \mathcal{O}$ o $a^{-1} \in \mathcal{O}$.

Si suponemos que se cumple $a \in \mathcal{O}$ entonces tendremos que $a+1 \in \mathcal{O}$ y utilizando el párrafo anterior, obtenemos que $y(a+1) \in P$, pero por otro lado $y(a+1) = y + x$, por lo que $y + x \in P$. Por otro lado, si suponemos que solamente se cumple la condición, $a^{-1} \in \mathcal{O}$, siguiendo un procedimiento análgo al anterior, obtendríamos que $(a^{-1}+1)x = y + x \in P$. Por lo tanto, P es un ideal del anillo $\mathcal{O}$.

(b) Si $x \in P$ entonces $x \in \mathcal{O}$ y $x \notin \mathcal{O}^*$, de donde $x^{-1} \notin \mathcal{O}$. Además, si $x^{-1} \notin \mathcal{O}$ entonces $x \in \mathcal{O}$, de donde $x \in P$.

(c) Sea $z \in \tilde{K}$. Si suponemos que $z \notin \mathcal{O}$ entonces $z^{-1} \in \mathcal{O}$. Por otro lado, como z^{-1} es también un elemento algebraico sobre K existen $a_r, ..., a_1 \in K$ tales que:

$$a_r(z^{-1})^r + a_{r-1}(z^{-1})^{r-1} + ... + a_1(z^{-1}) + 1 = 0$$

de donde obtenemos:

$$z^{-1}(a_r(z^{-1})^{r-1} + a_{r-1}(z^{-1})^{r-2} + ... + a_1) = -1,$$

por lo que $z = -(a_r(z^{-1})^{r-1} + a_{r-1}(z^{-1})^{r-2} + ... + a_1)$. Esto indica que $z \in K[z^{-1}]$ y además sabemos que $K[z^{-1}] \subset \mathcal{O}$. Así, $z \in \mathcal{O}$.

Que $\tilde{K} \cap P = \{0\}$ se sigue de que $\tilde{K} \subset \mathcal{O}$ y si $z \in \tilde{K}$ entonces $z^{-1} \in \tilde{K}$. □

Observación 1.1.2. Veamos dos cotas útiles para $[F : K(x)]$:

- Sea $\mathcal{O}$ un anillo de valoración de F/K, P su único ideal maximal y $0 \neq x \in P$. Por la proposición anterior $x \neq 0$ y $x \in P$ implica que $x \notin \tilde{K}$, es decir, x es un elemento trascendente y (Observación 1.0.1) obtenemos que $[F : K(x)] < \infty$.

- Sean $x_1, ..., x_n \in P$ tales que $x_1 = x$ y $x_i \in x_{i+1} \in P$ con $i = 1, ..., n-1$. Los elementos x_i serán linealmente independientes, por lo que $n \leq [F : K(x)]$.

Proposición 1.1.2. *Sea $\mathcal{O}$ un anillo de valoración de F/K. Si P es el anillo maximal de $\mathcal{O}$ entonces P es un ideal principal.*

Demostración. Supondremos que P no es un ideal principal. Escogemos un elemento $x_1 \in P$ tal que $0 \neq x_1$. Como $x_1\mathcal{O} \neq P$ entonces debe existir $x_2 \in P \backslash x_1\mathcal{O}$ por lo que $x_2x_1^{-1} \notin \mathcal{O}$ de donde $x_2^{-1}x_1 \in P$ por lo tanto, $x_1 \in x_2P$. Si hacemos inducción sobre un número infinito de elementos $x_1, x_2, ... \in P$ tales que $x_i \in x_{i+1}P$ para cualquier $i \geq 1$ llegamos a una contradicción con las cotas establecidas para $[F : K(x)]$ hechas en la observación 1.1.2. □

Teorema 1.1.1. *Si $\mathcal{O}$ un anillo de valoración discreta F/K y P el anillo maximal de $\mathcal{O}$ tal que $P = t\mathcal{O}$, entonces:*

(a) cada $0 \neq z \in F$ tiene una representación única $z = t^n u$, para alguna $n \in \mathbb{Z}$ y $u \in \mathcal{O}^*$;

(b) $\mathcal{O}$ es dominio de ideales principales. Más aún, si $P = t\mathcal{O}$ y $\{0\} \subsetneq I \subseteq \mathcal{O}$ entonces $I = t^n\mathcal{O}$ para alguna $n \in \mathbb{N}$.

La demostración de este teorema puede encontrarse en [15].

Definición 1.1.2. *(a) Llamamos **lugar** P de F/K al único ideal maximal P de algún anillo de valoración $\mathcal{O}$.*

(b) A todo elemento $t \in F$ tal que $P = t\mathcal{O}$ lo nombramos ***parámetro local de P****.*

(c) Al conjunto de lugares del campo de funciones F/K, lo denotaremos como $\mathbb{P}_F$.

En el teorema 1.1.2 veremos una condición suficiente para que un campo F/K contenga al menos un lugar P.

Observación 1.1.3. Un anillo de valoración $\mathcal{O}$ queda determinado por su lugar P, esto es $\mathcal{O} = \{z \in F \mid z^{-1} \notin P\}$. Siendo así, denotaremos como $\mathcal{O}_P$ al anillo de valoración del lugar P.

La siguiente definición permite dar una nueva interpretación a los elementos de $\mathbb{P}_F$ en términos de funciones cuyo dominio será el campo F y la imagen estará contenida en el conjunto $\mathbb{Z} \cup \{\infty\}$.

Definición 1.1.3. *Sea v una función tal que $v : F \mapsto \mathbb{Z} \cup \{\infty\}$. Diremos que v es* ***valoración discreta*** *si cumple las siguientes propiedades:*

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

(2) $v(zw) = v(z) + v(w), \ \forall\ z, w \in F$.

(3) $v(a) = 0, \ \forall\ 0 \neq a \in K$.

(4) $v(z + w) \leq mín\{v(z), v(w)\}$.

(5) Existe algún elemento $z \in F$ tal que $v(z) = 1$.

Observación 1.1.4. Para un campo de funciones F/K y $P \in \mathbb{P}_F$ definimos la valoración v_P de la siguiente manera: sea t un parámetro local de P, para cada $P \in \mathbb{P}_F$ asociamos la función: $v_P : F \mapsto \mathbb{Z} \cup \infty$ dada por

$$v_P := \begin{cases} n & \text{si } z \neq 0; \\ \infty & \text{si } z = 0. \end{cases}$$

Esta función cumple con ser una valoración discreta.

Definición 1.1.4. *Sea $P \in \mathbb{P}_F$.*

*(a) Al campo $F_P := O_P/P$ lo llamaremos el **campo residual del lugar P**.*

*(b) El **grado de un lugar** estará definido por $[F_P : K]$.*

(c) Al mapeo $x(P) : F \mapsto F_P \cup \{\infty\}$, dado por

$$x(P) = \begin{cases} x + P & x \in O_P; \\ \infty & x \in F \backslash O_P \end{cases}$$

*le llamaremos **mapeo natural** o canónico.*

Definición 1.1.5. *Sea $z \in P$ y $P \in \mathbb{P}_F$. Decimos que P es un **cero** de z si $V_P(z) > 0$. Si $V_P(z) = m > 0$ decimos que P es un **cero de orden m**. Si $V_P(z) < 0$, entonces diremos que P es un **polo** de z . Si $V_P(z) = -m$, P será un **polo de orden m**. También podemos decir que z tiene un cero (polo) de orden m en P si $v_P(z) = m > 0$ ($v_P(z) = m > 0$).*

Teorema 1.1.2. *Sea F/K un campo algebraico de funciones y R un subanillo de F con $K \subseteq R \subseteq F$. Supongamos que $\{0\} \neq I \subsetneq R$ es un ideal propio de R, entonces existe un lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ y $R \subseteq O_P$.*

Demostración. Sea $\mathcal{F} := \{S \mid S$ es un subanillo de F con $R \subseteq S$ y $IS \neq S\}$ donde por definición $IS = \{\sum a_v s_v | a_v \in I, s_v \in S\}$. Primero notamos que $\mathcal{F}$ es un conjunto no vacío pues $R \subseteq \mathcal{F}$. Queremos demostrar que $\mathcal{F}$ es un conjunto ordenado de manera inductiva por la inclusión por lo que supondremos que $\mathcal{H}$ es un subconjunto de $\mathcal{F}$ totalmente ordenado. Podemos observar que $T := \cup\{S|S \in \mathcal{H}\}$ es un subanillo de $\mathcal{F}$ con $R \subseteq T$. Ahora, para comprobar que $T \in \mathcal{F}$ es necesario verificar que $IT \neq T$ por lo que supondremos que el enunciado es falso. Si $IT = T$, entonces $1 = \sum_{v=1}^{n} a_v s_v$ con $a_v \in I$ y $s_v \in T$. Como $\mathcal{H}$ es un conjunto totalmente ordenado, existe una $S_0 \subset \mathcal{H}$ tal que $s_1, s_2, ..., s_n \in S_0$, por lo que $1 = \sum_{v=1}^{n} a_v s_v \in IS_0$ lo cual es una contradicción.

Utilizando el Lema de Zorn, tenemos que $\mathcal{F}$ tiene un elemento maximal, es decir, existe un anillo $O \subseteq F$ tal que $R \subseteq O \subseteq F$, con $IO \neq O$, siendo O un anillo maximal con respecto a estas propiedades. Falta demostrar que O es un anillo de valoración para el campo de funciones F/K.

Como $I \neq \{0\}$ y $IO \neq O$ es inmediato que $O \subsetneq F$ y $I \subseteq O \backslash O^*$. Supongamos que existe un elemento $z \in F$ tal que $z \notin O$ y $z^{-1} \notin O^*$. Entonces $IO[z] = O[z]$ y $IO[z^{-1}] = O[z^{-1}]$ y podemos dar elementos $a_0, ..., a_n, b_1, ..., b_m \in IO$ con:

$$1 = a_0 + a_1 z + \ldots + a_n z^n \qquad \text{y} \tag{1.1}$$

$$1 = b_0 + b_1 z^{-1} + \ldots + b_m z^{-m}. \tag{1.2}$$

Como m y n son enteros positivos, podemos suponer sin pérdida de generalidad que m y n son minimales y que $m \leq n$. Multiplicando 1.1 por $1 - b_0$ y 1.2 por $a_n z^n$, obtenemos:

$$\begin{aligned} 1 - b_0 &= (1 - b_0)a_0 + (1 - b_0)a_1 z + \ldots + (1 - b_0)a_n z^n \qquad \text{y} \\ 0 &= (b_0 - 1)a_n z^n + b_1 a_n z^{n-1} + \ldots + b_m a_n z^{n-m} \end{aligned}$$

Sumando estas dos últimas ecuaciones obtenemos una ecuación de la siguiente forma $1 = c_0 + c_1 z + ... + c_{n-1} z^{n-1}$ con coeficientes $c_i \in IO$ pero esto contradice la minimalidad de 1.1. Con esto hemos probado que para cualquier $z \in F$ sucede que $z \in O$ o $z^{-1} \in O$ por lo que O es un anillo de valoración. □

Como consecuencia del teorema anterior tenemos el siguiente resultado el cual indica que $\mathbb{P}_F \neq \emptyset$.

Corolario 1.1.1. *(El conjunto de lugares de F/K es no vacío.) Sea F/K un campo de funciones y $z \in F$ un elemento trascendente sobre K, entonces z tiene al menos un cero y al menos un polo.*

Demostración. Para poder aplicar el teorema anterior consideramos el anillo $R = K[z]$ y el ideal $I = zK[z]$. El teorema nos indica que existe un lugar $P \in \mathbb{P}_F$ con $z \in P$, es decir, P es un cero de z. El mismo argumento muestra que z^{-1} tiene un cero $Q \in \mathbb{P}_F$, por lo que Q es un polo de z. □

El siguiente resultado es conocido como **Teorema de Aproximación Débil**. Este teorema también es llamado *Teorema de Independencia*. La demostración de este teorema puede encontrarse en [15].

Teorema 1.1.3. *Sean $P_1, \ldots, P_n$ lugares de F/K diferentes dos a dos, $\gamma_1, ..., \gamma_n \in \mathbb{Z}$ y $x_1, ..., x_n \in F$, entonces existe $x \in F$ tal que $v_{P_i}(x - x_i) = \gamma_i$.*

Observación 1.1.5. Una consecuencia importante de este teorema es que el conjunto de lugares $\mathbb{P}_F$ de F/K es infinito.

Corolario 1.1.2. *Todo campo de funciones F/K tiene un número infinito de lugares.*

Demostración. Supondremos que solamente existe una cantidad finita de lugares, digamos $P_1, \ldots, P_n$. Utilizando el teorema de Aproximación Débil, sabemos que podemos encontrar un elemento $x \in F$ tal que $v_{P_i} > 0$ para todo $i = 0, \ldots, n$, esto quiere decir que x tiene ceros por lo que x es un elemento transcendente sobre K, pero esto contradice el corolario 1.1.1 pues tendríamos un elemento trascendente sobre K sin polos. □

Proposición 1.1.3. *Sea F/K un campo de funciones y $P_1, \ldots, P_r$ los ceros de $x \in F$, entonces:*

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

La demostración de esta proposición puede encontrarse en [15].

Corolario 1.1.3. *En un campo de funciones F/K cualquier elemento $0 \neq x \in F$ tiene solamente un número finito de polos y un número infito de ceros.*

Demostración. Si x es una constante, entonces x no tiene ceros ni polos. Si x es un elemento trascentente, la proposición anterior nos muestra que la cantidad de ceros de x es menor o igual a $[F : K(x)]$ y esta es una cantidad finita (1.0.1). Se utiliza el mismo argumento para decir que x^{-1} tiene una cantidad finita de ceros, es decir, x tiene una cantidad finita de polos. □

Observación 1.1.6. Como resumen de esta sección, remarcamos los siguientes resultados:

- $\mathbb{P}_F \neq \emptyset$;
- cualquier campo de funciones tiene un número infinito de lugares y
- cualquier elemento $0 \neq x \in F$ tiene solamente un número finito de polos y un número infito de ceros.

1.2. Divisores y espacios $\mathcal{L}(A)$

En esta sección se presenta el concepto de divisor. Utilizando la notación aditiva, diremos que el grupo de divisores para un campo algebraico de funciones, es el grupo libre generado por sus lugares. Después de tratar algunas propiedades de los elementos de dicho conjunto, se dará la definición de los espacio de Riemann Roch asociado a un divisor. Estos espacios son subconjuntos de los campos de funciones y representan una pieza medular para la teoría de códigos geométricos.

Definición 1.2.1. *Para cualquier campo de funciones F/K, definimos un **divisor D** como la suma formal:*

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

con $n_P \in \mathbb{Z}$ y $n_P = 0$, excepto en un número finito de lugares. Al conjunto de divisores de F/K lo denotaremos por $\mathcal{D}_F$. Definimos la suma entre divisores de la siguiente manera:

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

Definiremos un elemento identidad como:

$$0 := \sum_{P \in \mathbb{P}_F} r_P P, \quad con \quad r_P = 0 \ \forall P \in \mathbb{P}_F.$$

Observación 1.2.1. Observamos que definida como en el párrafo anterior, la suma de divisores es cerrada y asociativa. Dado que $n_P \in \mathbb{Z}$, entonces se puede formar el inverso aditivo de cada elemento D y con esto tenemos que $\mathcal{D}_F$ tiene estructura de grupo. De hecho, es un grupo abeliano.

Definición 1.2.2. *Sean $Q \in \mathbb{P}_F$, $D = \sum n_P P \in \mathcal{D}_F$ definimos:*

(a) la valoración de D en el lugar Q como $\boldsymbol{v_Q(D)} := n_Q$;

(b) el grado del divisor D como $\boldsymbol{grado(D)} := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot grado\ P$;

(c) el soporte del divisor D como $\boldsymbol{soporte(D)} := \{P \in \mathbb{P}_F | n_P \neq 0\}$.

Observación 1.2.2. Una característica de $\mathcal{D}_F$ es que existe un orden parcial en sus elementos: $D \leq D' \iff n_P \leq n'_P \ \forall \in P$.

Es posible definir un divisor a partir de un elemento x de F asociando a cada lugar P la valoración $v_P(x)$. La construcción natural para estos divisores es la descrita en la siguiente definición. Cabe señalar que en la sección anterior se dieron resultados que permiten saber que estos divisores quedan bien definidos.

Definición 1.2.3. *Sea $Z_x := \{P \in \mathbb{P}_F | P \text{ es cero de } x\}$ y $N_x := \{P \in \mathbb{P}_F | P \text{ es polo de } x\}$. Para cada $x \in F$ vamos a definir los siguientes divisores. Sea $x \in F$. Definimos:*

(a) al ***divisor de ceros de x*** *como* $\boldsymbol{(x)_0} := \sum_{P \in Z_x} v_P(x)P$;

(b) al ***divisor de polos de x*** *como* $\boldsymbol{(x)_\infty} := \sum_{P' \in N_x} (-v_{P'})(x)P'$ *y*

(c) al ***divisor principal de x*** *como* $\boldsymbol{(x)} := (x)_0 - (x)_\infty$.

Observación 1.2.3. El divisor principal de $x \in F$ puede ser escrito de la siguiente manera:

$$(x) = \sum_{P \in \mathbb{P}_F} v_P(x)P$$

Definición 1.2.4. *(a) Al conjunto de divisores principales de F/K lo denotaremos como $\mathcal{P}_F$. Claramente $\mathcal{P}_F$ es un subgrupo de $\mathcal{D}_F$.*

(b) Al grupo cociente $C_F := \mathcal{D}_F/\mathcal{P}_F$ lo llamamos ***grupo de clases de divisores****.*

Observación 1.2.4. Para cualquier $D \in \mathcal{D}_F$ el elemento correspondiente en el grupo C_F será la clase del divisor D y será denotada por $[D]$. Dos divisores son equivalentes si pertenecen a la misma clase, es decir: $D \sim D'$ si $[D] = [D']$. Es inmediato que si $D \sim D'$ implica que existe un divisor (x) tal que $D = D' + (x)$ con $x \neq 0$.

Definición 1.2.5. *Sea $A \in \mathcal{D}_F$, definimos* $\mathcal{L}(A) := \{x \in F | (x) + A \geq 0\} \cup \{0\}$.

Observación 1.2.5. Algunas observaciones inmediatas de la definición de $\mathcal{L}(A)$ son:

(a) si escribimos al divisor A como

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

con $n_i \geq 0$, $m_j \geq 0$ para $i = 1, \ldots r$ y $j = 1, \ldots s$, entonces los elementos del conjunto $\mathcal{L}(A)$ serán los elementos $x \in F$ que cumplan las siguientes características:

- x tiene ceros de orden $\geq m_j$ en los lugares Q_j y
- x tiene polos solamente en los lugares $P_1, \ldots P_r$ de orden a lo más n_i.

(b) $x \in \mathcal{L}(A)$ si y solamente si $v_P(x) \geq -v_P(A)$, para todo $P \in \mathbb{P}_F$.

(c) $A' \sim A$ con $A' \geq 0$ si y solamente si $\mathcal{L}(A) \neq \{0\}$.

Proposición 1.2.1. *El conjunto $\mathcal{L}(A)$ cumple con las siguientes propiedades:*

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

(b) Si $A' \in \mathcal{D}_F$ es tal que $A' \sim A$ entonces los espacios vectoriales $\mathcal{L}(A)$, $\mathcal{L}(A')$ son isomorfos.

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

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

Demostración.

(a) Sean $a \in K$ y $x, y \in \mathcal{L}(A)$. Se tiene que para cualquier $P \in \mathbb{P}_F$:

$$v_P(x+y) \geq min\{v_P(x), v_P(y)\} \geq -v_P(A)$$

además,

$$v_P(ax) \geq v_P(a) + v_P(x) \geq -v_P(A)$$

por lo que $x+y$ y ax pertenecen al espacio $\mathcal{L}(A)$.

(b) Si $A' \sim A$ entonces existe $0 \neq z \in F$ tal que $A' + (z) = A$. Consideramos el siguiente mapeo:

$$\begin{aligned} \phi : \quad \mathcal{L}(A) &\longrightarrow F, \\ x &\longmapsto xz, \end{aligned}$$

observamos que este mapeo es lineal y su imagen está contenida en el espacio $\mathcal{L}(A')$. De manera análoga:

$$\begin{aligned} \phi' : \quad \mathcal{L}(A') &\longrightarrow F, \\ x &\longmapsto xz^{-1}, \end{aligned}$$

es un mapeo lineal de $\mathcal{L}(A')$ a $\mathcal{L}(A)$. Como estos mapeos son inversos uno del otro, entonces se concluye que ϕ es un isomorfismo de espacios vectoriales.

(c) Sabemos que si $0 \neq x \in K$, entonces $(x) = 0$, por lo que $K \subseteq \mathcal{L}(0)$. Por otro lado, si $0 \neq x \in \mathcal{L}(0)$ entonces $(x) \geq 0$, por lo que x no tiene polos (observación 1.1.1) lo que indica que $x \in K$.

(d) Si suponemos que existe $0 \neq x \in \mathcal{L}(A)$ entonces $(x) \geq -A > 0$, lo que implica que x tiene ceros pero no polos y contradiciendo la observación 1.1.1. □

Observación 1.2.6. Queremos mostrar que para cualquier divisor A de F/K, el espacio $\mathcal{L}(A)$ es un espacio vectorial de dimensión finita sobre K. Para aclarar esta afirmación observemos que si $A, B \in \mathcal{D}_F$ son tales que $A \leq B$, entonces:

(a) $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ y

(b) $dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq grado(B) - grado(A)$.

El inciso (b) se demuestra a continuación. Utilizaremos el caso $B = A + P$ para algún $P \in \mathbb{P}_F$ (el caso general se sigue inductivamente). Escogemos un elemento $t \in F$ con $v_P(t) = v_P(B) = v_P(A) + 1$. Para $x \in \mathcal{L}(B)$ tenemos $v_P(x) \geq -v_P(B) \geq -v_P(t)$ por lo que $xt \in O_P$. De este modo que obtenemos el mapeo:

$$\psi : \begin{cases} \mathcal{L}(B) & \longrightarrow & F_P, \\ x & \longmapsto & (xt)P. \end{cases}$$

Los elementos del núcleo de ψ serán para los cuales se cumpla que $v_P(x) > 0$, es decir, para los cuales $v_P(x) \geq -v_P(A)$ dando como resultado que $ker(\psi) = \mathcal{L}(A)$. Así, ψ induce un mapeo inyectivo de $\mathcal{L}(B)/\mathcal{L}(A)$ a F_P por lo que:

$$dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq dim(F_P) = grado(B) - grado(A),$$

obteniendo el resultado deseado.

Proposición 1.2.2. *$\mathcal{L}(A)$ es un espacio vectorial de dimensión finita sobre K para cualquier $A \in \mathcal{D}_F$.*

Demostración. Si $A = A_+ - A_-$ con A_+ y A_- divisores positivos, observamos que $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$. Además, $0 \leq A_+$ implica que $dim(\mathcal{L}(A_+)/\mathcal{L}(0)) \leq grado(A_+)$. Utilizando que $\mathcal{L}(0) = K$ y la proposición 1.2.1, $dim\mathcal{L}(A_+) = dim(\mathcal{L}(A_+)/\mathcal{L}(0)) + 1$. De esta manera $dim(\mathcal{L}(A)) \leq grado(A_+) + 1$. □

Definición 1.2.6. *La **dimensión del divisor A** será la dimensión de $\mathcal{L}(A)$ como K-espacio vectorial.*

Teorema 1.2.1. *Cualquier divisor principal del campo F/K tiene grado cero. En particular, si $x \in F/K$ entonces $grado((x)_0) = grado((x)_\infty) = [F : K(x)]$.*

Demostración. Sea $n := [F : K(x)]$ y sea $B := (x)_\infty = \sum_{i=1}^{r} -v_{P_i}(x)P_i$ donde los lugares $P_1, ..., P_r$ son todos los polos de x, entonces usando el corolario 1.1.3 tenemos que:

$$grado(B) := \sum_{i=1}^{r} v_{P_i}(x^{-1}) \cdot grado(P_i) \leq [F : K(x)] = n,$$

por lo que basta demostrar que $n \leq grado(B)$.

Sea $\{u_1, \dots u_n\}$ una base de $F/K(x)$ y $C \in \mathcal{D}_F$ tales que $(u_i) \geq -C$ para $i = 1, \dots, n$. Como $x^i u_j \in \mathcal{L}(lB + C)$ para $0 \leq i \leq l$ y $1 \leq j \leq n$ se tiene que:

$$dim(lB + C) \geq n(l + 1) \quad \text{para toda } l \geq 0.$$

Observemos que los elementos $x^i u_j$ son linealmente independientes sobre K pues el conjunto $\{u_1, \dots u_n\}$ es linealmente independiente sobre $K(x)$.

Haciendo $c := grado(C)$, obtenemos que:

$$n(l + 1) \leq dim(lB + C) \leq l \cdot grado(B) + c + 1$$

por lo que:

$$l(grado(B) - n) \geq n - c - 1 \quad \text{para toda } l \geq 0.$$

Como el lado derecho de la desigualdad anterior es independiente de la elección de l la desigualdad solamente es posible cuando $grado(B) \geq 0$. Así, hemos probado que $grado((x)_\infty) = [F : K(x)]$. Como $(x)_0 = (x^{-1})_\infty$ se concluye que

$$grado((x)_0) = grado((x^{-1})_\infty) = [F : K(x^{-1})] = [F : K(x)]$$

con lo que se llega al resultado deseado. □

Corolario 1.2.1. *Algunas propiedades del espacio $\mathcal{L}(A)$ son:*

(a) Si $A, A' \in \mathcal{D}_F$ y $A \sim A'$ entonces $grado(A) = grado(A')$ y $dimA = dimA'$.

(b) Si $grado(A) < 0$ entonces $dimA = 0$.

(c) Si A es un divisor de grado cero, las siguientes proposiciones son equivalentes:

(i) A es un divisor principal.

(ii) $dimA \geq 1$.

(iii) $dimA = 1$.

Demostración.

(a) Se sigue de la proposición 1.2.1 y del teorema anterior.

(b) Si suponemos que $dimA > 0$, por la observación 1.2.5 tenemos que existe un divisor A' tal que $A' \sim A$ con $A' \geq 0$ entonces se tendría que $grado(A) = grado(A') \geq 0$.

(c) $(i) \Rightarrow (ii)$ Si $A = (x)$ es un divisor principal entonces $x^{-1} \in \mathcal{L}(A)$ lo que implica que $dim(A) \geq 1$.

$(ii) \Rightarrow (iii)$ Si suponemos que $dim(A) \geq 1$ y $grado(()A) = 0$, entonces $A' \sim A$ con $A' \geq 0$, por lo que $A' = 0$, obteniendo que $dim(A) = dim(A') = dim(0) = 1$.

$(iii) \Rightarrow (i)$ Supondremos que $dim(A) = 1$ y $grado(()A) = 0$. Tomamos un elemento $0 \neq z \in \mathcal{L}(A)$, este elemento cumple por definición del espacio $\mathcal{L}(A)$ que $(z)+A \geq 0$. Como $grado((z) + A) = 0$ se sigue que $(z) + A = 0$ por lo tanto $A = -(z) = (z^{-1})$ es un divisor principal. □

1.3. Teorema de Riemann-Roch

En la proposición 1.2.2 se estableció una cota inferior para la dimensión de un divisor. En esta sección veremos algunos resultados que permiten, bajo ciertas condiciones, establecer cotas superiores. Estas cotas sirven para cualquier divisor del campo de funciones e introduce al siguiente concepto: el género de un campo. Este concepto es de extrema importancia dentro de la teoría de los campos de funciones algebraicos y será medular en la implementación de códigos geométricos y su decodificación.

Proposición 1.3.1. *Existe una constante $\gamma \in \mathbb{Z}$ tal que , para todos los divisores $A \in \mathcal{D}_F$,*

$$grado(A) - dim\ A \geq \gamma.$$

Definición 1.3.1. *El* **género** *de F/K es definido por*

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

Observación 1.3.1. A partir de este momento g denotará el género del campo F/K. Se observa que el género de F/K siempre es un entero no negativo. Al siguiente resultado se le conoce como *Teorema de Riemann* y brinda información más precisa acerca de la dimensión de un divisor en un campo de funciones.

Teorema 1.3.1. *(Teorema de Riemann). Sea F/K un campo de funciones de género g, entonces:*

(a) Para cualquier divisor $A \in \mathcal{D}_F$, $\boldsymbol{dimA \geq grado(A) + 1 - g}$.

(b) Existe un entero c, que depende de F/K, tal que: $\boldsymbol{dimA = grado(A) + 1 - g}$ siempre y cuando $grado(A) \geq c$.

Demostración.

(a) Se concluye a partir de la definición de género.

(b) Escogemos un divisor A_0 con $g = grado(A_0) - dimA_0 + 1$ y hacemos

$c := grado(A_0) + g$. Si $grado(A) \geq c$, entonces:

$$dim(A - A_0) \geq grado(A - A_0) + 1 - g \geq c - grado(A_0 + 1) - g \geq 1,$$

por lo que tenemos que $\emptyset \neq \mathcal{L}(A - A_0)$. Seleccionamos $0 \neq z \in \mathcal{L}(A - A_0)$ y hacemos el divisor $A' - A + (z)$. Claramente $A' \geq A_0$. Por otro lado, tenemos:

$$grado(A) - dimA \;=\; grado(A') - dimA' = grado(A_0) - dimA_0 \;=\; g - 1,$$

por lo que $dimA \geq grado(A) + 1 - g$. □

Definición 1.3.2. *Para A un divisor de F/K, definimos como* índice de especialidad del divisor [1] *al entero* $\boldsymbol{i(A)} := dimA - grado(A) + g - 1$.

Definición 1.3.3. *(a) Un* adele *de F/K es un mapeo α de la forma:*

$$\alpha : \begin{cases} \mathbb{P}_F & \longrightarrow \quad F, \\ P & \longmapsto \quad \alpha_P. \end{cases}$$

tal que $\alpha_P \in \mathcal{O}_P$, excepto en un número finito de lugares.

(b) Denotamos como $\mathcal{A}_F$ al conjunto de los adeles de F/K.

(c) Si $x \in F$ diremos que ***el adele principal de x*** *como el adele de F cuyas componentes son todas iguales a x. (Ver observación 1.3.2.a).*

(d) Para $A \in \mathcal{D}_F$ definimos: $\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F | v_P(\alpha) \geq v_P(A)$ para toda $P \in \mathbb{P}_F\}$.

[1] Esta definición es muy importante para este trabajo pues además de representar la dimensión de un espacio vectorial (proposición 1.3.2) es fundamental para el cálculo de parámetros de algunos códigos.

Observación 1.3.2. Se hacen las siguientes observaciones:

(a) Podemos ver a un adele como un elemento del producto directo $\Pi_{P\in\mathbb{P}_F}F$, por lo que podemos usar la notación $\alpha = (\alpha_P)_{P\in\mathbb{P}_F}$ o simplemente $\alpha = (\alpha_P)$.

(b) Para un divisor A de F/K, $\mathcal{A}_F(A)$ es un espacio de dimensión finita sobre el campo K, sin embargo, el espacio $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$ es de dimensión finita sobre K, como se enuncia a continuación. Dicho resultado tiene como consecuencia una caracterización útil para el género de F/K. Las respectivas demostraciones pueden ser encontradas en [15].

Teorema 1.3.2. *Para cualquier $A \in \mathcal{D}_F$, el índice de especialidad es:*

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

Corolario 1.3.1. *Para cualquier F/K se cumple que:*

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

Definición 1.3.4. *(a) Un **diferencial de Weil** es un mapeo lineal $\omega : \mathcal{A}_F \mapsto K$ que se anula en $\mathcal{A}_F(A) + F$ para algún $A \in \mathcal{D}_F$.*

(b) Denotamos como $\mathbf{\Omega_F}$ al conjunto de todos los diferenciales de Weil ω de F.

(c) Para un divisor A, denotaremos como $\Omega_F(A)$ al conjunto de los diferenciales de Weil tales que se anulan en $\mathcal{A}_F(A) + F$.

Proposición 1.3.2. *Para $A \in \mathcal{D}_F$ se tiene que $dim\Omega_F(A) = i(A)$, como un espacio vectorial sobre el campo F.*

Demostración. El espacio $\Omega_F(A)$ es isomorfo al espacio de las formas lineales de $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$. Por otro lado, $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$ es un espacio de dimensión finita $i(A)$. Utilizando el teorema 1.3.2 obtenemos la igualdad deseada. □

Observación 1.3.3. Se hacen las siguientes observaciones acerca de Ω_F:

- El conjunto Ω_F tiene estructura de espacio vectorial sobre K y sobre F, de hecho, visto como un $F-$ espacio vectorial es de dimensión 1. La operación escalar para dar la estructura de $F-$espacio vectorial es la siguiente: para un elemento $x \in F$ y un $\omega \in \Omega_F$ definimos, $x\omega : \mathcal{A}_F \to K$ mediante $(x\omega)(\alpha) := \omega(x\alpha)$.

- Sea $M(\omega) := \{A\mathcal{D}_F \mid \omega \text{ se anula en } \mathcal{A}_F(A)+F\}$. Si $0 \neq \omega$ entonces existe un único divisor $W \in M(\omega)$ tal que $A \leq W$ para cualquier $A \in M(\omega)$. Como el divisor W es único, este resultado vincula a cada diferencial un divisor.

Definición 1.3.5. *(a) Denotamos por (ω) al divisor asociado a un diferencial de Weil, esto es si ω es un diferencial de Weil, $\omega \neq 0$ y ω queda determinado por las siguientes condiciones:*

(i) ω se anula en $\mathcal{A}_F((\omega) + F)$;

(ii) si ω se anula en $\mathcal{A}_F(A) + F$, entonces $A \leq (\omega)$.

(b) Para $0 \neq \omega \in \Omega_F$ y $P \in \mathbb{P}_F$, definimos $v_P(\omega) := v_P((\omega))$

(c) Un lugar P es un **cero** *(resp.* **polo***) si $v_P(\omega) > 0$ ($v_P(\omega) < 0$). Decimos también que ω es* **regular en P** *si $v_P(\omega) \geq 0$ y ω es* **regular** *si es regular en todo $P \in \mathbb{P}_F$.*

(d) Un divisor W es un **divisor canónico** *de F si $W = (w)$ para algún $\omega \in \Omega_F$.*

Observación 1.3.4. De la definición anterior se sigue que:

- $\Omega_F(A) = \{\omega \in \Omega_F \mid \omega = 0 \text{ o } (\omega) \geq A\}$ y

- $\Omega_F(0) = \{\omega \in \Omega_F \mid \omega \text{ es regular }\}$.

Además, de la proposición 1.3.2 y de la definición de índice de especialidad:

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

Proposición 1.3.3. *(a) Para $0 \neq x \in F$ y $0 \neq \omega \in \Omega_F$ se tiene que $(x\omega) = (x) + (\omega)$.*

(b) Cualesquiera dos divisores canónicos del campo F/K son equivalentes.

Demostración. Si ω se anula en el conjunto $\mathcal{A}_F(A) + F$, entonces $x\omega$ se anula en $\mathcal{A}_F(A + (x)) + F$ por lo que:

$$(\omega) + (x) \leq (x\omega). \tag{1.3}$$

Además, $(x\omega) + (x^{-1}) \leq (x^{-1}x\omega) = (\omega)$. Utilizando 1.3, obtenemos:

$$(\omega) + (x) \leq (x\omega) \leq -(x^{-1}) + (\omega) = (\omega) + (x),$$

por lo que queda demostrado el inciso (a). El inciso (b) se sigue como consecuencia de la observación 1.3.3 y del inciso (a). □

Teorema 1.3.3. *Sea $A \in \mathcal{D}_F$ y $W = (\omega)$ un divisor canónico de F/K. Entonces el mapeo:*

$$\mu : \begin{cases} \mathcal{L}(W - A) & \longrightarrow \quad \Omega_F(A), \\ x & \longmapsto \quad x\omega. \end{cases}$$

es un isomorfismo de $K-$espacios vectoriales. Además, se tiene que:

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

Demostración. Para $x \in \mathcal{L}(L - W)$, se tiene $(x\omega) = (x) + (\omega) \geq -(W - A) + W = A$, entonces $x\omega \in \Omega_F(A)$, así μ mapea $\mathcal{L}(W - A)$ en $\Omega_F(A)$. Claramente, el mapeo es lineal e inyectivo. Consideremos $\omega_1 \in \Omega_F(A)$, utilizando 1.3.3, $\omega_1 = x\omega$ con $x \in F$, entonces:

$$(x) + W = (x) + (\omega) + (x\omega) = (\omega_1) \geq A,$$

por lo que, $(x) \geq -(W - A)$, entonces $x \in \mathcal{L}(W - A)$ y $\omega_1 = \mu(x)$. Así, el mapeo es suprayectivo y se ha probado que $\dim \Omega_F A = dim(W - A)$, como $dim\Omega_F(A) = i(a)$, por lo que $i(A) = dim(W - A)$. □

Observación 1.3.5. A continuación se presenta el Teorema de Riemann-Roch. Este resultado es uno de los más importantes dentro de la teoría de campos algebraicos de funciones y junto con sus consecuencias serán de gran utilidad en la teoría de códigos geométricos. Su demostración es inmediata a partir de la definición de índice de especialidad y del teorema 1.3.3.

Teorema 1.3.4. *(Teorema de Riemann-Roch). Sea W un divisor canónico de F/K, entonces para cualquier $A \in \mathcal{D}_F$ se cumple que:*

$$dim(A) = grado(A) + 1 - g + dim(W - A) \tag{1.4}$$

Corolario 1.3.2. *Para un divisor canónico W, se tiene que:*

$$grado(W) = 2g - 2 \quad y \quad dim\ W = g.$$

Demostración. Para $A = 0$, $\mathcal{L}(A) = K$ y utilizando el Teorema de Riemann-Roch:

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

por lo que $dim\ W = g$. Si hacemos $A = W$, tendremos:

$$g = dim\ W = grado(W) + 1 - g + dim(W - W) = grado(W) + 2 - g,$$

entonces, $grado(W) = 2g - 2$. □

Observación 1.3.6. El Teorema de Riemann (teorema 1.3.1) nos indicaba que existe una constante c tal que $i(A) = 0$ siempre y cuando $grado(A) \geq c$. El siguiente teorema, nos da más información acerca de cómo escoger dicha constante.

Teorema 1.3.5. *Si A es un divisor tal que $grado(A) \geq 2g - 1$ entonces*

$$dim\ A = \deg A + 1 - g.$$

Demostración. Tenemos que $dim\ A = grado(A) + 1 - g + dim(W - A)$, donde W es un divisor canónico. Como $grado(A) \geq 2g-1$ y $grado(W) = 2g-2$, entonces $grado(W-A) < 0$ lo que implica que $\dim(W - A) = 0$. □

Definición 1.3.6. *Sea $P \in \mathbb{P}_F$. Decimos que un entero $n \geq 0$ es un orden polar en P si existe $x \in F$ tal que $(x)_\infty = nP$. En caso contrario diremos que n es un* ***salto en*** *P.*

Observación 1.3.7. En relación a la definición anterior, enunciamos:

- Un entero n es orden polar si y sólo si $dim(nP) > dim(n-1)P$.
- Denotaremos como $\boldsymbol{S_P}$ al conjunto $\{n \in \mathbb{Z} \mid n \text{ es orden polar en } P\}$ y como G_P al conjunto de números enteros que son saltos en P, es decir $\boldsymbol{G_P} = \mathbb{N} - S_P$.
- S_P es un semigrupo de $\mathbb{N}$. Verificamos la afirmación: si n_1 y n_2 en S_P entonces para cada uno de estos elementos existen $x_1, x_2 \in F$, respectivamente, tales que: $(x)_\infty = n_1P$ y $(x)_\infty = n_2P$. Por las propiedades de una valoración discreta, se tiene que $(x_1x_2)_\infty = (n_1 + n_2)P$, por lo que $(n_1 + n_2) \in S_P$.
- En el siguiente teorema encontramos una forma directa de calcular el género de un campo algebraico de funciones a través de este concepto.

Teorema 1.3.6. *(Teorema de Saltos de Weierstrass) Si F/K es un campo algebraico de funciones de género g y $P \in \mathbb{P}_F$, entonces $|G_P| = g$. Además, si $g > 0$ entonces $1 \in G_P$.*

Demostración. Consideramos la siguiente cadena de espacios:

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

y consideramos que $dim((2g-1)P) = 2g-1+1-g = g$, es decir, sólo en $(2g-1)-g$ espacios en la cadena se ha aumentado la dimensión y sabemos que este aumento se da de uno en uno, por lo que en el resto de los lugares de la cadena debe haber $(2g-1)-g-1 = g$ saltos en dimensión.

Por otro lado, si suponemos que $\mathbb{N} = S_P$, es decir, que no se tiene ningún salto de Weirstrass, esto implica que $|G_P| = 0 < g \ \forall g$, lo que contradice el párrafo anterior, por lo tanto, al menos $1 \in G_P$. □

1.4. Componentes Locales de los diferenciales de Weil

Definición 1.4.1. *Sea $P \in \mathbb{P}_F$. Consideramos el mapeo*

$$\begin{aligned} \iota_P : \quad F &\longrightarrow \mathcal{A}_F \\ x &\longmapsto \alpha \end{aligned}$$

tal que $\alpha_P = x$ y $\alpha_Q = 0$ para $Q \in \mathbb{P}_F - P$, i.e. $\iota_P(x)$ será el adele cuya componente P es x y todas las demás componentes son iguales a cero. Para ω un diferencial de Weil, definimos su **componente local** *mediante el mapeo $K-$lineal: $\omega_P : F \longrightarrow K$ con*

$$\omega_P(x) := \omega(\iota_P(x)).$$

Observación 1.4.1. Si $\omega \in \Omega_F$ y $\alpha = (\alpha_P) \in \mathcal{A}_F$ entonces $\omega_P(\alpha_P) = 0$ para casi todo lo P, excepto para un número finito de lugares. Esto lo podemos concluir de lo siguiente:

Supongamos que $\omega \neq 0$ y sea $W := (w)$ su divisor canónico. existe un conjunto finito $S \subseteq \mathbb{P}_F$ tal que $v_p(W) = 0$ y $v_P(\alpha_P) \geq 0$ para todo $P \notin S$. Haciendo el adele $\beta := (\beta_P)$ tal que $\beta_P = \alpha_P$ si $P \notin S$ y $\beta_P = 0$ si $P \in S$ entonces tenemos que $\beta \in \mathcal{A}_F(W)$ por lo tanto $\omega(\beta) = 0$. Por otro lado:

$$\alpha = \beta + \sum_{P \in S} \iota_P(\alpha_p)$$

por lo tanto,

$$\omega(\alpha) = \sum_{P \in S} \omega_P(\alpha_p).$$

Si $P \notin S$, $\iota_P(\alpha_P) \in \mathcal{A}_F(W)$, entonces $\omega(\alpha_P) = 0$. Así, se tiene que

$$\omega(\alpha) = \sum_{P \in \mathbb{P}_F} \omega_P(\alpha_P).$$

Proposición 1.4.1. *Sea $\omega \neq 0$ un diferencial de Weil de F/K y $P \in \mathbb{P}_F$, entonces:*

(a) $v_P(\omega) = máx\{r \in \mathbb{Z} \mid \omega_P(x) = 0$ *para toda* $x \in F$ *con* $v_P(x) \geq -r\}$,

(b) Si $\omega, \omega' \in \Omega_F$ *y* $\omega_P = \omega'_P$ *para algún* $P \in \mathbb{P}_F$, *entonces* $\omega = \omega'$.

Demostración. Sabemos que $v_P(\omega) = v_P(W)$. Sea $s := v_P(w)$, si $x \in F$ es tal que $v_P(x) \geq -s$ tenemos que $\iota_P(x) \in \mathcal{A}_F(W)$, por lo que $\omega_P(x) = \omega_P(\iota_P(x)) = 0$. Por otro lado, si suponemos que $\omega_P(x) = 0$ para toda $x \in F$ con $v_P \geq -s-1$. Sea $\alpha = (\alpha_Q)_{Q\in\mathbb{P}_F} \in \mathcal{A}_F(W+P)$ por lo que:

$$\alpha = (\alpha - \iota_P(\alpha_P)) + \iota_P(\alpha_P)$$

donde $\alpha - \iota_P(\alpha_P) \in \mathcal{A}_F(W)$ y $v_P(\alpha_P) \geq -s-1$, por lo tanto,

$$\omega(\alpha) = \omega(\alpha - \iota_P \geq (\alpha_P)) + \omega_P(\alpha_P) = 0,$$

es decir, el diferencial ω se anula en $\mathcal{A}_F(W+P)$ lo cual contradice la definición de W. Con lo anterior, tenemos que $v_P(\omega)$ queda caracterizada como:

$$v_P(\omega) = máx\{r \in \mathbb{Z} \mid \omega_P(x) = 0 \text{ para toda } x \in F \text{ con} v_P(x) \geq -r\ \},$$

en particular, si $\omega' \in \Omega_F$ es otro diferencial de Weil con $\omega'_P = \omega_P$ en algún lugar P, entonces $(\omega' - \omega)_P = 0$ entonces $\omega' = \omega$. Esto nos indica que un diferencial ω queda determinado por cualquiera de sus componentes locales. $\omega(\alpha) = \sum_{P\in\mathbb{P}_F} \omega_P(\alpha_P)$. En particular, $\sum_{P\in\mathbb{P}_F} \omega_P(1) = 0$.

1.5. Extensiones algebraicas de F/K y el Criterio de Eisenstein

Definición 1.5.1. *Sea F'/K' un campo de funciones.*

(i) Decimos que F'/K' es **extensión algebraica de** *F/K si $F' \geq F$ es a su vez una extensión algebraica y $K' \geq K$.*

(ii) Llamaremos a F'/K' una **extensión de constantes sobre** *F/K si*

$$F' = FK' = \{z \cdot a | z \in F,\ a \in K\}.$$

(iii) La extensión $F'/K' \supseteq F/K$ se dice **finita** *si $[F' : F] < \infty$.*

Observación 1.5.1. Si F'/K' es una extensión algebraica de F/K entonces:

(a) K'/K es algebraica, $K' \cap F = K$.

(b) F'/K' es extensión finita de F/K si y sólo si $[K' : K] < \infty$.

(c) Sea $F_1 = FK'$ entonces F_1/K' es una extensión de constantes de F/K y F'/K' es una extensión finita sobre F_1/K.

Definición 1.5.2. *Sea F'/K' una extensión de F/K. Decimos que el lugar $P' \in \mathbb{P}_{F'}$* **está sobre** *$P \in \mathbb{P}_F$ si $P \subseteq P'$. Diremos que P' es extensión de P y escribimos $P'|P$.*

Proposición 1.5.1. *Sea F'/K' una extensión de F/K. Sean $P' \in \mathbb{P}_{F'}$, $P \in \mathbb{P}_F$ con $O_{P'}$, O_P, $v_{P'}$ y v_P los anillos y las valoraciones correspondientes. Entonces, las siguientes afirmaciones son equivalentes:*

(1) $P|P'$.

(2) $O_P \subseteq O_{P'}$.

(3) Existe $e \in \mathbb{Z}$ con $e \geq 1$ tal que $v_{P'}(x) = ev_P(x)\ \forall x \in F$.

(1) $\Leftrightarrow$ (2) Supongamos que $P'|P$ pero $O_P \nsubseteq O'_P$. Esto quiere decir que existe un elemento $u \in F$ tal que $v_P(u) \geq 0$ pero $v_{P'}(u) < 0$. Por otro lado, $P \subseteq P'$, si $v_P(z) > 0$ entonces $v_{P'}(z) > 0$, por lo que $v_P(u) = 0$. Sea $t \in F$ tal que $v_P(t) = 1$, entonces $t \in P$ por lo que $t \in P'$ y sea $r := v_{P'}(t) > 0$, entonces:

$$\begin{aligned} v_P(u^r t) &= r v_P(u) + v_P t = 1 \\ v_{P'}(u^r t) &= r v_{P'}(u) + v_{P'} t \leq -r + r = 0 \end{aligned}$$

pues u no pertenece a $O_{P'}$. Entonces $u^r t \in P$ pero $u^r t \notin P'$ así que se tiene una contradicción al hecho de que $P \subseteq P'$. Entonces $O_P \subseteq O_{P'}$. Ahora supongamos que $O_P \subseteq O_{P'}$. Si $y \in P$ entonces, $y^{-1} \notin O_P$ por lo que $y^{-1} \notin O_{P'}$, entonces $y = (y-1)-1 \in P'$ por lo tanto, $P \subseteq P'$ por lo que P' está sobre P.

(2) $\Longrightarrow$ (3) Sea $u \in F$ tal que $v_P(u) = 0$ entonces $u, u^{-1} \in O_{P'}$. Entonces, $v_{P'}(u) = 0$, sea t un parámetro local de P, es decir, $v_P(t) = 1$. Sea $e := v_{P'}(t)$. Como $t \in P'$ entonces $e > 0$, más aún $e \geq 1$. Sea $x \in F$ y sea $r := v_{P'}(t) \in \mathbb{Z}$, entonces $v_P(xt^{-r}) = 0$ y

$$v_{P'}(x) = v_{P'}(xt^{-r}) + v_{P'}(t^r) = 0 + r v_{P'}(t^r) = e v_P(x).$$

(3) $\Longrightarrow$ (2) Por otro lado, sea x un elemento en O_P, esto implica que la valoración $v_P(x) \geq 0$. Por hipótesis existe un entero $e > 0$ tal que $v_{P'}(x) = e v_P(x) \geq 0$, es decir, $x \in O_{P'}$, por lo que si $x \in O_P$ entonces $x \in O_{P'}$ así, $O_P \subseteq O_{P'}$. Por lo que mediante la tercera afirmación se puede concluir la segunda y con esto la proposición queda demostrada. □

Observación 1.5.2. De la proposición anterior tenemos como consecuencia que existe una inmersión natural del campo residual F_P en el campo residual F'_P dada por

$$x(P) \longmapsto x(P') \quad \text{para } x \in O_P.$$

Con lo anterior establecemos que F_P puede ser considerado como subcampo de $F'_{P'}$.

Definición 1.5.3. *Sea F'/K' una extensión de F/K con $P' \in \mathbb{P}_{F'}$ y $P \in \mathbb{P}_F$ tal que $P|P'$, entonces:*

*(i) Al entero asociado a la igualdad $v_{P'}(x) = ev_P(x)$ de la proposición anterior le llamaremos **índice de ramificación de P' sobre P** y se le denotará como $e(P'|P)$.*

(ii) Diremos que $P|P'$ es ramificado si $e(P'|P) > 1$. Si $e(P'|P) = 1$, diremos que $P|P'$ no es ramificado.

*(iii) Llamaremos **grado relativo de** $P'|P$ a $f(P'|P) := [F_P : F_{P'}]$.*

Proposición 1.5.2. *Sea F'/K' una extensión de F/K. Entonces*

(a) Para todo $P' \in \mathbb{P}_{F'}$ existe un único lugar $P \in \mathbb{P}_F$ tal que $P'|P$ a saber que $P = P' \cap F$.

(b) Para $P \in \mathbb{P}_F$, P tiene al menos una extensión $P' \in \mathbb{P}_{F'}$ y por otro lado, sólo puede tener un número finito de ellas.

Demostración.

(a) Para la demostración de esta proposición es importante verificar que $F \cap P' \neq \emptyset$, esto es, verificar que existe un elemento $z \in F$ tal que $v_{P'} > 0$. Si se supone lo contrario, es decir, que $v_{P'} < 0$ entonces existe una ecuación tal que:

$$C_n t^n + C_{n-1} t^{n-1} + ... + C_1 t + C_0 = 0, \tag{1.5}$$

con $C_i \in F$, $c_0 \neq 0$ y $c_n \neq 0$. La hipótesis dice que $v_{P'}(C_0) = 0$ y:

$$v_{P'}(c_i t^i) = v_{P'}(c_i) + i v_{P'}(t) > 0$$

para $i = 1, \ldots n$ lo cual contradice a la desigualdad estricta del triángulo, así $F \cap P' \neq \emptyset$. Para completar la demostración de este inciso, tenemos que $O = F \cap O_P$ es un anillo de valoración de F/K con $P := P' \cap F$ su lugar asociado. Por lo tanto existe un único lugar $P \in \mathbb{P}_F$ tal que $P'|P$.

(b) Sea $P \in \mathbb{P}_F$ y sea $x \in F - K$ tal que P el único lugar cero de x, es decir $v_P(x) > 0$. Si $P'|P$ tenemos que $v'_P(x) = e(P'|P)v_P(x) > 0$ lo que implica que el lugar P' es un cero de x en $\mathbb{P}_{F'}$. Por otro lado, si suponemos que $v'_P(x) > 0$ y $Q = P' \cap F$ el lugar que está *por debajo* de P', así, $v_Q(x) > 0$ lo que nos dice que Q es un cero de x pero por nuestra elección x sólo tiene un lugar cero, por lo que $P = Q$. Así llegamos la conclusión de que $P'|P$ si y solamente si $v_{P'}(x) > 0$. □

Observación 1.5.3. Para cada lugar $P \in F$ tenemos que habrá un número finito de extensiones $P' \in \mathbb{P}_F$, la siguiente definición nos permite extender el grupo de divisores de F al grupo de divisores de F'.

Definición 1.5.4. *Sea F'/K' una extensión algebraica de F/K. Para $P \in \mathbb{P}_F$ definimos la* ***conorma de*** *P como:*

$$Con_{F|F'}(P) := \sum_{P|P'} e(P'|P)P'.$$

Observación 1.5.4. Observamos que la definición anterior es para un lugar P, sin embargo, se extiende de manera natural al grupo de divisores de F': sea $D \in \mathcal{D}_F$ tal que $D = \sum_{P \in \mathbb{P}_F} n_p P$, entonces:

$$Con_{F|F'}(D) = Con_{F|F'}(\sum_{P \in \mathbb{P}_F} n_P P) = \sum_{P \in \mathbb{P}_F} Con_{F|F'}(P).$$

Además, si $x \in F$, **el divisor principal de x en F'** será:

$$\begin{aligned}(x)^{F'} &= \sum_{P' \in \mathbb{P}_{F'}} v_{P'}(x)P' = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} e(P'|P)v_P(x)P' = \\ &= \sum_{P \in \mathbb{P}_F} Con_{F|F'}(P) = Con_{F|F'}(\sum_{P \in \mathbb{P}_F} v_P(x)P) = Con_{F|F'}(D),\end{aligned}$$

así, la conorma induce un homomorfismo de los grupos de clases de divisores

$$Con_{F|F'} : C_{\mathcal{F}} \longrightarrow C_{\mathcal{F}'}.$$

Lema 1.5.1. *Sea K'/K una extensión algebraica finita y x un elemento trascendente sobre K, entonces:*

$$[K'(x) : K(x)] \leq [K' : K]$$

Demostración. Si se supone que $K' : K(\alpha)$ para alguna $\alpha \in K'$, entonces

$$[K'(x) : K(x)] \leq [K' : K].$$

Si se toma un elemento $\varphi(\mathcal{T}) \in K(\mathcal{T})$ el polinomio minimal de α y si se supone que éste admite una descomposición como producto de dos polinomios mónicos $g(\mathcal{T})$ y $h(\mathcal{T})$ entonces se tiene que $g(\alpha) = 0$ ó $h(\alpha) = 0$. Sin pérdida de generalidad podemos suponer que $g(\alpha) = 0$. Ahora $g(\mathcal{T})$ es un polinomio de la siguiente forma:

$$g(\mathcal{T}) = \mathcal{T}^r + C_{r-1}(x)\mathcal{T}^{r-1} + ... + C_0(x) \tag{1.6}$$

con $C_i \in K(x)$. Si multiplicamos por un denominador en común $\mathcal{G}_i \in K[x]$ y evaluamos en α el polinomio 1.6 tenemos que:

$$0 = \mathcal{G}_r(x)(\alpha)^r + \mathcal{G}_{r-1}(x)(\alpha)^{r-1} + ... + \mathcal{G}_0(x). \tag{1.7}$$

Finalmente haciendo $x = 0$ en la ecuación 1.7 obtenemos una combinación lineal de potencias de α con un número de términos menor a φ, pues $grado(g) < grado(\varphi)$, por lo cual tenemos una contradicción. Así el polinomio φ es irreducible y esto asegura que $[K'(x) : K(x)] \geq [K' : K]$. □

Teorema 1.5.1. *Sea F'/K' una extensión algebraica de F/K. Sea $P \in \mathbb{P}_F$ y $P_1, ...P_m \in \mathbb{P}_{F'}$ todos los lugares sobre P. Sea $e_i = (P_i|P))$ y $f_i = (P_i|P)$, entonces:*

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

Demostración. Sea $x \in F$ cuyo único cero es P. Sea $r := v_P(x) > 0$, entonces, $P_1, P_2, ..., P_m$ serán todos los ceros de $x \in \mathbb{P}_{F'}$. Por otro lado tenemos:

$$\begin{aligned}[F' : K(x)] &= [F' : K'(x)][K'(x) : K(X)] = (\sum_{i=1}^{m} v_{P_i}(x) grado(P_i))[K' : K] = \\ &= \sum_{i=1}^{m} e_i v_P(x)[F'_{P_i} : K'][K' : K] = r \sum_{i=1}^{m} e_i [F'_{P_i} : F_P][F_P : K] = \\ &= r \cdot grado(P) \sum_{i=1}^{m} e_i f_i. \end{aligned} \tag{1.8}$$

Por otro lado:

$$[F' : K(x)] = [F' : F][F : K(x)] = [F' : F] r \cdot grado(P) \tag{1.9}$$

y utilizando las igualdades (1.8) y (1.9) obtenemos:

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

con lo que la demostración queda terminada. □

Corolario 1.5.1. *Si F'/K es una extensión finita de F/K y sea $P \in \mathbb{P}_F$, entonces:*

(a) $|\{P' \in \mathbb{P}_{F'} : P'|P\}| < [F' : F]$.

(b) Si $P' \in \mathbb{P}_{F'}$ *y* $P'|P$ *entonces* $e(P'|P) \leq [F' : F]$*y* $f(P'|P) \leq [F' : F]$.

(c) Para cualquier $A \in \mathcal{D}_F$ *se tiene:*

$$grado(con_{F|F'}(A)) = \frac{[F' : F]}{K' : K} grado(A). \tag{1.10}$$

Demostración. Los incisos (a) y (b) se siguen de la siguiente desigualdad:

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

pues $e_i \geq 1$ y $[F'_{P_i} : F_P] \geq 1$. Para demostrar el inciso (c) tomamos un divisor primo $A = P \in \mathbb{P}_F$. Se tiene:

$$\begin{aligned} grado(Con_{F'|F}(P)) &= grado(\sum_{P'|P} e(P'|P) \cdot P') = \sum_{P'|P} e(P'|P) grado(P) = \\ &= \sum_{P'|P} e(P'|P)[F'_P : K']. \end{aligned} \tag{1.11}$$

Utilizando 1.9 y sustituyendo en 1.11:

$$\begin{aligned} grado(Con_{F'|F}(P)) &= \sum_{P'|P} e(P'|P)[F'_P : K'] = \sum_{P'|P} e(P'|P)\frac{[K' : K]}{[F'_P : K]} = \\ &= \frac{1}{[K' : K]} \sum_{P'|P} e(P'|P)[F'_P : F_P])[F_P : K] = \\ &= \frac{1}{[K' : K]} \sum_{P'|P} e(P'|P) \cdot f(P'|P))grado(P) = \\ &= \frac{[F' : F]}{[K' : K]} \cdot grado(P) \end{aligned}$$

□

Observación 1.5.5. Ahora se tienen las herramientas necesarias para presentar y demostrar un criterio útil para determinar la irreducibilidad de ciertos polinomios sobre un campo de funciones.

Proposición 1.5.3. *(Criterio de Einsentein para la irreducibilidad de polinomios). Vamos a considerar un campo de funciones F/K y un polinomio*

$$\phi(T) = a_n T^n + a_{n-1}T^{n-1} + ... + a_0$$

con coeficientes $a_i \in F$ y también supondremos que existe al menos un $P \in \mathbb{P}_F$ que satisface al menos una de las siguientes condiciones:

(1) $V_P(a_n) = 0$, $V_P(a_i) \geq V_P(a_0) \geq 0$ $\forall i = 1, ..., n-1$ *y* $mcd(n, V_P(a_0)) = 1$.

(2) $V_P(a_n) = 0$, $V_P(a_i) \geq 0$ $\forall i = 1, ..., n-1$, $V_P(a_0) < 0$ *y* $mcd(n, V_P(a_0)) = 1$.

Entonces podremos decir que $\phi(T)$ es un polinomio irreducible sobre F. Si se tiene $F' = F(y)$ donde $\phi(y) = 0$ entonces P tiene una única extensión $P \in \mathbb{P}_F$ y $e(P'|P) = n$ y $f(P'|P) = 1$.

Demostración. Sea $F = F(y)$ una extensión de campo tal que $\phi(y) = 0$. Sabemos que el grado de la extensión $[F' : F]$ estará acotado superiormente por $grado(g)$, es decir $[F' : F] \leq n$ donde la igualdad se cumplirá si y solamente si el polinomio $\phi(y)$ es un irreducible en $F[T]$. Sea P' un lugar de F' extensión de P. Como $\phi(y)$=0,

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

Ahora, supongamos que se cumple la condición (1). Como $v_{P'}(a_n) = 0$ y $v_{P'}(a_i) > 0$ para todo $i = 1, \ldots, n-1$, podemos concluir que $v_{P'}(y) > 0$. Como $e = e(P'|P)$ tenemos:

$$v_{P'}(a_0) = e \cdot v_P(a_0) \quad \text{y} \quad v_{P'}(a_i y^i) = e v_P(a_i) + i v_{P'}(y)$$

pero $e v_P(a_i) + i v_{P'}(y) > e \cdot v_P(a_0)$ para $i = 1, ..., n-1$. Además, usando la desigualdad estricta del triángulo, obtendremos que:

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

. Considerando que el máximo común divisor de n y $v_P(a_0)$ es uno y por propiedades de divisibilidad de números enteros, concluimos que $n|e$ por lo que $n \leq e$. Por otro lado $n \geq [F' : F] \geq e$ por lo que obtenemos:

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

de donde se sigue el resultado. La demostración es similar si se supone que solamente se cumple la condición (2). □

1.6. Ejemplos de Campos Algebraicos de Funciones

El propósito de esta sección es presentar dos ejemplos concretos de campos de funciones y algunas de sus propiedades. Estos campos, los campos elípticos y los campos hermitianos, serán utilizados en la construcción de códigos geométricos del siguiente capítulo. De cada uno de estos ejemplos, se presentarán algunas de sus propiedades. Las demostraciones de éstas e información más detallada se pueden encontrar en el capítulo 6 de [15].

1.6.1. Campos elípticos

Definición 1.6.1. *Un campo de funciones F/K es nombrado* **elíptico** *si su género $g = 1$ y si existe un divisor $A \in \mathcal{D}_F$ tal que $grado(A) = 1$.*

Observación 1.6.1. Sea F/K un campo elíptico, entonces

(a) Del Teorema de Riemann Roch tenemos que $dimA = grado(A) + 1 - g$, por lo que si A es un divisor de grado 1 en F/K, entonces $dimA = 1$ por lo que A es equivalente a un divisor efectivo A_1 de grado 1, así $A_1 := P \in \mathbb{P}_F$ es un lugar de grado 1. De esta manera, en un campo elíptico existe un lugar de grado 1.

(b) Si $char(F) = 2$ existen $y, x \in F$ tales que $F = (x, y)$ y

$$y^2 + y = f(x) \quad \in \quad K[x] \quad \text{con} \quad grado(f) = 3,$$

ó

$$y^2 + y = x + \frac{1}{ax + b} \quad \text{con} \quad a, b, \in K \quad \text{y } a \neq 0.$$

Ejemplo 1.6.1. *Sea $K := \mathbb{F}_{2^3}$ donde $\alpha^3 + \alpha + 1 = 0$ y $F = K(x, y)$ con $y^2 + y + x^3 + x + 1 = 0$ y sea P_∞ el polo de $x \in \mathbb{P}_{K(x)}$.*

- *El criterio de Eisenstein nos indica que el polinomio $T^2 + T + (x^3 + x + 1)$ es un polinomio irreducible sobre $K[x]$, así $[F : K(x)] = 2$. Además, el mismo criterio nos*

dice que hay un único lugar Q_∞ que está encima del lugar P_∞ y que $e(Q_\infty|P_\infty) = 2$ por lo que $f(Q_\infty|P_\infty) = 1$ lo que implica Q_∞ es un lugar de grado 1 en F así:

$$V_{Q_\infty}(x) = 2 \cdot V_{P_\infty}(x) = -2$$

además,

$$\begin{aligned} V_{Q_\infty}(y^2 + y) &= \text{mín}\{\, V_{Q_\infty}(y^2),\ V_{Q_\infty}(y)\,\} \\ &= \text{mín}\{\, 2 \cdot V_{Q_\infty}(y),\ V_{Q_\infty}(y)\,\} \\ &= 2 \cdot V_{Q_\infty}(y), \end{aligned}$$

pero, $y^2 + y = -(x^3 + x + 1)$ de donde $V_{Q_\infty}(y^2 + y) = V_{Q_\infty}(x^3 + x + 1)$, así:

$$\begin{aligned} V_{Q_\infty}(y^2 + y) &= \text{mín}\{\, V_{Q_\infty}(x^3),\ V_{Q_\infty}(x),\ V_{Q_\infty}(1)\,\} \\ &= \text{mín}\{\, 3 \cdot V_{Q_\infty}(x),\ V_{Q_\infty}(x),\ V_{Q_\infty}(1)\,\} \\ &= 3 \cdot V_{Q_\infty}(x) = 3(-2) \end{aligned}$$

así, $2 \cdot V_{Q_\infty}(y) = 3(-2)$ por lo tanto:

$$V_{Q_\infty}(y) = -3.$$

De lo anterior,

$$\begin{aligned} (x)_\infty^F &= 2Q_\infty \\ y \quad (y)_\infty^F &= 3Q_\infty. \end{aligned}$$

- *Del párrafo anterior, tenemos que las funciones de la forma $x^i y^j$ pertenecerán al espacio $\mathcal{L}(rQ_\infty)$ siempre y cuando se cumpla:*

$$0 \le 2i + 3j \le r.$$

- *Sea $Q \in \mathbb{P}_F \backslash Q_\infty$ de grado 1. Si aplicamos el mapeo de la definición 1.1.4 (c) a las funciones x y y en el lugar Q, obtendremos $x_1 := x(Q)$, $y_1 := y(Q) \in \mathbb{F}_{2^3}$ tales que:*

$$y_1^2 + y = x_1^3 + x + 1 \tag{1.12}$$

es decir, los lugares de grado 1 quedarán determinados por los pares de elementos $(x_1, y_1) \in \mathbb{F}_{2^3}^2$ tales que 1.12 se cumpla.

1.6.2. Campos hermitianos

Definición 1.6.2. *Un* **c***ampo hermitiano de funciones (o simplemente «campo hermitiano») sobre* $\mathbb{F}_{q^2}$ *es un campo* $H = \mathbb{F}_{q^2}(x, y)$ *en donde se cumple que* $y^q + y = x^{q+1}$.

Ejemplo 1.6.2. *Sean* $q = 2^3$, $K = \mathbb{F}_{2^6}$ *y* $F = \mathbb{F}_{2^6}(x, y)$ *donde* $y^8 + y = x^9$. *Sea* P_∞ *el divisor de polos de* x *en* $\mathbb{P}_{\mathbb{F}_{2^3}(x)}$. *Por el Criterio de Eisenstein el polinomio* $\varphi(T) = T^8 + T + x^9$ *es irreducible en* $\mathbb{F}_{2^3}(x)[T]$. *Además,* P_∞ *tiene una única extensión* $Q_\infty \in \mathbb{P}_F$ *y:*

$$e(Q_\infty|P_\infty) = 8$$

$$y \quad f(Q_\infty|P_\infty) = 1,$$

de donde Q_∞ *es un lugar de grado 1 en* F. *Así:*

$$(x)^F_\infty = -v_{Q_\infty}(x)Q_\infty = -8v_{P_\infty}(x)Q_\infty = 8Q_\infty, \tag{1.13}$$

así $V_{Q_\infty}(y^2 + y) = V_{Q_\infty}(x^9)$ *por lo que:*

$$\text{mín}\{\ V_{Q_\infty}(y^2),\ V_{Q_\infty}(y)\ \} = 2V_{Q_\infty}(y) = -2 \cdot 9,$$

por lo tanto $V_{Q_\infty}(y) = -9$ *y*

$$(y)^F_\infty = 9Q_\infty. \tag{1.14}$$

así, De 1.13 y 1.14 obtenemos que 8 *y* 9 *son órdenes polares de* Q_∞ *en* F. *El subconjunto* $\boldsymbol{S}_{Q_\infty}$ *de enteros que son órdenes polares de* Q_∞ *forma un semigrupo, el cual queda descrito de la siguiente forma:*

$$\boldsymbol{S}_{Q_\infty} = \{\ s \in \mathbb{Z} \mid s = 9r + 8t \text{ con } r, t \geq 0\ \}. \tag{1.15}$$

El conjunto $\boldsymbol{G}_{Q_\infty}$ *de enteros positivos que no pertenecen a* $\boldsymbol{S}_{Q_\infty}$ *es el conjunto:*

$$\begin{aligned} \boldsymbol{G}_{Q_\infty} \quad = \quad & \{\ 1, 2, 3, 4, 5, 6, 7, 10, 11, 12, 13, 14, 15, 19, 20, \\ & 21, 22, 23, 28, 29, 30, 31, 37, 38, 39, 46, 47, 55\}. \end{aligned}$$

Si g *es el género de* F *y usando el Teorema de Saltos de Weierstrass, tenemos que:*

$$|\boldsymbol{G}_{Q_\infty}| = 28 = g.$$

Notemos además que $2g - 1 = 55$.

Observación 1.6.2. Un campo hermitiano $H = \mathbb{F}_{q^2}(x, y)$, se cumplen las siguientes

propiedades:

(a) El género de H es $g = q(q-1)/2$.

(b) H tiene $q^3 + 1$ lugares de grado 1 sobre $\mathbb{F}_{q^2}$ de los cuales:

- Uno será el polo común Q_∞ de y,
- para cada $\alpha \in \mathbb{F}_{q^2}$ existen q elementos $\beta \in \mathbb{F}_{q^2}$ tales que:

$$\beta^q + \beta = \alpha^{q+1}$$

y para cada uno de los pares (α, β) existe un único lugar tal que $P_{\alpha,\beta} \in \mathbb{P}_H$ de grado uno con $x(P_{\alpha,\beta}) = \alpha$ y $y(P_{\alpha,\beta}) = \beta$.

(c) Para $r \geq 0$ los elementos $x^i y^j$ que cumplen con $0 \leq i$, $0 \leq j \leq q-1$ y $iq + j(q+1) \leq r$ forman una base de $\mathcal{L}(rQ_\infty)$.

Capítulo 2

Códigos de Goppa

El principal objetivo de este capítulo es presentar el algoritmo de Skorobogatov para la decodificación de códigos geométricos. Comenzaremos dando las nociones básicas de la Teoría de Códigos y dando una clasificación de algunos tipos de códigos. Para mayor referencia se puede consultar [6] y [7]. Después, se presentará una construcción de los códigos geométricos y sus principales propiedades para terminar con un algoritmo de decodificación de éstos y dando explícitamente un ejemplo de éste.

2.1. Nociones básicas

Definición 2.1.1. *Un **código C** sobre el campo $\mathbb{F}_q$, será un subespacio vectorial de $\mathbb{F}_q^n$. Nos referimos a sus elementos como **palabras del código**. La **longitud de C** será n y su **dimensión** será la dimensión de C como $\mathbb{F}_q$-espacio vectorial. Un* **Código-**$[n,k]_q$ *será un código de longitud n, dimensión k definido sobre $\mathbb{F}_q$.*

Observación 2.1.1. En general, se puede definir un código sobre cualquier conjunto finito no vacío. En particular, cuando un código C se define sobre $\mathbb{F}_q$ y C es un subespacio vectorial de $\mathbb{F}_q^n$, el código recibe el nombre de **código lineal**.

Definición 2.1.2. *Sean $a = (a_1, \ldots, a_n)$ y $b = (b_1, \ldots, b_n)$ elementos de $\mathbb{F}_q^n$. Definimos*

$$\boldsymbol{d(a,b)} := |\{i; a_i \neq b_i\}|.$$

*como la **distancia de Hamming**. Para cada elemento a de $\mathbb{F}_q^n$ **el peso de a** será el entero $d(a, \overline{0}) := \boldsymbol{w}(a)$.*

Observación 2.1.2. La distancia de Hamming es una métrica. En particular, hacemos mención que se cumplirá la desigualdad del triángulo, es decir, para $a, b, c \in \mathbb{F}_q^n$:

$$d(a,c) \leq d(a,b) + d(b,c).$$

Definición 2.1.3. *(a) La **distancia mínima $d(C)$** de un código C será:*

$$d(C) := min\{d(a,b) \mid a, b \in C \text{ y } a \neq b\}.$$

(b) A un código $[n,k]_q$ con distancia mínima $d(C)$, lo denotaremos como $\boldsymbol{[n,k,d]_q}$.

*(c) El **peso mínimo $w(C)$** de un código C será:*

$$\boldsymbol{w}(C) := min\{w(c) \mid c \in C \text{ y } c \neq \overline{0}\}.$$

Observación 2.1.3. Como $d(a,b) = d(a-b, 0) = w(a-b)$ y C es un subespacio de $\mathbb{F}_q^n$, entonces la distancia mínima es igual a:

$$d(C) := min\{w(c) \mid 0 \neq c \in C\}.$$

Definición 2.1.4. *Sea C un código $[n,k]_q$. Una **matriz generadora de C** es una matriz de $k \times n$, cuyos renglones son los elementos de una base de C como un $\mathbb{F}_q$ espacio vectorial.*

Definición 2.1.5. *Para dos elementos $\boldsymbol{a} = (a_1, \ldots a_n)$, $\boldsymbol{b} = (b_1, \ldots b_n) \in \mathbb{F}_q^n$, definimos el producto interior de $\boldsymbol{a}$ y $\boldsymbol{b}$ como:*

$$< \boldsymbol{a}, \boldsymbol{b} >:= \sum_{i=1}^{n} a_i b_i.$$

Definición 2.1.6. *Sea C un código lineal.*

(i) El ***código dual*** $C^{\perp}$ ***de*** C *será el código lineal:*

$$\boldsymbol{C^{\perp}} := \{x \in \mathbb{F}_q^n \mid < x, y >= 0 \ \forall y \in C\}$$

(ii) Si $C = C^{\perp}$ se dice que el código C es **auto-dual**.

(iii) A una matriz generadora H para el código $C^{\perp}$, la nombramos ***matriz de verificación*** *para C.* [1]

Observación 2.1.4. Se hacen las siguientes observaciones acerca del código $C^{\perp}$ y de su matriz H:

(a) Se tiene que para todo código lineal C, $(C^{\perp})^{\perp} = C$.

(b) Si H es la matriz de verificación de C, entonces $c \in C$ si y solo si $H \cdot c = 0$. Esta afirmación le permite al receptor verificar si hubo errores de transmisión: si el producto $H \cdot c$ es distinto de cero, entonces la palabra c no pertenece al código.

(c) Si un código lineal C con parámetros $[n, k, d]$ tiene a G como matriz generadora y $G = (I|X)$, donde I es la matriz identidad de $k \times k$, entonces, la matriz $(-X^T|I')$, con I' la matriz identidad de $n-k \times n-k$ es una matriz de verificación para C.

Observación 2.1.5. Uno de los objetivos de la teoría de códigos es poder construir códigos cuya dimensión y distancia mínima sean muy grandes en comparación con su longitud por lo que se quiere establecer relaciones entre sus parámetros. La siguiente proposición establece una cota superior para la dimensión y la distancia mínima de un código C en términos de su longitud. Observemos que la cota no involucra a q. Por otro lado el resultado establece una cota superior para la distancia mínima de un código. En general, se conocen pocas cotas inferiores para este parámetro.

[1] Esta matriz también es conocida con el nombre de: matriz de verificación de paridad.

Proposición 2.1.1. *(Cota de Singleton). Para un $[n, k, d]$-código C, se tiene que*

$$k + d \leq n + 1. \tag{2.1}$$

Demostración. Sea $W \subseteq \mathbb{F}_q^n$ un subepacio dado por:

$$W := \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n \mid a_i = 0 \ \forall i \geq d\}.$$

Cualquier $a \in W$ tiene peso a lo más $d-1$, por lo que $W \cap C = 0$. Además, $dim\ W = d-1$ por lo que tenemos:

$$\begin{aligned} k + (d-1) &= dimC + dimW \\ &= dim(C + W) + dim(C \cap W) \\ &= dim(C + W) \leq n, \end{aligned}$$

por lo tanto, $k + d \leq n + 1$. □

Observación 2.1.6. Si un código cumple la igualdad en la ecuación 2.1 se dirá que es un código de **Distancia Máxima Separable** (o **MDS** por sus siglas en inglés, *Maximum Distance Separable*). Al número entero $\boldsymbol{s(C)} := n - k + 1 - d$, lo llamaremos **defecto de Singleton**.

Ejemplo 2.1.1. *(Códigos de Reed Solomon) Consideraremos el campo $\mathbb{F}_q$ con $q = p^r$ para p un número primo y $r \in \mathbb{Z}^+$, $n = q - 1$ y β un elemento primitivo del grupo multiplicativo $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Para un entero k tal que $1 \leq k \leq n$ consideramos el $\mathbb{F}_q$-espacio vectorial:*

$$\mathcal{L}_k := \{f \in \mathbb{F}_q[X] \mid grado(f) \leq k - 1\}$$

y el mapeo de evaluación:

$$\begin{aligned} ev: \ \mathcal{L}_k &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(\beta), f(\beta^2), ..., f(\beta^n)). \end{aligned}$$

Dado que un polinomio de grado menor a n tiene menos de n ceros, $ker(ev) = \{0\}$ *por lo que será un mapeo inyectivo. Definimos:*

$$C_k := \{(f(\beta), f(\beta^2), ..., f(\beta^n))|f \in \mathcal{L}_k\}$$

así, C_k *resulta ser un código lineal* $[n, k]_q$*. A este tipo de códigos se les conoce como códigos de Reed Solomon. Sea* $c \in C_k$*,* $c \neq 0$ *y sea* $Z = \{i \in \{1, ..., n-1\}|f(\beta^i) = 0\}$ *entonces:*

$$w(c) := n - |Z|,$$

como ya lo habíamos mencionado, f *no puede tener más ceros que su grado, es decir:* $|Z| \geq grado(F) \geq (k-1)$ *por lo que* $w(c) \geq n - (k+1)$*. Concluimos que* C_k *tiene parámetros* $[n, k, n-k+1]_q$*.*

2.2. Códigos Geométricos

Para esta sección, utilizaremos la siguiente notación:

- $F/\mathbb{F}_q$ será un campo de funciones algebraico de género g,
- $\{P_1, \ldots, P_n\}$ un conjunto de lugares (distintos dos a dos) de $F/\mathbb{F}_q$ y grado 1,
- $D := P_1 + \ldots + P_n$ un divisor de $F/\mathbb{F}_q$,
- G un divisor de $F/\mathbb{F}_q$ tal que $soporte(G) \cap soporte(D) = \emptyset$.

Definición 2.2.1. *El **Código de Goppa Geométrico** (o Código Geométrico)*[2] $\boldsymbol{C_{\mathcal{L}}(D,G)}$ *asociado a los divisores D y G lo definimos como:*

$$C_{\mathcal{L}}(D,G) := \{(x(P_1), \ldots, x(P_n)) \mid x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

Observación 2.2.1. Como $soporte(G) \cap soporte(D) = \emptyset$, si $x \in \mathcal{L}(G)$ entonces $v_{P_i} \geq 0$ para $i = 1, \ldots, n$, es decir, f está bien definida en P_i. Además, $grado(P_i) = 1$ por lo que el campo residual del lugar P_i será $\mathbb{F}_q$. Así $x(P_i) \in F_{P_i} = \mathbb{F}_q$. Vamos a considerar el mapeo de evaluación: $ev_D : \mathcal{L}(G) \to \mathbb{F}_q^n$ dado por:

$$ev_D(x) := (x(P_1), x(P_2), \ldots, x(P_n)) \ \in \ \mathbb{F}_q^n. \tag{2.2}$$

Se tiene que el mapeo ev_D es lineal y $C_{\mathcal{L}}(D,G)$ resulta la imagen de $\mathcal{L}(G)$ bajo este mapeo. De esta forma se establece una analogía de estos códigos con los códigos de Reed Solomon (ver ejemplo 2.1.1). Además, es posible ver a los códigos de Reed Solomon como un caso particular de los códigos geométricos, (ver [7]).

[2] En algunos textos, estos códigos son nombrados códigos AG*(Algebraic Geometric Codes)*. También se hace la aclaración de que exite otro tipo de códigos llamados Códigos de Goppa ó *Códigos Clásicos de Goppa.*

Teorema 2.2.1. *$C_{\mathcal{L}}(D,G)$ es un $[n,k,d]$-código donde:*

$$k = dim\ G - dim\ (G-D), \qquad y \qquad d \geq n - grado\ G.$$

Demostración. Consideremos el mapeo

$$\begin{aligned} \xi : \ \mathcal{L}(G) &\longrightarrow C_{\mathcal{L}}(D,G) \\ x &\longmapsto (x(P_1), \ldots, x(P_n)) \end{aligned}$$

Primero veamos que $ker(\xi) = \mathcal{L}(G-D)$: si $x \in ker(\xi)$ entonces $x(P_i) = 0$ para $i = 1, \ldots, n$ por lo que $V_{P_i} > 0$, es decir $V_{P_i} \geq 1$. Como $soporte(G) \cap soporte(D) = \emptyset$ entonces $(x) + G - (P_1 + \ldots + P_n) \geq 0$ por lo tanto $x \in \mathcal{L}(G-D)$, así $ker(\xi) \subseteq \mathcal{L}(G-D)$. La contención contraria es inmediata pues si $x \in \mathcal{L}(G-D)$ entonces $V_{P_i}(x) > 0$. De esta manera obtenemos que:

$$dim\mathcal{L}(G) - dim\mathcal{L}(G-D) = dimC_{\mathcal{L}}(D,G) = k.$$

Como solo nos interesan códigos no triviales, podemos suponer que $0 \neq C_{\mathcal{L}}(D,G)$. Sea $s \in \mathcal{L}(G)$, si $w(x) = d$ entonces hay d lugares P_i tales que $x(P_i) \neq 0$, consequentemente tenemos $n-d$ lugares con $x(P_i) = 0$, sean $P_{i_1}, P_{i_2}, \ldots, P_{i_{n-d}}$ dichos lugares. Tenemos que $V_{P_{i_1}}(x), V_{P_{i_2}}(x), \ldots, V_{P_{i_{n-d}}}(x) > 0$ por lo que $x \neq 0$ y

$$x \in \mathcal{L}(G - (P_{i_1} + P_{i_2} + \ldots + P_{i_{n-d}})).$$

Así, $0 \leq grado(G - (P_{i_1} + P_{i_2} + \ldots + P_{i_{n-d}})) = grado(G - (n-d)) = grado(G) - n + d$, obteniendo la desigualdad $d \geq grado(G) - n$. □

Corolario 2.2.1. *Sea G un divisor tal que $grado(G) < n$, entonces:*

(a) El mapeo $\xi : \mathcal{L}(G) \longrightarrow C_{\mathcal{L}}(D,G)$ es inyectivo.

(b) $C_{\mathcal{L}}(D,G)$ es un $[n,k,d]$-código, con: $k + d \geq 1 + n - g$.

(c) Si $2g - 2 < grado(G) < n$ entonces $k = grado(G) + 1 - g$.

(d) Si $\{x_i, \ldots, x_k\}$ es base de $\mathcal{L}(G)$, la matriz generadora de $C_{\mathcal{L}}(D, G)$ será:

$$M = \begin{pmatrix} x_1(P_1) & x_1(P_2) & \cdots & x_1(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ x_k(P_1) & x_k(P_2) & \cdots & x_k(P_n) \end{pmatrix}$$

Demostración.

(a) Del teorema (2.2.1) tenemos que $k = dim\ G - dim\ (G - D)$. Por otro lado:

$$\begin{aligned} grado\ (G - D) &= grado(G) - grado(D) \\ &= grado(G - n) < 0, \end{aligned}$$

así $dim\ (G - D) = 0$. Como $\mathcal{L}(G - D) = ker(\xi)$ por lo que el mapeo ξ es inyectivo.

(b) Por el teorema de Riemann-Roch y el teorema 2.2.1 se llega a que:

$$k = dim\ G \geq grado(G) + 1 - g,$$

por lo tanto:

$$\begin{aligned} k + d &\geq grado(G) + 1 - g + n - grado(G) \\ \Longrightarrow k + d &\geq 1 + n - g. \end{aligned}$$

Las afirmaciones (c) y (d) se siguen del teorema de Riemann-Roch y del teorema 2.2.1. □

Observación 2.2.2. Si suponemos que $grado(G) < n$, por la Cota de Singleton (proposición 2.1.1) y el corolario 2.2.1 (b):

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

Definición 2.2.2. *Llamamos* **distancia de diseño** *del código $C_{\mathcal{L}}(D, G)$ al número entero* $\boldsymbol{d^* := n - grado(G)}$.

Lema 2.2.1. *Sea dim $G > 0$ y $d^* > 0$. Entonces $d^* = d$ si y solo si existe un divisor D' con $0 \leq D' \leq D$, grado$(D') =$ grado(D) y dim$(G - D') > 0$.*

Demostración. Si suponemos que $d^* = d$, entonces existe un elemento $x \neq 0 \in \mathcal{L}(G)$ tal que cada palabra $(x(P_1), \ldots, x(P_n)) \in C_{\mathcal{L}}(D, G)$ tiene

$$k = n - d = n - d^* = grado(G)$$

entradas iguales a cero, sean $x(P_{i_j})$ con $j = 1, \ldots, grado(G)$ dichas entradas. Formamos el divisor $D' = \sum_{j=1}^{grado(G)} P_{i_j}$. Se tiene que $0 \leq D' \leq D$ de donde, $grado(D') = grado(G)$ y como $x \in \mathcal{L}(G - D')$ entonces $dim(G - D') > 0$.

Por otro lado, si D' cumple las hipótesis escogemos un elemento $y \neq 0 \in \mathcal{L}(G - D')$, así la palabra correspondiente al elemento y será $(y(P_1), \ldots, y(P_n))$ cuyo peso es claramente $n - grado(G) = d^* = d$, por lo que $d^* = d$. □

Observación 2.2.3. Para definir el siguiente código, utilizaremos los Diferenciales de Weil. Recordemos que para cada divisor A en $\mathcal{D}_F$, $\Omega_F(A)$ es el espacio de los diferenciales de Weil ω tal que $(\omega) \geq A$. Este espacio es un espacio vectorial de dimensión finita sobre $\mathbb{F}_q$ de dimensión $i(A)$. Para cada diferecial ω y para cada lugar P en $\mathbb{P}_F$, $\omega_P : F \longrightarrow \mathbb{F}_q$ denota la componente local de ω en P.

Definición 2.2.3. *Sea G y $D = P_1 + \ldots + P_n$ dos divisores que cumplen las características enunciadas al principio de esta sección. Definimos el código $C_\Omega(D, G)$ como:*

$$C_\Omega(D, G) := \{(\omega_{P_1}(1), \ldots, \omega_{P_n}(1)) \mid \omega \in \Omega_F(G - D)\}.$$

Teorema 2.2.2. *El código $C_\Omega(D, G)$ es un código $[n, k', d']$ donde $k' = i(G - D) - i(G)$ y $d' \geq grado(G) - (2g - 2)$. Además,*

(a) Si $grado(D) > 2g - 2$ se tiene que $k' = i(G - D) \geq n + g - 1 - grado(D)$.

(b) Si $2g - 2 < grado(G) < n$ entonces $k' = n + g - 1 - grado(G)$.

Demostración. Sea $P \in \mathbb{P}_F$ tal que $grado(P) = 1$ y ω un diferencial de Weil que cumple $v_P(\omega) \geq -1$. Queremos demostrar que $\omega_P(1) = 0$ si y solo si $v_P(\omega) \geq 0$. Primero observamos que para cada entero r, se tiene que:

$$v_p(\omega) \geq r \Longleftrightarrow \omega_P(x) = 0 \text{ para todo } x \in F \text{ con } v_p(x) \geq -r, \tag{2.4}$$

así, $v_P(\omega) \geq 0$ implica $\omega_P(1) = 0$. Por otro lado, si suponemos que $\omega_P(1) = 0$. Sea $x \in F$ con $v_P(x) \geq 0$. Como $grado(P) = 1$ entonces $x = a + y$ con $a \in \mathbb{F}_q$ y $v_P(y) \geq 1$. Así,

$$\omega_P(x) = \omega_P(a) + \omega_P(y) = a \cdot \omega_P + 0 = 0.$$

Como $v_P(\omega) \geq -1$ y $v_P(y) \geq 1$ entonces $\omega_P(y) = 0$.

Consideramos el mapeo:

$$\begin{aligned} \phi : \quad \Omega_F((G-D)) &\longrightarrow C_{\mathcal{L}}(D,G) \\ \omega &\longmapsto (\omega_{P_1}(1), \ldots, \omega_{P_n}(1)), \end{aligned}$$

por el lema 2.2.1 tenemos que ϕ es un mapeo suprabreyectivo con $ker(\phi) = \Omega_F(G)$, así,

$$k' = dim\ \Omega_F((G-D)) - dim\ G. \tag{2.5}$$

Sea $\phi_D(\omega)$ una palabra del código $C_{\mathcal{L}}(D,G)$ con peso m, es decir, $\omega_{P_{i_j}}(1) = 0$ con $j = 1, \ldots, (n-m)$ y sea M el divisor formado por tales lugares:

$$M := \sum_{j=1}^{(n-m)} P_{i_j}. \tag{2.6}$$

Observamos que $\omega \in \mathcal{L}(G - (D - M))$. Como $\Omega_F(A) \neq 0$ entonces $grado(A) \leq 2g - 2$ así, $2g - 2 \geq grado(G) - m$, por lo tanto la distancia mínima d' de $C_{\mathcal{L}}(D,G)$ cumple que: $d' \geq grado(G) - (2g-2)$. Si $grado(G) > 2g - 2$ entonces $i(G) = 0$ y además,

$$\begin{aligned} k' = i(G-D) &= dim\ (G-D) - grado((G-D)) - 1 + g \\ &= dim\ (G-D) + n + g - 1 - grado(G), \end{aligned}$$

con lo que queda demostrado el teorema. □

Observación 2.2.4. De la definición de $i(G)$ (1.3.2), obtenemos que:

$$i(G-D) - i(G) = dim(G-D) - dim(G) + grado(G). \tag{2.7}$$

Lema 2.2.2. *Sea $P \in \mathbb{P}_F$ con $grado(P) = 1$, ω un diferencial de Weil con $v_P(\omega) \geq -1$ y $x \in F$ con $v_P(x) \geq 0$, entonces $\omega_P(x) = x(P)\omega_P(1)$.*

Demostración. Si escribimos $x = a + y$ con $a = x(P) \in \mathbb{F}_q$ y $v_P(y) > 0$, entonces, usando las implicaciones del enunciado 2.4 tenemos que:

$$\omega_P(x) = \omega_P(y) = a \cdot \omega_P(1) + 0 = x(P) \cdot \omega_P(1),$$

obteniendo así la igualdad deseada. □

Teorema 2.2.3. *Los códigos $C_{\mathcal{L}}(D,G)$ y $C_{\Omega}(D,G)$ son códigos duales uno del otro, es decir:*

$$C_{\mathcal{L}}(D,G) = C_{\Omega}(D,G)^{\perp}.$$

Demostración. Primero observamos que para $P \in \mathbb{P}_F \backslash \{P_1, P_2, \ldots, P_n\}$ tenemos que $v_P(x) \geq -v_P(\omega)$, pues $x \in G$ y $\omega \in \Omega(G-D)$, utilizando 2.4, tenemos que:

$$\omega_P(x) = 0. \tag{2.8}$$

Para demostrar la afirmación vamos a probar $C_{\Omega}(D,G) \subseteq C_{\mathcal{L}}(D,G)^{\perp}$ y que los códigos $C_{\Omega}(D,G)$, $C_{\mathcal{L}}(D,G)^{\perp}$ tienen la misma dimensión. Sea $\omega \in \Omega_F(G-D)$ y sea $s \in \mathcal{L}(G)$. Se tiene que:

$$\begin{aligned}
0 = \omega(x) &= \sum_{P \in \mathbb{P}_F} \omega_P(x) \\
&= \sum_{i=1}^{n} \omega_{P_i}(x) && \text{[usando 2.8]} \\
&= \sum_{i=1}^{n} x(P_i) \cdot \omega_{P_i}(1) && \text{[usando 2.2.2]} \\
&=< (\omega_{P_1}(1), \ldots, \omega_{P_n}(1)), (x(P_1), \ldots, x(P_1)) >,
\end{aligned}$$

Por lo que $C_\Omega(D,G) \subseteq C_{\mathcal{L}}(D,G)^\perp$. Para demostrar que ambos códigos tienen la misma dimensión, debemos utilizar los teoremas 2.2.1 y 2.2.2 para justificar las siguientes igualdades:

$$dimC_\Omega(D,G) = i(G-D) - i(G) =$$

$$\begin{aligned} &= dim(G-D) - grado(G-D) - 1 + g - (dimG - grado(G) + 1 - g) \\ &= grado(D) + dim(G-D) - dimG \\ &= n - (dimG - dim(G-D)) \\ &= n - dimC_{\mathcal{L}}(D,G) = dimC_{\mathcal{L}}(D,G)^\perp, \end{aligned}$$

por lo tanto $dimC_\Omega(D,G) = dimC_{\mathcal{L}}(D,G)^\perp$. □

2.3. Código C_Ω en términos de un $C_{\mathcal{L}}$

Lema 2.3.1. *Existe un diferencial de Weil η tal que:*

$$v_{P_i}(\eta) = -1 \quad y \quad \eta_{P_i}(1) = (1) \quad para \quad i = 1, \ldots, n.$$

Demostración. Sea ω_0 un diferencial diferente de cero. Por el teorema de aproximación débil sabemos que existe un elemento $z \in F$ tal que $v_{P_i}(z) = -v_{P_i}(\omega_0) - 1$ para $i = 1, \ldots, n$. Haciendo $\omega := z\omega_0$ tenemos $v_{P_i}(\omega) = -1$, por lo que $a_i := \omega_{P_i}(1) \neq 0$. Por otro lado, utilizando otra vez el teorema de aproximación débil encontramos $y \in F$ tal que $v_{P_i}(y - q_i) > 0$. Así $v_{P_i}(y) = 0$ y $y(P_i) = a_i$. Haciendo $\eta := y^{-1}w$ se obtiene que $v_{P_i}(\eta) = v_{P_i}(\omega) = -1$ y $\eta_{P_i}(1) = \omega_{P_i}(y^{-1}) \cdot \omega_{P_i}(1) = a_i^{-1} \cdot a_i = 1$. □

Proposición 2.3.1. *Sea η un diferencial de Weil con $v_{P_i}(\eta) = -1$, $\eta_{P_i}(1) = (1)$ para $i = 1, \ldots, n$. Entonces:*

$$C_\Omega(D, G) = C_{\mathcal{L}}(D, H) \qquad con \qquad H := D - G + (\eta).$$

Demostración. Observamos que $soporte(D + G - (\eta)) \cap soporte(D) \neq \emptyset$ pues $v_{P_i}(\eta) = -1$ para toda $i = 1, ..., n$. Entonces $C_{\mathcal{L}}(D, D - G - (\eta))$ está bien definido. Por otro lado, tenemos un isomorfismo

$$\begin{aligned} \mu : \quad \mathcal{L}(D - G - (\eta)) \quad &\longrightarrow \Omega_F(G - D) \\ x \qquad\qquad &\longmapsto \qquad x\eta \end{aligned}$$

por lo que, para $x \in \mathcal{L}(D - G + (\eta))$ entonces, $(x\eta)_{P_i}(1) = \eta_{P_i}(x) = x(P_i) \cdot \eta_{P_i}(1) = x(P_i)$, de donde es inmediato que $C_\Omega(D, G) = C_{\mathcal{L}}(D, D - G + (\eta))$. □

Observación 2.3.1. Si suponemos que existe un diferencial de Weil η tal que

$$(\eta) = 2G - D \quad \text{y} \quad \eta_{P_i}(1) = (1) \quad \text{para todo} \quad i = 1, \ldots, n \quad \text{entonces,}$$

por la proposición anterior, $H = D - G + (\eta) = D - G + 2G - D = G$ eso quiere decir que $C_{\mathcal{L}}(D, G)^\perp = C_{\mathcal{L}}(D, H) = C_{\mathcal{L}}(D, G)$, por lo que tenemos un código auto-dual.

2.4. Ejemplo de un Código Geométrico

Al final de la primera parte de este trabajo dimos ejemplos concretos de campos de funciones. Utilizaremos esos campos para dar la construcción de algunos códigos. Empezaremos por los códigos elípticos.

Definición 2.4.1. *Un* **Código Elíptico** *será el código geométrico construido a partir de un campo elíptico.*

Observación 2.4.1. Utilizando que un campo elíptico tiene género 1 y el corolario 2.2.1, tenemos que $k + d \geq n$, por lo que obtenemos la siguiente relación:

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

es decir, $n = k + d$ o $n + 1 = k + d$.

Ejemplo 2.4.1. *Utilizaremos el campo* $K := \mathbb{F}_{2^3}$ *con elementos* $\{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ *donde* $\alpha^3 + \alpha + 1 = 0$ *y* $F := \mathbb{F}_8(x, y)$ *con* $y^2 + y + x^3 + x + 1 = 0$. *Este campo tiene 12 lugares de grado 1 los cuales etiquetamos de la siguiente forma:*

P_1	$(\alpha, 0)$	P_7	(α^3, α)
P_2	$(\alpha^2, 0)$	P_8	(α^6, α^2)
P_3	$(\alpha^4, 0)$	P_9	(α^5, α^4)
P_4	$(\alpha, 1)$	P_{10}	(α^3, α^3)
P_5	$(\alpha^2, 1)$	P_{11}	(α^5, α^5)
P_6	$(\alpha^4, 1)$	P_{12}	(α^6, α^6)

.

Si queremos construir un código $C_{\mathcal{L}}(D, G)$, *primero debemos indicar cuál será el divisor* D *y cuál será el divisor* G. *En este caso proponemos:*

$$D := \sum_{i=1}^{12} P_i \qquad y \qquad G = 4Q_\infty.$$

El siguiente paso es obtener la base del espacio $\mathcal{L}(4Q_\infty)$*. En este caso dicha base es el conjunto:* $\{1,\ y,\ x,\ x^2\}$*. Este código tiene dimensión* $dim(G) - dim(G - D)$*. Sabemos que si* $grado(G - D) < 0$ *entonces* $dim(G - D) = 0$*. Para este ejemplo:*

$$grado(G - D) = grado(G) - grado(D) = 4 - 12 < 0$$

por lo que $k = dim(C_{\mathcal{L}}(D, G)) = 4$*. De las desigualdades indicadas en 2.1 de la observación 2.2.2, tenemos que:*

$$12 = n + 1 - g \leq k + d \leq n + 1 = 13.$$

es decir, $d = 8$ *ó* $d = 9$*. Para saber la distancia de este código, utilizaremos el resultado del lema 2.2.1. Formamos el siguiente divisor:*

$$D' := P_2 + P_3 + P_4 + P_8,$$

y observamos que es inmediato que se cumplen las condiciones:

$$grado(D') = grado(G) \quad y \quad 0 \leq D' \leq D. \tag{2.9}$$

Queremos saber si $dim(G - D') > 0$*. Si* $f \in \mathcal{L}(G - D')$ *entonces* $(f) + 4Q_\infty \geq D'$*. Por la construcción del código, sabemos que* $soporte(D) \cap soporte(4Q_\infty) = \emptyset$*, en particular,* $soporte(D') \cap soporte(4Q_\infty) = \emptyset$ *por lo que* $v_{P_i}(4Q_\infty) = 0$*, así*

$$v_{P_i}((f) + 4Q_\infty) = v_{P_i}((f)) \geq 1,$$

es decir $f(P_i) = 0$ *con* $i = 2, 3, 4, 8$*. De esta manera, podemos proponer:*

$$f := y + \alpha x^2 + \alpha^2 x + 1$$

pues cumple que $f(P_i) = 0$ *y además es combinación lineal de elementos de la base de* $\mathcal{L}(4Q_\infty)$ *de donde,* $v_{Q_\infty}(f) \geq 4$*, así que podemos decir que* $f \in \mathcal{L}(4Q_\infty - D')$ *por lo que la dimensión de este espacio es mayor a cero y se cumplirán las condiciones necesarias para que se cumpla que* $d = d^* = n - dim(G) = 8$*. Así el código* $C_{\mathcal{L}}(D, 4Q_\infty)$ *tendrá los parámetros:* $[12, 4, 8]$.

Para construir la matriz H generadora del código, nombremos a los elementos de la base de $\mathcal{L}(4Q_\infty)$ *de la siguiente forma:*

$$1 = f_1,\ y = f_2,\ x = f_3,\ x^2 = f_4,$$

Buscamos funciones $g_1, g_2, g_3, g_4 \in \mathcal{L}(4Q_\infty)$ *tales que:*

$$\begin{array}{llll} g_1(P_1) = 1, & g_1(P_2) = 0, & g_1(P_3) = 0, & g_1(P_4) = 0 \\ g_2(P_1) = 0, & g_2(P_2) = 1, & g_2(P_3) = 0, & g_2(P_4) = 0 \\ g_3(P_1) = 0, & g_3(P_2) = 0, & g_3(P_3) = 1, & g_3(P_4) = 0 \\ g_4(P_1) = 0, & g_4(P_2) = 0, & g_4(P_3) = 0, & g_4(P_4) = 1 \end{array}.$$

por lo que deberemos resolver cuatro sistemas de ecuaciones. El primero será:

$$\begin{array}{rcl} af_1(P_1) + bf_2(P_1) + cf_3(P_1) + df_4(P_1) & = & 1 \\ af_1(P_2) + bf_2(P_2) + cf_3(P_2) + df_4(P_2) & = & 0 \\ af_1(P_3) + bf_2(P_3) + cf_3(P_3) + df_4(P_3) & = & 0 \\ af_1(P_4) + bf_2(P_4) + cf_3(P_4) + df_4(P_4) & = & 0 \end{array}.$$

Evaluando las funciones f_i *en los lugares* P_i*, obtenemos el sistema:*

$$\begin{array}{rcrcrcl} a & + & & + & c\alpha & + & d\alpha^2 = 1 \\ a & + & & + & c\alpha^2 & + & d\alpha^4 = 0 \\ a & + & & + & c\alpha^4 & + & d\alpha = 0 \\ a & + & b & + & c\alpha & + & d\alpha^2 = 0 \end{array}.$$

Resolviendo, obtenemos que $a = 1,\ b = 1,\ c = \alpha^2$ *y* $d = \alpha$*, por lo tanto:*

$$g_1 = 1 + y + \alpha^2 x + \alpha x^2.$$

De manera análoga obtenemos las funciones:

$$\begin{aligned} g_2 &= 1 + \alpha^4 x + \alpha^2 x^2. \\ g_3 &= 1 + \alpha x + \alpha^4 x^2. \\ g_4 &= y. \end{aligned}$$

De esta manera, la matriz generadora del código será:

$$H = \begin{pmatrix} g_1(P_1) & g_1(P_2) & g_1(P_3) & \dots & g_1(P_{12}) \\ & \vdots & & \vdots & \\ g_4(P_1) & g_4(P_2) & g_4(P_3) & \dots & g_4(P_{12}) \end{pmatrix}$$

evaluando, obtenemos:

$$H' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & \alpha^6 & \alpha & 0 & \alpha^2 & 1 & \alpha^3 \\ 0 & 1 & 0 & 0 & 1 & 0 & \alpha & \alpha^3 & \alpha & \alpha & \alpha & \alpha^3 \\ 0 & 0 & 1 & 0 & 0 & 1 & \alpha^2 & \alpha^2 & \alpha^6 & \alpha^2 & \alpha^6 & \alpha^2 \\ 0 & 0 & 0 & 1 & 1 & 1 & \alpha & \alpha^2 & \alpha^4 & \alpha^3 & \alpha^5 & \alpha^6 \end{pmatrix}$$

Por lo que una matriz G equivalente a una matriz generadora del código $C_\Omega(D, 4Q_\infty)$, será

$$G \sim \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \alpha^6 & \alpha & \alpha^2 & \alpha & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \alpha & \alpha^3 & \alpha^2 & \alpha^2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & \alpha & \alpha^6 & \alpha^4 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \alpha^2 & \alpha & \alpha^2 & \alpha^3 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & \alpha & \alpha^6 & \alpha^5 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ \alpha^3 & \alpha^3 & \alpha^2 & \alpha^6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Es consecuencia inmediata del Teorema 2.2.2 que la dimensión de este código será 8.

2.5. Decodificación

En esta sección se presentan los resultados necesarios para poder aplicar el Algoritmo de Skorobogatov a la decodificación de los códigos de Goppa. A lo largo de esta sección, C será el código $C_\Omega(D,G)$ de la definición 2.2.3 y los divisores D y G cumplen las hipótesis de la sección anterior.

Definición 2.5.1. *Sea $w \in \mathbb{F}_q^n$ y $\boldsymbol{f \in \mathcal{L}(G)}$. Definimos el **síndrome de w con respecto a f** como:*

$$\boldsymbol{s(w,f)} := \sum_{i=1}^{n} w_i f(P_i)$$

Notación: Para un conjunto R, $R^V := \{\delta \mid \delta : R \to \mathbb{F}_q \text{ es un mapeo } \mathbb{F}_q \text{ lineal}\}$.

Definición 2.5.2. *Definimos el **mapeo síndrome del código C** como:*

$$\begin{aligned} S : \ \mathbb{F}_q^n &\longrightarrow \mathcal{L}(G)^V \\ w &\longmapsto (f \overset{\delta}{\mapsto} s(w,f)). \end{aligned}$$

Observación 2.5.1. Las siguientes observaciones son inmediatas de las definiciones anteriores y serán útiles para el capítulo.

(a) $w \in C$ si y solamente si $s(w,f) = 0$ para toda $f \in \mathcal{L}(G)$.

(b) $S(w) = 0$ si y solo si $w = 0$.

(c) Si $M := dim(G)$ y $\mathcal{L}(G)$ tiene por base al conjunto $\{\gamma_1, \ldots, \gamma_M\}$, entonces S tiene una matriz asociada tal que la entrada (m,j) está dada por $\gamma_m(P_j)$ con $D = P_1 + \ldots + P_n$. Esta matriz coincide con la matriz generadora del código $C_{\mathcal{L}}(D,G)$.

Observación 2.5.2. Sea $A \in \mathcal{D}_F$. Si $f \in \mathcal{L}(A)$ y $h \in \mathcal{L}(G-A)$, entonces $fh \in \mathcal{L}(A)$.

Definición 2.5.3. *Sea $A \in \mathcal{D}_F$ con soporte$(A) \cap$ soporte$(G) = \emptyset$. Definimos la* ***función localizadora de errores*** *de la siguiente manera:*

$$\begin{aligned} \boldsymbol{E_w}: \quad \mathcal{L}(A) &\longrightarrow \mathcal{L}(G-A)^V \\ f &\longmapsto (h \mapsto s(w, fh)). \end{aligned}$$

Observación 2.5.3. Se hacen las siguientes observaciones acerca de la función E_w:

- Forma matricial de E_w: supongamos que $R := dim(A)$ y que $\{\alpha_1, \alpha_2, ..., \alpha_R\}$ forma una base de $\mathcal{L}(A)$. De la misma manera, supongamos que $T := dim(G - A)$ y $\{\beta_1, \beta_2, ..., \beta_T\}$ es una base de $\mathcal{L}(G-A)$, entonces, la función E_w tiene asociada una matriz cuya entrada (t, r) está dada por:

$$\sum_{i=1}^{n} w_i \beta_t \alpha_r(P_i). \tag{2.10}$$

- Si suponemos que $w \in \mathbb{F}_q$ es escrita como $w = e + c$ con $e \notin C$, $c \in C$, entonces $E_w = E_e$. Esta afirmación la podemos deducir de la siguiente manera: sea $f \in \mathcal{L}(G)$ y $E_w(f) = \varphi$, es decir, φ es un mapeo lineal tal que:

$$\begin{aligned} \varphi: \quad \mathcal{L}(G-A) &\longrightarrow \mathbb{F}_q \\ h &\longmapsto s(w, fh), \end{aligned}$$

  pero $s(w, fh) = s(e + c, fh) = s(e, fh) + s(c, fh) = s(e, fh)$, de donde podemos concluir que $E_w = E_e$.

Observación 2.5.4. En nuestro contexto, vamos a suponer que una palabra $c \in C$ es *transmitida* pero ocurren errores de transmisión produciendo que el receptor del mensaje obtenga simplemente $w \in \mathbb{F}_q^n \backslash C$ así que, sin pérdida de generalidad, diremos que $w = c + e$, donde $e \in \mathbb{F}_q^n$, pero no pertenece al código C.

Lema 2.5.1. *Sea $A \in \mathcal{D}_F$ tal que soporte$(A) \cap$ soporte$(D) = \emptyset$ y sea $w \in \mathbb{F}_q^n$ tal que $w = c + e$ con $\{Q_1, \ldots, Q_t\} \subseteq$ soporte(D) el conjunto de lugares donde ocurrieron errores (es decir, soporte$(e) = \{Q_1, \ldots, Q_t\}$) entonces $\mathcal{L}(A - \sum_{i=1}^{t} Q_i)$ es un subespacio de $ker(E_w)$.*

Demostración. Si $k \in \mathcal{L}(A - \sum_{i=1}^{t} Q_i)$ entonces $(k) + A \geq \sum_{i=1}^{t} Q_i$. Por hipótesis se tiene que soporte$(A) \cap$ soporte$(D) = \emptyset$ y $\{Q_1, \ldots, Q_t\} \subseteq$ soporte(D) por lo tanto, $v_{Q_i}(A) = 0$, de manera que $v_{Q_i}((k) + A) = v_{Q_i}(k) \geq 1$ lo que implica que $k(Q_i) = 0$.

Si $E_w(k) = \delta$, entonces δ está definida como sigue:

$$\begin{aligned} \delta : \quad \mathcal{L}(G - A) &\longrightarrow \mathbb{F}_q \\ h &\longmapsto s(e, hk), \end{aligned}$$

pero $s(e, hk) = \sum_{i=1}^{t} e_i hk(P) = \sum_{i=1}^{t} e_t h(Q_i)k(Q_i) = 0$ para toda h, por lo tanto δ es la función constante cero. Utilizando la observación 2.5.3, $E_e(k) = E_w(k) = \delta = 0$ por lo tanto, $k \in ker(E_w)$. □

Lema 2.5.2. *Si $t <$ dim(A) entonces $\mathcal{L}(A - \sum_{i=1}^{t} Q_i) \neq 0$.*

Demostración. Tenemos que $dim(A) \geq grado(A) + 1 - g > t$. Por otro lado:

$$\begin{aligned} dim(A - \sum_{i=0}^{t} Q_i) &\geq gradoA - t + 1 - g \\ &\geq (grado(A) + 1 - g) - t > 0, \end{aligned}$$

de donde se obtiene el resultado deseado. □

Observación 2.5.5. Si $A, G \in \mathcal{D}_F$ son tales que $grado(G - A) > t + 2g - 2$ entonces es inmediato que se cumple que $grado(G - A) \geq t + 2g - 1$. Además, como $t \geq 0$ entonces $grado(G - A) \geq 2g - 1$ (teorema 1.3.5). Así:

$$dim(G - A) = grado(G - A) + 1 - g.$$

Lema 2.5.3. *Si $A \in \mathcal{D}_F$ con soporte$(A) \cap$ soporte$(D) = \emptyset$ y grado$(G - A) > t + 2g - 2$ entonces ker$(E_w) = \mathcal{L}(A - \sum_{i=1}^{t} Q_i)$.*

Demostración. De la proposición 2.5.1 tenemos que $\mathcal{L}(A - \sum Q_i) \leq ker(E_w)$.

Demostraremos que $\mathcal{L}(A - \sum Q_i) \geq ker(E_w)$. Si $z \in ker(E_w)$ entonces $s(w, hz) = 0$ para toda $h \in \mathcal{L}(G - A)$ pero $s(w, hz) = s(e, hz) = 0 = \sum_{i=1}^{t} e_i hz(Q_i)$.
Definimos el mapeo $\mathbb{F}_q$ lineal:

$$\begin{aligned} \varphi : \mathcal{L}(G - A) &\longrightarrow & \mathbb{F}_q^t \\ h &\longmapsto & (h(Q_1), (h(Q_2), \ldots, (h(Q_t)). \end{aligned}$$

El núcleo de este mapeo será el espacio $\mathcal{L}(G - A - \sum_{i=1}^{t} Q_i)$. Tenemos que:

$$\begin{aligned} grado(G - A - \sum_{i=1}^{t} Q_i) &= grado(G - A) - t \\ &> t + 2g - 2 - t \\ &= 2g - 2, \end{aligned}$$

por lo que $grado(G - A - \sum_{i=1}^{t} Q_i) \geq 2g - 1$. Utilizando el Teorema de Riemann-Roch:

$$\begin{aligned} dim(G - A - \sum_{i=1}^{t} Q_i) &= grado(G - A - \sum_{i=1}^{t} Q_i) + 1 - g \\ &= grado(G - A) - t + 1 - g. \end{aligned}$$

Considerando que $dim(Im\ \varphi) = dim(G - A) - dim(ker(\varphi))$ obtenemos que:

$$dim(Im\ \varphi) = grado(G - A) + 1 - g - (grado(G - A) - t + 1 - g) = t$$

así φ es suprayectiva, por lo que existe $h_j \in \mathcal{L}(G - A)$ tal que:

$$\varphi(h_j) = (0, 0, ..., 1, .., 0) \in \mathbb{F}_q^n \tag{2.11}$$

donde la entrada con valor igual a 1 está localizada en la entrada j-ésima.

Utilizando esto, tenemos que :

$$\begin{aligned} 0 = s(w, h_j z) = s(e, h_j z) &= \sum_{i=1}^{t} e_i h_j(Q_i) z(Q_i) \\ &= e_j h_j(Q_j) z(Q_j) \\ &= e_j z(Q_j) \end{aligned}$$

como $e_j \neq 0$, $z(Q_j) = 0$, por lo tanto, Q_j es un cero de z lo que implica que $v_{Q_j}(z) > 0$ así, $z \in \mathcal{L}(A - \sum_{i=1}^{t})$ por lo que $ker(E_w) \leq \mathcal{L}(A - \sum_{i=1}^{t})$. □

Definición 2.5.4. *Sea* $\boldsymbol{P} = (P_1, P_2, P_3, \ldots, P_n)$ *y* $\boldsymbol{Q} = (Q_1, Q_2, \ldots, Q_t)$ *con* $Q_j = P_{i_j}$ *para* $i = 1, \ldots, t$. *Definimos los mapeos:*

- $\pi_Q : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^t$ *dado por* $\pi_Q(w) = (w_{i_1}, w_{i_2}, \ldots, w_{i_t})$.
- $\iota_Q : \mathbb{F}_q^t \longrightarrow \mathbb{F}_q^n$ *donde* $\iota_Q(v)_i = v_j$ *si* $i = i_j$ *para* $i = 1, \ldots, t$ *y* $\iota_Q(v)_i = 0$ *en otro caso.*

Definición 2.5.5. *Definimos el mapeo* S_Q *como sigue:*

$$\begin{aligned} S_Q : \mathbb{F}_q^t \longrightarrow & \quad \mathcal{L}(G)^V \\ v \longmapsto & \quad (g \mapsto \sum_{i=1}^{t} v_i g(Q_i)). \end{aligned}$$

Observación 2.5.6. La matriz asociada al mapeo S_Q es la matriz asociada a S restringida a los lugares Q.

Proposición 2.5.1. *Sea* $0 \neq f \in ker(E_w)$. *Supongamos que* $grado(G - A) > \varepsilon + g - 2$ *y que* $g \leq \varepsilon$. *Sea* $w = c + e$ *con* $c \in C$ *y* $e \notin C$ *tal que* $t := w(e) \leq \varepsilon$ *y* $t < dim(A)$. *Sea* $Q := (Q_1, \ldots, Q_t)$ *donde* $\{Q_1, \ldots, Q_t\} = soporte(e)$ *y está contenido en el conjunto de ceros de* f, *entonces:* $S_Q(x) = S(w)$ *tiene solución única* $\pi_Q(e)$.

Demostración. Sabemos que si la entrada i del vector e es igual a cero, el resultado de $S(e)$ no se verá afectado si removemos la columna i de la matriz S. Eliminando de

esta forma todas las columnas que no afectarán al resultado, obtendremos la matriz S_Q. Sabemos que $w = c + e$ de donde $S(w) = S(c + e) = S(c) + S(e)$, pero $S(c) = 0$, así que $S(w) = S(e)$. Así, el sistema a resolver será: $S_Q(X) = S(w) = S(e)$. Es inmediato que $x = \pi_Q(e)$ será una solución y para verificar su unicidad de la misma, supondremos que existe un vector $\sigma \in \mathbb{F}_q^t$ tal que es solución al sistema, es decir: $S_Q(\sigma) = S(w)$ con $\sigma \neq e$. Sea $\iota_Q(\sigma) := \sigma_I$. Tendremos que $S(\sigma_I) = S(e)$, por lo que:

$$S(\sigma_I) - S(e) = S(\sigma_I - e) = 0,$$

por lo que $\sigma_I - e$ es una palabra del código. Así,

$$wt(\sigma_I - e) \leq t. \tag{2.12}$$

Por otro lado, como $t \leq e$ entonces $t + (-2 + g) \leq e(-2 + g)$ de donde:

$$\begin{aligned} t + (-2 + g) &\leq e(-2 + g) \leq grado(G - A) \\ \Rightarrow \quad t + (-2 + g) &\leq grado(G) - grado(A), \end{aligned}$$

por lo que:

$$t \leq grado(G) - grado(A) - g + 2. \tag{2.13}$$

Además, como $t < dim(A)$ entonces:

$$t < grado(A) + 1 - g. \tag{2.14}$$

De las ecuaciones 2.13 y 2.14 obtenemos:

$$\begin{aligned} 2t &< grado(G) - grado(A) - g + 2 + grado(A) + 1 - g \\ \Rightarrow 2t &< grado(G) - 2g + 2 \end{aligned}$$

por lo que $t < grado(G) - 2g + 2 = d^*$, es decir, el valor t debe estar por debajo de la distancia del código. Así, la desigualdad 2.12 es una contradicción pues el peso de una palabra del código no puede ser menor a la distancia mínima con lo que queda demostrada la unicidad de la solución.

Teorema 2.5.1. *Sea $C_\Omega(D,G)$ un código de longitud n y distancia mínima d^* de diseño igual a $grado(G) - (2g-2)$ definido en un campo de funciones F/K de género g. Si $e \leq (d^* - 1 - g)/2$, entonces, para cada divisor A de grado $e+g$ con soporte disjunto al soporte de G, el Algoritmo de Skorobogatov aplicado a A decodifica al código $C_\Omega(D,G)$ hasta con e errores.*

Demostración. Sea w la palabra que queremos decodificar. Si $e \leq (d^*-1-g)/2$ entonces $2e+3g-1 \geq m$ por lo que si $A \in \mathcal{D}_F$ es de grado $e+g$ entonces $grado(G-A) = m-e-g$; así $grado(G-A) > e+2g-2$. Por otro lado, se cumple que $e < dim(A)$ por lo que el lema 2.5.3 nos asegura que $ker(E_w) = \mathcal{L}(A - \sum_{i=1}^{t} Q_i)$. Además el teorema de Riemann nos asegura que $\dim A - \sum_{i=1}^{t} Q_i \geq 1$ por lo que $\mathcal{L}(A - \sum_{i=1}^{t} Q_i) \neq \{0\}$. La proposición 2.5.1 indica que el mapeo $S_Q(x) = S(w)$ tendrá solución única $\pi_Q(e)$ en donde $w = c + e$ por lo que $e = \iota_Q(\pi_Q(e))$, con lo que $c = w - e$. □

Observación 2.5.7. Antes de presentar el «Algoritmo de Skorobogatov» hacemos las siguientes observaciones:

- Diremos que el «Algoritmo de Skorobogatov es aplicado a A» si utilizamos al divisor A en la construcción de la matriz E_w.
- Una mejora al algoritmo consiste en aumentar el valor de e, es decir, hacer que el algoritmo sea capaz de detectar y corregir un mayor número de errores. Para este objetivo hay por lo menos dos posibles caminos:
  (a) encontrar un divisor en A tal que $dim(\Omega(A))$ sea diferente de cero y muy cercana a g o,
  (b) aplicar el algoritmo en paralelo, s veces, a un conjunto de divisores $\{A_1, \ldots, A_s\}$ tal que al menos para una i, $i = 1, \ldots, s$, el algoritmo aplicado a A_i logre detectar y corregir a lo más $(d^* - 1)/2$ errores.

Algoritmo de Skorobogatov

Sea C un código $C_\Omega(D, G)$, $A \in \mathcal{D}_F$ con soporte disjunto a D y w la palabra a decodificar. El algoritmo de Skorobogatov consiste en los siguientes pasos:

Calcular la matriz E_w y $ker(E_w)$.

→ **si** $\boldsymbol{ker(E_w) = 0}$:

entonces la palabra tiene más de e errores por lo cual la *decodificación falla.*

→ **si** $\boldsymbol{ker(E_w) \neq 0}$:

- escoger un elemento $f \neq 0 \in ker(E_w)$;
- identificar los lugares P_i tales que $f(P_i) = 0$;
- formar el sistema de ecuaciones $S_Q(X) = S(w)$:
  - **si el sistema no tiene solución única:**
    (esto puede ser: tiene más de una solución ó no tiene solución) entonces w tiene más de e errores, por lo que la *decodificación falla.*
  - **si el sistema tiene solución única** $\boldsymbol{w_0}$**:**
    - si el peso de $\boldsymbol{w_0 > e}$, entonces w tiene más de e errores, por lo cual la *decodificación falla.*
    - si el peso de $\boldsymbol{w_0 \leq e}$, entonces la palabra w será decodificada como $w - i_Q(w_0)$.

2.5.1. Ejemplos de Decodificación

Ejemplo 2.5.1. *Vamos a considerar el campo de funciones* $F := \mathbb{F}_{2^3}(x,y)$ *y* $K := \mathbb{F}_{2^3}$, *donde:*

$$y^2 + y + x^3 + x + 1 = 0. \tag{2.15}$$

Trabajaremos con el código $C_{\mathcal{L}}(D, 8Q_\infty)$ *con* $D := \sum_{i=1}^{12} P_i := P$, *donde los* P_i *son lugares de grado 1 de F (ver ejemplo 2.4.1).*

Observamos que una base para el espacio $\mathcal{L}(8Q_\infty)$ *es el conjunto:*

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

De forma análoga al ejemplo 2.4.1, queremos encontrar funciones $g_i \in \mathcal{L}(8Q_\infty)$ *tales que para* $i, j = 1, \ldots, 8$ *se cumpla:*

$$g_i(P_j) = \begin{cases} 0 & si \quad i \neq j, \\ 1 & si \quad i = j \end{cases}$$

Resolviendo los sistemas de ecuaciones resultantes, encontramos que:

$$\begin{aligned}
g_1 &= \alpha^4 + \alpha^6 x + \alpha^2 x^2 + \alpha^5 x^3 + \alpha^4 x^4 + y + \alpha^2 xy + \alpha x^2 y \\
g_2 &= \alpha^2 + \alpha^4 x + x^2 + \alpha^6 x^3 + \alpha^6 x^4 + y + \alpha^4 xy + \alpha^2 x^2 y \\
g_3 &= \alpha^5 + x + \alpha^3 x^2 + \alpha^4 x^3 + \alpha^6 x^4 + y + \alpha xy + \alpha^4 x^2 y \\
g_4 &= \alpha^6 x + \alpha^6 x^2 + \alpha^6 x^4 + y + \alpha^2 xy + \alpha x^2 y \\
g_5 &= \alpha + x + \alpha^3 x^2 + \alpha x^3 + \alpha^3 x^4 + y + \alpha^4 xy + \alpha^2 x^2 y \\
g_6 &= \alpha^4 + \alpha^5 x + x^2 + \alpha^4 x^3 + x^4 + y + \alpha xy + \alpha^4 x^2 y \\
g_7 &= \alpha^5 + \alpha x + \alpha^6 x^2 + \alpha^5 x^3 + \alpha^6 x^4 \\
g_8 &= \alpha^5 + \alpha^3 x + \alpha^2 x^2 + \alpha^5 x^3 + \alpha^2 x^4
\end{aligned}$$

por lo que la matriz generadora del código $C_{\mathcal{L}}(D, 8Q_\infty)$ *será:*

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^3 & \alpha^5 & \alpha^6 & \alpha^4 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha & \alpha & 0 & \alpha^3 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \alpha^4 & \alpha^2 & \alpha^3 & \alpha^2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \alpha^5 & \alpha^5 & 1 & \alpha^4 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \alpha^5 & \alpha & \alpha^6 & \alpha^3 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \alpha^5 & \alpha^2 & \alpha & \alpha^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \alpha^2 & 1 & \alpha^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \alpha^6 & 0 & \alpha^6 & 1 \end{pmatrix}$$

La matriz de paridad de $C_{\mathcal{L}}(D, 8Q_\infty)$ *será la matriz G:*

$$G = \begin{pmatrix} \alpha^3 & \alpha & \alpha^4 & \alpha^5 & \alpha^5 & \alpha^5 & \alpha^2 & \alpha^6 & 1 & 0 & 0 & 0 \\ \alpha^5 & \alpha & \alpha^2 & \alpha^5 & \alpha & \alpha^2 & 1 & 0 & 0 & 1 & 0 & 0 \\ \alpha^6 & 0 & \alpha^3 & 1 & \alpha^6 & \alpha & \alpha^2 & \alpha^6 & 0 & 0 & 1 & 0 \\ \alpha^4 & \alpha^3 & \alpha^2 & \alpha^4 & \alpha^3 & \alpha^2 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

que resulta, de acuerdo a la poposición 2.3.1, ser la matriz generadora del código $C_\Omega(D, 8Q_\infty)$.

El algoritmo permite que el divisor A y G tengan soportes no disjuntos, por lo que lo escogeremos $A = 4Q_\infty$. *Un conjunto base para el espacio* $\mathcal{L}(A)$ *será:*

$$\{1 =: \lambda_1,\ y =: \lambda_2,\ x =: \lambda_3,\ x^2 =: \lambda_4\}.$$

Sumando los renglones de la matriz G, obtendremos la palabra del código $C_\Omega(D, 8Q_\infty)$*:*

$$v = (\alpha^5, \alpha^3, \alpha^6, \alpha^5, \alpha^3, \alpha^6, 1, 1, 1, 1, 1, 1)$$

Supondremos que v fue transmitida pero el receptor recibió:

$$w = (\alpha^5, \alpha, \alpha^6, \alpha^5, \alpha^3, \alpha^6, \alpha^4, 1, 1, 1, 1, 0),$$

es decir, hubo tres errores de transmisión. En este caso, $2g - 2 = 0$ *por lo que, haciendo referencia al lema 2.5.3,* $grado(G - A) = 4 > t$.

Para decodificar la palabra por medio del algoritmo de Skorobogatov, debemos calcular la matriz E_w. De la observación 2.5.3 sabemos que la matriz E_w será de la siguiente forma:

$$E_w = \begin{pmatrix} w \cdot \lambda_1\lambda_1(D) & w \cdot \lambda_2\lambda_1(D) & w \cdot \lambda_3\lambda_1(D) & w \cdot \lambda_4\lambda_1(D) \\ \vdots & \vdots & \vdots & \vdots \\ w \cdot \lambda_1\lambda_4(D) & w \cdot \lambda_2\lambda_4(D) & w \cdot \lambda_3\lambda_4(D) & w \cdot \lambda_4\lambda_4(D) \end{pmatrix}$$

pues en este caso $\mathcal{L}(A) = \mathcal{L}(G - A)$. Así, calculando cada entrada de la matriz E_w y escalonándola, obtenemos:

$$E_w = \begin{pmatrix} \alpha^5 & 0 & \alpha^3 & \alpha^5 \\ 0 & \alpha^4 & \alpha^3 & 1 \\ \alpha^3 & \alpha^3 & \alpha^5 & \alpha \\ \alpha^5 & 1 & \alpha & \alpha \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & \alpha^2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

de donde $ker(E_W) =< (0, 1, \alpha^2, 1) >$ por lo que si $f \in ker(E_W)$ entonces

$$f = \alpha^i(0\lambda_1 + 1\lambda_2 + \alpha^2\lambda_3 + 1\lambda_4) = \alpha^i(y + \alpha^2 x + x^2),$$

con $i \in \mathbb{Z}$. Haciendo $i = 0$, $f = y + \alpha^2 x + x^2$ y evaluando $f(P)$ obtenemos:

$$f(P) = (\alpha^5, 0, \alpha^5, \alpha^4, 1, \alpha^4, 0, 1, \alpha^2, 1, \alpha^6, 0) \tag{2.16}$$

por lo que ocurrieron a lo más tres errores y están localizados en las posiciones 2,7 y 12; es decir, en los lugares P_2, P_7 y P_{12}.

Para determinar el valor del error en cada entrada, utilizaremos la matriz asociada al mapeo S_Q dado en la definición 2.5.5. En este caso $Q = (P_2, P_7, P_{12})$:

$$\begin{aligned} S_Q : \mathbb{F}_8^3 &\longrightarrow \quad \mathcal{L}(8Q_\infty)^V \\ v &\longmapsto \quad (g \mapsto \sum_{i=1}^{3} v_i g(Q_i)), \end{aligned}$$

de manera que la matriz asociada será:

$$S_Q = \begin{pmatrix} 1 & 1 & 1 \\ \alpha^2 & \alpha^3 & \alpha^6 \\ \alpha^4 & \alpha^6 & \alpha^5 \\ \alpha^6 & \alpha^2 & \alpha^4 \\ \alpha & \alpha^5 & \alpha^3 \\ 0 & \alpha & \alpha^6 \\ 0 & \alpha^4 & \alpha^5 \\ 0 & 1 & \alpha^4 \end{pmatrix}$$

Debemos encontrar la solución de

$$S_Q(\overline{x}) = S(w), \tag{2.17}$$

donde S es el mapeo síndrome de w de la definición 2.5.2. En este caso:

$$S(w) = (\alpha^5, \alpha^3, \alpha^5, \alpha, \alpha, 0, \alpha^3, 1) \tag{2.18}$$

por lo que formamos la matriz S' y mediante operaciones elementales sobre sus renglones, obtenemos una matriz equivalente:

$$S' = \begin{pmatrix} 1 & 1 & 1 & \alpha^5 \\ \alpha^2 & \alpha^3 & \alpha^6 & \alpha^3 \\ \alpha^4 & \alpha^6 & \alpha^5 & \alpha^5 \\ \alpha^6 & \alpha^2 & \alpha^4 & \alpha \\ \alpha & \alpha^5 & \alpha^3 & \alpha \\ 0 & \alpha & \alpha^6 & 0 \\ 0 & \alpha^4 & \alpha^5 & \alpha^3 \\ 0 & 1 & \alpha^4 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & \alpha^5 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

así, obtenemos que la solución de 2.17 es

$$\overline{x_0} = (1, \alpha^5, 1) \quad con \quad wt(\overline{x_0}) \leq 3 = e$$

por lo que w será decodificada como $w - \iota_Q(\overline{x_0})$ *con*

$$\iota_Q(\overline{x_0}) = (0,1,0,0,0,0,\alpha^5,0,0,0,0,1)$$

de donde recuperaremos la palabra v:

$$\begin{array}{rcccccccccccccc} & (& \alpha^5, & \alpha, & \alpha^6, & \alpha^5, & \alpha^3, & \alpha^6, & \alpha^4, & 1, & 1, & 1, & 1, & 0 &) \\ + & (& 0, & 1, & 0, & 0, & 0, & 0, & \alpha^5, & 0, & 0, & 0, & 0, & 1 &) \\ \hline v = & (& \alpha^5, & \alpha^3, & \alpha^6, & \alpha^5, & \alpha^3, & \alpha^6, & 1, & 1, & 1, & 1, & 1, & 1 &). \end{array}$$

Observación 2.5.8. Existe la posibilidad de que $f(P)$ (ver ecuación 2.16) contenga ceros en lugares donde no existen errores. A estos casos se les denomina «ceros falsos». Si se sigue el proceso de decodificación, el valor del error en esos lugares de falsos ceros serán ceros, es decir, se notará que en esos lugares no hubo error.

2.6. Algoritmo de Skorobogatov Mejorado

Esta sección tiene como objetivo presentar una versión mejorada del Algoritmo de Decodificación de Skorobogatov que permite la detección y correción de un número mayor de errores. La idea central de esta mejora es la ejecución en paralelo del algoritmo de Skorobogatov aplicado a un conjunto de divisores con ciertas características.

Definición 2.6.1. *Sea $C_F = \mathcal{D}_F/\mathcal{P}_F$. Definimos los conjuntos:*

(i) $\mathbb{D}_k := \{D \in \mathcal{D}_F \mid grado(D) = k \text{ y } D \geq 0\}$.

(ii) $C_F^0 := \{[A] \in C_F \mid grado([A]) = 0\}$

A C_F^0 lo conocemos como el grupo de clases de divisores de grado cero.

Proposición 2.6.1. *Sea $D_0 \in \mathbb{D}_k$ y sea $\psi_k : \mathbb{D}_k \longrightarrow C_F^0$ dado por:*

$$\psi_k(D) := [D - D_0].$$

Si suponemos que $k \geq g$, entonces ψ_k es un mapeo suprayectivo.

Demostración. Sea $[M] \in C_F^0$. Debemos mostrar que existe un divisor $D \in \mathbb{D}_k$ tal que $[M] = [D - D_0]$. Como $[M] \in C_F^0$ entonces $grado(M) = 0$, por lo que $M + D_0$ tiene grado k, así, el teorema de Rieman-Roch indica que $dim\ \mathcal{L}(M + D_0) \geq 1$, por lo que existe $x \in F$ tal que $(x) + M + D_0 \geq 0$. Haciendo $D := (x) + M + D_0$, obtenemos, $D - D_0 := (x) + M$, lo que implica $D - D_0 \sim M$, por lo que $[M] = [D - D_0]$. □

Definición 2.6.2. *Sea $s \in \mathbb{Z}$ con $s \geq 2$. Definimos el mapeo ψ_k^s como:*

$$\begin{aligned} \psi_k^s : \mathbb{D}_k^s &\longrightarrow (C_F^0)^{(s-1)} \\ (D_1, D_2, ..., D_s) &\longmapsto ([D_1 - D_2], \ldots, [D_{s-1} - D_s]). \end{aligned}$$

Corolario 2.6.1. *Sean $k, l, s \in \mathbb{Z}$ tales que $s \geq 2$, $k \geq g$, $l \leq g - 1$. Si ψ_l^s es suprayectivo entonces debe existir alguna $A \in \mathbb{D}_k^s$ tal que $\psi_k^s(A)$ no está en la imagen de ψ_l^s.*

Proposición 2.6.2. *Sean $G \in \mathcal{D}_F$, $s, m \in \mathbb{Z}$ tales que $s \geq 2$, $grado(G) = m$ y $m \geq 4g-1$ en el caso de que m sea impar y $m \geq 4g-1$ en el caso de que m sea par. Sea $e = \left\lfloor \frac{d^*-1}{2} \right\rfloor$ con $d^* = m - 2g + 2$. Supongamos que ψ^s_{g-1} o ψ^s_{g-2} no es suprayectiva si m es impar o par, respectivamente. Entonces existe $\boldsymbol{A} = (A_1, \ldots, A_s)$ en $\mathbb{D}^s_{g+e}$ tal que para $\boldsymbol{Q} = (Q_1, \ldots, Q_e)$ con $Q_i \in \{P_1, \ldots, P_n\}$, existe al menos una i, $1 \leq i \leq s$ tal que el mapeo:*

$$\begin{aligned} \phi(A_i, \boldsymbol{Q}) : \mathcal{L}(G - A_i) &\longrightarrow & \mathbb{F}_q^e \\ h &\longmapsto & (h(Q_1), (h(Q_2), \ldots, (h(Q_e)). \end{aligned}$$

es suprayectivo.

Demostración. Por hipótesis, el mapeo ψ^s_{g-j} no es suprayectivo para $j = 1, 2$; por lo que existe $\boldsymbol{A} = (A_1, A_2, \ldots, A_s)$ en $\mathbb{D}^s_{g+e}(\boldsymbol{A})$ tal que no está en la imagen de ψ^s_{g-j}.
Sea $\boldsymbol{Q} := (Q_1, Q_2, \ldots, Q_e)$ tal que $Q_i \in \{P_1, ..., P_n\}$. Hay dos casos, m impar o m par.

(a) **Si m es impar**, $e = \dfrac{m-2g+1}{2}$ pues $d^* = m - 2g + 2$. Además, obtenemos que $m = 2e + 2g - 1$ por lo que:

$$\begin{aligned} grado(G - A_i) &= grado(G) - grado(A_i) \\ &= m - (e + g) \\ &= 2e + 2g - 1 - (e + g) \\ &= e + g - 1. \end{aligned}$$

Por otro lado, $m \geq 4g - 1$ de donde $m + (-2g + 1) \geq 4g - 1 + (-2g + 1)$ así,

$$m - 2g + 1 \geq 2g,$$

por lo que $e = \dfrac{m-2g+1}{2} \geq g$. Por el Teorema de Riemann- Roch y utilizando que $e + g - 1 \geq 2g - 1$, $dim(G - A_i) = (e + g - 1) + 1 - g = e$.
Sabemos que $dim(Im(\phi)) = dim(\mathcal{L}(G - A_i)) - dim(ker(\phi))$ por lo que el mapeo $\phi(A_i, Q)$ será suprayectivo si y solomente si $dim(ker(\phi)) = 0$.

(b) **Si *m* es par** se cumple que $e = \left\lfloor \frac{d^* - 1}{2} \right\rfloor = (m - 2g)/2$, entonces $m = 2e + 2g$. Calculando $grado(G - A_i)$:

$$\begin{aligned} grado(G - A_i) &= grado(G) - grado(A_i) \\ &= m - (e + g) \\ &= 2e + 2g - (e + g) \\ &= e + g. \end{aligned}$$

Como $m \geq 4g - 2$ entonces $m - 2g \geq 4g - 2 - 2g$ de donde $e = \frac{m - 2g}{2} \geq g - 1$. Así, $e + g \geq 2g - 1$ y podemos utilizar el Teorema de Riemann-Roch para calcular la dimensión de $\mathcal{L}(G - A_i)$:

$$dim(G - A_i) = grado(G - A_i) + 1 - g = e + g + 1 - g = e + 1.$$

Análogamente al caso anterior, el mapeo $\phi(A_i, Q)$ es suprayectivo en este caso si y solamente si $dim(ker(\phi)) = 1$.

Sabemos que $ker(\phi(A_i, Q)) = \mathcal{L}(G - A_i - \sum_{j=1}^{e} Q_j)$. El grado del divisor $A' = (G - A_i - \sum_{j=1}^{e} Q_j)$ será $g - 1$ y g respectivamente. Utilizando la proposición 1.3.2, tenemos que

$$i(A') = dim(\Omega_F(A')),$$

calculando el índice de especialidad del divisor A', tenemos:

$$i(A') = dim(A') - grado(A') + g - 1 = dim(\Omega_F(A')) \tag{2.19}$$

por lo que $dim(A') = 0$ si y solamente si $dim(\Omega_F(A') = 0$.

Vamos a suponer que para toda i, $1 \leq i \leq j$, el mapeo $\phi(A_i, Q)$ no es suprayectivo, esto es $\dim(\Omega_F(A')) > 0$. Sea $0 \neq \omega_i \in \Omega_F(A_i)$, por definición si (ω_i) es el divisor asociado al diferencial de Weil ω_i se tendrá que $(\omega_i) \geq A'$ (definición 1.3.5), es decir:

$$(\omega_i) \geq (G - A_i - \sum_{j=1}^{e} Q_j)$$

por lo que $E_i := (\omega_i) - (G - A_i - \sum_{j=1}^{e} Q_j)$ será un divisor efectivo. Por el corolario 1.3.2 sabemos que $grado((\omega_i)) = 2g - 2$ por lo que $grado(E_i) = 2g - 2 - (g - 1) = g - 1$ en el caso de que m sea impar y $grado(E_i) = 2g - 2 - (g) = g - 2$ en el caso de que m sea par. Todos los divisores de las formas diferenciales son equivalentes en C_F. Si denotamos por $\mathcal{K}$ a la clase canónica entonces

$$[E_i - A_j] = \mathcal{K} - [G - \sum_{j=1}^{e} Q_j]$$

no depende de la elección de i por lo que $[E_{i_1} - E_{i_2}] = [A_{i_1} - A_{i_2}]$ para toda i_1, i_2 con $1 \leq i_2$, $i_2 < s$, así que si $\boldsymbol{E} = (E_1, \ldots, E_s)$ entonces

$$\psi^s_{g-j}(\boldsymbol{E}) = \psi^s_{g+e}(\boldsymbol{A})$$

para el caso $j = 1$ cuando m es par y $j = 2$ cuando m es impar. Esto es una contradicción al corolario 2.6.1 pues siempre podríamos encontrar $\boldsymbol{A} \in \mathbb{D}^s_{g+e}$ tal que $\psi^s_{g+e}(\boldsymbol{A})$ esté en la imagen de (ψ^s_{g-j}). Por lo tanto, el mapeo $\phi(A_i, Q)$ siempre es suprayectivo. □

Observación 2.6.1. Diremos que el Algoritmo de Skorobogatov es aplicado a $\boldsymbol{A} = (A_1, \ldots, A_s)$ si es aplicado a cada una de los divisores A_i.

Teorema 2.6.1. *Sea $C := C_\Omega(D, G)$ un código geométrico de longitud n definido en un campo de funciones F/K de género g. Sean $m = grado(G)$ y $d^* = m - (2g - 2)$ la distancia de diseño del código. Si se cumple que $4g - 2 \leq m$, $e = \lfloor \frac{d^* - 1}{2} \rfloor$ y*

- *ψ^s_{g-2} no es suprayectivo en el caso en el que m es par ó*
- *ψ^s_{g-1} no es suprayectivo en el caso en el que m es impar,*

entonces existe $\boldsymbol{A} = (A_1, \ldots, A_s)$ (con $grado(A_i) = g + e$ y $soporte(A_i) \cap soporte(D) = \emptyset$ para toda $i = 1, \ldots, s$) tal que el Algoritmo de Skorobogatov aplicado a $\boldsymbol{A}$ decodifica el código C siempre y cuando el número de errores por palabra no exceda e.

Demostración. La prueba de este teorema es básicamente la demostración de la proposición anterior junto con el Algoritmo de Skorobogatov.
Escogemos $\boldsymbol{A} = (A_1, \ldots, A_s) \in \mathbb{D}^s_{g+e}$ tal que no se encuentre en la imagen de ψ^s_{g-2} o ψ^s_{g-1} en el caso de que el grado del divisor G sea par o impar respectivamente. La proposición anterior asegura que al menos un divisor A_i, $i = 1, \ldots, s$ decodifica exitosamente cada palabra del código C siempre y cuando no hayan ocurrido más de e errores. Además, utilizando la proposicion 2.5.1 si A_i, A_j decodifican con éxito la misma palabra, el resultado debe ser el mismo pues por hipótesis $e \geq g$ y $grado(G - F) > e + g - 2$. □

Observación 2.6.2. Se hacen las siguientes observaciones acerca del Teorema 2.6.1:

(a) Estos resultados sólo garantizan la existencia de un divisor capaz de decodificar por medio del Algoritmo de Skorovogatov, sin embargo, no existen métodos explícitos para construirlo. Además, el resultado tampoco incluye cotas prácticas para la cantidad de divisores que debemos probar para una decodificación exitosa.

(b) Un caso particular para acotar la cantidad de divisores que debemos usar es en el caso de que los campos sean maximales. En [11] se demuestra que si g es el género del campo, entonces los mapeos ψ^{2g}_{g-1} y ψ^{2g}_{g-2} son no suprayectivos, esto quiere decir que el algoritmo de Skorobogatov deberá ser aplicado al menos a $2g$ divisores. En la siguiente sección se presenta un ejemplo acerca de este caso.

2.6.1. Ejemplo del Algoritmo de Decodificación Mejorado

Ejemplo 2.6.1. *Trabajaremos con el campo hermitiano $H/\mathbb{F}_{2^6}$ tal que $y^8 + y = x^9$. Este campo es de género 28 y tiene exactamente 513 lugares de grado 1 (ver ejemplo 1.6.2). Sea $C := C_\Omega(D, 117Q_\infty)$, con el divisor $D := \sum_{i=1}^{129} P_i$ y P_i en el conjunto D' para $i = 1, \ldots 129$. (cuadro 2.3). Todos estos lugares son de grado 1 por lo que $grado(D) = 129$.*
La distacia de diseño de este código está dada por:

$$\begin{aligned} d^* &= grado(G) - (2g - 2) \\ &= 117 - (54) = 63 \end{aligned}$$

por lo que el Algoritmo de Skorobogatov podrá localizar y corregir hasta $(d^* - 1 - g)/2 = 17$ errores, sin embargo, de acuerdo al Teorema 2.6.1 existe un conjunto $A = \{A_1, A_2, \ldots, A_s\}$ de s divisores tales que $grado(A_i) = e + g$ para $i = 1, \ldots s$ y en el cual podemos encontrar al menos un divisor A_i para el cual el algoritmo de decodificación permite detectar y corregir hasta $e = (d^* - 1)/2 = 31$ errores.

Por otro lado, sabemos que H es un campo maximal, por lo que s está acotada por $2g$, es decir, no necesitaremos más de 56 divisores con grado 59 para decodificar con éxito siempre y cuando hayan ocurrido a lo más 31 errores en cada palabra. Los divisores A_i deben ser efectivos y tener soporte disjunto a D. El divisor más fácil de proponer es entonces $59Q_\infty$, sin embargo, necesitaremos 55 más. Una manera de escogerlos es la siguiente: sea $D^c := \{B \in \mathbb{P}^1_H \mid B \notin D'\}$. En este caso $D^c \neq \emptyset$, de hecho, $|D^c| = 384$ (Ver cuadro 2.4). Proponemos usar los divisores de la forma:

$$A_i = 58Q_\infty + B \quad con \quad B \in D^c.$$

Claramente el grado de cada divisor de esta forma, tiene grado 59. Una manera de calcular la base para cada uno de los espacios $\mathcal{L}(58Q_\infty + B)$ se puede encontrar en [9].

$$
\begin{aligned}
w = \; & (\alpha^{56}, 0, \alpha^{47}, \alpha^{49}, \alpha^{26}, \alpha^{44}, \alpha^{61}, \alpha^{30}, \alpha^{34}, \alpha^{12}, \alpha^{45}, \alpha^{58}, 1, \alpha^{29}, \alpha^{57}, \alpha^{6}, \alpha, \alpha, \alpha^{27}, \\
& \alpha^{13}, \alpha^{61}, \alpha^{27}, \alpha^{48}, \alpha^{2}, \alpha^{27}, \alpha^{50}, \alpha^{31}, \alpha^{8}, \alpha^{54}, \alpha^{21}, \alpha^{38}, \alpha^{27}, \alpha^{60}, \alpha^{33}, \alpha^{60}, \alpha^{24}, 0, \\
& \alpha^{2}, \alpha^{6}, \alpha^{55}, \alpha^{43}, \alpha^{18}, \alpha^{14}, \alpha^{44}, \alpha^{61}, \alpha^{9}, \alpha^{58}, \alpha^{52}, \alpha^{23}, \alpha^{17}, \alpha^{9}, \alpha^{60}, \alpha^{21}, \alpha^{55}, \alpha^{47}, \\
& \alpha^{22}, \alpha^{46}, 1, \alpha^{41}, \alpha^{46}, \alpha^{3}, \alpha^{5}, 0, \alpha^{43}, \alpha^{13}, \alpha^{2}, \alpha^{42}, \alpha^{33}, \alpha^{58}, \alpha^{46}, \alpha^{31}, \alpha^{28}, \alpha^{10}, \alpha^{17}, \alpha^{53}, \\
& \alpha^{29}, \alpha, \alpha, \alpha^{42}, \alpha^{58}, \alpha^{38}, \alpha^{46}, \alpha^{10}, \alpha^{24}, \alpha^{50}, \alpha^{14}, \alpha^{46}, \alpha^{3}, \alpha^{8}, \alpha^{14}, 0, \alpha, \alpha, \alpha, 1, 1, 1, 1, 1, 1, 0, \\
& 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)
\end{aligned}
$$

Cuadro 2.1: *Palabra w.*

Por último, si decodificamos la palabra w (ver cuadro 2.2), utilizando los divisores descritos en el párrafo de arriba, es decir, variando B sobre todo el conjunto D^c, el algoritmo no es exitoso para el siguiente conjunto de lugares:

Lugar	*Paso fallido*
$[\alpha^{59}, \alpha^{11}]$	*Sistema S_q sin solución*
$[\alpha^{31}, \alpha^{25}]$	*Sistema S_q sin solución*
$[\alpha^{55}, \alpha^{38}]$	*Sistema S_q sin solución*
$[\alpha^{28}, \alpha^{59}]$	*Sistema S_q sin solución*
$[\alpha^{8}, \alpha^{30}]$	*$f(P)$ no localiza errores*

para todos los demás, se logra detectar y corregir 31 errores en las posiciones: 1, 3, 4, 6, 9, 10, 11, 15, 16, 17, 19, 20, 28, 30, 31, 32, 39, 40, 42, 62, 65, 78, 89, 91, 92, 93, 100, 120, 121, 122 y 125, obteniendo la palabra c mostrada en el cuadro 2.2.

$$
\begin{aligned}
c = \; & (\alpha^{56}, \alpha^{13}, \alpha^{47}, 0, \alpha^{43}, \alpha^{44}, \alpha^{23}, \alpha^{30}, \alpha^{34}, \alpha^{52}, \alpha^{36}, \alpha^{25}, 1, \alpha^{29}, \alpha^{57}, \alpha^{26}, \alpha^{56}, 0, \alpha^{27}, \alpha^{53}, \\
& \alpha^{11}, \alpha^{27}, \alpha^{48}, \alpha^{2}, \alpha^{27}, \alpha^{50}, \alpha^{31}, \alpha^{8}, \alpha^{51}, \alpha^{21}, \alpha^{44}, \alpha^{60}, \alpha^{27}, \alpha^{33}, \alpha^{60}, \alpha^{24}, 0, \alpha^{2}, \alpha^{6}, \\
& \alpha^{12}, \alpha^{46}, \alpha^{18}, \alpha^{35}, \alpha^{44}, \alpha^{61}, \alpha^{9}, \alpha^{58}, \alpha^{52}, \alpha^{23}, \alpha^{17}, \alpha^{9}, \alpha^{60}, \alpha^{21}, \alpha^{55}, \alpha^{47}, \alpha^{22}, \alpha^{46}, 1, \\
& \alpha^{41}, \alpha^{46}, \alpha^{3}, \alpha^{5}, \alpha^{56}, \alpha^{43}, \alpha^{13}, \alpha^{25}, \alpha^{42}, \alpha^{33}, \alpha^{58}, \alpha^{46}, \alpha^{31}, \alpha^{28}, \alpha^{10}, \alpha^{17}, \alpha^{53}, \alpha^{29}, \\
& \alpha, \alpha, \alpha^{21}, \alpha^{58}, \alpha^{38}, \alpha^{46}, \alpha^{10}, \alpha^{24}, \alpha^{50}, \alpha^{14}, \alpha^{46}, \alpha^{3}, \alpha^{8}, \alpha^{35}, 0, 1, 1, 1, 1, 1, 1, 1, \\
& 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)
\end{aligned}
$$

Cuadro 2.2: *Palabra c.*

$D' = \{ [0,0], [0,1], [0,\alpha^{54}], [0,\alpha^{18}], [0,\alpha^{36}], [0,\alpha^{45}], [0,\alpha^{27}], [0,\alpha^{9}],$
$[1,\alpha^{21}], [1,\alpha^{42}], [1,\alpha^{59}], [1,\alpha^{31}], [1,\alpha^{55}], [1,\alpha^{62}], [1,\alpha^{47}], [1,\alpha^{61}],$
$[\alpha,\alpha], [\alpha,\alpha^{56}], [\alpha,\alpha^{51}], [\alpha,\alpha^{40}], [\alpha,\alpha^{5}], [\alpha,\alpha^{30}], [\alpha,\alpha^{7}], [\alpha,\alpha^{8}],$
$[\alpha^{56},\alpha^{21}], [\alpha^{56},\alpha^{42}], [\alpha^{56},\alpha^{59}], [\alpha^{56},\alpha^{31}], [\alpha^{56},\alpha^{55}], [\alpha^{56},\alpha^{62}], [\alpha^{56},\alpha^{47}], [\alpha^{56},\alpha^{61}],$
$[\alpha^{2},\alpha^{2}], [\alpha^{2},\alpha^{49}], [\alpha^{2},\alpha^{14}], [\alpha^{2},\alpha^{16}], [\alpha^{2},\alpha^{17}], [\alpha^{2},\alpha^{39}], [\alpha^{2},\alpha^{60}], [\alpha^{2},\alpha^{10}],$
$[\alpha^{49},\alpha^{21}], [\alpha^{49},\alpha^{42}], [\alpha^{49},\alpha^{59}], [\alpha^{49},\alpha^{31}], [\alpha^{49},\alpha^{55}], [\alpha^{49},\alpha^{62}], [\alpha^{49},\alpha^{47}], [\alpha^{49},\alpha^{61}],$
$[\alpha^{57},\alpha], [\alpha^{57},\alpha^{56}], [\alpha^{57},\alpha^{51}], [\alpha^{57},\alpha^{40}], [\alpha^{57},\alpha^{5}], [\alpha^{57},\alpha^{30}], [\alpha^{57},\alpha^{7}], [\alpha^{57},\alpha^{8}],$
$[\alpha^{20},\alpha^{50}], [\alpha^{20},\alpha^{53}], [\alpha^{20},\alpha^{22}], [\alpha^{20},\alpha^{46}], [\alpha^{20},\alpha^{52}], [\alpha^{20},\alpha^{12}], [\alpha^{20},\alpha^{38}], [\alpha^{3},\alpha^{58}],$
$[\alpha^{3},\alpha^{25}], [\alpha^{3},\alpha^{26}], [\alpha^{3},\alpha^{6}], [\alpha^{3},\alpha^{19}], [\alpha^{3},\alpha^{48}], [\alpha^{13},\alpha^{50}], [\alpha^{13},\alpha^{22}], [\alpha^{13},\alpha^{46}],$
$[\alpha^{13},\alpha^{52}], [\alpha^{13},\alpha^{12}], [\alpha^{13},\alpha^{38}], [\alpha^{50},\alpha^{51}], [\alpha^{50},\alpha^{5}], [\alpha^{50},\alpha^{30}], [\alpha^{50},\alpha^{7}], [\alpha^{50},\alpha^{8}],$
$[\alpha^{53},\alpha^{57}], [\alpha^{53},\alpha^{35}], [\alpha^{53},\alpha^{34}], [\alpha^{53},\alpha^{28}], [\alpha^{58},\alpha^{2}], [\alpha^{58},\alpha^{49}], [\alpha^{58},\alpha^{16}], [\alpha^{25},\alpha^{20}],$
$[\alpha^{25},\alpha^{4}], [\alpha^{21},\alpha^{21}], [\alpha^{21},\alpha^{42}], [\alpha^{21},\alpha^{59}], [\alpha^{21},\alpha^{31}], [\alpha^{21},\alpha^{55}], [\alpha^{21},\alpha^{62}], [\alpha^{21},\alpha^{47}],$
$[\alpha^{21},\alpha^{61}], [\alpha^{42},\alpha^{21}], [\alpha^{42},\alpha^{42}], [\alpha^{42},\alpha^{59}], [\alpha^{42},\alpha^{31}], [\alpha^{42},\alpha^{55}], [\alpha^{42},\alpha^{62}], [\alpha^{42},\alpha^{47}],$
$[\alpha^{42},\alpha^{61}], [\alpha^{4},\alpha^{57}], [\alpha^{20},\alpha^{33}], [\alpha^{3},\alpha^{11}], [\alpha^{13},\alpha^{53}], [\alpha^{50},\alpha^{56}], [\alpha^{50},\alpha^{40}], [\alpha^{53},\alpha^{4}],$
$[\alpha^{53},\alpha^{15}], [\alpha^{53},\alpha^{32}], [\alpha^{3},\alpha^{23}], [\alpha^{50},\alpha], [\alpha^{53},\alpha^{20}], [\alpha^{58},\alpha^{14}], [\alpha^{13},\alpha^{33}], [\alpha^{58},\alpha^{39}],$
$[\alpha^{58},\alpha^{10}], [\alpha^{58},\alpha^{17}], [\alpha^{25},\alpha^{57}], [\alpha^{58},\alpha^{60}], [\alpha^{25},\alpha^{35}], [\alpha^{25},\alpha^{15}], [\alpha^{25},\alpha^{34}], [\alpha^{25},\alpha^{32}],$
$[\alpha^{25},\alpha^{28}]\}$

Cuadro 2.3: *Conjunto D'.*

$D^c := \{$

$[\alpha^{4},\alpha^{20}]$	$[\alpha^{4},\alpha^{4}]$	$[\alpha^{4},\alpha^{35}]$	$[\alpha^{4},\alpha^{15}]$	$[\alpha^{4},\alpha^{34}]$
$[\alpha^{4},\alpha^{32}]$	$[\alpha^{4},\alpha^{28}]$	$[\alpha^{35},\alpha^{21}]$	$[\alpha^{35},\alpha^{42}]$	$[\alpha^{35},\alpha^{59}]$
$[\alpha^{35},\alpha^{31}]$	$[\alpha^{35},\alpha^{55}]$	$[\alpha^{35},\alpha^{62}]$	$[\alpha^{35},\alpha^{47}]$	$[\alpha^{35},\alpha^{61}]$
$[\alpha^{14},\alpha^{21}]$	$[\alpha^{14},\alpha^{42}]$	$[\alpha^{14},\alpha^{59}]$	$[\alpha^{14},\alpha^{31}]$	$[\alpha^{14},\alpha^{55}]$
$[\alpha^{14},\alpha^{62}]$	$[\alpha^{14},\alpha^{47}]$	$[\alpha^{14},\alpha^{61}]$	$[\alpha^{16},\alpha^{2}]$	$[\alpha^{16},\alpha^{49}]$
$[\alpha^{16},\alpha^{14}]$	$[\alpha^{16},\alpha^{16}]$	$[\alpha^{16},\alpha^{17}]$	$[\alpha^{16},\alpha^{39}]$	$[\alpha^{16},\alpha^{60}]$
$[\alpha^{16},\alpha^{10}]$	$[\alpha^{51},\alpha^{2}]$	$[\alpha^{51},\alpha^{49}]$	$[\alpha^{51},\alpha^{14}]$	$[\alpha^{51},\alpha^{16}]$
$[\alpha^{51},\alpha^{17}]$	$[\alpha^{51},\alpha^{39}]$	$[\alpha^{51},\alpha^{60}]$	$[\alpha^{51},\alpha^{10}]$	$[\alpha^{40},\alpha^{3}]$
$[\alpha^{40},\alpha^{13}]$	$[\alpha^{40},\alpha^{43}]$	$[\alpha^{40},\alpha^{37}]$	$[\alpha^{40},\alpha^{41}]$	$[\alpha^{40},\alpha^{24}]$
$[\alpha^{40},\alpha^{44}]$	$[\alpha^{40},\alpha^{29}]$	$[\alpha^{54},\alpha^{3}]$	$[\alpha^{54},\alpha^{13}]$	$[\alpha^{54},\alpha^{43}]$
$[\alpha^{54},\alpha^{37}]$	$[\alpha^{54},\alpha^{41}]$	$[\alpha^{54},\alpha^{24}]$	$[\alpha^{54},\alpha^{44}]$	$[\alpha^{54},\alpha^{29}]$
$[\alpha^{18},\alpha^{57}]$	$[\alpha^{18},\alpha^{20}]$	$[\alpha^{18},\alpha^{4}]$	$[\alpha^{18},\alpha^{35}]$	$[\alpha^{18},\alpha^{15}]$
$[\alpha^{18},\alpha^{34}]$	$[\alpha^{18},\alpha^{32}]$	$[\alpha^{18},\alpha^{28}]$	$[\alpha^{59},\alpha^{58}]$	$[\alpha^{59},\alpha^{25}]$
$[\alpha^{59},\alpha^{26}]$	$[\alpha^{59},\alpha^{6}]$	$[\alpha^{59},\alpha^{19}]$	$[\alpha^{59},\alpha^{48}]$	$[\alpha^{59},\alpha^{23}]$

Cuadro 2.4: *Conjunto D^c.*

...continúa D^c.

$[\alpha^{59}, \alpha^{11}]$	$[\alpha^{31}, \alpha^{58}]$	$[\alpha^{31}, \alpha^{25}]$	$[\alpha^{31}, \alpha^{26}]$	$[\alpha^{31}, \alpha^{6}]$	$[\alpha^{31}, \alpha^{19}]$
$[\alpha^{31}, \alpha^{48}]$	$[\alpha^{31}, \alpha^{23}]$	$[\alpha^{31}, \alpha^{11}]$	$[\alpha^{26}, \alpha^{3}]$	$[\alpha^{26}, \alpha^{13}]$	$[\alpha^{26}, \alpha^{43}]$
$[\alpha^{26}, \alpha^{37}]$	$[\alpha^{26}, \alpha^{41}]$	$[\alpha^{26}, \alpha^{24}]$	$[\alpha^{26}, \alpha^{44}]$	$[\alpha^{26}, \alpha^{29}]$	$[\alpha^{6}, \alpha^{50}]$
$[\alpha^{6}, \alpha^{53}]$	$[\alpha^{6}, \alpha^{22}]$	$[\alpha^{6}, \alpha^{46}]$	$[\alpha^{6}, \alpha^{52}]$	$[\alpha^{6}, \alpha^{12}]$	$[\alpha^{6}, \alpha^{38}]$
$[\alpha^{6}, \alpha^{33}]$	$[\alpha^{22}, \alpha]$	$[\alpha^{22}, \alpha^{56}]$	$[\alpha^{22}, \alpha^{51}]$	$[\alpha^{22}, \alpha^{40}]$	$[\alpha^{22}, \alpha^{5}]$
$[\alpha^{22}, \alpha^{30}]$	$[\alpha^{22}, \alpha^{7}]$	$[\alpha^{22}, \alpha^{8}]$	$[\alpha^{46}, \alpha^{57}]$	$[\alpha^{46}, \alpha^{20}]$	$[\alpha^{46}, \alpha^{4}]$
$[\alpha^{46}, \alpha^{35}]$	$[\alpha^{46}, \alpha^{15}]$	$[\alpha^{46}, \alpha^{34}]$	$[\alpha^{46}, \alpha^{32}]$	$[\alpha^{46}, \alpha^{28}]$	$[\alpha^{43}, \alpha]$
$[\alpha^{43}, \alpha^{56}]$	$[\alpha^{43}, \alpha^{51}]$	$[\alpha^{43}, \alpha^{40}]$	$[\alpha^{43}, \alpha^{5}]$	$[\alpha^{43}, \alpha^{30}]$	$[\alpha^{43}, \alpha^{7}]$
$[\alpha^{43}, \alpha^{8}]$	$[\alpha^{37}, \alpha^{2}]$	$[\alpha^{37}, \alpha^{49}]$	$[\alpha^{37}, \alpha^{14}]$	$[\alpha^{37}, \alpha^{16}]$	$[\alpha^{37}, \alpha^{17}]$
$[\alpha^{37}, \alpha^{39}]$	$[\alpha^{37}, \alpha^{60}]$	$[\alpha^{37}, \alpha^{10}]$	$[\alpha^{5}, \alpha^{3}]$	$[\alpha^{5}, \alpha^{13}]$	$[\alpha^{5}, \alpha^{43}]$
$[\alpha^{5}, \alpha^{37}]$	$[\alpha^{5}, \alpha^{41}]$	$[\alpha^{5}, \alpha^{24}]$	$[\alpha^{5}, \alpha^{44}]$	$[\alpha^{5}, \alpha^{29}]$,	$[\alpha^{30}, \alpha^{2}]$
$[\alpha^{30}, \alpha^{49}]$	$[\alpha^{30}, \alpha^{14}]$	$[\alpha^{30}, \alpha^{16}]$	$[\alpha^{30}, \alpha^{17}]$	$[\alpha^{30}, \alpha^{39}]$	$[\alpha^{30}, \alpha^{60}]$
$[\alpha^{30}, \alpha^{10}]$	$[\alpha^{36}, \alpha]$	$[\alpha^{36}, \alpha^{56}]$	$[\alpha^{36}, \alpha^{51}]$	$[\alpha^{36}, \alpha^{40}]$	$[\alpha^{36}, \alpha^{5}]$
$[\alpha^{36}, \alpha^{30}]$	$[\alpha^{36}, \alpha^{7}]$	$[\alpha^{36}, \alpha^{8}]$	$[\alpha^{45}, \alpha^{58}]$	$[\alpha^{45}, \alpha^{25}]$	$[\alpha^{45}, \alpha^{26}]$
$[\alpha^{45}, \alpha^{6}]$	$[\alpha^{45}, \alpha^{19}]$	$[\alpha^{45}, \alpha^{48}]$	$[\alpha^{45}, \alpha^{23}]$	$[\alpha^{45}, \alpha^{11}]$	$[\alpha^{15}, \alpha]$
$[\alpha^{15}, \alpha^{56}]$	$[\alpha^{15}, \alpha^{51}]$	$[\alpha^{15}, \alpha^{40}]$	$[\alpha^{15}, \alpha^{5}]$	$[\alpha^{15}, \alpha^{30}]$	$[\alpha^{15}, \alpha^{7}]$
$[\alpha^{15}, \alpha^{8}]$	$[\alpha^{34}, \alpha^{50}]$	$[\alpha^{34}, \alpha^{53}]$	$[\alpha^{34}, \alpha^{22}]$	$[\alpha^{34}, \alpha^{46}]$	$[\alpha^{34}, \alpha^{52}]$
$[\alpha^{34}, \alpha^{12}]$	$[\alpha^{34}, \alpha^{38}]$	$[\alpha^{34}, \alpha^{33}]$	$[\alpha^{17}, \alpha^{58}]$	$[\alpha^{17}, \alpha^{25}]$	$[\alpha^{17}, \alpha^{26}]$
$[\alpha^{17}, \alpha^{6}]$	$[\alpha^{17}, \alpha^{19}]$	$[\alpha^{17}, \alpha^{48}]$	$[\alpha^{17}, \alpha^{23}]$	$[\alpha^{17}, \alpha^{11}]$	$[\alpha^{39}, \alpha^{57}]$
$[\alpha^{39}, \alpha^{20}]$	$[\alpha^{39}, \alpha^{4}]$	$[\alpha^{39}, \alpha^{35}]$	$[\alpha^{39}, \alpha^{15}]$	$[\alpha^{39}, \alpha^{34}]$	$[\alpha^{39}, \alpha^{32}]$
$[\alpha^{39}, \alpha^{28}]$	$[\alpha^{52}, \alpha^{58}]$	$[\alpha^{52}, \alpha^{25}]$	$[\alpha^{52}, \alpha^{26}]$	$[\alpha^{52}, \alpha^{6}]$	$[\alpha^{52}, \alpha^{19}]$
$[\alpha^{52}, \alpha^{48}]$	$[\alpha^{52}, \alpha^{23}]$	$[\alpha^{52}, \alpha^{11}]$	$[\alpha^{12}, \alpha^{3}]$	$[\alpha^{12}, \alpha^{13}]$	$[\alpha^{12}, \alpha^{43}]$
$[\alpha^{12}, \alpha^{37}]$	$[\alpha^{12}, \alpha^{41}]$	$[\alpha^{12}, \alpha^{24}]$	$[\alpha^{12}, \alpha^{44}]$	$[\alpha^{12}, \alpha^{29}]$	$[\alpha^{41}, \alpha^{50}]$
$[\alpha^{41}, \alpha^{53}]$	$[\alpha^{41}, \alpha^{22}]$	$[\alpha^{41}, \alpha^{46}]$	$[\alpha^{41}, \alpha^{52}]$	$[\alpha^{41}, \alpha^{12}]$	$[\alpha^{41}, \alpha^{38}]$
$[\alpha^{41}, \alpha^{33}]$	$[\alpha^{24}, \alpha^{58}]$	$[\alpha^{24}, \alpha^{25}]$	$[\alpha^{24}, \alpha^{26}]$	$[\alpha^{24}, \alpha^{6}]$	$[\alpha^{24}, \alpha^{19}]$
$[\alpha^{24}, \alpha^{48}]$	$[\alpha^{24}, \alpha^{23}]$	$[\alpha^{24}, \alpha^{11}]$	$[\alpha^{55}, \alpha^{50}]$	$[\alpha^{55}, \alpha^{53}]$	$[\alpha^{55}, \alpha^{22}]$
$[\alpha^{55}, \alpha^{46}]$	$[\alpha^{55}, \alpha^{52}]$	$[\alpha^{55}, \alpha^{12}]$	$[\alpha^{55}, \alpha^{38}]$	$[\alpha^{55}, \alpha^{33}]$	$[\alpha^{62}, \alpha^{50}]$
$[\alpha^{62}, \alpha^{53}]$	$[\alpha^{62}, \alpha^{22}]$	$[\alpha^{62}, \alpha^{46}]$	$[\alpha^{62}, \alpha^{52}]$	$[\alpha^{62}, \alpha^{12}]$	$[\alpha^{62}, \alpha^{38}]$
$[\alpha^{62}, \alpha^{33}]$	$[\alpha^{19}, \alpha^{3}]$	$[\alpha^{19}, \alpha^{13}]$	$[\alpha^{19}, \alpha^{43}]$	$[\alpha^{19}, \alpha^{37}]$	$[\alpha^{19}, \alpha^{41}]$
$[\alpha^{19}, \alpha^{24}]$	$[\alpha^{19}, \alpha^{44}]$	$[\alpha^{19}, \alpha^{29}]$	$[\alpha^{48}, \alpha^{50}]$	$[\alpha^{48}, \alpha^{53}]$	$[\alpha^{48}, \alpha^{22}]$
$[\alpha^{48}, \alpha^{46}]$	$[\alpha^{48}, \alpha^{52}]$	$[\alpha^{48}, \alpha^{12}]$	$[\alpha^{48}, \alpha^{38}]$	$[\alpha^{48}, \alpha^{33}]$	$[\alpha^{60}, \alpha^{57}]$
$[\alpha^{60}, \alpha^{20}]$	$[\alpha^{60}, \alpha^{4}]$	$[\alpha^{60}, \alpha^{35}]$	$[\alpha^{60}, \alpha^{15}]$	$[\alpha^{60}, \alpha^{34}]$	$[\alpha^{60}, \alpha^{32}]$
$[\alpha^{60}, \alpha^{28}]$	$[\alpha^{10}, \alpha^{58}]$	$[\alpha^{10}, \alpha^{25}]$	$[\alpha^{10}, \alpha^{26}]$	$[\alpha^{10}, \alpha^{6}]$	$[\alpha^{10}, \alpha^{19}]$
$[\alpha^{10}, \alpha^{48}]$	$[\alpha^{10}, \alpha^{23}]$	$[\alpha^{10}, \alpha^{11}]$	$[\alpha^{32}, \alpha^{57}]$	$[\alpha^{32}, \alpha^{20}]$	$[\alpha^{32}, \alpha^{4}]$
$[\alpha^{32}, \alpha^{35}]$	$[\alpha^{32}, \alpha^{15}]$	$[\alpha^{32}, \alpha^{34}]$	$[\alpha^{32}, \alpha^{32}]$	$[\alpha^{32}, \alpha^{28}]$	$[\alpha^{28}, \alpha^{21}]$
$[\alpha^{28}, \alpha^{42}]$	$[\alpha^{28}, \alpha^{59}]$	$[\alpha^{28}, \alpha^{31}]$	$[\alpha^{28}, \alpha^{55}]$	$[\alpha^{28}, \alpha^{62}]$	$[\alpha^{28}, \alpha^{47}]$
$[\alpha^{28}, \alpha^{61}]$	$[\alpha^{27}, \alpha^{50}]$	$[\alpha^{27}, \alpha^{53}]$	$[\alpha^{27}, \alpha^{22}]$	$[\alpha^{27}, \alpha^{46}]$	$[\alpha^{27}, \alpha^{52}]$

...Continua D^c

$[\alpha^{27}, \alpha^{12}]$	$[\alpha^{27}, \alpha^{38}]$	$[\alpha^{27}, \alpha^{33}]$	$[\alpha^{9}, \alpha^{2}]$	$[\alpha^{9}, \alpha^{49}]$	$[\alpha^{9}, \alpha^{14}]$
$[\alpha^{9}, \alpha^{16}]$	$[\alpha^{9}, \alpha^{17}]$	$[\alpha^{9}, \alpha^{39}]$	$[\alpha^{9}, \alpha^{60}]$	$[\alpha^{9}, \alpha^{10}]$	$[\alpha^{7}, \alpha^{21}]$
$[\alpha^{7}, \alpha^{42}]$	$[\alpha^{7}, \alpha^{59}]$	$[\alpha^{7}, \alpha^{31}]$	$[\alpha^{7}, \alpha^{55}]$	$[\alpha^{7}, \alpha^{62}]$	$[\alpha^{7}, \alpha^{47}]$
$[\alpha^{7}, \alpha^{61}]$	$[\alpha^{8}, \alpha]$	$[\alpha^{8}, \alpha^{56}]$	$[\alpha^{8}, \alpha^{51}]$	$[\alpha^{8}, \alpha^{40}]$	$[\alpha^{8}, \alpha^{5}]$
$[\alpha^{8}, \alpha^{30}]$	$[\alpha^{8}, \alpha^{7}]$	$[\alpha^{8}, \alpha^{8}]$	$[\alpha^{23}, \alpha^{2}]$	$[\alpha^{23}, \alpha^{49}]$	$[\alpha^{23}, \alpha^{14}]$
$[\alpha^{23}, \alpha^{16}]$	$[\alpha^{23}, \alpha^{17}]$	$[\alpha^{23}, \alpha^{39}]$	$[\alpha^{23}, \alpha^{60}]$	$[\alpha^{23}, \alpha^{10}]$	$[\alpha^{11}, \alpha^{57}]$
$[\alpha^{11}, \alpha^{20}]$	$[\alpha^{11}, \alpha^{4}]$	$[\alpha^{11}, \alpha^{35}]$	$[\alpha^{11}, \alpha^{15}]$	$[\alpha^{11}, \alpha^{34}]$	$[\alpha^{11}, \alpha^{32}]$
$[\alpha^{11}, \alpha^{28}]$	$[\alpha^{47}, \alpha^{3}]$	$[\alpha^{47}, \alpha^{13}]$	$[\alpha^{47}, \alpha^{43}]$	$[\alpha^{47}, \alpha^{37}]$	$[\alpha^{47}, \alpha^{41}]$
$[\alpha^{47}, \alpha^{24}]$	$[\alpha^{47}, \alpha^{44}]$	$[\alpha^{47}, \alpha^{29}]$	$[\alpha^{61}, \alpha^{3}]$	$[\alpha^{61}, \alpha^{13}]$	$[\alpha^{61}, \alpha^{43}]$
$[\alpha^{61}, \alpha^{37}]$	$[\alpha^{61}, \alpha^{41}]$	$[\alpha^{61}, \alpha^{24}]$	$[\alpha^{61}, \alpha^{44}]$	$[\alpha^{61}, \alpha^{29}]$	$[\alpha^{44}, \alpha^{2}]$
$[\alpha^{44}, \alpha^{49}]$	$[\alpha^{44}, \alpha^{14}]$	$[\alpha^{44}, \alpha^{16}]$	$[\alpha^{44}, \alpha^{17}]$	$[\alpha^{44}, \alpha^{39}]$	$[\alpha^{44}, \alpha^{60}]$
$[\alpha^{44}, \alpha^{10}]$	$[\alpha^{29}, \alpha]$	$[\alpha^{29}, \alpha^{56}]$	$[\alpha^{29}, \alpha^{51}]$	$[\alpha^{29}, \alpha^{40}]$	$[\alpha^{29}, \alpha^{5}]$
$[\alpha^{29}, \alpha^{30}]$	$[\alpha^{29}, \alpha^{7}]$	$[\alpha^{29}, \alpha^{8}]$	$[\alpha^{38}, \alpha^{58}]$	$[\alpha^{38}, \alpha^{25}]$	$[\alpha^{38}, \alpha^{26}]$
$[\alpha^{38}, \alpha^{6}]$	$[\alpha^{38}, \alpha^{19}]$	$[\alpha^{38}, \alpha^{48}]$	$[\alpha^{38}, \alpha^{23}]$	$[\alpha^{38}, \alpha^{11}]$	$[\alpha^{33}, \alpha^{3}]$
$[\alpha^{33}, \alpha^{13}]$	$[\alpha^{33}, \alpha^{43}]$	$[\alpha^{33}, \alpha^{37}]$	$[\alpha^{33}, \alpha^{41}]$	$[\alpha^{33}, \alpha^{24}]$	$[\alpha^{33}, \alpha^{44}]\}$

Conclusiones

Uno de los principales problemas de la teoría de códigos es el de encontrar, siguiendo el teorema de Shannon [15], [7], códigos de longitud cada vez de mayor. Comparado con otros códigos, por ejemplo, con los códigos de Reed Solomon [7], los códigos de Goppa presentan la ventaja de que su longitud no depende exclusivamente del tamaño del alfabeto (campo base) sino de los lugares de grado uno que el campo algebraico que utilizamos para construir el código pueda tener.

El algoritmo de Skorobogatov resulta ser un buen método para decodificar códigos geométricos pues su implementación es, como lo hemos visto en este trabajo, posible si se obtienen las bases de los espacios adecuados. Una vez resuelto el problema de encontar dichas bases, la implementación del algoritmo dependerá de la ejecución de la aritmética del campo base. Además, el algoritmo tiene una versión mejorada, la cual es aún más poderosa que la versión normal considerando que nos permite mejorar la capacidad de corrección del código siempre y cuando éste sea construido a partir de un campo maximal.

Un ejemplo de los códigos para los cuales el algoritmo de Skorobogatov es un método viable de decodificación, son los códigos hermitianos sobre $\mathbb{F}_q$ donde $q = 2^s$. Esta familia de códigos sirve particularmente por dos razones, se conoce una manera práctica para la construcción de bases de los espacios necesarios para la aplicación del algoritmo y son campos maximales, es decir, podemos utilizar la versión mejorada del algoritmo de decodificación.

Preguntas abiertas

- El algoritmo mejorado usa como hipótesis la no suprayectividad de las funciones ψ^s_{g-1} y ψ^s_{g-2}, sin embargo no se conocen condiciones para las cuales se cumpla dicha condición en campos de funciones en general.

- Para los casos en los que sí se saben algunas condiciones para las cuales las funciones ψ^s_{g-1} y ψ^2_{g-2} no son suprayectivas (el caso hermitiano, por ejemplo) no se conocen explícitamente elementos en $(C_F^0)^{s-1}$ que no pertenezcan a la imagen de dichas funciones.

- Para el caso de curvas maximales, ¿Es posible acotar el número de divisores para los cuales el algoritmo de Skorobogatov falle?

Bibliografía

[1] Henri Cohen and Gerhard Frey, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. CRC Press, 2005.

[2] R. Dodunekova, S.M. Dodunekov, and T. Klove. Almost-mds and near-mds codes for error detection. *Information Theory, IEEE Transactions on*, 43(1):285 –290, jan 1997.

[3] John B. Fraleigh. *A first course in abstract algebra (Addison-Wesley series in mathematics)*. Addison-Wesley Pub. Co, July 1976.

[4] V.D. Goppa. *Geometry and Codes*. Mathematics and its Applications (Kluwer Academic).: Soviet Series. Kluwer Acad. Publ., 1988.

[5] Tom Hoholdt and Ruud Pellikaan. On the decoding of algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 41:1589–1614, 1995.

[6] S. Ling and C. Xing. *Coding Theory: A First Course*. Cambridge University Press, 2004.

[7] J. H. Van Lint. *Introduction to Coding Theory*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 3rd edition, 1998.

[8] J.H. Lint and G. Geer. *Introduction to coding theory and algebraic geometry*. DMV Seminar. Birkhauser, 1988.

[9] Hiren Maharaj, Gretchen L. Matthews, and Gottlieb Pirsic. Riemann-Roch spaces of the hermitian function field with applications to algebraic geometry codes and low-discrepancy sequences. *Journal of Pure and Applied Algebra*, 195(3):261 – 280, 2005.

[10] E. Martínez-Moro, C. Munera, and D. Ruano. *Advances In Algebraic Geometry Codes*. Series on Coding Theory and Cryptology. World Scientific, 2008.

[11] Ruud Pellikaan. On a decoding algorithm for codes on maximal curves. *IEEE Transactions on Information Theory*, 35(6):1228–1232, 1989.

[12] D. Rotillon and J. Thiongly. Decoding of codes on the klein quartic. In Gérard Cohen and Pascale Charpin, editors, *EUROCODE '90*, volume 514 of *Lecture Notes in Computer Science*, pages 135–149. Springer Berlin / Heidelberg, 1991.

[13] Alexei N. Skorobogatov and Serge G. Vladut. On the decoding of algebraic-geometric codes. *IEEE Transactions on Information Theory*, 36(5):1051–1060, 1990.

[14] Henning Stichtenoth. Self-dual Goppa codes. *Journal of Pure and Applied Algebra*, 55:199 – 211, 1988.

[15] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Springer, 1993.

Lista de símbolos

$C^{\perp}$ Código dual *40*

D Divisor *10*

E_w Función localizadora de errores *56*

F/K Campo de funciones *1*

S Síndrome del código C *55*

$[n, k, d]_q$ Parámetros de un código *39*

α Adele *18*

$\mathcal{D}_F$ Conjunto de divisores *10*

$\mathcal{O}$ Anillo de Valoración *2*

$\mathbb{P}_F$ Conjunto de lugares *4*

$\mathcal{P}_F$ Conjunto de divisores principales *11*

$d(C)$ Distancia mínima *39*

$d(a, b)$ Distancia de Hamming *39*

g Género de F/K *17*

$i(A)$ Índice de espacialidad de A *18*

$s(w, f)$ Síndrome de w respecto a f *55*

v_P Valoración Discreta *6*

$C_{\mathcal{L}}(D, G)$ Código de Goppa *43*

F_P Campo residual *6*

H Matriz de Verificación *40*

S_Q Mapeo S_Q *59*

$\mathbb{D}_k$ Conjunto de divisores efectivos de grado k *68*

ι_Q Mapeo ι *59*

C_F^0 Clase de divisores de grado cero *68*

$\mathcal{L}(A)$ Espacio de Riemann-Roch del divisor A *12*

π_Q Mapeo π *59*

d^* Distancia de diseño *45*

$s(C)$ Defecto de Singleton *41*

$\mathcal{A}_F$ Conjunto de adeles *18*

$\mathcal{D}_F$ Grupo de divisores *10*

Ω_F Diferenciales de Weil *19*

Índice alfabético