UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

CRIPTOGRAFÍA ASIMÉTRICA SOBRE CAMPOS DE FUNCIONES HIPERELÍPTICOS DE GÉNERO 2

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

M A T E M Á T I C O

P R E S E N T A:

EDUARDO RUIZ DUARTE

DIRECTOR DE TESIS:
DR. OCTAVIO PÁEZ OSUNA

Hoja de datos de jurado

1. Datos del alumno. Ruiz Duarte Eduardo 55 24 12 43 Universidad Nacional Autónoma de México Facultad de Ciencias Matemático 405065141
2. Datos del tutor Dr. Octavio Páez Osuna
3. Datos del sinodal 1 Dr. Rodolfo San Agustín Chi
4. Datos del sinodal 2 Dr. José de Jesús Galaviz Casas
5. Datos del sinodal 3 Mat. Julio César Guevara Bravo
6. Datos del sinodal 4 M. en C. Rolando Gómez Macedo
7. Datos del trabajo escrito Criptografía asimétrica sobre campos de funciones hiperelípticos de género 2 65p 2012

Education is a system of imposed ignorance
Noam Chomsky

Agradecimientos.

Este trabajo no pudo haber sido sin los consejos, asesoría y paciencia del Dr. Octavio Páez, también agradezco infinitamente a mis sinodales por darme consejos para el desarrollo de este trabajo.

Quiero agradecer infinitamente a mi madre María Guadalupe Duarte por haberme apoyado en mi desarrollo como persona y por siempre aconsejarme para alcanzar mis metas.

A Ximena Tochtli Bouchain quién me motiva a perseguir conocimiento y a hacer de esta vida algo más interesante.

También quiero agradecer a Gloria Duarte quién me enseñó a leer, Carlos Duarte quién me motivó con sus acciones a estudiar algo tan bello como son las matemáticas, a Miguel Ángel Duarte por su apoyo incondicional.

También quiero agradecer a aquellas personas con las que a lo largo de la carrera me hicieron amar las matemáticas con su pasión por ésta, personas como Ángel Zaldivar, Rubén Águeda, Daniel Allard y muchos más.

También a grandes amigos como Alejandro Sánchez, Omar Lara, Rommel Sánchez.

¡Gracias a todos!

Criptografiá asimétrica sobre campos de funciones hiperelípticos de género 2

Eduardo Ruiz Duarte
Facultad de Ciencias,
Universidad Nacional Autónoma de México,
rduarte@ciencias.unam.mx

13 de diciembre de 2012

Introducción

La criptografía asimétrica o de llave pública es relativamente nueva, y consiste básicamente en un sistema criptográfico que requiere dos llaves separadas, donde una es la secreta y la otra es pública, y ambas están matemáticamente relacionadas, una sirve para cifrar un texto y la otra para descifrar, ninguna de las dos llaves puede hacer ambas cosas, una de estas llaves es pública y la otra privada, y de la pública deberá ser un problema complejo el recuperar la privada, uno de estos problemas es el logaritmo discreto en un grupo G el cual trataremos más adelante.

El primer artículo documentado donde se hablaba de criptografía asimétrica fue en 1976 por Whitfield Diffie y Martin Hellman, "New directions in cryptography" [8] donde este descubrimiento revolucionó las telecomunicaciones. Ellos escribieron sobre un esquema que permite tener dos llaves, una pública y una privada aseguradas por el problema de logaritmo discreto el cual se define así:

Definición 1 *Sea G un grupo cíclico finito con n elementos. Describiremos al grupo multiplicativamente. Sea $b \in G$ un generador del grupo, entonces $\forall g \in G$ tenemos que $g = b^k$ para algún $k \in \mathbb{N}$. Además si $g = b^{k_1} = b^{k_2}$ tenemos que $k_1 \equiv k_2 \mod n$ lo que motiva a definir el siguiente morfismo:*

$$log_b : G \to \mathbb{Z}/n\mathbb{Z}$$
$$g \mapsto k$$

Éste es el morfismo que asigna a cada $g \in G$ la clase k módulo n con $b^k = g$ A esto le llamamos logaritmo discreto base b en G, y es un isomorfismo.

Un protocolo de intercambio de llaves sobre un canal no seguro (público)

basado en este morfismo es el protocolo Diffie-Hellman [8].
La seguridad de Diffie-Hellman consiste en calcular el isomorfismo, por ejemplo sobre $< \mathbb{F}_q^{\times}, \cdot >$ i.e. La parte multiplicativa del campo $\mathbb{F}_q$ se define así:

Supongamos que A=Alberto y B=Berenice quieren ponerse de acuerdo en un secreto, pero E=Eulalio tiene acceso a toda su negociación y ellos no desean que E conozca el secreto, Ellos lo resuelven de la siguiente manera:

1. A y B se ponen de acuerdo en un grupo cíclico finito $< \mathbb{F}_q^{\times}, \cdot >$ y un generador g públicamente
2. A escoge un elemento $\alpha \in \mathbb{Z}/(q-1)\mathbb{Z}$ privado, calcula $A_{pub} = g^{\alpha}$ y se lo manda a B públicamente
3. B escoge un elemento $\beta \in \mathbb{Z}/(q-1)\mathbb{Z}$ privado, calcula $B_{pub} = g^{\beta}$ y se lo manda a A públicamente
4. A calcula $(B_{pub})^{\alpha} = S_A$
5. B calcula $(A_{pub})^{\beta} = S_B$

$S_A = S_B$ ya que $S_A = (g^{\beta})^{\alpha}$ y $S_B = (g^{\alpha})^{\beta}$

En la práctica, un adversario que quiera obtener la llave secreta tiene que calcular los exponentes secretos α y β. Este protocolo es muy importante ya que permite a dos entidades poder negociar un secreto S a través de un canal no seguro, y como vimos anteriormente, el saber $A_{pub},\ B_{pub}$, la estructura del grupo y el generador no es suficiente para poder calcular logaritmos discretos fácilmente, i.e. α y β.

Existen algoritmos para calcular este logaritmo, aunque poco eficientes. el poder de cómputo avanza y es necesario considerar otros grupos así como estudiar la dificultad de resolver el problema de logaritmo discreto en ellos y no sólo enfocarse a $< \mathbb{F}_q^{\times}, \cdot >$

El objetivo de este documento es el presentar al grupo de clases de divisores de grado cero o jacobiana de una curva hiperelíptica como un candidato para la implementación de este protocolo. Es necesario estudiar a fondo la estructura algebraica asociada a la curva, en particular su campo de funciones algebraicas, para poder realizar implementaciones prácticas.

Índice general

1. Lugares y valoraciones discretas **7**
- 1.1. Anillos de valoración 7
- 1.2. Valoraciones 10
  - 1.2.1. Ceros y polos de elementos de $\mathbb{F}/\mathbb{K}$ 13
- 1.3. Campo de funciones racionales 14
- 1.4. Teorema de aproximación débil 15

2. Divisores y Jacobianas **17**
- 2.1. Divisores 19
- 2.2. El Teorema de Riemann-Roch 27
  - 2.2.1. Teorema de Clifford, Weierstrass y criterio de Eisenstein 35
- 2.3. Extensiones Algebraicas de $\mathbb{F}/\mathbb{K}$. 38

3. Campos de funciones hiperelípticos **43**
- 3.1. Divisores reducidos 45
  - 3.1.1. Representación con polinomios de clases de ${C_{\mathbb{F}}}^0$ 46
- 3.2. Implementación de adición usando divisores reducidos en ${C_{\mathbb{F}}}^0$. 47
  - 3.2.1. Idea general 47
  - 3.2.2. Adición explícita en ${C_{\mathbb{F}}}^0$ con divisores usando la representación de Mumford g=2 49
- 3.3. Ejemplo desarrollado $[D_1] \oplus [D_2]$ 53
- 3.4. Ejemplo desarrollado $2[D]$ 55
- 3.5. Diffie-Hellman hiperelíptico 57
  - 3.5.1. Problema de logaritmo discreto hiperelíptico 57
  - 3.5.2. Implementación de Diffie-Hellman hiperelíptico y ejemplo 57
- 3.6. Conclusión 58

Capítulo 1

Lugares y valoraciones discretas

1.1. Anillos de valoración

En esta sección construiremos la noción de "lugar" a través de anillos de valoración, analizaremos y demostraremos algunas propiedades para poder construir una valoración discreta que nos permitirá poder analizar un conjunto algebraico

Definición 2 *Un campo de funciones* $\mathbb{F}/\mathbb{K}$ *en una variable sobre* $\mathbb{K}$ *es una extensión* $\mathbb{K} \subseteq \mathbb{F}$ *tal que* $\mathbb{F}$ *es una extensión algebraica finita de* $\mathbb{K}(x)$ *para algún* $x \in \mathbb{F}$ *trascendente sobre* $\mathbb{K}$

Denotamos por $\tilde{\mathbb{K}}$ a los elementos de $\mathbb{F}/\mathbb{K}$ que son algebraicos sobre $\mathbb{K}$, este conjunto es:

$$\tilde{\mathbb{K}} := \{z \in \mathbb{F} \mid z \text{ es algebraico sobre } \mathbb{K}\} \tag{1.1}$$

Éste es subcampo de $\mathbb{F}$, y es llamado el campo de constantes de $\mathbb{F}/\mathbb{K}$.

Definición 3 *Un anillo de valoración del campo de funciones* $\mathbb{F}/\mathbb{K}$ *es un anillo* $\mathcal{O} \subseteq \mathbb{F}$ *con las siguientes propiedades*

a) $\mathbb{K} \subsetneq \mathcal{O} \subsetneq \mathbb{F}$

b) $\forall z \in \mathbb{F},\ z \in \mathcal{O}$ *o* $z^{-1} \in \mathcal{O}$

Veamos un ejemplo:

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x),\ g(x) \in \mathbb{K}[x],\ p(x) \nmid g(x) \right\} \tag{1.2}$$

Vamos a ver que éste es en efecto un anillo de valoración de $\mathbb{K}(x)/\mathbb{K}$

Demostración.
P.D. a) $\mathbb{K} \subsetneq \mathcal{O}_{p(x)} \subsetneq \mathbb{K}(x)$

$\mathbb{K} \subset \mathcal{O}_{p(x)}$ ya que si $w \in \mathbb{K}$, $w = \frac{a}{b}$ con $a, b \in \mathbb{K}$ y $p(x) \nmid b \Rightarrow w \in \mathcal{O}_{p(x)}$.
Ahora $\mathbb{K} \neq \mathcal{O}_{p(x)}$ ya que si $z \in \mathcal{O}_{p(x)}$, $z = \frac{a(x)}{b(x)}$ con $a(x),\ b(x) \in \mathbb{K}[x] \backslash \mathbb{K}$ y $p(x) \nmid b(x)$, claramente $z \notin \mathbb{K}$ por lo tanto $\mathbb{K} \neq \mathcal{O}_{p(x)}$.
Por otro lado todos los elementos de $\mathcal{O}_{p(x)}$ son de la forma $\frac{s}{t}$ con $s, t \in \mathbb{K}[x]$ y $p(x) \nmid t$ lo cual prueba que $\mathcal{O}_{p(x)} \subsetneq \mathbb{K}(x)$

P.D.) b) $\forall z \in \mathbb{K}(x),\ z \in \mathcal{O}_{p(x)}\ o\ z^{-1} \in \mathcal{O}_{p(x)}$

Sea $y \in \mathbb{K}(x)$ supongamos que $y \notin \mathcal{O}_{p(x)} \Rightarrow y = \frac{a(x)}{b(x)p(x)}$ e y está reducido $\Rightarrow y^{-1} = \frac{b(x)p(x)}{a(x)}$ y $p(x) \nmid a(x) \Rightarrow y^{-1} \in \mathcal{O}_{p(x)}$
análogamente si suponemos que $y^{-1} \notin \mathcal{O}_{p(x)}$ ■

Proposición 1.1.1 *Sea $\mathcal{O}$ un anillo de valoración del campo de funciones $\mathbb{F}/\mathbb{K}$ entonces:*

1. *$\mathcal{O}$ es anillo local i.e. sólo tiene un ideal máximo $P = \mathcal{O} \backslash \mathcal{O}^\times$ con*

$$\mathcal{O}^\times = \{z \in \mathcal{O} \,\big|\, \exists w \in \mathcal{O}, zw = 1\} \tag{1.3}$$

   Éste es el grupo de unidades de $\mathcal{O}$

2. *Si $0 \neq x \in \mathbb{F}$ entonces $x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$*

3. *Para $\tilde{\mathbb{K}}$ tenemos que $\tilde{\mathbb{K}} \subseteq \mathcal{O}$ y $\tilde{\mathbb{K}} \cap P = \{0\}$*

Por simplicidad, el anillo de valoración con ideal máximo P, cuando no sea ambiguo será denotado por $\mathcal{O}_p$ u $\mathcal{O}$

Demostración.
P.D. 1): P es el único ideal máximo de $\mathcal{O}$
a) Sea $x \in P$ y $z \in \mathcal{O} \Rightarrow xz \in P$ ya que si $xz \in \mathcal{O}^\times$ sucedería que $x \in \mathcal{O}^\times$ lo cual es falso por como definimos a P.

b) ahora si $x, y \in P$ hay que demostrar que $< P, + >$ es un grupo:
s.p.g. supongamos que $\frac{x}{y} \in \mathcal{O}$ y como $\mathbb{K} \subset \mathcal{O}$, $\frac{x}{y} + 1 \in \mathcal{O}$ y tenemos que

$x + y = y(\frac{x}{y} + 1)$ ya que $y \in P$ y $\frac{x}{y} + 1 \in \mathcal{O}$ y como demostramos en a) $\Rightarrow y(\frac{x}{y} + 1) \in P$
Esto demuestra que $x + y \in P$ y P es un ideal de $\mathcal{O}$
Supongamos que P no es máximo esto es que existe un I tal que $P \subsetneq I \neq \mathcal{O}$ con I otro ideal esto significa que existe un $z \in I$ tal que $z \notin P \Rightarrow z \notin \mathcal{O}\backslash\mathcal{O}^{\times} \Rightarrow z \in \mathcal{O}^{\times}$ por lo tanto $\mathcal{O}^{\times} \subset I$ lo que nos indica que $I = \mathcal{O}$ $\nleftrightarrow$ ya que $I \neq \mathcal{O}$ por lo tanto P es el único ideal máximo de $\mathcal{O}$

P.D. 2): $0 \neq x \in \mathbb{F}$ entonces $x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$

Sea $0 \neq x \in \mathbb{F}$ y $x \in P \Rightarrow x \notin \mathcal{O}^{\times}$ por lo que $x^{-1} \notin \mathcal{O}$
de regreso tenemos que si $x^{-1} \notin \mathcal{O} \Rightarrow x \in \mathcal{O}$ esto nos dice que $x \notin \mathcal{O}^{\times} \Rightarrow x \in P = \mathcal{O}\backslash\mathcal{O}^{\times}$

P.D. 3): $\tilde{\mathbb{K}} \subseteq \mathcal{O}$ y $\tilde{\mathbb{K}} \cap P = \{0\}$

Primero veamos que $\tilde{\mathbb{K}} \subseteq \mathcal{O}$
Sea $z \in \tilde{\mathbb{K}}$ supongamos que $z \notin \mathcal{O} \Rightarrow z^{-1} \in \mathcal{O}$ como z^{-1} es algebraico sobre $\mathbb{K}$ existe un polinomio

$$a_n(z^{-1})^n + \ldots + a_2(z^{-1})^2 + a_1 z^{-1} + 1 = 0 \tag{1.4}$$

$\Rightarrow z^{-1}a_n(z^{-}1)^{n-1} + ... + a_1 = -1$
$\Rightarrow z = -(a_n(z^{-1})^{n-1} + \ldots + a_1) \in \mathbb{K}[z^{-1}] \subseteq \mathcal{O}$
$\Rightarrow z \in \mathcal{O}$ $\perp$ ya que $z \notin \mathcal{O}$ por lo tanto $\tilde{\mathbb{K}} \subseteq \mathcal{O}$

Ahora basta ver que $\tilde{\mathbb{K}} \cap P = \{0\}$
Como $\tilde{\mathbb{K}}$ es campo y P no tiene elementos invertibles esto se sigue inmediatamente ■

Teorema 1.1.2 *Sea $\mathcal{O}$ un anillo de valoración del campo de funciones $\mathbb{F}/\mathbb{K}$ y sea P su único ideal máximo, entonces lo siguiente sucede:*

- *P es un ideal principal*
- *Si $P = t\mathcal{O}$ entonces para todo $0 \neq z \in \mathbb{F}$ tiene una única representación de la forma $z = t^n u$ para alguna $n \in \mathbb{Z}$ y $u \in \mathcal{O}^{\times}$*
- *$\mathcal{O}$ es un dominio de ideales principales. i.e., si $P = t\mathcal{O}$ y $\{0\} \neq I \subseteq \mathcal{O}$ es un ideal, entonces $I = t^n\mathcal{O}$ para alguna $n \in \mathbb{N}$*

Definición 4 *A continuación definiremos lo que es un lugar, variable uniformizadora y lo que es $\mathcal{O}_P$*

- *Un lugar P de $\mathbb{F}/\mathbb{K}$ es el ideal máximo de un anillo $\mathcal{O}$ de $\mathbb{F}/\mathbb{K}$, todo elemento $t \in P$ tal que $P = t\mathcal{O}$ es llamado elemento primo para P o variable uniformizadora.*

- $\mathbb{P}_{\mathbb{F}} := \{P \mid P \text{ es un lugar de } \mathbb{F}/\mathbb{K}\}$

- *Si $\mathcal{O}$ es un anillo de valoración de $\mathbb{F}/\mathbb{K}$ y P su ideal máximo, entonces $\mathcal{O}$ está determinado únicamente por P, $\mathcal{O} := \{z \in \mathbb{F} \mid z^{-1} \notin P\}$ por lo que queda justificada la notación $\mathcal{O}_P := \mathcal{O}$ éste es el anillo de valoración en el lugar P*

A continuación definiremos en términos de valoraciones lo que es $\mathcal{O}_P$ lo que será más útil posteriormente

1.2. Valoraciones

Definición 5 *Decimos que una valoración discreta de $\mathbb{F}/\mathbb{K}$ es una función $v : \mathbb{F} \to \mathbb{Z} \cup \{\infty\}$ con las siguientes propiedades:*

1. $v(x) = \infty \Leftrightarrow x = 0$
2. $v(xy) = v(x) + v(y)\ \forall x, y \in \mathbb{F}$
3. $v(x + y) \geq min\{v(x), v(y)\}\ \forall x, y \in \mathbb{F}$
4. $\exists z \in \mathbb{F}$ *tal que* $v(z) = 1$
5. $v(a) = 0\ \forall a \in \mathbb{K}$

En nuestro contexto, llamaremos a la propiedad 3) desigualdad del triángulo. El siguiente lema es de suma utilidad, pues nos permite calcular valoraciones en sumas de elementos de $\mathbb{F}$.

Lema 1.2.1 *Desigualdad del triángulo estricta*
Sea v una valoración discreta de $\mathbb{F}/\mathbb{K}$ y sea $x, y \in \mathbb{F}$ con $v(x) \neq v(y)$, entonces $v(x + y) = min\{v(x), v(y)\}$

Demostración. Sabemos que $v(ay) = v(y)$ para $0 \neq a \in \mathbb{K}$, en particular $v(-y) = v(y)$ y como $v(x) \neq v(y)$ podemos suponer que $v(x) < v(y)$ y supongamos que $v(x+y) \neq min\{v(x), v(y)\}$, entonces por la definición de valoración discreta tenemos que $v(x+y) > v(x)$ y tenemos que $v(x) = v((x+y)-y) \geq min\{v(x+y), v(y)\} > v(x)$, lo cual no es posible ■

La siguiente definición será primordial para el resto del documento, ya que nos indicará un parámetro importante de una función racional de $\mathbb{F}$ con respecto a un lugar P

Definición 6 *A un $P \in \mathbb{P}_{\mathbb{F}}$, le asociamos una función $v_P : \mathbb{F} \to \mathbb{Z} \cup \{\infty\}$ la cual es una valoración discreta de $\mathbb{F}/\mathbb{K}$ ya que si t es una variable uniformizadora de P entonces para todo $0 \neq z \in \mathbb{F}$ existe una única representación $z = t^n u$ con $u \in \mathcal{O}_P{}^{\times}$ y $n \in \mathbb{Z}$, entonces definimos $v_P(z) := n$ y $v_P(0) := \infty$*

Proposición 1.2.2 *La definición anterior no depende de t*

Demostración. Sea t' otra variable uniformizadora de P (i.e. $P = t\mathcal{O}$) entonces tenemos que $P = t\mathcal{O} = t'\mathcal{O}$ por lo que $t = t'w$ para algún $w \in \mathcal{O}_P{}^{\times}$ por lo que tenemos que $t^n u = (t'^n w^n)u = t'^n(w^n u)$ con $w^n u \in \mathcal{O}_P{}^{\times}$■

Con esto estamos listos para definir $\mathcal{O}_P$, P y $\mathcal{O}_P{}^{\times}$ en términos de v_P

Teorema 1.2.3 *Sea $\mathbb{F}/\mathbb{K}$ un campo de funciones, v_P como en la definición 5 es una valoración discreta de $\mathbb{F}/\mathbb{K}$ y se cumple que:*

1. $\mathcal{O}_P = \{z \in \mathbb{F} \mid v_P \geq 0\}$
2. $\mathcal{O}_P{}^{\times} = \{z \in \mathbb{F} \mid v_P = 0\}$
3. $P = \{z \in \mathbb{F} \mid v_P > 0\}$

Demostración. Hay que usar la definición 4, es fácil probar todas las condiciones, pero la que requiere un poco de más desarrollo es la desigualdad del triángulo, para la condición 1 es por definición, la 2 es usando propiedades de exponentes, la 4 es utilizando el parámetro uniformizador t tal que $P = t\mathcal{O}$ y tenemos que $t \in P \subset \mathcal{O}_P$, para la condición 5 tenemos que $\mathbb{K} \subset \mathbb{F}$ y $at^0 = a$

Ahora basta demostrar que $v_P(x+y) \geq min\{v_P(x), v_P(y)\} \forall x, y \in \mathbb{F}$
Sea $x, y \in \mathbb{F}$ con $v_P(x) = n$ y $v_P(y) = m$ y supongamos que $n \leq m < \infty$, entonces $x = t^n u_1$ y $y = t^m u_2$ con $u_1, u_2 \in \mathcal{O}_{\mathcal{P}}{}^{\times}$ por lo que $x + y = t^n(u_1 + t^{m-n}u_2) = t^n z$ con $z \in \mathcal{O}_P$ y si $z = 0$ $v_P(x+y) = \infty > min\{n, m\}$, si

esto no sucediera, tendría que pasar que $z = t^k u$ para algún $k \geq 0$ y $u \in \mathcal{O}_{\mathcal{P}}{}^{\times}$ entonces:

$$v_P(x+y) = v_P(t^{n+k}u) = n+k \geq n = min\{v_P(x), v_P(y)\} \tag{1.5}$$

Ahora para la parte 1 basta ver que las $z \in \mathbb{F}$ son de la forma $z = t^n u$ con $u \in \mathcal{O}^{\times}{}_P$ como $z \in \mathcal{O}_P$ puede suceder que $z = cu$ o $z = t^n u$ con $t \in P$ por definición de $\mathcal{O}_P$, si $z = cu$ entonces $c = t^0 c$ por lo que $v_P(z) = 0$, si $z = t^n u$ con $u \notin \mathcal{O}_P$ entonces $v_P(z) = n > 0$.
2 se sigue inmediatamente de 1.
Para demostrar 3 usamos que $P = t\mathcal{O}_P$ y P no tiene unidades por ser ideal de $\mathcal{O}_P$ y $P := \mathcal{O}_P \setminus \mathcal{O}_P{}^{\times}$ entonces $z = t^n u$ con $u \notin P$ por lo que $t^n \in P \Rightarrow v_P(z) = n > 0$ ■

Definición 7 *Campo de clases residuales y grado de un lugar*

1. $\mathbb{F}_P := \mathcal{O}_P/P$ *será el campo de clases residuales de* P*, eso es campo porque* P *es máximo en* $\mathcal{O}_P$*, estas clases las definiremos como* $x+P := x(P)$.

2. $grado(P) := [\mathbb{F}_P : \mathbb{K}]$ *será el grado de* P

Ahora vamos a demostrar que el $grado(P) < \infty$

Proposición 1.2.4 *Si* $P \in \mathbb{P}_{\mathbb{F}}$ *y* $0 \neq x \in P$ *entonces* $grado(P) \leq [\mathbb{F} : \mathbb{K}(x)] < \infty$

DEMOSTRACIÓN. Es fácil ver que $[\mathbb{F} : \mathbb{K}(x)] < \infty$ porque si $x \in \mathbb{F}$ y x es trascendente sobre $\mathbb{K}$ sucede si $[\mathbb{F} : \mathbb{K}(x)]$ es una extensión finita, sólo basta demostrar que si $z_1, ..., z_n \in \mathcal{O}_P$, cuyas clases residuales son $z_1(P), ..., z_n(P) \in \mathbb{F}_P$ son linealmente independientes sobre $\mathbb{K}$ también son linealmente independientes sobre $\mathbb{K}(x)$. Supongamos que existe una combinación lineal no trivial.

$$\sum_{i=1}^{n} \phi_i(x) z_i = 0 \tag{1.6}$$

Donde $\phi_i(x) \in \mathbb{K}(x)$, sin pérdida de generalidad supongamos que $\phi_i(x) = a_i + xg_i(x)$ con $a_i \in \mathbb{K}$ y $g_i(x) \in \mathbb{K}(x)$, donde no todos los $a_i = 0$. Como $x \in P$ y $g_i(x) \in \mathcal{O}_P$, $\phi_i(x)(P) = a_i(P) = a_i$, aplicando el mapeo $x \mapsto x(P)$ de $\mathbb{F}$ a $\mathbb{F}_P \cup \{\infty\}$ a (1.6) tenemos:

$$0 = 0(P) = \sum_{i=1}^{n} \phi_i(x)(P)z_i(P) = \sum_{i=1}^{n} a_i z_i(P) \tag{1.7}$$

Esto contradice la independencia lineal de $z_1(P), ..., z_n(P)$. ■

1.2.1. Ceros y polos de elementos de $\mathbb{F}/\mathbb{K}$

Definición 8 *Sea $z \in \mathbb{F}$ y $P \in \mathbb{P}_\mathbb{F}$, decimos que P es un cero de z si $v_P(z) > 0$ y P es un polo de z si $v_P(z) < 0$, si $v_P(z) = m > 0$ entonces P es cero de z de orden m, si $v_P(z) = -m < 0$ decimos que P es polo de z de orden m.*

Hasta ahora no hemos demostrado que $\mathbb{P}_\mathbb{F}$ tenga elementos, es decir que existan lugares, esto se puede ver en [5] donde básicamente un esbozo de la demostración es considerando el conjunto:

$\mathcal{F} := \{S \mid S$ es un subanilo de $\mathbb{F}$ con $R \subseteq S$ y $IS \neq S\}$
Donde I es un ideal propio de R, como $\mathcal{F}$ está ordenado por inclusión y al menos $R \in \mathcal{F}$ usando el lema de Zorn tenemos que $\mathcal{F}$ tiene un elemento máximo, esto significa que existe un anillo $\mathcal{O} \subseteq \mathbb{F}$ tal que $R \subseteq \mathcal{O} \subseteq \mathbb{F}$, $I\mathcal{O} \neq \mathcal{O}$ y $\mathcal{O}$ es máximo, en la demostración se prueba que $\mathcal{O}$ es un anillo de valoración usando lo anterior, de lo cual se deduce que $\mathbb{P}_\mathbb{F} \neq \emptyset$

Como consecuencia podemos demostrar el siguiente corolario suponiendo lo anterior:

Corolario 1.2.5 *Sea $\mathbb{F}/\mathbb{K}$ un campo de funciones, $z \in \mathbb{F}$ trascendente sobre $\mathbb{K}$, entonces z tiene al menos un cero y un polo, en particular $\mathbb{P}_\mathbb{F} \neq \emptyset$*

Demostración. Consideremos $R = \mathbb{K}(z)$ y a $I = z\mathbb{K}(z)$, por lo anterior sabemos que existe un lugar $P \in \mathbb{P}_\mathbb{F}$ con $z \in P$, por lo que P es un cero de z, de igual manera z^{-1} tiene un cero en $Q \in \mathbb{P}_\mathbb{F}$, por lo que Q es un polo de z ■

1.3. Campo de funciones racionales

A continuación veremos un caso interesante en el que $\mathbb{F} = \mathbb{K}(x)$ con x trascendente sobre $\mathbb{K}$, esto lo construiremos dado un polinomio mónico irreducible $p(x) \in \mathbb{K}[x]$, consideremos el siguiente anillo de valoración de $\mathbb{K}(x)/\mathbb{K}$:

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \,\middle|\, f(x), g(x) \in \mathbb{K}[x],\ p(x) \nmid g(x) \right\} \tag{1.8}$$

Su ideal máximo es:

$$P_{p(x)} := \left\{ \frac{f(x)}{g(x)} \,\middle|\, f(x), g(x) \in \mathbb{K}[x],\ p(x) \mid f(x),\ p(x) \nmid g(x) \right\} \tag{1.9}$$

Aquí la valoración la definimos como:

$$v_{p(x)} : \mathbb{K}(x) \to \mathbb{Z} \cup \{\infty\} \tag{1.10}$$

$$z \mapsto n \tag{1.11}$$

De modo que $z = p(x)^n \frac{f(x)}{g(x)}$ y $f(x),\ g(x) \in \mathbb{K}[x]$

Por el teorema 1.2.3 podemos definir en términos de valoraciones

$$\mathcal{O}_{p(x)} := \left\{ z \in \mathbb{K}(x) \middle| v_{p(x)} \geq 0 \right\} \tag{1.12}$$

$$P_{p(x)} := \left\{ z \in \mathbb{K}(x) \middle| v_{p(x)} > 0 \right\} \tag{1.13}$$

Y como en la definición 6, el campo residual será $\mathbb{K}_{p(x)} := \mathcal{O}_{p(x)}/P_{p(x)}$ y $grado(P_{p(x)}) = [\mathbb{K}_{p(x)} : \mathbb{K}]$.

Otro anillo de valoración de $\mathbb{K}(x)/\mathbb{K}$ importante es:

$$\mathcal{O}_{\infty} := \left\{ \frac{f(x)}{g(x)} \,\middle|\, f(x), g(x) \in \mathbb{K}[x],\ grad\, f(x) \leq grad\, g(x) \right\} \tag{1.14}$$

Su ideal máximo es:

$$P_{\infty} := \left\{ \frac{f(x)}{g(x)} \,\middle|\, f(x), g(x) \in \mathbb{K}[x],\ grad\, f(x) < grad\, g(x) \right\} \tag{1.15}$$

P_∞ será llamado el lugar infinito de $\mathbb{F} = \mathbb{K}(x)$, el símbolo ∞ es sólo notacional ya que por ejemplo en $\mathbb{K}(1/x)$ su lugar infinito sería $P_\infty := P_0$

1.4. Teorema de aproximación débil

Esta sección demostrará el teorema de aproximación débil con el cual podemos asegurar condiciones con las cuales podremos hacer criptografía próximamente.

Teorema 1.4.1 *Sea $\mathbb{F}/\mathbb{K}$ un campo de funciones y $P_1, P_2, ..., P_n \in \mathbb{P}_\mathbb{F}$ distintos lugares en pares de $\mathbb{F}/\mathbb{K}$, $x_1, x_2..., x_n \in \mathbb{F}$ y $r_1, r_2, ..., r_n \in \mathbb{Z}$ entonces existe una $x \in \mathbb{F}$ tal que*

$v_{Pi}(x - x_i) = r_i$ *con* $i = 1, 2, ..., n$

Lema 1.4.2 *Existe un $u \in \mathbb{F}$ tal que $v_1(u) > 0$ y $v_i(u) < 0$ para $i = 2, ..., n$*

Demostración. Procederemos por inducción sobre n.
Para $n = 2$ tenemos que $\mathcal{O}_{P_1} \nsubseteq \mathcal{O}_{P_2}$, $\mathcal{O}_{P_2} \nsubseteq \mathcal{O}_{P_1}$, como inicialmente vimos que los anillos de valoración son máximos y están contenidos propiamente en $\mathbb{F}$, existe $y_1 \in \mathcal{O}_{P_1} \backslash \mathcal{O}_{P_2}$ y $y_2 \in \mathcal{O}_{P_2} \backslash \mathcal{O}_{P_1}$ por lo que $v_1(y_1) \geq 0$, $v_2(y_1) < 0$, $v_1(y_2) < 0$ y $v_2(y_2) \geq 0$, por lo que y_1/y_2 tiene la propiedad deseada, i.e. $v_1(y_1/y_2) > 0$ y $v_2(y_1/y_2) < 0$.
Ahora para $n > 2$ tenemos que por hipótesis de inducción tenemos un y tal que $v_1(y) > 0\,, v_2(y) < 0, ..., v_{n-1}(y) < 0$, si $v_n(y) < 0$ ya terminamos, en el caso que $v_n(y) \geq 0$ tomamos z tal que $v_1(z) > 0$, $v_n(z) < 0$, y definimos $u := y + z^r$ con $r > 0$ y $rv_i(z) \neq v_i(y)$ para $i = 1, ..., n - 1$, se sigue que $v_1(u) \geq min\{v_1(y), rv_1(z)\} > 0$ y $v_i(u) = min\{v_i(y), rv_i(z)\} < 0$ para $i = 2, ..., n$ por la desigualdad del triángulo estricta ■

Lema 1.4.3 *Existe $w \in \mathbb{F}$ tal que $v_1(w-1) > r_1$ y $v_i(w) > r_i$ para $i = 2, ..., n$*

Demostración. Sea $u := y + z^r$ y $w := (1 + u^s)^{-1}$, tenemos que para una $s \in \mathbb{N}$ suficientemente grande, $v_1(w - 1) = v_1(-u^s(1 + u^s)^{-1}) = sv_1(u) > r_1$, y $v_i(w) = -v_i(1 + u^s) = -sv_i(u) > r_i$ para $i = 2, ..., n$. ■

Lema 1.4.4 *Dados $y_1, ..., y_n \in \mathbb{F}$, existe un elemento $z \in \mathbb{F}$ con $v_i(z-y_i) > r_i$ para $i = 1, ..., n$*

Demostración. Sea $s \in \mathbb{Z}$ tal que $v_i(y_j) \geq s$ para todo $i, j \in \{1, ..., n\}$, por el lema anterior existen $w_1, ..., w_n$ tal que:

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

Por lo que si construimos $z := \sum_{j=1}^{n} y_j w_j$ tenemos que $v_i(z - y_i) > r_i$. ■

Con estos últimos tres lemas, podemos demostrar el teorema de aproximación débil fácilmente.

Demostración.

Por el último lema podemos encontrar una $z \in \mathbb{F}$ tal que $v_i(z - x_i) > r_i$, $i = 1, ..., n$, ahora escogemos z_i tal que $v_i(z_i) = r_i$, por el mismo último lema tenemos que hay un z' tal que $v_i(z' - z_i) > r_i$ para $i = 1, ..., n$, por lo que se sigue lo siguiente:

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

Consideremos $x := z + z'$ y tenemos que:

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

La siguiente proposición se prueba con el teorema de aproximación débil la cual nos servirá para que en el siguiente capítulo demostremos que si $z \in \mathbb{F}$ es trascendente sobre $\mathbb{K}$, entonces ésta tiene el mismo número de ceros que de polos con multiplicidad contada, la prueba se puede ver en [5]

Proposición 1.4.5 *Sea $\mathbb{F}/\mathbb{K}$ un campo de funciones y sea $P_1, ..., P_r$ ceros de $x \in \mathbb{F}$ (i.e. $v_{P_i}(x) > 0,\ i \in \{1, ..., r\}$) entonces:*

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

En el siguiente capítulo construiremos divisores, los cuales nos ayudarán a manejar mejor la información de un elemento $z \in \mathbb{F}$ con respecto a sus ceros y polos, estos serán fundamentales para la construcción de la jacobiana.

Capítulo 2

Divisores y Jacobianas

Corolario 2.0.6 *Todo campo de funciones $\mathbb{F}/\mathbb{K}$ tiene un número infinito de lugares.*

Demostración. Supongamos que $\mathbb{F}/\mathbb{K}$ tiene un número finito de lugares, digamos $P_1, \ldots, P_n$. Por el Teorema 1.4.1 podemos encontrar una función $x \in F$ con $v_{P_i}(x) > 0$, para $i = 1, \ldots, n$. Entonces x es trascendente sobre $\mathbb{K}$ pues tiene ceros, pero x no tendría polos, contradiciendo el Corolario 1.2.5.■

Este último corolario es de suma importancia. De hecho demostraremos más adelante que todo elemento trascendente de $\mathbb{F}$ tiene tantos ceros como polos y un número finito de ellos. Un paso importante hacia este resultado es la siguiente

Proposición 2.0.7 *Sea $\mathbb{F}/\mathbb{K}$ un campo de funciones, $P_1, \ldots, P_n \in \mathbb{P}_\mathbb{F}$ ceros de $x \in F$. Entonces*

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

Demostración. Definimos $v_i := v_{P_i}, f_i := grado(P_i)$ y $e_i = v_i(x)$. Para toda i existe un elemento t_i (por ejemplo t_i parámetro local de P_i) con

$$v_i(t_i) = 1 \text{ and } v_k(t_i) = 0 \text{ for } k \neq i.$$

Escogemos funciones $s_{i1}, \ldots, s_{if_i} \in \mathcal{O}_{P_i}$ tales que los residuos

$$s_{i1}(P_i), \ldots, s_{if_i}(P_i)$$

sean una base para $\mathbb{F}_{P_i}$ sobre $\mathbb{K}$. Por el teorema de aproximación débil existen funciones $z_{ij} \in F$ tales que lo siguiente se cumple para toda i, j:

$$v_i(s_{ij} - z_{ij}) > 0 \text{ and } v_k(z_{ij}) \geq e_k \text{ for } k \neq i. \tag{2.1}$$

Afirmamos que los elementos

$$t_i^a \cdot z_{ij}, 1 \leq i \leq r, 1 \leq j \leq f_i, 1 \leq a \leq e_i$$

son linealmente independientes sobre $\mathbb{K}(x)$. En número son $\sum_{i=1}^{r} f_i e_i = \sum_{i=1}^{r} v_{P_i} \cdot grado(P_i)$, entonces la proposición se seguirá directamente.

El argumento es estándar: Supongamos que existe una combinación lineal no trivial de la forma

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija} z_{ij} = 0 \tag{2.2}$$

sobre $\mathbb{K}(x)$. Sin pérdida de generalidad podemos suponer que $\varphi_{ija} \in \mathbb{K}[x]$ y no todas las φ_{ija} son divisibles por x. entonces existen índices $k \in \{1, \ldots, r\}$ y $c \in \{1, \ldots, e_k - 1\}$ tales que

$$x | \varphi_{kja} \text{ para toda } a < c \text{ y toda } j \in \{1, \ldots, f_k\},$$
$$\text{y } x \nmid \varphi_{kjc} \text{ para alguna } j \in \{1, \ldots, f_k\}. \tag{2.3}$$

Multiplicando 2.2 por t_k^{-c} obtenemos

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija} t_i^a t_k^{-c} z_{ij} = 0. \tag{2.4}$$

Para $i \neq k$, todos los sumandos de 2.4 pertenecen a P_k ya que

$$v_k(\varphi_{ija} t_i^a t_k^{-c} z_{ij}) = v_k(\varphi_{ija}) + a v_k(t_i) - c v_k(t_k) + v_k(z_{ij})$$
$$\geq 0 + 0 - c + e_k > 0.$$

Para $i = k$ y $a < c$ tenemos que

$$v_k(\varphi_{kja} t_k^{a-c} z_{kj}) \geq e_k + a - c \geq e_k - c > 0.$$

(Notemos que $x | \varphi_{kja}$ y por lo tanto $v_k(\varphi_{kja}) \geq e_k$). Para $i = k$ y $a > c$, $v_k(\varphi_{kja} t_k^{a-c} z_{kj}) \geq a - c > 0$.

Combinando lo anterior con 2.4 obtenemos que

$$\sum_{j=1}^{f_k} \varphi_{kjc} z_{kj} \in P_k. \tag{2.5}$$

Observemos que $\varphi_{kjc}(P_k) \in \mathbb{K}$, y no todas las $\varphi_{kjc}(P_k) = 0$ (por 2.3), entonces 2.5 nos da la combinación lineal no trivial

$$\sum_{j=1}^{f_k} \varphi_{kjc}(P_k) \cdot z_{kj}(P_k) = 0$$

sobre $\mathbb{K}$. Esto es una contradicción, pues los elementos $z_{k1}(P_k), \ldots, z_{kf_k}(P_k)$ son una base de $\mathbb{F}_{P_k}/\mathbb{K}$. ■

Corolario 2.0.8 *En un campo de funciones $\mathbb{F}/\mathbb{K}$, todo elemento $0 \neq x \in F$ tiene un número finito de ceros y de polos.*

Demostración. Si x es una constante, entonces x no tiene ni ceros ni polos. Si x es trascendente sobre $\mathbb{K}$, el número de ceros está acotado por $[F : K(x)]$ por la Proposición 2.0.7. El mismo argumento muestra que x^{-1} tiene sólo un número finito de ceros, cada uno de ellos siendo un polo de x. ■

2.1. Divisores

Como el campo $\tilde{\mathcal{K}}$ de constantes de una extensión algebraica $\mathbb{F}/\mathbb{K}$ es una extensión finita de $\mathbb{K}$, y $\mathbb{F}$ se puede ver como un campo de funciones sobre $\mathcal{K}$, entonces podemos suponer que $\mathbb{F}/\mathbb{K}$ es un campo de funciones tal que $\mathbb{K}$ es el campo de constantes.

Definición 9 *Denotaremos por $Div(\mathbb{F})$, al grupo abeliano libre generado por los lugares de $\mathbb{F}/\mathbb{K}$. Le llamaremos el* ***grupo de divisores*** *de $\mathbb{F}/\mathbb{K}$.*

Llamaremos a los elementos de $Div(\mathbb{F})$ **divisores** de $\mathbb{F}/\mathbb{K}$. En otras palabras un divisor D es una suma formal de lugares

$$D = \sum_{P \in \mathbb{P}_\mathbb{F}} n_P P \text{ con } n_P \in \mathbb{Z}, \text{ y casi todas las } n_P = 0.$$

El **soporte** de un divisor $D \in Div(\mathbb{F})$ se define como

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

A veces es conveniente escribir

$$D = \sum_{P \in S} n_P P,$$

donde $S \subseteq \mathbb{P}_\mathbb{F}$ es un conjunto finito y $S \supseteq supp(D)$.

Un divisor de la forma $D = P$ con $P \in \mathbb{P}_\mathbb{F}$ se le llama **divisor primo** . Dados $D = \sum n_P P$ y $D' = \sum n'_P P$ se suman coeficiente a coeficiente:

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

El elemento cero del grupo $Div(\mathbb{F})$ es el divisor

$$0 := \sum_{P \in \mathbb{P}_\mathbb{F}} n_P P \text{ con todas las } n_P = 0.$$

Para $Q \in \mathbb{P}_\mathbb{F}$ y $D \in Div(\mathbb{F})$ definimos $v_Q(D) = n_Q$, entonces

$$supp(D) = \{P \in \mathbb{P}_\mathbb{F} | v_P(D) \neq 0\} \text{ y } D = \sum v_P(D) \cdot P.$$

Definimos un orden parcial en $Div(\mathbb{F})$ de la siguiente manera:

$$D_1 \leq D_2 :\Longleftrightarrow v_P(D_1) \leq v_P(D_2) \text{ para todo } P \in \mathbb{P}_\mathbb{F}.$$

Un divisor tal que $D \geq 0$ se dice **positivo** o **efectivo** . El **grado de un divisor** se define como

$$grado(D) := \sum_{P \in \mathbb{P}_\mathbb{F}} v_P(D) \cdot grado(P)$$

y define un homomorfismo $grado : Div(\mathbb{F}) \longrightarrow \mathbb{Z}$.

Como toda función $0 \neq x \in F$ tiene un número finito de ceros y de polos la siguiente definición tiene sentido.

Definición 10 *Sea $0 \neq x \in F$ y sean Z el conjunto de ceros y N el conjunto de polos de x en $\mathbb{P}_\mathbb{F}$. Definimos*

$$(x)_0 := \sum_{P \in Z} v_P(x)P, \text{ el divisor de ceros de } x,$$

$$(x)_\infty := -\sum_{P \in N} v_P(x)P, \text{ el divisor de polos de } x,$$

$$(x) := (x)_0 - (x)_\infty, \text{ el divisor principal de } x.$$

Claramente $(x)_0$ y $(x)_\infty$ son divisores positivos. Y

$$(x) = \sum_{P \in \mathbb{P}_\mathbb{F}} v_P(x)P. \tag{2.6}$$

Por lo tanto los elementos constantes distintos de cero en $\mathbb{F}$ se caracterizan como

$$x \in \mathbb{K} \Longleftrightarrow (x) = 0.$$

El conjunto

$$\mathcal{P}_F := \{(x) | 0 \neq x \in \mathbb{F}\}$$

es llamado el **grupo de divisores principales** de $\mathbb{F}/\mathbb{K}$. Es un subgrupo de $Div(\mathbb{F})$ pues si $0 \neq x, y \in \mathbb{F}$, entonces $(xy) = (x) + (y)$. El grupo cociente

$$C_\mathbb{F} := Div(\mathbb{F})/\mathcal{P}_F$$

le llamaremos el **grupo de clases de divisores**. Para $D \in Div(\mathbb{F})$, el elemento correspondiente en $C_{\mathbb{F}}$ se denota por $[D]$, la clase de D. Dos divisores D, $D' \in Div(\mathbb{F})$ se dicen equivalentes ($D \sim D'$) si $[D] = [D']$, esto es, $D = D' + (x)$ para alguna $x \in \mathbb{F}\backslash\{0\}$. Esta es una relación de equivalencia.

Los divisores principales serán el reemplazo que buscábamos para la descomposición en irreducibles de $\mathbb{K}(x)$.

Definición 11 *Dado un divisor $A \in Div(\mathbb{F})$ definimos*

$$\mathcal{L}(A) := \{x \in \mathbb{F} | (x) + A \geq 0\} \cup \{0\}.$$

Podemos interpretar la definición anterior como sigue: si escribimos

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

con $n_i > 0$ y $m_j > 0$ entonces $x \in \mathcal{L}(A)$ si y sólo si

1. x tiene ceros de orden $\geq m_j$ en los Q_j, para $j = 1, \ldots, s$ y
2. x sólo puede tener polos en $P_1, \ldots, P_r$, con orden polar P_i no mayor que las n_i, for $i = 1, \ldots, r$.

Se sigue que $x \in \mathcal{L}(A)$ si y sólo si $v_P(x) \geq -v_P(A)$ para todo $P \in \mathbb{P}_{\mathbb{F}}$. Tambien tenemos que $\mathcal{L}(A) \neq 0$ si y sólo si existe un divisor $A' \sim A$ con $A' \geq 0$.

Lema 2.1.1 *Sea $A \in Div(\mathbb{F})$. Tenemos que*

1. *$\mathcal{L}(A)$ es espacio vectorial sobre $\mathbb{K}$.*
2. *Si A' es un divisor equivalente a A entonces $\mathcal{L}(A) \simeq \mathcal{L}(A')$ como espacios vectoriales sobre $\mathbb{K}$.*

Demostración. (1) Sea $x, y \in \mathcal{L}(A)$ y $a \in \mathbb{K}$. Entonces

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

y $v_P(ax) = v_P(x) \geq -v_P(A)$ para todo $P \in \mathbb{P}_{\mathbb{F}}$ por lo tanto $x + y$ y ax son elementos de $\mathcal{L}(A)$.

(2) Por hipótesis $A = A' + (z)$ con $0 \neq z \in \mathbb{F}$. Consideremos el mapeo

$$\varphi : \left\{ \begin{array}{ccc} \mathcal{L}(A) & \to & \mathbb{F} \\ x & \mapsto & xz \end{array} \right.$$

Es un mapeo $\mathbb{K}$-lineal cuya imagen esta contenida en $\mathcal{L}(A')$. De manera similar el mapeo

$$\varphi' : \left\{ \begin{array}{ccc} \mathcal{L}(A') & \to & \mathbb{F} \\ x & \mapsto & xz^{-1} \end{array} \right.$$

es $\mathbb{K}$-lineal de $\mathcal{L}(A')$ a $\mathcal{L}(A)$. Y uno es el inverso del otro. Por lo tanto φ es un isomorfismo entre $\mathcal{L}(A)$ y $\mathcal{L}(A')$. ■

Lema 2.1.2 *1.* $\mathcal{L}(0) = K$.

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

Demostración. (1) Tenemos que $(x) = 0$ para $0 \neq x \in \mathbb{K}$, entonces $\mathbb{K} \subseteq \mathcal{L}(0)$. Si $0 \neq x \in \mathcal{L}(0)$ entonces $(x) \geq 0$ esto quiere decir que x no tiene polos y por lo tanto $x \in \mathbb{K}$.

(2) Supongamos que existe $0 \neq x \in \mathcal{L}(A)$. Entonces $(x) \geq -A > 0$, lo que implica que x tiene al menos un cero pero no tiene polos, lo cual es una contradicción. ■

El paso siguiente es demostrar que para todo $A \in Div(\mathbb{F})$, $\mathcal{L}(A)$ tiene dimensión finita sobre $\mathbb{K}$.

Lema 2.1.3 *Sean* $A, B \in Div(\mathbb{F})$ *tales que* $A \leq B$. *Entonces* $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ *y*

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

Demostración. Sea $x \in \mathcal{L}(A)$ entonces, para todo $P \in \mathbb{P}_{\mathbb{F}}$,

$$v_P(x) \geq -A \geq -B$$

por lo tanto $x \in \mathcal{L}(B)$. Para demostrar la otra afirmación supongamos primero que $B = A + P$ para algún $P \in \mathbb{P}_{\mathbb{F}}$, *i.e.*, los divisores A y B sólo difieren en el lugar P por uno. (El caso general se sigue por inducción). Por el Teorema de aproximación, podemos escoger un elemento $t \in \mathbb{F}$ tal que

$$v_P(t) = v_P(B) = v_P(A) + 1.$$

Para $x \in \mathcal{L}(B)$ tenemos que $v_P(x) \geq -v_P(B) = -v_P(t)$, y entonces $xt \in \mathcal{O}_P$. De esta manera obtenemos el mapeo $\mathbb{K}$-lineal

$$\psi : \left\{ \begin{array}{ccc} \mathcal{L}(B) & \to & \mathbb{F}_P, \\ x & \mapsto & (xt)(P). \end{array} \right.$$

x pertenece al kernel de ψ si y solo si $v_P(xt) > 0$, *i.e.* $v_P(x) > -v_P(A)$. Se sigue que $Ker(\psi) = \mathcal{L}(A)$, y que ψ induce un mapeo $\mathbb{K}$-lineal inyectivo de $\mathcal{L}(B)/\mathcal{L}(A)$ a $\mathbb{F}_P$. Entonces

$$dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq dim(\mathbb{F}_P) = grado(B) - grado(A).\blacksquare$$

Proposición 2.1.4 *Para todo divisor $A \in Div(\mathbb{F})$, el espacio $\mathcal{L}(A)$ tiene dimensión finita sobre $\mathbb{K}$. Esto es, si $A = A_+ - A_-$ con divisores positivos A_+ y A_-, entonces*

$$dim(\mathcal{L}(A)) \leq grado(A_+) + 1.$$

Demostración. Como $\mathcal{L}(A) \subseteqq \mathcal{L}(A_+)$, es suficiente demostrar que $dim(\mathcal{L}(A_+)) \leq grado(A_+) + 1$. Ahora bien $A_+ \geq 0$, entonces el Lema 2.1.3 dice que

$$dim(\mathcal{L}(A_+)/\mathcal{L}(0)) \leq grado(A_+).$$

Como $\mathcal{L}(0) = K$ por el Lema 2.1.2,

$$dim(\mathcal{L}(A_+)) = dim(\mathcal{L}(A_+)/\mathcal{L}(0)) + 1.\blacksquare$$

Definición 12 *Dado $A \in Div(\mathbb{F})$, al entero $l(A) := dim(\mathcal{L}(A))$ le llamaremos* ***la dimensión de el divisor*** *A.*

Teorema 2.1.5 *Todo divisor principal tiene grado cero. Sea $x \in \mathbb{F}/\mathbb{K}$ y denotemos por $(x)_0$ y $(x)_\infty$ el divisor de ceros y el divisor de polos de x respectivamente. Entonces*

$$grado((x)_0) = grado((x)_\infty) = [\mathbb{F} : \mathbb{K}(x)].$$

Demostración. Sean $n = [\mathbb{F} : \mathbb{K}(x)]$ y

$$B := (x)_\infty = \sum_{i=1}^{r} -v_{P_i}(x)P_i,$$

donde $P_1, \ldots, P_r$ son los polos de x. Entonces

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

por la Proposición 2.0.7. Por otro lado, podemos elegir una base $u_1, \ldots, u_n$ de $\mathbb{F}/\mathbb{K}(x)$ y un divisor $C \geq 0$ tales que $(u_i) \geq -C$ para $i = 1, \ldots, n$. Entonces

$$l(lB + C) \geq n(l + 1) \text{ para toda } l \geq 0, \tag{2.7}$$

pues $x^i u_j \in \mathcal{L}(lB + C)$ para $0 \leq i \leq l$, $1 \leq j \leq n$. Estos elementos son linealmente independientes sobre $\mathbb{K}$ ya que $u_1, \ldots, u_n$ son linealmente independientes sobre $\mathbb{K}(x)$. Sea $c := grado(C)$ se sigue que $n(l+1) \leq l(lB+C) \leq l \cdot grado(B) + c + 1$ por la Proposición 2.1.4. Entonces para toda $l \in \mathbb{N}$

$$l(grado(B) - n) \geq n - c - 1 \tag{2.8}$$

El lado derecho de 2.8 es independiente de l, de ahí que la desigualdad 2.8 solo es posible si $grado(B) \geq n$. Por lo tanto

$$grado(x)_\infty = [\mathbb{F} : \mathbb{K}(x)].$$

Como $(x)_0 = (x^{-1})_\infty$ entonces

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

Corolario 2.1.6 *(a) Sean $A, A' \in Div(\mathbb{F})$ dos divisores equivalentes. Entonces $l(A) = l(A')$ y $grado(A) = grado(A')$.*

(b) Si $grado(A) < 0$ entonces $l(A) = 0$

(c) Sea A un divisor de grado cero. Las siguientes afirmaciones son equivalentes

(1) A es principal.

(2) $l(A) \geq 1$.

(3) $l(A) = 1$

Demostración. (a) y (b) se siguen de los Lemas 2.1.1 y 2.1.2 respectivamente.

(c) (1) implica (2): Si $A = (x)$ entonces $x^{-1} \in \mathcal{L}(A)$, se sigue que $l(A) \geq 1$.

(2) implica (3): Si $l(A) \geq 1$ y $grado(A) = 0$ entonces $A \sim A'$ para algún divisor $A' \geq 0$, entonces, como $grado(A') = 0$ y $A' \geq 0$ tenemos que $A' = 0$, y así $l(A) = l(A') = l(0) = 1$.

(3) implica (1): Supongamos que $l(A) = 1$ y que $grado(A) = 0$. Sea $0 \neq z \in \mathcal{L}(A)$, entonces $(z) + A \geq 0$. Como $grado((z) + A) = 0$ se sigue que $(z) + A = 0$, por lo tanto $A = -(z) = (z^{-1})$ es un divisor principal.$\blacksquare$

Proposición 2.1.7 *Existe una constante $\gamma \in \mathbb{Z}$ tal que, para todo divisor $A \in Div(\mathbb{F})$, se tiene que*

$$grado(A) - l(A) \leq \gamma.$$

El énfasis en esta Proposición es que la constante γ no depende de A; solo depende de el campo de funciones $\mathbb{F}/\mathbb{K}$.

Demostración. Por el Lema 2.1.3

$$A_1 \leq A_2 \Rightarrow grado(A_1) - l(A_1) \leq grado(A_2) - l(A_2). \tag{2.9}$$

Fijamos un elemento $x \in \mathbb{F}$ y consideremos específicamente el divisor $B := (x)_\infty$. Como en la demostración del Teorema 2.1.5, existe un divisor $C \geq 0$ (que depende de x) tal que

$$l(lB + C) \geq (l+1)grado(B)$$

para toda $l \geq 0$ (ver ecuación 2.7). Por otro lado,

$$l(lB + C) \leq l(lB) + grado(C)$$

por el Lema 2.1.3. Combinando estas desigualdades obtenemos que

$$l(lB) \geq (l+1)grado(B) - grado(C)$$

$$= grado(lB) + ([\mathbb{F} : \mathbb{K}(x)] - grado(C)).$$

Por lo tanto

$$grado(lB) - l(lB) \leq \gamma \text{ para toda } l \geq 0 \tag{2.10}$$

con $\gamma \in \mathbb{Z}$. Queremos demostrar que 2.10 se satisface aún cuando sustituimos lB por cualquier divisor $A \in Div(\mathbb{F})$ (con la misma γ).

Afirmación. Dado un divisor A, existen divisores A_1, D y un entero $l \geq 0$ tal que $A \leq A_1, A_1$ D y $D \leq lB$.

Usando esta afirmación, demostramos la Proposición 2.1.7 de la siguiente manera:

$$\begin{array}{rcll} grado(A) - l(A) & \leq & grado(A_1) - l(A_1) & \text{por 2.9} \\ & = & grado(D) - l(D) & \text{por el Corolario 2.1.6} \\ & \leq & grado(lB) - l(lB) & \text{por 2.9} \\ & \leq & \gamma & \text{por 2.10.} \end{array}$$

Demostración de la afirmación. Sea $A_1 \geq A$ tal que $A_1 \geq 0$. Entonces

$$\begin{array}{rcll} l(lB - A_1) & \geq & l(lB) - grado(A_1) & \text{por el Lema 2.1.3} \\ & \geq & grado(lB) - \gamma - grado(A_1) & \text{por 2.10} \\ & > & 0 & \end{array}$$

para una l suficientemente grande. Entonces existe un elemento $0 \neq z \in \mathcal{L}(lB - A_1)$. Haciendo $D := A_1 - (z)$ obtenemos A_1 es equivalente a D y $D \leq A_1 - (A_1 - lB) = lB$ como queriamos.■

Definición 13 *El **género** g of $\mathbb{F}/\mathbb{K}$ está definido como*

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

Notemos que si $A = 0$ entonces

$$grado(0) - l(0) + 1 = 0 - 1 + 1 = 0$$

por lo tanto $g \geq 0$.

Teorema 2.1.8 (Teorema de Riemann) *Sea $\mathbb{F}/\mathbb{K}$ un campo de funciones de género g.*

(a) Para todo divisor $A \in Div(\mathbb{F})$,

$$l(A) \geq grado(A) + 1 - g.$$

(b) Existe un entero c, que depende de $\mathbb{F}/\mathbb{K}$, tal que

$$l(A) = grado(A) + 1 - g$$

si $gradoA \geq c$.

Demostración. (a) se sigue de la definición del género.

(b) Sea $A_0 \in Div(\mathbb{F})$ tal que $g = grado(A_0) - l(A_0) + 1$ y sea $c := grado(A_0) + g$. Si $grado(A) \geq c$ entonces

$$l(A - A_0) \geq grado(A - A_0) + 1 - g \geq c - grado(A_0) + 1 - g \geq 1.$$

Entonce existe un elemento $0 \neq z \in \mathcal{L}(A - A_0)$. Consideremos el divisor $A' := A + (z) \geq A_0$. Tenemos que

$$\begin{array}{rcll} grado(A) - l(A) & = & grado(A') - l(A') & \text{por el Corolario 2.1.6} \\ & \geq & grado(A_0) - l(A_0) & \text{por el Lema 2.1.3} \\ & = & g - 1. & \end{array}$$

Entonces $l(A) \leq grado(A) + 1 - g$.■

Calcular el género de un campo de funciones no es trivial. Pero podemos demostrar que el campo de funciones racionales $\mathbb{K}(x)$ tiene género cero: sea P_∞ el divisor de polos de x. Consideremos, para $r \geq 0$ el espacio vectorial $\mathcal{L}(rP_\infty)$. Tenemos que las funciones $1, x, \ldots, x^r$ pertenecen a $\mathcal{L}(rP_\infty)$ entonces

$$r + 1 \leq l(P_\infty) = grado(P_\infty) + 1 - g = r + 1 - g$$

para r suficientemente grande. Entonces $g \leq 0$. Pero $g \geq 0$ para todo campo de funciones, entonces $g = 0$ para $\mathbb{K}(x)$.

2.2. El Teorema de Riemann-Roch

En esta sección $\mathbb{F}/\mathbb{K}$ denota un campo de funciones algebraico de género g.

Definición 14 *Para $A \in Div(\mathbb{F})$ definimos el **índice de especialidad** de A como el entero*

$$i(A) := l(A) - grado(A) + g - 1.$$

Por el Teorema de Riemann, $i(A)$ es un entero no negativo, y $i(A) = 0$ si $grado(A)$ es suficientemente grande.

En esta sección interpretaremos el entero $i(A)$ como la dimensión of ciertos espacios vectoriales. El concepto de **adele** será fundamental para este propósito.

Definición 15 *Un **adele** de $\mathbb{F}/\mathbb{K}$ es un mapeo*

$$\alpha : \begin{cases} \mathbb{P}_\mathbb{F} & \to & \mathbb{F}, \\ P & \mapsto & \alpha_P, \end{cases}$$

tal que $\alpha_P \in \mathcal{O}_P$ excepto en un número finito de lugares$P \in \mathbb{P}_\mathbb{F}$. Consideraremos a los adeles como elementos del producto directo $\prod_{P \in \mathbb{P}_\mathbb{F}} F$. Usaremos la notación $\alpha = (\alpha_P)$.

La suma de adeles (coordenada a coordenada) es cerrada, y la multiplicación de un adele por un elemento de $\mathbb{K}$ es un adele. Así que al conjunto

$$\mathcal{A}_\mathbb{F} := \{\alpha | \alpha \text{ es un adele de } \mathbb{F}/\mathbb{K}\}$$

le llamaremos el **espacio de adeles** de $\mathbb{F}/\mathbb{K}$.

El **adele principal** de un elemento $x \in \mathbb{F}$ es el adele cuyas componentes son todas iguales a x. Esta última definición tiene sentido pues toda $x \in \mathbb{F}$ tiene un número finito de ceros y polos. De esta manera obtenemos una inmersión natural de $\mathbb{F}$ en $\mathcal{A}_{\mathbb{F}}$, que llamaremos la **inmersión diagonal**.

Las valoraciones v_P de $\mathbb{F}/\mathbb{K}$ se extienden de manera natural a $\mathcal{A}_{\mathbb{F}}$ como

$$v_P(\alpha) := v_P(\alpha_P),$$

aquí α_P es la P-componente de el adele α. Entonces, por definición de α, $v_P(\alpha) \geq 0$ excepto en un número finito de lugares.

Definición 16 *Dado $A \in Div(\mathbb{F})$ definimos*

$$\mathcal{A}_{\mathbb{F}}(A) := \{\alpha \in \mathcal{A}_{\mathbb{F}} | v_P(\alpha) \geq -v_P(A) \text{ para todo } P \in \mathbb{P}_{\mathbb{F}}\}$$

Este es un $\mathbb{K}$-subespacio vectorial de $\mathcal{A}_{\mathbb{F}}$. Conforme A recorre el conjunto ordenado $Div(\mathbb{F})$ los $\mathcal{A}_{\mathbb{F}}(A)$ forman una familia creciente de subespacios de $\mathcal{A}_{\mathbb{F}}$ cuya unión es $\mathcal{A}_{\mathbb{F}}$.

Lema 2.2.1 *Sean $A_1, A_2 \in Div(\mathbb{F})$ con $A_1 \leq A_2$. Entonces $\mathcal{A}_{\mathbb{F}}(A_1) \subseteq \mathcal{A}_{\mathbb{F}}(A_2)$ y*

$$dim(\mathcal{A}_{\mathbb{F}}(A_2)/\mathcal{A}_{\mathbb{F}}(A_1)) = grado(A_2) - grado(A_1). \tag{2.11}$$

Demostración: Para demostrar 2.11 hacemos inducción en

$$grado(A_2) - grado(A_1).$$

Si $grado(A_2) - grado(A_1) = 0$ entonces $A_2 = A_1$ y

$$dim(\mathcal{A}_{\mathbb{F}}(A_2)/\mathcal{A}_{\mathbb{F}}(A_1)) = 0.$$

Es suficiente entonces con demostrar 2.11 en el caso $A_2 = A_1 + P$ con $P \in \mathbb{P}_{\mathbb{F}}$. Sea $t \in \mathbb{J}$ tal que $v_P(t) = v_P(A_1) + 1$ y consideremos el mapeo lineal sobre $\mathbb{K}$ $\varphi :\longrightarrow \mathbb{F}_P$ dado por $\varphi(\alpha) := (t\alpha_P)(P)$. φ es sobre y $ker(\varphi) = \mathcal{A}_{\mathbb{F}}(A_1)$. Se sigue que

$$grado(A_2) - grado(A_1) = grado(P) = dim(\mathcal{A}_{\mathbb{F}}(A_2)/\mathcal{A}_{\mathbb{F}}(A_1)).\blacksquare$$

La sucesión

$$\begin{array}{rcl} 0 \to \mathcal{L}(A_2)/\mathcal{L}(A_1) & \to & \mathcal{A}_{\mathbb{F}}(A_2)/\mathcal{A}_{\mathbb{F}}(A_1) \\ & \to & (\mathcal{A}_{\mathbb{F}}(A_2) + \mathbb{F})/(\mathcal{A}_{\mathbb{F}}(A_1) + \mathbb{F}) \to 0 \end{array} \tag{2.12}$$

es exacta por lo que

$$\begin{array}{rcl} dim((\mathcal{A}_{\mathbb{F}}(\ \ A_2\ \ ) + \mathbb{F})/(\mathcal{A}_{\mathbb{F}}(A_1) + \mathbb{F})) & & \\ = & dim(\mathcal{A}_{\mathbb{F}}(A_2)/\mathcal{A}_{\mathbb{F}}(A_1)) - dim(\mathcal{L}(A_2)/\mathcal{L}(A_1)) & \\ = & (grado(A_2) - grado(A_1)) - (l(A_2) - l(A_1)). & \end{array}$$

Ahora supongamos que $B \in Div(\mathbb{F})$ es tal que $l(B) = grado(B) + 1 - g$. Si $B_1 \geq B$ entonces

$$l(B_1) \leq grado(B_1) + l(B) - grado(B) = grado(B_1) + 1 - g.$$

por el Lema 2.1.3. El Teorema 2.1.8 dice que

$$l(B_1) \geq grado(B_1) + 1 - g$$

por lo que

$$l(B_1) = grado(B_1) + 1 - g \text{ para todo } B_1 \geq B. \tag{2.13}$$

Dado $\alpha \in \mathcal{A}_{\mathbb{F}}$ podemos encontrar $B_1 \geq B$ tal que $\alpha \in \mathcal{A}_{\mathbb{F}}(B_1)$. Por 2.12 y por 2.13 tenemos que

$$\begin{array}{rcl} dim((\mathcal{A}_{\mathbb{F}}(B_1) + \mathbb{F}) & / & ((\mathcal{A}_{\mathbb{F}}(B) + \mathbb{F}) \\ & = & (grado(B_1) - l(B_1)) - (grado(B) - l(B)) \\ & = & (g-1) - (g-1) = 0. \end{array}$$

Es decir, $\mathcal{A}_{\mathbb{F}}(B1) + \mathbb{F} = \mathcal{A}_{\mathbb{F}}(B) + \mathbb{F}$. Como $\alpha \in \mathcal{A}_{\mathbb{F}}(B_1)$ tenemos que

$$\mathcal{A}_{\mathbb{F}} = \mathcal{A}_{\mathbb{F}}(B) + \mathbb{F}. \tag{2.14}$$

Llegamos a la primera interpretación de el índice de especialidad de un divisor:

Teorema 2.2.2 *Para cualquier divisor $A \in Div(\mathbb{F})$, el índice de especialidad es*

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

Demostración: Sea $A \in Div(\mathbb{F})$. Por el Teorema 2.1.8 existe un divisor $A_1 \geq A$ tal que $l(A_1) = grado(A_1) + 1 - g$. Por 2.14 tenemos que $\mathcal{A}_{\mathbb{F}} = \mathcal{A}_{\mathbb{F}}(A_1) + \mathbb{F}$ y 2.12 implica que

$$\begin{array}{rcl} dim(\mathcal{A}_{\mathbb{F}}/(\mathcal{A}_{\mathbb{F}}(A) + \mathbb{F})) & = & dim((\mathcal{A}_{\mathbb{F}}(A_1) + \mathbb{F})/(\mathcal{A}_{\mathbb{F}}(A) + \mathbb{F})) \\ & = & (grado(A_1) - l(A_1)) - (grado(A) - l(A)) \\ & = & g - 1 - l(A) - grado(A) = i(A). \blacksquare \end{array}$$

Como Corolario, obtenemos

Corolario 2.2.3 *g=dim((*$\mathcal{A}_{\mathbb{F}}$*/(*$\mathcal{A}_{\mathbb{F}}$*(0) +*$\mathbb{F}$*)).*

Demostración. $i(0) = l(0) - grado(0) + g - 1 = 1 - 0 + g - 1 = g$.■

Resulta útil pensar en el espacio dual de $\mathcal{A}_{\mathbb{F}}/(\mathcal{A}_{\mathbb{F}}(A) + \mathbb{F})$, es decir, en el espacio de funcionales lineales $(\mathcal{A}_{\mathbb{F}}/(\mathcal{A}_{\mathbb{F}}(A)+\mathbb{F}))^*$. El concepto de **diferencial de Weil** es fundamental para una segunda interpretación de el índice de especialidad de un divisor.

Definición 17 *Un* ***diferencial de Weil*** *de* $\mathbb{F}/\mathbb{K}$ *es un mapeo* $\mathbb{K}$*-lineal* $\omega : \mathcal{A}_{\mathbb{F}} \to \mathbb{K}$ *que se anula en* $\mathcal{A}_{\mathbb{F}}(A) + \mathbb{F}$ *para algún divisor* $A \in Div(\mathbb{F})$*. Llamaremos al conjunto*

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

el ***módulo de diferenciales de Weil*** *de* $\mathbb{F}/\mathbb{K}$*. Sea* $A \in Div(\mathbb{F})$*, definimos*

$$\Omega_F(A) := \{\omega \in \Omega_F | \omega \text{ se anula en } \mathcal{A}_{\mathbb{F}}(A) + \mathbb{F}\}.$$

Tenemos que Ω_F es un espacio vectorial sobre$\mathbb{K}$, de hecho, si ω_1 se anula en $\mathcal{A}_{\mathbb{F}}(A_1) + \mathbb{F}$ y ω_2 se anula en $\mathcal{A}_{\mathbb{F}}(A_2) + \mathbb{F}$ entonces $\omega_1 + \omega_2$ se anula en $\mathcal{A}_{\mathbb{F}}(A_3) + \mathbb{F}$ para todo divisor A_3 tal que $A_3 \leq A_1$ y $A_3 \leq A_2$, y $a\omega_1$ se anula en $\mathcal{A}_{\mathbb{F}}(A_1) + \mathbb{F}$ para $a \in \mathbb{K}$. Se sigue tambien que $\Omega_F(A)$ es un subespacio de Ω_F.

Lema 2.2.4 *Para todo* $A \in Div(\mathbb{F})$ *tenemos que* $dim(\Omega_F(A)) = i(A)$*.*

Demostración. El espacio $\Omega_F(A)$ Es isomorfo el spacio de formas lineales en $\mathcal{A}_{\mathbb{F}}/\mathcal{A}_{\mathbb{F}}(A)+\mathbb{F}$. El Lema se sigue pues la dimensión de $\mathcal{A}_{\mathbb{F}}/\mathcal{A}_{\mathbb{F}}(A)+\mathbb{F}$ es finita e igual a $i(A)$.■

Del Lema anterior podemos ver que $\Omega_F \neq \emptyset$ tomando un divisor $A \in Div(\mathbb{F})$ con $grado(A) \leq -2$. Entonces $dim(\Omega_F) = i(A) = l(A) - grado(A) + g - 1 \geq 1$, entonces $\Omega_F \neq \emptyset$.

De esto ùltimo se sigue que $\Omega_F \neq 0$ tomando un divisor $A \in Div(\mathbb{F})$ tal que $grado(A) \leq -2$. Entonces $dim(\Omega_F) = i(A) = l(A) - grado(A) + g - 1 \geq 1$, por lo que $\Omega_F \neq 0$.

Definición 18 *Para cada* $x \in \mathbb{F}$ *y* $\omega \in \Omega_F$ *definimos* $x\omega : \mathcal{A}_{\mathbb{F}} \to \mathbb{K}$ *como*

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

Si ω se anula en $\mathcal{A}_{\mathbb{F}}(A) + \mathbb{F}$ entonces $x\omega$ se anula en $\mathcal{A}_{\mathbb{F}}(A + (x)) + \mathbb{F}$. Esta definición le da a Ω_F la estructura de espacio vectorial sobre $\mathbb{F}$.

Proposición 2.2.5 *Ω_F es un espacio vectorial de dimensión uno sobre $\mathbb{F}$.*

Demostración. Sea $\omega_1 \in \Omega_F - \{0\}$. Tenemos que demostrar que para cada $\omega_2 \in \Omega_F$ existe $z \in \mathbb{F}$ tal que $\omega_2 = z\omega_1$. Supongamos que $\omega_2 \neq 0$ (si $\omega_2 = 0$ entonces $z = 0$). Y sean $A_1, A_2 \in Div(\mathbb{F})$ tales que $\omega_1 \in \Omega_F(A_1)$ y $\omega_2 \in \Omega_F(A_2)$.

Sea $B \in Div(\mathbb{F})$, $B \geq 0$, de grado suficientemente grande para que $l(A_i + B) = grado(A_i+B)+1-g$ para $i = 1, 2$ (esto es posible por el Teorema 2.1.8). Definimos los mapeos $\varphi_i : \mathcal{L}(A_i + B) \longrightarrow \Omega_F(-B)$ como $\varphi_i(x) := x\omega_i$. Estos mapeos son lineales (sobre $\mathbb{K}$) e inyectivos. Definimos $U_i = \varphi_i(\mathcal{L}(A_i + B)) \leq \Omega_F(-B)$.

Como

$$dim(\Omega_F(-B)) = i(-B) = 0 - grado(-B) + g - 1 = grado(B) + g - 1$$

tenemos que

$$dim(U_1) + dim(U_2) - dim(\Omega_F(-B)) =$$
$$grado(B) + (grado(A_1) + grado(A_2) + 3(1 - g)).$$

Observamos que el segundo sumando en el lado derecho de la ecuación anterior es independiente de B, por lo que $dim(U_1)+dim(U_2)-dim(\Omega_F(-B)) > 0$ si $grado(B)$ es lo suficientemente grande. Entonces

$$U_1 \cap U_2 = \varphi_1(\mathcal{L}(A_1 + B)) \cap \varphi_2(\mathcal{L}(A_2 + B)) \neq \{0\}.$$

Por lo que existen funciones $x_1 \in \mathcal{L}(A_1 + B)$ y $x_2 \in \mathcal{L}(A_2 + B)$ tales que $x_1\omega_1 = x_2\omega_2 \neq 0$ entonces $\omega_2 = x_1x_2^{-1}\omega_1$. Esto demuestra la Proposición.■

A cada diferencial de Weil le asociaremos un divisor como sigue: consideremos el conjunto

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

Lema 2.2.6 *Sea $0 \neq \omega \in \Omega_F$. Entonces existe un divisor, determinado de manera única, $W \in M(\omega)$ tal que $A \leq W$ para todo divisor $A \in M(\omega)$.*

Demostración. Por el Teorema de Riemann existe una constante c, que depende solo de $\mathbb{F}/\mathbb{K}$, tal que $i(A) = 0$ siempre que $grado(A) \geq c$. Como $dim(\mathcal{A}_{\mathbb{F}}/(\mathcal{A}_{\mathbb{F}}(A) + \mathbb{F})) = i(A)$ tenemos que $grado(A) < c$ para todo $A \in M(\omega)$. Así que podemos escoger $W \in M(\omega)$ de grado máximo.

Supongamos que exite un divisor $A_0 \in M(\omega)$ con $W < A_0$, *i.e.* $v_Q(A_0) > v_Q(W)$ para algún $Q \in \mathbb{P}_{\mathbb{F}}$. Demostraremos que

$$W + Q \in M(\omega). \tag{2.15}$$

Consideremos un adele $\alpha = (\alpha_P) \in \mathcal{A}_{\mathbb{F}}(W+Q)$. Lo escribimos como $\alpha = \alpha' + \alpha''$ con

$$\alpha' := \begin{cases} \alpha_P & \text{si} \quad P \neq Q, \\ 0 & \text{si} \quad P = Q, \end{cases} \text{ y } \alpha'' := \begin{cases} 0 & \text{si} \quad P \neq Q, \\ \alpha_P & \text{si} \quad P = Q \end{cases}$$

Entonces $\alpha' \in \mathcal{A}_{\mathbb{F}}(W)$ y $\alpha'' \in \mathcal{A}_{\mathbb{F}}(A_0)$, por lo tanto

$$\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0.$$

Se sigue que ω se anula en $\mathcal{A}_{\mathbb{F}}(W+Q)+\mathbb{F}$, con lo que queda demostrada 2.15. Se sigue tambien que tal divisor W es único.■

Lo anterior motiva la siguiente

Definición 19 *(a) El divisor (ω) de un diferencial de Weil $\omega \neq 0$ es el divisor de $\mathbb{F}/\mathbb{K}$ determinado de manera única que satisface*

1. *ω se anula en $\mathcal{A}_{\mathbb{F}}((\omega)) + \mathbb{F}$.*
2. *Si ω se anula en $\mathcal{A}_{\mathbb{F}}(A) + \mathbb{F}$ entonces $A \leq (\omega)$.*

(b) Dado $0 \neq \omega \in \Omega_F$ y $P \in \mathbb{P}_{\mathbb{F}}$ definimos $v_P(\omega) := v_p((\omega))$.

*(c) Decimos que un lugar P es un cero (resp. polo) si $v_P((\omega)) > 0$ (resp. $v_P((\omega)) < 0$). ω se dice que es **regular** en P si $v_P((\omega)) \geq 0$, ω se dice **regular** si es regular en todo $P \in \mathbb{P}_{\mathbb{F}}$.*

*(d) Se dice que un divisor W es **divisor canónico** de $\mathbb{F}/\mathbb{K}$ si $W = (\omega)$ para algún $\omega \in \Omega_F$.*

De la definición anterior podemos reescribir

$$\Omega_F(A) = \{\omega \in \Omega_F | \omega = 0 \text{ o } (\omega) \geq A\}$$

y, en particular que

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

Como ya sabíamos $dim(\Omega_F(0)) = g$.

Proposición 2.2.7 *(a) Dada $0 \neq x \in \mathbb{F}$ y $0 \neq \omega \in \Omega_F$ tenemos que $(x\omega) = (x) + (\omega)$.*

(b) Cualesquiera dos divisores canónicos de $\mathbb{F}/\mathbb{K}$ son equivalentes.

Demostración. (a) Si ω se anula en $\mathcal{A}_{\mathbb{F}}(A)+\mathbb{F}$ entonces $x\omega$ se anula en $\mathcal{A}_{\mathbb{F}}(A+(x))+\mathbb{F}$, por lo que $(\omega)+(x)\leq(x\omega)$, en particular $x\omega$ se anula en $\mathcal{A}_{\mathbb{F}}((\omega)+(x))+\mathbb{F}$ así que $(\omega)+(x)\leq(x\omega)$. De igual manera $(x\omega)+(x^{-1})\leq(x^{-1}x\omega)=(\omega)$, de lo que se sigue que

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

(b) Ya que Ω_F es un $\mathbb{F}$-espacio de dimensión uno cada $\omega\in\Omega_F$ se puede escribir como $\omega=f\omega_1$ para algún $\omega_1\in$
weild y $f\in\mathbb{F}$. Sean $W=(f\omega_1)=(\omega_1)+(f)$ y $W'=(g\omega_1)=(\omega_1)+(g)$ dos divisores canónicos. Vemos que ambos son claramente equivalentes a (ω_1).■

Este resultado nos dice que el conjunto de divisores canónicos de $\mathbb{F}/\mathbb{K}$ es una clase en el grupo de clases de divisores $C_{\mathbb{F}}$. A esta clase le llamaremos **la clase canónica** de $\mathbb{F}/\mathbb{K}$.

Teorema 2.2.8 *Sea A un divisor arbitrario y $W=(\omega)$ un divisor canónico de $\mathbb{F}/\mathbb{K}$. Entonces el mapeo*

$$\mu:\left\{\begin{array}{ccc}\mathcal{L}(W-A) & \to & \Omega_F(A),\\ x & \mapsto & x\omega\end{array}\right.$$

es un isomorfismo de espacios vectoriales sobre $\mathbb{K}$. En particular,

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

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

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

por lo que $x\omega\in\Omega_F(A)$. Entonces μ mapea $\mathcal{L}(W-A)$ en $\Omega_F(A)$. El mapeo μ es lineal e inyectivo. Queda demostrar que μ es sobre. Para demostrar esto, sea $\omega_1\in\Omega_F(A)$ un diferencial de Weil. Entonces $\omega_1=x\omega$ para $x\in\mathbb{F}$. Ya que $(x)+W=(x)+(\omega)=(x\omega)=(\omega_1)\geq A$ obtenemos que

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

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

Tenemos todas las herramientas para demostrar el siguiente

Teorema 2.2.9 (Riemann-Roch) *Sea W un divisor canónico de $\mathbb{F}/\mathbb{K}$. Entonces para todo $A\in Div(\mathbb{F})$,*

$$l(A)=grado(A)+1-g+l(W-A).\blacksquare$$

Corolario 2.2.10 *Para un divisor canónico W, tenemos que*

$$grado(W) = 2g - 2 \text{ y } l(W) = g.$$

Demostración. Para $0 = A \in Div(\mathbb{F})$ tenemos, por el teorema de Riemann-Roch que

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

Entonces $l(W) = g$. Para $A = W$ tenemos que

$$g = l(W) = grado(W) + 1 - g + l(W - W) = grado(W) + 2 - g.$$

Por lo tanto $grado(W) = 2g - 2$.■

La constante c en el teorema de Riemann se puede escoger igual a $2g-1$:

Teorema 2.2.11 *Si $A \in Div(\mathbb{F})$ tiene grado $\geq 2g-1$ entonces $i(A) = 0$* i.e.

$$l(A) = grado(A) + 1 - g.$$

Demostración. El teorema de Riemann-Roch dice que $l(A) = grado(A) + 1 - g + l(W - A)$ para un divisor canónico W de $\mathbb{F}/\mathbb{K}$. Pero $grado(W) = 2g - 2 < 2g - 1 = grado(A)$, por lo que $grado(W - A) < 0$ y entonces $l(W - A) = 0$.■

El teorema de Riemann-Roch caracteriza al género y a la clase canónica:

Teorema 2.2.12 *Supongamos que $g_0 \in \mathbb{Z}$ y $W_0 \in Div(\mathbb{F})$ satisfacen*

$$l(A) = grado(A) + 1 - g_0 + l(W_0 - A)$$

para todo divisor $A \in Div(\mathbb{F})$. Entonces $g_0 = g$ y el divisor W_0 es canónico.

Demostración. Tomando $A = 0$ y $A = W_0$ obtenemos, por hipótesis, que $l(W_0) = g_0$ y $grado(W_0) = 2g_0 - 2$ respectivamente. Sea A un divisor de $\mathbb{F}/\mathbb{K}$ con $grado(A) > max\{2g - 2, 2g_0 - 2\}$ entonces, por un lado $l(A) = grado(A) + 1 - g$, y por hipotesis $l(A) = grado(A) + 1 - g_0$. Entonces, $g = g_0$.

Ahora tomamos $A = W$. Entonces, por hipotesis, tenemos que $g = (2g - 2) + 1 - g + l(W_0 - W)$. Entonces $l(W_0 - W) = 1$. Como $grado(W_0 - W) = 0$ tenemos que el divisor$W_0 - W$ es principal. Y entonces W_0 W.■

Proposición 2.2.13 *Un divisor B es canónico si y sólo si $grado(B) = 2g-2$ y $l(B) \geq g$.*

Demostración. Supongamos que $grado(B) = 2g - 2$ y que $l(B) \geq g$ entonces, si W es un divisor canónico tenemos que

$$g \leq l(B) = grado(B) + 1 - g + l(W - B) = g - 1 + l(W - B).$$

Por lo tanto $l(W - B) \geq 1$. Como $grado(W - B) = 0$ se sigue que $B \sim W$ y entonces B es canónico.■

2.2.1. Teorema de Clifford, Weierstrass y criterio de Eisenstein

Para poder calcular el género un campo de funciones necesitamos tener cotas que nos permitan calcular la dimensión de un divisor por lo que enunciaremos y demostraremos un teorema importante dado por William Clifford.

Teorema 2.2.14 *(Clifford) Para todo* $A \in Div(\mathbb{F}/\mathbb{K})$ *con* $0 \leq grado(A) \leq 2g-2$ *tenemos que*

$$l(A) \leq 1 + \frac{1}{2} grado(A) \tag{2.16}$$

Nos ayudaremos del siguiente lema para poder demostrar el teorema anterior.

Lema 2.2.15 *Supongamos que* $A, B \in Div(\mathbb{F}/\mathbb{K})$, $l(A) > 0$ *y* $l(B) > 0$, *entonces:*

$$l(A) + l(B) \leq 1 + l(A+B) \tag{2.17}$$

Demostración.
Como $l(A) > 0$ y $l(B) > 0$ podemos encontrar $A_0, B_0 \geq 0$ tal que $A \sim A_0$ y $B \sim B_0$, entonces el conjunto:

$$X := \{D \in Div(\mathbb{F}/\mathbb{K}) \mid D \leq A_0, \mathcal{L}(D) = \mathcal{L}(A_0)\} \tag{2.18}$$

es no vacío ya que $A_0 \in X$. Como $grado(D) \geq 0$ para todo $D \in X$ existe un $D_0 \in X$ de grado mínimo y se sigue que:

$$l(D_0 - P) < l(D_0) \ \forall P \in \mathbb{P}_{\mathbb{F}} \tag{2.19}$$

Nosotros queremos demostrar

$$l(D_0) + l(B_0) \leq 1 + l(D_0 + B_0) \tag{2.20}$$

Por lo que se sigue inmediatamente que

$$l(A)+l(B) = l(A_0)+l(B_0) = l(D_0)+l(B_0) \leq 1+l(D_0+B_0) \leq 1+l(A_0+B_0) = 1+l(A+B) \tag{2.21}$$

Para probar 2.20 supongamos que $\mathbb{K}$ es un campo infinito y sea $Sup(B_0) = \{P_1, ..., P_r\}$, claramente tenemos que $\mathcal{L}(D_0 - P_i) \subsetneq \mathcal{L}(D_0)\ \forall i \leq r$, y como un espacio vectorial sobre un campo infinito no es la unión finita de subespacios propios, podemos encontrar un elemento:

$$x \in \mathcal{L}(D_0) \setminus \bigcup_{i=1}^{r} \mathcal{L}(D_0 - P_i) \tag{2.22}$$

Ahora consideremos el mapeo $\mathbb{K}$-lineal

$$\phi : \begin{cases} \mathcal{L}(B_0) \to & \mathcal{L}(D_0 + B_0)/\mathcal{L}(A_0) \\ x \quad \mapsto & xz \text{ mód } \mathcal{L}(A_0) \end{cases} \tag{2.23}$$

De 2.22 de sigue fácilmente que el núcleo de ϕ es $\mathbb{K}$ por lo que

$$l(B_0) - 1 \leq l(D_0 + B_0) - l(A_0) \tag{2.24}$$

Lo que prueba 2.20

Ahora demostraremos el **teorema de Clifford** 2.2.14 usando este lema. Demostración.

El caso en el que $l(A) = 0$ es trivial porque el grado de A es positivo o cero y menor que $2g - 2$ por lo que $0 \leq 1 + \frac{1}{2} grado(A)$.

Ahora si $l(W - A) = 0$ con W canónico tenemos que:

$$l(A) = grado(A)+1-g = 1+\frac{1}{2}grado(A)+\frac{1}{2}(grado(A)-2g) < 1+\frac{1}{2}grado(A) \tag{2.25}$$

como $grado(A) \leq 2g - 2$ solo queda considerar el caso en que $l(A) > 0$ y $l(W - A) > 0$ y usando 2.2.15 tenemos que

$$l(A) + l(W - A) \leq 1 + l(W) = 1 + g \tag{2.26}$$

por otro lado.

$$l(A) - l(W - A) = grado(A) + 1 - g \tag{2.27}$$

Si sumamos 2.26 y 2.27 con el teorema de Riemann-Roch obtenemos la desigualdad deseada ■

El siguiente corolario es consecuencia directa de Riemann-Roch

Corolario 2.2.16 *Si $A \in Div(\mathbb{F}/\mathbb{K})$ con $grado(A) \geq 2g - 1$ entonces:*

$$l(A) = grado(A) + 1 - g \tag{2.28}$$

Demostración. Por Riemann-Roch $l(A) = grado(A) + 1 - g + l(W - A)$ con W canónico, como $grado(A) \geq 2g-1$ y sabemos que $grado(W) = 2g-2$, tenemos que $W - A$ es un divisor de grado negativo, por lo que $l(W - A) = 0$ ■

Ahora definiremos lo que es el orden polar y salto de Weierstrass, que con el teorema de Clifford podremos establecer una cota para el género.

En diversos contextos, resulta interesante especificar funciones que tengan un único polo en algún lugar dado. Recordemos que si podemos controlar el número de polos de una función dada, automáticamente controlaremos el número de ceros de dicha función.

Definición 20 *Sea $P \in \mathbb{P}_{\mathbb{F}}$, decimos que $n > 0$ es un orden polar si existe un $z \in \mathbb{F}/\mathbb{K}$ tal que $(z)_\infty = nP$, de manera contraria diremos que n es un salto de Weierstrass*

La definición anterior se puede ver en términos del espacio $\mathcal{L}(iP)$

$$i \quad \text{es un salto para P} \Leftrightarrow \mathcal{L}((i-1)P) = \mathcal{L}(iP) \tag{2.29}$$

Proposición 2.2.17 *El conjunto de órdenes polares de de P denotado por $\mathbb{O}_P$ es un subsemigrupo de $< \mathbb{N}, + >$*

Demostración.

Sean $(w)_\infty = nP$ y $(z)_\infty = mP$ con $w, z \in \mathbb{F}/\mathbb{K}$ entonces tenemos que $(wz)_\infty = (n+m)P$ ■

La siguiente proposición nos dará una idea de como está conformado el semigrupo $\mathbb{O}_P$ de órdenes polares, el cual será muy útil al hacer más fácil la demostración de uno de los teoremas más importantes de este capítulo.

Proposición 2.2.18 *Sea $P \in \mathbb{P}_{\mathbb{F}}$, entonces para toda $n \geq 2g$ con g el género de $\mathbb{F}/\mathbb{K}$ existe un $x \in \mathbb{F}$ tal que $(x)_\infty = nP$*

Demostración.

Por el teorema 2.2.16 tenemos que $l((n-1)P) = (n-1)grado(P) + 1 - g$ y $l(nP) = ngrado(P) + 1 - g$ por lo que $\mathcal{L}((n-1)P) \subsetneq \mathcal{L}(nP)$, Por esto, todo $x \in \mathcal{L}(nP) \setminus \mathcal{L}((n-1)P)$ tiene un divisor de polos nP usando la definición

del espacio de Riemann de nP ■

Esto en otras palabras es que si $n \geq 2g$ entonces $n \in \mathbb{O}_P$ i.e. es orden polar

Teorema 2.2.19 *(Weierstrass) Supongamos que $\mathbb{F}/\mathbb{K}$ es de género $g > 0$ y P es un lugar de grado 1, entonces existen exactamente g saltos $i_1 < ... < i_g$ de P y tenemos que $i_1 = 1$ e $i_g \leq 2g - 1$*

Demostración.

Tenemos por Riemann-Roch que $l((2g-1)P) = (2g-1)+1-g = g$ queremos demostrar que hay g naturales i tal que $0 \leq i \leq 2g-1$ para los cuales $\mathcal{L}(iP) = \mathcal{L}((i+1)P)$, estos i son los g saltos de P que queremos demostrar que existen.
Consideremos la siguiente sucesión de espacios vectoriales.

$$\mathbb{K} = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq ... \subseteq \mathcal{L}((2g-1)P) \tag{2.30}$$

Donde $l(0) = 1$ y $l((2g-1)P) = g$ como vimos al principio de la demostración, observa que por la definición de salto y propiedades del espacio de Riemann de un divisor tenemos que

$$l(iP) \leq l((i-1)P) + 1 \quad \forall i \tag{2.31}$$

Por lo que en 2.30 tenemos $g-1$ números $1 \leq i \leq 2g-1$ con $\mathcal{L}((i-1)P) \subsetneq \mathcal{L}(iP)$ i.e. que no sucede que sean saltos, por lo que como son $2g-1$ elementos en la sucesión los restantes g son saltos.

Ahora, es fácil ver que 1 es un salto ya que si no lo fuera sucedería que $1 \in \mathbb{O}_P$ pero si esto sucediera, como $\mathbb{O}_P$ es un semigrupo, entonces con el 1 adentro significaría que no hay saltos lo cual es contradictorio porque $g > 0$ ■

2.3. Extensiones Algebraicas de $\mathbb{F}/\mathbb{K}$.

Definición 21 *(a) Un campo de funciones algebraicas $\mathbb{F}'/\mathbb{K}'$ se dice* extension algebraica *de $\mathbb{F}/\mathbb{K}$ si $\mathbb{F}' \supseteq \mathbb{F}$ es una estensión algebraica y $\mathbb{K}' \supseteq \mathbb{K}$.*

(b) La extensión $\mathbb{F}'/\mathbb{K}'$ *de* $\mathbb{F}/\mathbb{K}$ *se dice* extensión de constantes *si* $\mathbb{F}' = \mathbb{F}\mathbb{K}'$.

(c) $\mathbb{F}'/\mathbb{K}'$ *se dice* extensión finita *si* $[\mathbb{F}' : \mathbb{F}] < \infty$.

Si $\mathbb{F}'/\mathbb{K}'$ es una extensión algebraica de $\mathbb{F}/\mathbb{K}$ entonces la extensión $\mathbb{K}'/\mathbb{K}$ es algebraica y $\mathbb{K} = \mathbb{F} \cap \mathbb{K}'$. Tambien tenemos que $\mathbb{F}'/\mathbb{K}'$ es una extensión finita de $\mathbb{F}\mathbb{K}'/\mathbb{K}'$.

Por otro lado si $\mathbb{F}'/\mathbb{K}'$ es una extensión finita de $\mathbb{F}/\mathbb{K}$ entonces, considerando a $\mathbb{F}'$ como un campo de funciones algebraico sobre $\mathbb{K}$, tenemos que $\mathbb{K}'$ es el campo de constantes de $\mathbb{F}'/\mathbb{K}$, por lo que $[\mathbb{K}' : \mathbb{K}] < \infty$.

Ahor bien, supongamos que $[\mathbb{K}' : \mathbb{K}] < \infty$ y sea $x \in \mathbb{F} - \mathbb{K}$. Entonces x es trascendente sobre $\mathbb{K}'$ y $\mathbb{F}'/\mathbb{K}'(x)$ es una extensión finita por lo que

$$[\mathbb{K}'(x) : \mathbb{K}(x)] = [\mathbb{K}' : \mathbb{K}] < \infty$$

y entonces

$$[\mathbb{F}' : \mathbb{K}(x)] = [\mathbb{F}' : \mathbb{K}'(x)][\mathbb{K}'(x) : \mathbb{K}(x)] < \infty.$$

Como $\mathbb{K}(x) \subseteq \mathbb{F} \subseteq \mathbb{F}'$ tenemos que $[\mathbb{F}' : \mathbb{F}] < \infty$. En resumen, $\mathbb{F}'/\mathbb{K}'$ es una extensión algebraica finita de $\mathbb{F}/\mathbb{K}$ si y solo si $[\mathbb{K}' : \mathbb{K}] < \infty$.

Definición 22 *Consideremos una extensión algebraica* $\mathbb{F}'/\mathbb{K}'$ *de* $\mathbb{F}/\mathbb{K}$. *Un lugar* $P' \in \mathbb{P}_{\mathbb{F}'}$ *se dice que* ***está sobre*** $P \in \mathbb{P}_F$ *si* $P \subseteq P'$. *Tambien diremos que* P' *es una extensión de* P *o que* P *está debajo de* P', *y escribiremos* $P'|P$.

Proposición 2.3.1 *Sea* $\mathbb{F}'/\mathbb{K}'$ *una extensión algebraica de* $\mathbb{F}/\mathbb{K}$. *Supongamos que* $P \in \mathbb{P}_F$ *y que* $P` \in \mathbb{P}_{\mathbb{F}'}$, *sean* $\mathcal{O}_P \subseteq \mathbb{F}$ *y* $\mathcal{O}'_P \subseteq \mathbb{F}'$ *los anillos de valoración correspondientes,* v_P *and* $v_{P'}$ *las valoraciones dicretas correspondientes. Entonces las siguientes afirmaciones son equivalentes:*

1. $P'|P$.
2. $\mathcal{O}_P \subseteq \mathcal{O}'_P$.
3. *Existe un entero* $e \geq 1$ *tal que* $v_{P'}(x) = e \cdot v_P(x)$ *para toda* $x \in \mathbb{F}$. *Además, si* $P'|P$ *entonces* $P = P' \cap \mathbb{F}$ *y* $\mathcal{O}_P = \mathcal{O}'_P \cap \mathbb{F}$. *Es por esto último que a* P *se le llama la restricción de* P' *a* $\mathbb{F}$.

Demostración: El anillo $\mathbb{F} \cap \mathcal{O}'_P$ es un subanillo de $\mathbb{F}$ que contiene a $\mathcal{O}_P$. Entonces, como $\mathcal{O}_P$ es un subanillo maximal de $\mathbb{F}$, $\mathbb{F} \cap \mathcal{O}'_P = \mathcal{O}_P$ o bien $\mathbb{F} \cap \mathcal{O}'_P = \mathbb{F}$. Supongamos que esto último es lo que sucede. En particular $\mathbb{F} \subseteq \mathcal{O}'_P$. Sea $z \in \mathbb{F}' - \mathcal{O}'_P$. Como $\mathbb{F}'/\mathbb{F}$ es algebraica, tenemos que existe una ecuación no trivial

$$z^n + c_{n-1}z^{n-1} + \cdots + c_1 z + c_0 = 0 \tag{2.32}$$

con $c_i \in \mathbb{F}$. Tenemos entonces que $v_{P'}(z^n) = nv_{P'}(z) < 0$ pues $z \notin \mathcal{O}'_P$ y además

$$v_{P'}(z^n) < v_{P'}(c_i z^i) \text{ para } i = 0, 1, \ldots, n-1.$$

Por la desigualdad del triángulo estricta tenemos que

$$v_{P'}(z^n + c_{n-1}z^{n-1} + \cdots + c_1 z + c_0) = nv_{P'}(z) \neq v_{P'}(0).$$

Esta contradicción nos dice que $\mathcal{O}_P = \mathbb{F} \cap \mathcal{O}'_P$.

1) implica 2): supongamos que $P'|P$ y que $\mathcal{O}_P \not\subseteq \mathcal{O}'_P$. Entonces existe alguna función $u \in \mathbb{F}$ con $v_P(u) \geq 0$ y $v_{P'}(u) < 0$. Como $P \subseteq P'$ tenemos que $v_P(u) = 0$. Sea $t \in \mathbb{F}$ tal que $v_P(t) = 1$, y sea $r := v_{P'}(t)$. Como $P \subseteq P'$ tenemos que $r > 0$. Entonces

$$v_P(u^r t) = rv_P(u) + v_P(t) = 1,$$

Las dos ecuaciones anteriores dicen que $u^r t$ pertenece a P pero no pertence a P' lo que contradice la hipótesis $P \subseteq P'$.

2) implica 1): Supongamos ahora que $\mathcal{O}_P \subseteq \mathcal{O}'_P$ y sea $x \in P$, entonces $x^{-1} \notin \mathcal{O}_P$ por lo que $x^{-1} \notin \mathcal{O}'_P$ lo que implica que $(x^{-1})^{-1} = x \in P'$. Por lo tanto $P \subseteq P'$.

2) implica 3): Sea $u \in \mathbb{F}$ tal que $v_P(u) = 0$. Entonces $u, u^{-1} \in \mathcal{O}_P \subseteq \mathcal{O}'_P$ lo que implica que $v'_P(u) = 0$ (u es unidad). Sean $t \in \mathbb{F}$ tal que $v_P(t) = 1$ y $e := v'_P(t)$. Como $P \subseteq P'$ tenemos que $e \geq 1$. Sean $x \in \mathbb{F} - \{0\}$ y $r := v_P(x)$. Entonces $v_P(xt^{-r}) = 0$ y entonces

$$v'_P(x) = v'_P(xt^{-r}) + v'_P(t^r) = 0 + rv'_P(t) = ev_P(x).$$

3) implica 2): Sea $x \in \mathcal{O}_P$. Entonces $v_P(x) \geq 0$. Como $\mathcal{O}_P \subseteq \mathcal{O}'_P$, tenemos que $v'_P(x) = ev_P(x) \geq 0$ por lo que $x \in \mathcal{O}'_P$.

Sea $x \in P' \cap \mathbb{F}$. Tenemos entonces que $0 < v'_P(x) = ev_P(x)$ lo que implica que $v_P(x) > 0$.■

Una consecuencia importante de la Proposición anterior es que podemos inyectar de manera canónica el campo residual $\mathbb{F}_P$ en el campo residual $\mathbb{F}'_{P'}$ como sigue

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

Es decir podemos considerar a $\mathbb{F}_P$ como subcampo de $\mathbb{F}'_{P'}$. La proposición y la discusión anterior motiva la siguiente

Definición 23 *Sea $\mathbb{F}'/\mathbb{K}'$ una extensión algebraica de $\mathbb{F}/\mathbb{K}$, y sea $P' \in \mathbb{P}_{\mathbb{F}'}$ un lugar de $\mathbb{F}'/\mathbb{K}'$ sobre $P \in \mathbb{P}_F$.*

1. *Al entero* $e(P'|P) := e$ *con* $v_{P'}(x) = e \cdot v_P(x)$ *para toda* $x \in \mathbb{F}$ *se le llama el* **índice de ramificación** *de* P' *sobre* P. *Diremos que* $P'|P$ *es* ramificado *si* $e(P'|P) > 1$, *y* $P'|P$ *es* no ramificado *si* $e(P'|P) = 1$.

2. *A* $f(P'|P) := [\mathbb{F}'_{P'} : \mathbb{F}_P]$ *se le llama el* grado relativo *de* P' *sobre* P.

Ahora queremos investigar la existencia de extensiones de lugares en extensiones de campos de funciones. Sea pues $P \in \mathbb{P}'_{\mathbb{F}}$ donde $\mathbb{F}'/\mathbb{K}'$ es una extensión algebraica de $\mathbb{F}/\mathbb{K}$. Afirmamos que existe una función $0 \neq z \in \mathbb{F}$ tal que $v'_P(z) \neq 0$.

Supongamos que esta afirmación es falsa. Sea $t \in \mathbb{F}'$ con $v_{P'}(t) > 0$. Al ser t algebraico existe una ecuación de la forma

$$c_n t^n + c_{n-1} t^{n-1} + \cdots + c_t + c_0 = 0$$

con $c_i \in \mathbb{F}$, $c_0 \neq 0$ y $c_n \neq 0$. Por hipótesis tenemos que $v_{P'}(c_0) = 0$ y $v_{P'}(c_i t^i) = v_{P'}(c_i) + i v_{P'}(t) > 0$ para $i = 1, \ldots, n$. Esto último contradice la desigualdad del triángulo estricta.

La discusión anterior dice que $\mathcal{O} = \mathcal{O}'_P \cap \mathbb{F}$ es un anillo de valoración de $\mathbb{F}/\mathbb{K}$ y $P = P' \cap \mathbb{F}$ el lugar correspondiente. Es claro ahora que existe un único lugar $P \in \mathbb{P}_F$ tal que $P'|P$.

Ahora consideremos un lugar $P \in \mathbb{P}_F$. Sea $x \in \mathbb{F} - \mathbb{K}$ tal que P sea su único cero, es decir $v_P(x) > 0$. Entonces si $P'|P$ tenemos que $v'_P(x) = e(P'|P) v_P(x) > 0$ lo que dice que P' es un cero de x en $\mathbb{P}_{F'}$. Ahora supongamos que $v'_P(x) > 0$, y sea $Q = P' \cap \mathbb{F}$ el lugar que está debajo de P'. Entonces $v_Q(x) > 0$ lo que dice que Q es un cero de x y como x solo tiene a P como cero concluimos que $Q = P$.

En este contexto tenemos que

$$P'|P \text{ si y solo si } v_{P'}(x) > 0.$$

Teorema 2.3.2 *En una extensión finita* $\mathbb{F}'/\mathbb{K}'$ *de* $\mathbb{F}/\mathbb{K}$ *tenemos que*

1. $|\{P' \in \mathbb{P}_{F'} | P' \text{ está sobre } P\}| \leq [\mathbb{F}' : \mathbb{F}]$.

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

Demostración. [5] 3.1.11 y 3.1.12

La siguiente proposición nos permitirá saber si un polinomio con coeficientes en $\mathbb{F}$ es irreducible, lo cual es fundamental para poder estudiar mejor la estructura de la jacobiana del campo de funciones.

Proposición 2.3.3 *(Criterio de Eisenstein)*
Consideremos el campo de funciones $\mathbb{F}/\mathbb{K}$ y el polinomio

$$\phi(T) = a_n T^n + a_{n-1}T^{n-1} + ... + a_1 T + a^0 \tag{2.33}$$

Con $a_i \in \mathbb{F}$, y supongamos que existe un lugar $P \in \mathbb{P}_\mathbb{F}$ tal que alguna de las siguientes condiciones se satisface:

1. *$v_P(a_n) = 0$, $v_P(a_0) \geq v_P(a_i) > 0$ con $1 \leq i \leq n-1$ y $MCD(n, v_P(a_0)) = 1$*

2. *$v_P(a_n) = 0$, $v_P(a_i) \geq 0$ con $1 \leq i \leq n-1$, $v_P(a_0) < 0$ y $MCD(n, v_P(a_0)) = 1$*

Entonces $\phi(T)$ es irreducible en $\mathbb{F}[T]$.
Si $\mathbb{F}' = \mathbb{F}(y) = \mathbb{K}(x, y)$ con $\phi(y) = 0$, entonces P tiene una única extensión $P' \in \mathbb{P}_{\mathbb{F}'}$, $e(P' \mid P) = n$ y $f(P' \mid P) = 1$

Demostración.
Consideremos $\mathbb{F}' = \mathbb{F}(y)$ con $\phi(y) = 0$, tenemos que $[\mathbb{F}' : \mathbb{F}] = grado(\phi)$ si y sólo si $\phi(T)$ es irreducible. Sea P' alguna extensión de $P \in \mathbb{F}'$, entonces tenemos que:

$$-a_n y^n = a_0 + a_1 y + ... + a_{n-1} y^{n-1} \tag{2.34}$$

Supongamos que la primera condición (1) ocurre, entonces vemos que $v_{P'}(y) > 0$. sea $e := e(P' \mid P)$, entonces $v_{P'}(a_0) = e * v_P(a_0)$ y $v_{P'}(a_i y^i) = e * v_P(a_i) + i * v_{P'}(y) > e * v_P(a_0)$ para $1 \leq i \leq n-1$. Por la desigualdad del triángulo estricta en valoraciones tenemos que:

$$n * v_{P'}(y) = e * v_P(a_0) \tag{2.35}$$

Y como $MCD(n, v_P(a_0)) = 1$ tenemos que $n \mid e$ y entonces $n \leq e$. Ya habíamos visto que $n \geq [\mathbb{F}' : \mathbb{F}] \geq e$ por lo que:
$n = e = [\mathbb{F}' : \mathbb{F}]$.

Para la otra condición se sigue de manera similar.
■

Capítulo 3

Campos de funciones hiperelípticos

En este capítulo nos especializaremos en el estudio de campos de funciones hiperelípticos. Especificaremos elementos en su jacobiana usando parejas de polinomios. Esta representación nos permitirá realizar efectivamente las operaciones entre clases de divisores de grado cero.

Ahora veamos sobre campos de funciones no racionales los cuales serán muy relevantes para el fin de esta tesis

Definición 24 *Un campo de funciones $\mathbb{F}/\mathbb{K}$ es hiperelíptico si su género es $g \geq 2$ y contiene un subcampo racional $\mathbb{K}(x) \subseteq \mathbb{F}$ con $[\mathbb{F} : \mathbb{K}(x)] = 2$*

Lema 3.0.4

1. *Un campo de funciones $\mathbb{F}/\mathbb{K}$ de género $g \geq 2$ es hiperelíptico si y sólo si existe un divisor $A \in Div(\mathbb{F})$ con $grado(A) = 2$ y $l(A) \geq 2$*

2. *Todo $\mathbb{F}/\mathbb{K}$ de género 2 es hiperelíptico*

Demostración.
1) Supongamos que $\mathbb{F}/\mathbb{K}$ es hiperelíptico, escojamos un elemento $x \in \mathbb{F}$ tal que $[\mathbb{F} : \mathbb{K}(x)] = 2$ y consideremos su divisor de polos $A := (x)_\infty$. Tenemos que $grado(A) = 2$ por 2.1.5 y los elementos $1, x \in \mathcal{L}(A)$ son linealmente independientes sobre $\mathbb{K}$, por lo que $l(A) \geq 2$.
Ahora supongamos que $\mathbb{F}/\mathbb{K}$ tiene género $g \geq 2$ y que $A \in Div(\mathbb{F})$ es tal que $grado(A) = 2$ con $l(A) \geq 2$, entonces existe un divisor $A_1 \geq 0$ con $A_1 \sim A$, se sigue que $grado(A_1) = 2$, $l(A_1) \geq 2$ y tenemos que existe $x \in \mathcal{L}(A_1) \setminus \mathbb{K}$ y $(x)_\infty \leq A_1$ por lo que $[\mathbb{F} : \mathbb{K}(x)] = grado((x)_\infty) \leq 2$ por 2.1.5. Como $\mathbb{F}/\mathbb{K}$

no es racional, concluimos que $[\mathbb{F} : \mathbb{K}(x)] = 2$.

2) Si $\mathbb{F}/\mathbb{K}$ es de género 2, tenemos que si $W \in Div(\mathbb{F})$ es canónico, entonces $grado(W) = 2g - 2 = 2$ y $l(W) = g = 2$, lo que implica que $\mathbb{F}/\mathbb{K}$ es hiperelíptico ■

Ejemplo 3.0.5 *Sea* $\mathbb{F}(x, y)/\mathbb{K}(x)$ *tal que* $y^2 = x^m + ... + a_1x + a_0$ *con* $m > 2$ *impar, consideremos el polinomio* $T^2 + x^m + a_{m-1}x^{m-1} + ... + a_1x^1 + a_0 \in \mathbb{K}(x)[T]$ *y* $P_\infty = (x)_\infty$.

Por el criterio de Eisenstein el polinomio $T^2 - x^m - \cdots - a_1x - a_0 \in \mathbb{K}(x)[T]$ es irreducible y existe un único lugar Q_∞ encima de P_∞.
Por el mismo criterio tenemos que existe un único lugar $Q_\infty \in \mathbb{P}_\mathbb{F}$ tal que $e(Q_\infty \mid P_\infty) = 2$ por lo que $f(Q_\infty \mid P_\infty) = 1$ entonces $grado(Q_\infty) = 1$ en $\mathbb{F}/\mathbb{K}$, continuando con el ejemplo:

$$v_{Q_\infty}(y^2) = 2v_{Q_\infty}(y) = 2(-m) \tag{3.1}$$

Por lo que:

$$v_{Q_\infty}(y) = -m \tag{3.2}$$

De manera similar:

$$v_{Q_\infty}(x) = -2 \tag{3.3}$$

Por lo que:

$$(x)_\infty = 2Q_\infty \tag{3.4}$$

y

$$(y)_\infty = mQ_\infty \tag{3.5}$$

Tenemos entonces que 2 y m son órdenes polares de Q_∞ y como los órdenes polares forman un semigrupo por 2.2.17 entonces $2i$ es orden polar $\forall i \in \mathbb{N}$, así como todas las combinaciones lineales positivas de m y 2 son órdenes polares, por 2.2.19 1 es salto, ahora también tenemos que todo entero mayor que $2m - m - 2 = m - 2$ es una combinación positiva, pero como $2i$ es orden

polar y el salto más grande es menor o igual que $2m-m-2$ entonces existen a lo más $\frac{m-1}{2}$ saltos (porque la mitad son órdenes polares), por Weierstrass tenemos que:

$$g \leq \frac{m-1}{2} \tag{3.6}$$

ahora por otro lado:

Por el teorema de Clifford 2.2.14 tenemos que si consideramos la dimensión de $\mathcal{L}((m-1)Q_\infty)$

$$l((m-1)Q_\infty) \leq 1 + \frac{1}{2}grado((m-1)Q_\infty) = 1 + \frac{1}{2}(m-1) \tag{3.7}$$

Por otro lado tenemos el teorema de Riemann que nos dice que:

$$l((m-1)Q_\infty) \geq grado((m-1)Q_\infty) + 1 - g = m - 1 + 1 - g = m - g \tag{3.8}$$

Por lo que usando 3.7 y 3.8:

$$m - g \leq 1 + \frac{m-1}{2} \tag{3.9}$$

De esta última desigualdad tenemos que:

$$m - 1 + \frac{1-m}{2} \leq g \Rightarrow \frac{m-1}{2} \leq g \tag{3.10}$$

Por lo que usando 3.6 y 3.10 tenemos que:

$$g = \frac{m-1}{2} \tag{3.11}$$

3.1. Divisores reducidos

Para poder implementar la suma en $C^0_{\mathbb{F}}$ necesitamos representar sus elementos de una manera conveniente, el siguiente teorema es un paso importante en esa dirección el cual nos permitirá distinguir un representante para cada clase de equivalencia.

Teorema 3.1.1 *Dado un divisor $D \in Div(\mathbb{F}/\mathbb{K})$ con $grado(D) = 0$ existe un divisor de la forma $D' - rP$ con $D' \geq 0$ y $D \sim D'$, $grado(D') = r \leq g$ y $P \in \mathbb{P}_{\mathbb{F}'}$*

Demostración.

Sea $[D] \in {C_{\mathbb{F}}}^0$ una clase de divisores. Tenemos que $grado(D) = 0$. Sea $A := D + rP$ entonces $grado(A) = r \leq g$ y $l(A) \geq 1$.

Sea $f \in \mathcal{L}(A)$, recordemos que

$$\mathcal{L}(A) = \mathcal{L}(D + rP) := \{z \in \mathbb{F}/\mathbb{K} \mid (z) + D + rP \geq 0\} \tag{3.12}$$

Sea $D' := A + (f) = D + rP + (f) \geq 0$ por lo que $D' \sim A$ y claramente $r = grado(D') = grado(A) + grado(f) = grado(rP)$.

Con esto tenemos que $D' - rP = D + (f)$ por lo que $D \sim (D' - rP)$ y como $grado(D') = r \leq g$ esto reduce D a $D' - rP$■

El teorema anterior nos permitirá definir un representante de la clase $[D] \in {C_{\mathbb{F}}}^0$, a este divisor lo llamaremos **reducido**

La representación mencionada anteriormente es debido a Mumford.

En nuestro caso el cual es usando $\mathbb{F}_q(x, y)$ podemos tomar $P = Q_\infty$.

3.1.1. Representación con polinomios de clases de ${C_{\mathbb{F}}}^0$

Sean $\mathbb{F} = \mathbb{K}(x, y)/\mathbb{K}(x)$ un campo de funciones hiperelíptico, $[D] \in {C_{\mathbb{F}}}^0$, y $\tilde{D} := D' - rQ_\infty$ el divisor reducido en la clase de D. Supongamos que $SupD' = \{P_1, \ldots, P_s\}$ con $s \leq g$. Definimos $x_i := x(P_i) \in \mathcal{O}_{P_i}/P_i$, y de igual manera $y_i := y(P_i)$.

Definición 25 *El representante de la clase $[D] \in {C_{\mathbb{F}}}^0$ con $\mathbb{F} = \mathbb{K}(x, y)$ hiperelíptico de género g y $y^2 = f(x)$ lo representaremos por medio de $u(x), v(x) \in \mathbb{K}[x]$ tales que:*

- *$u(x)$ mónico*
- *$grad(v) < grad(u) \leq g$*
- *$u(x) \mid v(x)^2 - f(x)$*

Esta representación para el caso particular tratado en esta tesis que es con campos de funciones $\mathbb{F} = \mathbb{K}(x, y)$ hiperelípticos de género 2 con $y^2 = f(x)$ con $grado(f) = 2g + 1 = 5$ se puede reescribir como:

Definición 26 *Sea* $[D] \in {C_{\mathbb{F}}}^0$ *entonces representaremos de la clase* $[D]$ *como los polinomios* $u(x), v(x) \in \mathbb{K}[x]$ *tales que:*

- u *mónico*
- $u(x(P_i)) = 0$
- $v(x(P_i)) = y(P_i)$
- $grad(v) < grad(u) \leq 2$

Esta notación del representante de $[D]$ se le atribuye a Mumford [10] y es conveniente porque nos permite "recordar" los lugares en el soporte del representante de $[D]$ a través de las raíces de u y de evaluar v en $x(P_i)$, nos permitirá definir la operación en ${C_{\mathbb{F}}}^0$ de una manera más compacta. Para el caso particular de género 2 todo divisor estará dado por $\{u, v\}$ con $u(x) = x^2 + u_1 x + u_2$ y $v(x) = v_1 x + v_2$, con $u_i, v_i \in \mathbb{K}$ más adelante veremos un ejemplo de esto sobre $\mathbb{K} = \mathbb{Z}_{31}$ y $\mathbb{F} = \mathbb{K}(x, y)$ con $y^2 = x^5 - 1$.

Definición 27 *Los elementos de* ${C_{\mathbb{F}}}^0$ *están en correspondencia con los elementos del conjunto:*

$$\{< u, v >: u | v^2 - f\} \tag{3.13}$$

con u *mónico,* $g \geq grado(u) > grado(v)$

3.2. Implementación de adición usando divisores reducidos en ${C_{\mathbb{F}}}^0$

3.2.1. Idea general

Por el teorema 3.1.1 podemos encontrar representantes de divisores reducidos en ${C_{\mathbb{F}}}^0$. El algoritmo para operar con divisores reducidos en la forma de Mumford es el de **Cantor**[9], el cual opera en campos de funciones hiperelípticos de cualquier género, y hace operaciones sobre el anillo de polinomios para poder sumar dos elementos $< u_1, v_1 >$ y $< u_2, v_2 >$ de ${C_{\mathbb{F}}}^0$, ya que calcula el $d_1 = MCD(u_1, u_2)$ inicialmente, después $d = MCD(d_1, v_1 + v_2)$, para después hacer operaciones en el anillo de polinomios. Nuestro método opera

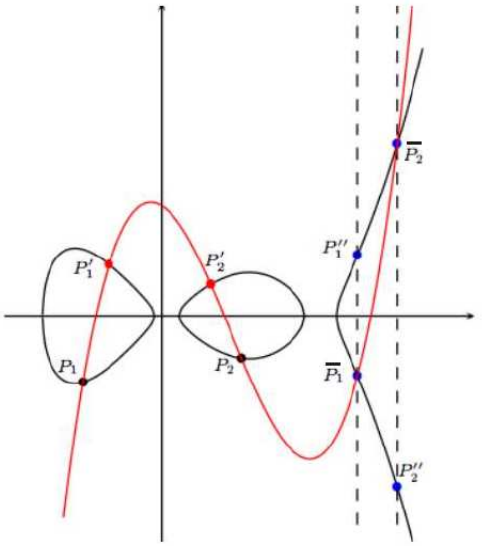

Figura 3.1:

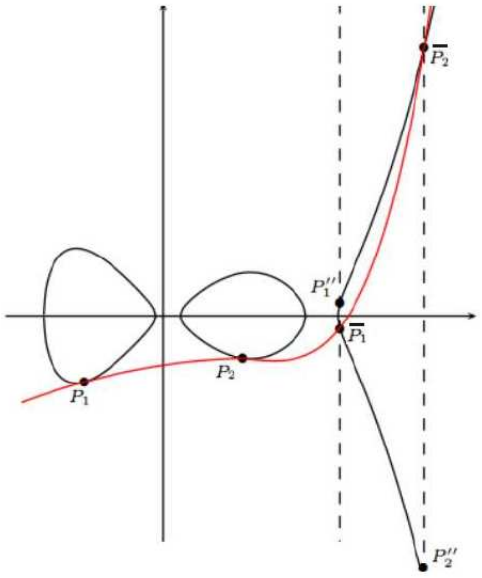

Figura 3.2:

sobre el campo base y ejemplificamos con género 2, esto intuitivamente para fines de mejor entendimiento podemos visualizarlo en $\mathbb{R}^2$. Vemos en este caso $y^2 - x^5 - 10x^4 + 9x^3 - 202x^2 - 8x + 192 \in \mathbb{R}[x, y]$, por lo que por 3.0.5 vemos que es de género 2 y denotaremos por Q_∞ al lugar infinito, tomaremos los P_i como lugares de grado 1, y $f \in \mathbb{R}[x, y]$ a la curva que intersecta la curva hiperelíptica (rojo), $v_{P_i}(f) = v_{P_i'}(f) = v_{P_i''}(f) = v_{\bar{P}_i}(f) = 1$, los divisores principales correspondientes dados por la parte punteada y la parte roja (A) son: (figura 3.1)

$A = P_1 + P_2 - 2Q_\infty \oplus P_1' + P_2' - 2Q_\infty \oplus \bar{P}_1 + \bar{P}_2 - 2Q_\infty$
$M = \bar{P}_1 + P_1'' - 2Q_\infty$
$N = \bar{P}_2 + P_2'' - 2Q_\infty$

Como estos divisores M y N son principales tenemos que:

$B = M + N = \bar{P}_1 + P_1'' - 2Q_\infty \oplus \bar{P}_2 + P_2'' - 2Q_\infty$

Como estamos trabajando en $C_{\mathbb{F}}{}^0$, y son principales tenemos que:

$A - B \sim 0 \Rightarrow$
$[P_1 + P_2 - 2Q_\infty] \oplus [P_1' + P_2' - 2Q_\infty] \ominus [P_1'' + P_2'' - 2Q_\infty] \sim 0 \Rightarrow$

$[P_1 + P_2 - 2Q_\infty] \oplus [P_1' + P_2' - 2Q_\infty] \sim [P_1'' + P_2'' - 2Q_\infty]$
Estos últimos divisores se pueden reducir usando 3.1.1.

Ahora del lado derecho de la figura podemos ver como calcular $2[D]$ con D divisor de manera similar, tenemos que la parte roja es una función f en $\mathbb{R}[x, y]$ y supongamos que $v_{\bar{P}_i}(f) = 1$, como tenemos que estamos trabajando en género 2 $v_{P_1}(f) = v_{P_2}(f) = 2$

Entonces:

$A = 2P_1 - 2Q_\infty \oplus 2P_2' - 2Q_\infty \oplus \bar{P}_1 + \bar{P}_2 - 2Q_\infty$
$M = \bar{P}_1 + P_1'' - 2Q_\infty$
$N = \bar{P}_2 + P_2'' - 2Q_\infty$

$$B = M + N = \bar{P}_1 + P_1'' - 2Q_\infty \oplus \bar{P}_2 + P_2'' - 2Q_\infty$$

Como estamos trabajando en ${C_\mathbb{F}}^0$, y son principales tenemos que:

$A - B \sim 0 \Rightarrow$
$[2P_1 - 2Q_\infty] \oplus [2P_2' - 2Q_\infty] \ominus [P_1'' + P_2'' - 2Q_\infty] \sim 0 \Rightarrow$
$[2P_1 - 2Q_\infty] \oplus [2P_2' - 2Q_\infty] \sim [P_1'' + P_2'' - 2Q_\infty]$

3.2.2. Adición explícita en ${C_\mathbb{F}}^0$ con divisores usando la representación de Mumford g=2

Aquí diviremos en dos partes, las cuales intuitivamente son como las dos figuras anteriores.

Sea $\mathbb{F}/\mathbb{K}$ con $\mathbb{F} = \mathbb{K}(x, y)$, tal que $y^2 = x^5 - 1$ y $\mathbb{K} = \mathbb{Z}_{31}$.

Caso 1: $[D_1] \oplus [D_2]$ con $Sop(D_1) \cap Sop(D_2) = \emptyset$

Dados dos divisores $D_1 = P_1 + P_2 - 2Q_\infty$ y $D_2 = P_1' + P_2' - 2Q_\infty$, queremos encontrar la clase de divisor $[P_1 + P_2 - 2Q_\infty] \oplus [P_1' + P_2' - 2Q_\infty]$, para encontrar éste, por el teorema de aproximación tenemos que existe una función $L \in \mathbb{K}(x, y)$, que tiene ceros a los lugares de grado 1 $P_1, P_2, P_1', P_2', \bar{P}_1, \bar{P}_2$, para esto hay que encontrar un polinomio de interpolación que pase por esos lugares, igualando con $y^2 = x^5 - 1$ y resolver para $\bar{P}_1, \bar{P}_2$ para finalizar con la involución hiperelíptica y encontrar $-[\bar{P}_1 + \bar{P}_2 - 2Q_\infty] = [P_1'' + P_2'' - 2Q_\infty]$.

Usando la notación de Mumford tenemos que si D es un divisor reducido como en el teorema 3.1.1, denotando a los lugares como $P = (x, y) \in Sop(D)$, entonces $D = (u, v)$ con $u(x) = 0$ y $v(x) = y$ para todo $P = (x, y) \in Sop(D)$ por lo que $grad(u) = 2$ y $grad(v) = 1$, esto fue para recordar, por lo que ahora para hacer la adición de ambos divisores tenemos:

$D_1 =< u = x^2 + ax + b, v = cx + d >$
$D_2 =< u' = x^2 + Ax + B, v' = Cx + D >$

Queremos encontrar $D_3 = (u'' = x^2 + \alpha x + \beta, v'' = \gamma x + \delta)$ que como en la figura anterior representaría que $P_1'', P_2'' \in Sop(D_3)$, el cual resulta de invertir $\bar{P}_1$ y $\bar{P}_2 \in Sop(L)$

Para encontrar los elementos restantes de $Sop(L)$ que son $\bar{P}_1$ y $\bar{P}_2$ basta encontrar el polinomio de interpolación para los lugares dados y luego ese polinomio de interpolación, elevarlo al cuadrado para igualarlo con $y^2 = x^5 - 1$:

Tenemos que:
$L(x) = px^3 + qx^2 + rx + s$

Queremos encontrar una función L tal que $v_P(L(x) - v(x)) > 0$ para $P \in Sop((u)_0)$ y $v_P(L(x) - v'(x)) > 0$ para $P \in Sop((u')_0)$ lo cual es equivalente:

$$L(x) - v(x) \equiv 0 \text{ mód } u(x)$$

$$L(x) - v'(x) \equiv 0 \text{ mód } u'(x)$$

notemos que esto es una aplicación del teorema de aproximación el cual nos garantiza la existencia de L
Como $grad(u) = grad(u') = 2$ tendremos las clases de residuos de la forma

$R_1x + R_2 \equiv 0$ mód $u(x)$
$R_3x + R_4 \equiv 0$ mód $u'(x)$

Por lo que $R_i = 0$ con lo que obtenemos un sistema de ecuaciones de 4x4 cuya solución son los coeficientes p, q, r, s de $L(x)$, si hacemos los cálculos reduciendo $L(x) - v(x)$ módulo $u(x)$ y $L(x) - v(x)$ módulo $u'(x)$ podemos

encontrar las $r_i = 0$ en términos de p, q, r y s .

$(px^3 + qx^2 + rx + s) - (cx + d) \equiv x(p(a^2 - b) - qa + r - c) + p(ab) - qb + s - d$ mód $x^2 + ax + b$

$(px^3 + qx^2 + rx + s) - (Cx + D) \equiv x(p(A^2 - B) - qA + R - C) + p(AB) - qB + s - D$ mód $x^2 + Ax + B$

Esto nos induce las 4 ecuaciones:

$R_1 = p(a^2 - b) - qa + r - c$
$R_2 = p(ab) - qb + s - d$
$R_3 = p(A^2 - B) - qA + R - C$
$R_4 = p(AB) - qB + s - D$

Como ya sabemos los valores a, b, c, d, A, B, C, D y queremos que $R_i = 0 \quad \forall 1 \leq i \leq 4$ para encontrar los coeficientes de $L(x)$ el sistema de ecuaciones queda así:

$$\left[\begin{array}{cccc|c} a^2 - b & -a & 1 & 0 & c \\ ab & -b & 0 & 1 & d \\ A^2 - B & -A & 1 & 0 & C \\ AB & -B & 0 & 1 & D \end{array}\right].$$

Las soluciones de esta matriz nos dan los coeficientes p, q, r, s de $L(x)$ por lo que al tenerlos ahora solo basta igualar con $y^2 = x^5 - 1$:

$\frac{L(x)^2 - x^5 + 1}{u(x)u'(x)} = u''(x)$

Esto sucede ya que $grad(L) = 6$ y tiene como factores a u y u' los cuales tienen como raíces a las coordenadas x de los lugares del $Sop(D_1)$ y $Sop(D_2)$ por lo que $u''(x)$ es el polinomio de grado 2 restante y éste tendrá como raíces a las coordenadas x del $Sop(D_3)$.

Para encontrar $v''(x)$ el cual $grad(v'') = 1$ bastaría con evaluar las raíces en $y^2 = x^5 - 1$ sobre $\mathbb{K}$ o fijarnos en que:

$L(x) \equiv -v''(x)$ mód $u''(x)$
Con lo que tendríamos listo al hacer la involución hiperelíptica $[D_1] \oplus [D_2] = [D_3] = (u''(x), v''(x))$.

Caso 2: 2[D]

Ahora sigue el caso de la figura anterior del lado derecho, queremos calcular $2[D] = [D] \oplus [D]$ en el cual buscaremos que si $D = P_1 + P_2 - 2Q_\infty$ deberá de ocurrir que los elementos no triviales del divisor principal (L) tengan multiplicidad 2, por lo que buscaremos como en la parte anterior construir un sistema de ecuaciones para poder encontrar $L \in \mathbb{K}(x, y)$ que tenga en los lugares P_1 y P_2 de su soporte $v_{P_1}(L) = v_{P_2}(L) = 2$ con v_{P_1}, v_{P_2} valoraciones de $\mathcal{O}_{P_1}, \mathcal{O}_{P_1} \subset \mathbb{K}(x, y)$ respectivamente.

Para esto vamos a considerar la derivada para poder encontrar las valoraciones deseadas.
Consideremos el divisor D en la forma de Mumford, esto es:
$D =< u(x) = x^2 + ax + b, v(x) = cx + d >$

También consideremos el polinomio cuyo divisor principal (L) tiene los elementos con multiplicidad 2 P_1 y P_2 $L(x) = Px^3 + Qx^2 + Rx + T$

Su derivada está dada por:

$L'(x) = 3Px^2 + 2Qx + R$

Por lo que igualaremos las derivadas de $y^2 - x^5 + 1$ y de $L(x)$ módulo $u(x) = x^2 + ax + b$ para obtener los coeficientes de L con multiplicidad 2:

$\frac{-5x^4}{2y} \equiv 3Px^2 + 2Qx + R$ mód $x^2 + ax + b$

Podemos usar $y = v(x)$ ya que $v(P_{1_x}) = y$ y $v(P_{2_x}) = y$ por como definimos v tenemos que:

$\frac{-5x^4}{2(cx+d)} \equiv 3Px^2 + 2Qx + R$ mód $x^2 + ax + b \quad \Rightarrow$

$2(cx + d)(3Px^2 + 2Qx + R) - 5x^4 \equiv R_1x + R_2$ mód $x^2 + ax + b$

El calcular esta operación nos dará los valores para R_1 y R_2:

$x(P(6a^2c - 6ad - 6bc) + Q(4d - 4ac) + R(2c) + 5a^3 - 10ab) + (P(6abc - 6bd) + Q(-4bc) + R(2d) + 5a^2b - 5b^2)$

Por lo que necesitamos que sean cero:

$R_1 = P(6a^2c - 6ad - 6bc) + Q(4d - 4ac) + R(2c) + 5a^3 - 10ab$
$R_2 = P(6abc - 6bd) + Q(-4bc) + R(2d) + 5a^2b - 5b^2$

Como en el caso anterior también hay que igualar con $y^2 = x^5 - 1$ módulo $u(x)\ L(x)^2 - x^5 + 1$, pero esto ya lo habíamos calculado por lo que:

$R_3 = P(a^2 - b) - Qa + R - c$
$R_4 = P(ab) - Qb + S - d$

Esto induce un sistema de ecuaciones, queremos encontrar los valores P, Q, R, S los cuales son los coeficientes de $L(x)$:

$$\left[\begin{array}{cccc|c} 6a^2c - 6ad - 6bc & -4ac + 4d & 2c & 0 & 10ab - 5a^3 \\ 6abc - 6bd & -4bc & 2d & 0 & 5b^2 - 5ba^2 \\ a^2 - b & -a & 1 & 0 & c \\ ab & -b & 0 & 1 & d \end{array}\right].$$

De manera similar ya con la solución de este sistema obtenemos los coeficientes de $L(x)$ por lo que ya estamos listos para calcular $2[D] = (u'(x), v'(x))$

Aquí como en el caso anterior al igualar con $y^2 = x^5 - 1$ y dividir por u^2 obtendremos los nuevos lugares, que en este caso son las raices de $u'(x)$.

$\frac{L(x)^2 - (x^5 - 1)}{u(x)^2} = u'(x)$

y
$\frac{L(x)}{u(x)} = -v'(x)$

Proyectamos y obtenemos:
$2[D] = (u'(x), v'(x))$

3.3. Ejemplo desarrollado $[D_1] \oplus [D_2]$

Supongamos que $\mathbb{K} = \mathbb{Z}_{31}$ y consideremos el campo de funciones hiperelíptico $\mathbb{F}/\mathbb{K}$ tal que $\mathbb{F} = \mathbb{K}(x, y)$ con $y^2 = x^5 - 1$.

Consideremos los divisores:

$[D_1] = (1, 0) + (6, 5) - 2\mathcal{Q}_\infty$
$[D_2] = (3, 5) + (4, 0) - 2\mathcal{Q}_\infty$

Vamos a calcular $[D_3] = [D_1] \oplus [D_2]$.

Tenemos que en notación de Mumford, estos divisores son:
$[D_1] =< u_1(x), v_1(x) >=< x^2 + 24x + 6, x + 30 >$
$[D_2] =< u_2(x), v_2(x) >=< x^2 + 24x + 12, 26x + 20 >$

Primero encontramos el polinomio de interpolación que pasa por los lugares del soporte de $[D_1]$ y $[D_2]$, el cual por el teorema de aproximación existe (En particular interpolación de Lagrange), este polinomio es de grado 3.

$L(x) = px^3 + qx^2 + rx + s$

Como vimos anteriormente, tenemos que las soluciones para los coeficientes de L están dados por:

$$\left[\begin{array}{cccc|c} a^2 - b & -a & 1 & 0 & c \\ ab & -b & 0 & 1 & d \\ A^2 - B & -A & 1 & 0 & C \\ AB & -B & 0 & 1 & D \end{array}\right].$$

Tal que:

$[D_1] =< u_1(x), v_1(x) >=< x^2 + ax + b, cx + d >$
$[D_2] =< u_2(x), v_2(x) >=< x^2 + Ax + B, Cx + D >$

Con $a, b, c, d, A, B, C, D \in \mathbb{Z}_{31}$, por lo que la matriz se ve como:

$$\left[\begin{array}{cccc|c} 12 & 7 & 1 & 0 & 1 \\ 20 & 25 & 0 & 1 & 30 \\ 6 & 7 & 1 & 0 & 26 \\ 9 & 19 & 0 & 1 & 20 \end{array}\right].$$

Si resolvemos esta matriz obtendríamos los valores de los coeficientes de L:

$p = 1$
$q = 5$

$r = 16$
$s = 9$

Por lo que $L(x) = x^3 + 5x^2 + 16x + 9$.

Ahora igualamos con $y^2 = x^5 - 1$ en $\mathbb{Z}_{31}[x]$, por lo que consideramos $L(x)^2 = x^5 - 1$ y como este polinomio cumple las 4 raíces de $u_1(x)$ y $u_2(x)$ ($L(x)$ fue construido con los lugares $[D_1]$ y $[D_2]$) y $L(x)^2 - x^5 + 1$ es de grado 6, las otras 2 raíces de $L(x)^2 - x^5 + 1$ definirán $u_3(x)$ tal que $[D_3] =< u_3(x), v_3(x) >$ ya que $u_1(x) \mid L(x)^2 - x^5 + 1$ y $u_2(x) \mid L(x)^2 + x^5 + 1$ por lo que:

$u_3(x) = \frac{L(x)^2 - x^5 + 1}{u_1(x)u_2(x)} = \frac{(x^3+5x^2+16x+9)^2 - x^5 + 1}{(x^2+24x+6)(x^2+24x+12)} = x^2 + 23x + 2$

Sólo basta calcular $v_3(x)$ el cual se obtiene calculando:

$L(x) \equiv -v_3(x)$ mód $u_3(x)$

Esto es:
$x^3 + 5x^2 + 16x + 9 \equiv -(25x + 14)$ mód $x^2 + 23x + 2$

Por lo que haciendo involución hiperelíptica tenemos que:

$v_3(x) = 6x + 17$

Esto es que:

$[D_1] \oplus [D_2] = [D_3] =< x^2 + 23x + 2, 6x + 17 >$

Si vemos a $[D_3]$ como un divisor, sus lugares explícitos son claramente de $\mathbb{F}$ es decir tienen grado 1

$[D_3] = (17, 26) + (22, 25) - 2\mathcal{Q}_\infty$

3.4. Ejemplo desarrollado $2[D]$

Usaremos el mismo campo de funciones $\mathbb{F} = \mathbb{K}(x, y)$ con $y^2 = x^5 - 1$ en $\mathbb{K} = \mathbb{Z}_{31}$

También usaremos el divisor obtenido anteriormente como ejemplo por lo

que:

$[D] = [D_3] = (17, 26) + (22, 25) - 2\mathcal{Q}_\infty$

que en su forma de Mumford se vería así:

$[D] =< x^2 + 23x + 2, 6x + 17 >$

Procedemos similarmente, sólo que aquí la matriz es:

$$\left[\begin{array}{cccc|c} 6a^2c - 6ad - 6bc & -4ac + 4d & 2c & 0 & 10ab - 5a^3 \\ 6abc - 6bd & -4bc & 2d & 0 & 5b^2 - 5ba^2 \\ a^2 - b & -a & 1 & 0 & c \\ ab & -b & 0 & 1 & d \end{array}\right].$$

Con $[D] =< x^2 + ax + b, cx + d >$.

La matriz resultante sería:

$$\left[\begin{array}{cccc|c} 10 & 12 & 12 & 0 & 13 \\ 26 & 14 & 3 & 0 & 0 \\ 0 & 8 & 1 & 0 & 6 \\ 15 & 29 & 0 & 1 & 17 \end{array}\right].$$

Cuyas soluciones son los coeficientes de $L(x)$:

$p = 10$
$q = 3$
$r = 13$
$s = 28$

De manera similar que en el ejemplo anterior obtendremos que:
$2[D] =< 7x^2 + 16x + 18, 23x + 19 >$

Lo hacemos mónico y obtenemos:

$2[D] =< x^2 + 20x + 7, 23x + 19 >$

$2[D] = 2(21, 6) - 2\mathcal{Q}_\infty$

3.5. Diffie-Hellman hiperelíptico

En la introducción vimos el protocolo Diffie-Hellman el cual permite a dos entidades poder compartir un secreto a través de un canal inseguro de comunicación, la seguridad de éste radica en la dificultad de poder calcular logaritmos en el grupo este problema se le llama "Problema de logaritmo discreto" replanteamos el problema para divisores de la siguiente manera.

3.5.1. Problema de logaritmo discreto hiperelíptico

Sea $\mathbb{F}_q$ un campo finito con q elementos, el problema de logaritmo discreto sobre $< {C_{\mathbb{F}}}^0, \oplus >$ consiste en que dados dos divisores D_1 y D_2, determinar una $m \in \mathbb{Z}$ tal que $D_2 = mD_1$ si ésta existe, en otras palabras es poder calcular la función de logaritmo de tal manera que $\log_{D_1}(D_2) = m$

La ventaja de las curvas hiperelípticas es que proveen la misma seguridad que una curva elíptica pero con una llave más chica, se ha demostrado que es equivalente la seguridad del popular esquema de llave pública basada en números primos RSA usando llaves de 1024-bits con curvas hiperelípticas de género 1 (elípticas) de 160-bits, los mismos ataques al problema de logaritmo discreto elíptico aplican en la generalización hiperelíptica de género 2, pero en éste las llaves proveen seguridad con 80-bits, esto es porque el orden de $< {C_{\mathbb{F}}}^0, \oplus >$ con un campo finito de 80-bits es aproximadamente 160-bits, estos ataques son el cálculo de índices y Pohlig-Hellman.

3.5.2. Implementación de Diffie-Hellman hiperelíptico y ejemplo

Se hizo una implementación en lenguaje C con la jacobiana del campo de funciones $\mathbb{Z}_{31}(x, y)$ tal que $y^2 = x^5 - 1$.
Esta implementación usa las matrices presentadas previamente y la forma de Mumford, el campo base es de característica p el cual se puede modificar, se hizo con un campo chico por razones de simplicidad.

Algoritmo:
1. A y B negocian públicamente $< C^0_{\mathbb{Z}_{31}}, \oplus >$ y $G = (12, 5) + (28, 2) - 2\infty$
2. A escoge un $a \in \mathbb{Z}$ al azar el cual será su llave privada, éste es $a = 16$

3. B escoge un $b \in \mathbb{Z}$ al azar el cual será su llave privada, éste es $b = 34$
4. A calcula su llave pública $D_A = \bigoplus_{i=1}^{a} G =< x^2 + 30x + 16, 10x + 7 >$
5. B calcula su llave pública $D_B = \bigoplus_{i=1}^{b} G =< x^2 + 28x + 16, 29x + 19 >$
6. Ambos intercambian llaves a través del canal público
7. A con la llave de B calcula $S_a = \bigoplus_{i=1}^{a} D_B =< x^2 + 20x + 7, 23x + 19 >$
8. B con la llave de A calcula $S_b = \bigoplus_{i=1}^{b} D_A =< x^2 + 20x + 7, 23x + 19 >$

Por lo que $S_b = S_a$, y ambos ya tienen un secreto compartido que pueden usar para cifrar comunicaciones, un atacante tendría que calcular a y b con las llaves públicas sabiendo G, lo cual equivaldría a calcular logaritmos base G en $< C^0_{\mathbb{Z}_{31}}, \oplus >$, y la igualdad se da porque:

$$S_a = \bigoplus_{i=1}^{a} \bigoplus_{i=1}^{b} G \tag{3.14}$$

y

$$S_b = \bigoplus_{i=1}^{b} \bigoplus_{i=1}^{a} G \tag{3.15}$$

3.6. Conclusión

La notación de Mumford es conveniente para poder calcular rápidamente la adición hiperelíptica, el grupo $< {C_{\mathbb{F}}}^0, \oplus >$ usando divisores reducidos en la forma de Mumford, el teorema de Riemann-Roch es la base que sustenta

el funcionamiento de este grupo, ya que con este se puede deducir la manera anaítica de poder calcular los representantes reducidos de las clases de divisores, y el teorema de Clifford y saltos de Weierstrass nos permiten poder calcular el género, los cuales considero son los resultados más interesantes en este documento, este grupo también es útil en términos criptográficos, como se definió en la introducción podemos utilizar el problema de logaritmo discreto en este grupo para generar sistemas criptográficos como Diffie-Hellman, el cual permite compartir llaves a través de canales no seguros, (internet, teléfono, et cétera), tambien se puede usar para criptografía de llave pública usando algoritmos como Elgamal.

Bibliografía

[1] Niederreiter and Xing, *Rational Points on Curves over Finite Fields.* Cambridge University Press, LMS 285, 2001.

[2] Blake, Seroussi, Smart, *Elliptic Curves in Cryptography.* Cambridge University Press, LMS 265, 1999.

[3] Thomas Wollinger, *Software and Hardware Implementation of Hyperelliptic Curve cryptosystems.* Ruhr-Universit"at Bochum, IT Security 1, 2004.

[4] Henry Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, Frederik Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography.* Chapmap Hall/CRC, Discrete athematics and its applications, 2006.

[5] Henning Stichtenoth *Algebraic Function Fields and Codes.* Springer, Graduate texts in mathematics, 2009.

[6] Neal Koblitz *Algebraic Aspects of Cryptography.* Springer, Algorithms and computation in mathematics, 1999.

[7] Klaus Hulek *Elementary Algebraic Geometry.* AMS, Student Mathematical Library 2003.

[8] Whitfield Diffie, Martin Hellman *New directions in cryptography.* IEEE, IEEE Transactions on Information Theory 22 1976.

[9] David G. Cantor *Computing in the Jacobian of a hyperelliptic curve.* AMS, Mathematics of Computation 48, AMS 1987.

[10] David Mumford *Tata Lectures on Theta II* Birkhauser Boston 1 edition 1992.