UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

CURVAS ELÍPTICAS Y ALGUNAS APLICACIONES

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
MATEMÁTICO

PRESENTA:
ANAYANZI DELIA MARTÍNEZ HERNÁNDEZ

DIRECTOR DE TESIS:
DR. OCTAVIO PÁEZ OSUNA

2008

Hoja de Datos de Jurado

1.	Datos del alumno. Martínez Hernández Anayanzi Delia 52 71 77 12 Universidad Nacional Autónoma de México Facultad de Ciencias Matemático 097131038
2.	Datos del tutor Dr. Osuna Páez Octavio
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 M en C María de Lourdes Guerrero Zarco
6.	Datos del sinodal 4 Mat Julio César Guevara Bravo
7.	Datos de la tesis Curvas elípticas y algunas aplicaciones 118 p. 2008

A mi abuela,

por ser el ejemplo de Amor,
de Libertad, de Lealtad,
de Fuerza
y de Voluntad de toda mi familia.

Agradecimientos

Agradezco infinitamente al Dr. Octavio Páez Osuna por su tiempo, su apoyo, paciencia y sobre todo por haberme enseñado otro mundo.

Agradezco a mi familia (Delia, Mariela e Yñigo) por el soporte, la dedicación y el amor.

Quiero agradecer a la maestra Graciela por haberme enseñado a leer.

Agradezco a mis amigos: a Adriana Mota por los años, a Edith Ordaz por ser otra hermana, a Ethel Ortega por todas las palabras, a Sergio Monroy por sus oídos, a Daniel García por sus ojos y a Jesús Cruz por las canciones. Gracias a Sergio Cabrera por todo lo que compartimos.

Índice General

Introducción

Este trabajo está motivado en el estudio de un tipo de curvas algebraicas llamadas *curvas elípticas* y su uso dentro de la Criptología y Teoría de Códigos.

La Criptología es la rama de las matemáticas encargada de estudiar maneras seguras de enviar y recibir mensajes. La Criptología Moderna está basada en ideas matemáticas y tiene numerosas aplicaciones dentro de la industria de la transmisión de datos. La Teoría de Códigos se encarga de las maneras de transmitir el mensaje.

Las curvas elípticas pueden ser objeto de estudio de diferentes ramas de La Matemática como lo son el análisis complejo, la topología y el álgebra.

El objetivo de este trabajo es comprender las mencionadas curvas en términos del álgebra de campos, para ser más preciso, comprender las curvas elípticas como **campos algebraicos de funciones** y revisar algunas aplicaciones directas en las áreas ya mencionadas.

Para alcanzar dicho objetivo, he dividido este trabajo en dos partes. La primera parte la comprenden los 2 primeros capítulos. En esta, se brindan las definiciones

y resultados de los campos algebraicos de funciones y sus respectivas extensiones, así como la definición de los *campos elípticos* y algunas de sus características.

Los principales resultados del primer capítulo son el Teorema de Riemann-Roch y el Teorema de Saltos de Weierstrass. El segundo capítulo forma la parte medular de este trabajo pues tiene como objetivo vincular a los campos elípticos con la ecuación de una curva elíptica y viceversa. Además, se deducen algunas de las propiedades claves del conjunto de soluciones de una curva elíptica.

La segunda parte, que consiste en los capítulos 3, 4 y 5, está dedicada a revisar algunas aplicaciones de las curvas elípticas como lo son: el problema de la factorización entera, el Problema de Logaritmo Discreto y sus implicaciones en la Criptología de curvas elípticas y por último la construcción de códigos elípticos.

El apéndice incluido consiste en algunas definiciones y resultados previos necesarios para este trabajo.

Parte I

Campos Elípticos

Capítulo 1

Campos de funciones algebraicos

En este capítulo se darán los primeros conceptos de la Teoría de Campos Algebraicos. Algunos conceptos previos se pueden encontrar en el apéndice de este trabajo. La mayor parte del material de este capítulo se puede encontrar en [1].

1.1 Anillos de valoración, lugares y valoraciones discretas

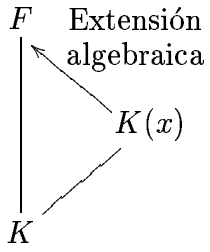


Figura 1.1: *Campo de Funciones Algebraico*

Definición* 1.1.1.** *Sea K un campo arbitrario y sea $F \supseteq K$ una extensión algebraica finita de $K(x)$, para algún elemento $x \in F$ trascendente sobre K. A dicha extensión F la denotaremos como F/K y la llamaremos* ***campo de funciones algebraico de una variable sobre *K. Por brevedad haremos referencia a F/K como* ***campo de funciones****.*

Dentro de F/K tenemos el conjunto de elementos que son algebraicos sobre K y lo denotamos como $\tilde{K}$. Este conjunto es un subcampo de F y nos referiremos a él como **campo de constantes de** F/K. Se tiene que $K \subseteq \tilde{K} \subseteq F$ y F también

puede ser tratado como campo de funciones sobre $\tilde{K}$.

Si $z \in F$ y z es un elemento trascendente sobre K, entonces, $K(z) \cong K(x)$, (Ver apéndice). Esto nos permite caracterizar a los elementos trascendentres sobre K de la siguiente manera: $z \in F$ si y sólo sí $[F : K(Z)] < \infty$.

Definición* 1.1.2.** *Diremos que el campo K es* ***algebraicamente cerrado en F *si $K = \tilde{K}$. En este caso también se dice que K es el campo completo de constantes de F.*

Definición* 1.1.3.** *En F, el anillo $\mathcal{O}$ es de* ***valoración *(o de valuación) si:*

1) $K \subset \mathcal{O} \subset F$, *con* $K \subsetneq \mathcal{O} \subsetneq F$ *y*
2) *Para cualquier elemento* $z \in F, z \in \mathcal{O}$ *ó* $z^{-1} \in \mathcal{O}$.

Al anillo $O^* = \{u \in \mathcal{O} | \ \exists \ u' \in \mathcal{O}$ tal que $uu' = 1\}$ lo llamaremos **anillo de unidades del anillo** O.

Definimos $P = \mathcal{O} - \mathcal{O}^*$. Si $x, \ y \in P$, entonces $\forall \ z \in \mathcal{O}$, se tiene que $zx \in P$ ya que si $zx \in \mathcal{O}^*$, x, sería unidad. Utilizando esta idea y asumiendo que $(\frac{y}{x}) \in \mathcal{O}$ obtenemos $1 + \frac{y}{x} \in \mathcal{O}$ por lo que $x(1 + \frac{y}{x}) = x + y \in P$. Por lo tanto P es un ideal de $\mathcal{O}$.

Por otro lado, si P no fuera ideal maximal de $\mathcal{O}$, entonces contendría unidades, lo cual implicaría que es igual al total.

Por la manera en la que P ha sido definido se sigue que si $x \in F$, $x \in P$ si y sólo si $x^{-1} \notin \mathcal{O}$, ya que si $x^{-1} \in \mathcal{O}$ implicaría que $x \notin \mathcal{O}$, lo cual sería una contradicción, por el hecho que $P \subseteq \mathcal{O}$. Por otro lado, si tomamos un elemento en el campo de constantes K, digamos z, entonces $z \in \mathcal{O}$, ya que si no lo estuviera, $z^{-1} \in \mathcal{O}$. Como z^{-1} es algebraico sobre K sabemos que existen $a_1, ..., a_r \in K$ tales que

$$(a_r(z^{-1})^r + ... + 1) \equiv 0,$$

si restamos 1 y factorizamos z^{-1} obtenemos

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

pero esto pasa si y solamente si

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

y si esta última igualdad fuera cierta entonces $z \in K[z^{-1}] \subseteq \mathcal{O}$ y generaría una contradicción. Por lo tanto $z \in \mathcal{O}$.

Estas características para el anillo de valoración $\mathcal{O}$ se pueden listar en la siguiente proposición:

***Proposición* 1.1.1.** *Sea $\mathcal{O}$ un anillo de valoración de un campo F/K y sea $\tilde{K}$, el campo de constantes de F/K. Entonces:*

a) $\mathcal{O}$ es un anillo local, es decir, el anillo $\mathcal{O}$ tiene un único ideal maximal, (que será P).
b) Sea $0 \neq x \in F$, $x \in P \iff x^{-1} \notin P$.
c) $\tilde{K} \subseteq \mathcal{O}$ y $\tilde{K} \cap P = \{0\}$.

***Lema* 1.1.1.** *Sea $\mathcal{O}$ un anillo de valoración del campo de funciones F/K, con P su único ideal maximal y $x \neq 0 \in P$. Sean $x_1, ..., x_n$ tales que $x_1 = x$ y $x_i \in x_{i+1}P$, para $i = 1, ...n-1$. Entonces $n \leq [F : K(x)] < \infty$.*

Demostración.
Dado que x es trascendente sobre K, entonces $[F : K(x)] < \infty$. Queda demostar que $\{x_1, ..., x_n\} \in P$ es un conjunto linealmente independiente sobre $K(x)$.

Supongamos $\Sigma_{i=1}^{n} \phi_i x_i = 0$ con $\phi_i \in K(x)$. Podemos suponer que ϕ_i son polinomios en la variable x. Sea $\alpha_i := \phi_i(0)$ el término constante de ϕ_i y definimos $j \in \{1, ..., n\}$ tal que $\alpha_j \neq 0$ $\forall i > j$. Obtendremos:

$$-\phi_j x_j = \sum_{i \neq j} \phi_i x_i \tag{1.4}$$

con $x_i \in \mathcal{O}$, para $i = 1, ..., n$. Observamos que $x_i \in x_j P$, para $i < j$ y $x_i = x g_i$ para $i > j$, donde g_i es un polinomio de x. Dividiendo (1.4) entre x_j obtenemos:

$$-\phi_j = \sum_{i<j} \phi_i \cdot \frac{x_i}{x_j} + \sum_{i>j} \frac{x}{x_j} \cdot g_i x_i$$

Dado que todos los elementos del lado derecho pertenecen a P, entonces $\phi_i \in P$. Por otro lado $\phi_j = \alpha_j + x g_j$ con $g_j \in K[x] \subseteq \mathcal{O}$ y $x \in P$ entonces, $\alpha_j = \phi_j + x g_j \in P \cap K$. Como $\alpha_j \neq 0$ se llega a una contradicción con la proposición anterior. $\diamondsuit$

***Definición* 1.1.4.** *Llamaremos **anillo de valoración discreta** a un anillo de valoración $\mathcal{O}$ con único ideal maximal P, siempre que se cumplan las siguientes condiciones:*

a) P *es un ideal principal.*

b) *Si* $P = t\mathcal{O}$ *entonces* $\forall\ 0 \neq\ z \in F,\ z = t^n u, u\ \in \mathcal{O}^*$, *para alguna* $n \in\ \mathbb{Z}$.

c) $\mathcal{O}$ *es dominio de ideales principales. Si* $P = t\mathcal{O}$ *y* $\{0\} \subsetneq I \subseteq \mathcal{O}$ *entonces* $I = t^n\mathcal{O}$ *para alguna* $n \in \mathbb{N}$.

Teorema 1.1.1. *Sea* $\mathcal{O}$ *un anillo de valoración del campo de funciones* F/K, *entonces* $\mathcal{O}$ *es un anillo de valoración discreta.*

Demostración.
Primero vamos a suponer que P no es un ideal principal. Sea $0 \neq x_1 \in P$ entonces $P \neq x_1\mathcal{O}$ lo cual implica que existe un elemento $x_2 \in\ (P - x_1 O)$ es decir $x_2 \notin x_1\mathcal{O}$, por lo que $x_2 x_1^{-1} \notin \mathcal{O}$, entonces $x_2^{-1}x_1\ \in\ P$ por lo que tenemos $x_1 \in x_2 P$ pues $x_2 x_2^{-1} x_1 = x_1 \in P$. Ahora $P \neq x_2 P \Rightarrow \exists x_3 \in (P \backslash x_2\mathcal{O}), x_3 x_2^{-1} \notin \mathcal{O} \Rightarrow x_3^{-1}x_2 \in P\ \Rightarrow x_2 \in x_3 P$. Por inducción construimos una sucesión no acotada $x_1, x_2, ...,$ contradiciendo el lema anterior. Por lo tanto se cumple la condición del inciso a).

Para verificar la la siguiente propiedad, supongamos $p = t\mathcal{O}$. Sea $z \in F$, por la definición de $\mathcal{O}$, $z \in \mathcal{O}$ ó $z^{-1} \in \mathcal{O}$. Supongamos que $z \in \mathcal{O}$, si $z \in \mathcal{O}^* \Rightarrow\ z = t \cdot u,\ u \in \mathcal{O}^*$. Supongamos que $z \in P,\ z = ta$. Sea $x_1 \in z,\ x_2 = t^{m-1}, ..., x_m = t$, donde m es maximal con la propiedad de que $z \in t^m O$. Como $z = t^m a$, si $a \notin \mathcal{O}^*\ \Rightarrow a \in P$ entonces $a = t \cdot h \Rightarrow z = t^{m+1} \cdot h$, lo cual contradice la maximalidad de m. Tenemos que se cumple la segunda condición.

Sea I ideal de $\mathcal{O}$ tal que $\{0\} \subsetneq I \subsetneq \mathcal{O}$. Sea $A = \{r | t^r \in I\}$. Afirmamos que $A \neq \emptyset$. Si $x \in I, x \neq 0, x = t^n \cdot u$ para n, $u \in O^* \Rightarrow xu^{-1} = t^n \in I$ entonces $A \neq \emptyset$. Sea $n = minA$ entonces $I = t_n \cdot \mathcal{O}$. Como $t^n \in I,\ t^n\mathcal{O} \subseteq I$. Sea $\mathcal{O} \neq y \in I$ entonces $y = t^s a, a \in \mathcal{O}^* s \geq n$ ent $s = n + r \Rightarrow y = t^r t^n a \in t^n\mathcal{O}$. Por lo tanto $t^n\mathcal{O} \subseteq I$ y $I \subseteq t^n\mathcal{O}$. Por lo tanto cumple con la última condición y el teorema es cierto. $\diamondsuit$

Definición 1.1.5. *Al único ideal maximal de un anillo de valoración* $\mathcal{O}$ *de* F/K, *le llamaremos* ***lugar P*** *del campo de funciones* F/K.

Definición 1.1.6. *Todo elemento* $t \in F$ *tal que* $P = t\mathcal{O}$ *lo nombramos* ***parámetro local,*** *variable de uniformización ó elemento primo de* P.

OBSERVACIÓN: Si $\mathcal{O}$ es un anillo de valoración de F/K, $\mathcal{O}$ queda determinado por su lugar P, esto es:

$$\mathcal{O} = \{z \in F | z^{-1} \notin P\}$$

Siendo así, denotaremos como $\mathcal{O}_p := \mathcal{O}$ al anillo de valoración del lugar P.

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

Definición* 1.1.7.** *Sea v una función tal que $v : F \mapsto \mathbb{Z} \cup \{\infty\}$. Diremos que v es* ***valoración discreta *si cumple las siguientes propiedades:*

1) $v(x) = \infty \Leftrightarrow x = 0$.
2) $v(zw) = v(z) + v(w), \ \forall \ z, w \in F$.
3) $v(a) = 0, \ \forall \ 0 \neq a \in K$.
4) $v(z + w) \leq min\{v(z), v(w)\}$.
5) *Existe algún elemento $z \in F$ tal que $v(z) = 1$.*

OBSERVACION:
$\star$ Si $x, y \in F$, si $x \neq y$ entonces podemos suponer sin pérdida de generalidad que $v(x) < v(y)$. Si $v(x + y) \neq min\{v(x), v(y)\}$, entonces $v(x + y) > v(y)$, con lo que obtenemos:

$$v(x) = v((y + x) - y) \geq min\{v(x + y), v(y)\} > v(x)$$

lo cual es una contradicción. Lo que hemos obtenido es la siguiente afirmación:

$$v(x + y) = min\{v(x), \ v(y)\}$$

igualdad a la que llamaremos **desigualdad estricta del triángulo**.

A continuación vamos a definir una valoración que puede ser utilizada para cualquier lugar P de F/K:

Escogemos un elemento primo t para P, es decir, un elemento con el cual podemos escribir cualquier elemento $z \in F$ como $z = t^n \cdot u$, con $u \in \mathcal{O}_p{}^*$ y $n \in \mathbb{Z}$. Por otro lado, para cada $P \in \mathbb{P}_F$ se puede asociar la siguiente función: $v_P : F \mapsto \mathbb{Z} \cup \infty$ dada por

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

Definida así, v_P tiene las siguientes propiedades:

$\star$ Si $a \in K \subseteq \mathcal{O}_P P$ entonces $a \in \mathcal{O}^* \Rightarrow a \notin P$ entonces $a = t^o \cdot a$, es decir,

$v_P(a) = 0, \forall a \in K.$

$\star$ Sea $x, y, \in F$ con $x = t^n u_1$ y $y = t^m u_2$ entonces:

$$v_P(xy) = v_P(t^n u_1 t^m u_2) = v_P(t^{n+m} u_1 u_2) = m + n = v_P(x) + v_P(y),$$

además,

$$x + y = t^n u_1 + t^m u_2 = t^n(u_1 + t^{m-n} u_2) = t^n z$$

para alguna $z \in \mathcal{O}$ y analizamos los dos casos posibles:

- Si $z = 0$ entonces,

$$v_P(z) = 0 \Rightarrow v_P(x + y) = \infty > min\{n, m\}.$$

- Si $z = t^k u$ entonces,

$$z = t^k u \Rightarrow v_P(t^{k+n} u) = k + n \geq n = min\{v_P(x), v_P(y)\}.$$

Con estas propiedades se afirma que v_P es una valoración discreta.

Definición* 1.1.8.** *Al campo $F_P := \mathcal{O}_P/P$ lo llamaremos el* ***campo residual del lugar P*. El* ***grado de un lugar*** *estará definido por $[F_P : K]$, es decir, $grad\ P := [F_P : K]$.*

OBSERVACIÓN: Como P es un ideal maximal de $\mathcal{O}_P$ entonces, $\mathcal{O}_P/P$ es un campo.

***Definición* 1.1.9.** *Al mapeo $x(P) : F \mapsto F_P \cup \{\infty\}$, dado por*

$$x(P) = \begin{cases} x + P & x \in \mathcal{O}_\mathcal{P} \\ \infty & x \in F \backslash \mathcal{O}_\mathcal{P} \end{cases}$$

le llamaremos "mapeo natural", ó canónico.

OBSERVACIÓN: De 1.1.1 sabemos que el campo K está contenido en todo anillo O_P y que $K \cap P = \{0\}$. Es decir, bajo el mapeo canónico, K es repartido en diferentes clases residuales, por lo que F_P contiene una copia del campo K. Esto también es válido para $\tilde{K}$

***Proposición* 1.1.2.** *Si P es un lugar de F/K, y $0 \neq x \in P$ entonces:*

$$deg\ P \leq [F : K(x)] < \infty.$$

Demostración.
Supongamos que existe un conjunto $\{z_i(P)\}_{i=1}^n$ linealmente independiente sobre K y una combinación lineal no trivial de elementos $z_1, z_2, ..., z_n \in \mathcal{O}_p$ tales que:

$$\sum_{i=1}^{n} \phi_i z_i = 0 \quad \text{con} \quad \phi_i \in K(x).$$

Para P un lugar, las clases residuales a las que pertenecen $z_1, z_2, \ldots, z_n$ son $z_1(P), z_2(P), \ldots, z_n(P)$ respectivamente. Sin pérdida de generalidad, podemos suponer que ϕ_i son polinomios de x y que no todos son divisibles entre x, es decir $\phi_i = a_i + xg_i$, con $g_i \in K(x)$ y $a_i \in K$. Como $x \in P$ y $g_i \in \mathcal{O}_p$:

$$\phi_i(P) = a_i(P) + xg_i(P) = a_i(P)$$

entonces,

$$0 = \mathcal{O}(P) = \sum_{i=1}^{n} \phi_i(P) z_i(P) = \sum_{i=1}^{n} a_i z_i(P)$$

lo cual contradice la independencia lineal de $\{z_i(P)\}_{i=1}^n$. Por lo tanto

$$[F_p : K] \leq [F : K(x)].$$

Si utilizamos el hecho de que $\mathbb{P}_F \neq \emptyset$ y escogemos alguna $p \in \mathbb{P}_F$, entonces, $\tilde{K}$ es sumergido dentro de F_P por el mapeo $O_p \mapsto F_P$, por lo tanto,

$$[\tilde{K} : K] \leq [F_P : K] < \infty. \diamondsuit$$

***Corolario* 1.1.1.** *Si $P \neq \emptyset \in \mathbb{P}_F$, entonces $[\tilde{K} : K] \leq deg\ P < \infty$.*

Ceros y Polos

Sea F/K un campo de funciones. Si tomamos un lugar P de grado 1, entonces estamos diciendo que $O_P/P = K$. (Más adelante veremos que cuando K es algebraicamente cerrado, todos los lugares son de grado 1). Por otro lado, el

mapeo canónico definido en 1.1.9 puede ser redefinido como $z(P) : F \mapsto K \cup \{\infty\}$, tal que:

$$z(P) = \begin{cases} z + P & z \in \mathcal{O}_{\mathcal{P}} \\ \infty & z \in F \backslash \mathcal{O}_{\mathcal{P}}. \end{cases}$$

logrando la misma regla de correspondencia. Además, el resultado de aplicar esta regla, no es alterado si ahora vemos a cada elemento z de F/K como una función con las siguientes características:

$$\begin{aligned} z: \ \mathbb{P}_F &\longrightarrow K \cup \{\infty\} \\ P &\longmapsto z(P) \end{aligned}$$

Estas ideas argumentan por qué a F/K se le llama **campo de funciones**. Las observaciones hechas anteriormente motivan a que nos preguntemos cómo se comporta z bajo $z(P)$. Recordemos que para que $z(P) \neq \infty$ su valoración deberá de ser mayor ó igual a cero.

***Definición* 1.1.10.** *Sea $z \in P$ y $P \in \mathbb{P}_F$. Llamamos:*

- ⋆ *P **cero** de z si $V_p(z) > 0$. Si $V_p(z) = m$ será **cero de orden m**.*
- ⋆ *P **polo** de z si $V_p(z) < 0$. Si $V_p(z) = -m$ será **polo de orden m**.*

El siguiente teorema asegura que $\mathbb{P}_F \neq \emptyset$.

***Teorema* 1.1.2.** *Sea F/K un campo de funciones, R subanillo de F, tal que $K \subseteq R \subseteq F$. Supongamos $0 \neq I$ ideal propio de R. Entonces existe $P \in \mathbb{P}_F$ tal que $I \subseteq P$ y $R \subseteq \mathcal{O}_p$.*

Demostración.
Sea $\mathcal{F} = \{S | S$ es subanillo de F con $R \subseteq S$ y $IS \neq I\}$. Un ideal para este subanillo queda definido por $IS = \{\sum i_v S_v | i_v \in I, t_v \in S\}$. Dado que $IR \neq I$ entonces $R \in \mathcal{F}$ por lo que $\mathcal{F} \neq \emptyset$. Por otro lado, si $\mathcal{H}$ es una familia de $\mathcal{F}$ totalmente ordenada, entonces

$$T = \cup_{S \in \mathcal{H}} S$$

es subanillo de $\mathcal{F}$ y $R \subset T$.

Demostraremos que $IT \neq I$. Si se supone que $IT = I$, entonces $1 \in I$, lo que implica:

$$1 = \sum i_v S_v, \quad i_v \in I, \ t_v \in T.$$

Como $\mathcal{H}$ es totalmente ordenado, entonces existe $S_0 \in H$ tal que $t_1, ..., t_n \in S_0$ por lo que:

$$1 = \sum_{v=1}^{n} a_v S_v \in IS_0$$

y se genera una contradicción pues $IS_0 \neq S_0$. Por el lema de Zorn $\mathcal{F}$ contiene un anillo maximal, i.e. existe un anillo $\mathcal{O} \in \mathcal{F}$ tal que $R \subseteq \mathcal{O} \subseteq F$, $I\mathcal{O} \neq \mathcal{O}$, $I \neq \mathcal{O}$. Falta verificar que $\mathcal{O}$ es un anillo valuado.

Vamos a suponer $z \in F$ y $z \notin O$ y $z^{-1} \notin \mathcal{O}$. Entonces $I\mathcal{O}[z] \neq \mathcal{O}[z]$ y $I\mathcal{O}[z] = \mathcal{O}[z]$. En este caso, podríamos encontrar $a_o, ..., a_n, b_o, ..., b_n \in I\mathcal{O}$ con

$$\begin{aligned} a_0 + a_1 z + ... + a_n z^n &= 1 \\ b_0 + b_1 z + ... + b_m z^m &= 1 \end{aligned}$$

con $1 \leq n, m$ y $m \leq n$. Multiplicando las ecuaciones anteriores por $(1 - b_0)$ y por $(a_n z^n)$ respectivamente, obtenemos:

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

Si sumamos las dos ecuaciones, obtendremos una ecuación de la forma:

$$1 = c_0 + c_1 z + ... + c_{n_1} z^{n-1} \text{ con } \; c_i \in I\mathcal{O},$$

lo cual es una contradicción con la minimalidad de n. Entonces, $z \in \mathcal{O}$ ó $z^{-1} \in \mathcal{O}$, para cualquier $z \in F$. Por lo tanto $\mathcal{O}$ es un anillo de valoración. $\diamondsuit$

***Corolario* 1.1.2.** *Sea F/K un campo de funciones F/K, $z \in F$, un elemento trascendente sobre K. Entonces z tiene al menos un lugar polo y al menos uno cero.*

Demostración.
Sea $R = K[z]$ y $I = zK[z]$. Por el teorema anterior existe $\mathcal{O}$, anillo de valoración tal que $R \subseteq \mathcal{O}$ y $zK[z] \subseteq P \Rightarrow z \in P$ y $v_p(z) > 0$ por lo tanto P es un cero de z. Con el mismo razonamiento, tenemos que z^{-1} tiene un cero en Q, entonces $V_Q(z) < O$, por lo tanto Q es un polo de z. $\diamondsuit$

1.1.1 El campo Funciones Racionales K(x)

En esta sección analizaremos algunas de las nociones anteriores de K(x) como campo de funciones.

Uno de los ejemplos más sencillos para un campo de funciones, es el **campo de funciones racionales**. Este caso se da cuando $K(x) = F$ para algún elemento x trascendente sobre K. Su construcción ha sido establecida en 5.1. Es este campo, todo elemento $0 \neq z \in K(x)$ tiene una única representación:

$$z = a \cdot \prod_i p_i(x)^{n_i},$$

donde $a \neq 0 \in K$, los polinomios $p_i(x) \in K[x]$ son mónicos, irreducibles y distintos dos a dos y $n_i \in \mathbb{Z}$.

Acontinuación presento información acerca de la naturaleza de los anillos de valoración de $K(x)$, acerca de sus lugares y consecuentemente de las valoraciones discretas resultantes.

- ⋆ Sea $p(x) \in K[x]$ un polinomio mónico e irreducible. El anillo:

$$O_{p(x)} := \left\{ \frac{f(x)}{g(x)} | f(x), g(x) \in K[x], p(x) \not| g(x) \right\} \tag{1.22}$$

será un anillo de valoración con ideal máximo:

$$P_{p(x)} := \left\{ \frac{f(x)}{g(x)} | f(x), g(x) \in K[x], p(x) | g(x),\ p(x) \| g(x) \right\} \tag{1.23}$$

Se tiene que $p(x)$ genera a $P_{p(x)}$ por lo que es un elemento primo. La valoración correspondiente $v_{P_{p(x)}}$ queda descrita como sigue: si escribimos $z = p(x)^n (f(x)/g(x))$ con $n \in \mathbb{N}$ y las restricciones al ideal $P_{p(x)}$ entonces $v_P(z) = n$.
Sea φ un homomorfismo de anillos, definido como sigue:

$$\varphi := \begin{cases} K[x] \longrightarrow O_P/P \\ f(x) \mapsto f(x)(P) \end{cases}$$

Queda claro que el ideal generado por $p(x)$ es el núcleo de φ. Además si se tiene un elemento z en O_P, éste puede ser escrito como $z = u(x)/v(x)$

con $u(x), v(x) \in K[x]$ tal que $p(x)$ no divide a $v(x)$, por lo que existen $a(x), b(x) \in K[x]$ tales que $1 = p(x)a(x) + v(x)b(x)$, así:

$$z = z \cdot 1 = \frac{u(x)p(x)a(x)}{v(x)} + u(x)b(x)$$

entonces $z(P) = u(x)b(x)(P) \in imag\varphi$, por lo que φ induce un isomorfismo ϕ entre $K[x]/ < p(x) >$ y O_P/P, es decir:

$$\phi := \begin{cases} K[x]/ < p(x) > \longrightarrow O_P/P \\ f(x) \ mod \ p(x) \mapsto f(x)(P) \end{cases}$$

Consecuentemente,

$$grado \ P = [O_P/P : K] \ = \ [K[x]/ < p(x) >: K] \ = \ grado \ p(x).$$

⋆ En el caso donde $p(x) = x - a$, con $\alpha \in K$ entonces escribiremos $P := P_\alpha$. Por el párrafo anterior el grado de $P = P_\alpha$ es igual a uno.
Si $f(x) \in K[x]$ entonces $(x - \alpha)|(f(x) - f(\alpha))$, es decir $\exists q(x) \in K[x]$ tal que $f(x) - f(\alpha) = q(x)(x - \alpha)$ por lo que $f(x) = f(\alpha) + q(x)(x - \alpha)$. Aplicando el mapeo canónico a $f(x)$ obtenemos:

$$f(x)P_\alpha = f(\alpha)P_\alpha + q(x)(x - \alpha)P_\alpha = f(\alpha)P_\alpha = f(\alpha)$$

Podemos escribir a $z \in K(x)$ como $z = \dfrac{f(x)}{g(x)}$ donde los polinomios $f(x)$ y $g(x)$ pertenecen al anillo $K[x]$ y son primos relativos, entonces:

$$z(P) = \frac{f(x)P_\alpha}{g(x)P_\alpha} = \frac{f(\alpha)}{g(\alpha)} = z(\alpha)$$

por lo que:

$$z(P) = z(\alpha) \ \textbf{para} \ z \in K(x).$$

donde $z(\alpha)$ queda definido como sigue:

$$z(\alpha) := \begin{cases} f(\alpha)/g(\alpha) & \text{si } g(\alpha) \neq 0. \\ \infty & \text{si } g(\alpha) = 0. \end{cases}$$

⋆ Otro ejemplo para un anillo valuado dentro del campo $K(x)$ es:

$$\mathcal{O}_\infty := \{\frac{f(x)}{g(x)} | f(x), g(x) \in K[x], grado \ f(x) \leq grado \ g(x)\} \qquad (1.32)$$

con ideal maximal:

$$\mathcal{P}_\infty := \left\{ \frac{f(x)}{g(x)} | f(x), g(x) \in K[x], grado\ f(x) < grado\ g(x) \right\} \qquad (1.33)$$

Consideremos el elemento $z = \dfrac{f(x)}{g(x)} \in \mathcal{P}_\infty$, es decir $grado\, f(x) < grado\, g(x)$.
Otra manera de escribir a z será:

$$z = \frac{1}{x} \cdot \frac{xf(x)}{g(x)}$$

donde $grado\ xf(x) \leq grado\ g(x)$, por lo que $z \in (1/x)\mathcal{O}_\infty$, así que $(1/x)$ es el parámetro local de $\mathcal{P}_\infty$.
Este lugar tiene grado 1 y la valoración discreta v_∞ correspondiente a este lugar está dada por:

$$v_\infty(f(x)/g(x)) = grado\ g(x) = grado\ f(x).$$

Sea $z \in K(x)$ donde

$$z = \frac{a_n x^n + ... + a_0}{b_m x^m + ... + b_0} \qquad \text{con } a_n, b_n \neq 0;$$

el mapeo $z(\mathcal{P}_\infty) = z(\infty)$ y queda definido como sigue:

$$z(\infty) := \begin{cases} a_n/b_n \text{ si n=m;} \\ 0 \quad \text{si } n < m\ ; \\ \infty \quad \text{si } n > m\ ; \end{cases}$$

Si tomamos un lugar P de $K(x)/K$ de grado 1, tenemos que el campo $\tilde{K}$ queda incrustrado dentro de F_P por lo que:

$$K \subseteq \tilde{K} \subseteq F_P = K \Rightarrow\ K = \tilde{K},$$

es decir, K es el campo de constantes para $K(x)/K$.

Teorema 1.1.3. *Para el campo de funciones racionales $K(x)/K$, sólo existen los lugares $P_{p(x)}$ y $\mathcal{P}_\infty$ definidos en 1.23 y en 1.33.*

Demostración.
Sea $P \in \mathbb{P}_{K(x)}$ con $P \neq \mathcal{P}_\infty$. Se demostrará que existe un polinomio irreducible $p(x) \in K[x]$ tal que $\mathcal{O}_{p(x)} = \mathcal{O}_P$.

Supongamos que $x \in \mathcal{O}_P$. En este caso, $K[x] \subseteq \mathcal{O}_P$. Sea $I := K[x] \cap P$. Se tiene que I es un ideal primo. El mapeo de la clase residual induce que $K[x]/I$ se pueda insertar dentro de $K(x)_P$, por lo que $I \neq 0$. Se tendrá que existe un único polinomio mónico e irreducible $p(x)$ tal que $I = K[x] \cap P = p(x) \cdot K[x]$. Además, cualquier $g(x) \in K[x]$ con $g(x) \not/ p(x)$ no está en I, entonces $g(x)$ no pertenece a P, así que $1/g(x) \in \mathcal{O}_P$. Por lo tanto, $\mathcal{O}_{p(x)} \subseteq \mathcal{O}_P$. Como los anillos de valoración son subanillos propios maximales de $K[x]$, entonces $\mathcal{O}_{p(x)} = \mathcal{O}_P$.

***Corolario* 1.1.3.** *Los lugares de $K(x)/K$ de grado uno, se encuentran en correspondencia biunívoca con $K \cup \{\infty\}$*

1.2 Independencia de Valoraciones

> El resultado más importante en este capítulo es el *Teorema débil de aproximación* al que también se le conoce como *Teorema de la independencia.*

En este capítulo utilizaremos que: F/K es un campo de funciones, $x_1, .., x_n \in F$, $P_1, ..., P_n \in \mathbb{P}_F$ son distintos dos a dos, $r_1, .., r_n \in \mathbb{Z}$ y $v_1, .., v_n$ son valoraciones discretas de F/K distintas dos a dos.

***Lema* 1.2.1.** *Existe $u \in F$ tal que $v_1(u) > 0$ y $v_i(u) < 0$, para $i = 2, ..., n$.*

Demostración.
Esta prueba se hace por inducción sobre n. Caso $n = 2$: dado que $\mathcal{O}_{P_1}$ y $\mathcal{O}_{P_2}$ son anillos maximales de F, se sigue que $\mathcal{O}_{P_1} \not\subseteq \mathcal{O}_{P_2}$ y $\mathcal{O}_{P_2} \not\subseteq \mathcal{O}_{P_1}$. Por otro lado, $\exists\ y_1 \in \mathcal{O}_1 \backslash \mathcal{O}_2$ y $\exists\ y_2 \in \mathcal{O}_{P_1}\ \mathcal{O}_{P_2}$ por lo que:

$$\begin{aligned} v_{P_1}(y_1) \geq 0,\ v_{P_2}(y_1) < 0 \text{ y} \\ v_{P_2}(y_2) \geq 0,\ v_{P_1}(y_2) < 0 \end{aligned}$$

Sea $u = y_1/y_2$ entonces

$$\begin{aligned} v_{P_1}(u) &= v_{P_1}(y_1) - v_{P_1}(y_2 > 0 \text{ y} \\ v_{P_2}(u) &= v_{P_2}(y_1) - v_{P_2}(y_2) < 0 \end{aligned}$$

Supongamos que existe $y \in F$ con $v_1(y) > 0$ y $v_i(y) < 0$ para $i = 2, ..., n-1$, entonces, se tienen dos casos:

- $\star$ $v_n(y) < 0$ entonces $u = y$
- $\star$ Si $v_n(y) \geq 0$. Sea $z \in F$ tal que $v_1(z) > 0$, $v_n(z) < 0$, $z \in \mathcal{O}_1 - \mathcal{O}_n$. Sea $u = y + z^r$, $r \geq 1$ donde r es un entero tal que $v_i(y) \neq r v_i(z)$, para $i = 2, ..., n-1$. Luego $v_1(u) \leq min\{v_i(y),\ r v_i(z)\} > 0$, y $v_i(u) = min\{v_i(y), r \cdot v_i(z)\} < 0$ para $i = 1, ..., n-1$. Además $v_n(u) \geq min\{v_i(y), r v_i(z)\} < 0$. $\diamondsuit$

***Lema* 1.2.2.** *Existe $\omega \in F$ tal que $v_1(\omega - 1) > r_1$ y $v_i(\omega) > r_i$ para $i = 1, ..., n$.*

Demostración.
Sea $u \in F$ como en (1.2.1) y sea $w := (1 + u^s)^{-1}$, entonces:

$$\begin{aligned} v_1(w-1) &= v_1(\frac{1}{i+u^s}, -1) \\ &= v_1(\frac{-u^s}{1+u^s}) \\ &= sv_1 - v_1(1+u^s) \\ &= sv_1(u) - min\{0, sv_1(n)\} \\ &= sv_1(u) > r_1 \end{aligned}$$

para s suficientemente grande. Además $v_i(w) = -v_i(1 + u^s) = -sv_i(u) > r_i$. $\diamondsuit$

***Lema* 1.2.3.** *Dadas $y_1, ..., y_n \in F$, existe $z \in F$ tal que $v_i(z - y_i) > r_i$ para $i = 1, ..., n$*

Demostración.
Sea $s \in \mathbb{Z}$ tal que $v_i(y_j) \geq s, \forall\ i, j, \in \{1, ..., n\}$. Por el lema anterior existe $w_1, ..., w_n \in F$ tal que $v_i(w_i - 1) > r_i - s$ y $v_i(w_j) > r_i - s$ para $i \neq j$. Se propone $z := \sum_{j=1}^{n} y_i v_i$ y se observa que $v_i(z - y_i) \geq min(v_i(z), v_i(y_i)) > r_i$ por lo que z cumple el lema.$\diamondsuit$

Teorema débil de aproximación:[1]

***Teorema* 1.2.1.** *Sean:*

$$\begin{aligned} P_1, ..., P_n &\in \mathbb{P}_F \\ \gamma_1, ..., \gamma_n &\in \mathbb{Z} \\ x_1, ..., x_n &\in F \end{aligned}$$

Entonces existe $x \in F$ tal que $v_{P_i}(x - x_i) = \gamma_i$.

[1] Este teorema también es llamado *teorema de independencia* ya que propone lo siguiente: si tenemos $v_1, ..., v_n$ valoraciones distintas de F/K, $z \in F$ y conocemos $v_i(z)_{i=1}^{n-1}$, entonces no podemos asegurar nada acerca del $v_n(z)$.

Demostración.
Por lema (1.2.3), $\exists\ z \in F$ tal que $v_i(z-x_i) > r_i$ para $i = 1, ...n$. Sean $z_1, ..., z_n \in F$ tal que $v_i(z_i) = r_i$. Nuevamente, por (1.2.3), $\exists\ z' \in F$ tal que $v_i(z' - z_i) > r_i$, para $i = 1, ...n$. Tenemos que :

$$v_i(z') = v_i((z' - z_i) + z_i) = min\{v_i(z' - z_i), v_i(z_i)\} = r_i \tag{1.39}$$

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

$$v_i((x - x_i) + z') = v_i((z - x_i) + z') = min\{v_i(z - x_i), v_i(z')\} = r_i.\diamondsuit \tag{1.40}$$

***Corolario* 1.2.1.** *El conjunto $\mathbb{P}_F$ de F/K es infinito.*

Demostración.
Supongamos que $\{P_1, .., P_n\} = \mathbb{P}_F$ con $n < \infty$, por el *Teorema de Aproximación*, podemos encontrar una función $x \neq 0$ tal que $v_{P_i}(x) > 0$, por lo que $x_i \in P_i$ para $i = 1, ..., n$. Como $\tilde{K} \cap P_i = \{0\}$, entonces x es un elemento trascendente sobre K, pero x no tiene polos, lo cual es una contradicción. $\diamondsuit$

***Proposición* 1.2.1.** *Si $\{P_1, ...P_n\} = \mathbb{P}_F$, son ceros de $\gamma \in F$, entonces,*

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

Demostración.
Sea $f_i := grado\ P_i$ y $e_i := v_i(x)$. Sabemos que para cualquier i existe un elemento $t_i \in F$ tal que $v_{P_i}(t_i) = 1$ y $v_{P_k}(t_i) = 0$ para $k \neq i$. Por otro lado, sea $f_i = grado\ P_i$ y $s_i 1, ..., s_{if_i} \in \mathcal{O}_{P_i}$ tal que $s_i 1(P_i), ..., s_{if_i}(P_i)$ forman una base para la clase residual F_{P_i} sobre K. Por el teorema (1.2) podemos encontrar un elemento $z_{ij} \in F$ con las siguientes caraterísticas:

$$v_{P_i}(s_{ij} - zij) > 0 \text{ y } v_{P_k}(z_{ij}) \geq v_k(x) \text{ para } k \neq i$$

Lo siguiente es verificar que elementos $t_i^a \cdot z_{ij}$ con $1 \leq i \leq r$,$1 \leq j \leq grado\ P_i$ y $0 \leq a < v_{P_i}(x)$, cuya suma es igual a $\sum_{i=1}^{r} v_{P_i}(x) grado\ P_i$, son linealmente independientes. Supondremos que no es cierto, es decir, supondremos que existe una combinación lineal no trivial tal que:

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i - 1} \varphi_{ija} t_i^a \cdot z_{ij} = 0 \tag{1.41}$$

sobre $K(x)$ y sin pérdida de generalidad podemos asumir que no todos los elementos φ_{ija} son divisibles por x. Siendo así, exiten $k \in 1, ..., r$ y $c \in 0, ..., e_k - 1$ tales que:

$$x|\varphi_{kja} \text{ para cualquier } a < c \text{ y cualquier } j \in 1, ..., f_k$$
$$\text{y } x \not|\varphi_{kjc} \text{ para algún } j \in 1, ..., f_k.$$

Multiplicando la ecuación (1.41) por t_k^{-c} obtenemos:

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija} t_k^{-c} t_i^a \cdot z_{ij} = 0 \tag{1.42}$$

Para $i \neq k$ todos los sumandos de (1.42) están en P_k pues:

$$\begin{aligned} v_k(\varphi_{ija} t_k^{-c} t_i^a z_{ij}) &= v_k(\varphi_{ija}) - c v_k(t_k) + v_k(t_i^a) + v_k(z_{ij}) \\ &\geq 0 + 0 - c + e_k(x) > 0 \end{aligned} \tag{1.43}$$

Para $i = k$ y $a < c$ tendremos que: $v_k(\varphi_{ija} t_k^{-c} t_i^a z_{ij}) \geq e_k + a - c \geq > 0$ y para $a > c$,

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

Por las desigualdades anteriores tenemos que:

$$\sum_{j=1}^{f_k} \varphi_{kjc} z_{kj} \quad \in \quad P_k. \tag{1.44}$$

También observamos que $\varphi kjc(P_k) \in K$ y $\varphi kjc(P_k) = 0$, por lo que existe una combinación lineal no trivial:

$$\sum_{j=1}^{f_k} \varphi_{kjc}(P_k) z_{kj}(P_k) = 0 \tag{1.45}$$

sobre K y se produce una contradicción pues los elementos $z_{k1}(P_k), .., z_{kf_k}(P_k)$ forman una base para F_{P_k}/K. $\diamondsuit$

***Corolario* 1.2.2.** *En un campo de funciones F/K un elemento $0 \neq x \in F$ tiene un número finito de ceros y de polos.*

Demostración.
Si $x \in K$, es decir x es constante, entonces, x, no tiene ni ceros ni polos. Si x es trascendente sobre K, el número de ceros de x es menor a $[F : K(x)] < \infty$. De la misma manera el número de ceros de x^{-1} es menor a $[F : K(x^{-1})] < \infty$. $\diamondsuit$

1.3 Divisores

Para cualquier campo de funciones racionales F, podemos construir una familia de elementos D, con la siguiente característica:

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

con $n_P \in \mathbb{Z}$ y $n_P = 0$ excepto en un número finito de lugares. Es decir, para obtener un elemento de esta familia, asociaremos un número entero a cada lugar y estableceremos una suma formal. [2] Los elemento de dicha familia varían en el número asociado al lugar, por lo que esta familia puede ser infinita. A esta familia la denotamos como $\mathcal{D}_F$.

Sean $D = \sum n_P P$ y $D' = \sum n_{P'} P'$ con $P, P' \in \mathbb{P}_F$ (claramente son elementos que pertenecen a la famila $\mathcal{D}_F$) entonces, podemos definir la suma entre ellos de la siguiente manera:

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

Esta suma es asociativa. También definiremos un elemento identidad como:

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

Dado que $n_P \in \mathbb{Z}$, entonces se puede formar el inverso aditivo de cada elemento D y con esto tenemos que $\mathcal{D}_F$ forma un grupo. La conmutatividad de éste, queda justificada por la conmutatividad en $\mathbb{Z}$, así $\mathcal{D}_F$ forma un grupo abeliano [3] y aunque no se utilizará el resultado en este trabajo cabe hacer mención que es un **grupo abeliano libre**. [4]

[2] En general, se puede definir el concepto de divisores para cualquier conjunto.

[3] Esta estructura es independiente al conjunto inicial que tomemos.

[4] Un grupo G es **libre** si existe un subconjunto S de G tal que todo elemento de G puede escribirse en una forma única como producto de elementos de S.

Definición* 1.3.1.** *Al grupo abeliano libre $\mathcal{D}_F$ generado por los lugares de un campo de funciones F lo llamaremos* ***grupo de divisores*. Los elementos de dicho grupo se llamaran divisores.*

Para $Q \in \mathbb{P}_F$ y para $D = \sum n_P P \in \mathcal{D}_F$ se define $v_Q(D) := n_Q$, en otras palabras $v_Q(D)$ será el número asociado al lugar Q en el divisor D. Para cada divisor D se tiene:

$$a)\textbf{grado D} := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot grado\ P$$

$$b)\textbf{soporte D} := suppD = \{P \in \mathbb{P}_F | n_P \neq 0\}$$

OBSERVACIÓN: Cada $P \in \mathbb{P}_F$ puede ser visto como un divisor. Esto es:

$$P := \sum_{Q \in \mathbb{P}_F} n_Q Q;\ con\ n_Q = 0\ \forall Q \neq P,\ Q\ \in \mathbb{P}_F\ y\ n_P = 1, \quad (1.49)$$

Denotaremos como $< P >$ al lugar P visto como divisor. A este tipo de divisores les llamaremos, **divisores primos**. Además, la definición de $grado(D)$ es consistente con esta interpretación, esto es:

$$\begin{aligned} grado\ < P > &= \sum_{Q \in \mathbb{P}_F} v_Q Q \cdot grado\ Q \\ &= v_P\ grado\ P; \qquad \text{utilizando 1.49} \\ &= grado\ P \end{aligned}$$

Otra caracteristica de $\mathcal{D}_F$ es que existe un orden parcial en sus elementos:

$$D \leq D' \Longleftrightarrow n_P \leq n'_P\ \forall \in P \quad (1.50)$$

Divisores Principales

Ahora formaremos un divisor a partir de un elemento x de F. Asociaremos a cada lugar P la valoración $v_P(x)$ correspondiente y tomamos la suma formal. Uno de los objetivos de formar estos divisores, es poder controlar la información acerca de la cantidad de ceros y de polos de x. Formalmente se construyen como sigue:

sean $x \in F$, $Z := \{P \in \mathbb{P}_F | P \text{ es cero de } X\}$ y $N := \{P \in \mathbb{P}_F | P \text{ es polo de } X\}$ entonces definimos:

- el **divisor cero de** x:

$$\begin{aligned}(\mathbf{x})_\mathbf{0} &= v_{P_1}(x)P_1 + ... + v_{P_n}(x)P_n \\ &= \sum_{P \in Z} v_P(x)P,\end{aligned}$$

- y, el **divisor polo de** x**:**

$$\begin{aligned}(\mathbf{x})_\infty &= -v_{P'_1}(x)P'_1 - ... - v_{P'_n}(x)P'_n \\ &= \sum_{P' \in N} (-v_{P'})(x)P'\end{aligned}$$

y se considerará el siguiente divisor

$$(x) := (x)_0 - (x)_\infty,$$

el cual llamaremos **el divisor principal de** x y se observa que $(x)_0 \geq 0$ y $(x)_\infty \geq 0$. El divisor principal de $x \in F$ puede ser representado de la siguiente manera:

$$(\mathbf{x}) = \sum_{\mathbf{P} \in \mathbb{P}_\mathbf{F}} \mathbf{v_P(x)P}$$

Denotaremos $\mathcal{P}_F$, al conjunto que de los divisores principales de los elementos $x \neq 0 \in F$ y lo llamaremos como **grupo de divisores principales**.

> OBSERVACIÓN: los elementos de F que sean y constantes diferentes de cero, quedan caracterizados por $x \in K \Leftrightarrow (x) = 0$. Esta caracterización queda justificada por las propiedades de la valoración v_P.

Sean $x, y, \in F$ dos elementos diferentes de cero. Entonces, $(x), (y) \in \mathcal{P}_F$. Suman-

do estos divisores obtenemos:

$$\begin{aligned}(x)+(y) &= \sum_{P\in Z} v_P(x)P + \sum_{P\in Z} v_P(y)P \\ &= \sum_{P\in Z}[v_P(x)+v_P(y)]P \\ &= \sum_{P\in Z}[v_P(xy)]P \\ &= (xy)\end{aligned}$$

Es decir, la suma de los divisores principales es cerradura , por lo que $\mathcal{P}_F$ es un subgrupo de $\mathcal{D}_F$ y se puede tomar el siguiente grupo factor:

$$\mathcal{C}_F := \mathcal{D}_F/\mathcal{P}_F{}^5$$

Para cualquier $D \in \mathcal{D}_F$ el elemento correspondiente en el grupo $\mathcal{C}_F$ será la clase del divisor D y será denotada por $[D]$. Diremos que dos elementos son equivalentes si pertenecen a la misma clase, es decir, $D \sim D'$ si $[D] = [D']$ y esto es equivalente a decir que existe un divisor (x) tal que $D = D' + (x)$ con $x \neq 0$.

OBSERVACIÓN: La relación $\sim$ descrita en el párrafo anterior es de equivalencia: $\star$ $D \sim D$, pues $D = D + (x)$ con $x \in K$, es decir la relacion es reflexiva.
$\star$ Sean $D = \sum_{P\in\mathbb{P}_F} n_P P$, $D' = \sum_{P\in\mathbb{P}_F} n'_P P$, si $D \sim D'$ entonces existe $x \in F$ tal que $D = D' + (x)$, es decir:

$$\begin{aligned}
& \sum_{P\in\mathbb{P}_F} n_P P && = \sum_{P\in\mathbb{P}_F} n'_P P + (x) \\
\Rightarrow \quad & \sum_{P\in\mathbb{P}_F} n_P P && = \sum_{P\in\mathbb{P}_F} n'_P P + \sum_{P\in\mathbb{P}_F} v_P(x)P \\
\Rightarrow \quad & \sum_{P\in\mathbb{P}_F} n_P P - \sum_{P\in\mathbb{P}_F} v_P(x)P && = \sum_{P\in\mathbb{P}_F} n'_P P \\
\Rightarrow \quad & \sum_{P\in\mathbb{P}_F} n_P P + \sum_{P\in\mathbb{P}_F} (-v_P(x))P && = \sum_{P\in\mathbb{P}_F} n'_P P \\
\Rightarrow \quad & \sum_{P\in\mathbb{P}_F} n_P P + \sum_{P\in\mathbb{P}_F} (v_P(x^{-1}))P && = \sum_{P\in\mathbb{P}_F} n'_P P
\end{aligned}$$

[5] En algunos textos, este grupo es nombrado *grupo de Picard*.

Por lo que existe $y = x^{-1} \in F$ tal que $D' = D + (y)$, es decir, $D' \sim D$ y la relación es simétrica.
$\star$ Sean $D, D', D'' \in \mathcal{P}_F$ tales que $D \sim D'$ y $D' \sim D''$ entonces, $\exists\ x$ y $\exists\ y$ tales que $D = D' + (x)$ y $D' = D'' + (y)$. Sustituyendo se tiene $D = D'' + (x) + (y)$ y se sabe que $(x) + (y) = (xy)$, por lo que $D = D'' + (xy)$ es decir, $\exists\ z = xy \in F$ tal que $D \sim D''$ por lo que la relación es transitiva y con esto podemos concluir que "$\sim$"es una relación de equivalencia.

***Definición* 1.3.2.** *Sea $A \in \mathcal{D}_F$, definimos:*

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

Este conjunto es interpretado de la siguiente manera: si $A = \sum n_i P_i - \sum m_i Q_i$ entonces los elementos de $\mathcal{L}(A)$ pueden tener polos solamente en los lugares P_i de a lo menos orden n_i y deben tener ceros de al menos orden m_i en el lugar Q_i.

De la definición del conjunto podemos obtener la siguiente desigualdad con la que los elementos $x \in \mathcal{L}(A)$ quedan caracterizados:

$$v_P(x) \geq v_P(A)\ \forall\ P\ \mathbb{P}_F$$

De manera inversa, si $x \in F$ y $A \in \mathcal{D}_F$ y si se cumple que $v_P(x) \geq v_P(A)$ para todo lugar P, entonces, es natural que $x \in \mathcal{L}(A)$. En los siguientes párrafos se deducirán algunas propiedades de este conjunto.

Supongamos $x \neq 0$ es un elemento del conjunto $\mathcal{L}(A)$ y sea $(x) + A := A'$, como $(x) + A \geq 0$ entonces $\exists\ A' \in \mathcal{P}_F$ tal que $A \sim A'$. Por otro lado, si $A \sim A'$ con $A' \geq 0$, entonces existe $(x) \in \mathcal{P}_F$ tal que $A' = A + (x)$ por lo que $A + (x) \geq 0$, es decir, $\exists\ x \neq 0$ tal que $x \in \mathcal{L}(A)$ por lo que $\mathcal{L}(A) \neq 0$.

Si x y $y \in \mathcal{L}(A)$ y $a \in K$, entonces, para cualquier $P \in \mathbb{P}_F$ se cumplen las siguientes propiedades:

$$\begin{aligned} \star\ v_P(x+y) &\geq min\{v_P(x), v_P(y)\} \geq -v_P(A) \\ \star\ v_P(ax) &= v_P(a) + v_P(x) \geq -v_P(A) \end{aligned}$$

Por otro lado, si $A \sim A'$ entonces se tendrá que $\mathcal{L}(A) \sim \mathcal{L}(A')$. Tal afirmación se puede verificar tomando el siguiente mapeo:

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

Observamos que si $A \sim A'$, entonces, existe $(z) \neq 0$ tal que $A = A' + (z)$. Por otro lado, sabemos $(xz) = (x) + (z)$ y por la definición del conjunto $\mathcal{L}(A)$, tenemos que si $x \in \mathcal{L}(A)$ entonces, $(x) + A \geq 0$, así que:

$$\begin{aligned} & (x) + (z) + A' \geq 0 \\ \Rightarrow \quad & (xz) + A' \geq 0 \\ \Rightarrow \quad & xz \in \mathcal{L}(A') \end{aligned}$$

Con este hecho, afirmamos que $im\phi \subseteq \mathcal{L}(A')$. De forma análoga obtendremos que $im\phi' \subseteq \mathcal{L}(A')$ donde ϕ' queda definido de la siguiente manera:

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

Estos mapeos son inversos uno del otro, por lo tanto ϕ es un isomorfismo entre $\mathcal{L}(A)$ y $\mathcal{L}(A')$.

Un caso particular de éstos espacios es cuando se tiene $A = 0 \in \mathcal{D}_F$. Sea x un elemento en el conjunto $\mathcal{L}(A)$ entonces $(x) \geq 0$, lo cual quiere decir que x no tiene polos, así que $x \in K$, por lo que $\mathcal{L}(0) = K$.

Otro caso importante de mencionar es si $0 > A \in \mathcal{D}_F$.Como en el caso anterior, supondremos que existe algún elemento $0 \neq x \in \mathcal{L}(A)$, entonces:

$$\begin{aligned} & (x) + A \geq 0 \\ \Rightarrow \quad & (x) \geq -A > 0 \end{aligned}$$

es decir, $(x) > 0$ y x tendrá al menos un cero, pero no tendrá polos, lo cual es imposible. Por lo tanto, si $A < 0$ entonces $\mathcal{L}(A) = \{0\}$. Así las siguientes propiedades quedan demostradas:

a) $\mathcal{L}(A) \neq 0$ si y sólo si existe un divisor $A' \sim A$ con $A' \geq 0$.
b) $\mathcal{L}(A)$ es un espacio vectorial sobre K.
c) Si $A' \in \mathcal{D}_F$ es tal que $A' \sim A$ entonces $\mathcal{L}(A) \sim \mathcal{L}(A')$.
d) $\mathcal{L}(0) = K$.
e) Si $A < 0$ entonces $\mathcal{L}(A) = 0$.

Dado que $\mathcal{L}(A)$ es K-espacio vectorial, entonces podemos considerar su dimensión la cual demostraremos que es finita.

***Lema* 1.3.1.** *Sean A, B divisores de F/K tal que $A \leq B$. Entonces $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ y*

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

Demostración.
Sea $x \in \mathcal{L}(A)$, por definición sabemos que $v_P(x) \geq -v_P(A)$. Por otro lado, si $A \leq B$ entonces $v_P(A) \leq v_P(B)$ lo que implica $-v_P(A) \geq -v_P(B)$ por lo que $(x) \geq v_P(B)$ por lo que $x \in \mathcal{L}(B)$, es decir, $\mathcal{L}(A) \subseteq \mathcal{L}(B)$.

Como $A \leq B$, entonces existe $P \in \mathbb{P}_F$ tal que $B = A + P$. Sea $x \in \mathcal{L}(A)$ entonces $(x) + A \geq 0$. Por otro lado tenemos que

$$(x) + B = (x) + A + P \geq 0,$$

por lo que $x \in \mathcal{L}(B)$, así la primera parte del enunciado queda demostrada.

Por el teorema de aproximación existe $t \in F$ tal que

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

Luego, si $x \in \mathcal{L}(B)$, entonces

$$v_P(xt) = v_P(x) + v_P(t) = v_P(x) + v_P(A) + 1 \geq 0, \tag{1.55}$$

Además $xt \in O_P$, es decir, la función está definida en P. Obtenemos el siguiente mapeo:

$$\begin{array}{rccl} \psi: & \mathcal{L}(B) & \longrightarrow & F_P \\ & x & \longmapsto & (xt)(P) := xt + (P) \end{array}$$

Tenemos que $x \in nuc\ \psi$, pues $v_P(xt) > 0$ lo cual implica $v_P(x) \geq -v_P(A)$, es decir, $x \in \mathcal{L}(A)$. Así tenemos que:

$$i)\ Nuc\psi = \mathcal{L}(A) \text{ y}$$
$$ii)\ \psi \text{ induce al mapeo inyectivo de } \phi : \mathcal{L}(B)/\mathcal{L}(A) \longrightarrow F_P.$$

Por lo tanto:

$$dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq dim(F_P/K) = grado\ B - grado\ A.\diamondsuit \qquad (1.56)$$

***Proposición* 1.3.1.** *Sea $A \in \mathcal{D}_F$, entonces el espacio $\mathcal{L}(A)$ es de dimensión finita como espacio vectorial sobre K. Más aún, si $A = A_+ - A_-$ con A_+ y A_- con divisores positivos, entonces:*

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

Demostración.
Si se tiene que $A = A_+ - A_-$ donde A_+, A_- son dos divisores mayores a cero, entonces se tendrá que $A \leq A_+$ por lo que $\mathcal{L}(A) \subseteq \mathcal{L}(A)$. Esto quiere decir que la dimensión de $\mathcal{L}(A)$ estará acotada por la dimensión de $\mathcal{L}(A_+)$. Sabemos que $0 \leq A_+$ y por el lema anterior tenemos que:

$$\begin{aligned} dim(\mathcal{L}(A_+)/\mathcal{L}(0)) &\leq grado\ (A_+) - grado\ 0 \\ &= grado\ (A_+) \end{aligned}$$

Por otro lado tenemos que $\mathcal{L}(0) = K$ por lo que $dim\mathcal{L}(0)) = 1$, así:

$$\begin{aligned} dim(\mathcal{L}(A_+)/\mathcal{L}(0)) &= dim\mathcal{L}(A_+) - dim\mathcal{L}(0) \\ &= dim\mathcal{L}(A_+) - 1 \end{aligned}$$

Por lo que, haciendo las correspondientes sustituciones en las desigualdades obtenidas,

$$dim(\mathcal{L}(A_+)/\mathcal{L}(0)) = dim(\mathcal{L}(A)) - 1 \leq grado\ (A_+),$$

es decir:

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

Queda demostrado que dim $\mathcal{L}(A)$ es un espacio vectorial de dimensión finita sobre K.

Definición* 1.3.3.** *Sea $A \in \mathcal{D}_F$,* ***la dimensión de *A, será $dim_k(\mathcal{L}(A))$*

Es decir, la dimensión de un divisor A, será la dimensión del espacio $\mathcal{L}(A)$. El cálculo de esta dimensión representa uno de los problemas fundamentales en la **teoría algebraica de funciones**. En la siguiente sección, veremos que el Teorema de Riemann-Roch es de gran utilidad para la solución de este problema.

El siguiente teorema es significativo pues además de describir el grado de un divisor principal, está diciendo que toda función $x \in F - K$ tiene tantos ceros como polos.

***Teorema* 1.3.1.** *Todo divisor principal tiene grado cero. Además, si $x \in F - K$ entonces*

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

Demostración.
Sea $n = [F : K(x)]$. Sea $B = (x)_\infty = -\sum_{i=1}^{r} v_{P_i}(x)P_i$, donde P_i denota los polos de x. Tenemos que

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

Queda por ver que $n \leq grado\ B$. Para verificar esto, seleccionaremos una base $\{u_1, .., u_n\}$ para F/K. Sea $C \in \mathcal{D}_F$ tal que $(u_i) + C \geq 0$ para $i = 1, ..., n$, es decir C es un divisor tal que $u_i \in \mathcal{L}(C))$ para $i = 1, ..., n$. Sea $\eta \geq 0$, entonces $x^i u_j \in \mathcal{L}(\eta B + C)$ para $0 \leq i \leq \eta$. Las funciones $u_i x^j$ son linealmente independientes sobre K pues las u_i forman un conjunto linealmente independiente sobre $K(x)$ y sobre K. Observamos que el índice j está acotado por η, es decir, existen $\eta + 1$ posiblidades de elección para j, por lo que:

$$n(\eta + 1) \leq dim(\eta B + C).$$

Sea $C := grado\ C$, entonces,

$$\begin{array}{lcll} & n(\eta+1) \leq dim(\eta B + C) & \leq grado\ (\eta B + C) + 1 & \\ \Rightarrow & n(\eta+1) \leq dim(\eta B + C) & \leq \eta grado\ (B + C) + 1 & \\ \Rightarrow & n\eta + n & \leq \eta grado\ (B) + C + 1 & \\ \Rightarrow & n - C - 1 & \leq \eta grado\ (B) - n & \forall \eta \geq 0 \end{array}$$

Si $(grado\ (B)-n) < 0$, entonces $\eta(grado\ (B)-n) < n-C-1$ para alguna $\eta > 0$. Por lo tanto $(grado\ (B)-n) \geq 0$ y $grado\ B \geq n$. Queda demostrado que

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

Además, como $(x)_0 = (x^{-1})_\infty$ entonces $grado\ ((x)_0) = grado\ ((x^{-1})_\infty) = [F : K(x)] = [F : K(x^{-1})]$, por lo que la función tiene el mismo número de ceros que de polos. $\diamondsuit$

***Corolario* 1.3.1.** *Sean $A, A' \in \mathcal{D}_F$,*

a) Si A' y A son tales que $mathcal L(A) \sim \mathcal{L}(A')$, entonces:

$$dim(A) = dim(A'),\ y\ grado\ A = grado\ A'.$$

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

c) Dado $A \in \mathcal{D}_F$, tal que $grado\ A = 0$, las siguientes proposiciones son equivalentes:

1) A es principal.

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

3) $dim(A) = 1$.

Demostración.

a) Tenemos que $dim(A) = dim(A')$ pues $\mathcal{L}(A) \cong \mathcal{L}(A') = \mathcal{L}(A + (x))$. Así pues:
$grado\ A' = grado\ (A + (x)) = grado\ (A) + 0$, es decir $grado\ A' = grado\ A$.

b) Si $dim(A) > 0$ entonces $\exists 0 \neq x \in \mathcal{L}(A)$.
Sea $A' = A + (x) \geq 0$, es decir, $A \sim A'$ pero $grado\ A' \geq 0$, lo cual genera una contradicción, por lo tanto $dim(A) = 0$.

c) (1) $\Leftrightarrow$ (2) Sea $A = (x), x \in F - K$. Entonces $x^{-1} \in \mathcal{L}(A)$, pero $(x)^{-1} = -(x)$, de donde $-(x) + A = -(x) + (x) = 0$ por lo tanto $dim(A) \geq 1$.
(2) $\Leftrightarrow$ (3) Supongamos que $dim(A) \geq 1$ y $grado\ A = 0$, $dim(A) \leq grado\ (A) + 1$, por lo tanto $dim(A) = 1$.
(3) $\Leftrightarrow$ (1): Supongamos que el $grado\ A = 0$ y $dim(A) = 1$. Se deberá

demostrar que A es principal.
Sea $z \in \mathcal{L}(A),\ z \neq 0$, entonces $(z) + A \geq 0$. Entonces:

$$\begin{aligned} & grado\ ((z) + A) && = 0 \\ \Rightarrow \quad & (z) + A && = 0 \\ \Rightarrow \quad & A && = -(z) \\ \Rightarrow \quad & A && = (z)^{-1}.\diamondsuit \end{aligned}$$

Con la finalidad de estudiar la dimensión del divisor A estableceremos cotas. Primero damos una cota inferior.

OBSERVACIÓN: Si $A \leq A_1$ entonces

$$grado\ A - dim(A) \leq grado\ A_1 - dim A_1.$$

Esta afirmación la podemos verificar de la siguiente manera: sea $B = (x)_\infty$, entonces para toda $\eta \geq 0$ tenemos

$$dim(\eta B + C) \geq (\eta + 1) grado\ B)$$

además:

$$\begin{aligned} dim(\eta B + C) &\leq grado\ (\eta B + C) + 1 + grado\ (C) + 1 \\ &\leq dim(\eta B) + grado\ (C). \end{aligned}$$

Luego,

$$\begin{aligned} \eta + 1 grado\ B &\leq dim(\eta B + C) \\ &\leq dim(\eta B) + grado\ C \end{aligned}$$

de donde:

$$\begin{aligned} & grado\ (\eta B) + grado\ B \leq dim(\eta B) + grado\ C, \\ \Rightarrow \quad & grado\ (\eta B) + grado\ B - grado\ C \leq dim(\eta B), \\ \Rightarrow \quad & grado\ (\eta B) + [F : K(x)] - grado\ C \leq dim(\eta B), \end{aligned}$$

y se cumplirá para toda $\eta \in \mathbb{N} - 0$.

Utilizando la notación de la observación anterior, sea $\{u_1, ..., u_n\}$ una base para $F/K(x)$y sea $\gamma = n - grado\ C$, es decir, γ no depende de ηB, sino de $F/K(x)$, podemos afirmar que *dado* $A \in \mathcal{D}_F$ *existen dos divisores* A_1, D *y un entero* $\eta \geq 0$

tal que $A \leq A_1$, $A_1 \sim D$ *y* $D \leq \eta B$. RAZÓN: Sea $A_1 \geq A$ tal que $A_1 \geq 0$ entonces:

$$\begin{aligned} dim(\eta B - A_1) &\geq dim(\eta B) - grado\ (A_1) \\ &\geq grado\ (\eta B) - \gamma - grado\ (A_1) \\ &\geq 0, \end{aligned}$$

para alguna $\eta > 0$. Por otro lado, existe $z \in \mathcal{L}(\eta B - A_1)$ con $(z) + \eta B - A_1 \geq 0$, por lo que:

$$\eta B \geq A_1 - (z) \sim A_1 \sim D$$

es decir $A_1 - (z)$.
Retomando la intención de proponer una cota inferior para $dimA$, tenemos que:

$$\begin{aligned} grado\ A - dimA &\leq grado\ (A_1) - dim(A_1) \\ &= grado\ D - dimD \\ &\leq grado\ (\eta B) - dim(\eta B) \\ &\leq \gamma. \end{aligned}$$

Siendo así, podemos enunciar la siguiente proposición cuya demostración consta de los párrafos anteriores.

***Proposición* 1.3.2.** *Existe alguna constante* $\gamma \in \mathbb{Z}$ *tal que* $\forall\ A \in \mathcal{D}_F$ *se tiene:*

$$deg\ A\ -\ dim\ A \leq \gamma.$$

***Definición* 1.3.4.** *El género de* F/K *es definido por :*

$$g := max\{deg\ A - dim\ A + 1 | A \in \mathcal{D}_F\}.$$

OBSERVACIÓN:El género deF/K es un entero no negativo y se sigue del hecho de que si tomamos $A = 0$ entonces $deg\ 0 - dim\ 0 + 1 = 0$.

Teorema de Riemann

***Teorema* 1.3.2.** *Sea F/K un campo de funciones de género g:*

1) Para toda $D \in \mathcal{D}_F$,

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

2) Existe $c \in \mathbb{Z}$ que depende de F/K tal que

$$dim(A) \geq grado\ (A) + 1 - g \text{ si } grado\ (A) \geq c.$$

Demostración.

1) Sea $A \in \mathcal{D}_F$, entonces $g \geq grado\ (A) - dim(A) + 1$ por lo que:
$$dim(A) \geq grado\ (A) + 1 - g.$$

2) Existe $A_0 \in \mathcal{D}_F$ tal que $g = grado\ (A_0) + dim(A_0 + 1)$. Sea $c := grado\ (A_0) + g$ lo que implica que $grado\ (A_0 = c - g)$. Sabemos que

$$\begin{aligned} dim(A - A_0) &\geq grado\ (A - A_0) + 1 - g \\ &= grado\ (A) - grado\ (A_0 + 1 - g) \\ &\geq c - grado\ (A_0 + 1 - g). \end{aligned}$$

Entonces existe un elemento z diferente de cero, $z \in \mathcal{L}(A - A_0$ tal que

$$(z) + A - A_0 \geq 0 \Rightarrow (z) + A \geq A_0.$$

Sea $A \sim A'$, por lo que $grado\ A' \geq c, A' \geq A$, así

$$\begin{aligned} grado\ A - dim(A) &= grado\ A' - dimA' \\ &\geq grado\ A_0 - dim(A_0) \\ &= c - g - (c - g + 1 - g) \\ &= g - 1. \end{aligned}$$

Por lo tanto, grado $A + 1 - g \geq dim(A)$ por lo cual $dim(A) = grado\ A + 1 - g$.$\diamondsuit$

> OBSERVACIÓN: **El campo $K(x)$ tiene género cero:** Supongamos que tiene $g \geq 0$. Sabemos que las funciones: $1, x, ...x^n \in \mathcal{L}(rp)$. Entonces: $r + 1 \leq dim(rp) = grado\ (rp) + 1 - g$ para $r > 0$. Entonces $g = 0$.

De ahora en adelante el campo de funciones F/K, tendrá género g.

1.4 Teorema de Riemann-Roch

El propósito de esta sección es enunciar y demostrar el teorema de Riemann-Roch.Durante esta sección g denotará el género de F/K.

***Definición* 1.4.1.** *Un* adele *de F/K será un mapeo α tal que:*

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

*tal que $\alpha_P \in \mathcal{O}_P$, excepto en un número finito de lugares. Denotamos como $\mathcal{A}_F$ al conjunto de los adeles de F/K, es decir, $\mathcal{A}_F = \{\alpha | \alpha$ es un adele de $F/K\}$. Además, si $x \in F$ diremos que **el adele principal de** x es el adele de F cuyas componentes son todas iguales a x.*

Dado que $\mathcal{A}_F$ se puede ver como espacio vectorial sobre K y sobre F, podemos hablar de $dim(\mathcal{A}_F/\mathcal{A}_F(A)+F)$, tomando a F como el conjunto de adeles principales. Si para cada $A \in \mathcal{D}_F$ de F/K se da la siguiente relación:

$$dimA - gradoA + g - 1 = dim(\mathcal{A}_F/(\mathcal{A}_F(A)+F)) \tag{1.58}$$

de la cual obtenemos, haciendo $A = 0$, otra caracterización para g:

$$\begin{aligned} dim(0) - deg(0) + g - 1 = 1 - 0 + g - 1 = g \\ \Rightarrow g = dim(\mathcal{A}_F/(\mathcal{A}_F(0)+F)). \end{aligned} \tag{1.59}$$

Al lado izquierdo de la igualdad (1.58) la llamaremos *índice de especialidad del divisor A* y lo denotaremos como $i(A)$. La demostración de la igualdad (1.58) se sigue de los siguientes hechos:

a) Si $A_1, A_2 \in \mathcal{D}_F$ y $A_1 \leq A_2$, entonces $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$.
Si $\alpha \in \mathcal{A}_F(A_1)$ entonces $v_P(\alpha) \geq -v_P(A_1) \geq v_P(A_2)$, pues $A_1 \leq A_2$, por lo tanto, $\mathcal{A}_F(A_1) \leq \mathcal{A}_F(A_2)$.

b) Si $A_1, A_2 \in \mathcal{D}_F$ entonces $dim((\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1 + F)) = (degA_2 - dimA_1) - (degA_1 - dimA_1)$.
Para confirmar el enunciado es necesario considerar la sigueinte cadena exacta:

$$0 \longrightarrow \mathcal{L}(A_2)/\mathcal{L}(A_1) \xrightarrow{\sigma_1} \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) \xrightarrow{\sigma_2}$$

$$\xrightarrow{\sigma_2} ((\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F) \longrightarrow 0$$

Tenemos que $nuc(\sigma_2) \subseteq Im(\sigma_1)$ pues si $\alpha \in \mathcal{A}_F(A_2)$ tal que $\sigma_2(\alpha + adeles(A_1)) = 0$ entonces existe $x \in F$ tal que $\alpha - x \in \mathcal{A}_F(A_1)$. Como $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ tenemos que $x \in \mathcal{A}_F(A_2) \cap F = \mathcal{L}(A_2)$, por lo que

$$\alpha + \mathcal{A}_F(A_1) = x + \mathcal{A}_F(A_1) = \sigma(x + \mathcal{L}(A_2)).$$

Por la exactitud de la cadena:

$$dim(\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F)) = dim(\mathcal{A}_F(A_2))/(\mathcal{A}_F(A_1)) - dim(\mathcal{L}(A_1)/\mathcal{L}(A_2)).$$

El teorema de aproximación, nos permite escoger una $t \in F$ tal que $v_P(t) = v_P(A_1) + 1$. Si consideramos el siguiente mapeo, donde $A_1 \leq A_2$,

$$\begin{aligned} \phi : \ \mathcal{A}_F(A_2) &\longrightarrow F_P, \\ \alpha &\longmapsto (t\alpha_P)(P) \end{aligned}$$

podemos observar que $Im\phi = F_P$ por lo que es mapero suprayectivo que tiene como núcleo a $\alpha(A_1)$ por lo que:

$$\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \cong F_P, \text{ de ésta manera:}$$
$$dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) = [F_P : K] = grapoP = gradoA_2 - gradoA_1$$

por lo que

$$\begin{aligned} dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) &= (degA_2 - degA_1) - (dimA_2 - dimA_1) \\ &= (degA_2 - dimA_1) - (degA_1 - dimA_1). \end{aligned}$$

c) Si $B \in \mathcal{D}_F$ tal que $dim(B) = grado(B) + 1 - g$, entonces $\mathcal{A}_F = \mathcal{A}_F(B) + F$. Si $B_1 \geq B$ entonces

$$dimB_1 \leq grado(B_1) + dim(B) - grado(B) = grado(B_1) + 1 - g.$$

Por otro lado, $dim(B_1) = gradoB_1 + 1 - g$ por el teorema de Riemann por lo que $dim(B_1) = grado(B_1) + 1 - g$ para toda $B_1 \leq B$. Sean $\alpha \in \mathcal{A}_F$ y $B_1 \in \mathcal{D}_F$ tal que $B_1 \leq B$ y $\alpha \in \mathcal{A}_F(B_1)$ y por el inciso anterior se tiene que:

$$dim(\mathcal{A}_F(B_1) + F/\mathcal{A}_F(B) + F) = gradoB_1 - dimB_1 - gradoB - dimB = 0$$

por lo que $\mathcal{A}_F(B_1) + F = \mathcal{A}_F(B) + F$. Como $\alpha \in \mathcal{A}_F(B_1)$ se sigue que $\alpha \in \mathcal{A}_F(B) + F$.

d) Por último, sea $A \in \mathcal{D}_F$, por el teorema de Riemann, $\exists\ A_1 \geq A$ tal que $dim(A_1) = grad(A_1) + 1 - g$ entonces $\mathcal{A}_F(A_1) + F = \mathcal{A}_F$, de donde:

$$\begin{aligned} dim(\mathcal{A}_F/(\mathcal{A}_F(A_1) + F) &= dim(\mathcal{A}_F(A_1) + F/(\mathcal{A}_F(A) + F) \qquad (1.60) \\ &= gradoA_1 - dimA_1 - gradoA + dimA \\ &= (g-1) + dim(A) - grado(A) \\ &= i(A). \end{aligned}$$

Definimos un **diferencial de Weil** como un mapeo lineal $\omega : \mathcal{A}_F \mapsto K$ que se anula en $\mathcal{A}_F(A) + F$ para algún $A \in \mathcal{D}_F$. Denotamos como $\Omega_F\ \mathcal{P}_F$ al conjunto de todos los diferenciales de Weil ω del campo F/K. Para un divisor A, denotaremos como $\Omega_F(A)$ al conjunto de los diferenciales de Weil tales que se anulan en $\mathcal{A}_F(A) + F$.

Existe un isomorfismo entre el espacio de formas lineales $\mathcal{A}_F/\mathcal{A}_F(A_1) + F$ y el espacio $\Omega_F(A)$. De párrafos anteriores tenermos que el espacio $\mathcal{A}_F/\mathcal{A}_F(A_1) + F$ es de dimensión finita igual a $i(A)$ por lo que $dim\Omega_F(A) = i(A)$. Para $x \in F$ y $\omega \in \Omega_F$ podemos definir $x\omega : \mathcal{A}_F :\mapsto K$ dado por $(x\omega)(\alpha) := \omega(x\alpha)$. Este mapeo $(x\omega)$ vuelve a ser un elemento de Ω_F pues para $\omega \in \Omega_F \exists A \in \mathcal{D}_F$ tal que ω se anula en $\mathcal{A}_F(A + (x)) + F$. Este mapeo proporciona la estructura a Ω_F de espacio vectorial sobre F.

***Proposición* 1.4.1.** *Ω_F es un espacio vectorial de dimensión 1 sobre F.*

Demostración.
Sea $\omega \in \Omega_F, \omega \neq 0$. Se tendrá que demostrar que para todo ω_2 de Ω_F, existe $t \in F$ tal que $\omega_2 = t\omega_1$. Suponemos que $\omega_2 \neq 0$ y sean A_1 y A_2 divisores tales que $\omega_1 \in \Omega_F(A_1)$ y $\omega_2 \in \Omega_F(A_2)$ y $B \in \mathcal{D}_F$ tal que:

$$dim(A_i + B) = grado(A_1 + B) + 1 - g, \text{ con } i = 1, 2.$$

la veracidad de ésta ecuación depende directamente de la elección de B y es posible gracias al teorema de Riemann de la sección pasada. También sabemos que en general dados $U_1, U_2 \leq V$, $V - espacios\ vectoriales$,

$$dim(U_1 \cap U_2) \geq dimU1 + dimU_2 - dim - V.$$

Definimos $\varphi_i : \mathcal{L}(A_i + B) \longrightarrow \Omega_F(-B)$ dado por $x \longmapsto x\omega_i$, con $i = 1, 2$. Sea $U_i = \varphi(\mathcal{L}(A_i + B) \subseteq \Omega_F(-B))$ como

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

Obtenemos que:

$$\begin{aligned} dim(U_1) + dim(U_2) - dim(\Omega_F(-B)) &= dim(U_1) + dim(U_2) - grado - g + 1 \\ &= dim(A + B) + dim(A_2 + B) - gradoB - g + 1 \\ &= dim(A_1 + B) + 1 - g + dim(A_2 + B) + 1 - g - gradoB + 1 - g \\ &= gradoB + (gradoA_1 + gradoA_2) + 3(1 - g) \quad (1.61) \end{aligned}$$

del término (1.62) observamos que sólamente $gradoB$ depende de B. Entonces si $gradoB$ es suficientemente grande:

$$dim(U_1 \cap U_2) \geq dimU1 + dimU_2 - dim - (\Omega_F(-B)) > 0.$$

Se sigue que $U_1 \cap U_2 \neq \{0\}$ y queda demostrado nuestro enunciado. $\diamondsuit$

***Lema* 1.4.1.** *Sea* $0 \neq \omega \in \Omega_F$ *y sea* $M(\omega) := \{A \in \mathcal{D}_F | \omega$ *se anula en* $\mathcal{A}_F(A) + F\}$, *entonces existe un único divisor* $W \in M(\omega)$, *tal que* $A \leq W$, *para cualquier* $A \in M(\omega)$.

Demostración.
Utilizando el teorema de Riemann, tenemos que existe una constante c que sólo depende del campo F/K con la propiedad de que $i(A) = 0\ \forall A \in \mathcal{D}_F$ de grado mayor o igual a c. Como $dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)) = i(A)$. Tenemos que el $gradoA < c\ \forall\ lA \in M(\omega)$, entonces podemos escoges un divisor $W \in M(\omega)$ de grado maximal.

Supongamos que W no es único. Entonces existe por lo menos algún divisor $A_0 \in M(\omega)$ con $A_0 \leq W$, es decir $v_Q(A_0) > v_Q(W)$ para alguna $Q \in \mathbb{P}_F$. Tendríamos que $M + Q \in M(W)$ pero esto contradice la condición de ser de grado maximal.

Por otro lado si consideramos un adele $\alpha = (\alpha_P) \in \mathcal{A}_F(W + Q)$ lo podemos reescribir como $\alpha = \alpha' + \alpha''$ con:

$$\alpha'_P := \begin{cases} \alpha_P & \text{para } P \neq Q. \\ 0 & \text{para } P = Q. \end{cases}$$

y

$$\alpha''_P := \begin{cases} 0 & \text{para } P \neq Q. \\ \alpha_P & \text{para } P = Q. \end{cases}$$

por lo que $\alpha' \in \mathcal{A}_F(W)$ y $\alpha'' \in \mathcal{A}_F(A_0)$ y $\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0$, entonces ω se anula en $\mathcal{A}_F(\omega + Q) + F$.$\diamondsuit$

Llamaremos a (ω) **el divisor de un diferencial de Weil**, si $\omega \neq 0$ y es aquél que es único y queda determinado por las siguientes condiciones: a)ω se anula en $\mathcal{A}_F((\omega) + F)$. b)Si ω se anula en $\mathcal{A}_F(A) + F$, entonces $A \leq (\omega)$.

Para $o \neq \omega \in \Omega_F$ y $P \in \mathbb{P}_F$, definimos $v_P(\omega) := v_P((\omega))$. De asta manera podemos decir que P es un cero (polo resp.) de ω si $v_P(\omega) > 0$, $(v_P(\omega) < 0)$. Además, si $v_P(\omega) \geq 0$ diremos que ω *es regular en* P. Si ω es regular en todos $P \in \mathbb{P}_F$ decimos que ω es regular.

Definición* 1.4.2.** *Un divisor $\Omega \in \mathcal{D}_F$ es* ***canónico *si $W = (\omega)$, para algún $\omega \in \Omega_F$.*

Observación: De la definición:

$$\Omega_F(A) = \{\omega \in \Omega_F | \omega = 0 \text{ ó } (\omega) \geq 0\}$$
$$\textit{por lo que} \quad \Omega_F(W) = \{\omega \in \Omega_F | \omega \textit{ es regular}\}$$

y como consecuencia de párrafos anteriores tenemos que: $dim\Omega_F(0) = g$.

***Proposición* 1.4.2.** *Sea* $0 \neq x \in F$ *y* $0 \neq \omega \in \Omega_F$, *entonces* $(x\omega) = (x) + (\omega)$.

Demostración.
Si ω se anula en $\Omega_F(A) + F$ entonces $x\omega$ se anula en $\Omega_F(A + (x)) + F$ por lo que $(x) + (\omega) \leq (x\omega)$. De forma análoga $(x\omega) + (x^{-1}) \leq (x^{-1}x\omega) = (\omega)$ por lo que implica $(\omega) + (x) \leq (x\omega) \leq (x) + (\omega) \Rightarrow (x) + (\omega) = (x\omega)$.$\diamondsuit$

Si se tienen W_1, W_2 divisores canónicos entonces $\omega_1 = (\omega_1)$ y $\omega_2 = (\omega_2)$. Por otro lado hemos demostrado que Ω_F tiene dimensión 1 sobre F, es decir, $\omega_2 = x\omega_1$, $x \in F$ por lo que $\omega_2 = (x\omega_1)$, lo que implica, usando la proposicón anterior que: $W_2 = (x) + (\omega) =)(x) + \omega_1$, entonces se tiene que W_1 y W_2 tienen el mismo grado y misma dimensión. Esto nos permite afirmar que los divisores canónicos forman una clase de divisores.

***Teorema* 1.4.1.** *Sea* $A \in \mathcal{D}_F$ *y* $W = (\omega)$ *y sea*

$$\begin{aligned} \eta : \mathcal{L}(W - A) &\longrightarrow \Omega_F(A) \\ x &\longmapsto x\omega \end{aligned}$$

Entonces, η *es un isomorfismo de espacios vectoriales.*

Demostración.
Sea $x \in \mathcal{L}(W - A)$ tenemos que $(x\omega) = (x) + (\omega) \geq -(W - A) + W = A$ pues $x\omega \in \Omega(A)$. Por lo que $Im(\eta) \leq \Omega(A)$. El mapeo Ω_F es lineal y si $c \in K$ entonces $c\eta(x) = cx\omega = \eta(cx\omega)$ y $\eta(x + y) = \omega(x + y) = \omega x + \omega y = \eta(x) + \omega(y)$. Además η es inyectiva pues $nuc(\eta) = 0 \in \mathcal{L}(A)$ y si $\omega_1 \in \mathcal{L}(A)$ $\exists$ x inF tal que $\omega_1 = x\omega$ entonces $\omega_1 = (x\omega) = (x)+(\omega) = A \Rightarrow (x)+W-A \geq 0$ por lo que $x \in \mathcal{L}(W-A)$, entonces, $\eta(x) = x\omega = \omega$, es decir, η es biyectiva. $\diamondsuit$

Teorema de Riemann-Roch

***Teorema* 1.4.2.** *Sea* $A \in \mathcal{D}_F$ *y* W *un divisor canónico de* F/K. *Entonces*

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

Demostración.
La demostración de este teorema se sigue de la definición de (1.58) y del teorema anterior. $\diamondsuit$

Observación: Si W es un divisor canónico de F/K, entonces,

$$grado(W) = 2g - 2 \text{ y } dim(W) = 0.$$

Esto se sigue del hecho de que si hacemos $A = 0$ entonces

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

por lo que $1 = 1 - g + dim(W)$ lo que implica que $dim(W) = g$. Por otro lado haciendo $A = W$ entonces $g = grado(W) + 1 - g + 1$, así $2g - 2 = grado(W)$.

1.5 Extensiones de campos de funciones algebraicos

Definición 1.5.1. *Diremos que un campo de funciones F'/K' es* extensión algebraica de F/K *si $F' \geq F$ es algebraica y $K' \geq K$. Llamaremos a F'/K' una* extensión de constantes sobre F/K *si $F' = FK' = \{z \cdot a | z \in F,\ a \in K\}$. La extensión $F'/K' \supseteq F/K$ se dice* finita *si $[F' : F] < \infty$.*

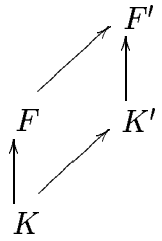


Figura 1.2: *Extensiones de Campos.*

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

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

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

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

Demostración.

a) Por hipótesis sabemos que para todo elemento β en F', podemos encontrar un polinomio en $F[x]$ para el cual β es raíz. En particular, si $\beta \in K'$ se puede encontrar un polinomio $f(x)$ en $F[x]$ para el cual β es raíz. Por otro lado, sabemos que $f(x)$ puede escribirse como:

$$f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n + ...$$

donde $a_i \in F$ y $a_i = 0$ excepto para un número finito de valores de i. Ahora supondremos que $f(x) \notin K[x]$, es decir, $f(x)$ tiene por lo menos un coeficiente el cual no se encuentra en el campo K. Supongamos que ese coeficiente es el a_i, entonces tenemos la siguiente igualdad:

$$a_i \beta^i = a_0 + a_1 \beta + a_2 \beta^2 + ... + a_n x^n + ...$$

donde el lado izquierdo pertenece a $F - K$ pero el derecho no, por lo que llegamos a una contradicción, es decir, $f(x) \in K[x]$ por lo que K' es algebraica sobre K.
Para verificar la segunda parte de este lema, suponemos que $\alpha \in F \cap K'$. Claramente $\alpha \in K$, por lo que $F \cap K' \subset K$. Por otro lado, si $\alpha \in K$ entonces $\alpha \in F \cap K'$.

b) Si asumimos que F'/K' es una extensión finita de F/K entonces F' puede ser considerado como un campo de funciones algebraicas sobre K con su campo de constantes K' por lo que se tiene que $[K' : K] < \infty$.
Ahora suponemos $[K' : K] < \infty$. Sea $x \in F - K$ entonces $F'/K(x)$ es una extensión finita (pues x es trascendental sobre K') y

$$[K'(x) : K(x)] < [K' : K] < \infty.$$

Luego,

$$[F' : K(x)] = [F' : K'(x)] \cdot [K'(x) : K(x)] < \infty,$$

Como $K(x) \subseteq F \subseteq F'$ esto implica que $[F' : F]$. $\diamondsuit$

***Definición* 1.5.2.** *Consideremos la estensión F'/K' sobre F/K. Decimos que el lugar $P' \in \mathbb{P}_{F'}$ está* sobre *$P \in \mathbb{P}_F$ si $P \subseteq P'$. También diremos que P' es extensión de P y escribimos $P'|P$.*

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

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

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

$$\begin{aligned} v_P(u^r t) &= r v_P(u) + v_P t = 1 \\ v_{P'}(u^r t) &= r v_{P'}(u) + v_{P'} t \leq -r + r = 0 \end{aligned} \tag{1.67}$$

pues u no pertenece a $O_{P'}$. Entonces $u^r t \in P$ pero $u^r t \notin P'$ por lo que se tiene una contradicción al hecho de que $P \subseteq P'$. Entonces $O_P \subseteq O_{P'}$.

Ahora supongamos que $O_P \subseteq O_{P'}$. Si $y \in P$ entonces, $y^{-1} \notin O_P$ por lo que $y^{-1} \notin O_{P'}$, entonces $y = (y-1)-1 \in P'$ por lo tanto, $P \subseteq P'$ por lo que P' está sobre P.

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

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

Por lo que la segunda afirmación implica la tercera.

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

OBSERVACIÓN: Bajo las hipótesis de la proposición anterior, se tiene que

$$O_P = F \cap O_{P'} \text{ y } P = F \cap P'$$

Por ser una intersección finita de anillos, tenemos que $F \cap O_{P'}$ es un subanillo de F. Por otro lado $O_P \subseteq F$ y $O_P \subseteq O_{P'}$ por lo que $O_P \subseteq F \cap O_{P'}$ y además O_P es un subanillo maximal, así $F = F \cap O_{P'}$ ó $O_P = F \cap O_{P'}$. Supongamos que $F = F \cap O_{P'}$, así $F \subseteq O_{P'}$. Sea $z \in F' \emptyset_{P'}$. Por ser F' una extensión algebraica de F sabemos que existen $a_0, ..., a_m \in F$ tales que:

$$a_n z^n + ... + a_1 z + a_0 = 0 \tag{1.69}$$

Tenemos que para $r = 0, ..., n-1$ se cumple que $v_{P'}(z^n) = n v_{P'(z)} < r v_{P'}(z)$, (recordemos que si $z \notin O_{P'}$ entonces $v_{P'}(z) < 0$). Luego, utilizando la desigualdad del triángulo:

$$v_{P'}(a_n z^n + ... + a_1 z + a_0) = n v_{P'(z)} \neq v_{P'}(0) = \infty.$$

Por lo que no existen escalares tales que 1.69 se cumpla. Así que $O_P = F \cap O_{P'}$. La otra parte de nuestra afirmación es más sencilla de verificar, basta suponer un elemento $x \in P$, es decir, la valoración en P es mayor estrictamente a cero. Luego, por la proposición anterior existe un entero $e > 0$ tal que $v'_P(x) = e v_P(x) > 0$, por lo que x pertenece al ideal P', es decir, $x \in P' \cap F$. Por otro lado, si $x \in P' \cap F$ entonces $v_{P'}(x) = e v_P(x) > 0$ para algún entero $e > 0$ por lo que $v_P(x) > 0$ entonces x pertence a P. Por lo tanto $P = P' \cap F$.

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

1) *Al entero asociado a la igualdad $v_{P'}(x) = e v_P(x)$ de la preposición anterior le llamaremos* ***índice de ramificación de P' sobre P*** *y se le denotará como $e(P'|P)$.*
2) *Diremos que $P|P'$ es remificado si $e(P'|P) > 1$. Si $e(P'|P) = 1$, diremos que $P|P'$ no es ramificado.*
3) *Llamaremos* ***grado relativo de*** *$P'|P$ a $f(P'|P) := [F_P : F_{P'}]$.*

***Proposición* 1.5.2.** *Sea F'/K' una extensión sobre F/K y $P' \in \mathbb{P}_{F'}$ un lugar sobre $P \in \mathbb{P}_F$. Entonces:*

a) $f(P'|P) < \infty \Leftrightarrow [F' : F] < \infty$
b) Si F''/K'' es una extensión de F'/K' y P'' un lugar sobre $P' \in \mathbb{P}_{F'}$, entonces:

$$\star \quad e(P''|P) = e(P'|P) \cdot e(P''|P')$$
$$\star \quad f(P''|P) = f(P'|P) \cdot f(P''|P')$$

Demostración.
a) Se tienen las siguientes contenciones:

$$K \subseteq F_P \subseteq F'_{P'} \text{ y } K \subseteq K' \subseteq F'_{P'}$$

donde $[F_P : K] < \infty$ y $[F_{P'} : K'] < \infty$, entonces:

$$[F'_{P'} : K] = [F'_{P'} : F_P][F_P : K] \text{ y } [F'_{P'} : K] = [F'_{P'} : K'][K' : K]$$

por lo que:

$$[F'_{P'} : F_P][F_P : K] = [F'_{P'} : K'][K' : K]$$

Así, $[F'_{P'} : F_P] < \infty \Leftrightarrow [K' : K]$ y esto último sucede si y solamente si $[F' : F] < \infty$.

b)Por la proposición 1.5.1 se tiene que existen dos enteros $e_1,\ e_2$ tales que $v_{P''}(x) = e_1 v_{P'}(x)$ y $v_{P'}(x) = e_2 v_P(x)$, luego:

$$v_{P''}(x) = e_1 v_{P'}(x) = e_1 e_2 v_P(x),$$

por lo que $e(P''|P) = e_1(P''|P')e_2(P''|P)$. Además se tiene que $F_P \subseteq F'_{P'} \subseteq F''_{P''}$, por lo que $f(P''|P) = f(P'|P) \cdot f(P''|P')$ $\diamondsuit$

***Proposición* 1.5.3.** *Sea F'/K' una extensión de F/K. Entonces*

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

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

Demostración.

a) Para la demostración de esta proposición es importante verificar el siguiente hecho:

$$F \cap P' \neq \emptyset \tag{1.71}$$

Esto es, habrá que verificar que existe un elemento z en el campo de funciones F tal que la valoración sobre el lugar P' es mayor a cero. Si se supone lo contrario, es decir, que $v_{P'} < 0$ entonces existe una ecuación tal que:

$$C_n t^n + C_{n-1} t^{n-1} + ... + C_1 t + C_0 = 0 \tag{1.72}$$

Con $C_i \in F$. Tomando la valoración en P' para (1.72), obtenemos

$$\begin{aligned} v_{P'}(0) &= v_{P'}(C_n t^n + C_{n-1}t^{n-1} + ... + C_1 t + C_0) \\ &\leq min\{v_{P'}(C_n t^n), ...v_{P'}(C_0\} \end{aligned}$$

y esto implicaría la siguiente igualdad:

$$\infty = v_{P'}(0) \leq v_{P'}(C_0) = 0$$

lo cual es una contradicción, así $F \cap P' \neq \emptyset$. Para completar la demostración de este inciso, hacemos $\mathcal{O} := F \cap \mathcal{O}_{\mathcal{P}'}$ y $P := P' \cap F$ entonces $P \subseteq \mathcal{O}$ pues $\mathcal{O}_{\mathcal{P}'} \supseteq P$. Por otro lado, si $z \in \mathcal{O}$, es decir, $z \in \mathcal{O}_{\mathcal{P}'}$ y $z \in F$ entonces el elemento inverso de z no pertenece a $\mathcal{O}_{\mathcal{P}'}$ por lo que tampoco está en el anillo $\mathcal{O}$. Además $K \not\subseteq \mathcal{O}_{\mathcal{P}'} \not\subseteq F$ por lo que $\mathcal{O}$ es un anillo valuado con P su correspondiente lugar y dada la construcción de éste, se tiene la unicidad.

$\diamondsuit$

1.5.1 Criterio de Eisenstein

Definición* 1.5.4.** *Para $P \in \mathbb{P}_F$ definimos la* ***conorma de *P como:*

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

Observamos que esta definición se da sobre un sólo P, pero se puede extender a muchos lugares simultenamente, es decir, a divisores:

$$\begin{aligned} con_{F|F'}(\sum_{P\in\mathbb{P}_F} n_P P) &= \sum_{P\in\mathbb{P}_F} con_{F|F'}(P) = \\ &= \sum_{P\in\mathbb{P}_F} n_P P \sum e(P'|P)\cdot P'. \end{aligned}$$

Tenemos que esta conorma es un elemento del grupo de divisores de F'. Ahora consideramosque F'/K' es una extensión algebraica de F/K y tomamos un elemento $x \in F$ diferente de cero y denotaremos como $(x)^F$, $(x)_0^F$ y $(x)_\infty^F$ al divisor principal, al divisor de ceros y al divisor de polos respectivamente y a $(x)^{F'}$, $(x)_0^{F'}$ y $(x)_\infty^{F'}$ a los divisores correspondientes pero de F'. Como vimos en las líneas de anteriores, es posible dar la conorma de un divisor, siendo así tenemos:

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

De manera análoga se tendrá que:

$$\begin{aligned} con_{F|_{F'}}((x)_0^F) &= (x)_0^{F'} \\ con_{F|_{F'}}((x)_\infty^F) &= (x)_\infty^{F'} \end{aligned}$$

Es decir, la conorma induce a un homomorfismo entre el grupo de divisores principales de F y el grupo de divisores prncipales de F', el cual no es necesariamente inyectivo.

Ahora, el objetivo particular es establecer una relación entre el grado de un divisor A y su conorma. Esto facilitará la búsqueda de un criterio para la irreducibilidad de polinomios.

Primero veremos algunos resultados acerca del grado de los campos "grandes"sobre los "pequeños". Si K'/K es una extensión **finita** de campos y x es un elemento trascendental sobre K, entonces:

$$[K'(x) : K(x)] = [K' : K]. \tag{1.74}$$

Este hecho lo podemos verificar de las siguientes observaciones:

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

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

.

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

$$g(\mathcal{T}) = \mathcal{T}^r + C_{r-1}(x)\mathcal{T}^{r-1} + ... + C_0(x) \tag{1.75}$$

con $C_i \in K(x)$. Si multiplicamos por un denominador en común $\mathcal{G}_i \in K[x]$ y evaluamos en α el polinomio 1.79 tenemos que:

$$0 = \mathcal{G}_r(x)(\alpha)^r + \mathcal{G}_{r-1}(x)(\alpha)^{r-1} + ... + \mathcal{G}_0(x). \tag{1.76}$$

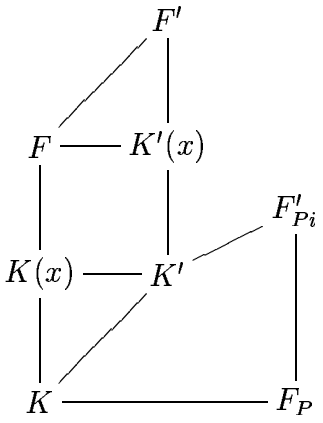
Finalmente haciendo $x = 0$ en la ecuación 1.76 obtenemos una combinación lineal de potencias de α con un número de términos menor a φ, pues $grado g < grado \varphi$, por lo cual tenemos una contradicción. Así el polinomio φ es irreducible y esto asegura que $[K'(x) : K(x)] \geq [K' : K]$

Antes de presentar el siguiente teorema, recordemos la siguiente notación:

Sea $P \in \mathbb{P}_F$, entonces $gradoP = [F_P : K]$ donde $F_P := \mathcal{O}_P/P$ y

si $P'|P$ entonces $f(P'|P) := [F'_{P'} : F_P]$.

También será útil el diagrama de la derecha siendo que de este podemos obtener la siguientes observaciones:



$$\begin{aligned}[F'_{P_i} : K] &= [F'_{P_i} : K'] \cdot [K' : K] \quad (1.77)\\ &= [F'_{P_i} : F_P] \cdot [F_P : K]\end{aligned}$$

y

$$[F' : K(x)] = [F' : F] \cdot [F : K(x)] \quad (1.78)$$

donde F'/K' una extensión algebraica de F/K, $P \in \mathbb{P}_F$ y $P_1, ...P_m \in \mathbb{P}_{F'}$ todos los lugares sobre P.

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

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

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

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

Por otro lado:

$$[F' : K(x)] = [F' : F] \cdot [F : K(x)] = [F' : F] \cdot rgradoP \tag{1.79}$$

y utilizando las igualdades (1.78) y (1.79) obtenemos:

$$[F' : F] = \cdot rgradoP.\diamondsuit$$

Este teorema brinda mucha información acerca de la relación que existe entre los lugares en $\mathbb{P}_{F'}$ y $[F' : F]$.

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

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

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

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

$$deg[con_{F|F'}(A)] = \frac{[F' : F]}{K' : K} gradoA. \tag{1.81}$$

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

$$m \leq \sum_{i=1}^{m} f_i \leq \sum_{i=1}^{m} e_i f_i = [F' : F] \tag{1.82}$$

pues $e_i \geq 1$ y $[F'_{P_i} : F_P] \geq 1$.

Para demostrar el inciso (c) tomamos un divisor primo $A = P \in \mathbb{P}_F$. Se tiene:

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

Utilizando 1.77 y sustituyendo en 1.83:

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

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

Criterio de Einsentein para la irreducibilidad de polinomios

Vamos a considerar un campo de funciones F/K y un polinomio $\phi(T) = a_nT^n + a_{n-1}T^{n-1} + ... + a_0$ con coeficientes $a_i \in F$ y también supondremos que existe al menos un $P \in \mathbb{P}_F$ que satisface al menos una de las siguientes condiciones:

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

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

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

1.6 Saltos de Weierstrass

Definición* 1.6.1.** *Sea $P \in \mathbb{P}_F$ Decimos que un entero $n \geq 0$ es un orden polar en P si existe $x \in F$ tal que $(x_\infty) = nP$. En caso contrario diremos que n es un* ***salto en *P.*

***Proposición* 1.6.1.** *Un entero n es orden polar si y sólo si*

$$dim(nP > dim(n-1)P).$$

Demostración.
Para obtener una prueba de esta proposición, primero vamos a suponer que n es un orden polar, es decir, existe $x \in F$ tal que $(x_\infty = nP)$ con $P \in \mathbb{P}_F$.

Inversamente, si suponemos que $dim(nP > dim(n-1)P)$, entonces $\mathcal{L}((n-1)P) \subset \mathcal{L}((n)P)$, esto quiere decir que existe por lo menos una función $x \in \mathcal{L}((n)P)\mathcal{L}((n-1)P)$, es decir, $(x)_\infty = nP$, por lo que n es orden polar en P. $\diamondsuit$

Denotaremos como S_P al conjunto $\{n \in \mathbb{Z} | n \text{ es orden polar en } P\}$ y como G_P al conjunto de números enteros que son saltos en P, es decir $G_P = \mathbb{N} - S_P$

> OBSERVACIÓN: S_P es un semigrupo de $\mathbb{N}$. Esto se verifica tomando dos elementos n_1 y n_2 en S_P. Se tiene que para cada uno de estos elemtentos, existen $x_1, x_2 \in F$ respectivamente tales que:
>
> $$(x)_\infty = n_1 P \text{ y } (x)_\infty = n_2 P$$
>
> y por las propiedades de una valoración discreta se tiene que $(x_1 x_2)_\infty = (n_1 + n_2)P$, por lo que $(n_1 + n_2) \in S_P$.

Teorema de Saltos de Weierstrass

***Teorema* 1.6.1.** *Sea F/K un campo algebraico de funciones de género g y sea $P \in \mathbb{P}_F$. Entonces: $|G_P| = g$. Además, si $g > 0$ entonces $1 \in G_P$.*

Demostración.
Consideramos la siguiente cadena de espacios:

$$K = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq ... \subseteq \mathcal{L}((2g-1)P) \subseteq \mathcal{L}(2gP) \tag{1.83}$$

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

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

Capítulo 2

Campos Elípticos

Este capítulo tiene como objetivos presentar la definición de *campo elíptico* y a partir de ella deducir algunas de sus propiedades teniendo como herramienta la teoría expuesta en el capítulo anterior.

"It is possible to write endlessly on elliptic curves.
(This is not a threat.)"
Serge Lang

De aquí en adelante, F denotará un campo algebraico de funciones y g su género.

Definición* 2.0.2.** *Un campo de funciones de F/K se dice* ***elíptico *si:*
1) g=1
2) Existe $A \in \mathcal{D}_F$ tal que $grado(A) = 1$

En las siguientes secciones se demostrará que a partir de esta definición se puede llegar a una ecuación de la forma $y^2 = x^3 + ax^2 + b^x + c,\ a, b, c \in K$ [1] y que a partir de una ecuación de esta forma, se puede obtener un campo elíptico.

[1] Al conjunto de soluciones de esta ecuación, junto con un punto al infinito, se le conoce comunmete como *curva elíptica.*

2.0.1 De la Definición a la Ecuación

De la definición de campo elíptico se obtienen los siguientes hechos:
Si existe $A \in \mathcal{D}_F$ con $grado(A) = 1$, entonces, por el Teorema de Riemann-Roch, $dimA = 1$. El divisor A será equivalente a un divisor A', el cual tiene el mismo grado y la misma dimensión que A, por lo que A', es un divisor primo, es decir, $A' = P \in \mathbb{P}_F$. Ésto quiere decir, que el campo, contiene por lo menos un lugar.

Recordemos que el espacio $\mathcal{L}(A)$ es un espacio vectorial sobre K. Siendo así, consideramos la siguiente cadena de espacios:

$$K = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq \mathcal{L}(3P) \subseteq ... \subseteq \mathcal{L}(nP) \subseteq ... \tag{2.1}$$

Sabemos que $dim(P) = 1$. Por otro lado tenemos que $dim(K) = 1$, por lo que $\mathcal{L}(P) = K$, además, $dim\mathcal{L}(nP) = n$, $\forall n \in \mathbb{N}$. Así se obtiene que la cadena de espacios es estrictamente creciente, es decir, $\mathcal{L}(nP) \subset \mathcal{L}((n+1)P)$ pero $\mathcal{L}(nP) \neq \mathcal{L}((n+1)P)$.

Sean $x_1 \in \mathcal{L}(2P)\backslash K$ y $y_1 \in \mathcal{L}(2P)\backslash\mathcal{L}(3P)$. Los divisores de polos de éstos elementos son:

$$(x_1)_\infty = 2P \text{ y } (y_1)_\infty = 3P,$$

así, utilizando el teorema 1.3.1, $[F : K(x_1)] = 2$ y $[F : K(y_1)] = 3$, por lo que $F = K(x_1, y_1)$. Los elementos

$$1,\ x_1,\ y_1,\ x_1^2,\ y_1^2,\ x_1y_1,\ x_1^3$$

pertenecen al espacio $\mathcal{L}(6P)$, por el párrafo anterior, la dimensión de éste espacio es 6, por lo que los elementos enunciados serán un conjunto linealmente dependiente, es decir, existen $\alpha_1, \beta_1, ..., \lambda_1, \mu_1 \in K$, tales que la siguiente igualdad es posible:

$$\alpha_1 y_1^2 + \beta_1 y_1 + \gamma_1 x_1 y_1 = \delta_1 x_3 + \epsilon_1 x_1^2 + \lambda_1 x + \mu_1. \tag{2.2}$$

Si en la igualdad anterior suponemos que $\alpha_1 = 0$ ésta se convierte en una ecuación de la interminada y_1 de grado uno, sobre $K(x_1)$, pero sabemos que $F = K(x_1, y_1)$ y $[F : K(x_1)] = 2$ lo cual resultaría una contradicción. Lo mismo ocurrirá si el coeficiente $\delta_1 = 0$ pues $[F : K(y_1)] = 3$.

Así, multiplicamos la ecuación (2.2) por $\alpha_1^3\delta_1^2$ para obtener:

$$\alpha_1^4\delta_1^2y_1^2+\alpha_1^3\delta_1^2\beta_1y_1+\alpha_1^3\delta_1^2\gamma_1x_1y_1=\alpha_1^3\delta_1^3x_3+\alpha_1^3\delta_1^2\epsilon_1x_1^2+\alpha_1^3\delta_1^2\lambda_1x+\alpha_1^3\delta_1^2\mu_1.$$

Ahora se reagruparán términos y se hará $y_2=\alpha_1^2\delta_1y_1$ y $x_2=\alpha_1\delta_1x_1$:

$$(\alpha_1^2\delta_1y_1)^2+\alpha_1^2\delta_1y_1(\alpha_1\delta_1\beta_1x_1+\alpha_1\delta_1\gamma_1)=(\alpha_1\delta_1x_1)^3+(\alpha_1\delta_1x_1)^2\alpha_1\epsilon_1+\alpha_1^2\delta_1\lambda_1(\alpha_1\delta_1x_1)+\alpha_1^3\delta_1^2\mu_1.$$

$$\Rightarrow y_2^2+y_2^2(\alpha_1\delta_1\beta_1x_1+\alpha_1\delta_1\gamma_1)=x_2^3+x_2^2\alpha_1\epsilon_1+\alpha_1^2\delta_1\lambda_1x_2+\alpha_1^3\delta_1^2\mu_1.$$

Donde renombraremos los coeficientes de la siguiente manera: $\alpha_1\delta_1\beta_1=\beta_2$, $\alpha_1\beta_1\gamma_1=\gamma_2$, $\alpha_1\epsilon_1=\epsilon_2$ $\alpha_1\delta_1\lambda_1=\lambda_2$y $\alpha_1\delta_1\mu_1\mu_2$. Así obtenemos la siguiente ecuación:

$$y_2^2+y_2(\beta_2x_1+\gamma_2)=x_2^3+x_2^2\epsilon_2+\lambda_2x_2+\mu_2. \tag{2.6}$$

La cual llamaremos, *Ecuación de Weierstrass asociada al campo elíptico F/K.*

Característica 2

A continuación, veremos algunas consideraciones si $CarcK=2$ Consideremos la ecuación resultante de la sección anterior:

$$y_2^2+y_2(\beta_2x_2+\gamma_2)=x_2^3+x_2^2\epsilon_2+\lambda_2x_2+\mu_2. \tag{2.7}$$

Supongamos que $\beta_2x_2+\gamma_2=0$. Esto tiene como consecuencia que la ecuacion (2.7) se convierta en

$$y_2^2=x_2^3+x_2^2\epsilon_2+\lambda_2x_2+\mu_2\ \in K(X_2) \tag{2.8}$$

(Que es un caso particular de una ecuación de Weierstrass). Es decir, $y_2^2\in K(X_2)$y sabemos que $F=K(X_1,Y_2)$ es una extensión de $K(X_2)$. Sea $F^{(2)}=\{x^2|x\in F\}$. El campo K es un *campo perfecto*, es decir, toda extensión de éste resulta ser una extensión separable. Además, $K(x_2)=K$.

Si $Y_2^2\in K(x_2)$ quiere decir que el campo $F/K(x_2)$ es puramente inseparable. Este hecho puede ser visto como que entre el campo $K(x_2)$ y el campo F no existe ningún campo intermedio.

Por otro lado tenemos que el género de $K(x_2)$ es igual a cero y el género del campo $F^{(2)}$ es igual a uno (Revisar prop 3.9.2) por lo que el campo F no es elíptico y esto trae una contradicción.

Volviendo a la ecuación:

$$y_2^2 + (\beta_2 X_2 + \gamma_2)y_2) = x_2^3 + \epsilon_2 x_2^2 + \lambda_2 x + \mu_2 \tag{2.9}$$

Sea $y_3 = y_2(\beta_2 x_2 + \gamma_2)^{-1}$, entonces, $F = K(x_2, y_3)$ y

$$y_3^2 + y_3 = (\beta_2 x_2 + \gamma_2)^{-2}(x_2^3 + \epsilon_2 x_2^2 + \lambda_2 x + \mu_2) \tag{2.10}$$

Si el coeficiente $\beta_2 = 0$, entonces convertiremos la ecuación (2.10) en

$$y_3^2 + y_3 = (x_2^3 + \epsilon_2 x_2^2 + \lambda_2 x + \mu_2)(\gamma_2)^{-2} \ \in \ K[x_2]$$

Es decir, se convierte en un polinomio de grado 3 en el campo $K[x_2]$. Haciendo un cambio de notación $(y = y_3)$ y $(x = x_2)$, esta idea la podemos expresar como:

$$\begin{gathered} \exists\ f(x) \ \in K[x] \text{ tal que} \\ y_2 + y = f(x) \text{ con grado de } f(x) = 3. \end{gathered}$$

Sea $\beta_2 \neq 0$ en la ecuación (2.10). Entonces:

$$\frac{x_2^3 + \epsilon_2 x_2^2 + \lambda_2 x_2 + \mu_2}{(\beta_2 x_2 + \delta_2)^2} = \nu x_2 + \frac{\sigma}{(\beta_2 x_2 + \gamma_2)^2} + \frac{\tau}{\beta_2 x_2 + \gamma_2}$$

Con $\nu, \rho, \ \sigma, \ \tau \ \in K$ y $\nu \neq 0$. De párrafos anteriores tenemos que $K = K^2$, entonces $\exists\ \sigma_1 \ \in \ K$ tal que $\sigma^2 = \sigma_1^2$, entonces:

$$y_4 = y_3 + \frac{\sigma_2}{\beta_2 x_2 + \gamma_2},$$

por lo que:

$$y_4^2 + y_2 = \nu x_2 + \rho_2 + \frac{\tau_2}{\beta_2 x_2 + \gamma_2},$$

para algunas $\nu_1, \rho_2 \in \ K$ con $\nu \neq 0$ y $\tau \neq 0$, pues ti $\tau = 0$ entonces el campo F sería racional.

2.0.2 De la Ecuación a la Definición

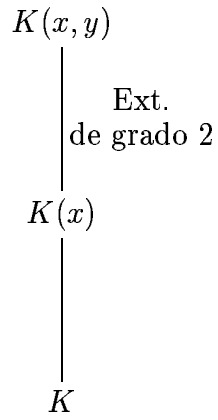


Figura 2.1: *Campo* $K(x,y)$.

En nuestro caso, utilizaremos como campo base un campo K arbitrario, $K(x) = F$ y $K(x,y) = F'$ tal como se puede observar en el diagrama de la izquierda. Tomaremos el elemento y^2 de tal manera que se cumpla la siguiente relación:

$$y^2 = x^3 + ax^2 + bx + c \tag{2.15}$$

donde $a, b, c \in K$. Por el Criterio de Einsenstein (C.I), tenemos que el polinomio $T^2 - x^3 - ax^2 - bx - c$ es irreducible donde $P_\infty \in \mathbb{P}_{K(x)}$ un polo de x que cumple las condiciones del (C.I), entonces P_∞ tiene una única extensión en $\mathbb{P}_{K(x,y)}$ a la cual denotaremos por Q_∞. El (C.I) también nos dice que $e(Q_\infty|P_\infty) = 2$ y $f(Q_\infty|P_\infty) = 1$.

Queremos determinar el género del campo $K(x,y)$. Esto es equivalente a determinar el número de saltos de Wierstrass en la siguiente cadena de espacios:

$$\mathcal{L}(0) \subseteq \mathcal{L}(Q_\infty) \subseteq \mathcal{L}(2Q_\infty) \subseteq \mathcal{L}(3Q_\infty) \subseteq ... \subseteq \mathcal{L}(rQ_\infty) \tag{2.16}$$

Recordaremos que determinar el número de saltos de Wierstrass, es determinar cuántas veces hay un "salto"de dimensión del espacio $\mathcal{L}((n-1)Q_\infty)$ al $\mathcal{L}((n)Q_\infty)$.

Por los resultados de la sección 1.3, $\mathcal{L}(0) = K$. El siguiente paso es buscar una función $z \in \mathcal{L}(Q_\infty)\backslash\mathcal{L}(0)$ para saber si hay un cambio en la dimensión del espacio $\mathcal{L}(Q_\infty)$. Primero tomaremos $z \in K(x)$. Sabemos que $e(Q_\infty|P_\infty) = 2$, por lo que $v_{Q_\infty}(z) = 2 \cdot v_{P_\infty}(z)$, por lo tanto v_{Q_∞} no podría ser igual a -1 y $z \notin K(x)$, así que la única manera para que exista una función z cuyo único polo sea el lugar Q_∞ es que $z \in K(x,y)\backslash K(x)$, pero como veremos más adelante, no existe tal función.

Ahora tomaremos la función $z = x$. Por la manera en la que se ha definido, x tiene un polo en P_∞ y éste es de orden -1 y se tiene la siguiente igualdad:

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

por lo que existe una función $z \in K(x,y)$ tal que tiene su único polo en Q_∞ de orden -2. Dicho en otras palabras -2 es un orden polar en Q_∞, y por 1.6.1 tenemos:

$$dim(\mathcal{L}(2Q_\infty)) > dim(\mathcal{L}(Q_\infty)), \tag{2.18}$$

así que hemos descubierto que existe un salto en $\mathcal{L}(Q_\infty)$.

Sea $z' = y^2 \in K(x,y)$. Podemos encontrar el valor de $v_(Q_\infty)(z)$, utilizando la igualdad 2.15 de la siguiente manera:

$$\begin{aligned} v_{Q_\infty}(y^2) &= v_{Q_\infty}(x^3 + ax^2 + bx + c) \\ &= min\{v_{Q_\infty}(x^3), v_{Q_\infty}(ax^2), v_{Q_\infty}(bx), v_{Q_\infty}(c)\} \\ &= min\{2 \cdot v_{P_\infty}(x^3), 2 \cdot v_{P_\infty}(ax^2), 2 \cdot v_{P_\infty}(bx), 2 \cdot v_{P_\infty}(c)\} \\ &= 2 \cdot v_(P_\infty)(x^3) = -3 \end{aligned}$$

Por lo que $y^2 \in \mathcal{L}(3Q_\infty)$.

Hemos conseguido una función z tal que $(z)_\infty = 2(Q_\infty)$ y una función z' tal que $(z')_\infty = 3(Q_\infty)$. Por otro lado, sabemos que la valoración discreta de un producto, es la suma de las valoraciones, por ejemplo:

$$v_{Q_\infty}(y^2 \cdot y^2) = v_{Q_\infty}(y^2) + v_{Q_\infty}(y^2) = -4 \quad \text{y}$$

$$v_{Q_\infty}(y^2 \cdot x) = v_{Q_\infty}(y^2) + v_{Q_\infty}(x) = -5 \tag{2.20}$$

Con estos resultados tenemos que -4 y -5 son órdenes polares en Q_∞ por lo que no hay saltos en dimensión. En general, cualquier $n \in \mathbb{Z}$ puede ser expresado como combinación lineal de -2 y -3, por lo que $n > 2$ siempre será un orden polar en Q_∞, por lo tanto no habrá ningún otro salto.

Siendo así, el único salto encontrado fue en $\mathcal{L}(Q_\infty)$ y utilizando el Teorema de Saltos de Wierstrass podemos afirmar que 1 es el género del campo $K(x,y)$, por lo que es un campo elíptico.

2.1 Aritmética de los Campos Elípticos

En esta sección se deduce la estructura de grupo abeliano de los lugares de grado uno de los campos elípticos. Cabe señalar que gracias a esta estructura las curvas elípticas han sido utilizadas para la criptografía.

Sea F/K un campo elíptico. En la sección (2) demostramos que $F = K(x, y)$ donde se cumplirá que $\forall x \in K(x, y)\ \exists\ y\ \in K(x, y)$ tal que:

$$y^2 = x^3 + ax^2 + bx + c \tag{2.21}$$

con $a, b, c \in K$. Además, de la definción (2) de la misma sección, tenemos que existe $A \in \mathcal{D}_F$ tal que $grado\ A = 1$. El Teorema de Riemann-Roch nos indica que

$$dim(A) = 1 + 1 - 1 > 0$$

por lo que podemos asegurar que existe $x \neq 0\ \in \mathcal{L}(A)$. Si hacemos $P := (x) + A$ tendremos que $P \sim A$. Por las propiedades de los divisores de ser grupo bajo la suma, P también es un divisor y es mayor a cero. Esta última afirmación se comprueba de la siguiente manera: primero se supone que $P = 0$, entonces A sería equivalente a un divisor principal y todo divisor principal tiene grado cero, por lo que tendríamos una contradicción.

El hecho de que $grado\ A = 1 = grado\ P$ tiene como consequencia inmediata la siguiente afirmación.

$$\mathbb{P}^{(1)}_{K(x,y)} = \{P \in \mathbb{P}_{K(x,y)} | grado\ P = 1\} \neq \emptyset$$

Este divisor primo P equivalente al divisor A, es único. Para comprobar esto, supondremos que existe un divisor $Q \neq P \in \mathbb{P}^{(1)}_{K(x,y)}$ tal que $A \sim Q$, esto implica que $P \sim Q$, *i.e.* $x \in F$ tal que $P - Q = (x)$, es decir, $(x)_\infty = -Q$ por lo que $grado(Q) = grado((x)_\infty) = [F : K(x)]$, como $Q \in \mathbb{P}^{(1)}_{K(x,y)}$ entonces, $1 = [F : K(x)]$ lo que implica que $F = K(x)$, lo cual es una contradicción, pues $F = K(x, y)$. En general, tendremos que para cualquier divisor A, existe un único lugar P de grado uno, con $A \sim P$.

Recordemos que el grupo $\mathcal{D}_F$ es el grupo de clases de divisores. De este grupo, vamos a separar las clases de divisores que tienen grado cero, en otras palabras, definimos: $C^0_{K(x,y)} := \{[D] \in\ \mathcal{P}_F | grado\ D = 0\}$.

Recordemos que a las funciones del campo F/K les podemos asociar un divisor principal. Estos divisores tienen grado cero. Lo contrario no es cierto, no todo

divisor de grado cero, se puede asociar a una función. Es por esto, que tomaremos el siguiente conjunto:

$$C^0_{K(x,y)} := \mathcal{D}^0_F/\mathcal{P}_F$$

donde $\mathcal{D}^0_F$ son los divisores de grado cero. Ahora veremos que se puede establecer una biyección entre los elementos de las clases de divisores de grado cero y los lugares de grado uno.

Biyección entre C^0_F y $\mathbb{P}^{(1)}_F$

Sea $P_0 \in \mathbb{P}^{(1)}_F$ un lugar fijo, definimos φ un mapeo tal que

$$\begin{aligned} \varphi: \ \mathbb{P}^{(1)}_F &\longrightarrow C^0_F, \\ P &\longmapsto [P - P_0] \end{aligned}$$

Sea $[B] \in C^0_F$. Como el divisor P_0 tiene grado uno, entonces el divisor $B + P_0$ tiene grado uno. Ya hemos visto que existe un único lugar P tal que $P \sim B + P_0$ por lo que $[P - P_0] = [B] = \varphi[P]$ por lo que, φ es un mapeo sobreyectivo.

Si se tiene $\varphi(P) = \varphi(Q)$ con $P, Q \in \mathbb{P}^{(1)}_F$, entonces se tendrá que $[P-P_0] = [Q-P_0]$ entonces $P - P_0 \sim Q - P_0$ lo que implica que $P \sim Q$, pero por la unicidad de P tenemos que $P = Q$. Así φ es un mapeo inyectivo por lo que es un mapeo biyectivo y su mapeo inverso queda descrito a continuación:

$$\begin{aligned} \varphi^{-1}: \ C^0_F &\longrightarrow \mathbb{P}^{(1)}_F, \\ [B] &\longmapsto [B + P_0] \end{aligned}$$

Sea $P, Q \in \mathbb{P}^{(1)}_{K(x,y)}$, vamos a definir:

$$P \oplus Q = \varphi^{-1}(\varphi(P) + \varphi(Q)). \tag{2.25}$$

***Proposición* 2.1.1.** *$\mathbb{P}^{(1)}_{K(x,y)}$ es un grupo abeliano bajo $\oplus$.*

Demostración.
Primero tenemos que

$$\begin{aligned} \varphi^{-1}(\varphi(P) + \varphi(Q)) &= \varphi^{-1}(P - P_0 + Q - P_0) \\ &= \varphi^{-1}(P + Q - 2P_0) \\ &= P + Q - P_0 \ \in \ \mathbb{P}^{(1)}_{K(x,y)} \end{aligned}$$

Además, $\varphi^{-1}(\varphi(P)+\varphi(Q)) = \varphi^{-1}(\varphi(Q)+\varphi(P))$.

Sean $P, Q, R \in \mathbb{P}_F$ tales que $P \in \mathbb{P}^{(1)}_{K(x,y)}$ y $(Q+R) \in \mathbb{P}^{(1)}_{K(x,y)}$. Sin pérdida de generalidad, supondremos que Q es de grado cero.

$$\begin{aligned}\varphi^{-1}(\varphi(P)+\varphi(Q+R)) &= \varphi^{-1}(P-P_0+(Q+R)-P_0)\\ &= \varphi^{-1}(P+Q+R-2P_0)\\ &= P+Q+R-P_0 \ \in \ \mathbb{P}^{(1)}_{K(x,y)}\end{aligned}$$

y por otro lado:

$$\begin{aligned}\varphi^{-1}(\varphi(P+Q)+\varphi(R)) &= \varphi^{-1}((P+Q)-P_0+R-P_0) \qquad (2.26)\\ &= \varphi^{-1}(P+Q+R-2P_0)\\ &= P+Q+R-P_0 \ \in \ \mathbb{P}^{(1)}_{K(x,y)}\end{aligned}$$

por lo que:

$$\varphi^{-1}(\varphi(P)+\varphi(Q+R)) = \varphi^{-1}(\varphi(P+Q)+\varphi(R)). \qquad (2.27)$$

Por lo que $\oplus$ es asociativa. Si sumamos a cualquier elemento $Q \in \mathbb{P}^{(1)}_{K(x,y)}$ el elemento P_0, entonces $Q \oplus P_0 = Q$, por lo que P_0 es el elemento neutro.

Denotemos como P' al inverso de P bajo $\oplus$. Esto quiere decir que:

$$\varphi^{-1}(\varphi(P)+\varphi(P')) \ = \ P_0$$

Por lo que:

$$\begin{aligned}P_0 &= P-P_0+P'-P_0+P_0\\ &\Longrightarrow 2P_0-P=P'\end{aligned}$$

Con lo que se está afirmando que es posible construir el inverso bajo $\oplus$ de todo elemento.$\diamondsuit$

Hemos dicho que existe una biyección entre los divisores de grado cero y los lugares de grado 1, los cuales tienen estructura de grupo abeliano.

Supongamos que $\varphi^{-1}(\varphi(P)+\varphi(Q)) = R$. Si aplicamos la función φ obtendremos $\varphi(P)+\varphi(Q)) = \varphi(R)$, lo que implica, $P+Q \sim R+P_0$ y esto se cumple si y solamente si:

$$\exists \ x \in F \text{ tal que } P+Q = R+P_0+(x). \qquad (2.28)$$

Sea $P \oplus Q = R$ y sea R' el elemento inverso de R bajo $\oplus$, entonces,

$$(P \oplus Q) \oplus R' = R \oplus R' = P_0,$$

por lo que tenemos:

$$\varphi^{-1}(\varphi(P \oplus Q) + \varphi(R') = P_0 \implies \varphi(P \oplus Q) + \varphi(R') = \varphi(P_0)$$

por lo que, $[P - P_0] + [Q - P_0] + [R' - P_0] \sim P_0 - P_0$ y esto implica que

$$P + Q + R' - 3P_0 \sim 0 \iff$$

$$\exists \ z \in F \text{ tal que } P + Q + R' - 3P_0 = (z). \tag{2.32}$$

de aquí que se deduce que $z \in \mathcal{L}(3P_0)$. Como ya hemos visto, la $dim\ \mathcal{L}(3P_0) = 3$ y tiene como base $1, x, y$ (descritos como en (2.0.1)) por lo que existe una combinación lineal de estos elementos tales que:

$$z = \alpha x + \beta y + \gamma \text{ con } \alpha, \beta, \gamma, \in K. \tag{2.33}$$

OBSERVACIÓN: Supongamos que $z \in \mathcal{L}(0) = K$, entonces $(z) = 0$ por lo que $\alpha = z$, con $\alpha \in K$. Además $(z) = P + Q + R' = 3P_0$ por lo que $P = Q = R' = P_0$, es decir, estaremos sumando el lugar P_0 con sí mismo.

Por otro lado, $z \in \mathcal{L}(P_0) \backslash \mathcal{L}(0) \Rightarrow (z) + P_0 > 0$ por lo que $(z) \geq 0$ y la única manera que esto ocurra es que $(z) = 0 \in \mathcal{L}(0)$, por lo que $z \notin \mathcal{L}(P_0) \backslash \mathcal{L}(0)$.

Supongamos que $z \in \mathcal{L}(2P_0) \backslash \mathcal{L}(P_0)$, entonces, $P + Q + R' - 3P_0 \geq -2P_0$, $\Rightarrow P + Q + R' - P_0 \geq 0$ entonces $P = P_0$ ó $Q = P_0$ ó $R' = P_0$. Si $Q = P_0$ entonces $R = P$, es decir, estamos sumando al lugar P el neutro multiplicativo del grupo y no tiene sentido decir algo sobre z. El caso es análogo para $P = P_0$. Cuando $R = P_0$, indica que los elementos que se están sumando son inversos uno del otro. Tenemos que $dim\ \mathcal{L}(2P_0) = 2$ y que su base son los elementos $\{1, x\}$, por lo que $z = \alpha x + \gamma$ con $\alpha, \gamma \in K$.

Por último, si $z \in \mathcal{L}(3P_0) \backslash \mathcal{L}(2P_0)$ tenemos z queda descrita de la forma (2.33).

Definición* 2.1.1.** *Llamaremos* ***Línea de P ***y*** Q *a la función z cuyo divisor se describe en (2.32).*

OBSERVACIÓN: Si $P \oplus Q = R$ y z es la línea asociada a z, entonces, z también es la línea asociada a Q y R' y la línea asociada a P y R'.

Antes de dar una forma de construccion de R a partir de P y Q debemos saber como construir R' a partir de R. En los párrafos anteriores obtuvimos que la línea asociada a R y R' pertenece al espacio $\mathcal{L}(2P_0)$, es decir, es de la forma $z = \alpha x + \gamma$ con $\alpha, \gamma \in K$. Sea $x(R) := x_3$, $y(R) := y_3$, y $x(R') := x_{3'}$, $y(R') := y_{3'}$, entonces se debe cumplir que:

$$0 = z(R) = \alpha x(R) + \gamma = \alpha x_3 + \gamma \quad \text{y} \quad 0 = z(R') = \alpha x(R') + \gamma = \alpha x_{3'} + \gamma$$

por lo que $\alpha x_3 + \gamma = \alpha x_{3'} + \gamma$, es decir, $x_3 = x_{3'}$. Además, ambos lugares deben cumplir con el ecuación de Wierstrass, por lo tanto:

$$y_3^2 = x_3^3 + ax_3^2 + bx_3 + c = x_{3'}^3 + ax_{3'}^2 + bx_{3'} + c = y_{3'}^2,$$

es decir, $y_3^2 = y_{3'}^2$, por lo que, $y_{3'} = -y_3$. Por lo tanto, si $x(R) := x_3$, $y(R) := y_3$, entonces $x(R') := x_3$ y $y(R') := -y_3$.

Supongamos que $P \neq Q$ y que $P \oplus Q = R$, con $x(P) := x_1, y(P) := y_1$, $x(Q) := x_2, y(Q) := y_2$, y $x(R') := x_3, y(R') := y_3$, donde sólo conocemos P y Q. Primero observamos que si $z = a'x + b'y + c'$ es la línea asociada a P y a Q, entonces:

$$\begin{aligned} 0 = z(P) &= a'x(P) + b'y(P) + c' = a'x_1 + b'y_1 + c' \\ 0 = z(Q) &= a'x(Q) + b'y(Q) + c' = a'x_2 + b'y_2 + c' \end{aligned}$$

Por lo que:

$$\begin{aligned} a'x_1 + b'y_1 + c' &= a'x_2 + b'y_2 + c' \\ \Rightarrow a'x_1 + b'y_1 &= a'x_2 + b'y_2 \\ \Rightarrow a'(x_1 - x_2) &= b'(y_2 - y_1) \\ \Rightarrow \frac{a'}{b'} &= \frac{(y_2 - y_1)}{(x_1 - x_2)} \\ \Rightarrow -\frac{a'}{b'} &= \frac{(y_2 - y_1)}{(x_2 - x_1)} \end{aligned}$$

Por otro lado sabemos que $0 = z(R') = a'x(R') + b'y(R') + c' = a'x_3 + b'y_3 + c'$ y si dividimos esta igualdad entre b', obtenemos:

$$\frac{a'}{b'}x_3 + y_3 + \frac{c'}{b'} = 0,$$

$$\Rightarrow y_3 = -\frac{a'}{b'}x_3 - \frac{c'}{b'}$$

$$\Rightarrow y_3 = \lambda x_3 + \nu$$

donde $\lambda := -\frac{a'}{b'}$ y $\nu = -\frac{c'}{b'}$. Como también queremos que R' sea un lugar de la curva por lo que sustituimos estos valores en la ecuación de Wierstrass correspondiente:

$$\begin{aligned} y_3^2 = (\lambda x_3 + v)^2 &= x_3^3 + ax_3^2 + bx_3 + c \\ \Rightarrow 0 &= x_3^3 + (a - \lambda^2)x_3^2 + (b - 2\lambda v)x + (c - v^2) \end{aligned} \tag{2.37}$$

La ecuación (2.38) es de tercer grado por lo que tiene tres raíces, digamos α, β, γ, (x_1, x_2 *y* x_3 respectivamente), por lo tanto:

$$(x_3 - \alpha)(x_3 - \beta)(x_3 - \gamma) = x_3^3 + (a - \lambda^2)x_3^2 + (b - 2\lambda v)x_3 + (c - v^2) \tag{2.38}$$

Desarrollando el lado izquierdo de la ecuación e igualando coeficientes obtenemos:

$$\begin{aligned} x_3^3 + (-x_2 - x_1 - \gamma)x_3^2 + x_1x_2 + x_2\gamma + x_2\gamma)x_3 + x_1x_2\gamma = \\ = x_3^3 + (a - \lambda^2)x_3^2 + (b - 2\lambda v)x_3 + (c - v^2), \end{aligned}$$

por lo que:

$$x(R) = x_3 = \lambda^2 - a - x_1 - x_2, \quad \text{y} \quad y(R) = -y_3 = -(\lambda^3 x_3 + v).$$

***Ejemplo* 2.1.1.** *Sea $y^2 = x^3 + 3x$ la ecuación de Weierstrass asociada al campo elíptico F/K donde $K = \mathbb{F}_{11}$. Sean P y Q dos lugares de grado 1 tal que:*

$$\begin{aligned} x(P) = 2, \quad y(P) = 6 \\ x(Q) = 3, \quad y(Q) = 5. \end{aligned}$$

En este caso, $\lambda = -1 \equiv 10 \ mod\ 11$ y $v = y_1 - \lambda x_1 = 6 - 10(2) = 8 \ mod\ 11$. Por lo que:

$$x_3 = 1 - 3 - 2 = 7 \ mod\ 11, \ y\ y_3 = 10(7) + 8 = 1 \ mod\ 11 \Longrightarrow$$

$$P \oplus Q = R \quad donde \quad x(R) = 7, y(R) = 10.$$

$\diamondsuit$

En el caso en el que queramos sumar el lugar P con sí mismo, la forma de deducir el resultado explicado arriba no funcionará pues será imposible calcular λ En este caso, se utiliza otro método.

Si $P = Q$,el divisor (2.32) de la línea z asociada a P y a Q, será de la forma:

$$(z) = 2P + R' - 3(P_0),$$

esto quiere decir que $z(P) = 0$, $z(R') = 0$ y $z^2(P) = 0$. Sea $x(P) := x_1$ y $y(P) := y_1$ y sea $z = a'x + b'y + c'$. Entonces, $0 = z(P) = a'x_1 + b'y_1 + c'$, de donde se obtiene:

$$y_1 = \lambda x_1 + \nu, \quad \text{donde} \quad \lambda = -\frac{a}{b} \quad \text{y} \quad \nu = -\frac{c}{b}$$

por lo que $0 = z(P) = y_1 - \lambda x_1 - \nu$, además:

$$\begin{aligned} 0 = z^(P) = (y_1 - \lambda x_1 - \nu)^2 &= (-1)^2(\lambda x_1 - y_1 + \nu)^2, \\ &= x_1^2\lambda^2 + y_1(-2\lambda x_1 - 2\nu) + y_1^2 + 2\lambda x_1\nu + \nu^2), \end{aligned}$$

por lo que:

$$\begin{aligned} y_1(2\lambda x_1 + 2\nu) &= x_1^2\lambda^2 + (x_1^3 + ax_1^2 + bx_1 + c) + 2\lambda x_1\nu + \nu^2) \\ \Rightarrow \quad y_1(2y_1) &= x_1^3 + x_1^2(a + \lambda^2) + x_1(b + 2\lambda\nu) + (c + \nu^2) \\ \Rightarrow \quad y_1 &= \left(\frac{x_1^2 + x_1(a + \lambda^2) + (b + 2\lambda\nu)}{2y_1}\right) x_1 + \left(\frac{c + \nu^2}{2y_1}\right), \end{aligned} \tag{2.44}$$

por lo tanto:

$$\lambda = \left(\frac{x_1^2 + x_1(a + \lambda^2) + (b + 2\lambda\nu)}{2y_1}\right) \quad \text{y} \quad \nu = \left(\frac{c + \nu^2}{2y_1}\right).$$

De la igualdad de la derecha obtenemos:

$$\begin{aligned} 2\lambda y_1 &= x_1^2 + x_1(a + \lambda^2) + (b + 2\lambda\nu) \\ \Rightarrow 2(\lambda y_1 - x_1\lambda - 2\nu) &= x_1^2 + x_1a + b \\ \Rightarrow 2(y - \nu) &= x_1^2 + x_1a + b \\ \Rightarrow 2(\lambda x_1) &= x_1^2 + x_1a + b \\ \Rightarrow \lambda^2 &= \frac{x_1^2 + x_1a + b}{x_1} \end{aligned}$$

Por lo que $(\lambda^2 + a)x_1 = x_1^2 + a1x_1 + b$ y al sustituir este resultado en la ecuación 2.44, obtenemos:

$$\lambda = \frac{2x_1^2 + 2ax_1 + 2b + 2\lambda\nu}{2y_1} \tag{2.46}$$

Por otro lado, sabemos que $y = \lambda x + \nu$ deberá cumplir que $y^2 = x^3 + ax^2 + bx + c$, por lo que:

$$\begin{aligned} \lambda^2 x^2 + 2\lambda\nu x + \nu^2 &= x^3 + ax^2 + bx + c \\ \Rightarrow \quad 0 &= x^3 + (a - \lambda^2)x^2 + (b - 2\lambda)x + (c - \nu^2) \end{aligned}$$

y a diferencia de la ecuación 2.38 queremos que ésta tenga una raíz de multiplicidad 2 y una sencilla:

$$(x - x_1)^2(x - x_3) = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda)x + (c - \nu^2).$$

Desarrollando el lado izquierdo de la ecuación obtenemos:

$$x^3 + (-2x_1 - x_3)x^2 + (x_1^2 + 2x_1x_3)x + (-x_1^2x_3) = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda)x + (c - \nu^2),$$

por lo que consideramos las siguientes igualdades:

- $-2x_1 - x_3 = a - \lambda^2, \quad \Rightarrow x_3 = \lambda - a - 2x_1,$
- $b - 2\lambda\nu = x_1^2 + 2x_1x_3,$

de donde:

$$\begin{aligned} b - 2\lambda\nu &= x_1^2 + 2x_1(\lambda^2 - a - 2x_1) = \\ &= x_1^2 + 2(x_1^2 + x_1a + b) - 2x_1a - 4x_1^2 = (\lambda^2) \\ &= -x_1^2 + 2b, \quad \Rightarrow \\ 2\lambda\nu &= x_1^2 - b. \end{aligned} \tag{2.48}$$

Sustituyendo este último valor en la ecuación 2.46:

$$\lambda = \frac{2x_1^2 + 2ax_1 + 2b + 2\lambda\nu}{2y_1} = \frac{3x_1^2 + 2ax_1 + b}{2y_1} \tag{2.49}$$

además,

$$v = \frac{2c - x_1^3 + bx_1}{2y_1}.$$

Por lo tanto:

$$y = \left(\frac{3x_1^2 + 2ax_1 + b}{2y_1}\right)x + \left(\frac{2c - x_1^3 + bx_1}{2y1}\right),$$

de donde concluimos que $x(R) = x_3$, $y(R) = -y_3$, donde:

$$x_3 = \lambda^2 - a - 2x_1$$

y

$$y_3 = \left(\frac{3x_1^2 + 2ax_1 + b}{2y_1}\right)x_3 + \left(\frac{2c - x_1^3 + bx_1}{2y1}\right).$$

***Ejemplo* 2.1.2.** *En el campo del ejemplo anterior, P era un lugar de grado 1 tal que: $x(P) = 2$ y $y(P) = 6$. Si queremos calcular $P \oplus P = 2P$, entonces*

$$\lambda = 3(2)^2 + 3 = 15 \equiv 4 \ mod\ 11, \quad y \quad v = -(2^3) + 6 \equiv 9 \ mod\ 11,$$

por lo que, $x_3 = 4^2 - 4 = 12 \equiv 1 \ mod\ 11$, y $y_3 = 4(1) + 13 \equiv 2 \ mod\ 11$. Dicho de otra manera, $P \oplus P = 2P$, donde $x(2P) = 10$, y $y(2P) = 9$. $\diamondsuit$

Definición* 2.1.2.** *El punto resultante de sumar P con P' para todo lugar sobre E, lo llamaremos,* ***punto al infinito *y lo denotaremos como $\mathcal{O}$.*

Notas

Como hemos visto, a cada campo elíptico se le puede asignar una ecuación del tipo 2.21 y cada ecuación de éstas representa a su vez, un campo elíptico. Una **curva elíptica** es una ecuación como 2.21 acompañada de un punto al infinito. Por lo anterior, a partir de este momento y por convenciena, nos referiremos a los campos elípticos como curvas elípticas, así como **puntos de la curva** a los lugares de grado uno correspondientes.

Un problema directo en el estudio de las curvas elípticas, es conocer la cantidad de soluciones, es decir de sus puntos. Si suponemos que K tiene $q = p^r$ elementos, una cota inmediata resulta ser $2q + 1$ lugares. Existen algunos resultados que mejoran esta cota, por ejemplo, en 1939 el alemán Helmut Hasse demostró que si $N = \{\text{número de puntos de la curva}\}$, entonces, $2q+1-2\sqrt{q} < N < 2q+1+2\sqrt{q}$.

2.2 Multiplicación Escalar de Puntos

En el capítulo anterior, hemos dicho que los puntos de una curva elíptica (es decir, los lugares de grado uno de un campo elíptico) forman un grupo abeliano. De manera natural, se define la multiplicación escalar de lugares de la siguiente manera:

$$kP = \overbrace{P \oplus P \oplus \ldots \oplus P}^{k \ veces}$$

donde $\oplus$ es la operación definida en (2.25).

Uno de los problemas básicos dentro de la criptología de curvas elípticas es encontrar formas eficientes de calcular kP. Observemos que con las formas explícitas de encontrar las sumas de puntos dadas en el capítulo anterior, el duplicar un punto costará aproximadamente 14 multiplicaciones, 6 sumas, el cálculo de un inverso multiplicativo, y por lo menos 2 reducciones de módulo. Estas cifras crecen en la práctica, pues se llegan a utilizar números de más de 30 dígitos. Existen algunos algoritmos que reducen drásticamente el número de operaciones en el cálculo de kP. Uno de dichos métodos es el **Algoritmo Double-and-Add** descrito a continuación.

La idea general es representar el número k en su forma binaria. Es decir, si $k = b_0 2^0 + b_1 2^1 + ...b_m 2^m$, con $b_i \in \{0, 1\}$ entonces kP lo podemos reescribir como: $kP = (b_0 2^0 + b_1 2^1 + ...b_m 2^m)P$.

Algortimo:	Double-and-Add (Utilizando representación binaria)
Entrada:	$k = \sum_{i=0}^{m-1} b_i 2^i$, $b_i \in \{0, 1\}$ $P = (x_1, y_1)$ $Q = \mathcal{O}$
Salida:	kP
	Para $i = (m-1) \rightarrow 0$: $Calcular \begin{cases} Q = 2P, \\ Si\ b_i == 1: \\ \quad Q = P + Q \end{cases}$ Regresa: Q.

Existen algunas maneras de reducir aún más la cantidad de operaciones para calcular kP. Una de ellas es el algoritmo **NAF Binario** (Binary Non-Adjacent Format), en el cual se utiliza una representación "signed binary"de k no adyacente. Esta representación se obtiene , como en el caso de la representación binaria, dividiendo entre 2, pero se permiten residuos 0,1 y -1, de tal manera que el cociente sea par y no existan números consecutivos si no son cero, [2]. El algoritmo Double-and-Add se modifica de la siguiente manera:

Algortimo:	Double-and-Add (Utilizando representación NAF)
Entrada:	$k = \sum_{i=0}^{m-1} b_i 2^i$, $b_i \in \{0, 1, -1\}$ $P = (x_1, y_1)$ $Q = \mathcal{O}$
Salida:	kP
	Para $i = (m-1) \rightarrow 0$: $Calcular \begin{cases} Q = 2P, \\ Si\ b_i == 1: \\ \quad Q = P + Q \\ Si\ b_i == -1: \\ \quad Q = P - Q \end{cases}$ Regresa: Q.

Actualmente se siguen investigando algoritmos para realizar estas operaciones de manera más rápida y con la menor cantidad recursos posibles. Un ejemplo es el algoritmo **Quad-and-Add** en el cual se desarrolla una rutina para **cuadruplicar** un punto. [2]

En general, estos algoritmos se enfocan en la forma en la que se puede representar el escalar, en la característica de K y en la ecuación de la curva elíptica.

Subgrupo de Torsión

Al conjunto $\mathcal{E}[n] := \{P \in \mathcal{E} | nP = \mathcal{O}\}$, se le denomina Subgrupo de Torsión de la curva $\mathcal{E}$.

[2]Este método es analizado en [3].

En la misma dirección, diremos que $P \in \mathcal{E}$ es de **orden m**,[3] si $mP = \mathcal{O}$ y m es el número entero más pequeño para el cual se cumple dicha igualdad. Si m no existe, diremos que tiene **orden infinito**.

Un resultado inmediato es que si P es de orden m y es de n-torsión, entonces, $m|n$.

Otro resultado, no tan inmediato pero que brinda mucha información acerca de como se comporta el subgrupo de torsión es el siguiente.

***Teorema* 2.2.1.** *Sea $\mathcal{E}$ es una curva elíptica definida sobre el campo K y sea $n > 0 \in \mathbb{Z}$. Si la caracaterística de K no divide a n ó es cero, entonces*

$$\mathcal{E}[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Si la característica de K es p y $p|n$, entonces:

$$\mathcal{E}[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad o \quad \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$$

donde $n = p^r n$ y $p \not| n'$

La demostración de este Teorema queda fuera de los alcances de este trabajo, pero puede consultarse en [4].

[3] Este *orden es diferente al orden polar de 1.6*

Resumen de la primera parte

Hasta aquí se ha cumplido el primer objetivo de este trabajo: presentar a los campos elípticos como un caso de campos algebraicos de funciones.

Para lograr esto, hemos tratado la teoría básica de dichos campos y sus extensiones considerando como ejes el Teorema de Riemann-Roch y el Teorema de Saltos de Weierstrass. Ambos brindan información acerca del *género* de un campo de funciones algebraico, convirtiéndose en concepto medular de esta sección. Por otro lado, estudiar el género de estos campos fue posible gracias al estudio del grupo de divisores.

Los teoremas mencionados son utilizados en el capítulo 3, en el cual y gracias a la teoría previa fue posible dar la definición de los campos elípticos y a partir de ella obtuvimos la construcción de una ecuación de Wierestrass. Inversamente y complementando dicho resultado, se demostró que a partir de una ecuación Weierstrass con ciertas características podemos llegar a un campo elíptico.

Con el fin de dar una visión más amplia acerca de estos campos y preparando la segunda parte de este trabajo, se analizaron algunos detalles acerca de la estructura y de la aritmética de los lugares de grado uno de los campos elípticos.

Parte II

Aplicaciones a las Curvas Elípticas

Capítulo 3

Factorización Entera

Este capítulo esta dedicado a mostrar el uso de las curvas elípticas dentro de la criptología y la teoría de códigos. También se hace mención de su utilización en la solución al problema de la factorización entera.

"... a problem that has fascinated many
mathematicians throughout history,
such as Eratosthenes (284-202), Fibonacci (1180-1250),
Fermat (1601-1665), Legendre (1752-1833)
and Gauss(1777-1855) ..."
(Hendrik W. Lenstra)

Recordemos que se llama **problema de la factorización entera** (PFE) al problema que consiste en exhibir los factores primos de un número entero dado. A través de los años, se han desarrollado algunas **pruebas de primalidad**, es decir, métodos a través de los cuales podemos saber si un número es primo o no, así como algoritmos para poder conocer los divisores de un número. Uno de los algoritmos más eficientes para resolver el PFE es el propuesto por H.W. Lenstra [6]. Dicho algoritmo es análogo al método **Pollard** $\rho - 1$,[1] el cual resumimos a continuación:

"Sea $n \geq 2$ el número entero que queremos factorizar. Se construye un número k que sea producto de potencias de primos *pequeños*, es decir, $k = [2 \cdot 3 \cdot \cdot ... \cdot K]$. Se selecciona un entero a que satisfaga que $1 < a < n$. Se calcula $d = mdc(a, n)$.

[1] Propuesto por John Pollard en 1974.

Si $d > 1$ entonces se habrá encontrado un divisor. En caso que $d = 1$ se buscará un divisor d' calculando $d' = mdc(a^k - 1, n)$. En este caso, si $d' = 1$, se deberá incrementar k, si $d' = n$, se debe cambiar a."

***Ejemplo* 3.0.1.** *Factorización de* $n = 7894561$ *utilizando el método Pollard* $\rho - 1$. *Sea* K, *la lista ordenada de los primeros 150 números primos y sea* k_{100} *el producto de los primeros 100 elementos de* K. *Debemos escoger un número* a *que esté entre* 1 *y* n, *sea* $a = 4000000$. *Como* $d = mdc(a, n) = 1$, *entonces deberemos calcular* $d' = mdc(a^{k_{100}} - 1, n)$. *Pero este es de nuevo uno por lo que deberemos sustituir* k_{101}. *A continuación se presentan los resultados de 5 iteraciones a este procedimiento.*

k_i	$d' = mdc(a^k - 1, n)$
k_{101}	1
k_{102}	1
k_{103}	1
k_{104}	1
k_{105}	71

Por lo que, 71 *es un divisor de* n.

Este algoritmo termina eventualente pues en algún momento, K será igual a un divisor p de n, sin embargo esto puede tomar *mucho* tiempo. El método es eficiente cuando n tiene como divisor a algún primo p que satisfaga que $p - 1$ es producto de potencias de primos pequeños, (En el caso del ejemplo dado, $70 = 2 \times 5 \times 7$). Este algoritmo está basado en el hecho que $(\mathbb{Z}/\mathbb{Z}_P)^*$ forma un grupo de orden $p - 1$, por lo que $p - 1 | k$ y $a^k \equiv 1$ en $(\mathbb{Z}/\mathbb{Z}_P)^*$.

La idea básica del algoritmo de Lenstra es cambiar el grupo $(\mathbb{Z}/\mathbb{Z}_P)*$ por el grupo de puntos de una curva elíptica y cambiar a por un punto P de dicha curva. La idea general queda descrita a continuación:

"Sea $\mathcal{E}$ una curva elíptica definida sobre $\mathbb{Z}_n$, donde n es el número que se pretende factorizar y P un punto sobre $\mathcal{E}$. Si existe $k \in \mathbb{Z}$ tal que kP no es posible de calcular ó da como resultado el punto al infinito, entonces habremos encontrado un factor de n."

Este método funciona ya que si suponemos $P = (x_P, y_P)$, $(k-1)P = (x_{k-1}, y_{k-1})$ y queremos sumar estos puntos, deberemos calcular el inverso multiplicativo de $(x_{k-1} - x_P)$ módulo n, el cual existe si y solamente si $mcd(x_{k-1} - x_P, n) = 1$. Al intentar calcularlo tenemos dos casos:

- $1 < mcd(x_{k-1} - x_P, n) < n$. En este caso habremos encontrado un divisor de n.

- $mcd(x_{k-1} - x_P, n) = 1$ ó $mcd(x_{k-1} - x_P, n) = n$. En cualquiera de estos casos no habremos obtenido información acerca de n por lo que deberemos escoger otra curva u otro punto.

Formalmente, el algoritmo de Lenstra es el siguiente:

Sea $n \geq 2$ el número entero a factorizar.

Paso 1. Verificar que $mcd(n, 6)) = 1$ y verificar que n no sea de la forma m^r para algún $r \geq 2$.

Paso 2. Escoger aleatoriamente $b, x_1, y_1 \in \mathbb{Z}_n$.

Paso 3. Sea $c := y_1^2 - x_1^3 - bx_1 (mod\ n)$. De esta forma la curva que utilizaremos será $\mathcal{E} := y^2 = x^3 + bx + c$ y el punto a sumar será $P = (x_1, y_1)$.

Paso 4. Verificar que $mcd(4b^3 + 27c^2, n) = 1$(En caso de que sea igual a n, se deberá regresar al paso 2 y hacer una nueva elección para b. En el caso que $1 < mcd(4b^3 + 27c^2, n) < n$ entonces habremos encontrado un factor no trivial de n y no es necesario seguir con los otros pasos). [2]

Paso 5. Se escoge un número k que sea producto de potencias de número primos *pequeños*.

Paso 6. Calculamos $kP = (x_k, y_k)$ (Ver sección (2.2)).

Paso 7. Si $kP = \mathcal{O}$ ó no es posible calcularlo, entonces:

$$d = mcd(x_{k-1} - x_P, n)$$

es un divisor no trivial de n. Si $kP \neq \mathcal{O}$ pero pertenece a la curva y $d = 1$ deberemos aumentar, k, ó cambiar la curva $\mathcal{E}$. Si $d = n$ deberemos disminuir K.

[2]El determinante de una curva elíptica $y^2 = x^3 + ax^2 + bx^2 + c$, será, $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^3$.

Una de las ventajas que tiene este algoritmo es que el tiempo de búsqueda depende del tamaño del divisor primo más pequeño de n, además, si no encontramos un divisor con una curva, podemos cambiar de curva, o de punto, hasta encontrar un divisor [6].

Al utilizar éste algoritmo, es conveniente utilizar los métodos para calcular kP, descritos en (2.2). A continuación se muestran dos ejemplos del uso del algoritmo de Lenstra.

***Ejemplo* 3.0.2.** *Factorización de* $n = 199843247$. *Antes de todo, es conveniente verificar que* n *no sea un número primo.Se tiene que*

$$\begin{aligned} 199843246 &= 2^{27}+2^{25}+2^{24}+2^{23}+2^{22}+2^{21}+2^{19}+2^{16}+2^{14}+ \\ &\quad +2^{12}+2^{11}+2^{10}+2^{8}+2^{7}+2^{5}+2^{3}+2^{2}+2^{1} \end{aligned}$$

por lo que:

$$2^{199843246} = 2^{(2^{27}+2^{25}+2^{24}+2^{23}+2^{22}+2^{21}+2^{19}+2^{16}+2^{14}+2^{12}+2^{11}+2^{10}+2^{8}+2^{7}+2^{5}+2^{3}+2^{2}+2^{1})}.$$

Después de calcular todos los sumandos y haciendo las reducciones modulo n, *podemos multiplicarlos para obtener:*

$$2^{199843246} \equiv \ mod\ 199843247. \tag{3.2}$$

Así, el Pequeño Teorema de Fermat [3] *nos asegura, que* n *no es un número primo. Utilizando el Teorema Chino del Residuo, encontramos que,* $mcd(199843247, 6) = 1$. *Utilizaremos el punto* $P = (1, 1)$ *y la curva* $y^2 = x^3 + 59x - 59$. *Calcularemos* kP, *donde* $k = 16296$. *Primero observamos que,*

$$16296 = 2^{13}+2^{12}+2^{11}+2^{10}+2^{9}+2^{8}+2^{7}+2^{5}+2^{3}$$

por lo que:

$$16296P = (2^{13}+2^{12}+2^{11}+2^{10}+2^{9}+2^{8}+2^{7}+2^{5}+2^{3})P$$

[3] Ver apéndice.

Calculamos los sumandos:

2^1P	$2P$	$959, 199813548$
2^3P	$2(2(2)P)$	$142634722, 33539717$
2^5P	$2(2(2^3P))$	$5784508, 152911406$
2^7P	$2(2(2^5P))$	$169802754, 196416866$
2^8P	$2(2^7P)$	$11812898, 62341168$
2^9P	$2(2^8P)$	$13592075, 60713669$
$2^{10}P$	$2(2^9P)$	$41756751, 77665319$
$2^{11}P$	$2(2^{10}P)$	$162046219, 1023294$
$2^{12}P$	$2(2^{11}P)$	$171948746, 183303558$
$2^{13}P$	$2(2^{12}P)$	$116509380, 17880653$

y sumamos:

$$(2^{12} + 2^{11} + 2^{10} + 2^9 + 2^8 + 2^7 + 2^5 + 2^3)$$

$2^3P + 2^5P$	$(32573211, 64333866)$
$(32573211, 64333866) + 2^7P$	$(122586107, 134071689)$
$(122586107, 134071689) + 2^8P$	$(84524000, 69800545)$
$(84524000, 69800545) + 2^9P$	$(118912774, 18013736)$
$(118912774, 18013736) + 2^{10}P$	$(190955731, 104499251)$
$(190955731, 104499251) + 2^{11}P$	$(132762455, 427350)$
$(132762455, 427350) + 2^{12}P$	$(3834541, 80821724)$

pero, al intentar calcular $(3834541, 80821724) + 2^{13}P$*, debemos calcular el inverso multiplicativo de* $116509380 - 3834541$ *mod* 199843247*, pero éste no existe, pues*

$$m.c.d(116509380 - 3834541, 199843247) = 10289 \neq 1$$

Por lo tanto, $10289 \mid 199843247$*. El divisor inmediato es* 19423*, el cual cumple que*

$$2^{19422} \equiv 1 \ mod\ 19423$$

por lo que es un número primo.

Capítulo 4

Problema del Logaritmo Discreto

Sea $< G, \times >$ un grupo finito cualquiera, $P \in G$ y $k \in \mathbb{Z}$. Definimos kP como el elemento en G, resultado de operar k veces con si mismo, es decir:

$$kP = \overbrace{P \times P \times \ldots \times P}^{k \ veces}$$

Sea $Q = kP$. Llamaremos a k el **logaritmo discreto de** Q. El **Problema del Logaritmo Discreto** (PLD), consiste en encontrar el logaritmo discreto de un elemento Q, conociendo P, dentro de un grupo finito.

En general, no se pide que el grupo G sea cíclico, aunque cuando el grupo no lo es, el PLD se cree mucho más difícil. Cuando G es un grupo cíclico y se conoce el orden de P, es aún más fácil, pues si suponemos que P es de orden n, $kP = Q$, si y sólo si, $nQ = 1_G$.

Actualmente, existen muchos sistemas de encriptación, protocolos de autentificación y sistemas de intercambio de llaves, cuya funcionalidad depende directamente de la difícil solución del PLD y de la existencia alguna solución alterna.

4.1 Ataques al PLD en $\mathbb{F}_p$

Como lo hemos mencionado, se conocen algunos algoritmos para atacar al PLD cuando se tiene un grupo cíclico. Estos algoritmos se pueden dividir en tres grupos según [7]. Estas divisiones son:

- ⋆ *Algoritmos de búsqueda exhaustiva.* También son conocidos como *Ataques por fuerza bruta.* Consisten en calcular $2P$,$3P$,...,kP, hasta obtener Q. Sobra decir que para ciertos grupos (los grandes) estos métodos pueden tomar mucho tiempo. Los algorimos *Baby Step-GiantStep* y *Pollard-Rho* se pueden clasificar dentro de este grupo.

- ⋆ *Algoritmos dependientes del orden de G.* Estos dependen de que el orden de G tenga como factores enteros a números primos pequeños. Como ejemplo de estos, se encuetra el algoritmo *Pohlig-Hellman.*

- ⋆ *Algoritmo Index-Calculus* Se considera el más eficiente a la fecha, sin embargo sólo funciona en determinados grupos.

Queda fuera del propósito de este trabajo analizar profundamente estos métodos, pero con el propósito de ser más ilustrativos a continuación se presentan algunos ejemplos. [1]

***Ejemplo* 4.1.1.** *Pollard-Rho. Este algoritmo tiene la ventaja de que requiere una cantidad mínima de almacenamiento. Supongamos que G es un grupo cíclico de orden n primo, α un generador de G, y β el elemento del que queremos saber su logaritmo discreto. A este grupo lo dividiremos en tres conjuntos, digamos, S_1, S_2 y S_3, de tal manera que contengan la misma cantidad de elementos y que $1 \notin S_2$. Después, generamos una lista de elementos $x_i \in G$, bajo la siguiente regla: $x_0 := 1$, y para $i \geq 0$,*

$$x_{i+1} := \begin{cases} \beta \cdot x_i & si\ x_i \in S_1. \\ x_i^2 & si\ x_i \in S_2. \\ \alpha \cdot x_i & si\ x_i \in S_3. \end{cases}$$

[1] El análisis de éstos métodos se puede entontrar en [7], [4] y [8].

De esta lista, se obtienen otras dos, bajo la siguiente correspodencia: $a_0 := 1$, $b_0 := 1$, *y para* $i \geq 0$,

$$a_{i+1} := \begin{cases} a_i & si\ x_i \in S_1. \\ 2 * a_i\ mod\ n & si\ x_i \in S_2. \\ a_i + 1\ mod\ n & si\ x_i \in S_3. \end{cases}$$

$$b_{i+1} := \begin{cases} b_i + 1\ mod\ n & si\ x_i \in S_1. \\ 2 * b_i\ mod\ n & si\ x_i \in S_2. \\ b_i & si\ x_i \in S_3. \end{cases}$$

Luego, se busca dentro de la primera lista, un elemento x_i *tal que sea igual al elemento* x_{2i}. *Conociendo tal i, se calcula* $r = b_i - b2i\ modn$ *y se calcula su inverso. El logaritmo buscado será el producto:* $r^{-1} \cdot (a_{2i} - ai)\ mod\ n$.

Este método funciona porque en la primera lista se generan x_i *de tal manera que* $x_i = \alpha^{a_i}\beta^{b_i}$, *y se buscan dos que cumplan que:* $\alpha^{a_i}\beta^{b_i} = \alpha^{a_{2i}}\beta^{b_{2i}}$, *por lo que:*

$$\begin{aligned} \beta^{(b_i - b_{2i})} &= \alpha^{(a_{2i} - a_i)} \Rightarrow \\ (b_i - b_{2i}) log_\alpha \beta &= (a_{2i} - a_i). \end{aligned}$$

Por ejemplo, sea $G = \mathbb{Z}_{383}$, $\alpha = 2$ *un generador de* G, $\beta = 217$. *Si generamos las listas que el algoritmo Pollard-Rho requiere obtenemos la siguiente tabla:*

i	x_i	a_i	b_i	x_{2i}	a_{2i}	b_{2i}
1	217	0	1	363	0	2
2	363	0	2	34	1	4
3	17	0	4	202	2	5
4	34	1	4	173	2	7
5	101	1	5	14	3	8
6	202	2	5	331	4	9
7	172	2	6	29	5	10
8	173	2	7	330	6	11

i	x_i	a_i	b_i	x_{2i}	a_{2i}	b_{2i}
9	346	3	7	256	13	22
10	14	3	8	34	14	23
11	28	4	8	202	15	24
12	331	4	9	173	15	26
13	206	4	10	14	16	27
14	29	5	10	331	17	28
15	58	6	10	29	18	29
16	330	6	11	330	19	30

Donde observamos que $x_{16} = x_{32}$, *luego,* $r = b_{16} - b_{32} = 172 \mod 191$ *y* $r^{-1} = 10 \mod 191$, *por lo que* $log_\alpha \beta = (a_{32} - b_{16}) = 10(13) = 130 \mod 191$. *Se verifica que* $2^{130} = 217 \mod 383$.

4.2 Problema del Logaritmo Discreto en Curvas Elípticas

Como ya hemos visto, los lugares de grado uno de un campo elíptico forman un grupo abeliano bajo la operación definida en (2.25). Esta estrucutra de grupo hace posible hablar acerca del **Problema del Logaritmo Discreto en Curvas Elípticas** (PLDCE)

***Ejemplo* 4.2.1.** *Sea E la curva definida por $y^2 = x^3 - 10 + 21$ sobre $\mathbb{F}_{557}$ y sea $P = (2,3) \in E$. Utilizando los algoritmos ya descritos obtenemos que: $188P = (2,554)$, pero $554 \equiv -3$ mod 557, por lo que $188P = -P$ y $189P = \mathcal{O}$. En este caso, encontrar el logaritmo discreto de $\mathcal{O}$ dado P, equivale a encontrar el orden del elemento.*

Encontrar el logaritmo discreto utilizando como grupo una curva elíptica se considera más difícil que entontrarlo en un grupo $\mathbb{F}_q$ con *p primo*. Esto se debe en parte a la complejidad computacional que implica calcular la multiplicación escalar de un punto. Es por esto, que en la práctica, gran parte de los esquemas criptográficos utilizan curvas elípticas.

***Ejemplo* 4.2.2.** *ElGamal es un esquema de cifrado de llave pública. Su creador es el criptógrafo egipcio americano Taher ElGamal. Fue dado a conocer en 1985, [9], distinguiendose del resto de los esquemas de clave pública por que en el cifrado es utilizada, además de la clave pública del receptor, la clave privada del emisor. A continuación se describe dicho esquema.*

Supongamos que $\mathcal{A}$ quiere mandar un mensaje a $\mathcal{B}$. Previamente, B ha escogido una curva elíptica E sobre $\mathbb{F}_q$ y un punto $P \in E$. También $\mathcal{B}$, debe escoger un número entero s y calcula $B = sP$. La curva E, el punto P y B serán parámetros públicos. Una vez que $\mathcal{A}$ tiene dichos parámetros, debe:

1. *Expresar su mensaje como $M \in E$.*
2. *$\mathcal{A}$ debe escoger un número entero secreto j y calcula $jP = M1$.*
3. *$\mathcal{A}$ debe calcular $M2 = M + jB$ y envía a $\mathcal{B}$ $M1$ y $M2$.*

Para que $\mathcal{B}$ pueda leer el mensaje deberá calcular $M2 - sM1$ pues:

$$M2 - sM1 = (M + jB) - stP = M + tsP - sjP = M.$$

Dado que B y P son públicos, es necesario que su logaritmo discreto sea muy difícil de encontrar.

4.2.1 Ataque al PLDEC

Una de las maneras encontradas de atacar el PLD en curvas elípticas, es transformar el problema al PLD en un grupo multiplicativo $\mathbb{F}_q^*$. Uno de estos ataques es conocido como el ataque MOV, propuesto por Menezes, Okamoto y Vanston, [10]. Utiliza un mapeo llamado *de Weil.* Este ataque afecta a las curvas clasificadas como *supersingulares.* [2]

La idea general del ataque MOV es la siguiente: Si $P, Q \in \mathbb{P}_F^1$ y $P, Q \in E[m]$, tales que $P = kQ$, entonces para obtener el logaritmo discreto de P dado Q, primero debemos encontrar $P \in \mathbb{P}_F^1$ tal que $e_m(P, S) \neq 1$, donde e_m denota el Mapeo de Weil. Después calculamos: $e_m(P, S) = a$ y $e_m(P, S) = b$, para finalmente encontrar el logaritmo discreto de b dado a.

Mapeo de Weil

Supongamos que E una curva elíptica y $\mathcal{O}$ su punto al infinito. Recordemos que $E[m]$ es el grupo de m-torsión de E. Supongamos $E[m] \subseteq E$. Sean $P, Q \in \mathbb{P}_F^1$ tales que $P, Q \in E[m]$y $P \neq Q$. Sean $A, B \in \mathcal{D}_F^0$ tales que:

$$A \sim P - \mathcal{O}$$
$$B \sim Q - \mathcal{O}$$

y $supp\ A \cap supp\ B = \emptyset$. Sean f_A, f_B dos funciones tales que

$$(f_A) = mA \quad y \quad (f_B) = mB \tag{4.6}$$

OBSERVACIÓN: La existencia de estas dos funciones queda asegurada por el Teorema de Aproximación.

Definimos el **Mapeo de Weil de P y Q** por:

$$\begin{aligned} e_m : E[m] \times E[m] &\rightarrow K^* \\ (P, Q) &\mapsto \frac{f_A(B)}{f_B(A)} \end{aligned} \tag{4.7}$$

[2] Una curva elíptica supersingular sobre $\mathbb{F}_q$ con $q = p^r$, p primo, será aquella que no es singular, que tiene exactamente $q + 1 - t$ puntos y donde se cumple $p|t$. En algunos textos, al número t se le nombra *traza* ó *traza de Frobenius.*

Este mapeo cumple las siguientes propiedades:

- ⋆ *Identidad.* $\forall\ P \in E[m],\ e_m(P,P) = 1$.
- ⋆ *Alternante.* $\forall\ P,\ Q \in E[m], e_m(P,Q) = e_m(Q,P)^{-1}$.
- ⋆ *Bilinealidad.* $\forall P,\ P',\ Q,\ Q' \in E[m],\ e_m(P \oplus P', Q) = e_m(P,Q)e_m(P',Q)$ *y* $e_m(P, Q \oplus Q') = e_m(P,Q)e_m(P,Q')$.
- ⋆ *No degenerado. Si* $P \in E[m]$, *entonces,* $e_m(P,\mathcal{O}) = 1$. *Si* $e_m(P,Q) = 1\ \forall Q$, *entonces* $P = \mathcal{O}$).
- ⋆ *Si* $E[n] \subseteq E(\mathbb{F}_{q^k})$ *entonces* $e_m(P,Q) \in \mathbb{F}_{q^k},\ \forall P, Q \in E[n]$.

Ahora veremos como podemos calcular dicho mapeo. Victor Miller, [11], [10], propuso el siguiente algoritmo para el cual es necesario saber cómo sumar dos divisores de grado cero. Supongamos que $D_1, D_2 \in \mathcal{D}_F^0$ con:

$$D_1 = P_1 - \mathcal{O} + (f_1)$$
$$D_2 = P_2 - \mathcal{O} + (f_2)$$

donde, $P_1, P_2 \in \mathbb{P}_F$ y $f_1, f_2 \in F/K$, entonces:

$$D_1 + D_2 = P_3 - \mathcal{O} - (f_1 * f_2 * f_3), \tag{4.8}$$

donde $P1 \oplus P_2 = P_3$, (con $\oplus$ definida en (2.25), $f_3 = \lambda/\nu$ siendo λ la línea de P_1 y P_2 y ν la línea de P_3 y su inverso P_3' bajo $\oplus$).

Para calcular el mapeo de Weil, debemos encontrar f_A y f_B. El algoritmo indica que primero debemos formar la cadena creciente de números: $1 = a_1, a_2, ..., a_t = m$, donde $t \leq 2log_2 m$ y a_i depende de a_j con $j < i$. Por ejemplo, si $m = 27$, $2log_2 m \approx 9.5$ formamos la cadena:

$$1 = a_1,\ a_2 = 2,\ a_3 = 3 = a_1 + a_2,\ a_4 = 6 = a_3 + a_3$$
$$a_5 = 12 = a_6 + a_6,\ a_6 = 24 = a_5 + a_5\ a_7 = 27a_6 + a_3.$$

de donde obtenemos que $t = 7$. Después escogemos aleatoriamente dos lugares T y U de grado uno tales que $P \oplus T$ y T sean distintos de $\pm a_i U$ y $\pm a_i(Q \oplus U)$ y

$Q \oplus U$ y U sean distintos de $\pm a_i T$ y $\pm a_i(P \oplus T)$ para toda i, $1 \leq i \leq t$. Una vez seleccionado los puntos, haremos $A = (P+T) - T$ y $B = (Q+U) - U$, entonces:

$$e_m(P,Q) \quad \mapsto \quad \frac{f_A(Q \oplus U)}{f_B(P \oplus T)} \frac{f_B(T)}{f_A(U)}.$$

Ataque MOV

El algoritmo del ataque MOV para curvas supersingulares queda descrito a continuación:

Algortimo:	Ataque Mov para curvas supersingulares
Entrada:	P de orden n en una curva supersingular $E(F_q)$. y $R \in < P >$.
Salida:	Un número entero l tal que $R = lP$.
	1) Determinar k y c correspondientes a la curva. 2)Escoger un punto $Q' \in E_{q^k}$ y hacer $Q = (cn_1/n)Q'$ 3)Calcular $\alpha = e_n(P,Q)$ y $\beta = e_n(R,Q)$. 4)Calcular el logaritmo discreto l' de β en base α en F_{q^k}. 5)Verificar que $l'P = R$. Si ocurre la igualdad, entonces $l' = l$. En caso contrario, el orden de α debe ser menor a n y se deberá regresar al paso 2. Regresa: l.

Para determinar k y c en el paso 1 del algoritmo, primero debemos clasificar la clase de la curva respecto a la siguiente lista, donde la curva $E(F_q)$ es supersíngular y $q = p^m$ para algún p primo.

(I) $t = 0$ y $E(F_q) \cong \mathbb{Z}_{q+1}$.
(II) $t = 0$, $E(F_q) \cong \mathbb{Z}_{(q+1)/2} \oplus \mathbb{Z}_2$ y $q \equiv 3 mod 4$.
(III) $t^2 = q$ y m es *par*.
(IV) $t^2 = 2q$, $p = 2$ y m es *impar*.
(V) $t^2 = 3q$, $p = 3$ y m es *impar*.
(VI) $t^2 = 4q$ y m es *par*.

Una vez identificada la clase de la curva podemos obtener c y k.

Clase de la curva	t	n_1	k	c
I	0	$q+1$	2	1
II	0	$(q+1)/2$	2	2
III	$\pm\sqrt{q}$	$q+1\mp\sqrt{q}$	3	$\sqrt{q}\pm 1$
IV	$\pm\sqrt{2q}$	$q+1\mp\sqrt{2q}$	4	$q\pm\sqrt{2q}+1$
V	$\pm\sqrt{3q}$	$q+1\mp\sqrt{3q}$	6	$(q+3)(q\pm\sqrt{3q}+1)$
VI	$\pm 2\sqrt{q}$	$\sqrt{q}\mp 1$	1	1

***Ejemplo* 4.2.3.** *Sea $E/K : y^2 = x^3 + 3x$ donde $K = \mathbb{F}_{11}$. Vamos a encontrar el logaritmo de $R = (3,6)$ dado $P = (1,9)$. Primero obtendremos información acerca de la curva.*

La cota de Hasse[3] *para campos elípticos, nos dice que si $\mathcal{N}$ es el número de puntos de la curva, entonces:*

$$q + 1 - 2\sqrt{q} < \mathcal{N} < q + 1 + 2\sqrt{q},$$

por lo que:

$$\begin{aligned} q + 1 - 2\sqrt{11} \; &< \mathcal{N} < \; q + 1 + 2\sqrt{11}, \\ 6.4 \; &< \mathcal{N} < \; 19.6. \end{aligned} \tag{4.10}$$

Buscamos los puntos de la curva y encontramos:

Punto	*Orden*	*Punto*	*Orden*
$P_0 = \mathcal{O}$	1	$P_6 = (3,5)$	3
$P_1 = (0,0)$	2	$P_7 = (3,6)$	3
$P_2 = (1,2)$	6	$P_8 = (6,5)$	4
$P_3 = (1,9)$	6	$P_9 = (6,6)$	4
$P_4 = (2,5)$	12	$P_{10} = (7,1)$	12
$P_5 = (2,6)$	12	$P_{11} = (7,10)$	12

Tenemos que $\mathcal{N} = 12 = q + 1$, por lo que $t = 0$, así que tenemos una curva clasificada como supersingular. Por otro lado, tenemos que $E/K \cong \mathbb{Z}_{12}$, entonces la curva es de clase I y tenemos que $n_1 = q + 1$, $k = 2$, y $c = 1$. Observamos que el orden de P es $n = 6$.

Escogemos $Q' = (6,6)$. Este punto debe pertenecer a la curva $E(\mathbb{F}_{11^2})$. Ahora hacemos:

$$Q = (cn_1/n)Q' = ((q+1)/6)Q' = 2Q' = (0,0) = P_1$$

Siguiendo el algortimo del ataque, debemos calcular dos mapeos de Weil: $e_6 = (P_3, P_1)$ y $e_6 = (P_7, P_1)$. Para ambos mapeos, utilizaremos la cadena $a_1 = 1$, $a_2 = 2$, $a_3 = 4$, $a_4 = 6$.

[3] La cota indica que si N el número de puntos en una curva de género g sobre un campo finito con q elementos, se cumple que: $q + 1 - 2g\sqrt{q} \leq N \leq q + 1 + 2g\sqrt{q}$.

⋆ **Mapeo de Weil:** $e_6(P_3, P_1)$. *Primero calcularemos el mapeo de Weil en los puntos* $P_3 = P$ *y* $P_1 = Q$. *Según el algoritmo de Miller, primero debemos escoger dos puntos* T *y* U *tales que:* $\pm a_i P$ *y* $\pm a_i(P \oplus T)$ *sean diferentes a* U *y* $Q \oplus U$ *y* T *y* $P \oplus T$ *sean diferentes a* $\pm a_i U$ *y* $\pm a_i(Q \oplus U)$. *Escogemos los puntos* $P_7 = T$ *y* $P_8 = U$ *y verificamos que cumplen las características necesarias para ser* T *y* U, *esto es:*

$$\pm a_i P = \{(1,9),(3,5),(3,6),\mathcal{O},(1,2),(3,6),(3,5),\mathcal{O}\}$$
$$\pm a_i(P \oplus T) = \{(1,2),(3,6),(3,5),\mathcal{O},(1,9),(3,5),(3,6),\mathcal{O}\}$$

y $\pm a_i Q$ *y* $\pm a_i(Q \oplus U)$ *son diferentes a* T *y* $P \oplus T$*:*

$$\pm a_i Q = \{(0,0),\mathcal{O},\mathcal{O},\mathcal{O},(0,0),\mathcal{O},\mathcal{O},\mathcal{O}\}$$
$$\pm a_i(Q \oplus U) = \{(6,6),(0,0),\mathcal{O},(0,0),(6,5),(0,0),\mathcal{O},(0,0)\}$$

Primero calcularemos el divisor $6(P_3 \oplus P_7) - 6\mathcal{O} = 6(P_2)6 - \mathcal{O}$*:*

$$\begin{aligned}
P_2 - \mathcal{O} &= P_2 - \mathcal{O} + (1) \Rightarrow \\
2P_2 - 2\mathcal{O} &= P_7 - \mathcal{O} + (\frac{(y+4x+5)}{(x+8)}) \Rightarrow \\
4P_2 - 4\mathcal{O} &= P_6 - \mathcal{O} + (\frac{(y+4x+5)^2}{(x+8)^2}.\frac{(y+3x+7)}{(x+8)}) \Rightarrow \\
6P_2 - 6\mathcal{O} &= (\frac{(y+4x+5)^3}{(x+8)^3}.\frac{(y+3x+7)}{(x+8)}.\frac{(x+8)}{(1)}) \\
&= (\frac{(y+4x+5)^3(y+3x+7)}{(x+8)^3}) \qquad (4.12)
\end{aligned}$$

y ahora debemos calcular el divisor correspondiente a $6P_7 - 6\mathcal{O}$*:*

$$\begin{aligned}
P_7 - \mathcal{O} &= P_7 - \mathcal{O} + (1) \Rightarrow \\
2P_7 - 2\mathcal{O} &= P_6 - \mathcal{O} + (\frac{(y+3x+7)}{(x+8)}) \Rightarrow \\
4P_7 - 4\mathcal{O} &= P_7 - \mathcal{O} + (\frac{(y+3x+7)^2}{(x+8)^2}.\frac{(y+8x+4)}{(x+8)}) \Rightarrow \\
6P_7 - 6\mathcal{O} &= (\frac{(y+3x+7)^3}{(x+8)^3}.\frac{(y+8x+4)}{(x+8)}.\frac{(x+8)}{(1)}) \\
&= (\frac{(y+3x+7)^3(y+8x+4)}{(x+8)^3}) \qquad (4.13)
\end{aligned}$$

De las ecuaciones 4.12 y 4.13 tenemos:

$$\begin{aligned}
(f_A) &= 6A \qquad (por \quad 4.6\ ) \\
&= m((P \oplus T) - T) = m(P \oplus T) - mT = \\
&= 6P_2 - 6P_7 = (6P_2 - 6\mathcal{O}) - (6P_7 - 6\mathcal{O}) = \\
&= (\frac{(y+4x+5)^3(y+3x+7)}{(x+8)^3}) - (\frac{(y+3x+7)^3(y+8x+4)}{(x+8)^3}) \\
&= (\frac{(y+4x+5)^3(y+3x+7)(x+8)^3}{(x+8)^3(y+3x+7)^3(y+8x+4)}) \\
&= (\frac{(y+4x+5)^3}{(y+3x+7)^2(y+8x+4)})
\end{aligned}$$

por lo que:

$$f_A = \frac{(y+4x+5)^3}{(y+3x+7)^2(y+8x+4)} \tag{4.14}$$

Ahora debemos calcular la función f_B, por lo que calcularemos el divisor hacemos $6(P_1 \oplus P_8) = 6(P_9)$ y calculamos:

$$\begin{aligned}
P_9 - \mathcal{O} &= P_1 - \mathcal{O} + (1) \ \Rightarrow \\
2P_9 - 2\mathcal{O} &= P_1 - \mathcal{O} + (\frac{(y+10x)}{(x)}) \ \Rightarrow \\
4P_9 - 4\mathcal{O} &= (\frac{(y+10x)^2}{(x)^2}.\frac{x}{1}) = (\frac{(y+10x)^2}{(x)}) \ \Rightarrow \\
6P_9 - 6\mathcal{O} &= (2P_9 - 2\mathcal{O}) + (P_9 - 4\mathcal{O}) = \\
&= P_1 - \mathcal{O} + (\frac{(y+10x)}{(x)}) + (\frac{(y+10x)^2}{(x)}) + (\frac{x}{1}) \\
&= P_1 - \mathcal{O} + (\frac{(y+10x)^3}{(x)})
\end{aligned} \tag{4.15}$$

y también calculamos $6P_8 - 6\mathcal{O}$:

$$\begin{aligned}
P_8 - \mathcal{O} &= P_1 - \mathcal{O} + (1) \ \Rightarrow \\
2P_8 - 2\mathcal{O} &= P_1 - \mathcal{O} + (\frac{(y+10x+1)}{(x)}) \ \Rightarrow \\
4P_8 - 4\mathcal{O} &= (\frac{(y+10x+1)^2}{(x)^2}.\frac{(x)}{(1)}) = (\frac{(y+10x+1)^2}{(x)}) \ \Rightarrow \\
6P_8 - 6\mathcal{O} &= (2P_8 - 2\mathcal{O}) + (4P_8 - 4\mathcal{O}) = \\
&= P_1 - \mathcal{O} + (\frac{(y+10x+1)}{(x)}) + (\frac{(y+10x+1)}{(x)}) + (\frac{x}{1}) \\
&= P_1 - \mathcal{O} + (\frac{(y+10x+1)^3}{(x)})
\end{aligned} \tag{4.16}$$

De las ecuaciones 4.15 y 4.16 tenemos:

$$\begin{aligned}(f_B) &= 6P_9 - 6P_8 = (6P_9 - 6\mathcal{O}) - (6P_8 - 6\mathcal{O}) = \\ &= P_1 - \mathcal{O} + (\frac{(y+10x)^3}{(x)}) - (P_1 - \mathcal{O} + (\frac{(y+10x+1)^3}{(x)}) = \\ &= (\frac{(y+10x)^3}{(y+10x+1)^3})\end{aligned}$$

por lo que:

$$f_B = \frac{(y+10x)^3}{(y+10x+1)^3} \tag{4.17}$$

Por último, evaluar:

$$\frac{f_A(Q \oplus U)}{f_B(P \oplus T)} \frac{f_B(T)}{f_A(U)} = \frac{f_A(P_1 \oplus P_8)}{f_B(P_3 \oplus P_7)} \frac{f_B(P_7)}{f_A(P_8)} = \frac{4}{7} \cdot \frac{3}{1} = 12(7^{-1}) = 12(8) = 8 \ mod\ 11 \tag{4.18}$$

por lo que: $e_6(P_3, P_1) = 8$.

⋆ **Mapeo de Weil:** $e_6 = (P_7, P_1)$. *Para calcular este mapeo utilizaremos nuevamente el algoritmo de Miller. Primero observamos que* $T = P_3$ *y* $U = P_8$ *cumplen las características necesarias para ser* T *y* U *pues:*

$$\pm a_i P = \{(0,0), \mathcal{O}, \mathcal{O}, \mathcal{O}, (0,0), \mathcal{O}, \mathcal{O}, \mathcal{O}\}$$
$$\pm a_i (P \oplus T) = \{(1,2), (3,6), (3,5), \mathcal{O}, (1,9), (3,5), (3,6), \mathcal{O}\}$$

son valores diferentes a U *y* $Q \oplus U$ *y* $\pm a_i Q$ *y* $\pm a_i (Q \oplus U)$ *son diferentes a* T *y* $P \oplus T$*:*

$$\pm a_i Q = \{(0,0), \mathcal{O}, \mathcal{O}, \mathcal{O}, (0,0), \mathcal{O}, \mathcal{O}, \mathcal{O}\}$$
$$\pm a_i (Q \oplus U) = \{(6,6), (0,0), \mathcal{O}, (0,0), (6,5), (0,0), \mathcal{O}, (0,0)\}$$

son valores diferentes a T *y* $P \oplus T$.
En el inciso anterior, ya calculamos el divisor correspondiente a $P_3 \oplus P_7 = P_2$*:*

$$6P_2 - 6\mathcal{O} = (\frac{(y+4x+5)^3 (y+3x+7)}{(x+8)^3})$$

y queda calcular $6P_3 - 6\mathcal{O}$*:*

$$\begin{aligned} P_3 - \mathcal{O} &= P_3 - \mathcal{O} + (1) \Rightarrow \quad (4.19) \\ 2P_3 - 2\mathcal{O} &= P_6 - \mathcal{O} + (\frac{(y+7x+6)}{(x+8)}) \Rightarrow \\ 4P_3 - 4\mathcal{O} &= P_7 - \mathcal{O} + (\frac{(y+7x+6)^2}{(x+8)^2} \cdot \frac{(y+8x+4)}{(x+8)}) \Rightarrow \\ 6P_3 - 6\mathcal{O} &= (\frac{(y+7x+6)^3}{(x+8)^3} \cdot \frac{(y+8x+4)}{(x+8)} \cdot \frac{(x+8)}{(1)}) \\ &= (\frac{(y+7x+6)^3(y+8x+4)}{(x+8)^3} \quad (4.20) \end{aligned}$$

De las ecuaciones 4.19 y 4.20 tenemos:

$$\begin{aligned} (f_A) &= 6(P_3 + P_7) - 6P_3 \\ &= (\frac{(y+4x+5)^3(y+3x+7)}{(x+8)^3} - (\frac{(y+7x+6)^3(y+8x+4)}{(x+8)^3} \\ &= (\frac{(y+4x+5)^3(y+3x+7)}{(y+7x+6)^3(y+8x+4)}) \end{aligned}$$

por lo que:

$$f_A = \frac{(y+4x+5)^3(y+3x+7)}{(y+7x+6)^3(y+8x+4)} \quad (4.21)$$

También hemos calculado los divisores $6(P_1 + P_8) - 6\mathcal{O}$, $6(P_8) - 6\mathcal{O}$, *por lo que, hemos calculado la función* f_B*:*

$$f_B = \frac{(y+10x)^3}{(y+10x+1)^3} \quad (4.22)$$

Por último, debemos hacer:

$$\frac{f_A(Q \oplus U)}{f_B(P \oplus T)} \frac{f_B(T)}{f_A(U)} = \frac{f_A(P_1 \oplus P_8)}{f_B(P_7 \oplus P_3)} \frac{f_B(P_3)}{f_A(P_8)} = \frac{9}{7} \cdot \frac{2}{5} = \frac{7}{2} = 7(2^{-1}) = 7(6) \equiv 9 \ mod\ 11 \quad (4.23)$$

lo que quiere decir que $e_6(P_7, P_1) = 9$

De este modo, ahora debemos calcular el logaritmo discreto l' *de* $\beta = e_6(P_7, P_1) = 9$ *en base* $\alpha = e_6(P_3, P_1) = 8$ *en* $\mathbb{F}_{11^2}$*. (Recordemos que esta operación es un ataque al problema del logaritmo discreto en un campo* $\mathbb{F}_p$*, ver sección 4.1). En este caso,* $l' = 10$*, y coincide que* $P_7 = l'P_3$*, así que el logaritmo de* P_7 *en base* P_3 *en la curva* E/K*, es* 10*.*

Notas

Otro famoso ataque es el que propusieron Frey y Rück, [12]. Este utiliza otro mapeo llamado de *Tate* para transformar el PLDCE a PLD sobre $\mathbb{F}_q$. Este ataque, además de funcionar para curvas supersingulares también afecta a las curvas ordinarias de traza 2, es decir, curvas donde $t = 2$.

Existen un tipo de curvas elípticas nombradas *curvas anómalas*. Estas curvas son las que su traza es 1, es decir, si la curva está definida sobre $\mathbb{F}_q$ el número de puntos de estas curvas es igual a q. A estas curvas se les considera altamente débiles criptográficamente hablando, pues el PLDCE se puede reducir a al PLD del grupo *aditivo* $\mathbb{F}_q$, [13].

Capítulo 5

Códigos Asociados a Curvas Elípticas

Es esta sección se dan algunas nociones básicas de la teoría de códigos y su relación con los campos elípticos.

Sea $\mathbb{F}_q$ el campo finito con q elementos. Consideraremos el espacio vectorial $\mathbb{F}_q^n$ cuya dimensión es n y cuyos elementos son las $n-tuplas$ $a = (a_1, \ldots, a_n)$ con $a_i \in \mathbb{F}_q$. Un **código C** sobre el campo $\mathbb{F}_q$, será un subespacio lineal de $\mathbb{F}_q^n$ y nos referiremos a sus elementos como **palabras del código**. La **longitud de C**, será n y su **dimensión** la dimensión de C como subespacio de $\mathbb{F}_q$. Un $[n,k]$ código es un código de longitud n y dimensión k.

En general, se puede definir un código sobre cualquier conjunto finito no vacío. Cuando se define sobre $\mathbb{F}_q$ el código recibe el nombre de **código lineal.**

***Definición* 5.0.1.** *Dados* $a = (a_1, \ldots, a_n)$ *y* $b = (b_1, \ldots, b_n)$ *elementos de* $\mathbb{F}_q^n$, *definimos la función d entre a y b como*

$$d(a,b) := |\{i; a_i \neq 0\}|.$$

y la llamamos la ***distancia de Hamming****. Para cada elemento a de* $\mathbb{F}_q^n$ *se define* ***el peso de a*** *como* $d(a,0) := w(a)$.

OBSERVACIÓN: La distancia de Hammming es una métrica.

La **distancia mínima d(C)** de un código C es definida como:

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

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

$$d(C) := min\{w(c) \mid 0 \neq c \in C\}. \tag{5.3}$$

Un $[n,k]$ código con una distancia mínima d se denotará como $[n,k,d]$. El **código dual $C^{\perp}$ de** C es el código lineal que consiste en todos los vectores ortogonales para cada palabra de C, en otras palabras:

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

donde $<,>$ representa el producto interno en $\mathbb{F}_q^n$.

Definición* 5.0.2.** *Sea C un código con parámetros $[n,k]$ sobre $\mathbb{F}_q$. La* ***matriz generadora de C *es una matriz de $k \times n$ cuyas filas son bases en C.*

Definición* 5.0.3.** *Un código C con parámetros $[n,k,d]$, es un código* ***h-extendible *si existe un código C' con parámetros $[n+h,k,d+h]$ tal que $\pi_{n,h} : \mathbb{F}_q^{n+h} \mapsto \mathbb{F}_q^n$, tal que $\pi_n(a_1,...,a_{n+h}) = (a_1,...,a_n)$.*

La siguiente proposición establece una cota superior para la dimensión y la distancia mínima de un código C, dada en términos de la longitud. Se le conoce como **Cota del Singulete**.

***Proposición* 5.0.1.** *Para un $[n,k,d]$-código C, se tiene lo siguiente:*

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

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

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

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

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

Al número entero $s(C) := n - k + 1 - d$ lo llamaremos **defecto del Singulete**. A los códigos que cumplen que $k + d = n + 1$, es decir para los cuales $s(C) = 0$, son llamados **códigos separables de distancia máxima** (códigos MDS). Si $s(C) = 1$ llamaremos a C, **código casi separable** (AMDS).

Se sabe que el código dual de un código MDS es un código MDS, pero en el caso de un código AMDS no siempre se tiene que el dual sea AMDS también. En el caso en el que sí lo sea, se decir, en el caso que se cumpla que $s(C) = s(C^{\perp}) = 1$ se dice que el código C, es **cercano** a ser MDS, (NMDS).

***Definición* 5.0.4.** *Sean $F/\mathbb{F}_q$ un campo de funciones algebraico de género g, $\{P_1, ...P_n\}$ un conjunto de lugares de $F/\mathbb{F}_q$ de grado 1, $D = P_1 + ...P_n$ y G un divisor de $F/\mathbb{F}_q$ tal que supp $G \cap$ supp$D = \emptyset$. El **código Goppa geométrico** $C_{\mathcal{L}}(D, G)$ asociado a los divisores D y G se define como:*

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

OBSERVACIÓN: Dado que el grado de los lugares P_i es uno, entonces $x(P_i) \in F_{P_i} = \mathbb{F}_q$.

***Teorema* 5.0.1.** *$C_{\mathcal{L}}(D, G)$ es un $[n, k, d]$-código donde:*

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

Demostración.
Consideremos el mapeo $\xi : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n$ dado por:

$$\xi(x) := ((x(P_1), \ldots, x(P_n))).$$

Si restringimos el codominio de ξ a $C_{\mathcal{L}}(D, G)$, entonces, tenemos un mapeo suprayectivo y el $ker\xi$ serán los elementos $x \in P_i$, es decir, los elementos tales que $v_{P_i}(x) > 0$. Se tiene que si $v_{P_i}(x) > 0$, entonces, $x \in \mathcal{L}(G - D)$ y por otro lado, si $x \in \mathcal{L}(G - D)$, entonces $0 \leq (x) + G - D$ así que $D \leq (x) + G$ por lo que $x \in ker\xi$, así que $ker\xi = \mathcal{L}(G - D)$.

Por lo tanto $k = dim\ C_{\mathcal{L}}(D, G) = dim\ \mathcal{L}(G) - dim\ \mathcal{L}(D, G)$. Supongamos que $C_{\mathcal{L}}(D, G) \neq 0$. Si $x \in \mathcal{L}(G)$, entonces, $w(\xi(x)) = d$, entonces se tiene que hay $n - d$ lugares en el soporte de D que son ceros de x, por lo que:

$$0 \neq x \in \mathcal{L}(G - (P_{i_1}, ..., P_{i_{n-d}})),$$

por lo que $0 \leq grado\ (G - (P_{i_1}, ..., P_{i_{n-d}})) = grado\ G - n + d$. Por lo que se tiene que $d \geq n - grado\ G$. $\diamondsuit$

***Corolario* 5.0.1.** *Sea G un divisor tal que grado $G < n$, entonces $C_{\mathcal{L}}(D,G)$ es un $[n,k,d]$-código, con:*

$$k + d \geq 1 + n - g.$$

Demostración.
Del teorema (5.0.1) tenemos que $k = dim\ G - dim\ (G-D)$. Por otro lado tenemos que:

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

así $dim\ (G-D) = 0$. Por el teorema de Riemann se llega a que:

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

por lo que:

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

Códigos Goppa de una curva elíptica

***Definición* 5.0.5.** *El código Goppa asociado a la curva elíptica $\mathcal{E}$, será el código geométrico Goppa construido con los parámetros de dicha curva.*

Del corolario 5.0.1, tenemos que $k + d \geq n$ pues $g = 1$, por lo que obtenemos la siguiente relación:

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

es decir, $n = k + d$ ó $n + 1 = k + d$. En el primer caso, tenemos uno del tipo MDS y en el segundo del tipo AMDS.

5.1 Un Código Elíptico

Código Goppa de la curva $y^2 = x^3 + x + 6$ sobre $\mathbb{F}_{11}$

Queremos estudiar el Código Goppa generado por la curva $y^2 = x^3 + x + 6$ sobre $\mathbb{F}_{11}$. Primero observamos que los puntos de la curva son:

$P_1 = (2,4)$	$P_6 = (5,9)$
$P_2 = (2,7)$	$P_7 = (7,2)$
$P_3 = (3,5)$	$P_8 = (7,9)$
$P_4 = (3,6)$	$P_9 = (8,3)$
$P_5 = (5,2)$	$P_{10} = (8,8)$

El divisor $D = \sum P_i$ correspondiente a este código, donde P_i son lugares de grado 1, estará dado por el divisor formado por la suma de los puntos de la curva. El divisor G correspondiente podemos construirlo a partir de Q_∞, es una extensión del lugar P_∞ que es un polo de x, de manera que $G = kQ_\infty$. Para mostrar el ejemplo, supongamos que $k = 5$. Ahora tenemos que dar una base para el espacio $\mathcal{L}(5Q_\infty)$:

$$\mathcal{L}(5Q_\infty) =< 1, x, y, xy, x^2 > .$$

Estos parámetros generan un código goppa con parámetros $[12, 5, 7]_{11}$ con matriz generadora:

	$(2,4)$	$(2,7)$	$(3,5)$	$(3,6)$	$(5,2)$	$(5,9)$	$(7,2)$	$(7,9)$	$(8,3)$	$(8,8)$
1	1	1	1	1	1	1	1	1	1	1
x	2	2	3	3	5	5	7	7	9	9
y	4	7	5	6	2	9	2	9	3	8
xy	8	3	4	7	10	1	3	8	2	9
x^2	4	4	9	9	3	3	5	5	9	9

Resumen y conclusiones segunda parte

En la segunda parte de este trabajo se abordaron algunas aplicaciones de los campos elípticos (ó curvas elípticas).

La primer aplicación fue una propuesta para la solución al problema de factorización entera. Cabe mencionar, que esta aplicación está basada en la estructura de grupo abeliano de los lugares de grado uno de un campo. Después encontramos un uso de las curvas elípticas a la criptografía. De nuevo, este uso es gracias a las características propias de las curvas. Por último, dimos la construcción de códigos elípticos. Esta aplicación depende directamente de la teoría desarrollada en la primera parte, tanto en notación, como en conceptos y resultados.

Actualmente, la criptografía de curvas elípticas es una de las herramientas más utilizadas para el intercambio de información y como consecuencia es un tema activo para la investigación matemática. Cabe mencionar que la seguridad de estos sistemas criptográficos dependen del desarrollo tecnológico, por lo tanto, a medida que la capacidad de cómputo conocida sea mayor estos sistemas, tal vez, se vuelvan obsoletos.

Además de los problememas relacionados directamente con la criptografía, existen algunos otros vinculados con las curvas elípticas, por ejemplo la Conjetura de Birch y Swinnerton-Dyer.

Apéndice

Grupos, Anillos y Campos

Un conjunto no vacío G será un **grupo** si en G se puede definir una operación "+" tal que si a, b, c son elementos cualesquiera del grupo, entonces se cumple:

1. $a + b$ es un elemento de G, para cualesquiera a y b.

2. $a + (b + c) = (a + b) + c$, es decir, "+" es una operación asociativa.

3. Existe un elemento *neutro* de G, al que se denotará como "0", tal que $a + 0 = 0 + a = a$ para cualquier elemento a de G.

4. Todo elemento de G tiene un inverso dentro de G, es decir, si $a \in G$ entonces $-a \in G$ y se cumple que $a + (-a) = (-a) + a = 0$.

Cuando se cumple que $a+b = b+a$ entonces se dice que G es un **grupo abeliano**.

Llamaremos anillo a un conjunto R no vacío en el cual, se pueden establecer dos operaciones, (a estas operaciones las denotaremos como "+" y "$\cdot$") y que cumplen los siguientes axiomas:

1. R forma un grupo abeliano con la operación "+".

2. La operacion "$\cdot$"es asociativa.

3. Para cualesquiera $a, b, c \in R$ se cumple que $(a + b) \cdot c = a \cdot c + b \cdot c$.

Que R sea **conmutativo** quiere decir que la operación "$\cdot$"es conmutativa. Llamamos **campo** a un anillo conmutativo si todo elemento de R tiene un inverso multiplicativo dentro de R.

Si un subconjunto N de R forma un grupo con la operación "+"y satisface que $rN \subseteq N \; \forall r \in R$ entonces lo llamaremos **ideal** de R. Si $N \nsubseteq M, \forall M$ ideal de R, se dice que N es **ideal maximal**.

Existen muchos resultados acerca de estas estructuras. Para fines de este trabajo, mencionaré sólo los que son de más utilidad. Si se requiere mayor información [14] ofrece una guía completa de estos temas.

***Teorema* .0.1.** *Si R es anillo conmutativo unitario, entonces M es ideal maximal de R si y solamente si R/M es un campo.*

Demostración.
Sea $(a+M) \in R/M$, $a \notin M$ Se mostrará que $(a+M)$ tiene inverso multiplicativo en R/M Sea $N = \{ra+m | r \in R, m \in M\}$. N es grupo aditivo pues $(r_1a+m_1)+(r_2a+m_2) = (r_1+r_2)a+(m_1+m_2)$, $0 = 0a+0y-(ra+m) = (-r)a+(-m)$. Además $r_1(ra+m) = (r_1m) \Rightarrow r_1(ra+m) \in N$ y $ra+m \in N$, por lo tanto N es ideal de R. Luego, $a = (1a+0) \Rightarrow a \in N$ para $m \in M$ y $m = 0a+m \Rightarrow M \subseteq N$, entonces $a \in N$ y $a \in M$, pero M es ideal maximal $N = R$. Como $1 \in N$, $\exists b \in R$ tal que $1 = ba + M$, por lo tanto $1 + M = (b+M)(a+M) \Rightarrow (b+M)$ es inverso multiplicativo de $a + M$.

Por otro lado, si R/M es campo, N cualquier ideal de R tal que $M \subset N \subset R$ y γ homomorfismo canónico de A, sobre R/M con $(o+M) \subseteq N\gamma \subset R/M$. La contradicción estará en que un campo no contiene ideales propios. Por lo tanto M es ideal maximal. $\diamondsuit$

Si R es un anillo conmutativo y $a \in R$ el ideal $\{ra | r \in R\}$ de todos los múltiplos del elemento a se le denomina **ideal principal generado por a** y se denotará como $< a >$. Un ideal N de R, es un ideal principal si $N =< a >$ para algún $a \in R$.

Sea F un campo. Llamaremos la **característica de** F al menor entero positivo n tal que $n \cdot a = 0$, $a \in F$. Si F es un campo finito entonces su característica deberá de ser igual a un número primo, pues de lo contario no será difícil encontrar divisores propios de cero dentro de F. Al subgrupo de F, $\{0, ..., p-1\}$. lo denotaremos como $\mathbb{F}_P$, y lo llamaremos **campo primo.**

Sea $< R, +, * >$ un anillo. Un **polinomio** $f(x)$ con coeficientes en R, es una suma formal infinita

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n + ...$$

donde $a_i \in R$ y $a_i = 0$ para todos, excepto un número finito de valores de i.

Al conjunto de todos los polinomios de un anillo R, lo denotaremos como $R[x]$. Éste conjunto será un anillo bajo la suma y la multiplicación polinomial. Algunas propiedades de R, se darán, gracias a las características del anillo R, por ejemplo, si R es conmutativo, entonces lo es $R[x]$, y si R tiene elemento unitario, entonces este también será unitario en $R[x]$.

A un anillo sin divisores propios de cero se llama **dominio entero**. La teoría de anillos (Ver [14]) nos dice que dado cualquier dominio entero D, es posible construir un campo de cocientes de D. Este campo de cocientes contiene una copia de D. Además si M es un campo que contiene a un dominio entero D, entonces L contiene al campo de cocientes de D.

Espacios Vectoriales

Sea K un campo y V un grupo abeliano. Diremos que V es un espacio vectorial sobre K si podemos definir una operación entre los elementos de K y los elementos de V tal que se cumplan las siguientes condiciones:

1. Leyes distributivas: $\alpha(a + b) = \alpha a + \alpha b$ y $(\alpha + \beta)a = \alpha a + \beta a$.

2. Ley asociativa: $\alpha(\beta a) = (\alpha\beta)a$.

3. Neutro multiplicativo: $1a = a$.

donde $a, b \in V$, $\alpha, \beta \in K$ y 1 es el neutro multiplicativo en K.

Dentro de cada espacio vectorial V, existe un subconjunto que al ser operado con los elementos del campo K, genera el espacio V. Cuando los elementos de este subconjunto son linealmente independientes, este recibe el nombre de **base**.

Llamaremos **dimensión** de el espacio vectorial V sobre F a la cardinalidad de su base.

Pequeño Teorema de Fermat

El siguiente teorema es llamado, "Pequeño Teorema de Fermat". Su demostración puede encontrarse en [14].

***Teorema* .0.2.** *(Fermat) Si $\alpha \in \mathbb{Z}$ y p es primo que no divide α, entonces p divide $\alpha^{p-1} - 1$, esto es, $\alpha^{p-1} = 1 \ mod \ p$, para $\alpha \not\equiv 0 \ mod \ p$.*

***Corolario* .0.1.** *Si $\alpha \in \mathbb{Z}$, entonces $\alpha^p = a \ mod \ p$, para cualquier p primo.*

Extensiones de Campos

Definición* .0.1.** *Un campo E es un campo de* ***extensión del campo *F si $F \leq E$.*

Definición* .0.2.** *Un elemento α de un campo de extensión E de F se le llamará* ***algebraico sobre *F si existe algún $f(x) \neq 0 \in F[x]$ tal que $f(\alpha) = 0$. Si α no es algebraico lo llamaremos* ***elemento trascendente*** *sobre el campo F.*

Definimos Φ_α un homomorfismo de evaluación como sigue:

$$\Phi_\alpha : F[x] \mapsto E \tag{16}$$

$$(a_0 + a_1x + a_2x^2 + ... + a_nx^n)\Phi_\alpha \longrightarrow a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n.$$

El núcleo de Φ_α es un ideal principal de $F[x]$ generado por algún $p(x) \in F[x]$. Entonces $Ker\ \Phi_\alpha =< p(x) >$ deberá de ser constituido por todos los elementos de $F[x]$ que tienen como cero a α, con lo que si $f(\alpha) = 0$ para algún $f(x) \in F[x]$ diferente de cero, entonces $f(x) \in< p(x) >$, lo que quiere decir que $f(x) = p(x)r(x)$. De lo anterior podemos observar que $p(x)$ deberá de ser de grado minimal y si existiera otro elemento en $< p(x) >$ con el mismo grado deberá de ser de la forma $p(x)a$ con $a \in F$. En el caso que $p(x)$ no fuera un elemento irreducible, es decir $p(x) = q(x)r(x)$ entonces $p(\alpha) = q(\alpha)r(\alpha) = 0$ lo cual quiere decir que $q(\alpha) = 0$ ó $r(\alpha) = 0$ ya que E es un campo y contradice la minimalidad de $p(x)$. Por lo tanto $p(x)$ debe de ser un polinomio irreducible.

Definición* .0.3.** *Sea $\alpha \in E$ algebraico sobre F. Al único polinomio mónico $p(x)$ del párrafo anterior se le llamará* ***polinomio irreducible *de α sobre F y lo denotaremos como $irr(\alpha, F)$. Al grado de $p(x)$ se le denotará como $grad(\alpha, F)$.*

De la definición (5.1) tenemos dos casos para un elemento $\alpha \in E$:

a) **El elemento α es algebraico sobre F.** En éste caso en $nuc\Phi_\alpha$ es $< irr(\alpha, F) >$, el cuál, como ya lo hemos mencionado, deberá de ser un ideal maximal de $F[x]$. Además, $F[x]/ < irr(\alpha, F) >$ es un campo y resulta ser isomorfo a la imagen de $(F[x])\Phi_\alpha$ en E. éste subcampo de E será el menor subacampo de E que contenga a F a y α. Lo denotaremos por $F(\alpha)$. (Figura 1).

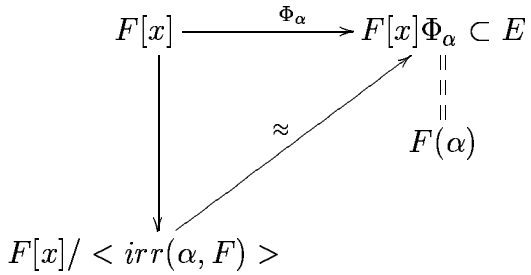


Figura 1: *a) Diagrama para un elemento algebraico.*

b) **El elemento α es trascendente sobre F.** Que el elemento α sea trascendente, quiere decir que no existe ningún polinomio diferente de cero en $F[x]$, para el cual α sea un cero. Esta condición pasa si y solamente si $f(x)(\Phi_\alpha) \neq 0$ para todos los polinomios de $F[x]$ no constantes, lo cual es cierto si y solamente si $nuc\ \Phi_\alpha = \{0\}$ y eso sucede si y sólo si Φ_α es un isomorfismo entre E y $F[x]$. A $Im\ \Phi_\alpha$ se le denotará por $F[\alpha]$. Como $F[\alpha] \subseteq E$ entonces E contiene al campo de cocientes de $F[\alpha]$ al que se hace referencia como $F(\alpha)$. (Ver Figura 2)

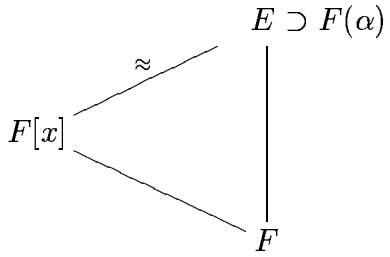


Figura 2: *a) Diagrama para un elemento trascendente.*

Definición* .0.4.** *Un campo de extensión E de un campo F es una* ***extensión simple de *F, si $E = F(\alpha)$, para algún $\alpha \in E$.*

El siguiente resultado se ilustra cómo es el campo $F(\alpha)$ en el caso de que α sea algebraico sobre F.

Teorema .0.3. *Sea E una extensión simple $F(\alpha)$ de un campo F con $\alpha \in E$ un elemento algebraico sobre F. Sean $n \geq 1$ el grado de $irr(\alpha, F)$. Entonces, todo elemento β de $E = F(\alpha)$ se puede expresar de manera única en la forma:*

$$\beta = b_0 + b_1\alpha_1 + ... + b_{n-1}\alpha^{n-1} \quad \textit{donde } b_i \in F.$$

EJEMPLO: El polinomio $p(x) = x^2 + x + 1 \ \in \mathbb{Z}_2[x]$ es irreducible sobre $\mathbb{Z}_2[x]$, pues ni el uno ni el cero de dicho campo son ceros de $p(x)$. Sabemos que existe un campo de extensión E de $\mathbb{Z}_2[x]$ que contiene algún cero α de x^2+x+1. Entonces, por el teorema anterior, $\mathbb{Z}_2(\alpha)$ tendrá como elementos a $0,\ 1,\ \alpha,\ 1+\alpha$. Los elementos anteriores forman un campo finito de cuatro elementos.

Si F tiene $q = p^n$, con p un número primo, elementos entonces E tiene q^n elementos, pues E es un espacio vectorial de dimensión n sobre F. Si E es un campo finito de caraterística p, donde p es un número primo, entonces E contiene exactamente p^n elementos, para algún entero positivo n.

Al subcampo de un campo E

$$\tilde{F} = \{\alpha \ \in E \mid \alpha \ es \ algebraico \ sobre \ F\}$$

se le denominará **cerradura algebraica**. Al campo que contenga a todos los ceros de algún conjunto de polinomio con coeficientes en el campo base se le llamará **campo de descomposición**. Este campo es un subcampo de la cerradura algebraica.

Sea E un campo finito con p^n elementos donde p es la característica de E. Se define $E^* := E - \{0\}$. E^* será un grupo multiplicativo de orden $p^n - 1$. Por lo que si α es un elemento de E^*, el orden de α dividirá a $p^n - 1$, por lo que tendremos $\alpha^{p^n-1} = 1$, de modo que $\alpha^{p^n} = \alpha$. Por lo tanto todo elemento del grupo E^* es solución al polinomio $X^{p^n} - X$. Además $X^{p^n} - X$, puede tener a lo m ás p^n elementos, por lo que si E es un campo finito de p^n elementos, entonces E, será el campo de descomposición del polinomio $X^{p^n} - X$.

Definición* .0.5.** *Un campo de extensión E de un campo F es un* ***extensión algebraica *de F, si todo elemento de E es algebraico sobre F.*

Si un campo de extensión E de un campo F es de dimensión finita n como espacio vectorial sobre F, entonces se dice que es una **extensión finita de grado n** sobre F. Denotamos como $[E : F]$ al grado n de E sobre F. Además, se tiene el siguiente resultado: "Un campo de extensión finita E de un campo F, es una extensión algebraica de F."

Campos de Funciones Racionales

Si F es un campo, entonces $F[x]$ no es un campo, pues $\nexists f(x) \in F[x]$ tal que $xf(x) = 1$. Por otro lado, $F[x]$ es un **dominio entero** y se sabe que a partir

de cualquier dominio entero D, es posible construir un campo de cocientes de D. Para el caso de $F[x]$, dicho campo de cocientes se denotará como $F(x)$. En otras palabras:

$$F(x) = \{\frac{f(x)}{g(x)} |\ f(x), g(x) \in F[x]\ y\ g(x) \not\equiv 0\}.$$

Este concepto se puede generalizar al caso del campo $F[x_0, x_1, ..., x_n]$, es decir, al campo de polinomios en n indeterminadas. Su campo cociente se denotará como $F(x_0, x_1, ..., x_n)$. A este campo se le llama **campo de funciones racionales en n indeterminadas sobre F**.

Bibliografía

[1] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Springer, 1993. ISBN 3540564896.

[2] Henri Cohen and Gerhard Frey, editors. *Handbook of elliptic and hyperelliptic curve cryptography.* CRC Press, 2005. ISBN 1–58488–518–1.

[3] Sangook Moon. A binary redundant scalar point multiplication in secure elliptic curve cryptosystems. *International Journal of Network Security,* 3 (2):132–137, 2006. URL `http://ijns.nchu.edu.tw/`.

[4] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography.* CRC Press, Inc., Boca Raton, FL, USA, 2003. ISBN 1584883650.

[5] Jr. Hendrik W. Lenstra. Elliptic curves and number-theoretic algorithms. *Mathematisch Instituut, Universitet van Amsterdam*, pages 99–120, 1987.

[6] Jr. Hendrik W. Lenstra. Factoring integers with elliptic curves. *Annals of Mathematics*, 126:649–673, 1987. ISSN 0003–486X.

[7] A. Menezes, P van Oorschot, and S. Vanstone. Handbook of applied cryptography - references, 2001. URL `citeseer.ist.psu.edu/428600.html`.

[8] Douglas R. Stinson. *Cryptography: Theory and Practice.* CRC Press, Inc., Boca Raton, FL, USA, 1995. ISBN 0849385210.

[9] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 10–18, New York, NY, USA, 1985. Springer-Verlag New York, Inc. ISBN 0-387-15658-5.

[10] Alfred Menezes, Scott Vanstone, and Tatsuaki Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. In *STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 80–89, New York, NY, USA, 1991. ACM. ISBN 0-89791-397-3.

[11] Victor S. Miller. Short programs for functions on curves. In *IBM Thomas J. Watson Research Center*, 1986.

[12] G. Frey, M. uller, and H. uck. The tate pairing and the discrete logarithm applied to elliptic curve cryptosystems, 1999. URL `citeseer.ist.psu.edu/frey98tate.html`.

[13] N. P. Smart. The discrete logarithm problem on elliptic curves of trace one. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12(3):193–196, 1999. URL `citeseer.ist.psu.edu/smart99discrete.html`.

[14] John B. Fraleigh. *A first course in abstract algebra (Addison-Wesley series in mathematics)*. Addison-Wesley Pub. Co, July 1976. ISBN 0201019841.

[15] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer, 1992.

[16] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976. URL `citeseer.ist.psu.edu/diffie76new.html`.

[17] Neal Koblitz. *A course in number theory and cryptography*. Springer-Verlag New York, Inc., New York, NY, USA, 1987. ISBN 0-387-96576-9.

[18] Friederike Brezing and Annegret Weng. Elliptic curves suitable for pairing based cryptography. *Des. Codes Cryptography*, 37(1):133–141, 2005. ISSN 0925-1022.

[19] Silverman and Suzuki. Elliptic curve discrete logarithms and the index calculus. In *ASIACRYPT: Advances in Cryptology – ASIACRYPT: International Conference on the Theory and Application of Cryptology*. LNCS, Springer-Verlag, 1998. URL `citeseer.ist.psu.edu/179336.html`.

[20] Andrew M. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In *Theory and Application of Cryptographic Techniques*, pages 224–314, 1984. URL `citeseer.ist.psu.edu/odlyzko84discrete.html`.

Índice de Materias