EL TEOREMA DE RIEMANN-ROCH
Y CÓDIGOS ÁLGEBRO-GEOMÉTRICOS

LUIS FELIPE MOSQUERA HERNÁNDEZ
Departamento de Matemáticas
Universidad del Valle

Resumen

En este documento se presenta un estudio de la construcción de los códigos introducidos por Goppa y de los aspectos fundamentales de la teoría de cuerpos de funciones algebraicas que requiere tal construcción.
Palabras clave: Teorema de Riemann-Roch

The Riemann-Roch Theorem and Algebro-Geometric codes

Abstract

This paper presents a study of the construction of the codes introduced by Goppa and the fundamental aspects of the theory of fields of algebraic functions that such construction requires.
Keywords: Riemann-Roch Theorem

Recibido: 02-12-2021
Aceptado: 20-5-2022
ORCID:
0000-0001-6972-9607

1. Introducción

Una de las áreas de aplicación del álgebra es la teoría de códigos cuyos inicios datan del año 1948 a raíz del artículo clásico de Shannon, *A Mathematical Theory of Communication* . Esta teoría se ocupa de la confiabilidad de la información a través de canales ruidosos y su principal objeto de estudio lo constituyen los códigos correctores de errores, cuyo propósito es agregar suficiente redundancia a un mensaje que se enviará por medio de un canal de tal forma que si no han ocurrido demasiados errores el receptor pueda recuperar el mensaje original. Es importante resaltar que estos son de gran utilidad en diversas aplicaciones, por ejemplo, a finales de los 60's y principio de los 70's la nave espacial de la NASA Mariner 9 tomó las primeras fotos a blanco y negro de Marte y las transmitió a través del espacio hasta la tierra usando un código conocido como Reed–Muller.

En el contexto de los códigos correctores de errores se destacan los códigos lineales, los cuales tienen estructura de espacio vectorial. Esta clase de códigos tiene asociado tres parámetros llamados; la longitud, la dimensión y la distancia mínima. Un problema central de esta teoría es construir códigos tales que la longitud no sea muy grande para que la transmisión de la información sea rápida y, que a su vez, la dimensión y la distancia mínima sean grandes en comparación con la longitud, pues de este modo se pueden transmitir una gran variedad de mensajes y se pueden corregir muchos errores.

Dentro de las construcciones de códigos lineales, vale la pena resaltar la presentada por Goppa en 1981, pues construyó códigos lineales a partir de un cuerpo de funciones algebraicas y mostró que los parámetros de estos dependen de las propiedades algebraicas que tenga el cuerpo de funciones subyacente. Por esta razón se pretende que el lector comprenda el Teorema de Riemann-Roch y sus implicaciones en los parámetros de estos últimos códigos, pues, un interés es la busqueda de cotas para la distancia miníma de ellos, diferentes a la proporcionada por la cota de singleton. Adicionalmente se exhibe la construcción de los códigos álgebro-geométricos de Goppa como una generalización del código de Reed-Solomon.

2. Cuerpos de Funciones Algebraicas

Un *cuerpo de funciones algebraicas* F/K de una variable sobre K es una extensión de cuerpos $F \supseteq K$ tal que F es una extensión algebraica de grado finito del cuerpo de funciones racionales $K(x)$ para algún $x \in F$ trascendente sobre K. Por brevedad nos referiremos a F/K como un cuerpo de funciones.

El conjunto $\widetilde{K} := \{z \in F : z \text{ es algebraico sobre } K\}$ es un subcuerpo de F cuyos elementos se les denomina *constantes*. Este cuerpo es llamado *el cuerpo de constantes* de F/K y es claro que satisface las inclusiones $K \subseteq \widetilde{K} \subsetneq F$. Además se dice que K es *el cuerpo completo de constantes de* F si $K = \widetilde{K}$.

Observemos que $F/\widetilde{K}$ es un cuerpo de funciones sobre $\widetilde{K}$ puesto que todo $x \in F$ que sea trascendente sobre K, lo es sobre $\widetilde{K}$, y como F es una extensión algebraica de grado finito sobre $K(x)$, también es algebraica de grado finito sobre $\widetilde{K}(x)$.

Ejemplo 2.1 *El ejemplo más simple de un cuerpo de funciones algebraicas sobre un cuerpo* K*, es el cuerpo de funciones racionales; F/K es llamado racional si $F = K(x)$ para algún $x \in F$ trascendente sobre K.*

Por el Teorema de Schmidt, toda extensión finitamente generada F de un cuerpo perfecto K es separablemente generada (es decir, existe una base de trascendencia separable)), es por esto que un cuerpo de funciones F/K puede representarse como una extensión algebraica simple de un cuerpo de funciones racionales $K(x)$; es decir, $F = K(x, y)$ donde $\varphi(y) = 0$ para algún polinomio irreducible φ con coeficientes en $K(x)$.

Ejemplo 2.2. *Sea $\mathbb{R}(x)$ el cuerpo de funciones racionales sobre los números reales. El polinomio $f(T) = T^2 + x^2 + 1 \in \mathbb{R}(x)(T)$ es irreducible sobre $\mathbb{R}(x)$. Si $F = \mathbb{R}(x, y)$ donde $y^2 + x^2 + 1 = 0$, entonces $[F : \mathbb{R}(x)] = 2$, luego F es un cuerpo de funciones sobre $\mathbb{R}$.*

Definición 2.1 *Un* anillo de valuación *de un cuerpo de funciones F/K es un anillo $\mathcal{O} \subseteq F$ con las siguientes propiedades:*

1. $K \subsetneq \mathcal{O} \subsetneq F$.
2. *Para todo $z \in F$, se cumple que $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$.*

Los anillos de valuación satisfacen lo siguiente:

Proposición 2.1[1] *Sea $\mathcal{O}$ un anillo de valuación de F/K. Entonces*

[1] Una prueba se ilustra en la página 2 de la referencia [6].

1. *$\mathcal{O}$ es un anillo local, es decir, $\mathcal{O}$ tiene un único ideal maximal a saber, $P = \mathcal{O} - \mathcal{O}^*$, donde $\mathcal{O} = \{z \in F : \text{existe } w \in \mathcal{O} \text{ con } wz = zw = 1\}$ es el grupo de unidades de $\mathcal{O}$.*
2. Sea $0 \neq x \in F$. Entonces $x \in P$ si y solo si $x^{-1} \notin \mathcal{O}$.
3. *El cuerpo de constantes $\tilde{K}$ de F/K satisface que $\tilde{K} \subseteq \mathcal{O}$ y $\tilde{K} \cap P = \{0\}$.*

De igual modo, el ideal maximal P de un anillo de valuación $\mathcal{O}$ cumple:

Proposición 2.2.[2] *Sea $\mathcal{O}$ un anillo de valuación de F/K y P su único ideal maximal. Entonces*

1. *P es un ideal principal.*
2. *Si $P = t\mathcal{O}$, entonces cada $0 \neq z \in F$ tiene una representación única de la forma $z = t^n u$ para algún $n \in \mathbb{Z}$ y $u \in \mathcal{O}^*$.*
3. *$\mathcal{O}$ es un dominio de ideales principales. Más precisamente, si $P = t\mathcal{O}$ e $I \neq \{0\}$ es un ideal de $\mathcal{O}$, entonces $I = t^n\mathcal{O}$ para algún $n \in \mathbb{N}$.*

Al único ideal maximal P de un anillo de valuación se le llama *lugar* y a todo elemento $t \in P$ tal que $P = t\mathcal{O}$ se le denomina *elemento primo* de P. Denotaremos por $\mathbb{P}_F := \{P: P \text{ es un lugar de } F/K\}$.

Observación 2.1. *De acuerdo al item 2. de la Proposición 2.1, se deduce que si $\mathcal{O}$ es un anillo de valuación de F/K y P es su ideal maximal, entonces $\mathcal{O}$ es determinado únicamente por P, a saber, $\mathcal{O} = \{z \in F: z^{-1} \notin P\}$. A razón de esto, $\mathcal{O}_P := \mathcal{O}$ es llamado el* anillo de valuación del lugar *P.*

Una descripción útil de los lugares se da en términos de valuaciones.

Definición 2.2. *Una* valuación discreta *de F/K es una función $v: F \to \mathbb{Z} \cup \{\infty\}$ con las siguientes propiedades:*

1. $v(x) = \infty$ *si y solo si* $x = 0$.
2. $v(xy) = v(x) + v(y)$ *para todo* $x, y \in F$.
3. $v(x + y) \geq min\{v(x), v(y)\}$ *para todo* $x, y \in F$.
4. *Existe* $z \in F$ *para el cual* $v(z) = 1$.
5. $v(a) = 0$ *para todo* $0 \neq a \in K$.

En este contexto el símbolo ∞ es usado para identificar un elemento no entero tal que $\infty + \infty = \infty, \infty + n = n + \infty = \infty$ y $\infty > m$, para todo $m, n \in \mathbb{Z}$. La propiedad (3) es conocida como *desigualdad triangular*. Es fácil verificar que la función v es sobreyectiva. En efecto, por la propiedad (4) de la definición anterior podemos elegir $z \in F$ tal que $v(z) = 1$. Entonces para todo $n \in \mathbb{Z}, n = n \cdot 1 = n \cdot v(z) = v(z^n)$, por la propiedad 2. en la Definición 2.2.

A un lugar $P \in \mathbb{P}_F$ le asociamos una función $v_P: F \to \mathbb{Z} \cup \{\infty\}$ (que resultará ser una valuación discreta de F/K) como sigue: sea t un elemento primo de P. Entonces cada elemento no nulo $z \in F$ tiene una representación única de la forma $z = t^n u$ para algún $n \in \mathbb{Z}$ y $u \in \mathcal{O}^*$. Definimos $v_P(z) := n$ y $v_P(0) := \infty$. Esta definición depende solo de P y no de la elección de t. En efecto, consideremos t' otro elemento primo de P. Entonces $P =$

[2] Consultar la página 3 de la referencia [6].

$t\mathcal{O} = t'\mathcal{O}$, así $t = t'w$ para algún $w \in \mathcal{O}$. Si $w \notin \mathcal{O}^*$, entonces $w = tw_1$ con $w_1 \in \mathcal{O}$ y por consiguiente $t = t'tw_1$, es decir, $t'w_1 = 1$, una contradicción porque $t' \in P$. Por lo tanto $z = t^n u = (t'^n w^n)u = t'^n(w^n u)$ con $w^n u \in \mathcal{O}^*$. El resultado que sigue establece que v_P es una valuación discreta de F/K.

Proposición 2.3 [3]. *Sea F/K un cuerpo de funciones.*

1. *Para un lugar $P \in \mathbb{P}_F$, la función v_P definida anteriormente es una valuación discreta de F/K. Más aún, si*

$$A = \{z \in F : v_P(z) \geq 0\},$$

$$B = \{z \in F : v_P(z) > 0\},$$

$$C = \{z \in F : v_P(z) = 0\},$$

entonces $\mathcal{O}_P = A$, $P = B$ y $\mathcal{O}_P{}^* = C$.

2. *$x \in P$ es un elemento primo de P si y solo si $v_P(x) = 1$.*

3. *Si v es una valuación discreta de F/K, entonces el conjunto*

$$P := \{z \in F : v(z) > 0\}$$

es un lugar de F/K, y $\mathcal{O}_P = \{z \in F : v(z) \geq 0\}$ es el correspondiente anillo de valuación.

4. *Cualquier anillo de valuación de F/K es un subanillo propio maximal de F.*

Sean P un lugar de F/K y $\mathcal{O}_P$ su anillo de valuación. El anillo $\mathcal{O}_P/P$ es un cuerpo el cual se denotará por $F_P := \mathcal{O}_P/P$ y lo llamaremos *el cuerpo de clases residuales* de P. Para $x \in \mathcal{O}_P$ definimos $x(P)$ como *la clase residual* de x módulo P, y si $x \in F - \mathcal{O}_P$ entonces $x^{-1} \in P$, luego $x^{-1}(P) = 0$, por lo que definimos $x(P) := \infty$. En este sentido el símbolo ∞ tiene una interpretación diferente a la dada anteriormente. De la Proposición 2.1 deducimos que $K \subseteq \mathcal{O}_P$ y $K \cap P = \{0\}$, de modo que podemos pensar en K como un subcuerpo de F_P mediante la inmersión $K \hookrightarrow F_P$ inducida al restringir el homomorfismo canónico $\pi : \mathcal{O}_P \to \mathcal{O}_P/P$ sobre K, además obsérvese que el anterior argumento también se aplica a $\widetilde{K}$ en lugar de K, así en definitiva consideramos a K y $\widetilde{K}$ como subcuerpos de F_P. La aplicación

$$\phi : \begin{cases} F & \longrightarrow F_P \cup \{\infty\}, \\ x & \longmapsto x(P) \end{cases}$$

donde $x(P) \in F_P$ si $x \in \mathcal{O}_P$ y $x(P) := \infty$ si $x \in F - \mathcal{O}_P$, es llamada la *aplicación de clases residuales* con respecto a P. En ocasiones se escribe $x + P := x(P)$ para $x \in \mathcal{O}_P$. Ahora en virtud de que $K \subseteq \widetilde{K} \subseteq F_P$ siendo P un lugar, definimos $\deg P := [F_P : K]$ como el *grado* de P. Un lugar de grado uno se llama *lugar racional* de F/K. El grado de un lugar es siempre finito, más concretamente se tiene lo siguiente:

[3] Una demostración puede encontrarse en la página 5 de [6].

Proposición 2.4. [4] *Si P es un lugar de F/K y $0 \neq x \in P$, entonces*

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

De esto último se sigue inmediatamente que el cuerpo $\widetilde{K}$ de constantes de F/K es una extensión finita de K. El próximo teorema garantiza que $\mathbb{P}_F$ es no vacío.

Teorema 2.1 (Existencia de Lugares). *Sea F/K un cuerpo de funciones y R un subanillo de F con $K \subseteq R \subseteq F$. Supongamos que $\{0\} \neq I \subsetneq R$ es un ideal propio de R. Entonces existe un lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ y $R \subseteq \mathcal{O}_P$.*

Demostración. Consideremos el conjunto

$$\mathcal{F} := \{ S : S \text{ es un subanillo de } F \text{ con } R \subseteq S \text{ y } IS \neq \mathrm{S} \}.$$

Por definición, IS es el conjunto de todas las sumas finitas $\sum a_v s_v$ con $a_v \in I$ y $s_v \in S$; más aún, IS un ideal de S. Ordenamos a $\mathcal{F}$ por inclusión. Puesto que R es un subanillo de F y $IR \neq R$ (porque I es un ideal propio de R) se tiene que $R \in \mathcal{F}$, luego $\mathcal{F}$ es no vacío. Sea $\mathcal{H} \subseteq \mathcal{F}$ un subconjunto totalmente ordenado de $\mathcal{F}$ y definamos $T := \cup_{S \in \mathcal{H}} S$. Entonces es claro que $R \subseteq T$, T es un subanillo de F y $S \subseteq T$ para todo $S \in \mathcal{H}$. Afirmamos que $IT \neq T$. En efecto, si esto es falso podemos escribir $1 = \sum_{i=1}^{n} a_i s_i$ donde $a_i \in I$ y $s_i \in T$ para todo i, pero dado que $\mathcal{H}$ es un conjunto totalmente ordenado, existe $\tilde{S} \in \mathcal{H}$ tal que $s_1, s_2, \ldots, s_n \in \tilde{S}$, así $1 = \sum_{i=1}^{n} a_i s_i \in I\tilde{S}$ y $I\tilde{S} = \tilde{S}$, una contradicción. De esta manera $T \in \mathcal{F}$. Empleando el Lema de Zorn, encontramos $\mathcal{O}$ tal que $\mathcal{O}$ es un subanillo de F, $R \subseteq \mathcal{O}$, $I\mathcal{O} \neq \mathcal{O}$ y $\mathcal{O}$ es maximal con respecto a estas propiedades. En lo que sigue mostraremos que $\mathcal{O}$ es un anillo de valuación de F/K. Como $I \neq \{0\}$ y $I\mathcal{O} \neq \mathcal{O}$, todo elemento de I no es una unidad de $\mathcal{O}$ (note que si $0 \neq x$ pertenece a I y es tal que $x \in \mathcal{O}^*$, entonces existe $w \in \mathcal{O}$ con $xw = 1$, luego para todo $z \in \mathcal{O}$, $z = 1 \cdot z = (xw) \cdot z = x(wz) \in I\mathcal{O}$, de modo que $I\mathcal{O} = \mathcal{O}$, una contradicción). Por lo tanto $I \subseteq \mathcal{O} - \mathcal{O}^*$. En principio $K \subseteq \mathcal{O} \subseteq F$, sin embargo por lo anterior; tanto K como F no pueden ser iguales a $\mathcal{O}$. Supongamos ahora que existe $z \in F$ con $z \notin \mathcal{O}$ y $z^{-1} \notin \mathcal{O}$. Consideremos los anillos $\mathcal{O}[z]$ y $\mathcal{O}[z^{-1}]$. Por la maximalidad del anillo $\mathcal{O}$ debe ocurrir que $\mathcal{O}[z] = I\mathcal{O}[z]$ y $\mathcal{O}[z^{-1}] = I\mathcal{O}[z^{-1}]$, por lo que en particular podemos encontrar elementos $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m \in I\mathcal{O}$ tales que

$$(1) \qquad 1 = a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n, \quad n \geq 0. \qquad \text{y}$$

$$(2) \qquad 1 = b_0 + b_1 z^{-1} + b_2 z^{-2} + \cdots + b_m z^{-m}, \quad m \geq 0.$$

Si $n = 0$, entonces $1 = a_0 \in I\mathcal{O}$ y en su efecto $I\mathcal{O} = \mathcal{O}$, una contradicción. Así $n \geq 1$. De manera similar se muestra que $m \geq 1$. Entonces los conjuntos

$$A := \{n \in \mathbb{Z}^+ : 1 = a_0 + a_1 z + \cdots + a_n z^n \text{ donde } a_i \in I\mathcal{O}\} \qquad \text{y}$$

$$B := \{m \in \mathbb{Z}^+ : 1 = b_0 + b_1 z^{-1} + \cdots + b_m z^{-m} \text{ donde } b_i \in I\mathcal{O}\},$$

son no vacíos por (1) y (2) en su orden, luego el principio del buen orden garantiza la existencia de un elemento mínimo tanto para A como para B. Sean m y n elegidos de manera minimal en (1) y (2) respectivamente y sin pérdida de generalidad supongamos $m \leq n$. Si multiplicamos (1) por $1 - b_0$ y (2) por $a_n z^n$ obtenemos,

$$\begin{aligned} 1 - b_0 &= (1 - b_0)a_0 + (1 - b_0)a_1 z + (1 - b_0)a_2 z^2 + \cdots + (1 - b_0)a_n z^n \quad \text{y} \\ 0 &= (b_0 - 1)a_n z^n + b_1 a_n z^{n-1} + \cdots + b_m a_n z^{n-m}, \end{aligned}$$

[4] Para conocer una prueba formal consulte la página 6 de [6].

luego la suma de estas ecuaciones da como resultado

$$1 = c_0 + c_1 z + \cdots + c_{n-1} z^{n-1},$$

donde los coeficientes $c_i \in I\mathcal{O}$. Esto es una contradicción con la minimalidad de n en (1). Por lo tanto, hemos demostrado que $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$ para todo $z \in F$ y por ende $\mathcal{O}$ es un anillo de valuación de F/K.

Observación 2.2 *Sea P un lugar de F/K. Si $degP = 1$, entonces $F_P = K$ y la aplicación de clases residuales aplica F sobre $K \cup \{\infty\}$. En particular, si K es un cuerpo algebraicamente cerrado y $P \in \mathbb{P}_F$, entonces P es racional. Así las cosas, si cada lugar es racional, podemos entender un elemento $z \in F$ como una función*

$$z : \begin{cases} \mathbb{P}_F & \longrightarrow K \cup \{\infty\}, \\ P & \longmapsto z(P). \end{cases} \tag{3}$$

Es por eso que F/K es llamado un cuerpo de funciones. *Los elementos de K interpretados como funciones en el sentido (3), son funciones constantes. Por esta razón K se denomina el* cuerpo de constantes de F.

Definición 2.3. *Sea $z \in F$ y $P \in \mathbb{P}_F$. Decimos que P es un cero de z si y solo si $v_p(z) > 0$; P es un polo de z si y solo si $v_p(z) < 0$. Si $v_p(z) = m > 0$, P es un cero de z de orden m; si $v_p(z) = -m < 0$, P es polo de z de orden m.*

En virtud del Teorema 2.1 obtenemos que cada elemento $z \in F$ trascendente sobre K tiene por lo menos un cero y por lo menos un polo. Más exactamente:

Corolario 2.1. *Sea F/K un cuerpo de funciones y $z \in F$ trascendente sobre K. Entonces z tiene por lo menos un cero y por lo menos un polo.*

Demostración. Consideremos el anillo $R = K[z]$ y el ideal $I = zK[z]$. Por el Teorema 2.1 existe un lugar $P \in \mathbb{P}_F$ con $z \in P$, por consiguiente P es un cero de z. Del mismo modo, si tomamos $R = K[z^{-1}]$ e $I = z^{-1}K[z^{-1}]$, existe un lugar $Q \in \mathbb{P}_F$ con $z^{-1} \in Q$, luego $v_Q(z^{-1}) > 0$, es decir, Q es un polo de z.

3. Cuerpos de funciones Racionales

Sea K un cuerpo y x un elemento trascendente sobre K. Denotemos por $K[x]$ el anillo de polinomios en la indeterminada x con coeficientes en K. El cuerpo de funciones racionales $F = K(x)$ se define como

$$K(x) := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], g(x) \neq 0 \right\}.$$

Dado un polinomio mónico e irreducible $p(x) \in K[x]$, el conjunto

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \nmid g(x) \right\} \tag{4}$$

resulta ser un anillo de valuación en $K(x)/K$. En efecto,

1. Cualquier $k \in K$ puede escribir de la forma $k = \frac{k}{1}$ y $p(x) \nmid 1$ por la irreducibilidad de $p(x)$ sobre K, luego $k \in \mathcal{O}_{p(x)}$. Además, $K \subsetneq \mathcal{O}_{p(x)}$ y $\mathcal{O}_{p(x)} \subsetneq K(x)$.

2. Supongamos que $z = \frac{f(x)}{g(x)} \in K(x) - \mathcal{O}_{p(x)}$ donde $f(x)$ y $g(x)$ son primos relativos. Como $p(x) \mid g(x)$, se sigue que $p(x) \nmid f(x)$, luego $z^{-1} = \frac{g(x)}{f(x)} \in \mathcal{O}_{p(x)}$.

Así mismo, notemos que si $z = \frac{f(x)}{g(x)} \in \mathcal{O}_{p(x)}^*$, entonces $z^{-1} = \frac{g(x)}{f(x)} \in \mathcal{O}_{p(x)}$ y por ende,

$$z \in A := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \nmid f(x), p(x) \nmid g(x) \right\}.$$

Recíprocamente, si $z \in A$, entonces es claro que $z \in \mathcal{O}_{p(x)}^*$, porque z y $z^{-1} \in \mathcal{O}_{p(x)}$.

De esta manera se sigue que el conjunto de unidades de este anillo de valuación viene dado por

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

y en consecuencia

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \mid f(x), p(x) \nmid g(x) \right\}, \tag{5}$$

es el correspondiente lugar de $\mathcal{O}_{p(x)}$. Cuando $p(x)$ es lineal escribimos $P_\alpha := P_{x-\alpha}$.

El anillo $\mathcal{O}_{p(x)}$ es llamado *anillo de valuación asociado al polinomio mónico e irreducible* $p(x)$.

Observación 3.1 *Supongamos que* $p(x), q(x) \in K[x]$ *son polinomios mónicos e irreducibles distintos. Si* $\mathcal{O}_{p(x)} = \mathcal{O}_{q(x)}$, *entonces* $P_{p(x)} = P_{q(x)}$, *por lo que* $p(x) \in P_{q(x)}$. *Sin embargo,* $v_{P_{q(x)}}(p(x)) = 0$, *una contradicción. En los términos anteriores, hemos probado que si* $p(x)$ *y* $q(x)$ *son polinomios mónicos e irreducibles distintos, entonces* $\mathcal{O}_{p(x)} \neq \mathcal{O}_{q(x)}$.

Otro anillo de valuación en $K(x)/K$ está dado por el conjunto

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} : \deg f(x) \leq \deg g(x) \right\}, \tag{6}$$

el cual tiene como ideal maximal

$$P_\infty = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], \deg f < \deg g(x) \right\}. \tag{7}$$

Este último es llamado el *lugar infinito de* $K(x)/K$. La etiqueta de"∞" depende del elemento generador de la extensión $K(x)/K$. Por ejemplo P_0 es el lugar infinito de $K(x^{-1})$.

Proposición 3.1. *Sea* $F = K(x)$ *el cuerpo de funciones racionales.*

1. *Si* $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ *es el lugar definido por (5) donde* $p(x) \in K[x]$ *es un polinomio irreducible sobre K, entonces* $p(x)$ *es un elemento primo de P y la correspondiente valuación discreta* v_P *puede describirse como sigue: si* $0 \neq z \in K(x)$ *se escribe como* $z = p(x)^n \cdot \left(\frac{f(x)}{g(x)}\right)$ *con* $f(x), g(x) \in K[x]$, $p(x) \nmid f(x)$ *y* $p(x) \nmid g(x)$, *entonces* $v_P(z) := n$. *En el*

caso $z = 0$, *definimos* $v_P(z) := \infty$. *Además, el cuerpo de clases residuales* $K(x)_P = \mathcal{O}_P/P$ *es isomorfo a* $K[x]/\langle p(x)\rangle$. *Consecuentemente* $\deg P = deg(p(x))$.

2. *En el caso especial cuando* $p(x) = x - \alpha$ *con* $\alpha \in K$, *el grado de* $P = P_\alpha$ *es 1, y la aplicación de clases residuales está dada por*

$$\phi : \begin{cases} K(x) & \longrightarrow K(x)_P \cup \{\infty\}, \\ z & \longmapsto z(P) = z(\alpha) \end{cases}$$

donde $z(\alpha)$ se define de la siguiente manera: si escribimos $z = \frac{f(x)}{g(x)}$ con $f(x), g(x)$ elementos de $K[x]$ primos relativos, entonces

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

3. *Finalmente, sea* P_∞ *el lugar infinito de* $K(x)/K$ *definido por (7). Entonces* P_∞ *es racional y un elemento primo de* P_∞ *es* $t = \frac{1}{x}$. *La correspondiente valuación discreta* v_∞ *está dada por*

$$v_\infty\left(\frac{f(x)}{g(x)}\right) = \deg g(x) - \deg f(x),$$

donde $f(x), g(x) \in K[x]$. *La aplicación de clases residuales correspondiente a* P_∞ *está determinada como sigue:*

$$\phi : \begin{cases} K(x) & \longrightarrow K(x)_{P_\infty} \cup \{\infty\}, \\ z & \longmapsto z(P_\infty) = z(\infty) \end{cases}$$

donde si

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

entonces

$$z(\infty) := \begin{cases} \dfrac{a_n}{b_m} & si \quad n = m, \\ 0 & si \quad n < m, \\ \infty & si \quad n > m. \end{cases}$$

4. K *es el cuerpo completo de constantes de* $K(x)/K$.

Podemos clasificar los lugares de un cuerpo de funciones racionales así:

Teorema 3.1. (Lugares de un Cuerpo de Funciones Racionales). *Sea* $F = K(x)$ *el cuerpo de funciones racionales sobre* K. *Si* $P \in \mathbb{P}_{K(x)}$, *entonces* $P = P_{p(x)}$ *para algún polinomio* $p(x) \in K[x]$ *mónico e irreducible ó* $P = P_\infty$.

Con base en lo anterior se obtiene lo siguiente:

Corolario 3.1. *Los lugares de $K(x)/K$ racionales están en correspondencia uno a uno con $K \cup \{\infty\}$.*

Demostración. Sea P un lugar racional de $K(x)/K$. Entonces $P = P_{p(x)}$ donde $p(x) = x - \alpha$ para algún $\alpha \in K$ ó $P = P_\infty$. De acuerdo con la Observación 3.1 tenemos la aplicación uno a uno

$$\phi : \begin{cases} \{\text{Lugares racionales de } K(x)/K\} & \longrightarrow K \cup \{\infty\}, \\ P_\alpha & \longmapsto \alpha \\ P_\infty & \longmapsto \infty. \end{cases}$$

4. Independencia de Valuaciones

El resultado más importante de esta sección es el Teorema de aproximación débil, también conocido como el Teorema de la Independencia.

Lema 4.1.[5] *Sea F/K un cuerpo de funciones algebraicas, $P_1, P_2, \dots, P_n \in \mathbb{P}_F$ lugares distintos dos a dos, $x_1, x_2, \dots, x_n \in F$ y $r_1, r_2, \dots, r_n \in \mathbb{Z}$. Entonces:*

1. *Existe $u \in F$ tal que $v_{P_1}(u) > 0$ y $v_{P_i}(u) < 0$ para $i = 2,3, \dots, n$.*
2. *Existe $w \in F$ tal que $v_{P_1}(w - 1) > r_1$ y $v_{P_i}(w) > r_i$ para $i = 2,3, \dots, n$.*
3. *Existe $z \in F$ con $v_{P_i}(z - x_i) > r_i$ para $i = 1,2, \dots, n$.*

De acuerdo al lema previo enunciamos el teorema mencionado.

Teorema 4.1.[6] *[Teorema de aproximación débil] Sea F/K un cuerpo de funciones algebraicas, $P_1, P_2, \dots, P_n \in \mathbb{P}_F$ lugares distintos dos a dos, $x_1, x_2, \dots, x_n \in F$ y $r_1, r_2, \dots, r_n \in \mathbb{Z}$. Entonces existe un elemento $x \in F$ que satisface*

$$v_{P_i}(x - x_i) = r_i \quad \text{para } i = 1,2, \dots, n.$$

Una consecuencia importante de este resultado se enuncia a continuación:

Corolario 4.1. *Cualquier cuerpo de funciones tiene infinitos lugares.*

Demostración. Supongamos que F/K es un cuerpo de funciones que tiene un número finito de lugares, digamos, $P_1, P_2, \dots, P_n$. Por el Teorema 4.1 existe $0 \neq x \in F$ con $v_{P_i}(x) > 0$ para $i = 1,2, \dots, n$. Entonces x es trascendente sobre K puesto que tiene ceros, sin embargo x no tiene polos, una contradicción con el Corolario 2.1.

Podemos estimar el número de ceros de un elemento $x \in F$. En ese sentido obtenemos:

[5] Los detalles de la demostración pueden ser consultados en las páginas 12-13 de [6].
[6] Una demostración se exhibe en la página 12 de [6].

Proposición 4.1. [7] *Sea F/K un cuerpo de funciones y $P_1, P_2, \dots, P_r \in \mathbb{P}_F$ ceros de $x \in F$. Entonces*

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

Nótese que la proposición anterior permite concluir que en un cuerpo de funciones F/K, todo elemento $0 \neq x \in F$ tiene un número finito de ceros y polos. Mas exactamente, si x es constante, x no tiene ceros ni polos. Si x es trascendente sobre K, el número de ceros es menor o igual que $[F: K(x)]$. El mismo argumento muestra que x^{-1} tiene un número finito de ceros, que finalmente corresponden a los polos de x.

5. Divisores

Definición 5.1. *El* grupo divisor *de F/K se define como el grupo abeliano libre (escrito aditivamente) que es generado por los lugares de F/K; se denota por* $\mathrm{Div}(F)$.

Un elemento D de $\mathrm{Div}(F)$ se denomina *divisor* de F/K y se interpreta como una suma formal

$$D = \sum_{P \in \mathbb{P}_F} n_p \, P \quad \text{con } n_P \in \mathbb{Z}, \text{ y casi todo } n_P = 0 \, .$$

El *soporte* de D se define por $\mathrm{Supp}(D) := \{P \in \mathbb{P}_F : n_P \neq 0\}$. Un divisor de la forma $D = P$ con $P \in \mathbb{P}_F$ es llamado *divisor primo*.

Dos divisores $D = \sum_{P \in \mathbb{P}_F} n_P \, P$ y $D' = \sum_{P \in \mathbb{P}_F} m_P \, P$ se suman coeficiente a coeficiente,

es decir,

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

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

$$0 := \sum_{P \in \mathbb{P}_F} r_P \, P \quad \text{donde } r_P = 0 \text{ para todo } P \in \mathbb{P}_F.$$

Para $Q \in \mathbb{P}_F$ y $D = \sum_{P \in \mathbb{P}_F} n_P \, P$ se define $v_Q(D) := n_Q$, por lo tanto suele escribirse

$$\mathrm{Supp}(D) = \{P \in \mathbb{P}_F : v_P(D) \neq 0\} \quad \text{y } D = \sum_{P \in \mathrm{Supp}(D)} v_P(D) \cdot P.$$

En $\mathrm{Div}(F)$ se define un orden parcial de la siguiente manera:

$$D_1 \leq D_2 \quad \text{sii } v_P(D_1) \leq v_P(D_2) \text{ para todo } P \in \mathbb{P}_F.$$

[7] Ver página 14 de [6].

Si $D_1 \leq D_2$ y $D_1 \neq D_2$, escribimos $D_1 < D_2$. Un divisor $D \geq 0$ es llamado *positivo* (o *efectivo*). El *grado* de un divisor está definido por

$$\deg D := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot \deg P,$$

y esto induce un homomorfismo de grupos deg: $\mathrm{Div}(F) \to \mathbb{Z}$.

Definición 5.2. *Sea $0 \neq x \in F$ y denotemos por M (resp. N) el conjunto de ceros (resp. polos) de x en $\mathbb{P}_F$. Entonces se define*

$(x)_0 := \sum_{P \in M} v_P(x)P$, *el* divisor cero *de* x

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

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

Claramente, por la Definición 5.2, $(x)_0 \geq 0$, $(x)_\infty \geq 0$ y

(8)

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

Diremos que dos divisores A y B son equivalentes si $A = B + (x)$ para algún $0 \neq x \in F$. Un primer resultado acerca de los divisores principales se muestra enseguida.

Teorema 5.1. *Todos los divisores principales tienen grado cero. Más explícitamente: sea $x \in F - K$ y denotemos por $(x)_0$ (resp. $(x)_\infty$) el divisor cero de x (resp. el divisor polo de x). Entonces*

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

Ejemplo 5.1. *Consideremos el cuerpo de funciones racionales $K(x)/K$ y un elemento no constante*

$$z = \frac{f(x)}{g(x)} \in K(x),$$

con $f(x)$ y $g(x)$ primos relativos. Escribamos $f(x) = \prod_{i=1}^{r} p_i(x)^{n_i}$ y $g(x) = \prod_{j=1}^{s} q_j(x)^{m_j}$ donde $p_i(x)$, $q_j(x)$ son polinomios irreducibles con coeficientes en K, y n_i, m_j enteros no negativos. Como $z \in K(x) - K$, se conoce por el Teorema 5.1 que $[K(x) : K(z)] = deg(z)_\infty$, pero

$$\begin{aligned}\deg(z)_\infty &= \sum_{j=1}^{s}(\beta_j \deg q_j(x)) + \max\{\deg f(x) - \deg g(x), 0\} \\ &= \deg g(x) + \max\{\deg f(x) - \deg g(x), 0\} \\ &= \max\{\deg f(x), \deg g(x)\}.\end{aligned}$$

En consecuencia, $[K(x):K(z)] = max\{degf(x), degg(x)\}$. *Ahora si* $K(x) = K(z)$, *entonces* $[K(x):K(z)] = 1$ *de donde se infiere que* $z = \frac{ax+b}{cx+d}$, *con* $a, b, c, d \in K$ *y* $ad - bc \neq 0$, *ya que* f *y* g *son primos relativos.*

Observación 5.1

1. $0 \neq x \in K$ *si y solo si* $(x) = 0$.
2. *Para* $0 \neq x \in F$ *y* P *un lugar de* F/K, $v_P((x)) = v_P(x)$ *por (8).*

Ejemplo 5.2. *El elemento* $u = \frac{(x+1)^2}{x-5}$ *del cuerpo de funciones racionales* $\mathbb{R}(x)$ *tiene divisor principal*

$$\begin{aligned}(u) &= 2 \cdot (x+1) + (-1) \cdot (x-5) \\ &= 2 \cdot ((x+1)_0 - (x+1)_\infty) + (-1) \cdot ((x-5)_0 - (x-5)_{P_\infty}) \\ &= 2 \cdot (x+1)_0 + (-2) \cdot (x+1)_\infty + (-1) \cdot (x-5)_0 + 1 \cdot (x-5)_\infty \\ &= 2P_{x+1} - 2P_\infty - P_{x-5} + P_\infty.\end{aligned}$$

Ejemplo 5.3. *Sea* $F = K(x)/K$ *el cuerpo de funciones racionales. Para* $0 \neq z \in K(x)$ *tenemos que* $z = a \cdot f(x)/g(x)$ *con* $a \in K - \{0\}, f(x), g(x) \in K[x]$ *polinomios mónicos y primos relativos. Escribamos*

$$f(x) = \prod_{i=1}^{r} p_i(x)^{n_i},\ g(x) = \prod_{j=1}^{s} q_j(x)^{m_j}$$

donde $p_i(x), q_j(x)$ *son polinomios distintos con coeficientes en* K, *mónicos e irreducibles. El divisor principal de z en* $Div(F)$ *es*

$$
\begin{aligned}
(z) = \left(\frac{af(x)}{g(x)}\right) &= (f(x)) - (g(x)) \\
&= (f(x))_0 - (f(x))_\infty - (g(x))_0 + (g(x))_\infty \\
&= (\prod_{i=1}^{r} p_i(x)^{n_i})_0 - (\prod_{i=1}^{r} p_i(x)^{n_i})_\infty - (\prod_{j=1}^{s} q_j(x)^{m_j})_0 + (\prod_{j=1}^{s} q_j(x)^{m_j})_\infty \\
&= \sum_{i=1}^{r} n_i (p_i(x))_0 - \sum_{i=1}^{r} n_i (p_i(x))_\infty - \sum_{j=1}^{s} m_j (q_j(x))_0 + \sum_{j=1}^{s} m_j (q_j(x))_\infty \\
&= \sum_{i=1}^{r} n_i P_{p_i(x)} - \sum_{j=1}^{s} m_j Q_{q_j(x)} - \sum_{i=1}^{r} n_i \deg p_i(x) P_\infty + \sum_{j=1}^{s} m_j \deg q_j(x) P_\infty \\
&= \sum_{i=1}^{r} n_i P_{p_i(x)} - \sum_{j=1}^{s} m_j Q_{q_j(x)} - \deg f(x) P_\infty + \deg g(x) P_\infty \\
&= \sum_{i=1}^{r} n_i P_{p_i(x)} - \sum_{j=1}^{s} m_j Q_{q_j(x)} + (\deg g(x) - \deg f(x)) P_\infty .
\end{aligned}
$$

Definición 5.3. *Para un divisor $A \in Div(F)$ definimos el espacio de Riemann-Roch asociado a A por*

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

Directamente de la definición se obtiene que:

1. $x \in \mathcal{L}(A)$ si y solo si $v_P(x) \geq -v_P(A)$ para todo $P \in \mathbb{P}_F$.
2. $\mathcal{L}(A) \neq \{0\}$ si y solo si existe un divisor $A' \sim A$ con $A' \geq 0$.

La definición 5.3 tiene la siguiente interpretación: si

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

con $n_i > 0, m_j > 0$, entonces $\mathcal{L}(A)$ consiste de todos los elementos $x \in F$ tales que

1. x tiene ceros de orden mayor o igual que m_j, en Q_j, para $j = 1,2,\dots,s$ y
2. x solo puede tener polos en $P_1, P_2, \dots, P_r$, con orden polar en P_i no mayor que n_i para $i = 1,2,\dots,r$.

El espacio de Riemann-Roch asociado a un divisor A resulta ser un espacio vectorial sobre K de dimensión finita. Al número $\ell(A) := \dim_K \mathcal{L}(A)$ se le llama la *dimensión* del divisor A. Si A y A' son divisores equivalentes, entonces $\mathcal{L}(A)$ y $\mathcal{L}(A')$ son isomorfos como espacios vectoriales, en particular $\ell(A) = \ell(A')$ y $\deg(A) = \deg(A')$, por el Teorema 5.1

Ejemplo 5.4. *En el cuerpo de funciones racionales $\mathbb{R}(x)/\mathbb{R}$, consideremos el divisor principal (u) donde $u = \frac{(x+1)^2}{x-5}$. Si $z \in \mathcal{L}((u))$, entonces sus ceros son de orden mayor o igual que 1 y 2 en P_{x-5} y P_∞ respectivamente. También z puede tener polos en P_{x+1} y P_∞ con orden polar no mayor que 2 y 1 respectivamente.*

Proposición 5.1.[8]

1. *Si* $\deg A < 0$, *entonces* $\ell(A) = 0$.
2. *Para un divisor* A *con* $\deg A = 0$, *las siguientes afirmaciones son equivalentes.*

   a. *A es un divisor principal.*

   b. $\ell(A) \geq 1$.

   c. $\ell(A) = 1$.

Definición 5.4. *El género* g *de un cuerpo de funciones* F/K *está definido por*

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

Observación 5.2. *El género de* F/K *es un entero no negativo. En efecto, según la Observación 5.1,* $K \subseteq \mathcal{L}(0)$, *más aún, si* $0 \neq x \in \mathcal{L}(0)$, *entonces* $(x) \geq 0$. *Esto significa que* x *no tiene polos, así que* $x \in K$ *por el Corolario 2.1. Por lo tanto* $\mathcal{L}(0) = K$. *Ahora si en la definición previa se toma el divisor* $A = 0$, *entonces* $\deg 0 - \ell(0) + 1 = 0$, *con lo cual* $g \geq 0$.

Teorema 5.2.[9] *[Teorema de Riemann] Sea* F/K *un cuerpo de funciones de género* g. *Entonces:*

1. *Para todo* $A \in Div(F)$, $\ell(A) \geq degA + 1 - g$.
2. *Existe* $c \in \mathbb{Z}$, *dependiente solo del cuerpo de funciones* F/K, *tal que*

$$\ell(A) = \deg A + 1 - g,$$

siempre que $degA \geq c$.

Ejemplo 5.5. *El cuerpo de funciones racionales* $K(x)/K$ *tiene género* $g = 0$. *El divisor cero y el divisor polo de* x *son respectivamente* $(x)_0 = P_0$ *y* $(x)_\infty = P_\infty$ *(notación como en la Proposición 3.1). Consideremos para* $r \geq 0$ *el espacio vectorial* $\mathcal{L}(rP_\infty)$ *y definamos* $T := \{1, x, \dots, x^r\}$. *Entonces:*

1. T es linealmente independiente sobre K.
2. $T \subseteq \mathcal{L}(rP_\infty)$.

De este modo en lo términos anteriores tenemos

$$\begin{aligned} r+1 &\leq \ell(rP_\infty) \ por\ (1) \\ &= \deg(rP_\infty) + 1 - g \ para\ r\ suficientemente\ grande \\ &= r \cdot \deg P_\infty + 1 - g \\ &= r + 1 - g. \end{aligned}$$

Por lo tanto, $g \leq 0$; *pero también* $g \geq 0$ *según la Observación 5.2, luego* $g = 0$.

[8] Ver página 20 de [6].
[9] El lector interesado en conocer una prueba puede remitirse a la página 23 de [6].

6. Teorema de Riemann-Roch

En esta sección F/K denota un cuerpo de funciones algebraicas de género g.

Definición 6.1. *Para $A \in Div(F)$ el entero $i(A) := \ell(A) - degA + g - 1$ se denomina el* índice de especialidad *de A.*

Las valuaciones discretas pueden extenderse de manera natural a $F^{\mathbb{P}_F}$ (conjunto de funciones de $\mathbb{P}_F$ a F) como sigue:

$$v_P(\alpha) := v_P(\alpha(P)) \text{ donde } \alpha \in F^{\mathbb{P}_F} \text{ y } P \in \mathbb{P}_F.$$

Con lo anterior podemos considerar a F inmerso en $F^{\mathbb{P}_F}$ vía la función inyectiva

$$\varphi' : \begin{cases} F & \longrightarrow F^{\mathbb{P}_F}, \\ x & \longmapsto \alpha_x \end{cases} \tag{9}$$

donde $\alpha_x(P) = x$ para todo $P \in \mathbb{P}_F$, además se tiene que

$$v_P(\varphi'(x)) = v_P(\alpha_x) = v_P(\alpha_x(P)) = v_P(x) \text{ para todo } P \in \mathbb{P}_F.$$

Se puede proporcionar dos interpretaciones para $i(A)$ en términos de la dimensión de ciertos espacios, como serán descritas por el Teorema 6.1 y el Lema 6.1 que enunciaremos más adelante.

Definición 6.2. *Sea F/K un cuerpo de funciones.*

1. *El conjunto*

$$\mathcal{A}_F := \{\alpha \in F^{\mathbb{P}_F} : \alpha(P) \in \mathcal{O}_P \text{ para casi todo } P \in \mathbb{P}_F\}$$

es llamado el espacio de adeles *de F/K.*

2. *A los elementos de $\mathcal{A}_F$ se les conoce como adeles de F/K. Este puede ser considerado como un elemento del producto directo $\prod_{P\in\mathbb{P}_F} F$ y por lo tanto, utilizamos la notación $\alpha = (\alpha_P)_{P\in\mathbb{P}_F}$, o simplemente $\alpha = (\alpha_P)$.*

Si se define la suma componente a componente, entonces $\mathcal{A}_F$ tiene estructura de espacio vectorial sobre K. El *adele principal* α_x de un elemento $x \in F$ es el adele cuyas componentes son todas iguales a x. En el contexto de la Definición 6.2, la función φ' definida en (9) resulta ser una inmersión de F en $\mathcal{A}_F$ y le llamaremos *la inmersión diagonal.*

Notación: Si P es un lugar de F/K y $\alpha \in \mathcal{A}_F$, escribiremos $v_P(\alpha_P)$ para denotar $v_P(\alpha(P))$.

Definición 6.3. *Para $A \in$ Div(F) definimos*

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

Este subespacio vectorial de $\mathcal{A}_F$ sobre K tiene dimensión infinita. En efecto, si $\alpha, \beta \in \mathcal{A}_F(A)$ y $a \in K$, entonces

$$v_P(\alpha+\beta) \geq \min\{v_P(\alpha), v_P(\beta)\} \geq -v_P(A),$$

y

$$v_P(a\alpha) = v_P(a) + v_p(\alpha) = v_P(\alpha) \geq -v_P(A)$$

siendo $P \in \mathbb{P}_F$ cualquier lugar de F/K. En consecuencia, $\alpha+\beta$ y $a\alpha$ son elementos de $\mathcal{A}_F(A)$. Ahora fijemos un lugar $Q \in I$ donde $I := \mathbb{P}_F - \text{Supp}(A)$ y consideremos un adele α donde

$$\alpha_P := \begin{cases} 1 & \text{si } P = Q \\ 0 & \text{si } P \neq Q. \end{cases}$$

La sucesión $\{\alpha_P\}_{P\in I}$ está contenida en $\mathcal{A}_F(A)$, luego $\text{Gen}\{\alpha_P\} \subseteq \mathcal{A}_F(A)$. Sea $B = \{\alpha_{Q_1}, \alpha_{Q_2}, \dots, \alpha_{Q_n}\}$ una base de $\text{Gen}\{\alpha_P\}$ sobre K. El adele β definido por

$$\beta_R := \begin{cases} 1 & \text{si } R \notin \text{Supp}(A),\ R \neq Q_i \text{ para todo } i = 1,2,\dots,n \text{ y } R \neq Q \\ 0 & \text{en otro caso,} \end{cases}$$

es un elemento de $\text{Gen}\{\alpha_P\}$ distinto de α_{Q_i}, por lo que existen únicos escalares $\theta_1, \theta_2, \dots, \theta_n \in K$ tales que $\beta = \sum_{i=1}^{n} \theta_i \alpha_{Q_i}$. Entonces para $R \notin \text{Supp}(A)$, $R \neq Q_i$ y $R \neq Q$ tenemos

$$0 = v_R(\beta) = v_R\left(\sum_{i=1}^{n} \theta_i \alpha_{Q_i}\right) = v_R(0) = \infty,$$

una contradicción. Por lo tanto, $\mathcal{A}_F(A)$ es un espacio vectorial sobre K de dimensión infinita.

Teorema 6.1 [10] Para cada divisor A, el índice de especialidad es

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

Notemos que aunque los espacios vectoriales $\mathcal{A}_F, \mathcal{A}_F(A)$ y F son de dimensión infinita sobre K, el teorema establece que el espacio cociente $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$ tiene dimensión finita sobre K. Ahora presentaremos el concepto de diferenciales de Weil con el fin de dar una segunda interpretación a el índice de especialidad de un divisor.

Definición 6.4. *Un* diferencial de Weil *de F/K es una aplicación $K-$lineal*

$$\omega: \mathcal{A}_F \to K$$

que se anula en $\mathcal{A}_F(A) + F$ para algún divisor $A \in \text{Div}(F)$. En otras palabras un diferencial de Weil ω es un funcional lineal tal que $\omega \in \text{Ann}(\mathcal{A}_F(A) + F)$ para algún $A \in \text{Div}(F)$.

[10] Consultar página 25 de [6].

Llamamos

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

el *módulo de diferenciales de Weil* de F/K, y para $A \in \text{Div}(F)$ se define

$$\begin{aligned} \Omega_F(A) &:= \{\omega \in \Omega_F: \omega \text{ se anula en } \mathcal{A}_F(A) + F\} \\ \Omega_F(A) &:= \{\omega \in \Omega_F : \omega \text{ se anula en } \mathcal{A}_F(A) + F\} \\ &= \text{Ann}(\mathcal{A}_F(A) + F). \end{aligned}$$

Observación 6.1.

1. *Resulta claro que* $\Omega_F = \bigcup_{A \in Div(F)} \Omega_F(A)$.

2. Ω_F *es un espacio vectorial sobre* K *con las operaciones usuales. Más exactamente, si* $\omega_1, \omega_2 \in \Omega_F$, *es decir, si* ω_1 *se anula en* $\mathcal{A}_F(A_1) + F$ *y* ω_2 *se anula en* $\mathcal{A}_F(A_2) + F$ *para algunos* $A_1, A_2 \in Div(F)$, *entonces* $\omega_1 + \omega_2$ *se anula en* $\mathcal{A}_F(A_3) + F$ *para cada divisor* A_3 *con* $A_3 \leq A_1$ *y* $A_3 \leq A_2$, *y* $a\omega_1$ *se anula en* $\mathcal{A}_F(A_1) + F$ *para* $a \in K$.

3. $\Omega_F(A)$ es un subespacio vectorial de Ω_F sobre K.

Lema 6.1 [11] Para $A \in \text{Div}(F)$, *tenemos que* $dim_K \Omega_F(A) = i(A)$.

En virtud del lema anterior puede deducirse que Ω_F es no vacío, pues bastaría en considerar un divisor A con $\deg A < -2$.

Definición 6.5. *Para* $x \in F$ *y* $\omega \in \Omega_F$ *definimos* $x\omega: \mathcal{A}_F \to K$ *por*

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

Obsérvese que (10) induce en Ω_F una estructura de espacio vectorial sobre F. De hecho, si ω se anula en $\mathcal{A}_F(A) + F$ para algún $A \in \text{Div}(F)$, entonces $x\omega$ se anula en $\mathcal{A}_F(A + (x)) + F$. Además se verifica que Ω_F es un espacio vectorial unidimensional sobre F. [12]

Se puede asociar un divisor a cada diferencial de Weil $\omega \neq 0$. Para ello consideremos (fijando ω) el conjunto

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

Lema 6.2. [13] *Sea* $0 \neq \omega \in \Omega_F$. *Entonces existe un divisor determinado de forma única* $W \in M(\omega)$ *tal que* $A \leq W$ *para todo* $A \in M(\omega)$.

Definición 6.6.

1. *El* divisor (ω) *de un diferencial de Weil* $\omega \neq 0$ *es el divisor de* F/K *determinado de forma única que satisface:*
   a. ω *se anula en* $\mathcal{A}_F((\omega)) + F$.
   b. *Si* ω *se anula en* $\mathcal{A}_F(A) + F$, *entonces* $A \leq (\omega)$.
2. *Para* $0 \neq \omega \in \Omega_F$ *y* $P \in \mathbb{P}_F$, *definimos* $v_P(\omega) := v_P((\omega))$.
3. *Un divisor* W *se llama divisor canónico de* F/K, *si* $W = (\omega)$ *para algún* $\omega \in \Omega_F$.

[11] Consultar página 27 de .
[12] Ver página 27 de .
[13] Para conocer más detalles consultar página 28 de .

En este sentido, $\Omega_F(A) = \{\omega \in \Omega_F : \omega = 0 \text{ o } (\omega) \geq A\}$.

Proposición 6.1.

1. *Para* $0 \neq x \in F$ *y* $0 \neq \omega \in \Omega_F$ *tenemos* $(x\omega) = (x) + (\omega)$.

2. *Si* ω_1, ω_2 *son diferenciales de Weil no nulos, entonces* $(\omega_1) = (\omega_2)$ *si y solo si* $\omega_1 = c\,\omega_2$ *para algún* $0 \neq c \in K$, *esto es, cualesquiera dos divisores canónicos de* F/K *son equivalentes.*

Demostración

1. Si ω se anula en $\mathcal{A}_F((\omega)) + F$, $x\omega$ se anula en $\mathcal{A}_F((x) + (\omega)) + F$, luego

$$(x) + (\omega) \leq (x\omega). \tag{12}$$

De igual forma, como $x\omega$ se anula en $\mathcal{A}_F((x\omega)) + F$, entonces $x^{-1}x\omega$ se anula en $\mathcal{A}_F((x^{-1}) + (x\omega)) + F$ y por lo tanto

$$(x^{-1}) + (x\omega) \leq (x^{-1}x\omega) = (\omega). \tag{13}$$

Combinando (12) y (13) obtenemos

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

Esto prueba (1).

2. Dado que Ω_F es un espacio vectorial sobre F de dimensión 1, existe un elemento no cero $c \in F$ tal que $\omega_1 = \text{c}\,\omega_2$, luego $(\omega_1) = (\text{c}\,\omega_2) = (c) + (\omega_2)$ de acuerdo con (1). Para terminar, el divisor $(c) = 0$ si y solo si $0 \neq c \in K$ (ver Observación 5.1).

Teorema 6.2. [14] *[Teorema de Dualidad] Sea* $A \in \text{Div}(F)$ *y* $W = (\omega)$ *un divisor canónico de* F/K. *Entonces la aplicación*

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

es un isomorfismo de espacios vectoriales sobre K. *En particular,* $i(A) = \ell(W - A)$.

Resumiendo los resultados de esta sección damos a conocer el Teorema de Riemann-Roch.

Teorema 6.3 (Teorema_de_Riemann-Roch) *Sea* W *un divisor canónico de* F/K. *Entonces para cada divisor* $A \in \text{Div}(F)$,

$$\ell(A) = \text{deg}A + 1 - g + \ell(W - A).$$

Ejemplo 6.1. *Haciendo* $A = 0$ *en el Teorema de Riemann-Roch se obtiene que*

$$1 = \ell(0) = \text{deg}0 + 1 - g + \ell(W - 0) = 1 - g + \ell(W - 0),$$

es decir, $\ell(W) = g$. *Ahora considerando* $A = W$ *en el Teorema 6.3, deducimos*

[14] Ver página 30 de [6].

$$g = \ell(W) = \deg W + 1 - g + \ell(W - W) = \deg W + 1 - g + \ell(0) = \deg W + 2 - g,$$

esto es, $\deg W = 2g - 2$.

Ejemplo 6.2. *Sea* $F = K(x)/K$ *el cuerpo de funciones racionales. Encontrar bases sobre* K *para los siguientes espacios vectoriales de Riemann-Roch:* $\mathcal{L}(rP_\infty), \mathcal{L}(rP_a)$ *y* $\mathcal{L}(P_{p(x)})$*, donde* $r \geq 0$ *y* P_∞*,* P_a *y* $P_{p(x)}$ *son los lugares definidos en la Sección 3.*

1. *Para* $\mathcal{L}(rP_\infty)$ *se tiene por el Teorema de Riemann-Roch y la Proposición 5.1* (1) *que* $\ell(rP_\infty) = \deg(rP_\infty) + 1 = r + 1$*. Una base sobre* K *para este espacio está dada por* $B = \{1, x, \dots, x^r\}$.

2. *En el caso de* $\mathcal{L}(rP_a)$*, su dimensión* $\ell(rP_a) = \deg(rP_a) + 1 = r + 1$*. Una base sobre* K *para dicho espacio es* $B = \{1, (x-a)^{-1}, \dots, (x-a)^{-r}\}$.

3. *Por último, si consideramos el espacio de Riemann-Roch* $\mathcal{L}(P_{p(x)})$*, tenemos que*

$$\ell(P_{p(x)}) = \deg(P_{p(x)}) + 1 = \deg p(x) + 1$$

y una base sobre K *es* $B = \{1, p(x)^{-1}, \dots, p(x)^{-\deg p(x)}\}$.

A continuación presentamos una caracterización del cuerpo de funciones racionales.

Proposición 6.2. *Para un cuerpo de funciones* F/K *las siguientes condiciones son equivalentes.*

1 . F/K *es racional; es decir,* $F = K(x)$ *para algún* $x \in F$ *trascendente sobre* K.

2. F/K *tiene género* 0 *y existe algún divisor* $A \in \mathrm{Div}(F)$ *con* $\deg A = 1$.

Si K es un cuerpo algebraicamente cerrado, siempre existe un divisor de grado 1. Por lo tanto, en este caso tenemos $g = 0$ si y solo si F/K es racional.

Ejemplo 6.3. *Sea* $F = \mathbb{R}(x, y)$ *donde* $y^2 + x^2 + 1 = 0$*. Por el ejemplo* 2.2 *sabemos que* $F/\mathbb{R}$ *es un cuerpo de funciones. Dado que el cuerpo de constantes de* F*,* $\widetilde{K}$*, es una extensión finita de* $\mathbb{R}$ *se sigue que* $\widetilde{K} = \mathbb{R}$ *o* $\widetilde{K} = \mathbb{C}$*. Suponiendo que* $\widetilde{K} = \mathbb{C}$*, se obtiene* $\mathbb{R}(x) \subsetneq \mathbb{C}(x) \subseteq \mathbb{R}(x, y)$*, luego* $\mathbb{C}(x) = \mathbb{R}(x, y)$*, pero esto no puede ser posible en vista de que* $y = \pm i\sqrt{x^2 + 1}$*, luego* $\widetilde{K} = \mathbb{R}$*, es decir,* $\mathbb{R}$ *es el cuerpo completo de constantes de* F*. Por otro lado, como todo elemento de* F *tiene un número finito de ceros y polos, podemos decir que* $v_Q(x) \geq 0$ *para todo* Q*, excepto en un número finito de lugares (los polos de* x *en* F*). Dado que* $\deg Q = [F_Q : \mathbb{R}]$ *es finito entonces de nuevo tenemos que* $\deg Q = 1$ *ó* $\deg Q = 2$*. Si* $\deg Q = 1$*, entonces* $x(Q) \in \mathbb{R}$*. Tomando clases residuales módulo* Q *en la igualdad* $y^2 + x^2 + 1 = 0$ *obtenemos*

$$(y(Q))^2 = -(x(Q))^2 - 1 \in \mathbb{R},$$

sin embargo, $y(Q) \in \mathbb{R}$ *puesto que*

$$v_Q(y^2) = v_Q(x^2 + 1) \geq \min\{v_Q(x^2), v_Q(1)\} \geq 0.$$

En ese orden de ideas, suponer que $\deg Q = 1$ *nos lleva a una contradicción. Por lo tanto,* $\deg Q = 2$*. Estudiemos a continuación los polos de* x*. Denotemos por* $Q_1, Q_2, \dots, Q_r$ *los polos de* x*, equivalentemente, los ceros de* $1/x$*, entonces dividiendo la igualdad* $y^2 + x^2 + 1 = 0$ *entre* x^2 *encontramos que*

$$\left(\frac{y}{x}\right)^2 + 1 + \left(\frac{1}{x}\right)^2 = 0.$$

Argumentando de igual forma que antes para algún lugar Q_j (cero de $1/x$) concluimos que todos los lugares de F son de grado 2. Teniendo en cuenta lo anterior, afirmamos que $g = 0$. Para ver esto, observemos que si $Q_1, Q_2, \dots, Q_r$ son ceros de x en F, entonces

$$0 \leq \sum_{i=1}^{r} v_{Q_i}(x)\deg Q_i \leq [F\colon \mathbb{R}(x)] = 2,$$

de ahí que existe un único $Q_i \in \mathbb{P}_F$ tal que $v_{Q_i}(x)\deg Q_i = 2$, siendo $\deg Q_i = 2$, así $v_{Q_i}(x) = 1$. El razonamiento anterior muestra que x sólo tiene un cero en F. Ahora dividiendo por x^2 la igualdad $y^2 + x^2 + 1 = 0$, se garantiza la existencia de un único lugar $Q' \in \mathbb{P}_F$ tal que $v_{Q'}(1/x) = 1$. Además,

$$v_{Q'}(y^2) = v_{Q'}(-x^2 - 1) = \min\{v_{Q'}(x^2), v_{Q'}(1)\} = -2,$$

esto es, $v_{Q'}(y) = -1$. Entonces para $r \geq 0$, el conjunto

$$B = \{1, x, \dots, x^r, y, yx, \dots, yx^{r-1}\} \subseteq \mathcal{L}(rQ'),$$

más aún, es linealmente independiente sobre $\mathbb{R}$ y por consiguiente

$2r + 1 \leq \ell(rQ') = \deg(rQ') - g + 1 = 2r - g + 1$ *para r suficientemente grande.*

Así las cosas, $g \leq 0$, y como $g \geq 0$, se sigue que $g = 0$. Por último, es claro que $F = \mathbb{R}(x, y)/\mathbb{R}$ no es el cuerpo de funciones racionales, dado que todos sus lugares son de grado 2 y en su efecto no existe un divisor A de grado 1.

7. Códigos Álgebro-Geométricos

Los códigos que se construyen a partir de cuerpos de funciones algebraicas fueron introducidos por primera vez por V. D. Goppa en 1981. En este apartado describiremos y desarrollaremos las propiedades de tales códigos, a los que usualmente se les conoce como códigos AG o álgebro-geométricos. Como motivación iniciamos estudiando los códigos Reed-Solomon sobre $\mathbb{F}_q$, que son un caso especial de códigos AG. De igual manera trabajaremos con códigos asociados a un cuerpo de funciones racionales.

Definición 7.1.

1. *Sea A un conjunto finito. Un código $\mathcal{C}$ de longitud n sobre A es un subconjunto del producto cartesiano A^n. A los elementos de $\mathcal{C}$ se les llaman palabras.*

2. *Sean $a = (a_1, \dots, a_n)$ y $b = (b_1, \dots, b_n)$ elementos de A^n, definimos la distancia de* Hamming *entre las palabras a y b por*

(14) $$d(a, b) := |\{i\colon a_i \neq b_i\}|,$$

esto es, $d(a, b)$ es el número de componentes en los cuales a y b difieren.

3. *La distancia mínima de un código $\mathcal{C}$, es parámetro de $\mathcal{C}$ dado por*

$$d := d(\mathcal{C}) = \min\{d(a, b)\colon a, b \in \mathcal{C}, a \neq b\}.$$

Dicho parámetro da una medida de lo bueno que es un código en relación con la detección y corrección de errores.

4. *Cuando $A = \mathbb{F}_q$ y $\mathcal{C}$ es un subespacio vectorial de $\mathbb{F}_q^n$ sobre $\mathbb{F}_q$, se dice que $\mathcal{C}$ es un código lineal y tenemos un parámetro adicional, a saber, su dimensión como subespacio vectorial de $\mathbb{F}_q^n$. Se Denota esto por $k := dim_{\mathbb{F}_q}\mathcal{C}$. Este nuevo parámetro mide la capacidad de transmisión de información del código.*

5. *El peso w de un elemento $a \in \mathbb{F}_q^n$ se define como $w(a) := d(a, 0) = |\{i: a_i \neq 0\}|$. En otras palabras, el peso de la palabra a es el número de sus componentes distintos de cero.*

6. *Diremos que $\mathcal{C}$ es un $[n, k, d]$ código lineal, si $\mathcal{C}$ tiene longitud n, dimensión k sobre el cuerpo $\mathbb{F}_q$ y distancia mínima d.*

7. *Sea $\mathcal{C}$ un $[n, k]$ código sobre $\mathbb{F}_q$. Una matriz generadora de $\mathcal{C}$ es una matriz de tamaño $k \times n$ cuyas filas forman una base de $\mathcal{C}$.*

8. *Sea $\mathcal{C} \subseteq \mathbb{F}_q^n$ un código lineal. Entonces*

$$\mathcal{C}^{\perp} := \{u \in \mathbb{F}_q^n : \langle u, c\rangle = 0 \text{ para todo } c \in \mathcal{C}\},$$

es llamado el dual *de $\mathcal{C}$.*

Dado un código $[n, k, d]$, existe una cota superior para d, más exactamente:

Proposición 7.1 (Cota de Singleton*) Sea $\mathcal{C}$ un $[n, k, d]$ código. Entonces*

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

Los códigos en donde $k + d = n + 1$ se conocen como *códigos de máxima distancia separable* (códigos MDS). A continuación se introducen los códigos Reed-Solomon, a los cuales se les estudiará diversas propiedades que poseen.

7.1 Códigos Reed-Solomon. Sea $n = q - 1$ y $\beta \in \mathbb{F}_q$ un elemento primitivo del grupo multiplicativo $\mathbb{F}_q{}^*$, es decir, $\mathbb{F}_q{}^* = \langle\beta\rangle = \{\beta, \beta^2, \dots, \beta^{q-1} = 1\}$. Para un entero k con $1 \leq k \leq n$, consideremos el espacio vectorial $k-$ dimensional

(15) $$\mathcal{L}_k := \{f \in \mathbb{F}_q[x] : \deg f \leq k - 1\},$$

y la aplicación evaluación $e_v : \mathcal{L}_k \to \mathbb{F}_q^n$ dada por

(16) $$e_v(f) := (f(\beta), f(\beta^2), \dots, f(\beta^n)) \in \mathbb{F}_q^n.$$

Notemos que para $a, b \in \mathbb{F}_q$ y $f, g \in \mathcal{L}_k$,

$$\begin{aligned} e_v(af + bg) &= \big((af + bg)(\beta), \dots, (af + bg)(\beta^n)\big) \\ e_v(af + bg) &= ((af + bg)(\beta), \dots, (af + bg)(\beta^n)) \\ &= ((af)(\beta) + (bg)(\beta), \dots, (af)(\beta^n) + (bg)(\beta^n)) \\ &= (af(\beta) + bg(\beta), \dots, af(\beta^n) + bg(\beta^n)) \\ &= (af(\beta), \dots, af(\beta^n)) + (bg(\beta), \dots, bg(\beta^n)) \\ &= a(f(\beta), \dots, f(\beta^n)) + b(g(\beta), \dots, g(\beta^n)) \\ &= ae_v(f) + be_v(g), \end{aligned}$$

Con esto se verifica que e_v es una aplicación $\mathbb{F}_q$- lineal e inyectiva. Por el Teorema de la dimensión para espacios vectoriales se sigue que $k = \dim_{\mathbb{F}_q} \mathrm{im}(e_v)$ y en su efecto,

$$\mathcal{C}_k := \{(f(\beta), f(\beta^2), \dots, f(\beta^n)) : f \in \mathcal{L}_k\} = \mathrm{im}(e_v(f)) \subseteq \mathbb{F}_q^n \tag{17}$$

es un $[n, k]$ código sobre $\mathbb{F}_q$. Llamamos a este código un *código RS o (código Reed-Solomon).*

El peso de una palabra $0 \neq c = e_v(f) \in \mathcal{C}_k$ viene dado por

$$\begin{aligned} w(c) &= |\{i \in \{1, 2, \dots, n\}; f(\beta^i) \neq 0\}| \\ &= n - |i \in \{1, 2, \dots, n\}; f(\beta^i) = 0| \\ &\geq n - \deg f \\ &\geq n - (k - 1). \end{aligned}$$

Así, la distancia mínima d de $\mathcal{C}_k$ satisface la desigualdad $d \geq n + 1 - k$, pero de otro lado $d \leq n + 1 - k$ por la cota de singleton; en consecuencia, los códigos Reed-Solomon son códigos MDS sobre $\mathbb{F}_q$. Observar que los códigos RS son de longitud pequeña en comparación con el tamaño del alfabeto $\mathbb{F}_q$, pues $n = q - 1$.

Resumiendo todo lo anterior tenemos que $\mathcal{C}_k$ es un $[n, k, d]$ código sobre $\mathbb{F}_q$, donde $n = q - 1$, y $d = q - k$.

7.2. Códigos AG. Nos interesarán principalmente los lugares racionales de un cuerpo de funciones sobre un cuerpo finito. Su número es finito y se puede estimar mediante el límite de Hasse-Weil (ver Teorema 5.2.3 de [6]). Este límite tiene muchas implicaciones teóricas numéricas y juega un papel crucial en las aplicaciones de los cuerpos de funciones algebraicas a la codificación.

Fijamos una notación válida para el resto del documento.

- $F/\mathbb{F}_q$ es un cuerpo de funciones algebraicas de género g.
- $P_1, P_2, \dots, P_n$ son lugares racionales de $F/\mathbb{F}_q$, distintos dos a dos.
- $D = P_1 + P_2 + \cdots + P_n$.
- G es un divisor de $F/\mathbb{F}_q$ tal que $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$. Esto significa que ningún P_i con $i = 1,2, \dots, n$ aparece en la expansión del divisor G.

Definición 7.2. *El* código álgebro-geométrico *o (código), $\mathcal{C}_{\mathcal{L}}(D, G)$, asociado a los divisores D y G se define por*

$$\mathcal{C}_{\mathcal{L}}(D, G) := \{(x(P_1), x(P_2), \dots, x(P_n)) : x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

Veamos que esta definición tiene sentido. Para $x \in \mathcal{L}(G)$, $v_{P_i}(x) \geq -v_{P_i}(G) = 0$ $(i = 1,2, \dots, n)$ porque $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$. La clase residual $x(P_i)$ de x módulo P_i es un elemento del cuerpo de clases residuales de P_i, F_{P_i}, pero como $\deg P_i = 1$, este cuerpo de clases residuales coincide con $\mathbb{F}_q$, así $x(P_i) \in \mathbb{F}_q$. Al igual que en (16), podemos considerar la aplicación $e_{vD} : \mathcal{L}(G) \to \mathbb{F}_q^n$, dada por

$$e_{vD}(x) := (x(P_1), x(P_2), \dots, x(P_n)) \in \mathbb{F}_q^n, \tag{18}$$

y es evidente que e_{vD} es $\mathbb{F}_q$- lineal y $\mathcal{C}_{\mathcal{L}}(D, G) = e_{vD}(\mathcal{L}(G))$. El siguiente teorema permitirá calcular (o por lo menos estimar) los parámetros n, k y d del código $\mathcal{C}_{\mathcal{L}}(D, G)$ haciendo uso del Teorema de Riemann-Roch.

Teorema 7.1. *$\mathcal{C}_{\mathcal{L}}(D,G)$ es un $[n,k,d]$ código con parámetros*

$$k = \ell(G) - \ell(G-D) \quad y \quad d \geq n - \deg G.$$

Demostración. La aplicación evaluación (18) es una aplicación $\mathbb{F}_q$ –lineal, sobreyectiva de $\mathcal{L}(G)$ a $\mathcal{C}_{\mathcal{L}}(D,G)$ con $\ker(e_{vD}) = \mathcal{L}(G-D)$. Verifiquemos esto último. Observemos que un elemento $x \in \ker(e_{vD})$ si y solo si $v_{P_i}(x) > 0$ para todo $i = 1,2,\dots,n$. Entonces, si $x \in \mathcal{L}(G-D)$, $v_{P_i}(x) \geq v_{P_i}(D) = 1$, así $x \in \ker(e_{vD})$. Por otro lado, sea $x \in \ker(e_{vD})$ y P un lugar cualquiera de $F/\mathbb{F}_q$. Si $P = P_i$ para algún $i = 1,2,\dots,n$; encontramos

$$v_P(x) \geq 1 = -v_P(G) + v_P(D),$$

y si $P \neq P_i$ $(i = 1,2,\dots,n)$, obtenemos

$$v_P(x) \geq -v_P(G) = -v_P(G) + v_P(D).$$

Por lo tanto, $x \in \mathcal{L}(G-D)$ de acuerdo con la Proposición 3.1.

De todo lo anterior y del Teorema de la dimensión se sigue que

$$k = \dim_{\mathbb{F}_q} \mathcal{C}_{\mathcal{L}}(D,G) = \ell(G) - \ell(G-D).$$

La afirmación con respecto a la distancia mínima d tiene sentido sólo si $\mathcal{C}_{\mathcal{L}}(D,G)$ no es el código $\{0\}$ por lo que supondremos esto. Escojamos un elemento $x \in \mathcal{L}(G)$ con $d = w(e_{vD}(x))$. Entonces exactamente $n-d$ lugares $P_{i_1},\dots,P_{i_{n-d}}$, en el soporte de D son ceros de x, así

$$0 \neq x \in \mathcal{L}(G - (P_{i_1} + \cdots + P_{i_{n-d}})),$$

luego concluimos por la Proposición 5.1(1) que

$$0 \leq \deg(G - (P_{i_1} + \cdots + P_{i_{n-d}})) = \deg G - n + d,$$

es decir, $d \geq n - \deg G$.

Corolario 7.1. [15] *Supongamos que* $\deg G < n$. *Entonces la aplicación evaluación*

$$e_{vD}: \mathcal{L}(G) \to \mathcal{C}_{\mathcal{L}}(D,G)$$

es inyectiva y tenemos:

1. $\mathcal{C}_{\mathcal{L}}(D,G)$ *es un* $[n,k,d]$ *código con*

19)

En consecuencia,

(20) $$d \geq n - \deg G \quad y \quad k = \ell(G) \geq \deg G + 1 - g.$$

2. *Si además,* $2g - 2 < degG$ *entonces* $k = degG + 1 - g$.

3. *Si* $\{x_1, x_2, \dots, x_k\}$ *es una base de* $\mathcal{L}(G)$ *sobre* $\mathbb{F}_q$, *entonces la matriz,*

[15] Para mayor información consultar página 50 de [6] .

$$M = \begin{bmatrix} x_1(P_1) & x_1(P_2) & \cdots & x_1(P_n) \\ x_2(P_1) & x_2(P_2) & \cdots & x_2(P_n) \\ \vdots & \vdots & \vdots & \vdots \\ x_k(P_1) & x_k(P_2) & \cdots & x_k(P_n) \end{bmatrix}$$

es una matriz generadora para $\mathcal{C}_{\mathcal{L}}(D, G)$.

La cota inferior (20) para la distancia mínima, es muy similar a la cota de singleton. Al juntar ambas cotas vemos que para $\deg G < n$,

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

Notemos que $k + d = n + 1$ si F es un cuerpo de funciones de género $g = 0$. En particular los códigos AG construidos a partir de un cuerpo de funciones racionales $\mathbb{F}_q(z)$ son códigos MDS siempre que $\deg G < n$.

7.2.1 *Códigos Álgebro-Geométricos Racionales*. En esta parte estudiamos los códigos AG asociados a divisores de un cuerpo de funciones racionales. Describiremos estos códigos mediante matrices generadoras y de chequeo de paridad. En la teoría de códigos, esta clase de códigos se conocen con el nombre de *códigos Reed-Solomon Generalizados*.

Definición 7.3. *Un código álgebro-geométrico* $\mathcal{C}_{\mathcal{L}}(D, G)$ *asociado a los divisores* D, G *de un cuerpo de funciones racionales* $\mathbb{F}_q(z)/\mathbb{F}_q$ *se dice que es* racional.

Como antes, supondremos que $D = P_1 + P_2 + \cdots + P_n$ donde los P_i son lugares racionales de $\mathbb{F}_q(z)/\mathbb{F}_q$ distintos dos a dos con $\text{Supp}(G) \cap \text{Supp}(D) = \emptyset$. Los siguientes resultados se derivan de lo expuesto anteriormente.

Proposición 7.2. [16] *Sea* $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$ *un* $[n, k, d]$ *código racional sobre* $\mathbb{F}_q$. *Entonces tenemos:*

1. $n \leq q + 1$.
2. $k = 0$ *si y solo si* $\deg G < 0$, *y* $k = n$ *si y solo si* $\deg G > n - 2$.
3. *Para* $0 \leq \deg G \leq n - 2$, $k = 1 + \deg G$ *y* $d = n - \deg G$. *En particular,* $\mathcal{C}$ *es un código* .
4. $\mathcal{C}^{\perp}$ *es también un código* AG *racional.*

A continuación se determinan matrices generadoras para códigos AG racionales.

Proposición 7.3. *Sea* $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$ *un* $[n, k, d]$ *código AG racional sobre* $\mathbb{F}_q$.

1. *Si* $n \leq q$, *existen elementos distintos dos a dos* $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ *y* $v_1, \ldots, v_n \in \mathbb{F}_q{}^*$ *(no necesariamente distintos) tales que*

$$\mathcal{C} = \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)) : f \in \mathbb{F}_q[z] \text{ y } \deg f \leq k - 1\}.$$

[16] Ver página 56 de [6] .

La matriz

$$M = \begin{bmatrix} v_1 & v_2 & \cdots & v_n \\ \alpha_1 v_1 & \alpha_2 v_2 & \cdots & \alpha_n v_n \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \cdots & \alpha_n^2 v_n \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \cdots & \alpha_n^{k-1} v_n \end{bmatrix} \tag{21}$$

es una matriz generadora para $\mathcal{C}$.

2. *Si* $n = q + 1$, $\mathcal{C}$ *tiene una matriz generadora*

$$M = \begin{bmatrix} v_1 & v_2 & \cdots & v_{n-1} & 0 \\ \alpha_1 v_1 & \alpha_2 v_2 & \cdots & \alpha_{n-1} v_{n-1} & 0 \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \cdots & \alpha_{n-1}^2 v_{n-1} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \cdots & \alpha_{n-1}^{k-1} v_{n-1} & 1 \end{bmatrix} \tag{22}$$

donde $\mathbb{F}_q = \{\alpha_1, \alpha_2, \ldots, \alpha_{n-1}\}$ *y* $v_1, v_2, \ldots, v_{n-1} \in \mathbb{F}_q{}^*$.

Demostración.

1. Sea $D = P_1 + P_2 + \cdots + P_n$. Dado que $n \leq q$ existe un lugar P de grado 1 que no está en el soporte de D. Seleccionemos un lugar $Q \neq P$ de grado 1 (por ejemplo $Q = P_1$). Para W un divisor canónico, $\deg(W - (Q - P)) = -2 < 0$, de ahí que $\ell(W - (Q - P)) = 0$. Entonces por el Teorema de Riemann-Roch $\ell(Q - P) = 1$, así que $Q - P$ es un divisor principal (ver Proposición 5.1 (2)).

Sea $Q - P = (z)$. Entonces z es un elemento generador del cuerpo de funciones racionales sobre $\mathbb{F}_q$ y P es el divisor polo de z. Como es usual, escribimos $P = P_\infty$. Por la Proposición 7.2, podemos partir del hecho de que $\deg G = k - 1 \geq 0$ (el caso $k = 0$ es trivial). El divisor $(k-1)P_\infty - G$ tiene grado cero y por el Teorema de Riemann-Roch su dimensión es mayor o igual a 1, luego es principal en virtud de la Proposición 5.1 (2), esto es, existe $u \in F_q(z)$ no cero tal que $(k-1)P_\infty - G = (u)$. El conjunto $B = \{u, zu, z^2u, \ldots, z^{k-1}u\}$ está contenido en $\mathcal{L}(G)$ y es linealmente independiente sobre $\mathbb{F}_q$. Lo primero es porque

$$\begin{aligned} (z^i u) &= i(z) + (u) \\ &= i(Q - P_\infty) + (k-1)P_\infty - G \\ &= iQ - iP_\infty + kP_\infty - P_\infty - G \\ &= iQ + (k - 1 - i)P_\infty - G \\ &\geq -G \end{aligned}$$

para $0 \leq i \leq k - 1$ y lo segundo se obtiene directamente del hecho de que z es trascendente sobre $\mathbb{F}_q$. Como $k \leq n$, entonces $\deg(G - D) = k - 1 - n < 0$ y por lo tanto, $|B| = k = \ell(G)$ según el Teorema 7.1. De esta manera B constituye una base de $\mathcal{L}(G)$ sobre $\mathbb{F}_q$ y en consecuencia

$$\mathcal{L}(G) = \{uf(z) : f \in \mathbb{F}_q[z] \text{ y } \deg f \leq k - 1\}.$$

Definiendo $\alpha_i := z(P_i) \in \mathbb{F}_q$ y $v_i := u(P_i) \in \mathbb{F}_q{}^*$, obtenemos

$$(uf(z)(P_i)) = u(P_i)f(z)(P_i) = u(P_i)f(z(P_i)) = v_i f(\alpha_i)$$

para $i = 1,2, \ldots, n$. De esta manera

$$\mathcal{C}_{\mathcal{L}}(D,G) = \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)) : \deg f \leq k-1\}.$$

La palabra en $\mathcal{C}$ correspondiente a uz^j es

$$\begin{aligned}((uz^j)(P_1),(uz^j)(P_2),\ldots,(uz^j)(P_n)) &= (u(P_1)z^j(P_1), u(P_2)z^j(P_2),\ldots,u(P_n)z^j(P_n)) \\ &= (v_1\alpha_1^j, v_2\alpha_2^j,\ldots,v_n\alpha_n^j),\end{aligned}$$

de modo que (21) es una matriz generadora de $\mathcal{C}$ por el Corolario 7.1 (3).

2. La prueba es esencialmente la misma como en el caso $n \leq q$. Dado que $n = q+1$, el Supp(D) contiene a todos los lugares de grado uno del cuerpo de funciones racionales sobre $\mathbb{F}_q$, así podemos escoger $z \in F$ tal que $P_n = P_\infty$ es el polo de z. Como antes, el divisor $(k-1)P_\infty - G = (u)$ con $0 \neq u \in F$, y $\{u, zu, \ldots, z^{k-1}u\}$ es una base de $\mathcal{L}(G)$ sobre $\mathbb{F}_q$. Para $1 \leq i \leq n-1 = q$, los elementos $\alpha_i := z(P_i) \in \mathbb{F}_q$ son distintos dos a dos, por lo que en definitiva tenemos $\mathbb{F}_q = \{\alpha_1, \alpha_2, \ldots, \alpha_{n-1}\}$. Más aún, $v_i := u(P_i) \in \mathbb{F}_q^*$ para $i = 1,2,\ldots,n-1 = q$.

La palabra correspondiente al elemento $uz^j \in \mathcal{L}(G)$ para $1 \leq j \leq k-2$ está dada por

$$((uz^j)(P_1),\ldots,(uz^j)(P_{n-1}),(uz^j)(P_n)) = (v_1\alpha_1^j,\ldots,\alpha_{n-1}^j v_{n-1},0),$$

$$\text{porque } v_{P_n}(uz^j) = v_{P_n}(u) + jv_{P_n}(z) = k-1-j \geq k-1+2-k = 1.$$

Ahora para $j = k-1$ tenemos

$$v_{P_n}(uz^{k-1}) = v_{P_n}(u) + v_{P_n}(z^{k-1}) = v_{P_n}(u) + (k-1)v_{P_n}(z) = k-1-k+1 = 0,$$

de ahí que, $uz^{k-1}(P_n) = z^{k-1}u(P_n) = z^{k-1}(P_n)u(P_n) = \gamma \neq 0$, y en su efecto

$$(uz^{k-1}(P_1), uz^{k-1}(P_2),\ldots,uz^{k-1}(P_n)) = (\alpha_1^{k-1}v_1, \alpha_2^{k-1}v_2,\ldots,\alpha_{n-1}^{k-1}v_{n-1},\gamma).$$

Sustituyendo u por $\gamma^{-1}u$ concluimos que la matriz (22) es una matriz generadora de $\mathcal{C}$, según el Corolario 7.1 (3).

Ejemplo 7.1. *Consideremos el código AG racional $\mathcal{C}_{\mathcal{L}}(D,G)$ sobre $F = \mathbb{F}_5(x)/\mathbb{F}_5$ donde $D = P_x + P_{x-1} + P_{x-2} + P_{x-3}$ y $G = P_{x^2+x+1}$. En este caso $n = 4$, y como $0 \leq \deg G = 2 \leq 4-2$ se sigue de la Proposición 7.2 (3) que $k = 3$ y $d = 2$. Por lo tanto, este código es un código MDS. De otro lado, tomemos en consideración los lugares racionales P_∞ y P_{x-1}. Entonces encontramos que $P_{x-1} - P_\infty = (x-1)$, $2P_\infty - G = \left(\frac{1}{x^2+x+1}\right)$ y el conjunto*

$$B = \left\{\frac{1}{x^2+x+1}, \frac{x-1}{x^2+x+1}, \frac{(x-1)^2}{x^2+x+1}\right\}$$

constituye una base para $\mathcal{L}(P_{x^2+x+1})$. Finalmente por la Proposición 7.3(1), una matriz generadora para el código dado es

$$M = \begin{bmatrix} v_1 & v_2 & v_3 & v_4 \\ \alpha_1 v_1 & \alpha_2 v_2 & \alpha_3 v_3 & \alpha_4 v_4 \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \alpha_3^2 v_3 & \alpha_4^2 v_4 \end{bmatrix}$$

donde $\alpha_{i+1} = (x-1)(P_{x-i})$ y $v_{i+1} = \left(\frac{1}{x^2+x+1}\right)(P_{x-i})$ para $i = 0,1,2,3$.

Definición 7.4. *Si $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_q^n$ donde $\alpha_i \neq \alpha_j$ siempre que $i \neq j$ y $v = (v_1,\ldots,v_n) \in {\mathbb{F}_q^*}^n$ donde los v_i no necesariamente son distintos, se define el código Reed-Solomon Generalizado denotado por $GRS_k(\alpha, v)$ como sigue:*

$$\mathrm{GRS}_k(\alpha, v) := \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \dots, v_n f(\alpha_n)) : f \in \mathbb{F}_q[z] \text{ y } \deg f \leq k-1\},$$

para un $k \leq n$ fijo.

Ejemplo 7.2 *En el caso* $\alpha = (\beta, \beta^2, \dots, \beta^n)$, *donde* $n = q-1$, β *es una raíz primitiva* n *–ésima de la unidad y* $v = (1,1, \dots, 1)$, *tenemos que*

$$\mathrm{GRS}_k(\alpha, v) = \{(f(\beta), f(\beta^2), \dots, f(\beta^n)) : f(z) \in \mathbb{F}_q(z) \text{ y } \deg f \leq k-1\}$$

es un código Reed-Solomon.

Un argumento similar al usado en (17) muestra que $\mathrm{GRS}_k(\alpha, v)$ es un $[n, k]$ código. La Proposición 7.3(1) establece que todos los códigos AG racionales sobre $\mathbb{F}_q$ de longitud $n \leq q$ son códigos Reed-Solomon Generalizados. Lo contrario también es cierto.

Proposición 7.4. *Cada código* $GRS_k(\alpha, v)$ *puede ser representado como un código racional.*

Demostración. Consideremos los elementos $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_q^n$ con cada α_i distinto y $v = (v_1, \dots, v_n) \in {\mathbb{F}_q^*}^n$ donde los v_i no necesariamente son distintos. Sea $F = \mathbb{F}_q(z)$ el cuerpo de funciones racionales sobre $\mathbb{F}_q$ y denotemos por P_i el cero de $z - \alpha_i$ $(i = 1,2, \dots, n)$ y por P_∞ el polo de z. Entonces $P_1, P_2, \dots, P_n, P_\infty$ son lugares racionales según la Proposición 3.1. Ahora por el Teorema de aproximación débil, existe $0 \neq u \in F$ con

$$u(P_i) = v_i(P_i) = v_i, \text{ para } i = 1,2, \dots, n. \tag{23}$$

Definamos $D := P_1 + P_2 + \cdots + P_n$ y $G := (k-1)P_\infty - (u)$. La prueba de la Proposición 7.3 muestra que $\mathrm{GRS}_k(\alpha, v) = \mathcal{C}_{\mathcal{L}}(D, G)$ para $n \leq q$.

Los mismos argumentos se aplican a un código de longitud $n = q+1$ sobre $\mathbb{F}_q$ que tiene una matriz generadora de la forma (22).

Agradecimientos

Agradezco a los profesores del departamento de matemáticas de la Universidad del Valle, el profesor H. Navarro Oyola por su apoyo como tutor y al profesor A. Garzón Rojas por hacer una lectura cuidadosa del documento y por sus comentarios que mejoraron la calidad del mismo.

REFERENCIAS

1. BC. ONDREJ VATER, *Weil diferentials*. Univerzita Karlova v Praze, págs 8-10, 2015.

2. C. CHEVALLEY, *Introduction to the Theory of Algebraic Functions of One Variable*. Mathematical Surveys and Monographs 006. American Mathematical Society, págs 2-4, 1951.

3. C.E SHANNON, *A Mathematical Theory of Communication* Reprinted with corrections from The Bell System Technical Journal,Vol. 27, pp. 379–423, 623–656, July, October, 1948.

4. D. DUMMIT, R. FOOTE, *Abstract Algebra*. Third edition, editorial John Wiley and Sons Inc, págs 196-198, 2003.

5. G. JERONIMO, J. SABIA, S. TESAURI, *Algebra Lineal*. Buenos Aires, págs 1-11, 23-33, 83-84, 95-102, agosto de 2008.

6. H. STICHTENOTH, *Algebraic Functions Fields and Codes*. Graduate Texts in Mathematics, 254. Second edition, Springer-Verlag, págs 1-62, 2008.

7. R. HILL, *An First Course in Coding Theory*. Clarendon Press. Oxford, págs 47-49, 1986.

8. S. CAÑEZ, *Notes on quotient spaces*. Págs 1-4, 2002.

9. S. ROMAN, *Field Theory*. Graduate Texts in Mathematics, 158. Second edition, Springer, New York, págs 41-66, 2006.

Luis Felipe Mosquera Hernández
Departamento de Matemáticas
Universidad del Valle
luis.felipe.mosquera@correounivalle.edu.co