Semigrupos de Weierstrass en Extensiones tipo Kummer

Luis Felipe Mosquera Hernández

Universidad del Valle

Facultad de Ciencias Naturales y Exactas

Programa Acádemico: Maestría en Ciencias Matemáticas

Santiago de Cali, Colombia

Junio 25 de 2024

Semigrupos de Weierstrass en Extensiones tipo Kummer

Luis Felipe Mosquera Hernández

Trabajo de investigación presentado como requisito
para optar por el título de:
Magister en Ciencias Matemáticas

Director:
Dr. Horacio Navarro Oyola

Universidad del Valle
Facultad de Ciencias Naturales y Exactas
Santiago de Cali, Colombia
Junio 25 de 2024

Dedicado a

Igual que lo mencionó Isaac Newton, no habría concebido este trabajo si no me hubiera parado en hombros de gigantes, por tanto dedico este documento a todos mis profesores.

Agradecimientos

Quiero agradecer a:

En primer lugar a mis padres Dilio Emir Mosquera Ocampo QEPD y María Iduara Hernández Gutiérrez porque siempre me han brindado su apoyo incondicional para poder cumplir todos mis objetivos personales y académicos. Ellos son los que con su cariño me han impulsado siempre a perseguir mis metas y nunca abandonarlas frente a las adversidades. Aunque mi padre ya no esté en este plano terrenal, siempre lo recordaré con mucho amor.

A mi esposa Luisa Carvajal Rios por su gran apoyo personal. Por estar siempre a mi lado, en los días buenos y en los no tan buenos que han acompañado este camino. Por ser la mejor compañera de vida que se puede tener.

A la Universidad del Valle por haberme recibido nuevamente como parte de su comunidad estudiantil. Siempre me sentiré orgulloso de ser un egresado de Univalle.

A mi director de tesis, el Dr Horacio Navarro Oyola por su dedicación y paciencia, sin sus conocimientos excelentes, palabras y correcciones precisas no hubiese podido lograr llegar a esta instancia tan anhelada. Gracias por su guía y todos sus consejos, los llevaré grabados para siempre en la memoria en mi futuro profesional.

A los distintos docentes que han sido parte de mi camino universitario, gracias por transmitirme los conocimientos necesarios para hoy poder estar aquí. Sin ustedes los conceptos serían solo palabras, y las palabras ya sabemos quién se las lleva, el viento.

Santiago de Cali, Colombia, Junio 25 de 2024. Luis Felipe Mosquera Hernández

Contenido

Palabras Claves

Semigrupos numéricos, conjunto Apéry, gaps, número de Frobenius, género, cuerpos de funciones, lugares racionales, lugares en el infinito, divisores, cuerpo de funciones racionales, divisor principal, divisor de polos, extensiones de Kummer, índice de ramificación, grado relativo, códigos lineales, códigos AG, códigos unipuntuales.

Notación

$\mathbb{N}$	los números naturales
$\mathbb{Z}$	los números enteros
$\mathbb{F}_q$	el cuerpo finito con q elementos
$[L : K]$	el grado de una extensión de cuerpo L/K
$\widetilde{K}$	la clausura algebraica de K
$K[T]$	el anillo de polinomios en una variable con coeficiente en K
F/K	el cuerpo de funciones algebraicas de una variable
$\widetilde{K}$	el cuerpo de constantes de F/K
F^*	las unidades del cuerpo F
$\mathcal{O}$	el anillo de valuación de F/K
P	el lugar de F/K
$\mathbb{P}_F$	el conjunto de lugares de F/K
$\mathcal{O}_P$	el anillo de valuación de un lugar P
v_P	la valuación discreta correspondiente a P

F_P	el cuerpo de clases residuales de P
$x(P)$	la clase residual de un elemento $x \in \mathcal{O}_P$ en F_P
$\deg P$	el grado de un lugar P
$\mathcal{O}_{p(x)}$	el anillo de valuación de $K(x)$, correspondiente a $p(x)$
$P_{p(x)}$	el ideal maximal de $\mathcal{O}_{p(x)}$
P_α	el lugar de $K(x)$ correspondiente a $x - \alpha$
$\mathcal{O}_\infty$	el anillo de valuación del lugar infinito de $K(x)$
P_∞	el lugar infinito de $K(x)$
$\mathrm{Div}(F)$	el grupo de divisores de F/K
$v_P(D)$	la valuación del divisor D con respecto al lugar P
$D_1 \leq D_2$	el orden de los divisores
$\deg D$	el grado de un divisor D
$(x)_0$	el divisor cero de x
$(x)_\infty$	el divisor polo de x
(x)	el divisor principal de x
$\mathscr{L}(A)$	el espacio vectorial de Riemann-Roch asociado al divisor A
$\ell(A)$	la dimensión de un divisor A
g	el género de F/K
$\mathbb{F}_q^n$	el espacio vectorial $n-$dimensional sobre $\mathbb{F}_q$
$d(a, b)$	la distancia de Hamming

$w(a)$	el peso de a
$\dim_{\mathbb{F}_q} \mathcal{C}$	la dimensión de un código $\mathcal{C}$ sobre $\mathbb{F}_q$
$[n,k], [n,k,d]$	un código con parámetros n,k; respectivamente n,k,d
$d(\mathcal{C})$	la distancia mínima del código $\mathcal{C}$
$\mathcal{C}_{\mathscr{L}}(D,G)$	el código álgebro-geométrico asociado a los divisores D,G
ϱ_{v_D}	la aplicación evaluación
$P'\|P$	el lugar P' debajo de P
$e(P'\|P)$	índice de ramificación de $P'\|P$
$f(P'\|P)$	grado relativo de $P'\|P$
$\mathrm{Con}_{F'/F}$	conorma de P en la extensión F'/F
$\mathrm{Char}\, K$	característica de K

Introducción

El estudio de los semigrupos numéricos ha proporcionado una herramienta que permite abordar problemas propios de la teoría de códigos y álgebra. La sencillez de este concepto permite plantear problemas de fácil comprensión pero cuya resolución dista mucho de ser trivial; este hecho atrajo a varios matemáticos como Frobenius y Sylvester a finales del siglo XIX, así surgió por ejemplo el problema de Frobenius, que buscaba encontrar una fórmula en función de números enteros positivos $n_1, \cdots, n_p$; para el entero más grande que no pudiese escribirse como combinación lineal de $n_1, \cdots, n_p$ ver [5].

Durante la segunda mitad del siglo pasado, los semigrupos numéricos volvieron a escena debido principalmente a sus aplicaciones en cuerpos de funciones algebraicas. Por ejemplo, el conocimiento de la estructura del semigrupo de Weierstrass en un lugar racional de un cuerpo de funciones algebraicas tiene varias implicaciones, entre estas se encuentra la busqueda de cotas superiores para el número de lugares racionales como las encontradas por Lewittes [9] y Geil-Matsumoto [10], y la construcción sobre cuerpos finitos de códigos álgebro-geométricos con buenos parámetros. Para este último, el Teorema de Riemann-Roch proporciona estimaciones para el cálculo de la dimensión y la distancia mínima del código, y en muchos casos concretos, tales determinaciones pueden también abordarse desde el punto de vista de los semigrupos numéricos. Asímismo, la teoría de semigrupos numéricos ha permitido encontrar información importante para algunos tipos especiales de códigos, por ejemplo los códigos unipuntuales y bipuntuales entre otros (Ver [3] Teorema 1.9).

En el artículo [2], Mendoza consideró extensiones de Kummer en donde el lugar P_∞ de $K(x)$ es totalmente ramificado y para éste lugar exhibió una descripción explícita de su semigrupo de Weierstrass y de su conjunto de gaps. De igual manera obtuvo resultados interesantes como el cálculo del número de Frobenius y condiciones suficientes para que el semigrupo sea simétrico.

Actualmente se tiene poco conocimiento acerca de los semigrupos de Weierstrass en lugares racionales que no son totalmente ramificados. Por lo tanto en este trabajo se estudiará el artículo [2] con el propósito de determinar, sí en extensiones de Kummer donde se omite la condición de ramificación total para P_∞, se puede describir el semigrupo de Weierstrass correspondiente a un lugar que extiende a P_∞.

En el capítulo 3 se estudia una familia particular de extensiones de tipo Kummer en donde se calculó su semigrupo de Weierstrass H; encontrando primeramente un conjunto S que está contenido en H, para luego determinar en los casos posibles su conjunto Apéry y con esto su género. De acuerdo a lo que se obtiene en este último cálculo, se procede a establecer o no la igualdad en la inclusión antes obtenida.

Capítulo **1**

Preliminares

En este capítulo se presentarán resultados necesarios para el desarrollo del trabajo. Esto incluye la teoría elemental de los semigrupos numéricos, la teoría de cuerpos de funciones algebraicas y un referente de teoría de códigos. Con el propósito de que el trabajo no sea demasiado extenso, en esta sección se omitirán las demostraciones de la mayoría de los resultados, los cuales se pueden consultar en [4], [7] y [8].

1.1 Semigrupos y Monoides

Las definiciones y diversas propiedades de los semigrupos y monoides que se dan en este capítulo, se siguió de [8]. Se inicia presentando una descripción de los semigrupos y monoides.

Definición 1.1. Un ***semigrupo*** es un par $(S, +)$ con S un conjunto y $+$ una operación binaria en S que es asociativa. Un ***sub-semigrupo*** T en un semigrupo S es un subconjunto de S que es cerrado bajo la operación binaria considerada en S.

Claramente la intersección de sub-semigrupos de un semigrupo S es nuevamente un sub-semigrupo de S, se sigue que dado un subconjunto $\emptyset \neq A$ de S, el sub-semigrupo más pequeño de S que contiene a A, es la intersección de todos los sub-semigrupos de S que contienen a A. Se denota este sub-semigrupo por $\langle A \rangle$ y es llamado *el sub-semigrupo*

generado por A. La forma más común de describir un semigrupo es a partir de sus elementos generadores.
Si $A = \{a_1, ..., a_r\}$ es un conjunto finito no vacío, entonces $\langle A \rangle$ corresponde al conjunto de todas las combinaciones lineales con coeficientes naturales no cero de los elementos de A, es decir,

$$\langle A \rangle := \{\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_r a_r : \ \lambda_i \in \mathbb{N} - \{0\} \text{ y } a_i \in A\}.$$

Se dice que S *es* ***generado*** *por* A, si $S = \langle A \rangle$. En este caso A es un *sistema de generadores de* S. Si A tiene finitos elementos se dice que S es *finitamente generado.*

Definición 1.2. Un semigrupo M es un ***monoide*** si tiene elemento identidad, esto es, existe $m \in M$ tal que $a + m = m + a = a$ para todo $a \in M$, tal elemento m es denotado por 0. Un subconjunto N de M es un ***sub-monoide*** de M si,

a) N es un sub-semigrupo de M,

b) $0 \in N$.

Al igual que en los semigrupos, la intersección de sub-monoides de un monoide es nuevamente un sub-monoide. La noción de sistema generador también se tiene en esta parte; dado un monoide M y un subconjunto A de M, el sub-monoide más pequeño de M que contiene a A es,

$$\langle A \rangle = \{\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_r a_r : \ \lambda_i \in \mathbb{N}, a_i \in A\},$$

este es llamado el ***sub-monoide*** *de* M *generado por* A. Se dice que el conjunto A es un *sistema de generadores de* M, si $M = \langle A \rangle$; cuando A es un conjunto finito se tiene que M es un monoide ***finitamente generado***.
Un ejemplo de un monoide es el conjunto de los números naturales con la operación de adición. Este monoide tiene como elemento generador al número 1.
La siguiente definición relaciona a dos conjuntos que tienen la estructura de semigrupo.

Definición 1.3. Dados dos semigrupos X, Y, una aplicación $f : X \longrightarrow Y$ es un *homo-*

morfismo de semigrupos si

$$f(a+b) = f(a) + f(b),$$

para todo $a, b \in X$. Se dice que f es un *monomorfismo, epimorfismo* o *isomorfismo*, si f es inyectiva, sobreyectiva o biyectiva, respectivamente.

Dos semigrupos X, Y se dice que son *isomorfos*, si existe un isomorfismo entre ellos, y lo denotamos por,

$$X \cong Y.$$

Asímismo, una aplicación $f : X \longrightarrow Y$ con X, Y monoides es un *homomorfismo de monoides*, si f es un homomorfismo de semigrupos y $f(0) = 0$.
Los conceptos de monomorfismo, epimorfismo e isomorfismo de monoides se definen al igual que en los semigrupos.
Ahora bien, se presenta una definición que será muy importante durante el desarrollo del trabajo. Llegando a este punto es bueno aclarar que en adelante el símbolo $\longrightarrow$ dentro de un conjunto, indicará la continuidad del mismo de manera consecutiva.

Definición 1.4. Sea $\mathbb{N} = \{0, 1, 2, \cdots, n, \longrightarrow\}$ el conjunto de los números naturales. Un ***semigrupo numérico*** es un conjunto $S \subseteq \mathbb{N}$ que es cerrado bajo la operación de adición, contiene el elemento cero y su complemento en $\mathbb{N}$ es finito, es decir, un sub-monoide de $\mathbb{N}$ con complemento finito.

Los semigrupos numéricos tienen una serie de atributos que los caracterizan, a los que llamamos invariantes.

Definición 1.5. Sea S un semigrupo numérico.

a) El *número de Frobenius* es el mayor entero que no está en S y se le identifica por $F(S)$.

b) El conjunto $G(S) := \mathbb{N} - S$ es llamado el *conjunto de gaps* de S; al cardinal de $G(S)$ se le conoce como el *género* de S y se denota por g_S.

Ilustremos los anteriores conceptos con algunos ejemplos.

Ejemplo 1.6. Dado $n \in \mathbb{N}$, el conjunto

$$O_n := \{0, n+1, n+2, n+3, \longrightarrow\}$$

es un semigrupo numérico cuyo conjunto de gaps está dado por

$$G(O_n) = \{1, 2, 3, \cdots, n\}.$$

De acuerdo a lo anterior se puede observar que el número de Frobenius es n al igual que su género.

Ejemplo 1.7. Sea el conjunto $S = \{6x+8y : x, y \in \mathbb{N}\}$. Si se desarrolla por extensión, se obtiene $S = \{0, 6, 8, 12, 14, 16, 18, 20, 22, 24, 26, \cdots\}$. Este conjunto no es un semigrupo numérico, pues $\mathbb{N} - S = \{1, 2, 3, 4, 5, 7, 9, 10, 11, 13, 15, 17, 19, 21, 23, 25, \cdots\}$ no es un conjunto finito, ya que, como se aprecia contiene a todos los números impares.

Ejemplo 1.8. Sea $S = \langle 5, 7, 9\rangle$. Tenemos que $S = \{0, 5, 7, 9, 10, 12, 14, \longrightarrow\}$ y por lo tanto $F(S) = 13, G(S) = \{1, 2, 3, 4, 6, 8, 11, 13\}$, y $g_S = 8$.

A continuación se muestra que todo semigrupo numérico (y por lo tanto todo submonoide de $\mathbb{N}$) es finitamente generado, admite un único sistema mínimo de generadores cuya cardinalidad está acotada superiormente por el elemento positivo más pequeño del monoide, para verificar esto se comienza enunciando el siguiente lema.

Lema 1.9. *Sea $A \subseteq \mathbb{N}$. Entonces $\langle A\rangle$ es un semigrupo numérico si y solo si* $\gcd(A) = 1$.

Demostración. Supongamos que $\langle A\rangle$ es un semigrupo numérico y sea $d = \gcd(A)$. Se debe probar que $d = 1$. En primera instancia observe que si $s \in \langle A\rangle$, entonces $s = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_r a_r$ donde $\lambda_i \in \mathbb{N}$ y $a_i \in A$, por hipótesis $d \mid a_i$ para cada i, luego también $d \mid s$.
Como $\langle A\rangle$ es un semigrupo numérico se tiene que $\mathbb{N} - \langle A\rangle$ es un conjunto finito. Entonces existe por lo menos una pareja de números naturales consecutivos $x, x+1 \in \langle A\rangle$. En el supuesto que no existieran los números naturales consecutivos $x, x+1$ en $\langle A\rangle$, entonces entre cada pareja de números naturales que estan en $\langle A\rangle$, podemos encontrar al menos

un número natural que pertenece a $\mathbb{N} - \langle A \rangle$, y dado que en $\langle A \rangle$ hay infinitas parejas de enteros no negativos, se obtendrán infinitos números naturales en $\mathbb{N} - \langle A \rangle$, es decir, el complemento de $\langle A \rangle$ no es finito, lo cual es una contradicción.
Finalmente, como $d = \gcd(A)$ y tanto x como $x + 1$ están en $\langle A \rangle$, entonces de acuerdo a lo mencionado al inicio, d divide simultáneamente a x y a $x + 1$, lo cual se cumple únicamente cuando $d = 1$.
Recíprocamente, supongamos que $\gcd(A) = 1$. Se debe verificar que $\mathbb{N} - \langle A \rangle$ es un conjunto finito. En efecto, como $\gcd(A) = 1$, el Lema de Bezoút garantiza la existencia de números enteros z_i tales que

$$1 = z_1 a_1 + z_2 a_2 + \cdots + z_n a_n$$

donde $a_i \in A$.
Transponiendo los términos z_i negativos al lado derecho se tiene,

$$z_{i_1} a_{i_1} + \cdots + z_{i_k} a_{i_k} = 1 - z_{j_1} a_{j_1} - \cdots - z_{j_l} a_{j_l} \in \langle A \rangle,$$

para algunos $i_1, \cdots, i_k, j_1, \cdots, j_l \in \{1, \cdots, n\}$, entonces existe $s \in \langle A \rangle$ tal que $s + 1 \in \langle A \rangle$. Se afirma que dado $n \in \mathbb{N}$, si $n \geq (s-1)s + (s-1)$ entonces $n \in \langle A \rangle$, En efecto, sean q y r números enteros tales que $n = qs + r$ con $0 \leq r < s$. Por hipótesis,

$$qs + r \geq (s-1)s + (s-1),$$

de donde se obtiene,

$$q \geq s - 1 + \frac{s - 1 - r}{s} \geq s - 1 \geq r,$$

y en consecuencia $n = (rs + r) + (q - r)s = r(s + 1) + (q - r)s \in \langle A \rangle$. De acuerdo a esto; si $n \in \mathbb{N} - \langle A \rangle$, entonces $n < (s-1)s + (s-1)$, es decir, $|\mathbb{N} - \langle A \rangle|$ es finito. □

Una consecuencia del lema anterior es que todo sub-monoide no trivial de $\mathbb{N}$ puede hacerse corresponder con un semigrupo numérico, como se muestra a continuación.

Proposición 1.10. *Sea M un sub-monoide no trivial de $\mathbb{N}$. Entonces $M \cong S$ donde S es un semigrupo numérico.*

Demostración. Sea $d = \gcd(M)$. En virtud del lema anterior se tiene que

$$S := \left\langle \frac{m}{d} : \ m \in M \right\rangle$$

es un semigrupo numérico, entonces la aplicación $f : M \longrightarrow S$ dada por $f(m) = \dfrac{m}{d}$ es un isomorfismo de monoides. □

Si A, B son subconjuntos de números enteros, se escribe $A+B = \{a+b : a \in A, b \in B\}$, por lo tanto, para un semigrupo numérico S, si se denota por $S^* := S - \{0\}$, el conjunto $S^* + S^*$ corresponde a un conjunto cuyos elementos están en S y son la suma de dos elementos no nulos en S.
Considerando la notación previa, el siguiente lema proporciona una forma general para obtener un sistema de generadores para un semigrupo numérico S.

Lema 1.11. *Sea S un semigrupo numérico. Entonces $S^* - (S^* + S^*)$ es un sistema de generadores de S. Más aún, cada sistema de generadores de S contiene a $S^* - (S^* + S^*)$.*

Demostración. Sea $s \in S^*$, entonces se presentan los siguientes casos:

- Caso 1: Si $s \in S^* - (S^* + S^*)$, se obtiene de manera inmediata la conclusión.
- Caso 2: Si $s \notin S^* - (S^* + S^*)$, entonces $s \in S^* + S^*$, luego existen $x, y \in S^*$ tales que $s = x + y$.

Note que s se ha expresado como la suma de x e y, y estos son menores que s, pero, como el conjunto de enteros positivos, menores que s, es finito, entonces, para cada uno de los x e y que se hallan, puede aplicarse nuevamente, el caso 1 o caso 2, hasta que, después de una cantidad finita de pasos, se obtenga solamente números que ya no admiten representarse como la suma de 2 elementos no nulos de S; lo cual implica que esta última colección de enteros positivos, estaría en $S^* - (S^* + S^*)$ y por consiguiente hemos probado que sus elementos generan a aquellos elementos que no están en $S^* - (S^* + S^*)$. Por lo tanto, $S^* - (S^* + S^*)$ es un sistema de generadores de S.
Para culminar la prueba, considerese A un sistema de generadores de S, y mostremos que $S^* - (S^* + S^*) \subseteq A$. Suponga que $x \in S^* - (S^* + S^*) \subseteq S = \langle A \rangle$, entonces existe $n \in$

$\mathbb{N}-\{0\}, \lambda_1, \lambda_2, \cdots, \lambda_n \in \mathbb{N}$ y $a_1, a_2, \cdots, a_n \in A$ tales que $x = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n$. Como $x \notin S^* + S^*$ se sigue que $x = a_i$ para algún $i \in \{1, 2, \cdots, n\}$. □

El siguiente conjunto es muy utilizado en las aplicaciones de semigrupos numéricos.

Definición 1.12. Sean S un semigrupo numérico y $n \in S^*$, el conjunto,

$$\mathrm{Ap}(S; n) := \{s \in S : s - n \notin S\},$$

es llamado el ***el conjunto apéry*** de n en S.

A continuación se presenta una caracterización del conjunto Apery.

Lema 1.13. *Sean S un semigrupo numérico y $n \in S^*$, entonces,*

$$\mathrm{Ap}(S; n) = \{0 = w(0), w(1), w(2), \cdots, w(n-1)\}$$

donde

$$w(i) = \text{mín}\{k \in S : k \equiv i \mod (n)\};$$

en particular este conjunto tiene n elementos.

Demostración. Sea $s \in \mathrm{Ap}(S; n)$, esto es, $s \in S$ con $s - n \notin S$, por el algoritmo de la división existen $t, r \in \mathbb{Z}$ tales que $s - n = nt + r$ con $0 \leq r < n$; de ahí que $s \equiv r$ mód (n). Veremos que s es el elemento mínimo que satisface esta condición. Suponga que $s' \in S, s' \equiv r \mod (n)$ y $s' < s$, como $s' \equiv r \mod (n)$ existe $t_1 \in \mathbb{Z}$ tal que $s' - r = nt_1$, más aún, el hecho de que $s' < s$ implica que $t \geq t_1$ con lo cual $s - n \in S$, puesto que,

$$s - n = nt + s' - nt_1 = n(t - t_1) + s' \in S.$$

Esto es una contradicción y por consiguiente $s = \text{mín}\{k \in S : k \equiv i \mod (n)\}$.
Por otro lado probemos que si $w(i) := \text{mín}\{k \in S : k \equiv i \mod (n)\}$, entonces $w(i) \in \mathrm{Ap}(S; n)$. Note que $w(i) \equiv i \mod (n)$, entonces $w(i) - n \equiv i \mod (n)$. Si $w(i) - n \in S$ se tiene una contradicción ya que $w(i) - n < w(i)$, luego $w(i) - n \notin S$, es decir, $w(i) \in \mathrm{Ap}(S; n)$. □

Ejemplo 1.14. Sea S el semigrupo numérico generado por $A = \{5, 7, 9\}$, entonces

$$S = \langle 5, 7, 9\rangle = \{0, 5, 7, 9, 10, 12, 14, \longrightarrow\},$$

y por lo tanto $\mathrm{Ap}(S; 5) = \{0, 7, 9, 16, 18\}$.

El conjunto Apéry nos permite caracterizar de forma única los elementos del semigrupo numérico.

Lema 1.15. *Sea S un semigrupo numérico y $n \in S^*$, entonces para todo $s \in S$ existe un único par $(k, w) \in \mathbb{N} \times \mathrm{Ap}(S; n)$ tal que $s = kn + w$.*

Demostración.
Existencia: Por el algoritmo de la división existen $q, i \in \mathbb{Z}$ con $0 \leq i < n$ tales que $s = nq + i$. Como $w(i)$ es el menor elemento de S que es congruente con i módulo n, tenemos $w(i) = np + i$ para algún $p \in \mathbb{Z}$, si restamos ambas igualdadades se obtiene: $s - w(i) = n(q - p)$, es decir, $s = n(q - p) + w(i)$. Note que $q > p$ pues $w(i) < s$. Así las cosas, podemos escribir $s = nk + w(i)$ donde $k = q - p$.
Unicidad: Suponga que $s \in S$ y admite las siguientes dos representaciones $s = k_1n+w_1$ y $s = k_2n+w_2$ donde $k_1, k_2 \in \mathbb{N}$ y $w_1, w_2 \in \mathrm{Ap}(S; n)$, entonces $(k_1-k_2)n+(w_1-w_2) = 0$. Debemos demostrar que $k_1 = k_2$ y $w_1 = w_2$. Considerando $k_2 > k_1$ se tiene que $w_1 - n = w_2 + (k_2 - k_1 - 1)n \in S$, lo cual es una contradicción. Asímismo, si $k_1 > k_2$ se cumple que $w_2 - n = w_1 + (k_1 - k_2 - 1)n \in S$, nuevamente un absurdo. En consecuencia, se tiene $k_1 = k_2$ y por ende $w_1 = w_2$. □

Una vez visto que todo semigrupo numérico es finitamente generado, es natural preguntarse si existe un único conjunto mínimo de generadores.

Definición 1.16. Un sistema de generadores de un semigrupo numérico es un *sistema mínimo de generadores,* si ninguno de sus subconjuntos propios generan el semigrupo numérico.

En la términos de la definición anterior, el Lema 1.11 establece que si S es un semigrupo numérico, entonces $S^* - (S^* + S^*)$ es un sistema mínimo de generadores, de hecho, por la definición anterior este sistema es único.

El siguiente resultado nos da información acerca de la cardinalidad del conjunto mínimo generador.

Teorema 1.17. *Sea S un semigrupo numérico, entonces el sistema mínimo de generadores de S, a saber $S^* - (S^* + S^*)$ es finito.*

Demostración. Por el Lema 1.15 se tiene que para cualquier $n \in S^*$, $S = \langle \mathrm{Ap}(S;n) \cup \{n\}\rangle$. Como $\mathrm{Ap}(S;n) \cup \{n\}$ es finito se deduce que $S^* - (S^* + S^*)$ es finito. □

Como todo sub-monoide de $\mathbb{N}$ es isomorfo a un semigrupo numérico, esta propiedad es válida para sub-monoides de $\mathbb{N}$.

Corolario 1.18. *Sea M un sub-monoide de $\mathbb{N}$, entonces M tiene un único sistema mínimo de generadores que además es finito.*

Demostración. Sea $d = \gcd(M)$, entonces $T := \left\{\frac{x}{d} : x \in M\right\}$ es un sub-monoide de M tal que $\gcd(T) = 1$; en virtud del Lema 1.9 esto significa que T es un semigrupo numérico. Ahora sea A el sistema mínimo de generadores de T. Como $\frac{x}{d} \in T$ se puede escribir $\frac{x}{d} = \lambda_1 a_1 + \cdots \lambda_n a_n$ para algunos $\lambda_i \in \mathbb{N}$ y $a_i \in A$, de aquí que,

$$x = d(\lambda_1 a_1 + \cdots + \lambda_n a_n) = \lambda_1 d a_1 + \cdots + \lambda_n d a_n,$$

lo cual permite deducir que $\{da : a \in A\}$ es un sistema mínimo de generadores de M. □

A continuación damos dos conceptos que se siguen de la Definición 1.16.

Definición 1.19. Sea S un semigrupo numérico y $\{n_1 < n_2 < \cdots < n_p\}$ su sistema mínimo de generadores. Entonces n_1 se llama *la multiplicidad de S* y se denota por $m(S)$. Asímismo, el cardinal del sistema mínimo de generadores de S se llama la *dimensión de inmersión de S* y se identifica por $e(S)$.

La siguiente proposición establece una relación entre la multiplicidad de un semigrupo numérico y su dimensión de inmersión.

Proposición 1.20. *Sea S un semigrupo numérico, entonces,*

a) $m(S) = \text{mín}(S^*)$.

b) $e(S) \leq m(S)$.

Demostración. Primeramente mostremos que la multiplicidad de S es el menor entero positivo en S. Suponga que $S = \langle n_1, n_2, \cdots, n_p \rangle$ con $0 < n_1 < n_2 < \cdots < n_p$, donde $\{n_1, n_2, \cdots, n_p\}$ es un sistema mínimo de generadores; cualquier $s \in S$ puede representarse como $s = \lambda_1 n_1 + \cdots + \lambda_p n_p$ con $\lambda_i \in \mathbb{N}$, entonces el entero positivo más pequeño de S es n_1.
Por otro lado, note que $\{m(S)\} \cup \text{Ap}(S; m(S)) - \{0\}$ es un sistema de generadores de S con cardinal $m(S)$, entonces $e(S) \leq m(S)$. □

Ejemplo 1.21. Sea S un semigrupo numérico, entonces $e(S) = 1$ si y solo si $S = \mathbb{N}$.

Ejemplo 1.22. Si $m \in \mathbb{Z}^+$, entonces $S = \{0, m, \longrightarrow\}$ es un semigrupo numérico con multiplicidad m. Un sistema mínimo de generadores para S es $\{m, m+1, \cdots, m+(m-1)\}$ y por lo tanto $e(S) = m = m(S)$.

El resultado siguiente nos proporciona una forma de encontrar el número de Frobenius y el género de un semigrupo numérico a partir del conjunto Apéry.

Proposición 1.23. *Sean S un semigrupo numérico y $n \in S^*$, entonces*

a) $F(S) = \text{máx}\{\text{Ap}(S; n)\} - n$.

b) $g_S = \dfrac{1}{n}\left(\displaystyle\sum_{w \in \text{Ap}(S;n)} w\right) - \dfrac{n-1}{2}$.

Demostración.

a) Por la definición 1.12 se tiene que $\text{máx}\{\text{Ap}(S; n)\} - n \notin S$. Sea $x > \text{máx}\{\text{Ap}(S; n)\} - n$, entonces $x + n > \text{máx}\{\text{Ap}(S; n)\}$ de modo que $x + n \notin \text{Ap}(S; n)$. Esto significa que $x + n \notin S$ o $x \in S$. Suponiendo que $x + n \notin S$, podemos considerar $w \in \text{Ap}(S; n)$ tal que $x + n \equiv w \mod (n)$, entonces $x + n = w + tn$ para algún $t \in \mathbb{Z}$, y como $w < x + n$ se infiere que $t \in \mathbb{Z}^+$. De acuerdo con lo anterior $x + n = w + tn \in S$ obteniendo así una contradicción; por lo tanto $x \in S$. En consecuencia, si x es un gap, entonces $x \leq \text{máx}\{\text{Ap}(S; n)\} - n$ y dado que $F(S)$ es el mayor gap de S tenemos lo deseado.

b) Por el Lema 1.13 se tiene que para cada $w \in \mathrm{Ap}(S;n)$, $w = w(i)$ para algún $i \in \{0,1,2\cdots,n-1\}$ donde $w(i) = i + k_i n$ siendo k_i un entero no negativo. Ahora se analizan los valores de k_i.

- Si $k_i = 0$, entonces $w(i) = i$, el cual tiene que pertenecer a S, pues los $w(i) \in S$.
- Si $k_i = 1$ entonces $w(i) = i + n \in S$, entonces $w(i) - n = i \notin S$ y por lo tanto, $i \in G(S)$. De este modo se ha encontrado un elemento de $G(S)$.
- Si $k_i = 2$, entonces $w(i) = i+2n \in S$, luego se tiene que $w(i)-n = i+n \notin S$ y $w(i) - 2n = i \notin S$, encontramos así dos elementos más de $G(S)$.

Por lo tanto el número de elementos de $G(S)$ viene dado por

$$\begin{aligned} g_S =& k_1 + k_2 + \cdots + k_{n-1} = \frac{1}{n}\left(nk_1 + nk_2 + \cdots + nk_{n-1}\right) \\ =& \frac{1}{n}((nk_1+1) + (nk_2+2) + \cdots + (nk_{n-1}+n-1) - (1+2+\cdots+n-1)) \\ =& \frac{1}{n}\left(w(1) + w(2) + \cdots + w(n-1) - \frac{(n-1)n}{2}\right) \\ =& \frac{1}{n}\left(\sum_{i=1}^{n-1} w(i)\right) - \frac{(n-1)}{2}. \end{aligned}$$

□

El siguiente ejemplo describe explicítamente el conjunto Apéry de un semigrupo numérico generado por 2 elementos.

Ejemplo 1.24. Considére S un semigrupo numérico minimalmente generado por $\langle a, b\rangle$. Observe que dos elementos de la forma xb, yb donde $x \neq y, 0 \leq x, y \leq (a-1)$ pertenecen a clases módulo a diferentes.

En efecto, si $xb \equiv yb \mod (a)$, entonces $a|b(x-y)$ y dado que $\gcd(a,b) = 1$, necesariamente $a|(x-y)$, De ahí se deduce que $x \equiv y \mod (a)$, y como $x, y < a$ se tiene $x = y$. Por otra parte, recordando que $\mathrm{Ap}(S;a)$ tiene a elementos y se han descrito a clases de equivalencia distintas, por el Lema 1.13 se concluye la igualdad $\mathrm{Ap}(S;a) = \{0, b, 2b, \cdots, (a-1)b\}$.

A continuación se enuncia un resultado que permite calcular el número de Frobenius y el género de un semigrupo numérico generado por dos elementos.

Proposición 1.25. *Sean $a, b \in \mathbb{Z}^+$ con $\gcd(a,b) = 1$, entonces,*

a) $F(\langle a, b\rangle) = ab - a - b$.

b) $g_{(\langle a,b\rangle)} = \dfrac{ab-a-b+1}{2} = \dfrac{F(\langle a,b\rangle)+1}{2}$.

Demostración.

a) $F(\langle a, b\rangle) = \text{máx}\{\text{Ap}(S;a)\} - a = (a-1)b - a = ab - b - a$.

b) De la Proposición 1.23,

$$\begin{aligned} g_{(\langle a,b\rangle)} &= \frac{1}{a}\left(\sum_{w\in \text{Ap}(S;a)} w\right) - \frac{a-1}{2} \\ &= \frac{1}{a}(0 + b + 2b + \cdots + (a-1)b) - \frac{a-1}{2} \\ &= \frac{b(1+\cdots+(a-1))}{a} - \frac{a-1}{2} \\ &= \frac{1}{a}\cdot\frac{b(a-1)a}{2} - \frac{a-1}{2} \\ &= \frac{b(a-1)}{2} - \frac{a-1}{2} \\ &= \frac{(b-1)(a-1)}{2}. \end{aligned}$$

□

El siguiente resultado establece una expresión que generaliza la parte (b) de la proposición anterior.

Lema 1.26. *Sea S un semigrupo numérico, entonces, $g_S \geq \dfrac{F(S)+1}{2}$.*

Demostración. Defina el conjunto

$$N(S) := \{s \in S : s < F(S)\}$$

y denote por $n(S)$ al cardinal de $N(S)$. Observando que

$$\{0, 1, 2, \cdots, F(S)\} = \{s \in S : s < F(S)\} \cup \{g_1, g_2, \cdots, F(S)\},$$

donde los g_i son los gaps de S, y que ésta unión es disjunta, tenemos que $1 + F(S) = n(S) + g_S$, es decir, $n(S) = 1 + F(S) - g_S$. Ahora, considére la aplicación

$$\varphi : \begin{cases} N(S) & \longrightarrow G(S), \\ s & \longmapsto F(s) - s, \end{cases}$$

entonces, claramente φ está bien definida y es inyectiva, luego se deduce $n(S) \leq g_S$ de manera que $g_S \geq F(S) + 1 - g_S$, resolviendo para g_S se obtiene lo deseado. □

Un tipo de semigrupos numéricos especiales son aquellos en donde se da la igualdad en la desigualdad anterior.

Definición 1.27. Sea S un semigrupo numérico con género g_S y número de Frobenius $F(S)$. Se dice que S es *simétrico* si $F(S) = 2g_S - 1$.

Sabemos que dado un semigrupo numérico S, siempre existirá un entero $F(S)$ que no está en S, tal que, si n es mayor que $F(S)$, entonces $n \in S$. Al número $F(S)$ se le ha denominado número de Frobenius.
Considére un semigrupo numérico S con número de Frobenius $F(S)$, si $s \in S$, entonces $F(S) - s \notin S$, ya que si $F(S) - s \in S$, entonces por la estructura de S, se debe tener que $(F(S) - s) + s \in S$, es decir, $F(S) \in S$, lo cual es absurdo y por ello debe cumplirse que $F(S) - s \notin S$. Pero, el caso contrario no es necesariamente cierto, es decir: si $F(S) - x \notin S$, entonces $x \in S$. Lo anterior no siempre ocurre y el siguiente ejemplo ilustra esta situación.

Ejemplo 1.28. Sea el semigrupo numérico $S = \{0, 5, 6, 7, 8, 9, \longrightarrow\}$. Se observa que todos los enteros que exceden a 4 están en S, entonces $F(S) = 4$, luego: $4 - 0 \notin S$ y $0 \in S$, $4 - 1 \notin S$ y $1 \notin S$, $4 - 2 \notin S$ y $2 \notin S$, $4 - 3 \notin S$ y $3 \notin S$. Aquí notamos que, si $F(S) - x \notin S$, entonces no puede afirmarse que $x \in S$.

En ese sentido tenemos lo siguiente.

Proposición 1.29. *Sea S un semigrupo numérico simétrico. Entonces $F(S) - s \notin S$ si y solo si $s \in S$.*

Demostración. De acuerdo a lo anterior basta ver que para un elemento $s \in \mathbb{N}$, si $F(S) - s \notin S$, entonces $s \in S$.
Considére el conjunto,

$$N(s) = \{s \in S : s < F(S)\},$$

ya definido en el Lema 1.26 y sea $N(s) = \{0, s_1, s_2, \cdots, s_k\}$, entonces $k+1 = 1+F(S)-g$ y como S es simétrico se obtiene $k = g_S - 1$. De esta manera se tiene g_S elementos en $N(s)$.
Dado que $F(S)-s_i \notin S$ para todo $i \in \{1, 2, \cdots, k = g_S-1\}$; sin pérdida de generalidad se puede decir que

$$\begin{aligned} F(S) - s_1 &= g_1, \\ F(S) - s_2 &= g_2, \\ &\vdots \\ F(S) - s_{g_S-1} &= g_{g_s-1}, \\ F(S) - 0 &= g_{g_S}, \end{aligned}$$

donde los elemetos g_i son los gaps de S, entonces si $s \in \mathbb{N}$ tal que $F(S)-s \notin S$, se sigue que $F(S) - s = g_i$ para algún $i \in \{1, 2, \cdots, g_S\}$, por lo tanto, $F(S) - s = F(S) - s_i$ de donde se deduce $s = s_i \in S$. □

Note que cuando $F(S)$ es un número par, entonces para n entero positivo, $F(S) = 2n$ con lo cual $F(S) - n = n$. Esto implica que, si $n \notin S$ entonces $F(S) - n$ no pertenecería a S; luego puede afirmarse lo siguiente; cuando el número de Frobenius $F(S)$ es par, entonces el semigrupo numérico S, no es simétrico.
El siguiente resultado permite decir cuando un elemento no hace parte de un semigrupo numérico generado por dos elementos.

Proposición 1.30. *Sean $x \in \mathbb{Z}$ y $n_1, n_2 \geq 2$ enteros positivos tales que* $\gcd(n_1, n_2) = 1$, *entonces $x \notin \langle n_1, n_2 \rangle$ si y solo si $x = n_1 n_2 - a n_1 - b n_2$, para algunos $a, b \in \mathbb{N}$.*

Demostración. Supongamos primero que $x \notin \langle n_1, n_2 \rangle$. Por la Proposición 1.25 el semigrupo numérico $\langle n_1, n_2 \rangle$ es simétrico y su número de Frobenius es $F(\langle n_1, n_2 \rangle) = n_1 n_2 - n_1 - n_2$, entonces la Proposición 1.29 implica que $n_1 n_2 - n_1 - n_2 - x \in \langle n_1, n_2 \rangle$; esto significa que existen $\lambda, \beta \in \mathbb{N}$ tales que $n_1 n_2 - n_1 - n_2 - x = \lambda n_1 + \beta n_2$, luego $x = n_1 n_2 - (\lambda + 1) n_1 - (\beta + 1) n_2$. Suponga ahora que $x = n_1 n_2 - a n_1 - b n_2$ para algunos $a, b \in \mathbb{N}$.
Si $x \in \langle n_1, n_2 \rangle$, entonces se deduce que $F(\langle n_1, n_2 \rangle) = n_1 n_2 - n_1 - n_2 \in \langle n_1, n_2 \rangle$, pues,

$$n_1 n_2 - n_1 - n_2 = n_1 n_2 - a n_1 - b n_2 + (a - 1) n_1 + (b - 1) n_2,$$

lo cual es una contradicción. □

Se presenta ahora algunos resultados importantes de la teoría de cuerpos de funciones.

1.2 Cuerpos de funciones algebraicas

A lo largo de esta sección K denotará un cuerpo arbitrario. De lo contrario se le indicará al lector. La mayoría de los resultados presentados en esta parte son tomados del referente bibliográfico [4] y parte del trabajo monográfico [6].

Definición 1.31. 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 dado que la suma, producto e inversos de elementos algebraicos son también elementos algebraicos; a los elementos de $\widetilde{K}$ se les denomina *constantes* y al cuerpo $\widetilde{K}$ se le llama *el cuerpo de constantes* de F/K, además, es claro que $K \subseteq \widetilde{K} \subsetneq F$.

El cuerpo K es *algebraicamente cerrado en* F (o K es *el cuerpo completo de constantes de* F) si $K = \widetilde{K}$.
Un cuerpo de funciones F/K suele representarse como una extensión algebraica simple de un cuerpo de funciones racionales $K(x)$; es decir,

$$F = K(x)(y) = K(x, y)$$

donde $\varphi(y) = 0$ para algún polinomio irreducible φ con coeficientes en $K(x)$.
Un *anillo de valuación* de un cuerpo de funciones F/K es un anillo $\mathcal{O} \subseteq F$ con las siguientes propiedades:

a) $K \subsetneqq \mathcal{O} \subsetneqq F$.

b) Para todo $z \in F$, se cumple que $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$.

Algunos resultados relacionados con anillos de valuación se muestran a continuación.

Teorema 1.32. *Sea $\mathcal{O}$ un anillo de valuación de F/K. Entonces*

(a) $\mathcal{O}$ es un anillo local, es decir, $\mathcal{O}$ tiene un único ideal maximal $P = \mathcal{O} - \mathcal{O}^*$, donde

$$\mathcal{O}^* = \{z \in F : \textit{existe } w \in \mathcal{O} \textit{ con } wz = zw = 1\ \},$$

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

(b) Sea P el único ideal maximal de $\mathcal{O}$, entonces

i) P es un ideal principal,

ii) 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 $u \in \mathcal{O}^*$.

Un *lugar* P de un cuerpo de funciones F/K es el ideal maximal de algún anillo de valuación $\mathcal{O}$ de F/K, al conjunto de lugares de F/K se le denota por $\mathbb{P}_F$.

Un *elemento primo* de un lugar P es aquel elemento $t \in P$ tal que $P = t\mathcal{O}$.

Si $\mathcal{O}$ es un anillo de valuación de F/K y P es su ideal maximal, entonces $\mathcal{O}$ es determinado de manera única por P, a saber,

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

Por esto, $\mathcal{O}_P := \mathcal{O}$ se llama *el anillo de valuación del lugar P*. Una segunda descripción útil de los lugares se da en términos de valuaciones. Una *valuación discreta* de F/K es una función sobreyectiva $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ con las siguientes propiedades;

a) $v(x) = \infty$ si y solo si $x = 0$,

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

c) $v(x + y) \geq \text{mín}\{v(x), v(y)\}$ para todo $x, y \in F$,

d) Existe $z \in F$ para el cual $v(z) = 1$,

e) $v(a) = 0$ 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 (c) es conocida como *desigualdad triangular*.
Una propiedad de utilidad al momento de trabajar con valuaciones es la *desigualdad triangular estricta*, la cual es consecuencia de los items anteriores y afirma que, dados $x, y \in F$ con $v(x) \neq v(y)$, entonces,

$$v(x + y) = \text{mín}\{v(x), v(y)\}.$$

Si P es un lugar de F, se puede asociarle una función $v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ (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

$$v_P(z) =: \begin{cases} n & si \quad z = t^n u \\ \\ \infty & si \quad z = 0. \end{cases}$$

También note que dado un lugar P, entonces,

$$\mathcal{O}_P = \{z \in F : v_P(z) \geq 0\} \text{ y } P = \{z \in F : v_P(z) > 0\} \ ,$$

donde v_P denota la valuación discreta de P.

Si z es un elemento no nulo de F y $P \in \mathbb{P}_F$, con $v_P(z) > 0$ se dice que P es un *cero* de z y si $v_P(z) = m > 0$, se dice que P *es un cero de* z *de orden* m. Asímismo, si $v_P(z) < 0$, entonces P es un *polo* de z y si $v_p(z) = -m < 0$, entonces P es *un polo de* z *de orden* m. En particular, si P es un cero (resp. un polo) de orden 1 de z, a P se le llama un *cero simple* (resp.*un polo simple*) de z. Se puede probar que un elemento z en F es un elemento primo para P, si P es un cero simple de z.

Dado P un lugar de F/K y $\mathcal{O}_P$ su anillo de valuación, el anillo $\mathcal{O}_P/P$ tiene una estructura de cuerpo. Este cuerpo se denota por $F_P := \mathcal{O}_P/P$ y se llama *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 se define $x(P) := \infty$. Puede pensarse en K como un subcuerpo de F_P mediante la inmersión $K \hookrightarrow F_P$ inducida al restringir el homomorfismo canónico $\pi : \mathcal{O}_P \longrightarrow \mathcal{O}_P/P$ sobre K, más aún, el argumento previo también es válido para $\widetilde{K}$; en definitiva se consideran a K y $\widetilde{K}$ subcuerpos de F_P. En virtud de lo anterior se define el *grado* de P como

$$\deg P := [F_P : K]$$

y se puede probar que todo lugar tiene grado finito y que

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

Un lugar de grado uno se llama *lugar racional* de F/K y serán de interés en los dos últimos capítulos de este trabajo.

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 $x \in F - \mathcal{O}_P$, se llama la *aplicación de clases residuales* con respecto a P.

En adelante F/K denotará un cuerpo de funciones con K su cuerpo completo de constantes.

A continuación se presentan los conceptos necesarios para definir el género de un cuerpo de funciones que es un invariante de gran importancia en esta teoría. Hasta ahora el conjunto de lugares $\mathbb{P}_F$ de un cuerpo de funciones F/K no tiene una estructura algebraica que relacione sus elementos, sin embargo, se puede pensar en el grupo abeliano libre generado por $\mathbb{P}_F$.

Definición 1.33. El *grupo divisor* de F/K se define como el grupo abeliano libre (escrito aditivamente) que es generado por los lugares de F/K y se denota por $\mathrm{Div}(F)$.

a) Los elementos de $\mathrm{Div}(F)$ se denominan *divisores* de F/K; en otras palabras, un divisor D es una suma formal,

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

b) Sean $D = \sum_{P \in \mathbb{P}_F} n_P P$ y $D' = \sum_{P \in \mathbb{P}_F} m_P P$ dos divisores de F. Se define la suma de D y D' como,

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

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

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

d) Para $Q \in \mathbb{P}_F$ y $D = \sum_{P \in \mathbb{P}_F} n_P P$ se define $v_Q(D) := n_Q$.

e) En $\mathrm{Div}(F)$ se tiene una relación de orden dada por,

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

Si $D_1 \leq D_2$ y $D_1 \neq D_2$, se escribe $D_1 < D_2$.

f) Un divisor $D \geq 0$ es llamado *positivo* (o *efectivo*).

Si D es un divisor de F/K, se define el *grado* de D como,

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

y *el espacio de Riemann-Roch* de D como,

$$\mathscr{L}(D) := \{x \in F : v_P(x) \geq -v_P(D) \text{ para todo } P \in \mathbb{P}_F\} \cup \{0\}.$$

Este es un espacio vectorial de dimensión finita sobre K y $\ell(D)$ denota su dimensión. El *género* de F/K se define por,

$$g := \text{máx}\{\deg D - \ell(D) + 1 : \ D \text{ es un divisor de } F/K\},$$

y se demuestra que es un entero no negativo.
Uno de los teoremas importantes de la teoría de cuerpos de funciones es el Teorema de Riemann-Roch, el cual permite calcular la dimensión de un divisor A.

Teorema 1.34. *Sea W un divisor canónico de F/K, entonces para cada divisor $A \in \mathrm{Div}(F)$,*

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

Puede verificarse que cada elemento distinto de cero $x \in F$ tiene un número finito de ceros y polos en $\mathbb{P}_F$. Si x es un elemento no nulo de F y se denota por M (resp. N) el

conjunto de ceros (resp. polos) de x en $\mathbb{P}_F$, entonces se define,

$$\begin{aligned}(x)_0 &:= \sum_{P\in M} v_P(x)P, \text{ el } \textit{divisor cero} \text{ de } x,\\ (x)_\infty &:= -\sum_{P\in N} v_P(x)P, \text{ el } \textit{divisor polo} \text{ de } x,\\ (x) &:= (x)_0 - (x)_\infty, \text{ el } \textit{divisor principal} \text{ de } x.\end{aligned}$$

Claramente $(x)_0 \geq 0$, $(x)_\infty \geq 0$ y

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

.

El ejemplo más sencillo de un cuerpo de funciones es el *cuerpo de funciones racionales* $K(x)/K$ donde x es un elemento trascendente sobre K. Este cuerpo tiene género $g = 0$ y una descripción muy particular de sus lugares. A continuación se estudia su estructura interna.

Definición 1.35. Sea K un cuerpo y x un elemento trascendente sobre K. Denote 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,

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

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

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \nmid g(x) \right\}, \tag{1.1}$$

es un anillo de valuación de $K(x)$ cuyo conjunto de unidades está dado por,

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

en consecuencia,

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

es el correspondiente lugar de $\mathcal{O}_{p(x)}$. En el caso particular cuando $p(x)$ es lineal, es decir, $p(x) = x - \alpha$ con $\alpha \in K$, se escribe $P_\alpha := P_{x-\alpha}$.

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

En $K(x)/K$ defina ahora,

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} : \deg f(x) \leq \deg g(x) \right\}. \tag{1.3}$$

Entonces $\mathcal{O}_\infty$ es un anillo de valuación de $K(x)$ que tiene como ideal maximal,

$$P_\infty = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], \deg f < \deg g(x) \right\}. \tag{1.4}$$

A este conjunto se le llama el *lugar infinito de* $K(x)/K$, y observe que la etiqueta de "∞"depende del elemento generador de la extensión $K(x)/K$; por ejemplo P_0 es el lugar infinito de $K(x^{-1})$.

Algunas propiedades que tiene el cuerpo de funciones racionales $K(x)/K$ se muestran a continuación.

Proposición 1.36. *Sea* $F = K(x)$ *el cuerpo de funciones racionales.*

(a) Si $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ *es el lugar definido por* (1,2) *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 en la forma*

$$z = p(x)^n \cdot \left(\frac{f(x)}{g(x)} \right)$$

con $f(x), g(x) \in K[x]$*,* $p(x) \nmid f(x)$ *y* $p(x) \nmid g(x)$*, entonces* $v_P(z) := n$*. Si* $z = 0$*, se define* $v_P(z) := \infty$*. Además, el cuerpo de clases residuales* $K(x)_P = \mathcal{O}_P/P$ *es*

isomorfo a $K[x]/\langle p(x)\rangle$, *consecuentemente,* $\deg P = \deg(p(x))$.

(b) *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 $z = \dfrac{f(x)}{g(x)}$ *con* $f(x)$, $g(x)$ *elementos de* $K[x]$ *primos relativos, entonces*

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

(c) *Sea* P_∞ *el lugar infinito de* $K(x)/K$ *definido por* (1,4), *entonces* $\deg P_\infty = 1$ *y un elemento primo de* P_∞ *es* $t = \dfrac{1}{x}$.

La correspondiente valuación discreta v_∞ *está dada por,*

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

donde $f(x), g(x) \in K[x]$ *y 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

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

si

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

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

Se termina la presentación de resultados del cuerpo de funciones racionales con una descripción de sus lugares.

Teorema 1.37. *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 $P = P_\infty$.*

Ahora se presentan algunos hechos relacionados con elementos de un cuerpo de funciones que tienen un único polo.

Sea $P \in \mathbb{P}_F$. Un entero $n \geq 0$ se llama un *número polo* de P, si existe un elemento $x \in F$ con $(x)_\infty = nP$. De lo contrario n se llama un *número gap* de P.

El conjunto de números polos asociados a un lugar P de un cuerpo de funciones F/K tiene una estructura de semigrupo numérico. Este hecho da paso a la siguiente definición, la cual estará presente a lo largo de este trabajo.

Definición 1.38. Dado F/K un cuerpo de funciones y P un lugar racional de F, se define el *semigrupo de Weierstrass* asociado a P por,

$$H(P) := \{s \in \mathbb{N} : (z)_\infty = sP \text{ para algún } z \in F\}.$$

Para denotar este conjunto simplemente se escribirá H cuando no haya confusión alguna.

Suponga que $P \in \mathbb{P}_F$. Como $(x)_\infty = 0$ para todo $x \in K - \{0\}$, de manera trivial $n = 0$ es un número polo de P. Asímismo, para $n \in \mathbb{N}$ es claro que $\ell((n-1)P) \leq \ell(nP)$ para

todo $P \in \mathbb{P}_F$, de modo que si $\ell(nP) \neq \ell((n-1)P)$, entonces, $\ell((n-1)P) < \ell(nP)$, es decir,

$$\ell((n-1)P) + 1 \leq \ell(nP). \tag{1.5}$$

Por otra parte, si P es un lugar racional, entonces

$$\ell(nP) \leq \ell((n-1)P) + 1, \tag{1.6}$$

y por lo tanto, combinando (1.5) y (1.6) se obtiene $\ell(nP) = \ell((n-1)P)+1$. En definitiva, si P es un lugar racional de F/K y $\ell((n-1)P) < \ell(nP)$, entonces $\ell((n-1)P) + 1 = \ell(nP)$.

El próximo resultado establece que el complemento de $H(P)$ en $\mathbb{N}$ es finito. El conjunto anterior se denota por $G(P)$ y se llama el ***conjunto de gaps de*** P.

Teorema 1.39. *Sea $P \in \mathbb{P}_F$, para cada $n \geq 2g$ existe un elemento $x \in F$ tal que $(x)_\infty = nP$; en consecuencia, si n es un gap de P, entonces $n \in \{1, 2, 3, \cdots, 2g-1\}$.*

Demostración. Si $n = 0$ se tiene $(x)_\infty = 0P$ para todo $x \in K - \{0\}$. Si $n \geq 1$, por el Teorema 1.34 se sigue que $\ell((n-1)P) = (n-1)\deg P + 1 - g$ y $\ell(nP) = n \deg P + 1 - g$, luego se tiene la inclusión propia $\mathscr{L}((n-1)P) \subsetneq \mathscr{L}(nP)$. Lo anterior significa que existe $x \in \mathscr{L}(nP) - \mathscr{L}((n-1)P)$; en ese sentido se afirma que cada elemento $x \in \mathscr{L}(nP) - \mathscr{L}((n-1)P)$ tiene divisor polo nP. En efecto, el hecho de que $x \in \mathscr{L}(nP) - \mathscr{L}((n-1)P)$ implica que,

$$(x) \geq -nP, \tag{1.7}$$

y que existe un lugar Q de F con $v_Q(x) \leq -n$. Observe que si $Q = P$, entonces $v_Q(x) \geq -n$ y en consecuencia, $v_Q(x) = -n$. Por otra parte, empleando (1.7) se tiene que $v_P(x) \geq -n$ y $v_Q(x) \geq 0$ para todo $Q \neq P$, lo cual muestra que si $Q \neq P$, entonces Q no es un polo de x obteniéndose así que $(x)_\infty = nP$. □

En los términos del teorema anterior puede decirse que para P un lugar racional, si $\ell(nP) = \ell((n-1)P) + 1$, entonces $n \in \mathbb{N}$ es un número polo de P; esto equivale a decir que para P un lugar racional, si n es un gap de P, entonces $\ell((n-1)P) = \ell(nP)$.

Teniendo en cuenta lo anterior, se caracterizan a continuación los gaps asociados a un lugar racional P de un cuerpo de funciones F/K.

Proposición 1.40. *Sea $P \in \mathbb{P}_F$ un lugar racional. Entonces n es un gap de P si y solo si $\ell(nP) = \ell((n-1)P)$.*

Demostración. Es suficiente con demostrar que si n es un número polo de P, entonces $\ell(nP) > \ell((n-1)P)$. En efecto, sea n un número polo de P, por definición existe $x \in F$ tal que $(x)_\infty = nP$, de ahi que $(x) = (x)_0 - nP \geq -nP$, lo anterior indica que $x \in \mathscr{L}(nP)$. De otro lado, suponga que $\ell(nP) = \ell((n-1)P)$, entonces se tiene $\mathscr{L}(nP) = \mathscr{L}((n-1)P)$, y por consiguiente $x \in \mathscr{L}((n-1)P)$, esto significa que $(x)_0 \geq P$, lo cual es una contradicción puesto que P es un polo de x. □

Ahora se presenta el Teorema de los gaps de Weierstrass.

Teorema 1.41. *Suponga que F/K tiene género $g > 0$ y sea P un lugar racional. Entonces existe exactamente g números gaps $i_1 < \cdots < i_g$ de P. Más aún; $i_1 = 1$ y $i_g \leq 2g - 1$.*

La siguiente observación nos muestra una de las aplicaciones de los semigrupos numéricos en lo que respecta a cuerpos de funciones algebraicas.

Observación 1.42. Dado n un entero positivo y P un lugar racional de F, se puede escribir

$$\{0, 1, 2, \cdots, n\} = \{x \in H(P) : x \leq n\} \cup \{x \in G(P) : x \leq n\}.$$

Entonces $\ell(nP) = s$, donde $s := |\{x \in H(P) : x \leq n\}|$. De igual modo, los semigrupos numéricos proporcionan información para la busqueda de bases del espacio de Riemman-Roch $\mathscr{L}(nP)$. Más concretamente:

1. Si $n \in H$, considére elementos z_j tales que $(z_j)_\infty^F = n_j P$ con $n_j \leq n$.

   El conjunto $B := \{z_1, z_2, \cdots, z_s\}$ es una base para el espacio de Riemann-Roch $\mathscr{L}(nP)$.

   En efecto, como

   $$(z_j)^F \geq -(z_j)_\infty^F = -n_j P \geq -nP,$$

se sigue que $z_j \in \mathscr{L}(nP)$ para todo $j \in \{1, 2, \cdots, s\}$. También se tiene que B es linealmente independiente sobre K, puesto que si B es linealmente dependiente, existen $\lambda_1, \cdots, \lambda_s \in K$ no todos ceros tales que

$$\lambda_1 z_1 + \cdots + \lambda_s z_s = 0. \tag{1.8}$$

Como los elementos $n_j \in H(P)$ se encuentra que las valuaciones $v_P(z_j) = -n_j$ son distintas para cada valor de j, luego aplicando la desigualdad triangular estricta a (1.8) se obtiene $n_t = \infty$ para algún $t \in \{1, 2, \cdots, s\}$; una contradicción. Por lo tanto, B es linealmente independiente sobre K. Finalmente dado que $\ell(nP) = |B|$ concluimos lo deseado.

2. Si n *es un número gap de* P. Un razonamiento análogo al anterior muestra que considerando elementos z_j tales que $(z_j)_\infty^F = n_j P$ con $n_j \leq n$; el conjunto $B := \{z_1, z_2, \cdots, z_s\}$ constituye una base para el espacio de Riemann-Roch $\mathscr{L}(nP)$.

Note que si $z_{j_1} = z_{j_2}$ para ciertos $j_1, j_2 \in \{1, 2, \cdots, s\}$, entonces $(z_{j_1})_\infty^F = (z_{j_2})_\infty^F$, es decir, $n_{j_1} Q_{\infty_i} = n_{j_2} Q_{\infty_i}$, luego se tiene $n_{j_1} = n_{j_2}$, en consecuencia $z_{j_1} \neq z_{j_2}$, siempre que $n_{j_1} \neq n_{j_2}$.

1.3 Extensiones de Cuerpos de Funciones

En adelante suponga que F'/K' (resp. F/K) es un cuerpo de funciones y que K' (resp. K) es su cuerpo completo de constantes.

Un cuerpo de funciones F'/K' se dice una *extensión algebraica* (resp. *extensión finita*) de un cuerpo de funciones F/K, si F'/F y K'/K son extensiones algebraicas (resp. extensiones finitas) de cuerpos.

Ahora se mencionan algunas definiciones y propiedades importantes de los lugares en una extensión algebraica de cuerpos de funciones F'/K' de F/K.

Sean $P \in \mathbb{P}_F$ y $Q \in \mathbb{P}_{F'}$. Si $P \subseteq Q$ se dice que P *está debajo de* Q o que Q *divide a* P y a este hecho se le denota por $Q|P$; en este caso se demuestra que existe un entero

positivo $e \geq 1$ tal que para todo $x \in F$ se cumple que,

$$v_Q(x) = e \cdot v_P(x).$$

El entero positivo e se conoce como el *índice de ramificación* de Q sobre P y se denota por $e(Q|P)$. También se prueba que para cada lugar $Q \in \mathbb{P}_{F'}$ existe un único lugar $P \in \mathbb{P}_F$ tal que $Q|P$, concretamente $P = Q \cap F$, y de manera recíproca que para cada lugar P de F existe al menos uno y a lo más un número finito de lugares en F' que extienden a P.

Un lugar $P \in \mathbb{P}_F$ *ramifica* en F'/F, si existe un lugar Q de F' que extiende a P tal que $e(Q|P) > 1$. En caso contrario se dice que P *no ramifica* en F'/F.

Si P está debajo de Q se prueba que la clase residual F'_Q es una extensión de cuerpo de la clase residual F_P vía la inmersión,

$$f : \begin{cases} F_P & \longrightarrow F'_Q \\ x(P) & \longmapsto x(Q). \end{cases}$$

El grado de F'_Q/F_P el cual puede ser infinito se denota por $f(Q|P)$ y es llamado el *grado relativo* de Q sobre P. Se prueba que $f(Q|P)$ es finito si y solo si F'/F es una extensión de cuerpo finita.

El siguiente resultado muestra que el índice de ramificación y el grado relativo están estrechamente relacionados.

Teorema 1.43. *Sean F'/K' una extensión finita de F/K, P un lugar de F/K y $P_1, \cdots, P_m$ todos los lugares de F'/K' que extienden a P, entonces,*

$$\sum_{i=1}^{m} e(P_i|P) f(P_i|P) = [F' : F].$$

Sean F'/K' una extensión de F/K de grado $[F' : F] = n$ y $P \in \mathbb{P}_F$. Se dice que el lugar P es *totalmente ramificado* en F'/F si existe un lugar Q que extiende a P con $e(Q|P) = n$. El Teorema 1.43 implica que Q es el único lugar que extiende a P y que

$f(Q|P) = 1$. También se dice que P se *descompone completamente* en F'/F si existen exactamente $[F' : F]$ lugares distintos en F' que extienden a P. Empleando nuevamente EL Teorema 1.43 se tiene que P se descompone completamente en F'/F si y sólo si $e(Q|P) = f(Q|P) = 1$ para todo lugar Q de F' que extiende a P.
Existe una relación entre el grado de los lugares y el grado relativo en una extensión de cuerpos de funciones finita. Más exactamente; dados $Q \in \mathbb{P}_{F'}$ y $P \in \mathbb{P}_F$ con P debajo de Q, se muestra fácilmente que,

$$\deg Q = \frac{f(Q|P) \deg P}{[K' : K]}.$$

En el caso particular cuando $K' = K$ entonces Q es racional si y sólo si P es racional y $f(Q|P) = 1$.
Para un lugar $P \in \mathbb{P}_F$, se define su *conorma* (respecto a F'/F) como el divisor

$$\mathrm{Con}_{F'/F}(P) := \sum_{P'|P} e(P'|P) \cdot P' \in \mathbb{P}_{F'},$$

donde la suma está definida sobre todos los lugares $P' \in \mathbb{P}_{F'}$ que están sobre P. La aplicación de la conorma puede extenderse a un homomorfismo de $\mathrm{Div}(F)$ a $\mathrm{Div}(F')$ de la siguiente manera:

$$\mathrm{Con}_{F'/F}\left(\sum_{P \in \mathbb{P}_F} n_P \cdot P\right) := \sum_{P \in \mathbb{P}_F} n_P \cdot \mathrm{Con}_{F'/F}(P).$$

Observe que la conorma envía divisores principales de F a divisores principales de F'. Más exactamente.

Proposición 1.44. *Sea F'/K' una extensión algebraica de F/K. Para un elemento x de F no nulo, denote por $(x)_0^F, (x)_\infty^F, (x)_\infty^F$, (resp. $(x)_0^{F'}, (x)_\infty^{F'}, (x)_\infty^{F'}$) el divisor cero, el divisor polo y divisor principal de x en* $\mathrm{Div}(F)$ *(resp. de x en* $\mathrm{Div}(F')$*). Entonces*

$$\mathrm{Con}_{F'/F}\left((x)_0^F\right) = (x)_0^{F'}, \mathrm{Con}_{F'/F}\left((x)_\infty^F\right) = (x)_\infty^{F'} \text{ y } \mathrm{Con}_{F'/F}\left((x)^F\right) = (x)^{F'}.$$

A continuación se describe un método que a menudo se usa para determinar todos los

lugares de F' que están sobre el lugar $P \in \mathbb{P}_F$, por conveniencia se introduce la siguiente notación.

- $\overline{F} = F_P = \mathcal{O}_P/P$ el cuerpo de clases residuales de P,
- $\overline{a} = a(P) \in \overline{F}$ es la clase residual de $a \in \mathcal{O}_P$,
- Si $\varphi(T) = \sum c_i T^i$ es un polinomio con $c_i \in \mathcal{O}_P$, se define $\overline{\varphi}(T) = \sum \overline{c}_i T^i \in \overline{F}[T]$.

Cada polinomio $\gamma(T) \in \overline{F}[T]$ se corresponde con un polinomio cuyos coeficientes están en $\mathcal{O}_P$. Para ver esto, escriba

$$\gamma(T) := \overline{a_0} + \overline{a_1}T + \cdots + \overline{a_n}T^n$$

con $\overline{a_i} \in \overline{F}$. Considerando los elementos $a_0, a_1, \cdots, a_n \in \mathcal{O}_P$; el polinomio

$$\varphi(T) = a_0 + a_1 T + \cdots + a_n T^n$$

determina tal polinomio, además note que $\deg(\gamma(T)) = \deg(\varphi(T))$.
Con esto en mente enunciamos el Teorema de Kummer.

Teorema 1.45. *Suponga que $F' = F(y)$ donde y es entero sobre $\mathcal{O}_P$ y considere el polinomio minimal de y sobre F, $\varphi(T) \in \mathcal{O}_P[T]$, sea,*

$$\overline{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\epsilon_i},$$

la descomposición de $\overline{\varphi}(T)$ en factores irreducibles sobre $\overline{F}$, es decir, los polinomios $\gamma_1(T), \cdots, \gamma_r(T)$ son polinomios mónicos e irreducibles, diferentes dos a dos en $\overline{F}$ y $\epsilon_i \geq 1$. Escoja polinomios mónicos $\varphi_i(T) \in \mathcal{O}_P[T]$ con $\overline{\varphi_i}(T) = \gamma_i(T)$ y $\deg(\varphi_i(T)) = \deg(\gamma_i(T))$, entonces para $i = 1, 2, \cdots, r$ existen lugares $P_i \in \mathbb{P}_{F'}$ tales que,

$$P_i|P,\ \varphi_i(y) \in P_i \ y\ f(P_i|P) \geq \deg(\gamma_i(T)),$$

además $P_i \neq P_j$ para $i \neq j$.

En el caso en que $\epsilon_i = 1$ para $i = 1, 2, \cdots, r$, existe, para $1 \leq i \leq r$ exactamente un lugar $P_i \in \mathbb{P}_{F'}$ con $P_i|P$ y $\varphi_i(y) \in P_i$.
Los lugares $P_1, \cdots, P_r$, son todos los lugares de F' que extienden a P, y

$$\mathrm{Con}_{F'/F}(P) = \sum_{i=1}^{r} \epsilon_i P_i = \sum_{i=1}^{r} e(P_i|P) P_i.$$

Por lo tanto $\epsilon_i = e(P_i|P)$. Más aún el cuerpo de clases residuales $F'_{P_i} = \mathcal{O}_{P_i}/P_i$ es isomorfo a $\overline{F}[T]/\langle \gamma_i(T) \rangle$ y en consecuencia $f(P_i|P) = \deg(\gamma_i(T)))$.

Ahora presentamos los resultados más relevantes de extensiones de tipo Kummer en cuerpos de funciones.
Sea F/K un cuerpo de funciones donde K contiene una $n-$ésima raíz de la unidad (con $n > 1$ y primo relativo con $\mathrm{Char}(K)$), suponga que $u \in F$ tal que,

$$u \neq w^d \text{ para todo } w \in F \text{ y } d \mid n, d > 1. \tag{1.9}$$

Sea

$$F' = F(y) \text{ con } y^n = u, \tag{1.10}$$

entonces F'/F es llamado una *extensión de Kummer de F.*

Proposición 1.46. *Sea F'/F una extensión de Kummer como la descrita anteriormente, entonces,*

a) El polinomio $\Phi(T) = T^n - u$ es el polinomio minimal de y sobre F (en particular este es irreducible sobre F), y la extensión F'/F tiene grado $[F' : F] = n$.

b) Sea $P \in \mathbb{P}_F$ y $P' \in \mathbb{P}_{F'}$ un lugar sobre P, entonces,

$$e(P'|P) = \frac{n}{r_P},$$

donde,

$$r_P := \gcd(n, v_P(u)) > 0, \tag{1.11}$$

es el máximo común divisor de n y $v_P(u)$.

c) Si K' denota el cuerpo de constantes de F' y g (resp. g') el género de F/K (resp. F'/K'), entonces,

$$g' = 1 + \frac{n}{[K' : K]} \left(g - 1 + \frac{1}{2} \sum_{P \in \mathbb{P}_F} \left(1 - \frac{r_P}{n}\right) \deg P \right),$$

donde r_P es definido por (1,11).

Del resultado anterior se sigue el siguiente corolario.

Corolario 1.47. *Sea F/K un cuerpo de funciones y $F' = F(y)$ con $y^n = u \in F$, donde* $\mathrm{Char}(K)$ *no divide a n y K contiene una $n-$ésima raíz primitiva de la unidad. Suponga que existe un lugar $Q \in \mathbb{P}_F$ tal que* $\gcd(n, v_Q(u)) = 1$. *Entonces K es el cuerpo completo de constantes de F'.*

Las extensiones de Kummer tienen las siguientes propiedades:

Proposición 1.48. *Sea F'/K' una extensión de Kummer de F/K. Suponga que $P_1, P_2, \cdots, P_r$ son todos los lugares de F' que están sobre $P \in \mathbb{P}_F$, entonces,*

a) $e(P_i|P) = e(P_j|P)$ y $f(P_i|P) = f(P_j|P)$ para todo i, j. Por lo tanto $e(P) := e(P_i|P)$ y $f(P) := f(P_i|P)$ son llamados el índice de ramificación de P en F'/F y el grado relativo de P en F'/F respectivamente.

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

1.4 Códigos algebraicos-geométricos

Terminamos los preliminares con algunas definiciones y resultados asociados a la teoría de códigos algebraicos geométricos.

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 llama *palabras.*

Sean $a = (a_1, \ldots, a_n)$ y $b = (b_1, \ldots, b_n)$ elementos de A^n, se define la *distancia de Hamming* entre las palabras a y b por,

$$d(a, b) := |\{i : a_i \neq b_i\}|, \tag{1.12}$$

esto es, $d(a, b)$ es el número de componentes en los cuales a y b difieren.
Se puede verificar que la distancia de Hamming es una métrica en A^n. Un parámetro fundamental de un código $\mathcal{C}$ es la *distancia mínima* entre sus palabras. Este parámetro viene dado por,

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

La distancia mínima da una medida de lo bueno que es un código en relación con la detección y corrección de errores.
También se define el *peso* w de un elemento $a \in A^n$ 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.
Se considera un caso especial cuando $A = \mathbb{F}_q$, el cuerpo finito con Q elementos y $\mathcal{C}$ es un subespacio vectorial de $\mathbb{F}_q^n$ sobre $\mathbb{F}_q$. En este caso se dice que $\mathcal{C}$ es un *código lineal* y tenemos un parámetro adicional, a saber, su dimensión como subespacio vectorial de $\mathbb{F}_q^n$. Denote esto por $k := \dim_{\mathbb{F}_q} \mathcal{C}$. Este nuevo parámetro mide la capacidad de transmisión de información del código. En lo que sigue solo se consideran códigos lineales.
Cuando $\mathcal{C}$ es un subespacio vectorial se puede probar que la distancia mínima es igual al mínimo de los pesos de los elementos no nulos de $\mathcal{C}$, es decir,

$$d = d(\mathcal{C}) = \text{mín}\{w(c) : c \neq 0 \text{ y } c \in \mathcal{C}\}.$$

Se dice 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,bajo esta noción, se busca tener $[n, k, d]$ códigos con dimensión y distancia mínima lo más grandes posible. Una manera simple de describir un código lineal $\mathcal{C}$ explícitamente, es conociendo una base de $\mathcal{C}$ (como espacio vectorial sobre $\mathbb{F}_q$).

Definición 1.49. 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 $\mathcal{C}$.

En general, los parámetros de un código lineal están relacionados de la siguiente manera:

Proposición 1.50. *Sea $\mathcal{C}$ un $[n,k,d]$ código. Entonces $k+d \leq n+1$.*

La desigualdad anterior se le conoce como la *cota de Sigleton.*
Los códigos que se construyen a partir de cuerpos de funciones algebraicas fueron introducidos por primera vez por V. D. Goppa en 1981. A estos códigos les llamamos **códigos AG**. Llegando a este punto se presenta la siguiente notación:

- $F/\mathbb{F}_q$ es un cuerpo de funciones algebraicas de género g.
- $P_1, P_2, \ldots, P_n$ 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 ningún P_i con $i = 1, 2, \ldots, n$ aparece en la expansión del divisor G.

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

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

Considere la aplicación evaluación $e_{vD} : \mathscr{L}(G) \longrightarrow \mathbb{F}_q^n$, dada por,

$$e_{vD}(x) := (x(P_1), x(P_2), \ldots, x(P_n)) \in \mathbb{F}_q^n, \tag{1.13}$$

se tiene que, e_{vD} es $\mathbb{F}_q$- lineal y $\mathcal{C}_{\mathscr{L}}(D,G) = e_{vD}(\mathscr{L}(G))$.
El siguiente teorema permite calcular (o por lo menos estimar) los parámetros n, k y d del código $\mathcal{C}_{\mathscr{L}}(D,G)$ haciendo uso del Teorema 1.34.

Teorema 1.51. *$\mathcal{C}_{\mathscr{L}}(D,G)$ es un $[n,k,d]$ código con parámetros,*

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

Más aún, si $\deg G < n$, *la aplicación evaluación $e_{vD} : \mathscr{L}(G) \longrightarrow \mathcal{C}_{\mathscr{L}}(D,G)$ es inyectiva y se tiene,*

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

$$d \geq n - \deg G \quad y \quad k = \ell(G) \geq \deg G + 1 - g. \tag{1.14}$$

En consecuencia,

$$k + d \geq n + 1 - g. \tag{1.15}$$

(b) Si además, $2g - 2 < \deg G$ *entonces* $k = \deg G + 1 - g$.

(c) Si $\{x_1, x_2, \ldots, x_k\}$ *es una base de* $\mathscr{L}(G)$ *sobre* $\mathbb{F}_q$*, entonces la matriz,*

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

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

Observe que la cota inferior (1.15) para la distancia mínima, es muy similar a la cota de sigleton. Al combinar ambas cotas se deduce que para $\deg G < n$,

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

En virtud del Teorema 1.51, por lo general se supone que $\deg G < n$ para obtener una cota significativa para la distancia mínima del código $\mathcal{C}_{\mathscr{L}}(D,G)$.

En particular cuando G es un múltiplo de un lugar racional Q de $F/\mathbb{F}_q$ y D es el divisor formado por la suma de lugares racionales distintos a Q, se llama a $C_{\mathscr{L}}(D,G)$ un código AG *unipuntual*.

Capítulo **2**

Semigrupos de Weierstrass en extensiones de Kummer con un lugar en el infinito

En este capítulo se expone con detalle el artículo [2] en el cual se describe explícitamente el semigrupo de Weierstrass $H(Q_\infty)$ correspondiente al único lugar que extiende a P_∞ en una extensión de Kummer $y^n = f(x)$ donde $f(x) \in K(x)$ y $\gcd(n, \deg(f(x))) = 1$. Sea K la clausura algebraica del cuerpo finito $\mathbb{F}_q$ con q elementos. Considére el cuerpo de funciones $F/K(x)$ de tipo Kummer dado por la ecuación,

$$y^m = \prod_{i=1}^{r}(x - \alpha_i)^{\lambda_i}, \tag{2.1}$$

donde $\alpha_1, \cdots, \alpha_r \in K$ son elementos distintos dos a dos, $\lambda_i \in \mathbb{N}$, $1 \leq \lambda_i < m$, $m \geq 2$ y $r \geq 2$ son enteros positivos, $\lambda_0 := \sum_{i=1}^{r}\lambda_i$, $\gcd(m, q) = 1$, y $\gcd(m, \lambda_0) = 1$.
Para probar el resultado principal de este capítulo se necesita los siguientes dos lemas.

Lema 2.1. *Para m, λ enteros positivos se cumple que*

$$\sum_{i=0}^{\lambda-1}\left\lfloor \frac{im}{\lambda} \right\rfloor = \frac{(m-1)(\lambda-1) + \gcd(m, \lambda) - 1}{2}. \tag{2.2}$$

Demostración. Defina $S(m,\lambda) := \sum_{i=0}^{\lambda-1}\left\lfloor \frac{im}{\lambda}\right\rfloor$, para $i = 0,1,2,\cdots,\lambda-1$, suponga que $mi = q_i\lambda + r_i$ con $0 \leq r_i < \lambda$, entonces $q_i = \left\lfloor \frac{im}{\lambda}\right\rfloor$ y $S(m,\lambda) = \sum_{i=0}^{\lambda-1} q_i$ de modo que,

$$m\sum_{i=0}^{\lambda-1} i = \lambda S(m,\lambda) + \sum_{i=0}^{\lambda-1} r_i. \tag{2.3}$$

Como $\sum_{i=0}^{\lambda-1} i = \frac{(\lambda-1)\lambda}{2}$, es suficiente calcular $\sum_{i=0}^{\lambda-1} r_i$, si escribe $c = \gcd(m,\lambda)$, entonces $m = cM$ y $\lambda = cN$ para ciertos M, N enteros positivos que además satisfacen $\gcd(M,N) = 1$, como $r_i \equiv 0 \mod (c)$ se tiene $r_i = cR_i$ con $0 \leq R_i < N$ y por consiguiente $Mi = q_iN + R_i$, es decir, $Mi \equiv R_i \mod (N)$, dado que $\gcd(M,N) = 1$ e $i \in \{0,1,\cdots,\lambda-1\}$ el cual es un conjunto completo de residuos módulo cN, puede decirse también que el conjunto $\{Mi : 0 \leq i \leq \lambda-1\}$ lo es y en consecuencia $\{R_i : 1 \leq i \leq \lambda-1\}$. Ahora teniendo en cuenta que $0 \leq R_i \leq N-1$, y que $i \in \{0,1,2,\cdots,\lambda-1\}$ cubre un conjunto completo de residuos módulo N exactamente c veces, se tiene, $\sum_{i=0}^{\lambda-1} r_i = c\sum_{i=0}^{\lambda-1} R_i = c\left(c\sum_{j=0}^{N-1} j\right) = c^2\frac{(N-1)N}{2}$. Por lo tanto de (2.3) se obtiene,

$$m\frac{(\lambda-1)\lambda}{2} = \lambda\sum_{i=0}^{\lambda-1}\left\lfloor \frac{im}{\lambda}\right\rfloor + \frac{c^2(N-1)N}{2},$$

con lo cual,

$$\begin{aligned}
\sum_{i=0}^{\lambda-1}\left\lfloor \frac{im}{\lambda}\right\rfloor &= \frac{m(\lambda-1)\lambda - c^2(N-1)N}{2\lambda} = \frac{m(\lambda-1)\lambda - c^2N^2 + c^2N}{2\lambda} \\
&= \frac{m(\lambda-1)\lambda - (cN)^2 + c(cN)}{2\lambda} = \frac{m(\lambda-1)\lambda - \lambda^2 + c\lambda}{2\lambda} \\
&= \frac{m(\lambda-1)\lambda - (\lambda-c)\lambda}{2\lambda} = \frac{m(\lambda-1) - \lambda + c}{2} \\
&= \frac{m(\lambda-1) + c - (\lambda-1) - 1}{2} = \frac{(m-1)(\lambda-1) + c - 1}{2}.
\end{aligned}$$

□

Lema 2.2. *Sean* $r, m, \lambda_0, \lambda_1, \lambda_2, \cdots, \lambda_r$ *enteros positivos tales que* $\lambda_0 := \sum_{i=1}^{r} \lambda_i$ *y* $r < \lambda_0$. *Para* $k \in \{r, r+1, \cdots, \lambda_0 - 1\}$, *se define*

$$\eta_k := \text{máx} \left\{ \rho_{s_1, s_2, \cdots, s_r} : \sum_{i=1}^{r} s_i = k, 1 \leq s_i \leq \lambda_i \right\},$$

donde $\rho_{s_1, s_2, \cdots, s_r} := \text{mín} \left\{ \left\lfloor \frac{s_i m}{\lambda_i} \right\rfloor : 1 \leq i \leq r \right\}$,
entonces la sucesión $\{\eta_k\}_{k=r}^{\lambda_0 - 1}$ *es tal que* $\eta_r \leq \eta_{r+1} \leq \cdots \leq \eta_{\lambda_0 - 1,}$ *y sus elementos tienen la misma multiplicidad de los elementos del conjunto* $S := \left\{ \left\lfloor \frac{s_i m}{\lambda_i} \right\rfloor : 1 \leq s_i < \lambda_i, 1 \leq i \leq r \right\}$.
En particular,

$$\sum_{k=r}^{\lambda_0 - 1} \eta_k = \frac{(m-1)(\lambda_0 - r) - r + \sum_{i=1}^{r} \gcd(m, \lambda_i)}{2}.$$

Demostración. Si $\eta_k = \rho_{u_1, u_2, \cdots, u_r} = \left\lfloor \frac{u_j m}{\lambda_j} \right\rfloor$ para algún $j \in \{1, 2, \cdots, r\}$ con $\sum_{i=1}^{r} u_i = k$ y $1 \leq u_i \leq \lambda_i$ para todo $i = 1, 2, \cdots, r$, entonces $u_j < \lambda_j$.
En efecto, si $u_j = \lambda_j$, entonces $m = \left\lfloor \frac{u_j m}{\lambda_j} \right\rfloor \leq \left\lfloor \frac{u_i m}{\lambda_i} \right\rfloor \leq \frac{u_i m}{\lambda_i} \leq m$ para todo i. Por lo tanto, $\frac{u_i m}{\lambda_i} = m$ de donde se concluye $u_i = \lambda_i$ para todo i.
De acuerdo a lo anterior

$$k = \sum_{i=1}^{r} u_i = \sum_{i=1}^{r} \lambda_i = \lambda_0,$$

lo que contradice que $k \in \{r, \cdots, \lambda_0 - 1\}$.

De otro lado, note que para $r \leq k \leq \lambda_0 - 2$ se cumple,

$$\eta_k = \rho_{u_1, \cdots, u_j, \cdots, u_r} \leq \rho_{u_1, \cdots, u_j + 1, \cdots, u_r} \leq \eta_{k+1}.$$

Para ver esto, considére la $r-$upla $(u_1, \cdots, u_j + 1, \cdots, u_r)$. Si $\rho_{u_1, \cdots, u_j + 1, \cdots, u_r} = \left\lfloor \frac{u_t m}{\lambda_t} \right\rfloor$ con $t \in \{1, \cdots, r\} - \{j\}$, entonces $\rho_{u_1, \cdots, u_j, \cdots, u_r} \leq \rho_{u_1, \cdots, u_j + 1, \cdots, u_r}$. De igual manera, si $\rho_{u_1, \cdots, u_j + 1, \cdots, u_r} = \left\lfloor \frac{(u_j + 1)m}{\lambda_j} \right\rfloor$, el hecho $u_j < u_j + 1$ implica que $\left\lfloor \frac{u_j m}{\lambda_j} \right\rfloor \leq$

$\left\lfloor \frac{(u_j+1)m}{\lambda_j} \right\rfloor$, luego $\rho_{u_1,\cdots,u_j,\cdots,u_r} \leq \rho_{u_1,\cdots,u_j+1,\cdots,u_r}$. Ahora, puesto que $\sum_{i=1}^{r} u_i + 1 = k+1, 1 \leq u_t \leq \lambda_t$ para todo $t \in \{1,\cdots,r\} - \{j\}$, y como $1 \leq u_j + 1 \leq \lambda_j$, pues $u_j < \lambda_j$; se deduce que $\rho_{u_1,\cdots,u_j+1,\cdots,u_r} \leq \eta_{k+1}$. En consecuencia, $\eta_r \leq \eta_{r+1} \leq \cdots \leq \eta_{\lambda_0-1}$ es una sucesión no decreciente.

En lo que resta observe que $S = A$ donde $A := \{\eta_k : k = r,\cdots,\lambda_0 - 1\}$ y que la multiplicidad de los elementos de cada conjunto es la misma. Efectivamente, por definición de η_k se cumple la inclusión $A \subseteq S$. También observe que el cardinal del conjunto A es $|A| = (\lambda_0 - 1) - (r-1) = \lambda_0 - r$, y si escribimos $S = \bigcup_{i=1}^{r} \theta_i$ donde $\theta_i := \left\{ \left\lfloor \frac{s_i m}{\lambda_i} \right\rfloor : 1 \leq s_i < \lambda_i \right\}$ se sigue que $|S| = \sum_{i=1}^{r} |\theta_i| = \sum_{i=1}^{r} (\lambda_i - 1) = \lambda_0 - r$. Por lo tanto, $|A| = |S|$ contando multiplicidades. En este sentido, para probar que $A = S$ es suficiente mostrar que si el valor de η_k aparece $n \geq 1$ veces en A, entonces η_k aparece al menos $n-$veces en S. Lo anterior significa que existen diferentes elementos $j_1, j_2, \cdots, j_n \in \{1,\cdots,r\}$ y $s_{j_1},\cdots,s_{j_n}$ con,

$$1 \leq s_{j_i} \leq \lambda_{j_i} - 1 \text{ y } \eta_k = \left\lfloor \frac{s_{j_1} m}{\lambda_{j_1}} \right\rfloor = \cdots = \left\lfloor \frac{s_{j_n} m}{\lambda_{j_n}} \right\rfloor. \tag{2.4}$$

Para probar esto, suponga sin pérdida de generalidad que

$$\eta_{k-1} < \eta_k = \eta_{k+1} = \cdots = \eta_{k+(n-1)}$$

con $\eta_{k-1} = 0$ si $k = r$. Como $A \subseteq S$ existe $j_1 \in \{1,\cdots,r\}$ y $s_{j_1} \in \{1,\cdots,\lambda_{j_1} - 1\}$ tales que $\eta_k = \left\lfloor \frac{s j_1 m}{\lambda_{j_1}} \right\rfloor$.

Para cada $i \in \{1,\cdots,r\}$ defina,

$$\Gamma_i := \left\{ s \in \mathbb{N} : \eta_k \leq \left\lfloor \frac{sm}{\lambda_i} \right\rfloor \text{ y } 1 \leq s \leq \lambda_i \right\}.$$

A continuación se afirma que $\Gamma_i \neq \emptyset$ para todo i. En efecto, si supone que $i = j_1$, entonces $\eta_k = \left\lfloor \frac{s_{j_1} m}{\lambda_{j_1}} \right\rfloor$ y $1 \leq s_{j_1} < \lambda_{j_1}$, es decir, $s_{j_1} \in \Gamma_{j_1,}$. Por otro lado, si $i \neq j_1$,

entonces $\dfrac{s_{j_1}\lambda_i}{\lambda_{j_1}} \leq \lambda_i - 1$, luego $\left\lfloor \dfrac{s_{j_1}\lambda_i}{\lambda_{j_1}} \right\rfloor + 1 \leq \lambda_i$. Más aún, como

$$\frac{s_{j_1}\lambda_i}{\lambda_{j_1}} < \left\lfloor \frac{s_{j_1}\lambda_i}{\lambda_{j_1}} \right\rfloor + 1,$$

se sigue que

$$\left(\frac{s_{j_1}\lambda_i}{\lambda_{j_1}}\right)\frac{m}{\lambda_i} < \left(\left\lfloor \frac{s_{j_1}\lambda_i}{\lambda_{j_1}} \right\rfloor + 1\right)\frac{m}{\lambda_i},$$

y por consiguiente,

$$\left\lfloor \left(\frac{s_{j_1}\lambda_i}{\lambda_{j_1}}\right)\frac{m}{\lambda_i} \right\rfloor \leq \left\lfloor \left(\left\lfloor \frac{s_{j_1}\lambda_i}{\lambda_{j_1}} \right\rfloor + 1\right)\frac{m}{\lambda_i} \right\rfloor.$$

Así pues, en definitiva $\Gamma_i \neq \emptyset$ para todo i.

En virtud del principio del buen orden, Γ_i admite un elemento mínimo; sea $t_i := \min \Gamma_i$. Con la existencia de los elementos t_i, se da lugar a la existencia de los elementos j_i, y s_{j_i} que satisfacen (2.4).

Por definición de los conjuntos Γ_i se tiene,

- $t_{j_1} = s_{j_1}$, puesto que, $s_{j_1} \in \mathbb{N}$,

$$\eta_k = \left\lfloor \frac{s_{j_1}m}{\lambda_{j_1}} \right\rfloor = \min_{1\leq i\leq r}\left\{ \left\lfloor \frac{s_i m}{\lambda_i} \right\rfloor \right\}$$

  y $1 \leq s_{j_1} \leq \lambda_{j_1} - 1$.

- Como $t_i - 1 \notin \Gamma_i$ para todo i, entonces se satisface la desigualdad

$$\left\lfloor \frac{(t_i - 1)m}{\lambda_i} \right\rfloor < \eta_k. \tag{2.5}$$

- $\rho_{t_1,\cdots,t_r} = \min_{1\leq i\leq r}\left\{ \left\lfloor \dfrac{t_i m}{\lambda_i} \right\rfloor \right\} = \left\lfloor \dfrac{s_{j_1}m}{\lambda_{j_1}} \right\rfloor = \eta_k.$

Para ver lo último, consideremos el conjunto

$$\left\{ \left\lfloor \frac{t_1 m}{\lambda_1} \right\rfloor, \cdots, \left\lfloor \frac{t_{j_1} m}{\lambda_{j_1}} \right\rfloor, \cdots, \left\lfloor \frac{t_r m}{\lambda_r} \right\rfloor \right\}.$$

Si $\rho_{t_1,\cdots,t_r} = \left\lfloor \dfrac{t_{j_1}m}{\lambda_{j_1}} \right\rfloor$, entonces trivialmente $\rho_{t_1,\cdots,t_r} = \eta_k$. Ahora, si $\rho_{t_1,\cdots,t_r} = \left\lfloor \dfrac{t_s m}{\lambda_s} \right\rfloor$

con $s \in \{1, \cdots, r\} - \{j_1\}$ se tiene que $\rho_{t_1,\cdots,t_r} \leq \eta_k$, pero por definición del conjunto Γ_i también se cumple $\eta_k \leq \rho_{t_1,\cdots,t_r}$. Más aún, note que $k = \sum_{i=1}^{r} t_i$. En efecto, si ponemos $k' := \sum_{i=1}^{r} t_i$, entonces por definición $\eta_k \leq \eta_{k'}$ y como $\eta_{k-1} < \eta_k = \eta_{k+1} = \cdots = \eta_{k+(n-1)}$ se obtiene $k \leq k'$. Por otra parte, suponga que $(u_1, \cdots, u_r)$ es una $r-$upla tal que $\eta_k = \rho_{u_1,\cdots,u_r}, \sum_{i=1}^{r} u_i = k$ y $1 \leq u_i \leq \lambda_i$. Si existe $j \in \{1, \cdots, r\}$ tal que $u_j < t_j$, es decir, $u_j \leq t_j - 1$, se sigue que $\left\lfloor \frac{u_j m}{\lambda_j} \right\rfloor \leq \left\lfloor \frac{(t_j - 1)m}{\lambda_j} \right\rfloor$ y con esto

$$\eta_k = \rho_{u_1,\cdots,u_r} = \min_{1 \leq i \leq r} \left\{ \left\lfloor \frac{u_i m}{\lambda_i} \right\rfloor \right\} \leq \left\lfloor \frac{u_j m}{\lambda_j} \right\rfloor \leq \left\lfloor \frac{(t_j - 1)m}{\lambda_j} \right\rfloor < \eta_k$$

por (2.5), una contradicción. En consecuencia $t_i \leq u_i$ para todo $i = 1, \cdots, r$, y así $k' = \sum_{i=1}^{r} t_i \leq \sum_{i=1}^{r} u_i = k$. Con base a lo anterior se deduce que $k = k'$.

Por lo tanto, vamos a proceder a demostrar que existen distintos elementos $j_2, \cdots, j_n \in \{1, \cdots, r\} - \{j_1\}$ tales que

$$\eta_k = \left\lfloor \frac{t_{j_1} m}{\lambda_{j_1}} \right\rfloor = \left\lfloor \frac{t_{j_2} m}{\lambda_{j_2}} \right\rfloor = \cdots = \left\lfloor \frac{t_{j_n} m}{\lambda_{j_n}} \right\rfloor.$$

Dado que $t_i = \min \Gamma_i$ para cualquier i, en particular se tiene $\eta_k \leq \left\lfloor \frac{t_i m}{\lambda_i} \right\rfloor$, para todo i. Para probar la existencia de los elementos $j_2, \cdots, j_n$, en primer lugar suponga que $\eta_k < \left\lfloor \frac{t_j m}{\lambda_j} \right\rfloor$ para cada $j \in \{1, \cdots, r\} - \{j_1\}$; entonces $\eta_k < \rho_{t_1,\cdots,t_{j_1}+1,\cdots,t_r} \leq \eta_{k+1}$ ya que $\sum_{i=1}^{r} t_i + 1 = k + 1$, lo cual es una contradicción pues $\eta_k = \eta_{k+1}$.

De acuerdo al razonamiento previo existe $j_2 \in \{1, \cdots, r\} - \{j_1\}$ tal que $\eta_k = \left\lfloor \frac{t_{j_1} m}{\lambda_{j_1}} \right\rfloor = \left\lfloor \frac{t_{j_2} m}{\lambda_{j_2}} \right\rfloor$ y $t_{j_2} < \lambda_{j_2}$; en segundo lugar, argumentando de manera muy similar se tiene la existencia de un elemento $j_3 \in \{1, \cdots, r\} - \{j_1, j_2\}$ tal que

$$\eta_k = \left\lfloor \frac{t_{j_1} m}{\lambda_{j_1}} \right\rfloor = \left\lfloor \frac{t_{j_2} m}{\lambda_{j_2}} \right\rfloor = \left\lfloor \frac{t_{j_3} m}{\lambda_{j_3}} \right\rfloor$$

y $t_{j_3} < \lambda_{j_3}$; en efecto, si $\eta_k < \left\lfloor \frac{t_j m}{\lambda_j} \right\rfloor$ para todo $j \in \{1, \cdots, r\} - \{j_1, j_2\}$, se tiene $\eta_k < \rho_{t_1, \cdots, t_{j_1+1}, \cdots, t_{j_2+1}, \cdots, t_r} \leq \eta_{k+2}$, lo cual es una contradicción. Continuando con este proceso se obtienen distintos elementos $j_1, j_2, \cdots, j_n \in \{1, \cdots, r\}$ tales que

$$\eta_k = \left\lfloor \frac{t_{j_1} m}{\lambda_{j_1}} \right\rfloor = \cdots = \left\lfloor \frac{t_{j_n} m}{\lambda_{j_n}} \right\rfloor \text{ y } t_{j_i} < \lambda_{j_i} \text{ para cada } i = 1, \cdots, n.$$

Finalmente empleando el lema anterior,

$$\begin{aligned} \sum_{k=r}^{\lambda_0 - 1} \eta_k = \sum_{i=1}^{r} \sum_{s=1}^{\lambda_i - 1} \left\lfloor \frac{sm}{\lambda_i} \right\rfloor &= \sum_{i=1}^{r} \frac{(m-1)(\lambda_i - 1) - 1 + \gcd(m, \lambda_i)}{2} \\ &= \frac{(m-1)(\lambda_0 - r) - r + \sum_{i=1}^{r} \gcd(m, \lambda_i)}{2}. \end{aligned}$$

□

El teorema principal de este capítulo se presenta a continuación:

Teorema 2.3. *Sea $m \geq 2$ y $r \geq 2$ enteros positivos tales que p no divide a m, donde $p = \mathrm{Char}(\mathbb{F}_q)$. Sea $F/K(x)$ el cuerpo de funciones algebraicas dado por la ecuación de Kummer,*

$$y^m = \prod_{i=1}^{r} (x - \alpha_i)^{\lambda_i}, \tag{2.6}$$

donde $\lambda_i \in \mathbb{N}$, $1 \leq \lambda_i < m$, $\alpha_1, \cdots, \alpha_r \in K$ son elementos distintos dos a dos, $\lambda_0 := \sum_{i=1}^{r} \lambda_i$ y $\gcd(m, \lambda_0) = 1$, entonces el semigrupo de Weierstrass en el único lugar Q_∞ de F que extiende al lugar P_∞ de $K(x)$, está determinado por,

$$H(Q_\infty) = \langle m, \lambda_0 \rangle \cup \bigcup_{k=r}^{\lambda_0 - 1} B_k,$$

donde $B_k = \{mk - k'\lambda_0 : k' = 1, \cdots, \eta_k\}$ y η_k se define como en el Lema 2,2.
En particular,

$$H(Q_\infty) = \langle m, \lambda_0, mk - \lambda_0 \eta_k : k = r, \cdots, \lambda_0 - 1 \rangle. \tag{2.7}$$

Demostración. Se inicia calculando algunos divisores principales de F; sea $P_{\alpha_i} \in P_{K(x)}$

el lugar correspondiente a $\alpha_i \in K$. Para $k \in \{r, \cdots, \lambda_0 - 1\}$, sean $s_1, s_2, \cdots, s_r$ enteros positivos tales que $1 \leq s_i \leq \lambda_i$ y $\sum_{i=1}^{r} s_i = k$, entonces, de acuerdo a la Proposición 1.44 se tiene,

$$\begin{aligned}(x-\alpha_i)^F &= \mathrm{Con}_{F/K(x)}[(x-\alpha_i)_{K(x)}] = \mathrm{Con}_{F/K(x)}[P_{\alpha_i}] - \mathrm{Con}_{F/K(x)}[P_\infty] \\ &= \sum_{Q|P_{\alpha_i}} e(Q|P_{\alpha_i})Q - \sum_{Q|P_\infty} e(Q|P_\infty)Q.\end{aligned} \tag{2.8}$$

Dado que $F/K(x)$ es una extensión de tipo Kummer se tiene por la Proposición 1.46,

$$e(Q|P_{\alpha_i}) = \frac{m}{\gcd\left(m, v_{P_{\alpha_i}}\left(\prod_{i=1}^{r}(x-\alpha_i)^{\lambda_i}\right)\right)} = \frac{m}{\gcd(m,\lambda_i)},$$

donde $Q \in \mathbb{P}_F$ con $Q|P_{\alpha_i}$ y

$$e(Q|P_\infty) = \frac{m}{\gcd\left(m, v_{P_\infty}\left(\prod_{i=1}^{r}(x-\alpha_i)^{\lambda_i}\right)\right)} = \frac{m}{\gcd(m,-\lambda_0)} = m,$$

donde $Q \in \mathbb{P}_F$ con $Q|P_\infty$. Note que lo último establece que P_∞ es totalmente ramificado en F. Entonces reemplazando lo anterior en (2.8) se obtiene,

$$(x-\alpha_i)^F = \frac{m}{\gcd(m,\lambda_i)} \sum_{Q|P_{\alpha_i}} Q - mQ_\infty. \tag{2.9}$$

Por otro lado, de (2,6) se sigue,

$$\begin{aligned}m(y)^F &= \left(\prod_{i=1}^{r}(x-\alpha_i)^{\lambda_i}\right)^F = \sum_{i=1}^{r}\lambda_i(x-\alpha_i)^F = \lambda_1(x-\alpha_1)^F + \cdots + \lambda_r(x-\alpha_r)^F \\ &= \lambda_1\left(\frac{m}{\gcd(m,\lambda_1)}\sum_{Q|P_{\alpha_1}} Q - mQ_\infty\right) + \cdots + \lambda_r\left(\frac{m}{\gcd(m,\lambda_r)}\sum_{Q|P_{\alpha_r}} Q - mQ_\infty\right),\end{aligned}$$

por lo que,

$$(y)^F = \lambda_1 \left(\frac{1}{\gcd(m,\lambda_1)} \sum_{Q|P_{\alpha_1}} Q - Q_\infty \right) + \cdots + \lambda_r \left(\frac{1}{\gcd(m,\lambda_r)} \sum_{Q|P_{\alpha_r}} Q - Q_\infty \right).$$

Reorganizando las expresiones del lado derecho se deduce,

$$(y)^F = \sum_{i=1}^{r} \frac{\lambda_i}{\gcd(m,\lambda_i)} \sum_{Q|P_{\alpha_i}} Q - \lambda_0 Q_\infty.$$

Del mismo modo,

$$\left(\frac{\prod_{i=1}^{r}(x-\alpha_i)^{s_i}}{y^{\rho_{s_1,\cdots,s_r}}} \right)^F = \left(\prod_{i=1}^{r}(x-\alpha_i)^{s_i} \right)^F - (y^{\rho_{s_1,\cdots,s_r}})^F = \sum_{i=1}^{r} s_i (x-\alpha_i)^F - \rho_{s_1,\cdots,s_r}(y)^F$$

$$= \frac{s_1 m}{(m,\lambda_1)} \sum_{Q|P_{\alpha_1}} Q - s_1 m Q_\infty + \cdots + \frac{s_r m}{(m,\lambda_r)} \sum_{Q|P_{\alpha_r}} Q - s_r m Q_\infty$$
$$- \rho_{s_1,\cdots,s_r} \left(\frac{\lambda_1}{(m,\lambda_1)} \sum_{Q|P_{\alpha_1}} Q + \cdots + \frac{\lambda_r}{(m,\lambda_r)} \sum_{Q|P_{\alpha_r}} Q \right) + \rho_{s_1,\cdots,s_r} \lambda_0 Q_\infty.$$

Realizando las simplificaciones correspondientes se tiene,

$$\left(\frac{\prod_{i=1}^{r}(x-\alpha_i)^{s_i}}{y^{\rho_{s_1,\cdots,s_r}}} \right)^F = \sum_{i=1}^{r} \frac{s_i m - \lambda_i \rho_{s_1,\cdots,s_r}}{(m,\lambda_i)} \sum_{Q|P_{\alpha_i}} Q - (mk - \lambda_0 \rho_{s_1,\cdots,s_r}) Q_\infty.$$

Ahora, se comprueba que

$$\langle m, \lambda_0 \rangle \cup \bigcup_{k=r}^{\lambda_0 - 1} B_k = \langle m, \lambda_0, mk - \lambda_0 \eta_k : k = r, \cdots, \lambda_0 - 1 \rangle$$

donde $B_k = \{mk - \lambda_0 k' : k' = 1, \cdots, \eta_k\}$.

Suponga que $z \in \langle m, \lambda_0 \rangle \cup \bigcup_{k=r}^{\lambda_0 - 1} B_k$. Es claro que si $z \in \langle m, \lambda_0 \rangle$, entonces $z \in \langle m, \lambda_0, mk - \lambda_0 \eta_k : k = r \cdots, \lambda_0 - 1 \rangle$. Si $z \in \bigcup_{k=r}^{\lambda_0 - 1} B_k$, z admite una representación de la forma $z = mk - \lambda_0 k'$ con $k' = 1, \cdots, \eta_k$. Más aún, si escribe

$$z = mk - \lambda_0 \eta_k + \lambda_0 \eta_k - \lambda_0 k' = mk - \lambda_0 \eta_k + \lambda_0(\eta_k - k') + 0 \cdot m,$$

se nota que $z \in \langle m, \lambda_0, mk - \lambda_0 \eta_k : k = r, \cdots, \lambda_0 - 1 \rangle$. El argumento previo permite establecer la inclusión

$$\langle m, \lambda_0 \rangle \cup \bigcup_{k=r}^{\lambda_0 - 1} B_k \subseteq \langle m, \lambda_0, mk - \lambda_0 \eta_k : k = r, \cdots, \lambda_0 - 1 \rangle.$$

Para verificar la inclusión en el otro sentido, y por consiguiente la igualdad, es suficiente observar que $mk - \lambda_0 \eta_k \in B_k$. Note también que por definición de η_k se tiene que $\eta_k < \dfrac{s_i m}{\lambda_i}$ para todo i, de manera que $0 < mk - \lambda_0 \eta_k \in H(Q_\infty)$ para $r \leq k < \lambda_0$ y por lo tanto,

$$\langle m, \lambda_0 \rangle \cup \bigcup_{k=r}^{\lambda_0 - 1} B_k \subseteq H(Q_\infty). \tag{2.10}$$

Se verifica que estas uniones realmente son disjuntas; para $k \in \{r, \cdots, \lambda_0 - 1\}$ y $k' \in \{1, \cdots, \eta_k\}$, un elemento de B_k puede ser escrito como $mk - k'\lambda_0 = m\lambda_0 - (\lambda_0 - k)m - k'\lambda_0$, luego $B_k \cap \langle m, \lambda_0 \rangle = \emptyset$ en virtud de la Proposición 1.30. También $B_{k_1} \cap B_{k_2} = \emptyset$, siempre que $k_1 \neq k_2$; más específicamente argumentado por el contrarecíproco, suponga que

$$mk_1 - \lambda_0 k_1' = mk_2 - \lambda_0 k_2'$$

para $r \leq k_1, k_2 < \lambda_0$, $1 \leq k_1' \leq \eta_{k_1}$ y $1 \leq k_2' \leq \eta_{k_2}$. Entonces $m(k_1 - k_2) = \lambda_0(k_1' - k_2')$. Se debe demostrar que $k_1 = k_2$; en caso contrario, se sigue de la última igualdad que λ_0 divide a $m(k_1 - k_2)$, y como $\gcd(m, \lambda_0) = 1$, el Lema de Euclidés establece que λ_0 divide a $k_1 - k_2$. En ese sentido $\lambda_0 \leq k_1 - k_2 \leq \lambda_0 - 3$, lo cual es una contradicción, así $k_1 = k_2$.

Por último note que la igualdad en (2.10) se cumple.

En efecto, por la Proposición 1.46, si g' es el género del cuerpo de funciones $F/K(x)$, entonces,

$$\begin{aligned} g' &= 1+m\left[-1+\frac{1}{2}\left(\sum_{i=1}^{r}\left(1-\frac{(m,\lambda_i)}{m}\right)+\left(1-\frac{1}{m}\right)\right)\right] \\ &= 1+m\left[-1+\frac{1}{2}\left(r-\sum_{i=1}^{r}\frac{(m,\lambda_i)}{m}+\left(\frac{m-1}{m}\right)\right)\right] \\ &= 1-m+\frac{mr}{2}-\frac{1}{2}\sum_{i=1}^{r}(m,\lambda_i)+\frac{m-1}{2} = 1-m+\frac{m(r+1)-1-\sum_{i=1}^{r}(m,\lambda_i)}{2} \\ &= \frac{m(r-1)+1-\sum_{i=1}^{r}(m,\lambda_i)}{2} = \frac{(m-1)(r-1)+r-\sum_{i=1}^{r}(m,\lambda_i)}{2}. \end{aligned}$$

Ahora, según la Proposición 1.25,

$$g_{\langle m,\lambda_0\rangle} = \frac{(m-1)(\lambda_0-1)}{2},$$

y de acuerdo con el Lema 2.2,

$$\left|\bigcup_{k=r}^{\lambda_0-1}{}^{\cdot} B_k\right| = \sum_{k=r}^{\lambda_0-1}\eta_k = \frac{(m-1)(\lambda_0-r)-r+\sum_{i=1}^{r}(m,\lambda_i)}{2},$$

Asímismo, por (2,10) se tiene la inclusión,

$$\bigcup_{k=r}^{\lambda_0-1}{}^{\cdot} B_k \subseteq H(Q_\infty)-\langle m,\lambda_0\rangle, \tag{2.11}$$

y como

$$\left|\bigcup_{k=r}^{\lambda_0-1}{}^{\cdot} B_k\right| = g_{\langle m,\lambda_0\rangle}-g' = |H(Q_\infty)-\langle m,\lambda_0\rangle|,$$

lo expuesto en (2,11) resulta ser una igualdad. □

Ejemplo 2.4. Para la extensión de cuerpo de funciones $F/K(x)$ dado por la ecuación

de Kummer $y^5 = x(x-1)^2$ definida sobre $\mathbb{F}_q$ con q no divisible por 5, el sistema de generadores para el semigrupo $H(Q_\infty)$ es dado, por

$$H(Q_\infty) = \langle 3, 4, 5\rangle.$$

Más precisamente, siguiendo la notación del Teorema 2.3; se tiene los valores $r = 2$, $m = 5, \lambda_1 = 1, \lambda_2 = 2$, $\lambda_0 = 3$ y $\gcd(5,3) = 1$. Entonces

$$H(Q_\infty) = \langle 5, 3, 10 - 3\eta_2\rangle.$$

Resta solamente calcular η_2. En efecto, por definición de η_k para $k = 2$,

$$\begin{aligned} \eta_2 &= \text{máx}\{\rho_{s_1,s_2} : s_1 + s_2 = 2, 1 \leq s_1 \leq 1, 1 \leq s_2 \leq 2\} \\ &= \text{máx}\{\rho_{s_1,s_2} : s_1 + s_2 = 2, s_1 = 1, s_2 = 1\}, \end{aligned}$$

de manera que $\rho_{s_1,s_2} = \text{mín}\left\{\left\lfloor \frac{1\cdot 5}{1}\right\rfloor, \left\lfloor \frac{1\cdot 5}{2}\right\rfloor\right\} = 2.$

Ejemplo 2.5. Considére el cuerpo de funciones $F/K(x)$ dado por la ecuación de Kummer $y^{10} = x^2(x-3)^2(x-1)^3$ sobre $\mathbb{F}_7$. Continuando con la notación del Teorema 2.3 se tiene que para $m = 10, r = 3, p = 7, \lambda_1 = \lambda_2 = 2$, $\lambda_3 = 3$ y $\lambda_0 = 7$,

$$H(Q_\infty) = \langle 10, 7, 10k - \lambda\eta_k : k = 3, 4, 5, 6\rangle, \tag{2.12}$$

donde

$$\eta_3 = \text{máx}\{\rho_{1,1,1}\} = \rho_{1,1,1} = 3, \qquad \eta_4 = \text{máx}\{\rho_{2,1,1}, \rho_{1,1,2}, \rho_{1,2,1}\} = \rho_{1,1,2} = 5,$$

$$\eta_5 = \text{máx}\{\rho_{1,1,3}, \rho_{1,2,2}, \rho_{2,1,2}\} = 5, \qquad \eta_6 = \text{máx}\{\rho_{2,1,3}, \rho_{2,2,2}, \rho_{1,2,3}\} = \rho_{2,2,2} = 6.$$

En consecuencia,

$$H(Q_\infty) = \langle 5, 7, 9\rangle.$$

Capítulo **3**

Semigrupos de Weierstrass en extensiones de Kummer con más de un lugar en el infinito

Al momento de considerar extensiones de Kummer donde el lugar P_∞ no es totalmente ramificado, el problema de encontrar el semigrupo de Weierstrass asociado a un lugar de F que extiende a P_∞, es un interrogante abierto en la teoría de cuerpos de funciones en el que se conoce muy poca información al respecto. La dificultad radica en el hecho de que no hay una forma general de encontrar funciones generadoras que tengan polo de un orden específico, esto es debido a que ahora, el cálculo de estos semigrupos depende en gran medida de la ecuación que define a la extensión. En este capítulo del trabajo calculamos explicítamente el semigrupo de Weierstrass correspondiente a las extensiones de P_∞ de una familia particular de extensiones de Kummer. Cabe mencionar que la estrategia a utilizar se basa primero en encontrar un conjunto S cuyo conjunto generador $\langle S\rangle$ está contenido en H, para luego emplear la Proposición 1.23 la cual permitirá conocer el género de $\langle S\rangle$. Observe que para este proceso, se debe calcular el conjunto Apéry de $\langle S\rangle$, y como veremos éste hecho no es trivial.

3.1 Una extensión de Kummer con más de un lugar en el infinito.

Supongamos que K es la clausura algebraica de $\mathbb{F}_q$ donde $\mathbb{F}_q$ es un cuerpo finito con $q = p^s$ elementos. Consideremos sobre K la extensión de cuerpo de funciones $F/K(x)$ dada por la ecuación

$$y^{2n} = (x - \alpha_1)^{2k} x(x - \alpha_2), \tag{3.1}$$

donde $\alpha_1, \alpha_2 \in K$ son elementos distintos no nulos, $2n$ no es divisible por p y n, k son enteros positivos tales que $n > 1, n > k$, $d = (n, k)$ y $(n, k + 1) = 1$. Sobre este cuerpo de funciones el lugar P_∞ no es totalmente ramificado, dado que si $Q_\infty | P_\infty$, entonces por la Proposición 1.46 tenemos $e(Q_\infty|P_\infty) = \dfrac{n}{(n, k + 1)} = n$. De hecho sólo existen dos lugares de F que están sobre P_∞. Más exactamente de (3,1) se tiene

$$\left(\frac{y^n}{x^{k+1}}\right)^2 = \frac{(x - \alpha_1)^{2k} x(x - \alpha_2)}{x^{2k+2}},$$

por lo que definiendo el polinomio

$$\varphi(T) := T^2 - \frac{(x - \alpha_1)^{2k} x(x - \alpha_2)}{x^{2k+2}},$$

y haciendo reducción módulo P_∞, obtenemos

$$\overline{\varphi}(T) = T^2 - 1 = (T - 1)(T + 1) \in K[T].$$

Por lo tanto, el Teorema de Kummer 1.45 establece que existen sólo dos lugares de F, digamos, $Q_{\infty 1}, Q_{\infty 2}$ que están sobre P_∞. Más aún, $f(Q_{\infty i}|P_\infty) = 1$ para $i = 1, 2$, por lo cual $\deg(Q_{\infty i}) = [F_{Q_{\infty i}} : K] = [F_{Q_{\infty i}} : F_{P_\infty}][F_{P_\infty} : K] = 1 \cdot 1 = 1$.

Para el cálculo de los índices de ramificación correspondientes a los lugares $P_{x-\alpha_1}, P_x$ y $P_{x-\alpha_2}$ de $K(x)$, procedemos así: supongamos que $P'|P_{x-\alpha_1}, P''|P_x$ y $P'''|P_{x-\alpha_2}$. Entonces

$$e(P'|P_{x-\alpha_1}) = \frac{2n}{(2n, 2k)} = \frac{n}{(n, k)} = \frac{n}{d}, \quad e(P''|P_x) = 2n \quad \text{y} \quad e(P'''|P_{x-\alpha_2}) = 2n,$$

luego los lugares P_x y $P_{x-\alpha_2}$ son totalmente ramificados en F. En lo que respecta al lugar $P_{x-\alpha_1}$ se puede decir lo siguiente: De (3,1) se deduce

$$\frac{y^{2n}}{(x-\alpha_1)^{2k}} = x(x-\alpha_2) \text{ si y sólo si } \left(\frac{y^{n/d}}{(x-\alpha_1)^{k/d}}\right)^{2d} = x(x-\alpha_2)\ ,$$

de manera que definiendo $\varphi(T) := T^{2d} - x(x-\alpha_2)$ y reduciendo módulo $P_{x-\alpha_1}$ sobre sus coeficientes se obtiene $\overline{\varphi}(T) = T^{2d} - \alpha_1(\alpha_1-\alpha_2) \in K[T]$. Como K es la clausura algebraica de $\mathbb{F}_q$ y $\mathbb{F}_q$ es un cuerpo perfecto, tenemos que el polinomio anterior es separable y en consecuencia el Teorema de Kummer 1.45 afirmar que existen exactamente $2d$ lugares de F sobre $P_{x-\alpha_1}$, llamémoslos, $P'_1, P'_2, \cdots, P'_{2d}$ con $\deg P'_i = 1$ para $i = 1, 2, \cdots, 2d$.

De acuerdo a lo expuesto previamente desarrollamos el cálculo de algunos de los divisores principales del cuerpo de funciones dado por (3,1). Para este fin utilizamos la Proposición 1.44 obteniendo;

$$(x-\alpha_1)^F = \frac{n}{d}(P'_1 + \cdots + P'_{2d}) - n(Q_{\infty 1} + Q_{\infty_2}) \tag{3.2}$$

$$(x-\alpha_2)^F = 2nP''' - n(Q_{\infty 1} + Q_{\infty_2}) \tag{3.3}$$

$$(x)^F = 2nP'' - n(Q_{\infty_1} + Q_{\infty_2}), \tag{3.4}$$

y

$$(y)^F = \frac{k}{d}(P'_1 + \cdots + P'_{2d}) + P'' + P''' - (k+1)(Q_{\infty_1} + Q_{\infty_2}). \tag{3.5}$$

Por ejemplo para ver (3.8) procedemos así:

$$\begin{aligned}(y^{2n})^F &= ((x-\alpha_1)^{2k})^F + (x)^F + (x-\alpha_2)^F = 2k(x-\alpha_1)^F + (x)^F + (x-\alpha_2)^F \\ &= \frac{2nk}{d}(P'_1 + \cdots + P'_{2d}) + 2nP'' + 2nP''' - 2n(k+1)(Q_{\infty 1} + Q_{\infty 2}),\end{aligned}$$

de donde encontramos

$$(y)^F = \frac{k}{d}(P'_1 + P'_2 + \cdots + P'_{2d}) + P'' + P''' - (k+1)(Q_{\infty 1} + Q_{\infty 2}).$$

De las propiedades que se muestran en la Proposición 1.46 obtenemos:

Proposición 3.1. *El género g del cuerpo de funciones dado por* (3,1) *es* $g = 2n-d-1$.

Demostración. Note que cualquier lugar de $K(x)/K$ distinto a los lugares mencionados antes, no ramifica. Entonces por la Proposición 1.46 (c) se tiene

$$\begin{aligned} g &= 1+2n\left[-1+\frac{1}{2}\left[\left(1-\frac{d}{n}\right)+\left(1-\frac{1}{2n}\right)+\left(1-\frac{1}{2n}\right)+\left(1-\frac{1}{n}\right)\right]\right] \\ &= \frac{4n-2d-2}{2} = 2n-d-1. \end{aligned}$$

□

Sea H el semigrupo de Weierstrass asociado a los lugares $Q_{\infty 1}$ y $Q_{\infty 2}$ de F. Dependiendo de las condiciones sobre n y k; estamos interesados en describir este conjunto.

Proposición 3.2. *Consideremos el cuerpo de funciones dado por* (3,1) *y el conjunto* $S := \{n, n+k+1\}$. *Entonces* $S \subseteq H$ *y* $\langle S\rangle \subseteq H$.

Demostración. La relación (3.1) puede reescribirse en la forma

$$\underbrace{\left(\frac{y^n}{(x-\alpha_1)^k}-x\right)}_{a}\underbrace{\left(\frac{y^n}{(x-\alpha_1)^k}+x\right)}_{b} = -x\alpha_2, \tag{3.6}$$

con lo cual

$$v_{Q_{\infty i}}(a)^F + v_{Q_{\infty i}}(b)^F = -n, \tag{3.7}$$

para $i \in \{1,2\}$ fijo. Más aún, se tiene que

$$v_{Q_{\infty i}}\left(\frac{y^n}{(x-\alpha_1)^k}\right) = n(-(k+1)) - k(-n) = -n \quad \text{y} \quad v_{Q_{\infty i}}(x) = -n,$$

luego se deducen las desigualdades

$$v_{Q_{\infty i}}(a) \geq -n \text{ y } v_{Q_{\infty i}}(b) \geq -n. \tag{3.8}$$

También como $a+b=\dfrac{2y^n}{(x-\alpha_1)^k}$ se infiere la relación

$$-n \geq \text{mín}\{v_{Q_{\infty i}}(a), v_{Q_{\infty i}}(b)\}. \tag{3.9}$$

Entonces de (3.7), (3.8) y (3.9), para $i \in \{1,2\}$ se deduce dos posibles casos a saber;

$$v_{Q_{\infty i}}(a) = -n \quad \text{y} \quad v_{Q_{\infty i}}(b) = 0 \quad \text{ó} \quad v_{Q_{\infty i}}(a) = 0 \quad \text{y} \quad v_{Q_{\infty i}}(b) = -n.$$

Lo anterior significa que si $Q_{\infty i}$ es un polo de a, entonces $Q_{\infty i}$ no es un polo de b o viceversa.

Dado que

$$v_{P''}\left(\frac{y^n}{(x-\alpha_1)^k}\right) = n\cdot 1 - k\cdot 0 = n \quad \text{y} \quad v_{P''}(x) = 2n$$

tenemos $v_{P''}(a) = n$ y $v_{P''}(b) = n$, es decir, P'' es un cero de a y b. Un cálculo similar muestra que $v_{P_i'}(a) = v_{P_i'}(b) = v_{P'''}(a) = v_{P'''}(b) = 0$. En vista de lo anterior podemos decir que

$$(a)^F = nP'' - nQ_{\infty 1} \tag{3.10}$$

y

$$(b)^F = nP'' - nQ_{\infty 2}, \tag{3.11}$$

demostrándose así que $n \in H$. Para culminar la prueba, consideremos el divisor principal del elemento $yab^{-1} \in F$. Entonces

$$\begin{aligned}(yab^{-1})^F &= (y)^F + (a)^F - (b)^F \\ &= \frac{k}{d}(P_1' + \cdots + P_{2d}') + P'' + P''' - (n+k+1)Q_{\infty_1} + (n-k-1)Q_{\infty_2},\end{aligned}$$

y como $n-k-1 \geq 0$ se infiere que $n+k+1 \in H$. □

Observación 3.3. Es bueno resaltar que conocer la existencia de los elementos a y b de F que cumplen (3.10) y (3.11) es muy importante, pues las funciones generadoras que se buscan están en términos de ellos. Asímismo es de notar que garantizar la existencia de estos no es simple, pues depende fuertemente de la ecuación que define a la extensión de cuerpo $F/K(x)$ del cuerpo de funciones racionales $K(x)/K$.

Bajo hipótesis adicionales para n y k tenemos algunos hechos importantes: Para comenzar note que si $d = 1$, entonces $(n, k) = 1$ y $(n, k + 1) = 1$ implican que n es un número impar.

Teorema 3.4. *Si $d = 1$ en* (3,1), *entonces $H = \langle n, n + k + 1\rangle$ si y sólo si $n + k = 4$.*

Demostración. Si $S := \{n, n+k+1\}$, entonces en virtud de la Proposición 3.2 tenemos que $\langle S\rangle \subseteq H$. Supongamos que $n + k = 4$. Para demostrar que $H = \langle S\rangle$ basta con verificar que $g_S = g$, siendo g_S el género del semigrupo numérico $\langle S\rangle$. En efecto, por la Proposición 1.25

$$\begin{aligned} g_S &= \frac{n(n+k+1)-n-n-k-1+1}{2} = \frac{n^2+nk+n-n-n-k-1+1}{2} \\ &= \frac{n^2+k(n-1)-n}{2} = \frac{n(n-1)+k(n-1)}{2} = \frac{(n-1)(n+k)}{2} = \frac{(n-1)(4)}{2} \\ &= 2n-2 = g. \end{aligned}$$

Recíprocamente, si suponemos $H = \langle S\rangle$, entonces $g = g_S$, es decir, $2n-2 = \dfrac{(n-1)(n+k)}{2}$, lo cual implica que $n + k = 4$. □

Observación 3.5. Si en el teorema anterior $d \neq 1$, entonces el resultado ya no es válido. En efecto, si $H = \langle n, n + k + 1\rangle$, entonces $g = g_S$, es decir,

$$\frac{(n-1)(n+k)}{2} = 2n - d - 1. \tag{3.12}$$

Teniendo en cuenta la naturaleza de los números g, n y k, la igualdad (3.12) implica que d es impar y par a la vez, un absurdo.

Ejemplo 3.6. Consideremos la extensión de Kummer $y^6 = (x-1)^2x(x-4)$ sobre $\mathbb{F}_7$. En este caso $n = 3$, $k = 1$ y $n + k = 4$. Por lo tanto, su género es $g = 4$ y el semigrupo de Weierstrass asociado a los lugares $Q_{\infty 1}$ y $Q_{\infty 2}$ está dado por $H = \langle 3, 5\rangle$.

Proposición 3.7. *Si suponemos que $n < 2k$ en* (3,1), *entonces*

$$S := \{n, n + k + 1, 2k + 2\} \subseteq H, \tag{3.13}$$

y $\langle S\rangle \subseteq H$.

Demostración. Por la Proposición 3.2 solamente se debe probar que $2k+2 \in H$. En efecto, para el elemento $y^2ab^{-1}(x-\alpha_1)^{-1}$ tenemos

$$\begin{aligned}(y^2ab^{-1}(x-\alpha_1)^{-1})^F &= 2(y)^F + (a)^F - (b)^F - (x-\alpha_1)^F \\ &= \left(\frac{2k-n}{d}\right)(P_1' + \cdots + P_{2d}') + 2P'' + 2P''' + (2n-2(k+1))Q_{\infty 2} - 2(k+1)Q_{\infty 1}.\end{aligned}$$

Como $\dfrac{2k-n}{d} \geq 0$, $n > k$ y $k \geq 1$ se sigue que $2k+2 \in H$. □

De acuerdo al resultado previo, si consideramos $d = 1$ para el cuerpo de funciones dado por (3.1) se tiene:

Teorema 3.8. *Si $d = 1$ y $n < 2k$ en* (3,1), *entonces*

$$H = \langle n, n+k+1, 2k+2\rangle \text{ si y sólo si } k = 3 \text{ y } n = 5.$$

Demostración. Definamos $S := \{n, n+k+1, 2k+2\}$. En primera instancia note que por la Proposición 3.7 tenemos $\langle S\rangle \subseteq H$. Procedamos a calcular el género g_S. Para comenzar, afirmamos que el conjunto Apéry A de $\langle S\rangle$ con respecto a n está dado por $A = \{0\} \cup A_1 \cup A_2$, donde

$$A_1 := \{n + ik + i : \ 1 \leq i \leq n-2 \text{ con } i \text{ impar}\} \text{ y } A_2 := \left\{i(2k+2) : \ 1 \leq i \leq \frac{n-1}{2}\right\}.$$

Para probar este hecho, debemos ver que A tiene n elementos distintos módulo n, $A \subseteq \langle S\rangle$ y que si $x \in A$, entonces $x - n \notin \langle S\rangle$. En efecto, consideremos $1 \leq i, j \leq \dfrac{n-1}{2}$ números enteros, entonces

$$i(2k+2) \equiv j(2k+2) \pmod n \text{ sii } i \equiv j \pmod n \text{ sii } i = j \text{ pues } i, j < n.$$

De igual forma, para $1 \leq i, j \leq n-2$ con i, j impar tenemos

$$\begin{aligned} n + i(k+1) &\equiv n + j(k+1) \pmod n \text{ sii } i(k+1) \equiv j(k+1) \pmod n \text{ sii} \\ i &\equiv j \pmod n \text{ sii } i = j \text{ pues } i, j < n.\end{aligned}$$

Ahora, sean i, j tales que $1 \leq i \leq n-2$ donde i es impar y $1 \leq j \leq \dfrac{n-1}{2}$. Entonces

$$\begin{aligned} n + i(k+1) &\equiv 2(k+1)j \pmod{n} \text{ sii } i(k+1) \equiv 2(k+1)j \pmod{n} \text{ sii} \\ i &\equiv 2j \pmod{n} \text{ sii } i = 2j \text{ pues } i, 2j < n. \end{aligned}$$

Lo anterior garantiza que hay n elementos distintos módulo n en A. Acto seguido veamos que $A \subseteq \langle S \rangle$. Claramente $(2k+2)i \in \langle S \rangle$ para todo $i \in \mathbb{N}$. De otro lado, sea $1 \leq i \leq n-2$ siendo i impar. Dado que $n+k+1 \in \langle S \rangle$ y $(2k+2)j \in \langle S \rangle$ para todo j, se sigue que $n+k+1+2j(k+1) \in \langle S \rangle$, es decir, $n+(k+1)(2j+1) \in \langle S \rangle$, y $2j+1$ es un número impar. Reemplanzando $2j+1$ por i obtenemos que $n+i(k+1) \in \langle S \rangle$. Consecuentemente $A \subseteq \langle S \rangle$. Resta ver que $n+i(k+1)-n$ y $(2k+2)j-n$ no pertencen a $\langle S \rangle$ para $1 \leq i \leq n-2$ impar y $1 \leq j \leq \dfrac{n-1}{2}$. Efectivamente, supongamos que existen $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{N}$ no todos ceros tales que

$$i(k+1) = \lambda_1 n + \lambda_2(n+k+1) + \lambda_3(2k+2).$$

Entonces $\lambda_1 + \lambda_2 = 0$ y $\lambda_2 + 2\lambda_3 = i$. Esto implica que $\lambda_1 = \lambda_2 = 0$, y por consiguiente i es par, una contradicción. De igual forma, si existen $\beta_1, \beta_2, \beta_3 \in \mathbb{N}$ no todos ceros que satisfacen la relación

$$(2k+2)j - n = \beta_1 n + \beta_2(n+k+1) + \beta_3(2k+2),$$

se infiere $\beta_1 + \beta_2 = -1$, lo cual es absurdo. Por lo tanto, $A = \mathrm{Ap}(\langle S \rangle; n)$. Ahora bien, en virtud de la Proposición 1.23

$$\begin{aligned} g_S &= \frac{1}{n}\left(\sum_{i=1}^{\frac{n-1}{2}}[n+(2i-1)k+(2i-1)] + \sum_{i=1}^{\frac{n-1}{2}}[i(2k+2)]\right) - \frac{n-1}{2} \\ &= \frac{1}{n}\left(n\left(\frac{n-1}{2}\right) + k\left(\frac{n-1}{2}\right)^2 + \left(\frac{n-1}{2}\right)^2 + (2k+2)\frac{(n-1)(n+1)}{8}\right) - \frac{n-1}{2} \\ &= \frac{1}{n}\left(n\left(\frac{n-1}{2}\right) + k\left(\frac{n-1}{2}\right)^2 + \left(\frac{n-1}{2}\right)^2 + \frac{(k+1)(n^2-1)}{4}\right) - \frac{n-1}{2} \end{aligned}$$

$$= \frac{k(n-1)^2}{4n} + \frac{(n-1)^2}{4n} + \frac{(k+1)(n^2-1)}{4n} = \frac{(k+1)(n-1)^2}{4n} + \frac{(k+1)(n^2-1)}{4n}$$
$$= \frac{(k+1)\left((n-1)^2+n^2-1\right)}{4n} = \frac{(k+1)\left(2n^2-2n\right)}{4n} = \frac{(k+1)(n-1)}{2}.$$

Supongamos que $k=3$ y $n=5$. Entonces $g_S = g$ y en consecuencia $H = \langle S \rangle$.
De igual forma, si $H = \langle S \rangle$, entonces $g_S = g = 2n-2$ lo cual implica que $k=3$, y puesto que $n \leq 2k$ con n es impar, se deduce $n=5$.

□

Ejemplo 3.9. Dada la extensión de Kummer $y^{10} = (x+1)^6 x(x+3)$ sobre $\mathbb{F}_q$ donde q no divide a 10; se tiene que $n=5$ y $k=3$ por lo cual

$$H = \langle 5, 8, 9 \rangle.$$

Proposición 3.10. *Si suponemos $n > 2k+1$ en* (3,1)*, entonces*

$$S := \{n, n+k+1, n+2k+2\} \subseteq H. \tag{3.14}$$

En particular como H es un semigrupo numérico tenemos que $\langle S \rangle \subseteq H$.

Demostración. Los elementos n y $n+k+1$ se encuentran en H según la Proposición 3.2. Considerando el divisor principal del elemento y^2ab^{-1} tenemos

$$\begin{aligned}(y^2ab^{-1})^F &= 2(y)^F + (a)^F - (b)^F \\ &= \frac{2k}{d}(P_1' + \cdots + P_{2d}') + 2P'' + 2P''' + (n-2k-2)Q_{\infty 2} - (n+2k+2)Q_{\infty 1}.\end{aligned}$$

En vista de que $n > 2k+1$, se deduce $n-2k-2 \geq 0$ y consecuentemente $n+2k+2$ es un elemento de H. □

El próximo teorema establece condiciones para n y k que hacen de la inclusión (3.14) una igualdad.

Teorema 3.11. *Si en* (3,1) *suponemos $n > 2k+1$ y $d=1$, entonces*

$$H = \langle n, n+k+1, n+2k+2 \rangle \text{ si y solo si } n=5 \text{ y } k=1.$$

Demostración. Definiendo $S := \{n, n+k+1, n+2k+2\}$ se sigue que $\langle S\rangle \subseteq H$. Al igual que antes, empezamos calculando el género g_S de $\langle S\rangle$ utilizando la Proposición 1.23. Para esto, afirmamos que el conjunto Apéry de $\langle S\rangle$ con respecto a n está dado por $A = \{0\} \cup A_1 \cup A_2$, donde

$$A_1 := \left\{ in + jk + j : \ 1 \leq i \leq \frac{n-1}{2} \text{ y } 1 \leq j \leq n-2 \text{ con } j \text{ impar} \right\},$$

y

$$A_2 := \left\{ i(n+2k+2) : 1 \leq i \leq \frac{n-1}{2} \right\}.$$

Primero comprobemos que A tiene n elementos diferentes módulo n. Para $1 \leq i, j \leq n-2$ donde i, j son impares tenemos

$$i(k+1) \equiv j(k+1) \pmod{n} \ \text{ sii } \ i \equiv j \pmod{n} \ \text{ sii } \ i = j, \ \text{ pues } i, j < n.$$

Análogamente, para $1 \leq i, j \leq \dfrac{n-1}{2}$ se cumple

$$i(n+2k+2) \equiv j(n+2k+2) \pmod{n} \ \text{ sii } \ i \equiv j \pmod{n} \ \text{ sii } \ i = j.$$

Ahora bien, si consideramos $1 \leq i \leq n-2$ con i impar y $1 \leq j \leq \dfrac{n-1}{2}$ entonces

$$\begin{aligned} i(k+1) &\equiv j(n+2k+2) \pmod{n} \ \text{ sii } \ i(k+1) \equiv 2j(k+1) \pmod{n} \ \text{ sii} \\ i &\equiv 2j \pmod{n} \ \text{ sii } \ i = 2j \ \text{ dado que } i, 2j < n. \end{aligned}$$

Así las cosas, se infiere que A tiene n elementos diferentes módulo n. Veamos enseguida que los elementos del conjunto A pertencen a $\langle S\rangle$. Claramente $j(n+2k+2) \in \langle S\rangle$ para todo $j \in \mathbb{N}$. Por otra parte observe que

$$(n+2k+2) + (n+k+1) = 2n+3k+3,$$

$$(n+2k+2) + (2n+3k+3) = 3n+5k+5,$$

$$\vdots$$

$$(n+2k+2)+\left(\frac{n-5}{2}\right)n+(n-6)k+(n-6)=\left(\frac{n-3}{2}\right)n+(n-4)k+(n-4),$$

$$(n+2k+2)+\left(\frac{n-3}{2}\right)n+(n-4)k+(n-4)=\left(\frac{n-1}{2}\right)n+(n-2)k+(n-2).$$

En definitiva, $A_1 \subseteq \langle S\rangle$ y por consiguiente $A \subseteq \langle S\rangle$. También note que $n+k+1-n = k+1 \notin \langle S\rangle$, pues si existen $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{N}$ no todos ceros para el cual

$$k+1 = \lambda_1 n + \lambda_2(n+k+1) + \lambda_3(n+2k+2),$$

encontramos $\lambda_1+\lambda_2+\lambda_3 = 0$ y $\lambda_2+2\lambda_3 = 1$; que son ecuaciones inconsistentes para todo valor de λ_i, $i = 1,2,3$. Argumentando de forma similar se ve que $2n+3k+3-n, 3n+5k+5-n, \cdots, \left(\frac{n-1}{2}\right)n+(n-2)k+(n-2)-n$ no pertenecen a $\langle S\rangle$. Asímismo, los elementos $n+2k+2-n, 2(n+2k+2)-n, \cdots, \left(\frac{n-1}{2}\right)(n+2k+2)-n \notin \langle S\rangle$. En efecto, (determinamos la razón para $2(n+2k+2)-n = n+4k+4$ pero la forma de proceder es esencialmente la misma para los otros casos): Si existen $\beta_1, \beta_2, \beta_3 \in \mathbb{N}$ no todos ceros tales que

$$n+4k+4 = \beta_1 n + \beta_2(n+k+1) + \beta_3(n+2k+2),$$

entonces encontramos $\beta_1+\beta_2+\beta_3 = 1$ y $\beta_2+2\beta_3 = 4$, lo cual es absurdo de acuerdo al origen de los escalares $\beta_i, i = 1,2,3$. Por lo tanto, el conjunto Apéry de $\langle S\rangle$ con respecto

a n es A. Consecuentemente; por la Proposición 1.23

$$\begin{aligned}
g_S &= \frac{1}{n}\left(\sum_{i=1}^{\frac{n-1}{2}}[in+(k+1)(2i-1)+i(n+2k+2)]\right)-\frac{n-1}{2}\\
&= \frac{1}{n}\left(\sum_{i=1}^{\frac{n-1}{2}}[2in+(k+1)(4i-1)]\right)-\frac{n-1}{2}\\
&= \frac{1}{n}\left(\frac{n(n-1)(n+1)}{4}+\frac{(k+1)(n-1)(n+1)}{2}-\frac{(k+1)(n-1)}{2}\right)-\frac{n-1}{2}\\
&= \frac{1}{n}\left(\frac{n(n-1)(n+1)}{4}+\frac{n(n-1)(k+1)}{2}\right)-\frac{n-1}{2}\\
&= \frac{1}{n}\left(\frac{n(n-1)}{2}\left(\frac{n+1}{2}+k+1\right)\right)-\frac{n-1}{2}=\frac{n^2-1}{4}+\frac{k(n-1)}{2}=\frac{n^2+2nk-2k-1}{4}.
\end{aligned}$$

Suponiendo $H=\langle S\rangle$ se sigue $g_S=g$, lo cual significa que $k=\dfrac{-(n-7)}{2}$. Como $k\geq 1$ entonces $n\leq 6$, pero teniendo en cuenta que n es impar y mayor que 1, se tiene que $n\in\{3,5\}$. Si $n=3$, no existe $k<n$ que satisfaga la condición $n>2k+1$, luego $n=5$. Entonces las posibilidades para k son $\{1,2,3,4\}$, no obstante, de acuerdo a la restricción $n>2k+1$, vemos que la única opción para k es $k=1$.

En el sentido recíproco, dado que $\langle S\rangle\subseteq H$, y que ambos semigrupos numéricos tienen el mismo género cuando $n=5$ y $k=1$, deducimos $H=\langle S\rangle$. □

Ejemplo 3.12. Supongamos que tenemos la extensión de $\mathbb{F}_{11}(x)$ de tipo Kummer $y^{10}=(x+3)^2x(x+5)$. Entonces $H=\langle 5,7,9\rangle$ con lo cual empleando la observación 1.42 encontramos que $\ell(6Q_{\infty_1})=2$, es decir, la cantidad de elementos de H que son menores o iguales a 6. Más aún, una base para el espacio de Riemann-Roch $\mathscr{L}(6Q_{\infty_1})$ es

$$B=\left\{1,\frac{y^5}{(x+3)-x}\right\}$$

Si en el Teorema 3.11 hacemos $n=2k+1$ tenemos lo siguiente:

Proposición 3.13. *Si en* (3,1) *consideramos* $n=2k+1$ *y* $d=1$*, entonces*

$$\langle n,n+k+1,n+k+2,n+k+3,\cdots,n+k+k\rangle\subseteq H, \tag{3.15}$$

es decir,

$$\langle 2k+1, 3k+2, 3k+3, 3k+4, \cdots, 3k+k, 3k+(k+1)\rangle \subseteq H.$$

Demostración. Los elementos n y $n+k+1$ pertenecen a H por la Proposición 3.2. Consideremos $0 \leq i \leq k-1$ un número entero y definamos $\gamma := ab^{-1}(x-\alpha_1)^{-i}y^{2i+1}$. Entonces, como $(\gamma)^F = (a)^F - (b)^F - i(x-\alpha_1)^F + (2i+1)(y)^F$ y

$$(a)^F - (b)^F = -nQ_{\infty 1} + nQ_{\infty 2},$$

$$i(x-\alpha_1)^F = -in(P_1' + P_2') - inQ_{\infty 1} + inQ_{\infty 2}$$

y

$$(2i+1)(y)^F = (2i+1)(k(P_1' + P_2') + P'' + P''' - (k+1)(Q_{\infty 1} + Q_{\infty 2}),$$

simplificando obtenemos

$$(\gamma)^F = (k-i)(P_1' + P_2') + (2i+1)P'' + (2i+1)P''' + (k-i)Q_{\infty 2} - (i+3k+2)Q_{\infty 1}.$$

Claramente $k-i$ y $2i+1$ son números enteros positivos, luego el elemento $i+3k+2 \in H$ para todo $0 \leq i \leq k-1$. Así pues (3.15) se sigue del hecho de que H es un semigrupo numérico. □

Obteniendo el conjunto Apéry del semigrupo numérico anterior se puede probar que la inclusión (3.15), en efecto es una igualdad.

Teorema 3.14. *Con las mismas hipótesis de la proposición anterior,*

$$H = \langle n, n+k+1, n+k+2, n+k+3, \cdots, n+k+k\rangle.$$

Demostración. Comenzamos definiendo $S := \{n, n+k+1, n+k+2, n+k+3, \cdots, n+k+k\}$. Para probar que $H = \langle S\rangle$ es suficiente con verificar que $g_S = g$. Para tal fin, en primera instancia se afirma que el conjunto Apéry de $\langle S\rangle$ con respecto a n está dado

por $A = \{0\} \cup A_1 \cup A_2$, donde

$$A_1 := \{n + k + i : 1 \leq i \leq k\} \text{ y } A_2 := \{2(n + k + 1) + i : 0 \leq i \leq k - 1\}.$$

Igualmente que en los Teoremas 3.8 y 3.11 mostremos que A tiene $n = 2k+1$ elementos diferentes módulo n, $A \subseteq \langle S \rangle$ y si $x \in A$, entonces $x - n \notin \langle S \rangle$.

Para $1 \leq i, j, \leq k$ tenemos

$$n + k + i \equiv n + k + j \pmod{n} \text{ sii } i \equiv j \pmod{n} \text{ sii } i = j \text{ dado que } i, j < n.$$

Asímismo, para $0 \leq i, j \leq k - 1$ se cumple

$$2(n + k + 1) + i \equiv 2(n + k + 1) + j \pmod{n} \text{ sii } i = j \text{ puesto que } i, j < n.$$

Por último, si consideramos $1 \leq i \leq k$ y $0 \leq j \leq k - 1$, entonces

$$2(n + k + 1) + j \equiv n + k + i \pmod{n} \text{ sii } j + 1 \equiv k + i \pmod{n} \text{ sii } j + 1 = k + i.$$

De acuerdo con esto tenemos $n = 2k + 1$ elementos distintos módulo n. Ahora bien, verifiquemos que $A \subseteq \langle S \rangle$. Claramente $n+k+i \in \langle S \rangle$ con $0 \leq i \leq k$. Del mismo modo, escribiendo

$$2(n + k + 1) = (n + k + 1) + (n + k + 1)$$

$$2(n + k + 1) + 1 = (n + k + 1) + (n + k + 2)$$

$$2(n + k + 1) + 2 = (n + k + 1) + (n + k + 3)$$

$$\vdots$$

$$2(n + k + 1) + (k - 1) = (n + k + 1) + (n + k + k),$$

se demuestra que $2(n + k + 1) + i \in \langle S \rangle$ para todo $0 \leq i \leq k - 1$. A continuación, probemos que $x \in A$ implica que $x - n \notin S$. Supongamos que para $0 \leq i \leq k$ fijo,

existen $\lambda_0, \lambda_1, \cdots, \lambda_k \in \mathbb{N}$ no todos ceros tales que

$$n+k+i-n = k+i = \lambda_0 n + \sum_{j=1}^{k} \lambda_j (n+k+j) = n\left(\sum_{j=0}^{k} \lambda_j\right) + k\left(\sum_{j=1}^{k} \lambda_j\right) + \sum_{j=1}^{k} j\lambda_j,$$

luego, se debe satisfacer $0 = \sum_{j=0}^{k} \lambda_j$ y $1 = \sum_{j=1}^{k} \lambda_j$, de donde $\lambda_0 = -1$, una contradicción. En el mismo sentido, si suponemos que para i fijo con $0 \leq i \leq k-1$; existen $\beta_0, \beta_1, \cdots, \beta_k \in \mathbb{N}$ no todos ceros que cumplen la relación

$$\begin{aligned} 2(n+k+1)+i-n &= n+2k+2+i = \beta_0 n + \sum_{j=1}^{k} \beta_j (n+k+j) \\ &= n\left(\sum_{j=0}^{k} \beta_j\right) + k\left(\sum_{j=1}^{k} \beta_j\right) + \sum_{j=1}^{k} j\beta_j, \end{aligned}$$

entonces $\sum_{j=0}^{k} \beta_j = 1$ y $\sum_{j=1}^{k} \beta_j = 2$ con lo cual $\beta_0 = -1$, de nuevo una contradicción. Por lo tanto, $\mathrm{Ap}(\langle S \rangle; n) = A$. Finalmente, empleando la Proposición 1.23 encontramos

$$\begin{aligned} g_S &= \frac{1}{n}\left(\sum_{i=1}^{k} [n+k+i] + \sum_{i=0}^{k-1} [2(n+k+1)+i]\right) - \frac{n-1}{2} \\ &= \frac{1}{n}\left(nk + k^2 + \sum_{i=1}^{k} i + 2k(n+k+1) + \sum_{i=1}^{k-1} i\right) - \frac{n-1}{2} = \frac{k(3n+4k+2)}{n} - \frac{n-1}{2} \\ &= \frac{6nk + 8k^2 + 4k - n^2 + n}{2n}. \end{aligned}$$

Reemplazando $n = 2k+1$ en la última igualdad obtenemos $g_S = 4k = 2n-2 = g$. □

Ejemplo 3.15. Consideremos la extensión de Kummer $y^{14} = (x-1)^6 x(x-3)$ sobre $\mathbb{F}_5$. Observando que $n = 7$ y $k = 3$, el teorema anterior implica que $H = \langle 7, 11, 12, 13 \rangle$. El conjunto Apéry de H con respecto a $n = 7$ está dado por

$$\mathrm{Ap}(H; 7) = \{0, 11, 12, 13, 22, 23, 24\},$$

de manera que el número de frobenius es $F(H) = \mathrm{máx}\{\mathrm{Ap}(H; 7)\} - 7 = 17$.

Note que si $n = 2k$, las hipótesis dadas en (3.1) implican que $d = k$ y k es un número par. El resultado próximo describe explicítamente el conjunto H para este caso:

Teorema 3.16. *Dada la extensión de Kummer*

$$y^{2n} = (x - \alpha_1)^{2k} x(x - \alpha_2),$$

con $n = 2k, (n, k) = d$ *y* $(n, k + 1) = 1$, *el semigrupo de Weierstrass asociado a los lugares* Q_{∞_1} *y* Q_{∞_2} *que están sobre el lugar* P_∞ *está dado por*

$$H = \langle n, 2k + 2, 2k + 4, \cdots, 2k + k, n + k + 1, n + k + 2, \cdots, n + k + (k - 1)\rangle. \quad (3.16)$$

Demostración. Sea $S := \{n\} \cup A_1 \cup A_2$, siendo

$$A_1 := \left\{2(k + i) : 1 \leq i \leq \frac{k}{2}\right\} \text{ y } A_2 := \{n + k + i : 1 \leq i \leq k - 1\}. \quad (3.17)$$

Para probar que $H = \langle S\rangle$ es suficiente con demostrar que A_1 y A_2 están contenidos en H, y que $g_S = g$. Efectivamente, para constatar lo primero procedemos de la siguiente manera: por la Proposición 3.2 se garantiza que los elementos n y $n + k + 1$ pertenecen a H. Por otra parte consideremos las siguientes situaciones:

1. El divisor principal $(ab^{-1}y^i(x - \alpha_1)^{-i/2})^F$ con $2 \leq i \leq k$ par. Entonces

$$\begin{aligned}
&(ab^{-1}y^i(x - \alpha_1)^{-i/2})^F = (a)^F - (b)^F + i(y)^F - \frac{i}{2}(x - \alpha_1)^F = nQ_{\infty 2} - nQ_{\infty 1} \\
&+ \frac{ik}{d}\left(P_1' + \cdots + P_{2d}'\right) + iP'' + iP''' - i(k + 1)Q_{\infty 1} - i(k + 1)Q_{\infty 2} \\
&- \frac{in}{2d}(P_1' + \cdots + P_{2d}') + \frac{in}{2}Q_{\infty 1} + \frac{in}{2}Q_{\infty 2} = \left(\frac{ik}{d} - \frac{in}{2d}\right)\left(P_1' + \cdots + P_{2d}'\right) + iP'' \\
&+ iP''' + \left(n - ik - i + \frac{in}{2}\right)Q_{\infty 2} - \left(n + ik + i - \frac{in}{2}\right)Q_{\infty 1}.
\end{aligned}$$

   Como $n = 2k$ y $d = k$ obtenemos

$$(ab^{-1}y^i(x - \alpha_1)^{-i/2})^F = iP'' + iP''' + (2k - i)Q_{\infty 2} - (2k + i)Q_{\infty 1},$$

   es decir, los elementos $2k + i$ con $2 \leq i \leq k$ par pertenecen a H.

2. El divisor principal $(\gamma)^F$ para $\gamma := ab^{-1}y^j(x-\alpha_1)^{-\left(\frac{j-1}{2}\right)}$, donde $1 \leq j \leq k-1$ es impar. Entonces

$$(\gamma)^F = (a)^F - (b)^F + j(y)^F - \left(\frac{j-1}{2}\right)(x-\alpha_1)^F$$
$$= n(Q_{\infty 2} - Q_{\infty 1}) + \frac{jk}{d}(P_1' + \cdots + P_{2d}') + j(P'' + P''') - j(k+1)(Q_{\infty 1} + Q_{\infty 2})$$
$$- \left(\frac{n(j-1)}{2d}\right)(P_1' + \cdots + P_{2d}') + \left(\frac{n(j-1)}{2}\right)Q_{\infty 1} + \left(\frac{n(j-1)}{2}\right)Q_{\infty 2} = jP''$$
$$+ jP''' + \left(\frac{jk}{d} - \frac{n(j-1)}{2d}\right)(P_1' + \cdots + P_{2d}') + \left(n - j(k+1) + \frac{n(j-1)}{2}\right)Q_{\infty 2}$$
$$- \left(n + j(k+1)\frac{n(j-1)}{2}\right)Q_{\infty 1} = \left(\frac{2djk - jnd + nd}{2d^2}\right)(P_1' + \cdots + P_{2d}') + jP''$$
$$+ jP''' + \left(n - jk - j + \frac{jn}{2} - \frac{n}{2}\right)Q_{\infty 2} - \left(n + jk + j - \frac{jn}{2} + \frac{n}{2}\right)Q_{\infty 1}.$$

Sustituyendo $n = 2k$ y $d = k$ se sigue

$$(\gamma)^F = (P_1' + \cdots + P_{2d}') + jP'' + jP''' + (k-j)Q_{\infty 2} - (3k+j)Q_{\infty 1},$$

con lo cual se evidencia que $3k + j \in H$ para todo $1 \leq j \leq k-1$ impar.

3. El divisor principal $\left(ab^{-1}y^{k+j}(x-\alpha_1)^{-\left(\frac{k+j}{2}\right)}\right)^F$ siendo $2 \leq j \leq k-2$ par. Entonces

$$\left(ab^{-1}y^{k+j}(x-\alpha_1)^{-\left(\frac{k+j}{2}\right)}\right)^F = (a)^F - (b)^F + (k+j)(y)^F - \left(\frac{k+j}{2}\right)(x-\alpha_1)^F$$
$$= nQ_{\infty 2} - nQ_{\infty 1} + \frac{k(k+j)}{d}(P_1' + \cdots + P_{2d}') - (k+j)(k+1)Q_{\infty 1}$$
$$- (k+j)(k+1)Q_{\infty 2} + (k+j)P'' + (k+j)P''' - \frac{n(k+j)}{2d}(P_1' + \cdots + P_{2d}')$$
$$+ \frac{n(k+j)}{2}Q_{\infty 1} + \frac{n(k+j)}{2}Q_{\infty 2}$$

$$= \left(\frac{k(k+j)}{d} - \frac{n(k+j)}{2d}\right)(P_1' + \cdots + P_{2d}') + (k+j)P'' + (k+j)P'''$$
$$+ \left(n - (k+j)(k+1) + \frac{n(k+j)}{2}\right)Q_{\infty 2} - \left(n + (k+j)(k+1) - \frac{n(k+j)}{2}\right)Q_{\infty 1}.$$

Escribiendo $n = 2k$ y $d = k$ encontramos

$$\left(ab^{-1}y^{k+j}(x-\alpha_1)^{-\left(\frac{k+j}{2}\right)}\right)^F = (k+j)P'' + (k+j)P''' + (k-j)Q_{\infty 2} - (3k+j)Q_{\infty 1},$$

luego $3k + j \in H$ para $2 \leq j \leq k-1$ par.

Para mostrar que $g_S = g$, observe que el conjunto Apéry de $\langle S \rangle$ con respecto a n está dado por $A = \{0\} \cup A_1 \cup A_2 \cup A_3$, donde A_1 y A_2 están definidos en (3.17) y $A_3 := \left\{ n + 4k + (2i-1) : 1 \leq i \leq \frac{k}{2} \right\}$.

Tal como en las demostraciones anteriores, para justificar este hecho debemos probar que $A \subseteq \langle S \rangle$, A tiene n elementos diferentes módulo n y si $x \in A$, entonces $x - n \notin \langle S \rangle$. Evidentemente los conjuntos A_1 y A_2 están contenidos en $\langle S \rangle$. También, dado que $n + 4k + i = (n + k + i) + (2k + 2)$ con $i \in \{1, 3, 5, \cdots, k-3, k-1\}$, entonces obtenemos la inclusión $A \subseteq \langle S \rangle$.

Ahora bien, para $1 \leq i, j \leq k-1$ tenemos

$$n + k + i \equiv n + k + j \pmod{n} \text{ sii } i \equiv j \pmod{n} \text{ sii } i = j \text{ porque } i, j < n.$$

Del mismo modo, si $i, j \in \{2, 4, \cdots, k-2, k\}$, entonces

$$2k + i \equiv 2k + j \pmod{n} \text{ sii } i \equiv j \pmod{n} \text{ sii } i = j \text{ pues } i, j < n.$$

Más aún, considerando $i, j \in \{1, 3, 5, \cdots, k-1\}$ vemos que

$$n + 4k + i \equiv n + 4k + j \pmod{n} \text{ sii } i \equiv j \pmod{n} \text{ sii } i = j, \text{ ya que } i, j < n.$$

De otro lado, suponiendo $1 \leq i \leq k-1$, $2 \leq j \leq k$ par y $1 \leq l \leq k-1$ impar encontramos que

$$n + k + i \equiv 2k + j \pmod{n} \text{ sii } k + i \equiv j \pmod{2k} \text{ sii } k + i \equiv j \pmod{k} \text{ sii } i = j.$$

Un razonamiento similar determina que

$$2k + j \equiv n + 4k + l \pmod{n} \text{ sii } j \equiv l \pmod{2k} \text{ sii } j = l, \text{ dado que } j, l < 2k.$$

Por todo lo anterior, tenemos $n = 2k$ elementos distintos módulo n en A. A continuación demostremos que si $x \in A$, entonces $x - n \notin \langle S \rangle$. Para este fin consideremos que para $1 \leq i \leq k-1$ fijo, existen $\lambda_1, \lambda_2, \cdots, \lambda_{\frac{k}{2}}, \gamma_0, \gamma_1, \cdots, \gamma_{k-1} \in \mathbb{N}$ no todos ceros tales que

$$\begin{aligned} n + k + i - n = k + i &= \gamma_0 n + \sum_{j=1}^{k-1} \gamma_j (n + k + j) + \sum_{j=1}^{\frac{k}{2}} \lambda_j (2(k + j)) \\ &= n \left(\sum_{j=0}^{k-1} \gamma_j \right) + k \left(\sum_{j=1}^{\frac{k}{2}} 2\lambda_j + \sum_{j=1}^{k-1} \gamma_j \right) + \left(\sum_{j=1}^{\frac{k}{2}} 2j\lambda_j + \sum_{j=1}^{k-1} j\gamma_j \right) \end{aligned}$$

Entonces debe tenerse

$$\sum_{j=0}^{k-1} \gamma_j = 0 \quad \text{y} \quad 2 \left(\sum_{j=1}^{\frac{k}{2}} \lambda_j \right) = 1 + \gamma_0. \tag{3.18}$$

De acuerdo a la naturaleza de los $\lambda_i s'$ y $\gamma_i s'$ observamos que (3.18) produce una contradicción, luego los elementos $k + i \notin \langle S \rangle$. Análogamente, para i fijo con $2 \leq i \leq k$ par; si tenemos la combinación lineal no trivial

$$\begin{aligned} 2k + i - n &= \gamma_0 n + \sum_{j=1}^{k-1} \gamma_j (n + k + j) + \sum_{j=1}^{\frac{k}{2}} \lambda_j (2(k + j)) \\ &= n \left(\sum_{j=0}^{k-1} \gamma_j \right) + k \left(\sum_{j=1}^{\frac{k}{2}} 2\lambda_j + \sum_{j=1}^{k-1} \gamma_j \right) + \left(\sum_{j=1}^{\frac{k}{2}} 2j\lambda_j + \sum_{j=1}^{k-1} j\gamma_j \right) \end{aligned}$$

con λ_j y $\gamma_j \in \mathbb{N}$, entonces debe cumplirse en particular que $\sum_{j=0}^{k-1} \gamma_j = -1$, lo cual es absurdo teniendo en cuenta la procedencia de los elementos γ_j. Así pues, $2k+j-n \notin \langle S \rangle$. Por último, sea $1 \leq i \leq k-1$ con i impar. Entonces si suponemos que $n + 4k + i - n$

admite representarse como

$$\begin{aligned} 4k+i &= \gamma_0 n + \sum_{j=1}^{k-1} \gamma_j (n+k+j) + \sum_{j=1}^{\frac{k}{2}} \lambda_j (2(k+j)) \\ &= n\left(\sum_{j=0}^{k-1} \gamma_j\right) + k\left(\sum_{j=1}^{\frac{k}{2}} 2\lambda_j + \sum_{j=1}^{k-1} \gamma_j\right) + \left(\sum_{j=1}^{\frac{k}{2}} 2j\lambda_j + \sum_{j=1}^{k-1} j\gamma_j\right) \end{aligned}$$

para algunos $\lambda_i s'$ y $\gamma_i s' \in \mathbb{N}$ no todos ceros, entonces debe constatarse las igualdades

$$\sum_{j=0}^{k-1} \gamma_j = 0, \qquad \sum_{j=1}^{\frac{k}{2}} \lambda_j = 2, \qquad \text{y} \qquad \sum_{j=1}^{\frac{k}{2}} 2j\lambda_j + \sum_{j=1}^{k-1} j\gamma_j = i. \tag{3.19}$$

De (3.19) se garantiza la existencia de algún $\lambda_j \neq 0$ y el hecho de que $\gamma_j = 0$ para todo j. Por lo tanto, la última igualdad de (3.19) establece que $\sum_{j=1}^{\frac{k}{2}} 2j\lambda_j = i$, lo cual es una contradicción con la paridad de i. Como consecuencia de lo anterior se prueba que $A = \mathrm{Ap}(\langle S \rangle; n)$. Ahora mostremos seguidamente que $g_S = g$. En efecto, por la Proposición 1.23,

$$\begin{aligned} g_S &= \frac{1}{n}\left(\sum_{j=1}^{k-1} [n+k+j] + \sum_{j=1}^{\frac{k}{2}} [2(k+j)] + \sum_{j=1}^{\frac{k}{2}} [n+4k+(2j-1)]\right) - \frac{n-1}{2} \\ &= \frac{1}{n}\left(n(k-1) + k(k-1) + \frac{k(k-1)}{2} + k^2 + \frac{k(k+2)}{4} + \frac{nk}{2} + 2k^2 + \frac{k^2}{4}\right) - \frac{n-1}{2} \\ &= \frac{1}{n}\left((k-1)\left(n+k+\frac{k}{2}\right) + k\left(k + \frac{k+2}{4} + \frac{n}{2} + 2k + \frac{k}{4}\right)\right) - \frac{n-1}{2} \\ &= \frac{1}{n}\left((k-1)\left(n+\frac{3k}{2}\right) + k\left(\frac{7k}{2} + \frac{n}{2} + \frac{1}{2}\right)\right) - \frac{n-1}{2} \\ &= \frac{1}{n}\left(5k^2 + \frac{3kn}{2} - k - n\right) - \frac{n-1}{2} = \frac{8k^2-3k}{2k} - \frac{2k-1}{2} = 3k-1 = g \end{aligned}$$

como se deseaba. □

Ejemplo 3.17. Consideremos la extensión de Kummer $y^8 = (x-1)^4 x(x-2)$ sobre $\mathbb{F}_{11}$. Calculemos bases para los espacios de Riemann-Roch $\mathscr{L}(10Q)$ y $\mathscr{L}(9Q)$ siendo Q un lugar que extiende al lugar P_∞.

Por el Teorema 3.16, el semigrupo de Weierstrass asociado a los lugares Q_{∞_i} está dado por $H = \langle 4, 6, 7\rangle$ y por lo tanto, el conjunto de gaps es $G = \{1, 2, 3, 5, 9\}$. Definiendo $s_1 := |\{x \in H : x \leq 10\}|$ y $s_2 := |\{x \in H : x \leq 9\}|$; y observando que 10 es un número polo y 9 es un número gap, la Proposición 1.40 establece que

$$\ell(10Q_{\infty_1}) = s_1 = 6 \quad \text{y} \quad \ell(9Q_{\infty_1}) = s_2 = 5.$$

Para exhibir una base de estos espacios vectoriales, primeramente consideremos los conjuntos

$$T_1 := \{z_j \in F : (z_j)_\infty^F = n_j Q_{\infty_1} \text{ con } n_j \in \mathbb{N} \text{ y } n_j \leq 10\}$$

y

$$T_2 := \{z_j \in F : (z_j)_\infty^F = n_j Q_{\infty_1} \text{ con } n_j \in \mathbb{N} \text{ y } n_j \leq 9\}.$$

Estamos buscando elementos $z_j \in F$ que garantizan que n_j se encuentre en H. De acuerdo con T_1, las posibilidades para n_j son $n_j = 0, 4, 6, 7, 8, 10$. Así pues, empleando de nuevo el Teorema 3.16 se puede decir que haciendo $\theta_1 := \dfrac{y^4}{(x-1)^2} - x$, $\theta_2 := \dfrac{y^4}{(x-1)^2} + x$, $\theta_3 := x - 1$ y $\theta_4 := y$ se tiene

$$z_1 = 1, \qquad z_2 = \theta_1(\theta_2)^{-1}(\theta_3)^{-2}(\theta_4)^4, \qquad z_3 = \theta_1(\theta_2)^{-1}(\theta_3)^{-1}(\theta_4)^2, \quad ,$$

$$z_4 = \theta_1(\theta_2)^{-1}\theta_4, \quad z_5 = \theta_1(\theta_2)^{-1}, \quad z_6 = \theta_1(\theta_2)^{-1}(\theta_3)^{-3}(\theta_4)^6$$

con lo cual

- $v_{Q_{\infty_1}}(z_1) = 0$
- $v_{Q_{\infty_1}}(z_2) = -8$
- $v_{Q_{\infty_1}}(z_3) = -6$
- $v_{Q_{\infty_1}}(z_4) = -7$
- $v_{Q_{\infty_1}}(z_5) = -4.$
- $v_{Q_{\infty_1}}(z_6) = -10$

En consecuencia, una base para $\mathscr{L}(10Q_{\infty_1})$ es $B = \{z_1, z_2, z_3, z_4, z_5, z_6\}$. De igual modo, teniendo presente T_2 las opciones para n_j son $n_j = 0, 4, 6, 7, 8$ por lo que conservando la notación anterior $B = \{z_1, z_2, z_3, z_4, z_5\}$ es una base para $\mathscr{L}(9Q_{\infty_1})$.

Ejemplo 3.18. De acuerdo al código

```
K<x>:= FunctionField ((GF(11)));
```

```
P<t>:=PolynomialRing(K);
F<y>:=FunctionField(t^8-(x-1)^4*x*(x-2));
print "Numero de lugares racionales de K(x)/K";
u:= NumberOfPlacesDegECF(K, 1);
u;
print "Lugares racionales de K(x)/K";
Places(K,1);
O:=Places(K,1);
print "Lugar Infinito de K(x)/K";
D:=O[1];
D;
print "genero del cuerpo K(x,y)/K";
Genus(F);
print "Numero de lugares racionales de K(x,y)/K";
n:= NumberOfPlacesDegECF(F, 1);
n;
print "Lugares racionales de K(x,y)/K";
Places(F,1);
L:=Places(F,1);
print "Lugares que extienden al Polo de x";
W:=Decomposition(F, D);
W;
```

ejecutado en MAGMA, tenemos que los lugares racionales del cuerpo de funciones dado en el ejemplo anterior son:

$$Q_{\infty 1} := \left(\frac{1}{x}, \frac{5y^4}{x^3} + \frac{y}{x} + 6\right), \quad Q_{\infty 2} := \left(\frac{1}{x}, \frac{6y^4}{x^3} + \frac{y}{x} + 6\right), \quad P_1 := (x, y), \quad P_2 := (x + 9, y),$$

$$P_3 := (x + 3, y + 1), \quad P_4 := (x + 3, y + 10), \; P_5 := (x + 6, y + 1), \; P_6 := (x + 6, y + 10),$$

$$P_7 := (x + 1, y + 5), \quad P_8 := (x + 1, y + 6), \; P_9 := (x + 8, y + 5), \; P_{10} := (x + 8, y + 6).$$

Si consideramos el código unipuntual $\mathcal{C}_{\mathscr{L}}(D, G)$ sobre $\mathbb{F}_{11}$, donde $G := 9Q_{\infty 1}$, y $D :=$

$\sum_{i=1}^{10} P_i$ se tiene que $\deg G < n = 10$, luego el Teorema 1.51 determina que la dimensión del código $\mathcal{C}_{\mathscr{L}}(D, G)$ sobre $\mathbb{F}_{11}$ es $k = 5$. Denotando por $1(P_j) := a_{1j}$ y $z_i(P_j) = a_{ij}$ donde $1 \leq j \leq 10$ e $2 \leq i \leq 5$, la matriz

$$A = (a_{ij}) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 7 & 7 & 1 & 1 & 2 & 2 & 4 & 4 \\ 0 & 0 & 5 & 5 & 4 & 4 & 6 & 6 & 10 & 10 \\ 0 & 0 & 9 & 2 & 6 & 5 & 9 & 2 & 7 & 4 \\ 1 & 10 & 2 & 2 & 5 & 6 & 7 & 7 & 3 & 3 \end{bmatrix}$$

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

Dentro de nuestro análisis identificamos que para $k = 1, 2$; el conjunto H puede describirse explícitamente. A continuación presentamos los hechos relacionados aquí:

Proposición 3.19. *Si $k = 1$ en* (3,1), *entonces*

$$H = \langle n, n+2, n+4, n+6, \cdots, 2n-1 \rangle. \tag{3.20}$$

Demostración. Definamos $S := \{n, n+2, n+4, n+6, \cdots, 2n-1\}$. Debemos verificar que $\langle S \rangle \subseteq H$ y que $g_S = g$. Para lo primero consideremos el divisor principal del elemento $(ab^{-1}y^i)$ con $0 \leq i \leq \dfrac{n-1}{2}$. Entonces,

$$\begin{aligned} (ab^{-1}y^i)^F &= (a)^F - (b)^F + i(y)^F \\ &= nP'' - nQ_{\infty 1} - nP'' + nQ_{\infty 2} + i(P_1' + P_2' + P'' + P''' - 2Q_{\infty 1} - 2Q_{\infty 2}) \\ &= nQ_{\infty 2} - nQ_{\infty 1} + i(P_1' + P_2') + iP'' + iP''' - 2iQ_{\infty 1} - 2iQ_{\infty 2} \\ &= i(P_1' + P_2') + iP'' + iP''' + (n-2i)Q_{\infty 2} - (n+2i)Q_{\infty 1}, \end{aligned}$$

de ahí que $n+2i \in H$ para $0 \leq i \leq \dfrac{n-1}{2}$, luego como H tiene estructura de semigrupo concluimos que $\langle S \rangle \subseteq H$. Para lo segundo, afirmamos que el conjunto Apéry de $\langle S \rangle$ con

respecto a n está dado por $A = \{0\} \cup A_1 \cup A_2$, donde

$$A_1 := \left\{ n + 2i : 1 \leq i \leq \frac{n-1}{2} \right\} \quad \text{y} \quad A_2 := \left\{ 3n + (2i-1) : 1 \leq i \leq \frac{n-1}{2} \right\}.$$

Efectivamente, veamos que $A \subseteq \langle S \rangle$, A tiene n elementos diferentes módulo n y si $x \in A$, entonces $x - n \notin \langle S \rangle$. Es evidente que $A_1 \subseteq \langle S \rangle$. Asímismo, dado que

$$3n + i = 2n - 1 + n + (i+1)$$

con $i \in \{1, 3, 5, \cdots, n-4, n-2\}$, se establece la inclusión $A_2 \subseteq \langle S \rangle$, y por consiguiente que $A \subseteq \langle S \rangle$. Ahora bien, sean $i, j \in \{2, 4, 6, \cdots, n-3, n-1\}$. Entonces

$$n + i \equiv n + j \pmod{n} \text{ sii } i \equiv j \pmod{n} \text{ sii } i = j \text{ porque } i, j < n.$$

De forma análoga, para $i, j \in \{1, 3, 5, \cdots, n-4, n-2\}$ tenemos

$$3n + i \equiv 3n + j \pmod{n} \text{ sii } i \equiv j \pmod{n} \text{ sii } i = j \text{ puesto que } i, j < n.$$

Por último, también note que si $2 \leq i \leq n-1$ es par y $1 \leq j \leq n-2$ es impar se cumple

$$n + i \equiv 3n + j \pmod{n} \text{ sii } i \equiv j \pmod{n} \text{ sii } i = j \text{ pues } i, j < n.$$

Consecuentemente podemos decir que A esta formado por n elementos distintos módulo n. Acto seguido probemos que $x \in A$ implica que $x - n \notin \langle S \rangle$. Para comenzar supongamos que para $1 \leq i \leq \dfrac{n-1}{2}$ fijo, existen $\lambda_0, \lambda_1, \cdots, \lambda_{\frac{n-1}{2}} \in \mathbb{N}$ no todos ceros tales que

$$n + 2i - n = 2i = \sum_{j=0}^{\frac{n-1}{2}} [\lambda_j (n + 2j)] = n \sum_{j=0}^{\frac{n-1}{2}} \lambda_j + 2 \sum_{j=0}^{\frac{n-1}{2}} j\lambda_j,$$

luego debe cumplirse $\lambda_0 = \lambda_1 = \cdots = \lambda_{\frac{n-1}{2}} = 0$, una contradicción. De igual manera, si suponemos que para i fijo con $1 \leq i \leq \dfrac{n-1}{2}$; existen $\beta_0, \beta_1, \cdots, \beta_{\frac{n-1}{2}} \in \mathbb{N}$ no todos

ceros que satisfacen la combinación lineal

$$3n+(2i-1)-n=2n+2i-1=\sum_{j=0}^{\frac{n-1}{2}}[\beta_j(n+2j)]=n\sum_{j=0}^{\frac{n-1}{2}}\beta_j+2\sum_{j=0}^{\frac{n-1}{2}}j\beta_j,$$

entonces debe tenerse

$$\sum_{j=0}^{\frac{n-1}{2}}\beta_j=2 \text{ y } \quad 2\sum_{j=0}^{\frac{n-1}{2}}j\beta_j=2i-1. \tag{3.21}$$

Observando que la última igualdad de (3.21) es absurda, se infiere que $A=\mathrm{Ap}(\langle S\rangle;n)$, y así la Proposición 1.23 permite concluir que

$$\begin{aligned} g_S &= \frac{1}{n}\left(\sum_{j=1}^{\frac{n-1}{2}}[n+2j]+[3n+(2j-1)]\right)-\frac{n-1}{2}=\frac{1}{n}\left(\sum_{j=1}^{\frac{n-1}{2}}[4n+4j-1]\right)-\frac{n-1}{2} \\ &= \left(2(n-1)+\frac{n^2-1}{2n}-\frac{n-1}{2n}\right)-\frac{n-1}{2}=\frac{5(n-1)}{2}-\frac{n-1}{2}=2n-2=g \end{aligned}$$

□

Antes de enunciar el resultado cuando $k=2$ en (3.1) debemos enunciar la siguiente proposición.

Proposición 3.20. *Consideremos la extensión de Kummer*

$$y^{2n}=(x-\alpha_1)^{2k}x(x-\alpha_2)$$

con $d=(n,k),(n,k+1)=1$ *y* $n>2$.

a) Si i *es un entero positivo tal que* $n-ik-i\geq 0$, *entonces* $n+ik+i\in H$.

b) Si i *es un entero positivo con* $ik-n\geq 0$ *y* $2n-ik-i\geq 0$, *entonces* $ik+i\in H$.

Demostración.

a) El divisor principal del elemento $y^i ab^{-1}$ está dado por

$$\begin{aligned}(y^i ab^{-1})^F &= i\frac{k}{d}(P_1' + \cdots + P_{2d}') + iP'' + iP''' - i(k+1)Q_{\infty 1} - i(k+1)Q_{\infty 2} \\ &+ nP'' - nQ_{\infty 1} - nP'' + nQ_2 \\ &= \frac{ik}{d}(P_1' + \cdots + P_{2d}') + iP'' + iP''' + (n - ik - i)Q_{\infty 2} - (n + ik + i)Q_{\infty 1}.\end{aligned}$$

Como $n - ik - i \geq 0$, se establece que $n + ik + i \in H$.

b) Del mismo modo, calculando el divisor principal del elemento $y^i ab^{-1}(x - \alpha_1)^{-1}$ obtenemos

$$\begin{aligned}(y^i ab^{-1}(x - \alpha_1)^{-1})^F &= \left(\frac{ik - n}{d}\right)(P_1' + \cdots + P_{2d}') + iP'' + iP''' + (2n - ik - i)Q_{\infty 2} \\ &- (ik + i)Q_{\infty 1}.\end{aligned}$$

Debido a que $ik - n \geq 0$ y $2n - ik - i \geq 0$ se sigue lo requerido.

□

Como consecuencia de la proposición anterior tenemos el siguiente corolario.

Corolario 3.21. *Supongamos que $k = 2$ en* (3,1)*. Entonces*

$$\langle n, n+3, n+6, \cdots, n+3(i-1), n+3i, 3j_1, 3j_2, 3j_3, 3j_4, \cdots, 3j\rangle \subseteq H,$$

donde $i := \text{máx}\{s \in \mathbb{Z}_+ : n - 2s - s \geq 0\}$, $j_1 := \text{mín}\{s \in \mathbb{Z}_+ : 2s - n \geq 0\}$, $j := \text{máx}\{s \in \mathbb{Z}_+ : 2n - 2s - s \geq 0\}$ *y* $j_2 \leq j_3 \leq j_4 \leq \cdots \leq j$ *son números naturales consecutivos mayores que* j_1 *y menores o iguales que* j*.*

Es importante decir que el corolario anterior no garantiza la igualdad para el conjunto H. No obstante, si se implementa el uso del software GAP, este corolario da paso a una conjetura. Llegando a este punto se puede decir que la dificultad radica en el hecho de no poder encontrar una expresión que permita determinar el género del semigrupo en cuestión.

Conjetura 3.22. *Dada la extensión de Kummer*

$$y^{2n} = (x - \alpha_1)^4 x(x - \alpha_2)$$

con $d = (n, 2), (n, 3) = 1$ *y* $n > 2$,

$$H = \langle n, n+3, n+6, \cdots, n+3(i-1), n+3i, 3j_1, 3j_2, 3j_3, 3j_4, \cdots, 3j \rangle,$$

siendo $i := \text{máx}\{s \in \mathbb{Z}_+ : n - 2s - s \geq 0\}$, $j_1 := \text{mín}\{s \in \mathbb{Z}_+ : 2s - n \geq 0\}$, $j := \text{máx}\{s \in \mathbb{Z}_+ : 2n - 2s - s \geq 0\}$ *y* $j_2 \leq j_3 \leq j_4 \leq \cdots \leq j$ *números naturales consecutivos mayores que* j_1 *y menores o iguales que* j.

Ejemplo 3.23. Calculemos el semigrupo de Weierstrass H con respecto a la extensión de Kummer $y^{22} = (x-1)^4 x(x-2)$ definida sobre $\mathbb{F}_5$.
El género de esta extensión de cuerpos de funciones es $g = 20$ de acuerdo con la Proposición 3.1. Siguiendo la escritura del Corolario 3.21 tenemos $n = 11$, por lo que $i = 3$, $j_1 = 6$ y $j = 7$. Note que en este caso $j_2 = j$. En ese orden de ideas,

$$S := \langle 11, 11+3, 11+6, 11+9, 3 \cdot 6, 3 \cdot 7 \rangle = \langle 11, 14, 17, 20, 18, 21 \rangle \subseteq H.$$

Por otra parte, si empleamos el sofware GAP y ejecutamos el código

```
gap> LoadPackage("NumericalSgps");
gap> s:=NumericalSemigroup(11,14,17,20,18,21);
<Numerical semigroup with 6 generators>
gap> Genus(s);
20
```

encontramos que S tiene género 20, de donde se infiere entonces que la inclusión previa realmente corresponde a una igualdad, y por consiguiente

$$H = \langle 11, 14, 17, 20, 18, 21 \rangle.$$

Ejemplo 3.24. Determine el semigrupo de Weierstrass H con respecto a la extensión

de Kummer $y^{38} = (x-3)^4 x(x-7)$ definida sobre $\mathbb{F}_{11}$.
Como antes, en virtud de la Proposición 3.1 el género de esta extensión de cuerpos de funciones es $g = 36$. Continuando con la notación del Corolario 3.21 tenemos $n = 19$, por lo que $i = 6$, $j_1 = 10$ y $j = 12$. En este caso $j_2 = 11$ y por tal razón,

$$\begin{aligned} S: &= \langle 19, 19+3, 19+6, 19+9, 19+12, 19+15, 19+18, 3\cdot 10, 3\cdot 11, 3\cdot 12\rangle \\ &= \langle 19, 22, 25, 28, 31, 34, 37, 30, 33, 36\rangle \subseteq H. \end{aligned}$$

Por otra parte, el código

```
gap> LoadPackage("NumericalSgps");
gap> s:=NumericalSemigroup(19,22,25,28,31,34,37,30,33,36);
<Numerical semigroup with 10 generators>
gap> Genus(s);
36
```

programado en el software GAP, muestra que S tiene género 36 con lo cual se obtiene la igualdad en la inclusión anterior y en consecuencia

$$H = \langle 19, 22, 25, 28, 31, 34, 37, 30, 33, 36\rangle.$$

Capítulo **4**

Conclusiones

Esperamos que este trabajo de investigación sirva como un primer avance en lo que respecta a la busquedad de la descripción del semigrupo de Weierstrass correspondiente a las extensiones del lugar infinito de $K(x)$ cuando se omite la condición de ramificación en extensiones de Kummer. Asímismo, esperamos que aquellas personas interesadas en este tipo de problemas puedan aportar un poco más de información a la suscitada aquí, puesto que actualmente se conoce muy poca al respecto.

Inicialmente el objetivo del trabajo era muy ambicioso, pues tal como se mencionó en la introducción, en la literatura ya existe un trabajo en el cual la extensión de Kummer $F/K(x)$ dada por la igualdad

$$y^m = \prod_{i=1}^{r} (x - \alpha_i)^{\lambda_i},$$

con $\lambda_i \in \mathbb{N}$, $1 \leq \lambda_i < m$ donde $m, r \geq 2$ son enteros positivos tales que $(m, q) = 1$, $\alpha_1, \cdots, \alpha_r$ son elementos distintos por pares, $\lambda_0 := \sum_{i=1}^{r} \lambda_i$ y $(m, \lambda_0) = 1$, tiene explícitamente descrito el semigrupo de Weierstrass $H(Q_\infty)$ asociado al unicó lugar Q_∞ que extiende al lugar P_∞ de $K(x)$, esto es, cuando P_∞ es totalmente ramificado. Surge entonces la pregunta natural de si es posible de alguna manera obtener un resultado similar cuando se elimina la condición de ramificación total.

Es así como en esta dirección se comienza a estudiar algunos casos particulares en donde

$(m, \lambda_0) \neq 1$ llegándose a concluir lo siguiente:

- Desafortunadamente, este problema continúa siendo de una complejidad considerable, pues durante la busquedad de funciones generadoras que permiten establecer que un número $s \in H$, evidenciamos que este proceso depende en gran medida de la escritura de la ecuación, dado que de entrada es necesario realizar un estudio no trivial que identifique la existencia de dos elementos que son determinantes al momento de construir la función generadora.

- El problema general se particularizó en especial a la familia de ecuaciones (3,1) como consecuencia del hecho de que en este contexto se pudieron realizar ciertas manipulaciones algebraicas que permitieron identificar dos elementos a y b de tal manera que el lugar $Q_{\infty i}$ con $i = 1, 2$ no sea un polo de manera simultánea de estos. El resultado se siguió ejecutándose un arreglo de diferencia de cuadrados.

- Teniendo en cuenta la manera en que fue abordado el problema de encontrar el semigrupo de Weierstrass asociado a las extensiones de P_∞ con respecto al cuerpo de funciones (3.1), podemos decir que el conjunto Apéry es muy necesario para dar respuesta a esto, pues utilizando la Proposición 1.23, se pudo conocer el género del semigrupo numérico en cuestión.

- El cálculo del género de un semigrupo numérico generado por n elementos es un problema propio de la teoría de semigrupos. Se puede dar respuesta a esta cuestión siempre que conozcamos el conjunto Apéry de manera explícita. Sin embargo hubo un caso en donde el conocimiento de este conjunto se hizo muy dificil por la estructura interna del semigrupo. Así las cosas, logramos conjeturar gracias al software GAP, la igualdad del semigrupo de Weierstrass en el cuerpo de funciones dado por la ecuación de Kummer $y^{2n} = (x - \alpha_1)^4 x(x - \alpha_2)$ con $n \in \mathbb{N}$ y $\alpha_1, \alpha_2 \in K$ elementos diferentes.

- Si conocemos el semigrupo de Weierstrass asociado a un lugar racional P, podemos determinar la dimensión del divisor nP con $n \in \mathbb{N}$. Llegando a este punto, es bueno aclarar que si bien, el Teorema de Riemann-Roch nos brinda una manera

de estimar las dimensiones de cualquier divisor, el hecho de clasificar a n como un número polo o gap de P, muestra que este cálculo en particular puede tratarse utilizando teoría de semigrupos numéricos.

- Los semigrupos numéricos también nos proporcionan información para la busqueda de bases del espacio de Riemman-Roch $\mathscr{L}(nQ)$. Definiendo $s := |\{x \in H(Q) : x \leq n\}|$ se tiene $s = \ell(nQ)$.

  1. Si $n \in H$, consideramos elementos z_j tales que $(z_j)_\infty^F = n_j Q$ con $n_j \leq n$. El conjunto $B := \{z_1, z_2, \cdots, z_s\}$ es una base para el espacio de Riemann-Roch $\mathscr{L}(nQ)$.
  2. Si *n es un número gap de Q,* consideramos elementos z_j tales que $(z_j)_\infty^F = n_j Q$ con $n_j \leq n$. Entonces el conjunto $B := \{z_1, z_2, \cdots, z_s\}$ constituye una base para el espacio de Riemann-Roch $\mathscr{L}(nQ)$.

  En esta parte es bueno resaltar que los códigos unipuntuales, pueden describirse por medio de sus matrices generadoras gracias a lo anterior.

- Para un futuro trabajo se espera poder abordar nuevamente el problema desde un punto de vista más general. Empleando el software MAGMA se pudo observar que muchas veces existe un patrón entre los elementos generadores del semigrupo. El impedimiento para encontrar un resultado desde un punto de vista analítico fue precisamente la dificultad de describir el conjunto Apéry de tales semigrupos y por consiguiente su género.

Bibliografía

[1] S. Roman, *Field Theory*. Graduate Texts in Mathematics, 158. Second edition, Springer, New York, págs 41-66, 2006.

[2] Erik A. R. Mendoza (2022). *On kummer extensions with one place at infinity.*

[3] Gretchen L. Matthews *Weierstrass Pairs and Minimum Distance of Goppa Codes* Louisiana State University and Agricultural - Mechanical College.

[4] Henning Stichtecnoth (2009). *Algebraic Function Field and Codes. Springer-Verlag, Berlin.*

[5] J. L. Ramírez Alfonsín (2005). *The Diophantine Frobenius Problem*, Oxford University Press.

[6] Mosquera Hernandez, L. (2021). *Códigos algebro-geométricos de Goppa.*

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

[8] J.C. Rosales, P.A. Garcia-Sánchez (2009). *Numerical Semigroups,* Springer New York Dordrecht Heidelberg London.

[9] J. Lewittes. *Places of degree one in function fields over finite fields.* J. Pure Appl. Algebra, 69(2):177–183, 1990.

[10] O. Geil and R. Matsumoto. *Bounding the number of $\mathbb{F}_q$-rational places in algebraic function fields using Weierstrass semigroups.* J. Pure Appl. Algebra, 213(6):1152–1156, 2009.