Semigrupos deWeierstrass en Extensiones de Kummer con más de un lugar en el infinito

Luis Felipe Mosquera Hernández
Departamento de Matemáticas
Universidad del Valle, Cali, Colombia.

Universidad del Valle

REVISTA DE CIENCIAS

Recibido: 13-06-2025
Aceptado: 19-02-2026

ORCID Luis Felipe Mosquera Hernández
0000-0001-6972-9607

Resumen

Al considerar extensiones de Kummer *F/K(x)* donde el lugar *P∞* no está completamenteramificado, el problema de encontrar el semigrupo de Weierstrass asociado a un lugar de *F* que extiende *P∞* es una cuestión abierta en la teoría de cuerpos de funciones, para la cual se conoce muy poca información. La dificultad radica en que no existe una forma general de encontrar funciones generadoras con un polo de un orden específico, ya que el cálculo de estos semigrupos depende en gran medida de la ecuación que define la extensión. En este artículo de investigación, se calcula explícita mente el semigrupo de Weierstrass correspondiente a las extensiones de *P∞* de una familia particular de extensiones de Kummer.

Palabras clave: Semigrupos numéricos, conjunto de Apéry, género, campo funcional, extensiones de Kummer, lugar, índice de ramificación, espacio de Riemann-Roch.

Abstract

When considering Kummer extensions F/K(x) in which the place P∞ is not totally ramified, the problem of determining the Weierstrass semigroup associated with a place of F lying above P∞ remains an open question in the theory of function fields, with only limited results available in the literature. This difficulty arises from the lack of a general method to construct generating functions having poles of prescribed order, since the computation of such semigroups depends strongly on the defining equation of the extension. In this research article, we explicitly determine the Weierstrass semigroup corresponding to the extensions of P∞ for a specific family of Kummer extensions.

Keywords: Numerical semigroups; Apéry sets; genus; function field; Kummer extensions; place; ramification index; Riemann–Roch space.

Citación sugerida:
Mosquera-Hernández, L. F. (2026). Semigrupos de Weierstrass en Extensiones de Kummer con más de un lugar en el infinito. Revista de Ciencias, 29(1): e20214997. https://doi.org/10.25100/rc.v29i1.14997

1. Introducción

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 ellas la búsqueda de cotas superiores para el número de lugares racionales, como los encontrados por Lewittes [**9**] y Geil-Matsumoto [**10**], y la construcción de códigos algebro geométricos con buenos parámetros sobre cuerpos finitos. Para esto último, el Teorema de Riemann-Roch proporciona estimaciones para calcular la dimensión y la distancia mínima del código, y en muchos casos concretos, dichas determinaciones también pueden abordarse desde la perspectiva de semigrupos numéricos.

En el artículo [**2**], Mendoza consideró extensiones de Kummer donde el lugar P_∞ de $K(x)$ está completamente ramificado y, para este lugar, proporcionó una descripción explícita de su semigrupo de Weierstrass y su conjunto de gaps. En este artículo, estudiamos el semigrupo de Weierstrass de una familia particular de extensiones de tipo Kummer donde el lugar P_∞ no está completamente ramificado. Comenzamos enunciando algunos resultados importantes.

Definición 1. *Sea S un semigrupo numérico y $n \in S - \{0\}$, el conjunto,*

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

se denomina el **conjunto de apéry** *de n en S.*

Lema 2. *Sea S un semigrupo numérico y $n \in S - \{0\}$, entonces,*

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

donde

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

en particular, este conjunto tiene n elementos.

Proposición 3. *Sea S un semigrupo numérico $\cdots \in S - \{0\}$, entonces*

a) El número de Frobenius de S es $F(S) = \max\{\mathrm{Ap}(S;n)\} - n$.

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

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

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

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

Para un polinomio mónico e irreducible $p(x) \in K[x]$, se define el anillo de valuación en $K(x)/K$

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \nmid g(x) \right\}. \tag{1}$$

Este anillo es local con ideal máximal

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \mid f(x), p(x) \nmid g(x) \right\}. \tag{2}$$

Al conjunto anterior se le llama ***lugar*** de $\mathcal{O}_{p(x)}$. Existe otro anillo de valuación en $K(x)/K$, a saber

$$\mathcal{O}_{\infty} := \left\{ \frac{f(x)}{g(x)} : \deg f(x) \leq \deg g(x) \right\} \tag{3}$$

cuyo ideal maximal es

$$P_{\infty} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], \deg f < \deg g(x) \right\}. \tag{4}$$

Este conjunto es llamado el ***lugar infinito*** de $K(x)/K$.

Suponga que K es la clausura algebraica de $\mathbb{F}_q$ donde $\mathbb{F}_q$ es el cuerpo finito con $q = p^s$ elementos, $s \in \mathbb{N}$ y p un número primo. Considere sobre K la extensión de cuerpo de funciones $F/K(x)$ dada por la ecuación,

$$y^{2n} = (x - \alpha_1)^{2k} x(x - \alpha_2), \tag{5}$$

donde $\alpha_1, \alpha_2 \in K$ son elementos distintos de cero, n, k son enteros positivos tales que $2n$ no es divisible por p, $n > 1, n > k$, $d = (n, k)$ y $(n, k + 1) = 1$. Sobre este cuerpo de funciones P_{∞} no está totalmente ramificado, ya que si $Q_{\infty}|P_{\infty}$, entonces por la Proposición 3.7.3 de [**4**] se tiene $e(Q_{\infty}|P_{\infty}) = \dfrac{n}{(n, k+1)} = n$, de hecho sólo hay dos lugares de F que están en P_{∞}, más exactamente de (5) se tiene,

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

entonces si consideramos el polinomio

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

y hacemos reducción módulo P_{∞}, se obtiene,

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

Por lo tanto, El Teorema de Kummer [1] establece que solo hay dos polos de F, digamos, $Q_{\infty 1}, Q_{\infty 2}$ que se encuentran en P_{∞}. Además, $f(Q_{\infty i}|P_{\infty}) = 1$ para $i = 1, 2,$, por lo que

$$\deg(Q_{\infty i}) = [F_{Q_{\infty i}} : K] = [F_{Q_{\infty i}} : F_{P_{\infty}}][F_{P_{\infty}} : K] = 1 \cdot 1 = 1.$$

Para calcular el índice de ramificación correspondiente a los lugares $P_{x-\alpha_1}, P_x$ y $P_{x-\alpha_2}$ de $K(x)$, se procede como sigue.

[1] Teorema 3.3.7 de [**4**]

Suponga que $P'|P_{x-\alpha_1}, P''|P_x$ y $P'''|P_{x-\alpha_2}$, entonces

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

entonces los lugares P_x y $P_{x-\alpha_2}$ están totalmente ramificados en F. Para el polo $P_{x-\alpha_1}$ de (5) se sigue,

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

tal que definiendo $\varphi(T) := T^{2d} - x(x-\alpha_2)$ y reduciendo módulo $P_{x-\alpha_1}$ en 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, se tiene que el polinomio anterior es separable y en consecuencia el Teorema de Kummer establece que existen exactamente $2d$ lugares de F sobre $P_{x-\alpha_1}$, que se identifican por, $P'_1, P'_2, \cdots, P'_{2d}$ con $\deg P'_i = 1$ para $i = 1, 2, \cdots, 2d$.

De acuerdo con lo anterior, se desarrolla el cálculo de algunos de los divisores principales del cuerpo de funciones dado por (5). Para este propósito, se utiliza la Proposición 3.1.9 de [**4**], obteniendo:

$$\begin{aligned} (x-\alpha_1)^F &= \frac{n}{d}(P'_1 + \cdots + P'_{2d}) - n(Q_{\infty 1} + Q_{\infty_2}) \\ (x-\alpha_2)^F &= 2nP''' - n(Q_{\infty 1} + Q_{\infty_2}) \\ (x)^F &= 2nP'' - n(Q_{\infty_1} + Q_{\infty_2}), \end{aligned} \tag{6}$$

y

$$(y)^F = \frac{k}{d}(P'_1 + \cdots + P'_{2d}) + P'' + P''' - (k+1)(Q_{\infty_1} + Q_{\infty_2}). \tag{7}$$

Por ejemplo, para ver la última igualdad se procede de la siguiente manera.

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

de donde se obtiene

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

Proposición 4. *El género g del cuerpo de funciones dado por* (5) *es*

$$g = 2n - d - 1.$$

Demostración. Note que cualquier lugar en $K(x)/K$ distinto de los lugares mencionados anteriormente

no está ramificado, por lo que, por la Proposición 3.7.3 (c) de [**4**], 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 con los lugares $Q_{\infty 1}$ y $Q_{\infty 2}$ de F. Dependiendo de las condiciones en n y k; se busca describir este conjunto.

Proposición 5. *Considere el cuerpo de funciones dado por* (5) *y el conjunto* $S := \{n, n+k+1\}$, *entonces* $S \subseteq H$ *y* $\langle S\rangle \subseteq H$.

Demostración. La relación (5) se puede reescribir en la forma,

$$\underbrace{\left(\frac{y^n}{(x-\alpha_1)^k}-x\right)}_{a}\underbrace{\left(\frac{y^n}{(x-\alpha_1)^k}+x\right)}_{b} = -x\alpha_2, \tag{8}$$

con que

$$v_{Q_{\infty i}}(a)^F + v_{Q_{\infty i}}(b)^F = -n, \tag{9}$$

para $i \in \{1,2\}$ fijo. Además,

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

entonces

$$v_{Q_{\infty i}}(a) \geq -n \text{ y } v_{Q_{\infty i}}(b) \geq -n. \tag{10}$$

Además, como $a+b = \dfrac{2y^n}{(x-\alpha_1)^k}$, se obtiene

$$-n \geq \text{mín}\{v_{Q_{\infty i}}(a), v_{Q_{\infty i}}(b)\}. \tag{11}$$

Entonces, de (9), (10) y (11), para $i \in \{1,2\}$ hay dos 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.

Dado que

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

se tiene $v_{P''}(a) = n$ 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, decimos que,

$$(a)^F = nP'' - nQ_{\infty 1} \tag{12}$$

y

$$(b)^F = nP'' - nQ_{\infty 2}, \tag{13}$$

demostrando así que $n \in H$.

Para completar la demostración, considere el divisor principal del elemento $yab^{-1} \in F$. Por lo tanto,

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

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

Observación 6. Es de resaltar que conocer la existencia de los elementos a y b de F que satisfacen (12) y (13) es muy importante, ya que las funciones generadoras están en términos de ellos. Asímismo es de notar que determinar su existencia no es sencillo, ya que depende en gran medida de la ecuación que define la extensión del cuerpo $F/K(x)$ del cuerpo de funciones racionales $K(x)/K$.

Bajo hipótesis adicionales para n y k, se obtienen algunos resultados.

Para comenzar note que si $d = 1$, entonces $(n, k) = 1$ y $(n, k+1) = 1$ implican que n es un número impar.

Teorema 7. *Si $d = 1$ en (5), entonces $H = \langle n, n+k+1\rangle$ si y solo si $n + k = 4$.*

Observación 8. El teorema 7 es falso si $d \neq 1$, ya que si $H = \langle n, n+k+1\rangle$, entonces $g = g_S$, es decir,

$$\frac{(n-1)(n+k)}{2} = 2n - d - 1. \tag{14}$$

Considerando la naturaleza de los números g, n y k, la igualdad (14) implica que d es tanto par como impar, lo cual es imposible.

Ejemplo 9. *Considere 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 10. *Si en (5), $n < 2k$, entonces*

$$S := \{n, n+k+1, 2k+2\} \subseteq H, \tag{15}$$

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

Demostración. Por la Proposición 5 basta con demostrar que $2k+2 \in H$.

En efecto, para el elemento $y^2ab^{-1}(x-\alpha_1)^{-1}$ se tiene

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

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

Según el resultado anterior, si consideramos $d=1$ para el cuerpo de funciones dado por (5) se tiene el siguiente resultado.

Teorema 11. *Si $d=1$ y $n<2k$ en (5), entonces*

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

Demostración. Defina $S := \{n, n+k+1, 2k+2\}$. Por la Proposición 10 se tiene la inclusión $\langle S\rangle \subseteq H$. Se afirma entonces que el conjunto de Apéry A de $\langle S\rangle$ con respecto a n está dado por $A = \{0\} \cup A_1 \cup A_2$, donde

$$A_1 := \{n + ik + i :\ 1 \leq i \leq n-2 \text{ con } i \text{ impar}\}$$

y

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

Para demostrar esto, se debe 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, considere los enteros i, j con $1 \leq i, j \leq \dfrac{n-1}{2}$, entonces,

$$i(2k+2) \equiv j(2k+2) \pmod n \text{ si y solo si } i \equiv j \pmod n \text{ si y solo si } i = j \text{ ya que } i, j < n.$$

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

$$\begin{aligned} n + i(k+1) &\equiv n + j(k+1) \pmod n \text{ si y solo si } i(k+1) \equiv j(k+1) \pmod n \text{ si y solo si} \\ i &\equiv j \pmod n \text{ si y solo si } i = j \text{ entonces } i, j < n.\end{aligned}$$

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

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

Lo anterior muestra que hay n elementos distintos módulo n en A. Ahora se verifica que $A \subseteq \langle S\rangle$, claramente $(2k+2)i \in \langle S\rangle$ para todo $i \in \mathbb{N}$. Por otro lado, sea $1 \leq i \leq n-2$ i impar, entonces como $n+k+1 \in \langle S\rangle$ y $(2k+2)j \in \langle S\rangle$ para todo j, se deduce 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; Reemplazando $2j+1$ por i se obtiene $n+i(k+1) \in \langle S\rangle$. Por lo tanto, $A \subseteq \langle S\rangle$. Queda por ver que $n+i(k+1)-n$ y $(2k+2)j-n$ no pertenecen a $\langle S\rangle$ para $1 \leq i \leq n-2$ impar y $1 \leq j \leq \dfrac{n-1}{2}$, de hecho, si se supone 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 lo tanto i es par, lo cual es una contradicción. De manera similar, si existen $\beta_1, \beta_2, \beta_3 \in \mathbb{N}$ no todos los ceros que satisfacen la relación,

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

se deduce que $\beta_1 + \beta_2 = -1$, lo cual no puede ser, por lo tanto, $A = \mathrm{Ap}(\langle S\rangle; n)$. Ahora, por la Proposición 3,

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

Suponga 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 que implica que $k=3$, y como $n \leq 2k$ con n es impar, se deduce que $n=5$. □

Ejemplo 12. *Dada la extensión de Kummer $y^{10} = (x+1)^6 x(x+3)$ sobre $\mathbb{F}_q$ donde q no divide a 10; Se deduce que $n=5$ y $k=3$, por lo que*

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

Proposición 13. *Si en* (5), $n > 2k+1$, *entonces*

$$S := \{n, n+k+1, n+2k+2\} \subseteq H. \tag{16}$$

En particular, dado que H *es un semigrupo numérico, se deduce que* $\langle S\rangle \subseteq H$.

Demostración. Por la Proposición 5 se tiene que n, $n+k+1 \in H$. Considerando el divisor principal del elemento y^2ab^{-1} se tiene

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

Como $n > 2k+1$, se deduce que $n-2k-2 \geq 0$ y, en consecuencia, $n+2k+2$ es un elemento de H. □

El siguiente teorema establece las condiciones para que la inclusión (16) sea una igualdad.

Teorema 14. *Si en* (5) *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 $\langle S\rangle \subseteq H$. De forma similar al argumento anterior, se comienza calculando el género g_S de $\langle S\rangle$ usando la Proposición 3, para esto, se afirma que el conjunto de 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 note que A tiene n elementos distintos módulo n, ya que para $1 \leq i, j \leq n-2$ donde i, j son impares se tiene

$$i(k+1) \equiv j(k+1) \pmod n \text{ si y solo si } i \equiv j \pmod n \text{ si y solo si } i = j, \text{ ya que } i, j < n.$$

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

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

Si se considera $1 \leq i \leq n-2$ con i impar y $1 \leq j \leq \dfrac{n-1}{2}$ entonces,

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

Por lo tanto, se infiere que A tiene n elementos diferentes módulo n. Ahora observe que los elementos del conjunto A pertenecen a $\langle S \rangle$. Claramente $j(n+2k+2) \in \langle S \rangle$ para todo $j \in \mathbb{N}$. Por otra parte note 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 resumen, $A_1 \subseteq \langle S \rangle$ y, por lo tanto, $A \subseteq \langle S \rangle$. También se demuestra que $n+k+1-n = k+1 \notin \langle S \rangle$, ya que si existen $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{N}$ no todos los ceros para lo cual,

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

se sigue que $\lambda_1 + \lambda_2 + \lambda_3 = 0$ y $\lambda_2 + 2\lambda_3 = 1$; que son ecuaciones inconsistentes para cada valor de λ_i, $i = 1, 2, 3$. Argumentando de manera similar, se observa que $2n+3k+3-n, 3n+5k+5-n, \cdots, \left(\dfrac{n-1}{2}\right) n + (n-2)k + (n-2) - n$ no pertenecen a $\langle S \rangle$. Asimismo, los elementos $n+2k+2-n, 2(n+2k+2)-n, \cdots, \left(\dfrac{n-1}{2}\right)(n+2k+2) - n \notin \langle S \rangle$. En efecto, (el cálculo se hace para $2(n+2k+2)-n = n+4k+4$ pero el procedimiento es el mismo para los demás casos): Si existen $\beta_1, \beta_2, \beta_3 \in \mathbb{N}$ no todos los ceros tales que

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

se sigue que $\beta_1 + \beta_2 + \beta_3 = 1$ y $\beta_2 + 2\beta_3 = 4$, lo cual es imposible según el origen de los escalares $\beta_i, i = 1, 2, 3$, por lo tanto, el conjunto de Apéry de $\langle S \rangle$ con respecto a n es A. En consecuencia; por

la Proposición 3

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

Suponiendo $H=\langle S\rangle$, se deduce que $g_S=g$, lo que 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 hay ningún $k<n$ que satisfaga la condición $n>2k+1$, luego $n=5$, por lo tanto, las posibilidades para k son $\{1,2,3,4\}$, sin embargo, según la restricción $n>2k+1$, la única opción para k es $k=1$.

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

Ejemplo 15. *Suponga que se tiene la extensión de Kummer de $\mathbb{F}_{11}(x)$ dada por $y^{10}=(x+3)^2x(x+5)$. Entonces $H=\langle 5,7,9\rangle$. Además, usando la observación*[2] *se encuentra que la dimensión del espacio de Riemann-Roch $\mathscr{L}(6Q_{\infty_1})$ es 2, es decir, el número de elementos de H que son menores o iguales a 6. Más aún, una base para este espacio vectorial es*

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

Como consecuencia del teorema anterior se obtiene:

Proposición 16. *Si en (5) se considera $n=2k+1$ y $d=1$, entonces,*

$$\langle n,n+k+1,n+k+2,n+k+3,\cdots,n+k+k\rangle\subseteq H, \tag{17}$$

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 5. Considere $0\leq i\leq k-1$ un entero y defina

$$\gamma:=ab^{-1}(x-\alpha_1)^{-i}y^{2i+1},$$

[2] Véase la observación 1.42 página 16 de [7]

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 se obtiene,

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

Claramente, $k-i$ y $2i+1$ son enteros positivos, por lo que el elemento $i+3k+2 \in H$ para todo $0 \leq i \leq k-1$. Por lo tanto, se obtiene la inclusión (17), ya que H es un semigrupo numérico. □

Obteniendo el conjunto de Apéry del semigrupo numérico anterior, se puede demostrar que la inclusión (17), es en efecto una igualdad.

Teorema 17. *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. Sea

$$S := \{n, n+k+1, n+k+2, n+k+3, \cdots, n+k+k\}.$$

Para demostrar que $H = \langle S \rangle$ es suficiente verificar que $g_S = g$, en efecto, primero se afirma que el conjunto de Apéry de $\langle S \rangle$ con respecto a n está dado por $A = \{0\} \cup A_1 \cup A_2$, donde,

$$A_1 := \{n+k+i : 1 \leq i \leq k\},$$

y

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

Como en los Teoremas 11 y 14 se demostrará 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 $1 \leq i, j, \leq k$ se tiene,

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

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

$$2(n+k+1)+i \equiv 2(n+k+1)+j \pmod{n} \text{ si y solo si } i = j \text{ ya que } i, j < n.$$

Finalmente, considere $1 \leq i \leq k$ y $0 \leq j \leq k-1$, entonces,

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

De acuerdo con esto se tiene $n = 2k+1$ elementos distintos módulo n. Ahora se demuestra 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 obtiene que $2(n+k+1)+i \in \langle S \rangle$ para todo $0 \leq i \leq k-1$

A continuación se demuestra que $x \in A$ implica que $x - n \notin S$. Suponga 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 lo cual $\lambda_0 = -1$, lo cual es una contradicción. En el mismo sentido, si supone que para i fijo con $0 \leq i \leq k-1$; existen $\beta_0, \beta_1, \cdots, \beta_k \in \mathbb{N}$ no todos los ceros que cumplan 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 $\beta_0 = -1$, un imposible, por lo tanto, $\mathrm{Ap}(\langle S\rangle; n) = A$.

Finalmente, empleando la Proposición 3 se deduce,

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

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

Ejemplo 18. *Considere 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 de Apéry de H con respecto a $n = 7$ está dado por

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

de modo que el número de Frobenius es $F(H) = \max\{\mathrm{Ap}(H;7)\} - 7 = 17$.

Note que si $n = 2k$, las suposiciones dadas en (5) implican que $d = k$ y k es un número par. El siguiente resultado describe explícitamente el conjunto H para este caso.

Teorema 19. *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 se encuentran sobre el lugar P_∞ viene dado por,

$$H = \langle n, 2k+2, 2k+4, \cdots, 2k+k, n+k+1, n+k+2, \cdots, n+k+(k-1)\rangle. \tag{18}$$

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

$$A_1 := \left\{2(k+i) : 1 \le i \le \frac{k}{2}\right\} \text{ y } A_2 := \{n+k+i : 1 \le i \le k-1\}. \tag{19}$$

Para probar que $H = \langle S\rangle$ es suficiente demostrar que A_1 y A_2 están contenidos en H, y que $g_S = g$. En efecto, para verificar lo primero se procede de la siguiente manera: Por la Proposición 5 se garantiza que los elementos n y $n+k+1$ pertenecen a H. Por otro lado, considere 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

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

Como $n = 2k$ y $d = k$, se tiene:

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

es decir, los $2k+i$ elementos con $2 \leq i \leq k$ pares 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

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

Reemplazando $n = 2k$ y $d = k$ se obtiene,

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

lo que demuestra que $3k + j \in H$ para todo $1 \leq j \leq k-1$ impar.

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

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

Escribiendo $n = 2k$ y $d = k$ se encuentra que,

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

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

Para mostrar que $g_S = g$, observe que el conjunto de 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 (19) y $A_3 := \left\{n + 4k + (2i-1) : 1 \leq i \leq \frac{k}{2}\right\}$. Como en los argumentos anteriores, para justificar este hecho debemos demostrar 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 $\langle S \rangle$, además, dado que $n + 4k + i = (n + k + i) + (2k + 2)$ con $i \in \{1, 3, 5, \cdots, k-3, k-1\}$, entonces se obtiene la inclusión $A \subseteq \langle S \rangle$.

Ahora, para $1 \leq i, j \leq k-1$ se tiene,

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

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

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

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

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

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

$$n+k+i \equiv 2k+j \pmod{n} \text{ si y solo si } k+i \equiv j \pmod{k} \text{ si y solo si } i=j.$$

Un razonamiento similar determina que,

$$2k+j \equiv n+4k+l \pmod{n} \text{ si y solo si } j \equiv l \pmod{2k} \text{ si y solo si } j=l, \text{ ya que } j,l<2k.$$

De lo anterior se tiene $n=2k$ elementos distintos módulo n en A.

A continuación se demuestra que si $x \in A$, entonces $x-n \notin \langle S \rangle$. En efecto, suponga 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 los 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,

$$\sum_{j=0}^{k-1} \gamma_j = 0 \quad \text{y} \quad 2\left(\sum_{j=1}^{\frac{k}{2}} \lambda_j\right) = 1+\gamma_0. \tag{20}$$

Como $\lambda_i s'$ y $\gamma_i s'$ son números naturales, se deduce que (20) induce una contradicción, entonces los elementos $k+i \notin \langle S \rangle$.

Análogamente, para i fijo con $2 \leq i \leq k$ par; si se tiene 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 imposible. Por lo tanto, $2k+j-n \notin \langle S \rangle$.

Finalmente, sea $1 \leq i \leq k-1$ con i impar. Entonces, si supone que $n+4k+i-n$ se puede representar

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

$$\sum_{j=0}^{k-1} \gamma_j = 0, \qquad \sum_{j=1}^{\frac{k}{2}} \lambda_j = 2, \qquad \text{y} \qquad \sum_{j=1}^{\frac{k}{2}} 2j\lambda_j + \sum_{j=1}^{k-1} j\gamma_j = i. \tag{21}$$

De (21) 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 en (21) establece que $\sum_{j=1}^{\frac{k}{2}} 2j\lambda_j = i$, lo que contradice la paridad de i. Como consecuencia de lo anterior, se prueba que $A = \mathrm{Ap}(\langle S\rangle; n)$.

Ahora se muestra que $g_S = g$. En efecto, por la Proposición 3,

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

□

Ejemplo 20. *Considere la extensión de Kummer $y^8 = (x-1)^4 x(x-2)$ sobre $\mathbb{F}_{11}$. Determine bases para los espacios de Riemann-Roch $\mathscr{L}(10Q)$ y $\mathscr{L}(9Q)$ donde Q es una extensión de P_∞.*

*Por el Teorema 19, el semigrupo de Weierstrass asociado con 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 polar y 9 es un número gap, la Proposición 1.40 de [**7**] implica que*

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

Para determinar una base para estos espacios vectoriales, primero defina 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

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

Se buscan elementos $z_j \in F$ tales que n_j esté en H. Según T_1, las posibilidades para n_j son $n_j = 0, 4, 6, 7, 8, 10$. Luego, usando el Teorema 19, se deduce que si $\theta_1 := \dfrac{y^4}{(x-1)^2} - x$, $\theta_2 := \dfrac{y^4}{(x-1)^2} + x$, $\theta_3 := x - 1$ 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, considerando 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 21. *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 "Número 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 "género del campo K(x,y)/K";
Genus(F);
print "Número 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:=Lugares(F,1);
imprimir "Lugares que se extienden hasta el polo de x";
W:=Descomposición(F, D);
W;
```

ejecutado en MAGMA, se tiene 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 considera 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 $\deg G < n = 10$, entonces el Teorema 1.51 de [**7**] 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 $1 \leq j \leq 10$ y $2 \leq i \leq 5$, 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 $\mathcal{C}_{\mathscr{L}}(D, G)$.

Proposición 22. *Si $k = 1$ en (5), entonces,*

$$H = \langle n, n+2, n+4, n+6, \cdots, 2n-1 \rangle. \tag{22}$$

Demostración. Define $S := \{n, n+2, n+4, n+6, \cdots, 2n-1\}$. Debe verificarse que $\langle S \rangle \subseteq H$ y que $g_S = g$. Para lo primero, considere 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 $0 \leq i \leq \dfrac{n-1}{2}$, y como H es un semigrupo, se concluye $\langle S \rangle \subseteq H$.

Para lo segundo, 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

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

Para comprobar esto, se prueba que $A \subseteq \langle S \rangle$, A tiene n elementos distintos módulo n y si $x \in A$, entonces $x - n \notin \langle S \rangle$. Está claro que $A_1 \subseteq \langle S \rangle$. Del mismo modo, 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, en consecuencia, $A \subseteq \langle S \rangle$. Ahora, sean $i, j \in \{2, 4, 6, \cdots, n-3, n-1\}$, entonces,

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

De igual forma para $i, j \in \{1, 3, 5, \cdots, n-4, n-2\}$ se tiene

$$3n + i \equiv 3n + j \pmod{n} \text{ si y solo si } i \equiv j \pmod{n} \text{ si y solo si } i = j \text{ ya que } i, j < n.$$

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

$$n + i \equiv 3n + j \pmod{n} \text{ si y solo si } i \equiv j \pmod{n} \text{ si y solo si } i = j \text{ ya que } i, j < n.$$

En consecuencia, se puede decir que A está formado por n elementos distintos módulo n. Ahora se demuestra que $x \in A$ implica que $x - n \notin \langle S \rangle$. Suponga 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 los 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 $\lambda_0 = \lambda_1 = \cdots = \lambda_{\frac{n-1}{2}} = 0$, lo cual es una contradicción.

De igual modo, si supone 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 los 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 se debe tener,

$$\sum_{j=0}^{\frac{n-1}{2}} \beta_j = 2 \text{ y } \quad 2\sum_{j=0}^{\frac{n-1}{2}} j\beta_j = 2i-1. \tag{23}$$

Observando que la última igualdad de (23) es imposible, se infiere que $A = \mathrm{Ap}(\langle S\rangle; n)$, y así, la Proposición 3 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 exponer el resultado cuando $k = 2$ en (5), se debe enunciar la siguiente proposición.

Proposición 23. *Considere 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 deduce que $n + ik + i \in H$.

b) Ahora, calculando el divisor principal del elemento $y^i ab^{-1}(x-\alpha_1)^{-1}$, se obtiene,

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

Dado que $ik - n \geq 0$ y $2n - ik - i \geq 0$, se deduce la conclusión.

□

Como consecuencia de la proposición anterior, se sigue:

Corolario 24. *Suponga que $k = 2$ en (5), 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 destacar que el corolario anterior no garantiza la igualdad para el conjunto H. No obstante, al usar el software GAP, este corolario se convierte en una conjetura. Se puede decir que la dificultad radica en no poder encontrar una expresión que permita determinar el género del semigrupo en cuestión.

Conjetura 25. *Dada la extensión de Kummer,*

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

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

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

con $i := \text{máx}\{s \in \mathbb{Z}_+ : n-2s-s \geq 0\}$, $j_1 := \text{mín}\{s \in \mathbb{Z}_+ : 2s-n \geq 0\}$, $j := \text{máx}\{s \in \mathbb{Z}_+ : 2n-2s-s \geq 0\}$ 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.

Ejemplo 26. *Calcule 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 $g = 20$ según la Proposición 4. Siguiendo la notación del Corolario 24, se tiene $n = 11$, por lo que $i = 3, j_1 = 6$ y $j = 7$. Note que en este caso $j_2 = j$, luego en ese orden de ideas,*

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

Si ejecutamos el código en el software GAP;

```
gap> LoadPackage("NumericalSgps");
gap> s:=NumericalSemigroup(11,14,17,20,18,21);
<Semigrupo numérico con 6 generadores>
gap> Genus(s); 20
```

Se encuentra que S tiene género 20, de donde se infiere que la inclusión anterior corresponde a una igualdad, y por lo tanto

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

Ejemplo 27. *Determine el semigrupo de Weierstrass H con respecto a la extensión de Kummer $y^{38} = (x-3)^4x(x-7)$ definida sobre $\mathbb{F}_{11}$. Como antes, por la Proposición 4 el género de esta extensión de cuerpos de funciones es $g = 36$. Continuando con la escritura del Corolario 24 se tiene $n = 19$, por lo que $i = 6$, $j_1 = 10$ y $j = 12$ en este caso $j_2 = 11$ y, por lo tanto,*

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

Ahora el código

```
gap> LoadPackage("NumericalSgps");
gap> s:=NumericalSemigroup(19,22,25,28,31,34,37,30,33,36);
<Semigrupo numérico con 10 generadores>
gap> Género(s);
36
```

programado en el software GAP, muestra que S tiene género 36, obteniendo así igualdad en la inclusión anterior y, en consecuencia,

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

Agradecimientos

Agradezco a los revisores de este artículo por sus comentarios los cuales mejoraron la calidad de este documento. Asímismo agradezco a la Universidad del Valle y a mi profesor Horacio Navarro Oyola por su apoyo durante mis estudios de maestría.

REFERENCIAS

1. Roman S. Teoría de Campos. Textos de Posgrado en Matemáticas, 158. Segunda edición. Nueva York: Springer. 2006, págs. 41-66.

2. Mendoza EA. Sobre extensiones de Kummer con un lugar en el infinito.W. Gretchen L. Matthews. Pares de Weierstrass y distancia mínima de los códigos de Goppa. Universidad Estatal de Luisiana y Colegio Agrícola y Mecánico. 2022.

3. Stichtecnoth H. Campo de funciones algebraicas y códigos. Segunda edición. Berlín: Springer-Verlag. 2009.

4. Ramírez Alfonsín JL. El problema diofántico de Frobenius. Reino Unido: Oxford University Press. 2005.

5. Mosquera Hernández LF. Códigos algebro-geométricos de Goppa. RevCiencias. [Internet]. 2022. Sep 25; 25(1): e11795.

6. Mosquera Hernández LF. Semigrupos de Weierstrass en Extensiones de Kummer. 2024.

7. Hill R. Un primer curso de teoría de la codificación. Reino Unido: Oxford University Press. 1986, págs. 49.

8. Rosales JC. y García-Sánchez PA. Semigrupos numéricos. Volumen 20. Nueva York: Springer. 2009.

9. Lewittes J. Lugares de grado uno en cuerpos de funciones sobre cuerpos finitos. *J. Pure Appl. Algebra*. 1990; 69(2): 177–183.

10. Geil O. y Matsumoto R. Acotación del número de lugares **F**q-racionales en cuerpos de funciones algebraicas utilizando semigrupos de Weierstrass. *J. Pure Appl. Algebra*. 2009; 213(6): 1152–1156.

Fondos y colaboradores:

El autor declara que la investigación fue realizada de manera independiente con la colaboración del profesor Horacio Navarro Oyola, financiada con recursos propios y sin contar con apoyo institucional ni financiero externo.

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