Revista Integración
Escuela de Matemáticas
Universidad Industrial de Santander
Vol. 26, No. 2, 2008, pág. 117–121

Números polares de P_∞ en el cuerpo de funciones hermitianas

Wilson Olaya León*

Resumen. En este artículo presentamos una caracterización de los números polares (o no lagunas) del lugar infinito en el cuerpo de funciones hermitianas. Más aún, mostraremos que en dicho cuerpo de funciones los números polares de P_∞ determinan una base explícita para el espacio vectorial asociado al divisor mP_∞.

Abstract. In this paper we present a description of pole numbers (or no-gaps) of the infinite place in the hermitian function field. Moreover, we show that in this function field, the pole numbers determine one explicit base for the vector space associated with the divisor mP_∞.

1. Introducción

Un tema actual de investigación en la teoría de cuerpos de funciones algebraicas consiste en encontrar bases explícitas para el espacio vectorial asociado a un divisor arbitrario. Esto repercute, en la teoría de códigos correctores de errores, en la necesidad de establecer algoritmos de decodificación para los códigos geométricos de Goppa, lo cual a sido una de las limitaciones para la implementación de esos códigos lineales, ver [1]. En el caso del cuerpo de funciones hermitianas, mostramos en este trabajo que los números polares de P_∞ determinan una base explícita del espacio vectorial $L(mP_\infty)$.

Palabras y frases claves: Números polares, lagunas de Weierstrass, cuerpo de funciones hermitianas.
Key words: Pole numbers, Weierstrass's gaps, Hermitian function field.
MSC2000: Primaria: 14H05. Secundaria: 11R58, 11T71.

* Universidad Industrial de Santander UIS, A.A. 678, Bucaramanga-Colombia,
e-mail: wolaya@uis.edu.co

2. Notación

$\mathbb{F}_q$	El cuerpo finito con q elementos.
$F/\mathbb{F}_q$	El cuerpo de funciones algebraicas sobre $\mathbb{F}_q$.
$H/\mathbb{F}_{q^2}$	El cuerpo de funciones hermitianas.
P_∞	El lugar infinito de $H/\mathbb{F}_{q^2}$.
$\text{grad}(A)$	El grado del divisor A.
$L(A)$	El espacio vectorial asociado al divisor A.
$\dim(A)$	La dimensión del divisor A; $\dim(A) := \dim(L(A))$.
$\text{Sop}(A)$	El soporte del divisor A.

3. Preliminares

El cuerpo de funciones hermitianas es un ejemplo especial de cuerpos de funciones maximales; es decir, cuerpos que alcanzan la cota superior de Hasse-Weil para el número de lugares de grado uno. Se sabe que esto es posible para cuerpos de funciones algebraicas sobre cuerpos de constantes $\mathbb{F}_{q^2}$, y el número de lugares de grado uno es $N = q^2+1+2gq$, donde g es el género del cuerpo de funciones, ver [4].

Denotaremos por $H := \mathbb{F}_{q^2}(x, y)$, con $y^q + y = x^{q+1}$. Por lo tanto, $H/\mathbb{F}_{q^2}$ es el cuerpo de funciones hermitianas con género $g = \dfrac{q(q-1)}{2}$ y $N = q^3 + 1$ lugares de grado uno.

Los cuerpos de funciones maximales son importantes en la construcción de códigos geométricos de Goppa, puesto que optimizan los parámetros del código lineal, ya que la longitud del código está acotada por el número de lugares de grado uno.

Si $F/\mathbb{F}_q$ es un cuerpo de funciones algebraicas con género g y $P_1, P_2, \ldots, P_n$ son distintos lugares de grado uno, tomando $D = \sum_{i=1}^{n} P_i$ y G cualquier otro divisor de $F/\mathbb{F}_q$ tal que ninguno de los P_i esta en el soporte de G, se define el código geométrico de Goppa asociado a los divisores D y G como

$$C_L(D, G) := \{(x(P_1), x(P_2), \ldots, x(P_n)) : x \in L(G)\}.$$

Este es un $[n, k, d]$-código q-ario, donde $k = \dim G - \dim(G - D)$ y $d \geq n - \text{grad}(G)$. Más aún, si $\text{grad}(G) < n$, entonces $k = \dim G$, y conociendo una base para $L(G)$ fácilmente se puede construir una matriz generadora para $C_L(D, G)$.

Observe que usando el teorema de Riemann-Roch los parámetros del código $C_L(D, G)$ solo dependen del grado del divisor G (fijados n y g). Por lo tanto, si deseamos conseguir códigos geométricos de Goppa con parámetros prefijados, lo que comúnmente se hace es tomar $G = mP$, donde $m > 0$ y P es un lugar de grado uno que no esté en el soporte

de D (por lo general el lugar infinito). Estos códigos se conocen como códigos sobre un lugar, ver [3].

Pensando en esto, es de interés determinar los elementos en F que tienen solamente un polo en el lugar infinito de $H/\mathbb{F}_{q^2}$. En general, para cualquier lugar de un cuerpo de funciones algebraicas se establece la siguiente definición.

Definición 3.1. Sea P un lugar de $F/\mathbb{F}_q$. Un entero $n \geq 0$ se denomina número polar de P si, y solo si, existe un elemento $z \in F$ con $(z)_\infty = nP$. En cualquier otro caso se dice que n es un número laguna de P.

Observe que n es un número polar de P si, y solo si, $L\left((n-1)P\right) \subset L(nP)$. En consecuencia, $L\left((n-1)P\right) = L(nP)$ si, y solo si, n es un número laguna de P.

4. Resultado principal

Hagamos $H(P_\infty) := \{n \geq 0 : n \text{ es un número polar de } P_\infty \text{ en } H\}$.

Afirmación 4.1. $H(P_\infty) = \{n = iq + j(q+1),\ i \geq 0,\ 0 \leq j \leq q-1\}$.

Demostración. Primero veamos que para $n = iq+j(q+1)$ con $i \geq 0,\ 0 \leq j \leq q-1$, existe $z \in H$ tal que $(z)_\infty = nP_\infty$. En efecto, para $z = x^i y^j$ con $i \geq 0,\ 0 \leq j \leq q-1$, tenemos que $(z)_\infty = (iq + j(q+1))\, P_\infty = nP_\infty$, ya que $(x)_\infty = qP_\infty$ y $(y)_\infty = (q+1)P_\infty$.

Ahora mostraremos que $H(P_\infty)$ es generado por q y $q+1$. Sea $\varphi(T) = T^q + T - x^{q+1}$ el polinomio minimal de y sobre $\mathbb{F}_{q^2}(x)$; puesto que el único lugar que es ramificado en H es P_∞, tenemos que $\{y^j : 0 \leq j \leq q-1\}$ es una base entera para $\mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}(x)$ (ver en [4] el numeral III.5.10(d)).

Ahora, si $n \in H(P_\infty)$, entonces existe $z \in H$ tal que $(z)_\infty = nP_\infty$. Supongamos que $z = \sum_{j=0}^{q-1} z_j y^j$ con $z_j \in \mathbb{F}_{q^2}[x]$. Entonces $z = \sum_{j=0}^{q-1} \sum_{i \geq 0} a_{ij} x^i y^j$ con $a_{ij} \in \mathbb{F}_{q^2}$. En consecuencia,

$$\begin{aligned} -n = \upsilon_{P_\infty}(z) &= \text{mín}\{\upsilon_{P_\infty}(x^i y^j) : a_{ij} \neq 0\} \\ &= \text{mín}\{i\upsilon_{P_\infty}(x) + j\upsilon_{P_\infty}(y) : a_{ij} \neq 0\} \\ &= \text{mín}\{iq + j(q+1) : a_{ij} \neq 0\}. \end{aligned}$$

Luego n es una combinación lineal de q y $q+1$. Por lo tanto, q y $q+1$ generan $H(P_\infty)$. ☑

Observación 4.2. En este caso,

$$H(P_\infty) = \{n = iq + j(q+1),\ i \geq 0,\ 0 \leq j \leq q-1\} = \{n = aq + b : 0 \leq b \leq a\}.$$

Ahora bien, si tomamos $\overline{H}(P_\infty) := \{n : n \text{ es una laguna de } P_\infty \text{ en } H\}$, entonces tenemos que $\overline{H}(P_\infty) = \{n = aq+b : 0 \leq a < b \leq q-1\}$. Además, fácilmente se verifica el teorema de las lagunas de Weierstrass, que garantiza la existencia de exactamente $g = \dfrac{q(q-1)}{2}$ números laguna; más aún, $2g-1$ es una de ellas, pues $2g-1 = q^2-q-1 = q(q-2)+(q-1) \in \overline{H}(P_\infty)$.

En la siguiente afirmación mostramos que la dimensión del espacio vectorial $L(mP_\infty)$ es el cardinal del conjunto de los números polares menores o iguales a m. Denotaremos $H_m(P_\infty) := \{n \in H(P_\infty) : n \leq m\}$.

Afirmación 4.3. $\dim(mP_\infty) = |H_m(P_\infty)| = |\{n \in H(P_\infty) : n \leq m\}|$.

Demostración. Consideremos la cadena de espacios vectoriales

$$\mathbb{F}_{q^2} = L(0) \subseteq L(P_\infty) \subseteq \cdots \subseteq L(mP_\infty).$$

De un lado sabemos que $\dim L(iP_\infty) \leq \dim L((i-1)P_\infty) + 1$. De otro, tenemos que i es un número polar de P_∞ si, y solo si, $\dim(iP_\infty) > \dim((i-1)P_\infty)$. En consecuencia, si i es un número polar de P_∞ entonces $\dim L(iP_\infty) = \dim L((i-1)P_\infty) + 1$. Además, como $0 \in H(P_\infty)$ y $\dim L(0) = 1$, tenemos que la dimensión en la cadena aumentará tantas veces como elementos tenga $H_m(P_\infty)$, es decir, $\dim(mP_\infty) = |H_m(P_\infty)|$. ☑

Utilizando las dos afirmaciones anteriores podemos determinar una base explícita para el espacio vectorial $L(mP_\infty)$.

Proposition 4.1. *Una base para $L(mP_\infty)$ está dada por*

$$\{z \in H : (z)_\infty = nP_\infty \text{ para } n \in H_m(P_\infty)\}.$$

Demostración. Primero veamos que los elementos del conjunto pertenecen a $L(mP_\infty)$. En efecto, $(z)_\infty = (iq + j(q+1))P_\infty \geq -mP_\infty = -G$, ya que $iq + j(q+1) \leq m$.

Ahora, para ver que son linealmente independientes, obsérvese que $z = x^i y^j$ con $i \geq 0,\ 0 \leq j \leq q-1$ y el conjunto $\{y^j : 0 \leq j \leq q-1\}$ es una base para $\mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}(x)$. ☑

Referencias

[1] Arnaldo GARCIA and Henning STICHTENOTH, "Topics in Geometry", *Coding Theory and Cryptography*, Springer, 2007.

[2] Jacobus H. VAN LINT. *Introduction to Coding Theory*, second edition, Springer-Verlag, 1992.

[3] Jacobus H. VAN LINT and Gerard VAN DER GEER. *Introduction to Coding Theory and Algebraic Geometry*, Birkhauser, Verlag Basel, 1988.

[4] Henning STICHTENOTH. *Algebraic Function Field and Codes*, Springer-Verlag, Berlin, 1993.

Wilson Olaya
Escuela de Matemáticas
Universidad Industrial de Santander
Bucaramanga, Colombia, A.A. 678
e-mail: wolaya@uis.edu.co.