Ciencias Matemáticas, Vol. 29, No. 2, Pag. 127-130, 2015
Recibido 09-2015

Relación entre el automorfismo de Frobenius y los homomorfismos de inmersión del campo $GF(p^n)$ en el campo $GF(p^m)$

Relation between Frobenius automorphism and the embedding homomorphisms from field $GF(p^n)$ in field $GF(p^m)$

Oristela Cuéllar Justiz[1]*, Eberto R. Morgado Morales[1], Evaristo Madarro Capó[1], Guillermo Sosa Gómez[2]

Resumen Es bien conocido, que para todo campo de Galois $GF(p^m)$, siendo p un número primo y m un número natural, y todo número natural n que es divisor de m, existe un único subcampo del campo de Galois $GF(p^m)$ que es isomorfo a $GF(p^n)$. En un artículo anterior publicado en la Revista Ciencias Matemáticas [5] se obtuvieron las diferentes maneras de definir un homomorfismo de inmersión entre los campos $GF(p^n)$ y $GF(p^m)$, cuando n divide a m. En este artículo veremos la relación existente entre el automorfismo de Frobenius y los homomorfismos de inmersión y se enuncia y demuestra un teorema que establece que el número de maneras de realizar la inmersión es igual al orden del grupo cíclico $Aut(GF(p^n))$, de automorfismos del campo $GF(p^n)$, el cual es de orden n y es generado por el llamado automorfismo de Frobenius F_p. Ilustraremos el resultado anterior tomando como ejemplo los homomorfismos de inmersión del campo $GF(8)$ en el campo $GF(64)$.

Abstract It is well known that for every Galois field $GF(p^m)$, where p is a prime number, m is a natural number and every natural number n, which is a divisor of m, there exists a unique subfield of the Galois field $GF(p^m)$ isomorphic to $GF(p^n)$. In a previous paper published in the journal Ciencias Matemáticas [5], the different ways of defining the embedding homomorphisms of the Galois fields $GF(p^n)$ into $GF(p^m)$, where n divides m. In the present paper we examine the relationship between the Frobenius Automorphism and the embedding homomorphisms. We will also give the statement and the proof of a theorem, which state that the number of ways of performing the embedding is equal to the order of the cyclic group $Aut(GF(p^n))$ of automorphisms of the field $GF(p^n)$, which is of order n and is generated by the so called Frobenius Automorphism F_p. We will illustrate this result taking as an example the embedding homomorphisms of the fields $GF(8)$ in the field $GF(64)$.

Palabras Clave
automorfismo de Frobenius, homomorfismos de inmersión

[1] *Universidad Central "Marta Abreu" de Las Villas, Santa Clara, Cuba, oristela@uclv.edu.cu*
[2] *Centro de Investigaciones en Matemática (CIMAT), Guanajuato, México*
***Autor para Correspondencia**

1. Introducción

Los campos finitos, también llamados campos de Galois, tienen múltiples aplicaciones en diferentes ramas del conocimiento y de la investigación científica: En la Combinatoria, en la Teoría de Los Números, la Geometría Algebraica, la Biología Matemática, la Teoría de Galois, en la Criptografía. En Criptografía los campos finitos se utilizan ampliamente en la implementación de muchos de los códigos conocidos, así como en su decodificación. Es bien sabido que todo campo finito K tiene cardinalidad p^n, donde p es un número primo y n un número natural [1], [2]. Por otra parte, para cada número primo p y cada número natural n existe un campo finito con p^n elementos, único salvo isomorfismos. Analizando los homomorfismos entre campos finitos de diferente cardinalidad, se ha logrado, sobre la base de la literatura revisada [3], diseñar algoritmos para la determinación de los n homomorfismos de inmersión que existen entre los campos $GF(p^n)$ y $GF(p^m)$.

Los campos $GF(p^n)$ y $GF(p^m)$ son extensiones algebraicas del campo primo $GF(p)$, donde p es un número primo, y nym son números naturales tales que n es un divisor de m .

Un homomorfismo de inmersión del campo $GF(p^n)$ en el campo $GF(p^m)$ es un homomorfismo inyectivo $h : GF(p^n) \rightarrow$

$GF(p^m)$ tal que $h(a)=a, \forall a \in GF(p)$. Siempre existe al menos un homomorfismo inyectivo $h: GF(p^n) \to GF(p^m)$. Dicho homomorfismo sumerge al campo $GF(p^n)$ en $GF(p^m)$, lo cual significa que el subcampo de $GF(p^m)$, imagen de h, es isomorfo a $GF(p^n)$.

En [5] se obtuvieron las diferentes maneras de definir un homomorfismo de inmersión, del campo de Galois $GF(p^n)$ en el también campo de Galois $GF(p^m)$ siendo p un número primo, *myn* naturales con n divisor de m.

Sea K un campo finito de característica p. Llamamos automorfismo de Frobenius a la función $F_p: K \to K$ definida por $F_p: x \to x^p$. Esta función F_p es aditiva [1, 2, 4], ya que, cualesquiera que sean x, y, $(x+y)^p = x^p + y^p$ [1, 2] y es multiplicativa, ya que, cualesquiera que sean x, y, $(xy)^p = x^p y^p$. Como el Kernel de F_p es, evidentemente, el ideal trivial $\{0\}$, F_p es un endomorfismo inyectivo. Como el conjunto K lo suponemos finito la función F_p es también sobreyectiva. Luego, es un automorfismo del campo K. Es fácil ver que, si K es el campo $GF(p^n)$, toda función de la forma $(F_p)^k$, para $0 \le k \le n-1$, es también un automorfismo. Estos son los únicos automorfismos del campo $GF(p^n)$, por lo que el grupo $Aut(GF(p^n))$, de todos los automorfismos, es cíclico, de orden n y generado por el automorfismo de Frobenius F_p.

2. Relación entre los grupos de automorfismos de los campos $GF(p^n)$ y $GF(p^m)$

Consideremos la función

$$Rest: Aut(GF(p^m)) \to Aut(GF(p^n))$$

tal que: $F_p^t \to B_p^t$, la cual asigna a cada automorfismo de $GF(p^m)$, expresado como una potencia del automorfismo de Frobenius F_p de $GF(p^m)$, la correspondiente potencia del automorfismo de Frobenius B_p de $GF(p^n)$. Esto no es más que la restricción del automorfismo F_p^t de $GF(p^m)$ al automorfismo B_p^t del subcampo $GF(p^n)$, visto como subcampo de $GF(p^m)$.

Esta función es, evidentemente, un epimorfismo, cuyo kernel es el subgrupo formado por los F_p^t cuyo exponente t es múltiplo de n, siendo el orden del kernel igual al número k tal que $m = nk$.

Estamos ahora en condiciones de enunciar y probar el siguiente teorema

Teorema 1 *La cantidad de maneras de sumergir el campo de Galois $GF(p^n)$ en el también campo de Galois $GF(p^m)$, siendo n un divisor de m, es igual al número n, que es el orden del grupo de automorfismos del campo $GF(p^n)$.*

Demostración. Sean

$$G = Aut_{GF(p)}(GF(p^n)) = \{Aut\ B_{p^j} : GF(p^n) \to GF(p^n)\}.$$

Si $\alpha \in GF(p^n)$ entonces $\alpha \to \alpha^p$.

$B_{p^j}(\alpha) = \alpha^{p^j}, j = 0, n' - 1$,

$$G' = Aut_{GF(p)}(GF(p^m)) = \{Aut\ F_{p^j} : GF(p^m) \to GF(p^m)\}.$$

Si $\beta \in GF(p^m)$ entonces $\beta \to \beta^p$. $F_{p^j}(\beta) = \beta^{p^j}$, $j = \overline{0, m-1}$,

El grupo G' es generado por el automorfismo de Frobenius $F_p: GF(p^m) \to GF(p^m)$ por tanto $F_{p^j} = (F_p)^j$.

Sean h_r y h_s ambos homomorfismos de inmersión, tales que $h_r(\alpha) = \beta^{k_r}$ y $h_s(\alpha) = \beta^{k_s}$, siendo $k_r = rk_1$, $k_S = sk_1$ y $k_1 = \frac{p^m-1}{p^n-1}$.

Tomemos a uno de estos automorfismos por ejemplo para un $0 < t < m-1$ y evaluemos $F_{p^t} = (F_p)^t$ en β^{k_r}

$$F_{p^t}\left(\beta^{k_r}\right) = \left(F_p\left(\beta^{k_r}\right)\right)^t = \left(\left(\beta^{k_r}\right)^p\right)^t$$
$$F_{p^t}\left(\beta^{k_r}\right) = \left(\beta^{k_r}\right)^{p^t} = \beta^{k_r p^t}$$

Sea $k_r p^t = rk_1 p^t = (rp^t)k_1$, como $r < p^n - 1$ y primo relativo con $p^n - 1$, el $mcd(rp^t, p^n - 1) = 1$, si consideramos $rp^t = s$, entonces $sk_1 = k_s$ y

$$k_r p^t = rk_1 . p^t = (rp^t)k_1 = sk_1 = k_s$$
$$F_{p^t}\left(\beta^{k_r}\right) = \left(\beta^{k_r}\right)^{p^t} = \beta^{k_r p^t} = \beta^{k_s}$$
$$F_{p^t}\left(\beta^{k_r}\right) = \left(F_p\left(\beta^{k_r}\right)\right)^t = \beta^{k_s}$$

Hemos probado que existe un automorfismo $F_{p^t} = (F_p)^t$, del campo $GF(p^m)$ tal que $F_{p^t}\left(\beta^{k_r}\right) = \beta^{k_s}$. Esto implica que $F_{p^t} \circ h_r = h_r \circ B_{p^t} = h_s$, es decir, que, dados dos homomorfismos de inmersión, uno se obtiene del otro por composición con un automorfismo. Esto, a su vez, significa que el número de homomorfismos de inmersión es igual al número n, de automorfismos del campo $GF(p^n)$. ■

3. Homomorfismos de inmersión del campo $GF(8)$ en $GF(64)$

En [5] se analizaron los posibles homomorfismos de inmersión del campo de Galois $GF(8)$ en el campo $GF(64)$

$$h_1(\alpha) = \beta^9 h_2(\alpha) = \beta^{18} h_3(\alpha) = \beta^{27}$$
$$h_4(\alpha) = \beta^{36} h_5(\alpha) = \beta^{45} h_6(\alpha) = \beta^{54}$$

Se mostró que el campo de Galois $GF(8)$ se sumerge de tres maneras diferentes en el campo de Galois $GF(8)$

$$h_3(\alpha) = \beta^{27}, h_5(\alpha) = \beta^{27}, h_6(\alpha) = \beta^{27}$$

$$M(h_3)=\begin{bmatrix}1&0&1\\0&1&1\\0&1&1\\0&1&0\\0&0&1\\0&0&0\end{bmatrix},M(h_5)=\begin{bmatrix}1&1&0\\0&0&0\\0&0&0\\0&0&1\\0&1&1\\0&0&0\end{bmatrix},M(h_6)=\begin{bmatrix}1&1&1\\0&1&0\\0&1&0\\0&0&1\\0&1&1\\0&0&0\end{bmatrix}.$$

Veremos ahora la relación que existe entre los automorfismos de Frobenius y las diferentes maneras de sumergir un campo en el otro.

3.1 Automorfismo de Frobenius del campo $GF(64)$

Es fácil notar que el automorfismo F_2 de $GF(64)$ es el que tiene por Matriz:

$$M(F_2)=\begin{bmatrix}1&0&0&1&0&0\\0&0&0&1&0&0\\0&1&0&0&1&0\\0&0&0&0&1&0\\0&0&1&0&0&1\\0&0&0&0&0&1\end{bmatrix}.$$

También vemos que

$$M\left(F_2^2\right)=\begin{bmatrix}1&0&0&1&1&0\\0&0&0&0&1&0\\0&0&1&1&0&1\\0&0&1&0&0&1\\0&1&0&0&1&1\\0&0&0&0&0&1\end{bmatrix},M\left(F_2^3\right)=\begin{bmatrix}1&0&1&1&1&1\\0&0&1&0&0&1\\0&1&0&0&0&1\\0&1&0&0&1&1\\0&0&1&1&0&0\\0&0&1&0&0&1\end{bmatrix},$$

$$M\left(F_2^4\right)=\begin{bmatrix}1&1&1&1&0&0\\0&1&0&0&1&1\\0&0&0&1&0&1\\0&0&1&1&0&0\\0&1&0&0&0&0\\0&0&0&0&0&1\end{bmatrix},M\left(F_2^5\right)=\begin{bmatrix}1&1&0&0&0&0\\0&0&1&1&0&0\\0&0&0&0&1&1\\0&1&0&0&0&0\\0&0&0&1&0&0\\0&0&0&0&0&1\end{bmatrix},$$

y

$$M\left(F_2^6\right)=\mathbf{I}_6,$$

donde $\mathbf{I}_6$ es la matriz identidad de orden 6.

Multiplicando cada una de estas matrices a la izquierda de $M(h_3)$, $M(h_5)$, $M(h_6)$ vemos que, aplicando cada uno de los automorfismos después de aplicada la función de inmersión, h_i obtenemos que

$$\begin{aligned}F_2\circ h_3=h_6,(F_2)^2\circ h_3=h_5,(F_2)^3\circ h_3=h_3\\(F_2)^4\circ h_3=h_6,(F_2)^5\circ h_3=h_5,(F_2)^6\circ h_3=h_3\\F_2\circ h_5=h_3,(F_2)^2\circ h_5=h_6,(F_2)^3\circ h_5=h_5\\(F_2)^4\circ h_5=h_3,(F_2)^5\circ h_5=h_6,(F_2)^6\circ h_5=h_5\\F_2\circ h_6=h_5,(F_2)^2\circ h_6=h_3,(F_2)^3\circ h_6=h_6\\(F_2)^4\circ h_6=h_5,(F_2)^5\circ h_6=h_3,(F_2)^6\circ h_6=h_6\end{aligned}$$

Es decir, que la composición con el automorfismo de Frobenius F_2 convierte cada homomorfismo de inmersión en el otro, no existiendo otros homomorfismo de inmersión salvo h_3, h_5, h_6.

En el caso analizado la cantidad de inmersiones posibles coincide con el orden n, del grupo de automorfismos $Aut(GF(8))$ del campo de partida.

3.2 El automorfismo de Frobenius B_2 de $GF(8)$

Este automorfismo es el que tiene por Matriz:

$$M(B_2)=\begin{bmatrix}1&0&0\\0&0&1\\0&1&1\end{bmatrix},$$

la cual cumple que

$$M\left(B_2^2\right)=\begin{bmatrix}1&0&0\\0&1&1\\0&1&0\end{bmatrix}$$

y $M\left(B_2^3\right) = \mathbf{I}_3$.

Multiplicando la matriz $M(B_2)$ a la derecha de $M(h_3)$, $M(h_5)$ y $M(h_6)$ vemos que, aplicando la función de inmersión h_i, después de aplicado el automorfismo B_2, obtenemos que

$$M(h_3)M(B_2) = M(h_6)$$
$$M(h_5)M(B_2) = M(h_3)$$
$$M(h_6)M(B_2) = M(h_5)$$

lo cual significa que $h_3 \circ B_2 = h_6, h_5 \circ B_2 = h_3, h_6 \circ B_2 = h_5$. Es decir, que en este caso también ocurre que la composición con el automorfismo de Frobenius convierte cada homomorfismo de inmersión en el otro existente, no existiendo ningún otro homomorfismo de inmersión salvo h_3, h_5, h_6 .

Hemos visto así, que la cantidad de inmersiones posibles coincide con el orden, 3, del grupo de automorfismos $Aut(GF(8))$ del campo de partida.

Todos los cálculos realizados para obtener los resultados que se presentan en este artículo fueron realizados con el Mathematica 9.0 y con el software BiGFSoP patentado por los autores de este trabajo.

4. Conclusiones

Este artículo da continuidad a un artículo anterior titulado Ïnmersión de un campo de Galois $GF(p^n)$ en otro de mayor cardinalidad"[5]. Se analizó la relación existente entre el automorfismo de Frobenius y los homomorfismos de inmersión. Los resultados obtenidos en estos dos trabajos nos han permitido diseñar dos algoritmos para la determinación de los homomorfismos de campos finitos de igual y diferente cardinalidad.

Se enunció y demostró un teorema que establece que el número de maneras de realizar la inmersión del campo $GF(p^n)$ en el también campo de Galois $GF(p^m)$ es igual al orden del grupo cíclico $Aut(GF(p^n))$, de automorfismos del campo $GF(p^n)$, el cual es de orden n y es generado por el llamado automorfismo de Frobenius F_p. .

Se ilustró tomando como ejemplo los homomorfismos de inmersión del campo $GF(8)$ en el campo $GF(64)$, la relación existente entre el automorfismo de Frobenius y las funciones de inmersión, mostrándose que la composición con el automorfismo de Frobenius convierte cada homomorfismo de inmersión en otro ya existente.

Referencias

[1] Lidl, R., Niederraiter, H., *Konechnye Polya. Tomo I y II*, Moscú: Mir, 1998.

[2] Lidl, R., Niederraiter, H., *Introduction to finite fields and their applications*, Cambridge University Press, New York, 1994.

[3] http://mathwiki.cs.ut.ee, [Consultado: abril 10, 2015].

[4] Fraleigh, Jonh F., *A first Course in Abstract Algebra*. Adisson Wesley Publishing Company, 1972.

[5] Cuellar Justiz, O., Sosa Gomez, G., *Inmersión de un campo de Galois GF(pn) en otro de mayor cardinalidad*. Revista Ciencias Matematicas Vol. 27 No. 2, 2013.