Inmersión de un campo de Galois *GF(pn)* en otro de mayor cardinalidad

Oristela Cuellar Justiz, Guillermo Sosa Gómez (oristela@uclv.edu.cu)
Departamento de Matemáticas, Universidad Central Marta Abreu, Las Villas

Resumen

Es bien conocido [1], 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 $GF(p^n)$. De aquí resulta que, para campos de Galois $GF(p^n)$ y $GF(p^m)$, siendo n un divisor de m, existe al menos un homomorfismo inyectivo $h: GF(p^n) \rightarrow GF(p^m)$. Dicho homomorfismo sumerge a $GF(p^n)$ en $GF(p^m)$, lo cual significa que el subcampo de $GF(p^m)$, imagen de h, es el que es isomorfo a $GF(p^n)$. En el presente trabajo, veremos las diferentes maneras de definir un homomorfismo de inmersión, en ciertos casos particulares. Veremos las diferentes maneras de sumergir un campo en otro tomando como ejemplo el caso de los campos *GF(8)* en *GF(64)*.

Abstract

It is well known [1], that for every Galois Field $GF(p^m)$, where p is a prime number and m a natural number , and every natural number n which is a divisor of m, there is a unique subfield of the Galois Field $GF(p^m)$, which is isomorphic to the field $GF(p^n)$. From these follows that, for Galois fields $GF(p^n)$ and $GF(p^m)$, being n a divisor of m, there're is, at least, an injective homomorphism $h: GF(p^n) \rightarrow GF(p^m)$. Such an homomorphism embeds $GF(p^n)$ into $GF(p^m)$, It means that the subfield of $GF(p^m)$, image of h, is that which is isomorphic to $GF(p^n)$. In the present work we will see different ways of defining an embedding homomorphism in certain particular case. We will see the different ways of embedding a field in another one, taking, as an example, the case of the fields *GF(8)* into *GF(64)*.

1. Introducción

La teoría de los campos finitos es una rama del Álgebra moderna que se ha convertido en muy actual desde la última mitad del siglo pasado teniendo en cuenta sus múltiples aplicaciones. Los campos finitos, también llamados campos de Galois, tienen aplicación en la Combinatoria, en la Teoría de Números, la Geometría Algebraica, la Biología Matemática, la Teoría de Galois y en la Criptografía. En Criptografía los campos finitos se utilizan en la construcción de la mayoría de los códigos conocidos y 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. En este caso el número primo p es la característica del campo, esto es, el menor entero positivo tal que

$$pa = a + a + {}^{p\ veces} a = 0, \text{ para todo a elemento de } K.$$

Por otra parte, para cada número primo p y cada número natural n existe un campo finito con p^n elementos, único salvo isomorfismos. (Teorema de existencia y unicidad de campos

finitos [1]). En el presente trabajo nos proponemos examinar las diferentes maneras de sumergir un campo de Galois de p^n elementos en uno de p^m elementos, cuando n es un divisor de m.

2. Desarrollo del trabajo

Los campo $GF(p^m)$ y $GF(p^n)$, son extensiones algebraicas del campo primo $\mathbb{Z}p = GF(p)$, de grados m y n ,respectivamente , (y cada uno se obtiene al adjuntarle a $GF(p)$ una raíz, primitiva, de un polinomio irreducible, de grado m, o grado n, según el caso.

Aquí recordamos al lector que se llama campo primo a un campo que no contiene subcampos propios. En el caso de los campos finitos, o campos de Galois, los campos primos son los anillos $\mathbb{Z}p$, de restos módulo p, para p primo. Los campos $GF(p^n)$, de p^n elementos, se construyen todos de manera similar. Tomemos, para ilustrar, un campo $GF(p^n)$, de p^n elementos. Veamos brevemente algunas formas de representar los elementos del mismo.

Sea α una raíz de un polinomio f, irreducible sobre $\mathbb{Z}p = GF(p)$, llamado *polinomio característico de la extensión*. El campo $GF(p^n)$ se puede representar como el conjunto de los polinomios en α de grado $\leq n-1$, incluido el polinomio nulo, que no tiene grado, todos con coeficientes en $\mathbb{Z}p = GF(p)$. En este caso, α se llama *elemento definitorio* de $GF(p^n)$. Es decir

$$GF(p^n) = \left\{ \sum_{i=0}^{n-1} c_i \alpha^i \,\middle|\, c_i \in \mathbb{Z}p \right\}$$

La representación que se obtiene de esta manera no es única para $GF(p^m)$.

Basta notar que, de existir dos polinomios distintos f y g, irreducibles sobre $GF(p)$, de un mismo grado n y con raíces α y β respectivamente. Entonces los anillos cocientes $\frac{\mathbb{Z}p[x]}{f(x)\mathbb{Z}p[x]}$ y $\frac{\mathbb{Z}p[x]}{g(x)\mathbb{Z}p[x]}$ son isomorfos entre sí, e isomorfos al campo $GF(p^n)$. Pero α^m y β^m no se representan como un mismo polinomio, evaluado en α o en β, según el caso.

Otra forma de ver la extensión $GF(p^n)$ es como espacio vectorial de dimensión n sobre su subcampo primo $\mathbb{Z}p = GF(p)$. Si tomamos al conjunto $\{1,\alpha,\alpha^2, \ldots, \alpha^{n-1}\}$ (donde α es el elemento definitorio de $GF(p^n)$), como una base de $GF(p^n)$, llamada base polinomial, entonces los elementos de $GF(p^n)$ quedarán representados como combinaciones lineales

$$\sum_{i=0}^{n-1} c_i a^i, \text{ con } c_i \in \mathbb{Z}p$$

Es bien sabido que el grupo multiplicativo de un campo $GF(q)$, con $q = p^n$, denotado $(GF(q))^*$, es cíclico. Un generador del grupo $(GF(q))^*$ se llama elemento primitivo del campo $GF(q)$. [1, 2, 3]

Teniendo en cuenta esta propiedad obtenemos que, otra forma muy común de representar un campo $GF(q)$, es representando sus elementos no nulos como potencias de un elemento fijo α.

Sea $GF(p^n)$ una extensión algebraica de $\mathbb{Z}p = GF(p)$, cuyo elemento definitorio α es raíz de un polinomio irreducible f de grado n. Si todo elemento de se puede expresar como una potencia de α (equivalentemente, α es un elemento primitivo de se dice entonces que $GF(p^n)$ es un *polinomio primitivo*.

Esto nos permite plantear $GF(p^m) = \{\alpha^k | 0 \leq k \leq p^m - 1\}$ siempre que α sea raíz de un polinomio primitivo de grado m, sobre $GF(p)$.

Si α es un elemento primitivo de $GF(p^n)$, es decir un elemento de orden $p^n - 1$ en el grupo multiplicativo $GF(p^n)$ y β es un elemento primitivo en $GF(p^m)$, esto es, un elemento de orden $p^m - 1$ en el grupo multiplicativo $(GF(p^n))^*$ entonces un homomorfismo de inmersión $h: GF(p^n) \rightarrow GF(p^m)$ debe convertir α en un elemento β^k de su mismo orden, es decir, de orden $p^n - 1$. Para ello es necesario que sea múltiplo del entero $\frac{p^m - 1}{p^n - 1}$. (Este número es entero, ya que por ser n divisor de m, $p^m - 1$ es divisible por $p^n - 1$). La cantidad de valores que puede tomar k es igual a $\varphi(p^n - 1)$, siendo φ la llamada función tótem de Euler, que asigna a cada número natural la cantidad de naturales menores que, y primos relativos con él.

Como un homomorfismo de campos necesariamente convierte el cero en cero y el uno en uno, es decir, cada elemento neutro, el aditivo y el multiplicativo, en el neutro correspondiente, convierte también cada constante, es decir, cada elemento del campo primo $GF(p)$ siendo p la característica de ambos campos, en sí misma. Por consiguiente, el homomorfismo de inmersión h es también una aplicación lineal, esto es, un homomorfismo de espacios vectoriales, vistos ambos campos como espacios vectoriales sobre su subcampo primo $\mathbb{Z}p = GF(p)$. De acuerdo con ello el homomorfismo puede ser representado matricialmente, tomando como bases los siste-

mas $\{1,\alpha,\alpha^2, \ldots, \alpha^{n-1}\}$ y $\{1,\beta,\beta^2, \ldots, \beta^{m-1}\}$ de potencias, linealmente independientes, de los elementos primitivos α y β, de los campos $GF(p)$ y $GF(p^m)$, respectivamente. Estas bases, que pueden considerarse como las bases canónicas de ambos $GF(p)$) - espacios vectoriales, dan lugar a matrices mxn, esto es, de m filas y n columnas, representantes de los diferentes homomorfismos de inmersión de $GF(p)$ y $GF(p^m)$.

Denotando al entero $\frac{p^m-1}{p^n-1}$ como k_1 y k_t como a cada entero tk_1 para cada y primo relativo con el mismo, resulta que los elementos β^{k_t} son los de orden p^n-1 n el campo $GF(p^m)$. Esto significa que las funciones h_t de $GF(p^n)$ en $GF(p^m)$, definidas como $h_t(0)=0$ y $h_t(\alpha^i)=\beta^{ik_t}$ para cada son homomorfismos multiplicativos entre los monoides $(GF(p^n))^*$ y $(GF(p^m))^*$.

Por el llamado teorema de existencia de las aplicaciones lineales sabemos que para cada función ht existe una única aplicación lineal $f_t: GF(p^n)\rightarrow GF(p^m)$ tal que $f_t(\alpha^i)=h_t(\alpha^i)$ para todo $i \in \{0,1,2,...,n-1\}$, ya que $\{1,\alpha, \alpha^2,..., \alpha^{n-1}\}$ es una base del espacio de partida $GF(p^n)$ [4,5]. Entonces, los homomorfismos de inserción son las funciones que coinciden con su aplicación lineal asociada en todo su dominio $GF(p^n)$, es decir, son las que son multiplicativas y, al mismo tiempo aditivas y $\mathbb{Z}p$-lineales.

3. Obtención de los elementos del campo como los componentes de una sucesión recurrente lineal

Al polinomio irreducible $p(x)=x^n-\sum_{i=0}^{n-1}c_i x^i$ asociamos la matriz cuadrada

$$M_{p(x)}=\begin{pmatrix} 0 & 0 & .. & 0 & c_0 \\ 1 & 0 & .. & 0 & c_1 \\ 0 & 0 & .. & 0 & c_2 \\ .. & .. & .. & .. & \vdots \\ 0 & 0 & 0 & 1 & c_{n-1} \end{pmatrix}$$

a la que llamamos matriz acompañante del polinomio $p(x)$. No es difícil probar que el polinomio característico $Det(M_{p(x)}-zI_n)$ es precisamente $p(x)$ y que representando como matrices columnas a los elementos

$$0,1,\alpha,\alpha^2,\alpha^3,\ldots,\alpha^{n-1},an=\sum_{i=0}^{n-1}(-c_i)\alpha^i,\alpha^{n+1},\ldots,\alpha^{p^n-2}$$

$GF(p^n)$, siendo α un elemento primitivo, dicha matriz convierte cada elemento no nulo en su siguiente como potencia de α, siendo las correspondientes matrices columnas los componentes vectoriales de una sucesión recurrente lineal cuyo período es un divisor del número p^n-1. Si el polinomio es, además de irreducible, un polinomio primitivo, entonces, el período de la sucesión es exactamente p^n-1, que es el máximo posible. Esto es necesario para que el elemento α, raíz de $p(x)$, sea un generador del grupo multiplicativo $(GF(p^n))^*$.

A continuación veremos un teorema que nos da una condición necesaria y suficiente para que las funciones sean la misma función.

Teorema 1:

Para campos de Galois $GF(p^n)$ y $GF(p^m)$, siendo n un divisor de m, y los elementos primitivos $\alpha \in GF(p^n)$ y $\beta \in GF(p^n)$consideremos la función hr: $GF(p^n)\rightarrow GF(p^m)$ definida por: $h_t(0)=0, h_t(\alpha^i)=\beta^{k_t i}$ donde $k_t=t\,k_1$ siendo $k_1=\frac{p^m-1}{p^n-1}$ y t primo relativo con p^n-1. Denotemos f_t por a la aplicación lineal, única

$$f_t: GF(p^n)\rightarrow GF(p^m)$$

tal que, $h_t(\alpha^i)=f_t(\alpha^i)$ para todo $i \in \{0,1,2,...n-1\}$, esto es, para el cero y para los elementos de la base $(1,\alpha, \alpha^{n-1})$ de $GF(p^n)$. Entonces, para que h_t y f_t sean la misma función es suficiente, y necesario, que se verifique la igualdad $h_t(\alpha^n)=f_t(\alpha^n)$.

Demostración:

La condición es, obviamente, necesaria. Probemos que es suficiente:

El elemento β^{k_t} es del mismo orden que α, que es igual a p^n-1. La función h_t, así definida, es obviamente un homomorfismo de monoides, entre los monoides multiplicativos $(GF(p^n))^*$ y $(GF(p^m))^*$ y, restringida, es un homomorfismo de grupos entre los grupos multiplicativos, (cíclicos), $(GF(p^n))^*$ y $(GF(p^m))^*$.

Siendo α raíz del polinomio primitivo

$$p(x)=x^n-\sum_{i=0}^{n-1}c_i x^i\ ,$$

se tiene la igualdad $\alpha^n=\sum_{i=0}^{n-1}c_i\alpha^i$. Los elementos del campo $GF(p^n)$ son, además del cero, los términos de la sucesión recurrente lineal [1] $(\alpha^j)_{j=0}^{\infty}$, donde los primeros n términos son $1,\alpha, \alpha^2,..., \alpha^{n-1}$ y para $r \geq 0$ se cumple la relación de recurrencia

lineal:

$$a^{n+r} = \sum_{i=0}^{n-1} c_i \alpha^{j+r}$$

esto es, para $j \geq n$,

$$a^{j} = \sum_{i=0}^{n-1} c_i \alpha^{i+j-n}$$

Esta es la S.R.L. cuyo polinomio generador es el polinomio primitivo

$$p(x) = x^n - \sum_{i=0}^{n-1} c_i x^i$$

siendo su período igual a $p^n - 1$, que es el orden del elemento primitivo α, generador del grupo multiplicativo $(GF(p^n))^*$.

Necesitamos probar que, para todo natural se verifica la igualdad $h_t(\alpha^{n+r}) + f_t(\alpha^{n+r})$. Lo probaremos usando el método de inducción completa, aplicado a la variable natural r.

Para $r = 1$.

$f_t(\alpha^{n+1}) = f_t(\alpha n.\alpha) = f_t\left(\left(\sum_{i=0}^{n=1} c_i \alpha^i\right).\alpha^1\right) = f_t\left(\sum_{i=0}^{n=1} c_i \alpha^{i+1}\right)$,por ley distributiva,

$= \sum_{i=0}^{n-1} c^i f_t(\alpha^{i+1})$, por ser f_t una aplicación lineal,

$= \sum_{i=0}^{n-1} c^i h_t(\alpha^{i+1})$, por ser f_t y h_t coincidentes para todos los exponentes menores o iguales que n,

$= \sum_{i=0}^{n-1} c^i h_t(\alpha)^i.h_t(\alpha)$, por ser h_t multiplicativa,

$= \left(\sum_{i=0}^{n-1} c^i h_t(\alpha)^i\right).h_t(\alpha)$, de nuevo por ley distributiva,

$= \left(\sum_{i=0}^{n-1} c^i f_t(\alpha)^i\right).h_t(\alpha)$, de nuevo por la coincidencia de ambas para exponentes menores que n,

$= \left(\sum_{i=0}^{n-1} c^i f_t(\alpha)^i\right).h_t(\alpha) = f_t(\alpha^n).h_t(\alpha).h_t(\alpha^n).h_t(\alpha^n.\alpha) = h_t(\alpha^{n+1})$

de nuevo por la coincidencia y por ser h_t multiplicativa.

Queda pues probado que $f_t(\alpha^{n+1}) = h_t(\alpha^{n+1})$

Suponiendo ahora cierta la igualdad para todo exponente menor a $n + r$, para $r \geq 2$, obtenemos:

$f_t(\alpha^{n+r}) = f_t(\alpha^n \cdot \alpha^r) = f_t\left(\left(\sum_{i=0}^{n-1} c_i a^i\right) \cdot \alpha^r\right) = f_t\left(\sum_{i=0}^{n-1} c_i \alpha^{i+r}\right)$,

por ley distributiva,

$= \sum_{i=0}^{n-1} c^i f_t(\alpha^{i+r})$, por ser f_t una aplicación lineal,

$= \sum_{i=0}^{n-1} c^i h_t(\alpha^{i+r})$, por ser f_t y h_t coincidentes para todos los exponentes i menores que

$= \sum_{i=0}^{n-1} c^i h_t(\alpha)^i.h_t(\alpha^r)$, por ser h_t multiplicativa,

$= \left(\sum_{i=0}^{n-1} c^i h_t(\alpha)^i\right).h_t(\alpha^r)$, de nuevo por ley distributiva,

$= \left(\sum_{i=0}^{n-1} c^i f_t(\alpha)^i\right).h_t(\alpha^r)$, de nuevo por la coincidencia de ambas para exponentes menores que $n + r$,

$= f_t\left(\sum_{i=0}^{n-1} c^i (\alpha)^i\right).h_t(\alpha) = f_t(\alpha^n).h_t(\alpha) =$

$= h_t(\alpha^n).h_t(\alpha) = h_t(\alpha^n.\alpha) = h_t(\alpha^{n+1})$

de nuevo por la coincidencia y por ser h_t multiplicativa

Queda así probado que $f_t(\alpha^{n+r}) = h_t(\alpha^{n+r})$, para todo r natural.

Por consiguiente, ambas funciones coinciden en todo su dominio. El teorema queda demostrado.

Nota: El teorema 1 significa que, siendo las sucesiones recurrentes lineales $(f_t(\alpha^j))_{j=0}^{\infty}$ y $(h_t(\alpha^j))_{j=0}^{\infty}$, del mismos grado n, con la misma relación de recurrencia y con los primeros n componentes iguales, ambas son necesariamente iguales, en todos sus términos.

Homomorfismos entre los campos *GF(8)* y *GF(64)*

El campo *GF(8)* se obtiene como extensión de *GF(2)* = {0,1} mediante la adjunción de una raíz de un polinomio irreducible de grado 3.

El polinomio $x^3 + x + 1$ es irreducible sobre el campo binario $\mathbb{Z}_2 = GF(2)$. Es además primitivo, ya que cualquiera de sus raíces es de orden $7 = 2^3 - 1$, Sea α una raíz de este polinomio. Por ser primitivo el polinomio cualquiera de sus raíces genera al grupo multiplicativo $(GF(8))^*$ del campo *GF*(8). El campo se describe como $GF(8) = \{1, \alpha, \alpha^2, 1 + \alpha, \alpha + \alpha^2, 1 + \alpha + \alpha^2, 1 + \alpha^2\}$

El campo $GF(64) = GF(2)(\alpha)$ donde α es una raíz del polinomio irreducible de grado 6 $x^6 + x + 1 \in GF(2)[x]$.

Un homomorfismo $h: GF(8) \rightarrow GF(64)$ inyectivo convierte al grupo cíclico $(GF(8))^*$ en un subgrupo del grupo cíclico $(GF(64))^*$. Luego, h convierte al generador α en un elemento que es también de orden 7, que es el orden del grupo multiplicativo $(GF(8))^*$, dentro del grupo $(GF(64))^*$, que es de orden $2^6 - 1 = 63$. En el campo GF(64) el elemento β^9 es de orden 7 y , en general, elementos de orden 7 son los de la forma β^{9t} donde cada t es un entero positivo que es primo relativo con 7. Es decir, $t \in \{1,2,3,4,5,6\}$.

Por tanto $\beta^9, \beta^{18}, \beta^{27}, \beta^{37}, \beta^{45}, \beta^{54}$ son los elementos de orden 7.

Por consiguiente, hay 6 posibilidades para definir h:

h_1: $\alpha \rightarrow \beta^9 = \beta^3 + \beta^4 = (0,0,0,1,1,0)$

h_2: $\alpha \rightarrow \beta^{18} = 1 + \beta + \beta^2 + \beta^3 = (1,1,1,1,0,0)$

h_3; $\alpha \rightarrow \beta^{27} = \beta + \beta^2 + \beta^3 = (0,1,1,1,0,0)$

h_4; $\alpha \rightarrow \beta^{36} = \beta + \beta^2 + \beta^4 = (0,1,1,0,1,0)$

h_5; $\alpha \rightarrow \beta^{45} = 1 + \beta^3 + \beta^4 = (1,0,0,1,1,0)$

h_6; $\alpha \rightarrow \beta^{54} = 1 + \beta + \beta^2 + \beta^4 = (1,1,1,0,1,0)$

Aquí, representamos cada expresión polinómica en β, de grado menor igual a 6, como el sexteto de ceros y unos asociado a la misma.

Cada función h_t tiene una aplicación lineal asociada f_t.

Sean $\{1,\alpha\}\{1,\beta,\beta^2,\beta^3,\beta^4,\beta^5\}$las bases de los campos $GF(8)$ y $GF(64)$ respectivamente. Las matrices asociadas a dichas aplicaciones lineales con respecto a estas bases son

$$M(f_1)=\begin{bmatrix}1&0&1\\0&0&1\\0&0&1\\0&1&1\\0&1&0\\0&0&0\end{bmatrix}, M(f_2)=\begin{bmatrix}1&1&0\\0&1&1\\0&1&1\\0&1&0\\0&0&1\\0&0&0\end{bmatrix}, M(f_3)=\begin{bmatrix}1&0&1\\0&1&1\\0&1&1\\0&1&0\\0&0&1\\0&0&0\end{bmatrix},$$

$$M(f_4)=\begin{bmatrix}1&0&0\\0&1&0\\0&1&0\\0&0&1\\0&1&1\\0&0&0\end{bmatrix}, M(f_5)=\begin{bmatrix}1&1&0\\0&0&1\\0&0&1\\0&1&1\\0&1&0\\0&0&0\end{bmatrix}, M(f_6)=\begin{bmatrix}1&1&1\\0&1&0\\0&1&0\\0&0&1\\0&1&1\\0&0&0\end{bmatrix}$$

Representando como matrices columnas a los elementos de ambos campos, tendríamos:

$$GF(8)=\left\{\begin{array}{l}0=\begin{bmatrix}0\\0\\0\end{bmatrix}, 1=\begin{bmatrix}1\\0\\0\end{bmatrix}, \alpha=\begin{bmatrix}0\\1\\0\end{bmatrix}, \alpha^2=\begin{bmatrix}0\\0\\1\end{bmatrix},\\ \alpha^3=1+\alpha\begin{bmatrix}1\\1\\0\end{bmatrix}, \alpha^4=\alpha+\alpha^2=\begin{bmatrix}0\\1\\1\end{bmatrix},\\ \alpha^5=1+\alpha+\alpha^2=\begin{bmatrix}1\\1\\1\end{bmatrix}, \alpha^6=1+\alpha^2=\begin{bmatrix}1\\0\\1\end{bmatrix}\end{array}\right\}$$

mientras los de $GF(64)$ se representan según la tabla (Anexo 1) tomando la transpuesta de la matriz fila correspondiente a cada potencia obtenida.

Analicemos ahora cada uno de los casos por separado y recordemos que según el teorema 1, f_t y h_t para que sean la misma función es suficiente, y necesario, que se verifique la igualdad $f_t(\alpha^3)=h_t(\alpha^3)$.

Caso 1: h_1: $\alpha\rightarrow\beta^9$

$$h_1(0)=0=\begin{bmatrix}0\\0\\0\\0\\0\\0\end{bmatrix}, h_1(\alpha^0)=h_1(1)=1=\begin{bmatrix}1\\0\\0\\0\\0\\0\end{bmatrix}, h_1(\alpha)=\beta^9=\begin{bmatrix}0\\0\\0\\1\\1\\0\end{bmatrix},$$

$$h_1(\alpha^2)=\beta^{18}=\begin{bmatrix}1\\1\\1\\1\\0\\0\end{bmatrix}, h_1(\alpha^3)=\beta^{27}=\begin{bmatrix}0\\1\\1\\1\\0\\0\end{bmatrix}$$

La matriz, $M(f_1)=\begin{bmatrix}1&0&1\\0&0&1\\0&0&1\\0&1&1\\0&1&0\\0&1&0\end{bmatrix}$ actúa sobre los elementos de la manera siguiente

$$\begin{bmatrix}0\\0\\0\end{bmatrix}\rightarrow\begin{bmatrix}0\\0\\0\\0\\0\\0\end{bmatrix};\begin{bmatrix}1\\0\\0\end{bmatrix}\rightarrow\begin{bmatrix}1\\0\\0\\0\\0\\0\end{bmatrix},\begin{bmatrix}0\\1\\0\end{bmatrix}\rightarrow\begin{bmatrix}0\\0\\0\\1\\1\\0\end{bmatrix}\begin{bmatrix}0\\0\\1\end{bmatrix}\rightarrow\begin{bmatrix}1\\1\\1\\1\\0\\0\end{bmatrix},\begin{bmatrix}1\\1\\0\end{bmatrix}\rightarrow\begin{bmatrix}1\\0\\0\\1\\1\\0\end{bmatrix}$$

Se aprecia que el elemento imagen, obtenido por el producto matricial es el que corresponde, como potencia de β, según la sustitución h_1: $\alpha\rightarrow\beta^9$ excepto en el caso de

$$h_1(\alpha^3)=\beta^{27}=\begin{bmatrix}0\\1\\1\\1\\0\\0\end{bmatrix}\neq\begin{bmatrix}1\\0\\0\\1\\1\\0\end{bmatrix}$$

Es decir, ambas funciones, la aditiva f_1 y la multiplicativa h_1, no son la misma. De aquí resulta que la sustitución no define un homomorfismo de campos.

Caso 2. h_2: $\alpha\rightarrow\beta^{19}$

$$h_2(\alpha^3)=\beta^{54}=1+\beta+\beta^2+\beta^4\begin{bmatrix}1\\1\\1\\0\\1\\0\end{bmatrix}$$

Si hacemos lo mismo con la matriz $M(f_2)$, vemos que la misma transforma el elemento α^3 de *GF(8)* en un elemento de *GF(64)* diferente de β^{54}

$$\begin{bmatrix}1&1&1\\0&1&1\\0&1&1\\0&1&0\\0&0&1\\0&0&0\end{bmatrix}\begin{bmatrix}1\\1\\0\end{bmatrix}=\begin{bmatrix}0\\1\\1\\1\\0\\0\end{bmatrix}\neq\begin{bmatrix}1\\1\\1\\0\\1\\0\end{bmatrix} \qquad f_2(\alpha^3)\neq h_2(\alpha^3)$$

Al igual que en el caso 1 las funciones, la aditiva f_2 y la multiplicativa h_2 no son la misma. De aquí resulta que la sustitución h_2: $\alpha\rightarrow\beta^{18}$ tampoco define un homomorfismo de campos.

Caso 3 : h_3: $\alpha\rightarrow\beta^{27}$

$$h_3(\alpha^3)=\beta^{81}=\beta^{18}=1+\beta+\beta^2+\beta^3=\begin{bmatrix}1\\1\\1\\1\\0\\0\end{bmatrix}$$

Si hacemos lo mismo con la matriz, $M(f_3)$ vemos que la misma transforma el elemento α^3 de $GF(8)$ en un elemento de $GF(64)$ igual a β^{18}.

$$\begin{bmatrix}1&0&1\\0&1&1\\0&1&1\\0&1&0\\0&0&1\\0&0&0\end{bmatrix}\begin{bmatrix}1\\1\\0\end{bmatrix}=\begin{bmatrix}1\\1\\1\\1\\0\\0\end{bmatrix}=\begin{bmatrix}1\\1\\1\\1\\0\\0\end{bmatrix} \qquad f_3(\alpha^3)=h_3(\alpha^3)$$

En este caso ambas funciones la aditiva f_3 y la multiplicativa h_3 son la misma función De aquí resulta que la sustitución h_3: $\alpha\rightarrow\beta^{27}$ define un homomorfismo de campos que inserta *GF(8)* en *GF(64)*

Caso 4: h_4: $\alpha\rightarrow\beta^{36}$

$$h_4(\alpha^3)=\beta^{108}=\beta^{45}=1+\beta^3+\beta^3=\begin{bmatrix}1\\0\\0\\1\\1\\0\end{bmatrix}$$

Si hacemos lo mismo con la matriz, $M(f_4)$ vemos que la misma transforma el elemento α^3 de *GF(8)* en un elemento de *GF(64)* desigual de β^{45}

$$\begin{bmatrix}1&0&0\\0&1&0\\0&1&0\\0&0&1\\0&1&1\\0&0&0\end{bmatrix}\begin{bmatrix}1\\1\\0\end{bmatrix}=\begin{bmatrix}1\\1\\1\\0\\1\\0\end{bmatrix}\neq\begin{bmatrix}1\\0\\0\\1\\1\\0\end{bmatrix} \qquad f_4(\alpha^3)\neq h_4(\alpha^3)$$

En este caso ambas funciones f_4 y la multiplicativa h_4 no son la misma función. De aquí resulta que la sustitución h_4: $\alpha\rightarrow\beta^{36}$ no define un homomorfismo de campos.

Caso 5: h_5: $\alpha\rightarrow\beta^{45}$

$$h_5(\alpha^3)=\beta^{135}=\beta^9=\beta^3+\beta^4=\begin{bmatrix}0\\0\\0\\1\\1\\0\end{bmatrix}$$

Si hacemos lo mismo con la matriz, $M(f_5)$ vemos que la misma transforma el elemento α^3 de *GF(8)* en un elemento de *GF(64)* igual a β^{36}

$$\begin{bmatrix}1&1&0\\0&0&1\\0&0&1\\0&1&1\\0&1&0\\0&0&0\end{bmatrix}\begin{bmatrix}1\\1\\0\end{bmatrix}=\begin{bmatrix}0\\0\\0\\1\\1\\0\end{bmatrix}=\begin{bmatrix}1\\0\\0\\1\\1\\0\end{bmatrix} \qquad f_5(\alpha^3)=h_5(\alpha^3)$$

En este caso ambas funciones f_5 y h_5 son la misma función. De aquí resulta que la sustitución h_5: $\alpha\rightarrow\beta^{45}$ define un homomorfismo de campos que inserta *GF(8)* en *GF(64)*.

Caso 6: h_6: $\alpha\rightarrow\beta^{54}$

$$h_6(\alpha^3)=\beta^{162}=\beta^{36}=\beta+\beta^3+\beta^4=\begin{bmatrix}0\\1\\0\\1\\1\\0\end{bmatrix}$$

Si hacemos lo mismo con la matriz, *M(f6)* vemos que la misma transforma el elemento α^3 de *GF(8)* en un elemento de *GF(64)* igual a β^{36}

$$\begin{bmatrix}1&1&1\\0&1&0\\0&1&0\\0&0&1\\0&1&1\\0&0&0\end{bmatrix}\begin{bmatrix}1\\1\\0\end{bmatrix}=\begin{bmatrix}0\\1\\1\\0\\1\\0\end{bmatrix}=\begin{bmatrix}0\\1\\1\\0\\1\\0\end{bmatrix} \qquad f_6(\alpha^3)=h_6(\alpha^3)$$

En este caso ambas funciones f_6 y h_6 son la misma función. De aquí resulta que la sustitución h_6: $\alpha \rightarrow \beta^{54}$ define un homomorfismo de campos que inserta *GF(8)* en *GF(64).*

4. Conclusión

Hemos visto que el campo de Galois *GF(8)*, se sumerge de tres maneras diferentes en el campo *GF(64)*. h_3: $\alpha \rightarrow \beta^{27}$, h_5: $\alpha \rightarrow \beta^{45}$, h_6: $\alpha \rightarrow \beta^{54}$ aunque en los tres casos el subcampo isomorfo a *GF(8)* es el mismo, pues está formado por los mismos elementos: 0,1, β^9, β^{18}, β^{27}, β^{36}, β^{45}, β^{54}.

Anexo 1

Potencia de β	Polinomio de grado menor o igual que 5 y secuencia binaria correspondiente
β^0	$1 = (1,0,0,0,0,0)$
β^1	$\beta = (0,1,0,0,0,0)$
β^2	$\beta^2 = (0,0,1,0,0,0)$
β^3	$\beta^3 = (0,0,0,1,0,0)$
β^4	$\beta^4 = (0,0,0,0,1,0)$
β^5	$\beta^5 = (0,0,0,0,0,1)$
β^6	$1 + \beta = (1,1,0,0,0,0)$
β^7	$\beta + \beta^2 = (0,1,1,0,0,0)$
β^8	$\beta^2 + \beta^3 = (0,0,1,1,0,0)$
β^9	$\beta^3 + \beta^4 = (0,0,0,1,1,0)$
β^{10}	$\beta^4 + \beta^5 = (0,0,0,0,1,1)$
β^{11}	$1 + \beta + \beta^5 = (1,1,0,0,0,1)$
β^{12}	$1 + \beta^2 = (1,0,1,0,0,0)$
β^{13}	$\beta + \beta^3 = (0,1,0,0,1,0)$
β^{14}	$\beta^2 + \beta^4 = (0,0,1,0,1,0)$
β^{15}	$\beta^3 + \beta^5 = (0,0,0,1,0,1)$
β^{16}	$1 + \beta + \beta 4 = (1,1,0,0,1,0)$
β^{17}	$\beta + \beta^2 + \beta^5 = (0,1,1,0,0,1)$
β^{18}	$1 + \beta + \beta^2 + \beta^3 = (1,1,1,1,0,0)$
β^{19}	$\beta + \beta^2 + \beta^3 + \beta^5 = (0,1,1,1,1,0)$
β^{20}	$\beta^2 + \beta^3 + \beta^4 + \beta^5 = (0,0,1,1,1,1)$
β^{21}	$1 + \beta + \beta^3 + \beta^4 + \beta^5 = (1,1,0,1,1,1)$
β^{22}	$1 + \beta^2 + \beta^4 + \beta^5 = (1,0,1,0,1,1)$
β^{23}	$1 + \beta^3 + \beta^5 = (1,0,0,1,0,1)$
β^{24}	$1 + \beta^4 = (1,0,0,0,1,0)$
β^{25}	$\beta + \beta^5 = (0,1,0,0,0,1)$
β^{26}	$1 + \beta + \beta^2 = (1,1,1,0,0,0)$
β^{27}	$\beta + \beta^2 + \beta^3 = (0,1,1,1,0,0)$
β^{28}	$\beta^2 + \beta^3 + \beta^4 = (0,0,1,1,1,0)$
β^{29}	$\beta^3 + \beta^4 + \beta^5 = (0,0,0,1,1,1)$
β^{30}	$1 + \beta + \beta^4 + \beta^5 = (1,1,0,0,1,1)$
β^{31}	$1 + \beta^2 + \beta^5 = (1,0,1,0,0,1)$
β^{32}	$1 + \beta^3 = (1,0,0,1,0,0)$
β^{33}	$\beta + \beta^4 = (0,1,0,0,1,0)$
β^{34}	$\beta^2 + \beta^5 = (0,0,1,0,0,1)$
β^{35}	$1 + \beta + \beta^3 = (1,1,0,1,0,0)$
β^{36}	$\beta + \beta^2 + \beta^4 = (0,1,1,0,1,0)$
β^{37}	$\beta^2 + \beta^3 + \beta^5 = (0,0,1,1,0,1)$
β^{38}	$1 + \beta + \beta^3 + \beta^4 = (1,1,0,1,1,0)$
β^{39}	$\beta + \beta^2 + \beta^4 + \beta^5 = (0,1,1,0,1,1)$
β^{40}	$1 + \beta + \beta^2 + \beta^3 + \beta^5 = (1,1,1,1,0,1)$
β^{41}	$1 + \beta^2 + \beta^3 + \beta^4 = (1,0,1,1,1,0)$
β^{42}	$\beta + \beta^3 + \beta^4 + \beta^5 = (0,1,0,1,1,1)$
β^{43}	$1 + \beta + \beta^2 + \beta^4 + \beta^5 = (1,1,1,0,1,1)$
β^{44}	$1 + \beta^2 + \beta^3 + \beta^5 = (1,0,1,1,0,1)$
β^{45}	$1 + \beta^3 + \beta^4 = (1,0,0,1,1,0)$
β^{46}	$\beta + \beta^4 + \beta^5 = (0,1,0,0,1,1)$
β^{47}	$1 + \beta + \beta^2 + \beta^5 = (1,1,1,0,0,1)$
β^{48}	$1 + \beta^2 + \beta^3 = (1,0,0,1,0,0)$
β^{49}	$\beta + \beta^3 + \beta^4 = (0,1,0,1,1,0)$
β^{50}	$\beta^2 + \beta^4 + \beta^5 = (0,0,1,0,1,1)$
β^{51}	$1 + \beta + \beta^3 + \beta^5 = (1,1,0,1,0,1)$
β^{52}	$1 + \beta^2 + \beta^4 = (1,0,1,0,1,0)$
β^{53}	$\beta + \beta^3 + \beta^5 = (0,1,0,1,1,0)$
β^{54}	$1 + \beta + \beta^2 + \beta^4 = (1,1,1,0,1,0)$
β^{55}	$\beta + \beta^2 + \beta^3 + \beta^5 = (0,1,1,1,0,1)$
β^{56}	$1 + \beta + \beta^2 + \beta^3 + \beta^4 = (1,1,1,1,1,0)$
β^{57}	$\beta + \beta^2 + \beta^3 + \beta^4 + \beta^5 = (0,1,1,1,1,1)$

Potencia de β	Polinomio de grado menor o igual que 5 y secuencia binaria correspondiente
β^{58}	$1 + \beta + \beta^2 + \beta^3 + \beta^4 + \beta^5 = (1,1,1,1,1,1)$
β^{59}	$1 + \beta^2 + \beta^3 + \beta^4 + \beta^5 = (1,0,1,1,1,1)$
β^{60}	$1 + \beta^3 + \beta^4 + \beta^5 = (1,0,0,1,1,1)$
β^{61}	$1 + \beta^4 + \beta^5 = (1,0,0,0,1,1)$
β^{62}	$1 + \beta^5 = (1,0,0,0,0,1)$
β^{63}	1

Referencias bibliográficas

[1] LIDL RUDOLF, HARALD NIEDERRAITER. Campos finitos. Moscú. Mir 1998. Tomo 1 y 2.

[2] JOHN F. FRALEIGH, A first course in abstract Álgebra. .Addison Wesley publishing company, 1967.Fourth printing, 1972.

[3] MINIEIEV N.P., CHUBARIKOV V.N. Conferencias sobre cuestiones aritméticas de la Criptografía. Moscú. Editorial de la Universidad de Moscú 2010.

[4] JOSEFA MARÍN MOLINA, ÁNGEL BALAGUER BESER, ELENA ALEMANY MARTINEZ. Un Curso de Álgebra con ejercicios (I).Universidad Politécnica de Valencia. 2004.

[5] FRED IZABO, Linear Álgebra: An Introduction Using Maple. Harcourt. Academic Press. Año 2002.