Miscelánea Matemática **53** (2011) 81–100 SMM

Sobre algunas aplicaciones de los campos de Galois

Horacio Tapia-Recillas

htr@xanum.uam.mx

Departamento de Matemáticas
Universidad Autónoma Metropolitana-Iztapalapa
09340 México, D.F., MEXICO

Resumen

En esta nota se bosquejan algunas aplicaciones de los Campos de Galois.

1. Introducción

En su trabajo [**13**], Evaristo Galois resolviendo congruencias módulo un primo p, quizá sin percibirlo de esa manera, introdujo lo que actualmente se conoce como *enteros modulares módulo* p, uno de los campos finitos con p elementos mas importantes, ya que a partir de éste se construyen otros campos con p^n elementos para cualquier entero $n > 1$. En su trabajo [**12**] Galois introdujo las ideas sobre lo que ahora se conoce como la *Teoría de Galois*. De gran relevancia en la actualidad es el caso $p = 2$, el campo de los *números binarios*. El estudio de los Campos de Galois no tuvo grandes avances por mucho tiempo; pero en las últimas décadas debido a las aplicaciones que tienen en diversas áreas de la Matemática así como en otras de gran relevancia en nuestros días como son las Comunicaciones digitales y Seguridad Informática, ha habido un gran desarrollo y estudio sobre diversos aspectos de los Campos de Galois. Presentar en forma detallada dónde y cómo se usan actualmente los campos de Galois sería interesante, pero también una gran tarea. El propósito de esta nota es mencionar a grandes rasgos algunas áreas donde los campos de Galois se ponen de manifiesto, sin proporcionar detalles sobre la misma área o aplicación. El lector interesado en profundizar en alguna de estas áreas o aplicaciones puede consultar, por ejemplo, las referencias proporcionadas en la bibliografía.

2. Construcción de Campos Finitos

En esta sección se introducirá el concepto de *Campo de Galois* o *Campo Finito*, el cual se motivará a partir de un caso concreto y se dará su construcción en forma general. Asimismo se mencionarán algunas de las propiedades mas importantes de dichos objetos algebraicos.

2.1. Un ejemplo

Recordemos que el campo de los *números binarios* es $(GF(2), +, *)$ donde $GF(2) = \{0, 1\}$ es el anillo de enteros módulo 2, con las operaciones de suma "$+$" y producto "$*$" usuales en esos anillos. Una de las propiedades que debe satisfacer un anillo para que sea *campo* es que cualquier elemento distinto de cero tiene un inverso, cosa que sucede (trivialmente) en este caso ya que el único elemento distinto de cero de $GF(2)$ es el 1, además de que este anillo es un domino entero. Al campo de los números binarios tambien se acostumbra denotarlo por $\mathbb{F}_2$.

Sea $GF(2)[x]$ el anillo de polinomios en una indeterminada con coeficientes en $GF(2)$. Es fácil ver que el polinomio $f(x) = x^2 + x + 1 \in GF(2)[x]$ es irreducible sobre $GF(2)$. Considérese ahora el anillo cociente, es decir, las clases de equivalencia de $GF(2)[x]$ módulo el ideal $\langle f(x)\rangle$ generado por el polinomio $f(x)$:

$$GF(2)[x]/\langle f(x)\rangle = \{a(x) + \langle f(x)\rangle : a(x) \in GF(2)[x]\}$$

Usando el algoritmo de la división en el anillo $GF(2)[x]$ (recordemos que este anillo es euclidiano y de ideales principales), se tiene que para cualquier elemento $a(x) \in GF(2)[x]$:

$$a(x) = f(x)q(x) + r(x),\ 0 \leq \text{gr}(r(x)) \leq 1.$$

Por lo tanto, un representante de la clase $[a(x)] = a(x) + \langle f(x)\rangle$ de $a(x)$ es de la forma $a_0 + a_1x$ con $a_0, a_1 \in GF(2)$. Por consiguiente los elementos del anillo $GF(2)[x]/\langle f(x)\rangle$ se pueden identificar con el conjunto

$$GF(2^2) = \{a_0 + a_1x : a_0, a_1 \in GF(2)\} = \{0, 1, \alpha, 1 + \alpha\},$$

donde $\alpha = [x] = x + \langle f(x)\rangle$.

Obsérvese que:

1. $GF(2^2)$ tiene cardinalidad $2^{\text{gr}(f(x))} = 4$.

2. Dado que en $GF(2)$, $1 = -1$, $\alpha \in GF(2^2)$ es una raíz de $f(x)$, es decir, $\alpha^2 = \alpha + 1$.

3. El conjunto $GF(2^2)$ es un campo. Para esto basta describir la tabla de la suma "$+$" y el producto "$*$". La tabla de la suma es:

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

La relación $\alpha^2 = \alpha+1$ permite realizar la aritmética multiplicativa sobre $GF(2^2)$, como se ve en la siguiente tabla:

$*$	1	α	$\alpha+1$
1	1	α	$\alpha+1$
α	α	$\alpha+1$	1
$\alpha+1$	$\alpha+1$	1	α

De las tablas anteriores se puede observar lo siguiente:

a) La pareja $(GF(2^2), +)$ es un grupo conmutativo.

b) Si $GF(2^2)^* = GF(2^2) \setminus \{0\}$, la pareja $(GF(2^2)^*, *)$ es un grupo multiplicativo. En particular todo elemento distinto de cero tiene un inverso.

c) Mas aún, $GF(2^2)^*$ es un grupo cíclico:

$$GF(2^2)^* = \langle\alpha\rangle = \{1, \alpha, \alpha^2 = 1 + \alpha\}.$$

d) $GF(2^2)$ es un espacio vectorial de dimensión 2 sobre $GF(2)$. Una base está dada por $\{1, \alpha\}$.

De las observaciones anteriores se sigue que $(GF(2^2), +, *)$ es un *campo* con 4 elementos, llamado de *Galois* o *finito*.

2.2. Caso general

Veamos ahora cómo se construye, en general, un campo finito. Sea p un número primo y $\mathbb{Z}_p = GF(p)$ el campo de los enteros módulo p, al cual se le llama *campo primo*. Sea $GF(p)[x]$ el anillo de polinomios en la indeterminada x con coeficientes en $GF(p)$ y $f(x) \in GF(p)[x]$ un polinomio irreducible de grado n. Sea

$$GF(p)[x]/\langle f(x)\rangle = \{a(x) + \langle f(x)\rangle : a(x) \in GF(p)[x]\}$$

el anillo de clases residuales de $GF(p)[x]$ módulo el ideal $\langle f(x)\rangle$ generado por $f(x)$.

Dado que $GF(p)[x]$ es un anillo euclidiano (y de ideales principales), si $a(x) \in GF(p)[x]$, por el algoritmo de la división,

$$a(x) = q(x)f(x) + r(x),\ 0 \leq \text{gr}(r(x)) \leq n-1,$$

y un representante de la clase $a(x) + \langle f(x)\rangle$, de $a(x) \in GF(p)[x]$, es de la forma:

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1},\ a_i \in GF(p).$$

Por lo tanto, los elementos de $GF(p)[x]/\langle f(x)\rangle$ se pueden identificar con el conjunto:

$$\mathbb{F} = \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1},\ a_i \in GF(p)\}.$$

A continuación se mencionarán algunas de las propiedades de $\mathbb{F}$, para las cuales, por falta de espacio, no se dará una demostración; sin embargo el lector interesado puede consultar estas y otras propiedades, por ejemplo en [**22**],[**25**],[**23**], o bien dar su propia demostración.

1. $(\mathbb{F}, +, *)$ es un campo con p^n elementos, donde "$+$" y "$*$" son las operaciones usuales del anillo cociente. A este campo se acostumbra denotarlo por $GF(p^n)$ o bien $\mathbb{F}_{p^n}$ y se le llama el *campo de Galois* o el *campo finito* con p^n elementos.

2. La clase residual $\alpha \in GF(p^n)$ del polinomio x es tal que $f(\alpha) = 0$, es decir, α es una raíz de $f(x)$.

3. $GF(p^n)^* = GF(p^n) \setminus \{0\}$ es un grupo cíclico de orden $p^n - 1$. A un generador de este grupo se le llama *primitivo*.

4. El campo $GF(p^n)$ es un $GF(p)$-espacio vectorial de dimensión n y una base (natural) es:

   $$\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}.$$

   Por consiguiente, $GF(p^n)$ es una extensión de grado n de $GF(p)$.

5. El campo de Galois con p^n elementos es único módulo isomorfismos.

El lector podrá observar que para construir un campo de Galois con p^n elementos es necesario un polinomio irreducible con coeficientes en $GF(p)$ de grado $n \geq 2$. Es interesante preguntarse cómo obtener tales polinomios.

3. Algunas aplicaciones de los campos de Galois

Una vez que se ha introducido el concepto de campo de Galois, en las siguientes líneas se dará un bosquejo de algunas aplicaciones de estos campos, las cuales son muchas y de diversa índole, haciendo énfasis en el uso de estructuras asociadas a los campos de Galois. Sin mayor detalle se mencionarán algunas otras áreas donde estos campos son también importantes.

3.1. Códigos lineales detectores-correctores de errores

Los *códigos* han sido usados a lo largo de la historia del Hombre, pero en las últimas décadas su uso se ha extendido a diversas áreas y actividades cotidianas. Por ejemplo; muchos de los productos que se adquieren en el mercado tienen el llamado código de barras, cuando se viaja (por autobús, avión, etc.) se asigna un código al boleto del pasajero, actualmente todos los libros tienen asignado un código conocido como el ISBN, en varios servicios de correspondencia también se asignan códigos a los artículos que se desea enviar, la contraseña que se usa en una cuenta de correo electrónico, el número de cuenta en un banco, la contraseña asignada ("pin") y el número de tarjeta de crédito son algunos ejemplos de códigos que se encuentran en varios y diversos contextos.

De particular importancia son los códigos que se usan en el manejo de la información digital, particularmente los llamados *códigos detectores-correctores de errores*. Como su nombre lo indica, estos códigos se usan para detectar y corregir errores que se adquieren en la transmisión de la información (digital), no importando el medio que se use para tal propósito. Para fijar un poco las ideas consideremos el siguiente ejemplo que estoy seguro el lector ha vivido: en algunas ocasiones cuando se hace una llamada telefónica, ya sea por el teléfono convencional (fijo) o el móvil (celular), se ha tenido la experiencia de que "hay mucho ruido" y se ha pedido a la contraparte o ella nos ha solicitado terminar la llamada y volver a comunicarnos. En general este problema se resuelve volviendo a hacer la llamada telefónica. Otro ejemplo es cuando se está escuchando la radio, y se tiene ruido en la señal y no es claro lo que se escucha; o bien en el caso de la televisión. Una situación similar, pero más complicada por sus alcances, se tiene

con los satélites, las naves espaciales, o bien, en tomografía médica. Estos son algunos ejemplos de la siguiente situación:

Se tiene una estación emisora y una estación receptora y se envía información de una a otra (por diversos medios). Es muy factible que en el "camino", por diversos motivos, dicha información adquiera errores de tal manera que la información recibida no sea la misma que la enviada originalmente. Así, la pregunta es: ¿cómo detectar y corregir los errores adquiridos en la transmisión de la información?

Se han estudiado diversos aspectos de este problema y uno de ellos es por medio de los llamados *códigos lineales detectores-correctores de errores*. Una área de la matemática muy usada en esta problemática es el Álgebra Lineal pero sobre campos de Galois, $GF(p^n)$, y de particular importancia para las aplicaciones es el caso $p = 2$, extensiones (finitas) del campo de los números binarios con 2^n elementos, por ejemplo $n = 4, 5, 6, 7$.

Un código lineal detector-corrector de errores de longitud n sobre el campo de Galois $GF(q)$, q una potencia de un primo p, se puede definir como la imagen de una función lineal entre los $GF(q)$-espacios lineales $GF(q)^m$ y $GF(q)^n$. La dimensión k del código es la dimensión de la imagen. Los parámetros de un código lineal son su longitud n, dimensión k, y su distancia mínima d (de Hamming): $[n, k, d]$. Desde el punto de vista de las aplicaciones los códigos binarios ($p = 2$) son los más usados, pero desde un punto de vista matemático, los códigos lineales se pueden estudiar sobre cualquier campo de Galois $GF(q)$. Una forma adecuada de describir estos códigos es por medio de una matriz *generadora* o bien por medio de una matriz de *chequeo de paridad* cuyas entradas están en el campo en cuestión (binario por ejemplo). Son varios los códigos lineales que se han estudiado y aplicado en diversos contextos, entre los cuales se pueden mencionar los de: Hamming, Simplex, BCH, Reed-Solomon, Reed-Muller, Goppa, etc. Cabe recordar que los códigos de Reed-Solomon se han usado en diversas aplicaciones siendo una de las más "cotidianas" en los aparatos reproductores de CD's y DVD's. Los códigos de Reed-Muller se han usado en la transmisión de imágenes de cuerpos celestes.

Otra forma como los campos de Galois se usan en los códigos lineales es la siguiente: el espacio lineal $GF(q)^n$ es isomorfo, como espacio vectorial, a $R_n = GF(q)[x]/\langle x^n - 1\rangle$, la representación polinomial de $GF(q)^n$. Un $[n, k, d]$ código lineal C se dice *cíclico* si para cada elemento (palabra de código) $c = (c_0, c_1, ..., c_{n-1})$ el vector $(c_{n-1}, c_0, ..., c_{n-2})$ es tambien un elemento de C. Por medio de la representación polinomial

se puede ver que un $[n, k, d]$ código lineal C es cíclico si y solo si su imagen bajo este isomorfismo es un ideal del anillo R_n. Como este anillo es de ideales principales, el ideal asociado a un código lineal cíclico está generado por un polinomio, conocido como el *polinomio generador* del código. El código de Reed-Solomon es cíclico y gracias a esta propiedad su implementación es muy fácil pues solo se hacen corrimientos de las coordenadas y no consumen muchos recursos computacionales. Un problema interesante en los campos de Galois es realizar aritmética rápida para ser usada en los códigos lineales, tanto en la codificación como en la decodificación, además en otras aplicaciones como en cifrado de datos, generación de sucesiones, etc. Cabe mencionar que actualmente los códigos detectores-correctores de errores no solo se estudian sobre campos de Galois, sino también sobre otras estructuras algebraicas como son los *anillos de Galois*, anillos de cadena finita, anillos de Frobenius, etc.

3.1.1. El código de Reed-Solomon

Como un ejemplo de códigos lineales a continuación se presenta el código de Reed-Solomon. La siguiente descripción de este código es básicamente la forma original propuesta por estos autores.

Sea $\mathbb{F}_q$ un campo finito con q elementos donde q es una potencia de un número primo. Sean $n = q - 1$, $\Gamma = \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ y $\alpha \in \Gamma$ un elemento primitivo, es decir, un generador del grupo mutliplicativo $\mathbb{F}_q^*$. Por consiguiente,

$$\mathbb{F}_q = \{0, 1, \alpha, ..., \alpha^{q-2}\}.$$

Sea k un entero positivo y $\mathcal{P}_k = \{f(x) \in \mathbb{F}_q[x] : \ \mathrm{gr}(f(x)) \leq k-1\} \cup \{0\}$. Es fácil ver que $\mathcal{P}_k$ es un espacio vectorial sobre $\mathbb{F}_q$ de dimensión k y una base natural es $\{1, x, ..., x^{k-1}\}$.

Considérese la siguiente función *evaluación*:

$$ev_\Gamma : \mathcal{P}_k \longrightarrow \mathbb{F}_q^n, \ ev_\Gamma(f(x)) = \left(f(1), f(\alpha), ..., f(\alpha^{n-1})\right).$$

Es fácil ver que esta función es $\mathbb{F}_q$-lineal e inyectiva, por consiguiente su imagen es un subespacio lineal de $\mathbb{F}_q^n$ el cual es el código de Reed-Solomon sobre $\mathbb{F}_q$ y se denota por $RS(q, k)$. Este código es de longitud n y dimensión k (la función ev_Γ es inyectiva). Mas aún, su distancia mínima es $d = n - k + 1$ (ejercicio al lector), es decir, $RS(q, k)$ es un $[n, k, n - k + 1]$ código lineal sobre $\mathbb{F}_q$. El código de Reed-Solomon

tiene varias propiedades interesantes, entre otras es un *MDS*-código (*Maximum Distance Separable*) y es *cíclico*.

Dado que $\{1, x, ..., x^{k-1}\}$ es una base (natural) de $\mathcal{R}_k$, si $ev_\Gamma(x^i) = \mathbf{r}_i = (1, \alpha^i, ..., \alpha^{(q-2)i})$ para $i = 0, 1, ..., k-1$, una *matriz generadora* de este código es aquella cuyos renglones son $\mathbf{r}_0, \mathbf{r}_1, ..., \mathbf{r}_{k-1}$.

En algunos casos es importante considerar el *código extendido* de Reed-Solomon:

$$\widehat{RS}(q,k) = \{\big(f(1), f(\alpha), ..., f(\alpha^{n-1}), f(0)\big) \ : \ f \in \mathcal{R}_k\},$$

el cual tiene parámetros $[n+1, k, d+1]$ y es también un *MDS*-código sobre $\mathbb{F}_q$.

3.2. Cifrado de datos

En criptografía, también conocida como cifrado de datos, los campos de Galois juegan un papel muy importante. Actualmente la criptografía tiene una gran aplicación en diversas problemáticas que incluyen el comercio y banca electrónica, firma y factura digital, tarjetas inteligentes, votación electrónica, entre otros. En las siguientes líneas se mencionarán algunos sistemas de cifrado dando énfasis a los campos de Galois. El lector interesado en adentrarse en esta área puede consultar por ejemplo: [**20**],[**26**],[**33**],[**37**].

Actualmente los sistemas de cifrado de datos se dividen en tres grupos: de llave privada, de llave pública, y de flujo o cascada. Los primeros tienen la característica que la llave que se usa para cifrar es la misma que se usa para descifrar; por esta razón se les llama *simétricos*. Los cifrados de llave pública tienen la característica que la llave K se compone de dos partes, una de las cuales se hace pública, C, y la otra, D, la conserva la entidad poseedora de la llave. Una propiedad que tienen las partes C y D es que no se puede obtener una de la otra, en particular, $C \neq D$. Por este motivo a dichos sistemas se las llama *asimétricos*. Estos dos tipos de cifrado caen en la clase de cifrados de bloques. Los cifrados de flujo tienen la característica de que la llave se va mezclando con el texto a cifrar, y no se separan en bloques como en los otros dos sistemas.

Entre los sistemas de cifrado de llave privada más representativos actualmente se encuentran el Data Encryption Standard (DES), Advanced Encryption Standar (AES), SAFER, y Twofish. En las siguientes líneas se mencionarán algunas estructuras algebraicas relacionadas con los campos de Galois sobre las cuales se basan estos sistemas. El lector

interesado en la construcción explícita y detallada, así como el funcionamiento de estos sistemas puede consultar, por ejemplo, las referencias antes mencionadas.

El sistema de cifrado DES

Este sistema maneja bloques para cifrar y llaves de $2^6 = 64$ bits, es decir, elementos del espacio vectorial $GF(2)^6$. Una forma alternativa de ver esos bloques es usando el anillo $GF(2)[x,y]/\langle x^8-1, y^8-1\rangle$. En la construcción de este sistema intervienen varias permutaciones las cuales se pueden ver como permutaciones en el campo de Galois $GF(2)[z]/\langle f(z)\rangle$ donde $f(z) = z^8+z^4+z^3+z^2+1 \in GF(2)[z]$ es irreducible. Otras estructuras algebraicas usadas en el sistema DES, basadas en el campo de Galois $GF(2)$, incluyen las siguientes:

$$GF(2)[x,y]/\langle x^7-1, y^4-1\rangle,$$
$$GF(2)[u]/\langle u^4+u+1\rangle,$$
$$GF(2)[v]/\langle v^7+v+1\rangle.$$

Una de las partes medulares de los sistemas de cifrado simétricos son las llamadas *cajas de sustitución* (S-boxes). Estas cajas son básicamente funciones sobre espacios lineales de dimensión finita sobre campos de Galois.

Por ejemplo, en el sistema DES, una caja de sustitución es una función

$$S : GF(2)^2 \times GF(2)^4 \longrightarrow GF(2)^4,$$

donde $GF(2)$ es el campo de los números binarios y $GF(2)^n$ es el $GF(2)$-espacio vectorial de dimensión n. Para conocer los detalles de la definición explícita de estas funciones sugerimos al lector consultar por ejemplo [**26**],[**33**] o [**37**].

El sistema de cifrado AES

Son varias las estructuras algebraicas usadas en el diseño del sistema de cifrado AES, en las cuales los campos de Galois juegan un papel muy importante. A continuación se mencionarán algunas de ellas. Para mayor detalle el lector puede consultar por ejemplo [**6**] o las referencias antes mencionadas.

La principal y básica estructura algebraica usada en el sistema AES es el campo binario de Galois $GF(2)$ (llamados *bits*). Este sistema maneja los *bytes* (un byte son ocho bits) y por lo tanto estos se pueden representar como elementos del $GF(2)$-espacio vectorial $GF(2)^8$.

Si $GF(2)[x]$ es el anillo de polinomios en una indeterminada con coeficientes en $GF(2)$ y $\langle x^8 - 1\rangle$ es el ideal de este anillo generado por el polinomio $x^8 - 1$, el anillo cociente $R_8 = GF(2)[x]/\langle x^8 - 1\rangle$ es también un $GF(2)$ espacio vectorial de dimensión 8. Existe un isomorfismo (natural) de $GF(2)$-espacios vectoriales entre $GF(2)^8$ y R_8, llamado la representación polinomial del primero. Por consiguiente, a los bytes se les puede representar como polinomios en una indeterminada de grado a los más 7 con coeficientes binarios (con la aritmética dada por la relación $x^8 = 1$). Como el lector debe saber, este anillo tiene, entre otras, la propiedad de ser de ideales principales. Esta propiedad es muy importante en el estudio de códigos cíclicos, como ya se comentó anteriormente.

Existe otra forma de representar a los bytes usando campos de Galois y que es muy importante en el cifrado AES ya que sobre ésta se define la caja de sustitución. Esta estructura algebraica es la del campo finito

$$GF(2^8) = GF(2)[x]/\langle f(x)\rangle,$$

donde $f(x) = x^8 + x^4 + x^3 + x + 1 \in GF(2)[x]$ es irreducible.

Como $GF(2^8)$ es un $GF(2)$-espacio vectorial de dimensión 8, existe un isomorfismo (natural) entre $GF(2)^8$ y este campo. Así, los bytes se pueden representar como polinomios en una indeterminada con coeficientes binarios de grado a lo más 7, excepto que ahora su aritmética esta regida por la relación $x^8 = x^4 + x^3 + x + 1$.

Otra propiedad importante de este campo de Galois que se usa en el sistema AES es que el grupo $GF(2^8)^* = GF(2^8) \setminus \{0\}$ es cíclico de orden $2^8 - 1 = 255$. Por consiguiente un byte distinto de cero se puede identificar con un polinomio de grado a lo mas 7 o bien con una potencia de un generador de este grupo cíclico.

El modo de operación del sistema AES es por medio de *estados*. Un estado se representa como un arreglo rectangular $4 \times N$ donde cada entrada es un byte y N depende de la longitud del bloque a cifrar, por ejemplo si $N = 4$ se tiene un arreglo de 16 bytes. Así, un *estado* se puede representar como un elemento del espacio vectorial $[GF(2)^8]^{4N}$. Una forma algebraica de representar un estado es por medio de la identificación del espacio vectorial $[GF(2)^8]^{4N}$ con el anillo de polinomios $GF(2^8)[x, y/\langle x^4 - 1, y^N - 1\rangle]$. Por ejemplo, si $N = 4$ los estados, es decir, el espacio vectorial $[GF(2^8)]^{16}$, se identifican con el anillo $GF(2^8)[x, y]/\langle x^4 - 1, y^4 - 1\rangle$.

El campo de Galois $GF(2^8)$ también se usa para definir la caja de sustitución del sistema AES de la siguiente manera: como $GF(2^8)$ es un campo, todo elemento distinto de cero tiene inverso (multiplicativo) y se tiene naturalmente la siguiente función:

$$\phi : GF(2^8) \longrightarrow GF(2^8), \;\; \phi(\gamma) = \gamma^{-1}, \; \phi(0) = 0.$$

la cual es una permutación. Dado que el grupo multiplicativo de este campo tiene orden 255, esta permutación se puede expresar como $\phi(x) = x^{254}$, es decir, ϕ es un polinomio de permutación.

Otras funciones que se usan en la definición de la caja de sustitución del AES son las siguientes:

$$L, \psi : GF(2^8) \longrightarrow GF(2^8), \;\; L(\alpha) = c_0\alpha, \; \psi(\beta) = d_0 + \beta,$$

donde c_0 y d_0 son elementos fijos del campo $GF(2^8)$, (para la definición de estas constantes sugerimos al lector consultar por ejemplo, [**6**]). La caja de sustitución es la función:

$$S : GF(2^8) \longrightarrow GF(2^8), \; S = \psi \circ L \circ \phi.$$

El sistema de cifrado Twofish

Este es otro sistema de cifrado de llave privada donde los campos de Galois se ponen de manifiesto. Este sistema maneja bloques de texto y llaves formados por bytes, es decir, elementos del espacio vectorial $GF(2)^8$, los cuales se concatenan para formar palabras, vistas como elementos de $GF(2)^{32}$. Las cajas de sustitución de este sistema se pueden ver como funciones $S : GF(2)^8 \longrightarrow GF(2)^8$. Otra componente de Twofish es una matriz de tipo MDS (Maximum Distance Separable) cuyas entradas son bytes. Para realizar operaciones es necesario identificar a los bytes con elementos de un campo. Este campo es $GF(2^8) = GF(2)[x]/\langle v(x)\rangle$, donde $v(x) = x^8 + x^6 + x^5 + x^3 + 1 \in GF(2)[x]$ es irreducible sobre $GF(2)$. Este sistema además usa una matriz de tipo Reed-Solomon cuyas entradas son también bytes. Para efectuar las operaciones se identifica el espacio $GF(2)^8$ con el campo de Galois con 2^8 elementos, pero ahora descrito de la siguiente manera: $GF(2^8) = GF(2)[x]/\langle w(x)\rangle$ donde $w(x) = x^8 + x^6 + x^3 + x^2 + 1$. Dado que el campo de Galois con 2^8 elementos es único módulo isomorfismos, estos dos campos son isomorfos. Para más detalles sobre este sistema el lector puede consultar por ejemplo [**11**].

El sistema de cifrado SAFER

En sistema de cifrado SAFER (**S**ecure **A**nd **F**ast **E**ncryption **R**outine) también usa fuertemente los campos de Galois, particularmente el campo $GF(257)$. El elemento $45 \in GF(257)$ es un generador del grupo cíclico $GF(257)^*$ y este grupo se puede identificar con $\mathbb{Z}_{256}$, con lo cual se define la permutación

$$exp : \mathbb{Z}_{256} \longrightarrow \mathbb{Z}_{256},\ exp(x) = 45^x.$$

que juega un papel importante en este sistema de cifrado. La permutación inversa de *exp* se denota por *log*. Para mayores detalles de cómo se usan estas funciones en el diseño del sistema SAFER el lector puede consultar, por ejemplo, [**24**].

El sistema de cifrado basado en curvas elípticas

Actualmente el RSA y el basado en curvas elípticas son los sistemas de cifrado de datos más representativos de clase de cifrados de llave pública. El sistema RSA (por las iniciales de sus creadores: **R**ivest-**S**hamir-**A**dleman) está basado en la estructura del anillo de enteros modulares donde el módulo es un entero grande (del orden de ciento cincuenta dígitos) el cual es el producto de dos números primos, donde se usan varios resultados de Teoría de Números como el Teorema (pequeño) de Fermat y de Euler, entre otros.

Las curvas elípticas definidas sobre un campo algebraicamente cerrado han sido objeto de estudio desde hace mucho tiempo por diversos motivos. Recientemente N. Koblitz y V. Miller, en forma independiente, presentaron un sistema de cifrado de llave pública basado en el grupo de puntos (racionales) de una curva elíptica definida sobre un campo de Galois, el cual, para aplicaciones, se toma el campo de la forma $GF(2^n)$ para diversos valores de n, por ejemplo $n = 160$.

En este sistema de cifrado los campos de Galois se manifiestan de varias maneras. Para definir una curva elíptica se necesita un campo, el cual para propósitos de cifrado debe ser de Galois, $GF(q)$, con $q = p^n$ elementos, p un número primo y $n > 0$ un entero.

La relación que define una curva elíptica en general es un polinomio cúbico en dos indeterminadas con coeficientes en un campo, el cual bajo ciertas condiciones se lleva a la forma normal de Weierstrass. Si el campo sobre el cual se está trabajando es de Galois, $GF(q)$, el polinomio que define a la curva elíptica se puede reducir a una relación de la siguiente forma (dependiendo de la característica del campo):

$$f(x, y) = y^3 - ax^3 - bx - c \in GF(q)[x, y],$$

y la curva elíptica, E, sobre $GF(q)$ se define como:

$$E = \{P = (x, y) \in GF(q) \times GF(q) : f(x, y) = 0\}.$$

En el conjunto E (o mejor dicho, de los $GF(q)$-puntos racionales de E) se puede definir una operación que le da una estructura de grupo abeliano a este conjunto. Si $P, Q \in E$ cuyas coordenadas son elementos de $GF(q)$, las coordenadas de $P+Q$ son en general funciones racionales en las coordenadas de P y Q, las cuales a su vez son elementos del campo de Galois $GF(q)$. En este contexto una de las cuestiones importantes de los campos de Galois es realizar aritmética *rápida* para obtener las coordenadas explícitas del elemento $P + Q$, en particular nP, donde $n > 0$ es un entero. En un campo de Galois uno de los principales problemas es determinar el inverso de un elemento (distinto de cero). En los últimos años se han llevado a cabo investigaciones para realizar aritmética rápida sobre campos de Galois y que no ocupe muchos recursos computacionales, con aplicaciones a cifrados de datos, códigos detectores-correctores de errores, generación de sucesiones, etc. Para mayores detalles sobre este sistema de cifrado el lector puede consultar por ejemplo [**20**],[**15**] o [**26**].

Recientemente la llamada criptografía *basada en identidad* ha llamado la atención de varios grupos de trabajo, donde las formas bilineales de J. Tate y A. Weil, así como los campos de Galois juegan un papel importante.

3.3. Geometría algebraica sobre campos de Galois

Otra de las áreas donde los campos de Galois son de gran utilidad es en la geometría algebraica, particularmente las curvas algebraicas. A fines de la década de los 80, V.D. Goppa ([**41**]), introdujo los códigos lineales geométrico-algebraicos tambien conocidos como códigos de Goppa, sobre una curva algebraica definida sobre un campo de Galois. Dada una curva algebraica no-singular, irreducible de género $g \geq 0$ definida sobre un campo de Galois $GF(q)$, con divisores D y G con soporte ajeno, si $L(G)$ es el $GF(q)$-espacio vectorial de funciones racionales asociado a G, la función evaluación

$$ev_D : L(G) \longrightarrow GF(q)^n,\ ev_D(f) = (f(P_1), ..., f(P_n)),$$

(donde $sop(D) = \{P_1, ..., P_n\}$), determina un código lineal sobre el campo $GF(q)$.

El teorema de Riemann-Roch (y consecuencias) son una herramienta muy útil en el estudio de estos códigos particularmente para determinar su dimensión y cotas sobre la distancia mínima. Las diferenciales sobre la curva también son de gran utilidad en el estudio del código dual de un código de Goppa. La geometría propia de la curva en cuestión así como los divisores que se usen, proporcionan información más detallada sobre los códigos asociados. Una forma alternativa del estudio de estos códigos es a través de los campos de funciones. El lector interesado en esta área puede consultar por ejemplo [**27**],[**35**],[**42**].

Como ejemplo de códigos geométrico-algebraicos se tiene el código extendido de Reed-Solomon introducido en la Sección 3.1.1. En este caso la curva se toma como la recta proyectiva sobre el campo finito $\mathbb{F}_q$ (el género es $g = 0$), los divisores son $G = P_\infty$ y D que es la suma de los otros puntos de la recta proyectiva. Se puede ver que el $\mathbb{F}_q$-espacio vectorial $L(G)$ es isomorfo a $\mathcal{R}_k$ y una matriz generadora de este código de Goppa es básicamente la descrita anteriormente para el código de Reed-Solomon. Para mayores detalles y otros ejemplos el lector interesado puede consultar [**30**],[**35**].

Otro problema interesante relacionado con geometría algebraica sobre campos de Galois es determinar el número de puntos (racionales) de una variedad algebraica definida sobre uno de estos campos. Un caso particular e interesante es el de las curvas algebraicas, en especial las elípticas, hecho que se usa en los códigos de Goppa y cifrado de datos, respectivamente.

No sólo las curvas algebraicas sobre campos de Galois han sido estudiadas por varios grupos de investigación sino que también variedades algebraicas de dimensión mayor sobre campos de Galois son objeto de estudio, particularmente en conexión con áreas como teoría de códigos y criptografía (códigos definidos sobre la variedad de Veronese o intersección completa; cifrado sobre jacobianos, por ejemplo de curvas hiperelípticas).

3.4. Sucesiones

El estudio de *sucesiones* ha sido muy importante en varias áreas de Matemáticas y estas se manifiestan de diversas maneras en diferentes contextos en la naturaleza y actividad humana, de las cuales la sucesión de Fibonacci es un representante. Debido al desarrollo de las comunicaciones digitales, las sucesiones sobre estructuras algebraicas finitas, particularmente campos de Galois es un tema de gran relevancia actualmente. Una pregunta interesante en este tema es la generación

de sucesiones con propiedades particulares que permitan su aplicación en diversos contextos. Algunas de estas propiedades incluyen pseudo-aleatoriedad, correlación, generación rápida y eficiente, entre otras. De particular importancia son las sucesiones binarias (por sus aplicaciones) que se obtienen por medio de recurrencias lineales, como es el caso de la sucesión de Fibonacci, y una forma de generarlas es por medio de los llamados *Registros de Cambio de Retro-alimentación Lineal* (Linear Feed-back Shift Register, LFSR), los cuales se pueden implementar en hardware para una mayor rapidez en la generación de la sucesión y su aplicación en tiempo real. En el caso de sucesiones binarias generadas por recurrencias lineales, estas se pueden obtener por medio de la función traza definida sobre una extensión finita de los números binarios, es decir, sobre un campo de Galois. De particular importancia son las sucesiones de máxima longitud, las llamadas *m-sucesiones*. Aunque las sucesiones binarias son las más estudiadas por sus aplicaciones, desde el punto de vista matemático se pueden usar campos de Galois mas generales y otras estructuras algebraicas que incluyen los anillos de enteros modulares, $\mathbb{Z}_m$, o bien los anillos de Galois. Cabe mencionar que el estudio de sucesiones, particularmente sobre estructuras discretas, es de tal importancia que hay congresos internacionales dedicados a este tema, una de ellas es la SETA (**Se**quences and **T**heir **A**pplications). El lector interesado en este tema puede consultar por ejemplo [**22**] o [**25**] para un primer acercamiento.

Las sucesiones, en particular las m-sucesiones, tienen aplicación en una gran variedad de contextos. A continuación se mencionan algunos de ellos.

1. Los sistemas de posicionamiento global (Global Positioning Systems, GPS) usan un LFSR para transmitir rápidamente una sucesión que indica la posición de un objeto.

2. Los LFSR se usan para generar números pseudoaleatorios para su uso, por ejemplo, en cifrados de cascada como es el A5/1 y A5/2, empleados en teléfonos celulares con GMS, y el E0 usado en Bluetooth. Sin embargo, debido a que la sucesión es generada a base de recurrencias lineales son suceptibles del criptoanálisis, pero se modifican para que sean más robustas y se puedan usar en otros contextos.

3. Las sucesiones obtenidas por LSFR también se usan en transmisiones y comunicaciones digitales, por ejemplo para tener una

modulación y demodulación robusta y eficiente. Entre las empresas transmisoras que usan LFSR se cuentan, entre otras, las siguientes: ATSC Standards (digital TV transmission system North America), DAB (Digital Audio Broadcasting system for radio), DVB-T (digital TV transmission system Europe, Australia, parts of Asia), NICAM (digital audio system for television). Entre las empresas de comunicación digital que usan LFSR se pueden mencionar: IBS (INTELSAT business service), IDR (Intermediate Data Rate service), SDI (Serial Digital Interface transmission), Data transfer over PSTN (according to the ITU-T V-series recommendations), CDMA (Code Division Multiple Access) cellular telephony, 100BASE-T2 "fast" Ethernet (scrambles bits using an LFSR), 1000BASE-T Ethernet, the most common form of Gigabit Ethernet, (scrambles bits using an LFSR), PCI Express 3.0, SATA, USB 3.0, IEEE 802.11a (scrambles bits using an LFSR).

4. Otras aplicaciones

A continuación se mencionarán algunos otros ejemplos, sin entrar en detalle, donde los campos de Galois juegan un papel importante.

1. **Funciones especiales.** El estudio de funciones sobre campos finitos ha conducido a determinar aquellas con propiedades adecuadas para su uso en criptografía, teoría de códigos, compartición de secretos, esquemas de autenticación, etc., de entre las cuales se cuentan las funciones booleanas, bent, casi-bent, perfectamente no-lineales, entre otras.

2. **Esquemas de compartición de secretos.** La idea de estos esquemas es que se pueda compartir un secreto entre un número n de entidades (personas) asignando a cada una de ellas cierta información de tal manera que reuniendo cualesquiera $k \leq n$ de esas porciones de información se pueda recuperar el secreto, pero que con un número menor que k de personas no se pueda recuperar dicho secreto. Uno de los primeros sistemas de esta naturaleza fue introducido por A. Shamir usando interpolación de Lagrange, el cual se puede realizar sobre cualquier campo, en particular sobre campos de Galois. En la literatura se encuentran otros esquemas de compartición de secretos basados en conceptos como funciones booleanas con ciertas propiedades donde los campos de Galois se hacen presentes.

3. **Esquemas de autenticación.** En la actualidad es muy importante que al establecer una conexión para la transmisión de información, las partes involucradas se autentiquen. Para tal fin se han introducido los esquemas de autenticación. Conceptos como campos de Galois, funciones bent, perfectamente no-lineales, etc. son usados para la descripción de este tipo de esquemas, pero también otras estructuras algebraicas como los *anillos de Galois* han sido usados para tal propósito.

4. **Polinomios de permutación.** Otro tema interesante en relación con los campos de Galois son las permutaciones sobre estos campos, particularmente aquellas inducidas por polinomios. Este tipo de permutaciones tiene aplicación en diversas áreas incluyendo criptografía como es el caso de sistemas de cifrado DES y AES. Una componente importante en los turbo códigos son los intercambiadores (interleavers) que bajo ciertas condiciones se pueden determinar como polinomios de permutación.

5. **Sumas exponenciales.** Las sumas exponenciales sobre campos y anillos de Galois es otro de los temas que han llamado la atención de varios grupos de investigación por la gran variedad de aplicaciones en teoría de códigos (cotas sobre la distancia mínima), estudio de funciones booleanas (funciones bent), etc.

5. Otras áreas

Además de las áreas mencionadas donde los campos de Galois tienen una gran aplicación, existen otros temas y áreas de estudio en los cuales la influencia de las ideas de E. Galois ha prevalecido. Entre estas se cuentan, por supuesto, la Teoría de Galois, Cohomología de Galois, conjuntos (invariantes) de Galois, geometrías de Galois, algunas áreas de combinatoria, sistemas dinámicos sobre campos de Galois, matrices y grupos clásicos sobre campos de Galois, información cuántica y su relación con campos de Galois, inclusive biología y bioinformática, solo por nombrar algunas.

Mención especial debe darse a la demostración del *Último Teorema de Fermat* dada por A. Wiles, donde la teoría de Representaciones de Galois y su conexión con curvas elípticas y formas modulares juega un papel importante.

6. Comentarios finales

En las últimas décadas, sobre todo con el desarrollo de las comunicaciones e información digital, los campos de Galois han tenido, y se espera sigan teniendo, un papel relevante en su desarrollo y aplicación a problemas en diversas áreas del quehacer humano. Cabe señalar que desde hace varias décadas se tienen eventos académicos y congresos dedicados al estudio de los campos de Galois y aplicaciones, como es The International Conference on Finite Felds and Applications, además se tienen varias revistas especializadas donde se publica sobre diversos aspectos y aplicaciones de los campos de Galois. Entre estas revistas se pueden mencionar por ejemplo: Finite Fields and Their Applications; Designs, Codes and Cryptography; IEEE Transactions on Information Theory; Applicable Algebra in Engineering, Communication and Computing (AAECC); Journal of Combinatorial Theory, Discrete Mathematics; Pure and Applied Algebra; Advances in Mathematics of Communications (AMC), entre otras.

No cabe la menor duda que a 200 años, la influencia de las ideas de E. Galois ha prevalecido y han sido pilar para la obtención de nuevos resultados y para la solución de problemas en diversas áreas del conocimiento. ¡ A sus 200 años Evaristo Galois sigue vigente !

Agradezco las observaciones y sugerencias de los árbitros, las cuales mejoraron la presentación de este manuscrito.

Bibliografía

1. E. Assmus y J. Key, *Designs and their codes*, Cambridge Univ. Press, 1993.
2. E. Berlekamp, *Algebraic coding theory*, McGraw-Hill Co., 1968.
3. R. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley, Publ., 1984.
4. I. Blake y R. Mullin, *An Introduction to algebraic and Combinatorial Coding Theory*, Academic Press, 1976.
5. P. Cameron y J. van Lint, Graph theory, coding theory and block designs, London Math. Soc., Lecture Notes Series, tomo 19, Cambridge Univ. Press, 1975.
6. J. Daemen y V. Rijmen, *The Design of Rinjdael*, Springer-Verlag, 2001.
7. C. Dávalos, S. Díaz, J. Torres, H. Tapia-Recillas, y R. Basurto, Elementos de criptografía clásica, Matemática Aplicada y su Enseñanza, SMM, 2005.
8. A. M. et al., *Applications of Finite Fields*, Kluwer Academic Publ., 1993.

9. D. H. et al., Coding theory and cryptography, the essentials, Pure and Applied Mathematics, Marcel Dekker, 2000.
10. H. T.-R. et al., Sistemas de cifrado, Notas del III Coloquio del Departamento de Matemáticas, UAM-I, 2010.
11. B. S. et al. Twofish, *a 128-bit block cipher*, http://www.nist.gov/aes.
12. E. Galois, *Memoire sur les conditions des resolubilité de equations par radicaux*, 1830.
13. ———, *Sur la théorie des nombres*, 1830.
14. V. Goppa, *Geometry and Codes*, Kluwer Academic Publ., 1988.
15. D. Hankerson, A. Menezes, y S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, 2004.
16. D. Hardy, F. Richman, y C. Walker, *Applied Algebra: Codes, Ciphers and Discrete Algorithms*, 2nd ed., CRC Press, 2009.
17. J. Hirschfeld, *Projective geometries over Finite Fields*, Clarendon Press, Oxford, 1979.
18. W. Huffman y V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge Univ. Press, 2003.
19. N. Koblitz, *A Course in Number Theory and Cryptography, 2nd ed.*, GTM, 1994.
20. ———, Algebraic aspects of cryptography, Algortithms and Computation in Mathematics, tomo 3, Springer-Verlag, 1998.
21. N. Lauritzen, *Concrete Abstract Algebra*, Cambridge Univ. Press, 2005.
22. R. Lidl y H. Niederreiter, Finite fields, Encyclopedia of Mathematics and its Applications, Cambridge Univ. Press., 2000.
23. F. MacWilliams y N. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publ., 1978.
24. J. Massey, Safer k-64: A byte-oriented block -ciphering algorithm, LNCS, tomo 809, Springer, 1994, 1–17.
25. McEllice, *Finite field for Computer Scientist and Engineers*, Kluwer Academic Publ., 1987.
26. A. Menezes, S. Vanstone, y P. van Oorschot, *Handbook of Applied Cryptography*, CRC Press, 1997.
27. C. Moreno, Algebraic curves over finite fields, Cambridge Tracts in Mathematics, Cambridge Univ. Press, 1991.
28. W. Peterson, *Error-correcting codes*, The M.I.T. Press, 1968.
29. V. Pless, *Introduction to the Theory of Error-Correcting Codes*, John Wiley & Sons, 1982.
30. V. Pless y W. H. (editors), *Handbook of Coding Theory*, tomo I, II, Elsevier, 1998.
31. C. Rentería, H. Tapia-Recillas, y W. Velez, Breve introducción a códigos detectores-correctores de error, Aportaciones Matemáticas, tomo 7, SMM, 1990.
32. S. Roman, *Coding and Information Theory*, GTM, Springer-Verlag,

1992.
33. B. Schneier, *Applied cryptography*, John Wiley & Sons Inc., 1998.
34. I. E. Shparlinski, *Computational and Algorithmic Problems in Finite Fields*, Kluwer Academic Publ., 1992.
35. W. Stallings, *Cryptography and Network Security: Principles and Practices*, 3rd ed., Prentice Hall.
36. H. Stichtenoth, *Algebraic Functions Fields and Codes*, Universitext, Springer-Verlag, 1993.
37. D. Stinson, *Cryptography: Theory and Practice*, CRC Press, 1995.
38. H. Tapia-Recillas, Campos finitos y aplicaciones a teoría de códigos, Notas del I Coloquio del Departamento de Matemáticas, UAM-I, 2008.
39. _____, Curvas algebraicas y teoría de códigos, Notas del IV Coloquio del Departamento de Matemáticas, UAM-I, 2011.
40. J. van Lint y G. van der Geer, *Introduction to Coding Theory and Algebraic Geometry*, DMV Seminar Band 12, Birkhäuser, 1988.
41. J. von zur Gathen y J. Gerhard, *Modern Computer Algebra*, Cambridge Univ. Press, 1999.
42. J. Walker, *Codes and Curves*, Student Math. Library, AMS, 2000.