

Polinomios de permutación Algunos problemas de interés

VÍCTOR S. ALBIS
Universidad Nacional de Colombia
Bogotá, Colombia

RESUMEN. Se realiza una corta revisión de los polinomios de permutación de coeficientes en cuerpos y anillos finitos y se plantea la posibilidad de estudiar las diversas generalizaciones de polinomios de permutación a cierto tipo de álgebras finitas.

Key words and phrases. Finite fields and algebras, permutation polynomials

1991 Mathematics Subject Classification. Primary 11T06. Secondary 11T55, 11T71.

ABSTRACT. A short revision of results on permutation polynomials over finite fields and rings is presented. Also the possibility of extending these results to some type of finite algebras is explored.

Introducción

En el marco de una investigación que realizamos con un grupo de estudiantes nos hemos propuesto el estudio de los polinomios de permutación (*vide infra*) en ciertos tipos de álgebras finitas, que nacen del estudio de la aritmética de polinomios de coeficientes en un cuerpo finito o campo de Galois. El interés actual en los polinomios de permutación

en estructuras algebraicas finitas estriba en su eventual aplicación en la teoría algebraica de códigos y la criptografía. En particular, la teoría de los polinomios de permutación sobre cuerpos finitos interactúa con áreas como la geometría finita (que algunos llaman geometría de Galois), la teoría de los grupos (incluyendo los grupos de Mathieu y los grupos de Lie) y la teoría de grafos. Sobre estos temas existen importantes y extensas exposiciones en los libros [5], [16], [17], [28], [30] (por supuesto hay muchos más). Además, desde 1995 existe la revista especializada *Finite fields and Applications*, hecho que evidencia el interés actual de la comunidad matemática en los cuerpos finitos, sus propiedades y aplicaciones.

En este trabajo, en gran parte expositivo, sólo mencionaremos tangencialmente las aplicaciones de los polinomios de permutación a la criptografía y la teoría de códigos, tocando solamente los aspectos puramente teóricos de estos polinomios dentro de un contexto histórico-bibliográfico. Como siempre nos han atraído las conexiones entre la literatura, el arte y otras manifestaciones culturales con la matemática, en la primera sección presentamos un ejemplo fascinante del papel protagónico de un criptograma en un cuento de EDGAR ALLAN POE, *El escarabajo dorado*.

En la segunda sección enunciamos algunos resultados clásicos de la teoría de los polinomios de permutación, la mayoría de ellos descubiertos y demostrados por LEONARD EUGENE DICKSON en su magnífico y aún influyente libro *Linear Groups with an Exposition of the Galois Field Theory* [15].¹ También allí exponemos algunas de las conjeturas, muchas de ellas todavía sin resolver, sobre los polinomios de permutación sobre cuerpos finitos. En cierta forma pretendemos, de manera incompleta, por cierto, establecer un *status artis* de las mismas.

La sección tercera contiene la extensión de la noción de polinomio de permutación a los anillos $\mathbb{Z}/p^n\mathbb{Z}$, donde p es un número primo y n

¹El propósito inicial del libro de DICKSON era determinar cuáles de los grupos ortogonales, unitarios y simplécticos sobre un cuerpo finito eran simples. De hecho listó todas las clases de isomorfía de los grupos simples que conocía. Por ejemplo, demostró que $PSL(2, 4)$ y $PSL(2, 5)$ son isomorfos. Cuarenta años más tarde, JEAN DIEUDONNÉ demostró que la lista de DICKSON estaba completa.

un entero mayor o igual que 1, con el enunciado de algunos resultados recientes, muy pocos, que consideramos ilustrativos.

En la última sección indicamos cómo estudiar los problemas análogos de las secciones anteriores en los anillos $K[X]/(p(X)^\nu)$, donde K es cuerpo finito de característica $p \neq 0$, $p(X) \in K[X]$ es un polinomio irreducible y unitario y $\nu \geq 1$ es un entero. Establecemos algunos de los resultados más elementales, dejando para una publicación más extensa, los resultados obtenidos.

1. Una fantasía codificada

Quizás una de las más antiguas referencias en la literatura a *mensajes en clave* o *criptogramas* (y con propósitos militares) se deba al emperador romano JULIO CÉSAR.

Para muchos de nosotros la primera reminiscencia de un criptograma se remonta a la adolescencia y está relacionada con la lectura del cuento de EDGAR ALLAN POE² titulado *The gold-bug* (*El escarabajo dorado*) [53].

Según esta narración, el personaje, WILLIAM LEGRAND, descifra un mensaje escrito con tinta simpática en un pergamino o vitela que por casualidad encuentra en una playa junto con un raro espécimen entomológico que lucía como una calavera humana, con visos dorados, que explica el título del cuento (POE, el narrador, le llama, burlándose de LEGRAND, un *scarabaeus caput hominis*).

Asociando estos hechos aparentemente independientes³ y usando otras pistas, el personaje establece que probablemente el criptograma indicaba

²EDGAR ALLAN POE estudió en la Academia Militar de West Point, establecimiento en el cual el estudio de las matemáticas era de importancia obligatoria y quizás los contenidos de sus cursos de matemáticas eran de los más avanzado en la Norteamérica de ese entonces.

³En la vitela aparece como encabezamiento una calavera (símbolo de la piratería) y como rúbrica la figura de un muchacho (en inglés *kid*) que POE insiste en que es una cabra.

el lugar en donde el legendario pirata WILLIAM KIDD⁴ había enterrado un fabuloso tesoro.

En la época de POE eran bien conocidos los métodos para descifrar mensajes cifrados en los cuales se reemplazaban las letras por otros signos. Al respecto dice:

... and it may well be doubted wether human ingenuity can construct an enigma of the kind which human ingenuity may not, by proper application, resolve... –indeed in all cases of secret writing– the first question regards the language of the cipher, for the principles of solution, so far, especially, as the more simple ciphers are concerned, depend upon, and are varied by, the genius of the particular idiom. In general, there is no alternative but experiment (directed by probabilities) of every tongue known to him [the one that deciphers].

Como LEGRAND consideraba a KIDD poco educado, supuso que descifrar su mensaje era una tarea sencilla. De hecho partió de la hipótesis de que el lenguaje original del mensaje era el inglés, pensando que KIDD no dominaba ni el español ni el francés, lenguas también de uso común y extendido en Tierra Firme y el Caribe. El mensaje es el siguiente:

53 † † † 305)6*; 4826)4†) · 4†) : 806*; 48 † 8¶(60))85; 1 † (: : † * 8 † 83
 (88)5 * †; 46(: 88 * 96*?; 8) * †(; 485); 5 * †2 : * † (: ; 4956 * 2(5*
 – 4)8¶(8*; 4069285);)6 † 8)4 † †; 1(†9; 48081; 8 : 8 † 1; 48 † 85; 4)
 485 † 528806 * 81(†9; 48; (88; 4(†?34; 48; (88 : 4(†?34; 48)4†; 161; : 188; †?;

De aquí obtiene la siguiente tabla:

⁴Nacido en Inglaterra se estableció en Nueva Inglaterra. Combatió contra los franceses en las Antillas y en 1695 recibió patente de corso para combatir a los piratas que merodeaban las costas de Madagascar, a los cuales finalmente se unió. Ejerció la piratería alrededor de Madagascar. Al regresar a América fue arrestado y enviado a Londres, donde fue juzgado por piratería y ahorcado en 1701. En Nueva Inglaterra siempre existió la leyenda del enterramiento de sus grandes botines en algún lugar de sus costas.

8	aparece	33	;	aparece	26
4	aparece	19	‡)	aparecen	16
*	aparece	13	5	aparece	12
6	aparece	11	(aparece	9
† 1	aparecen	8	0	aparece	6
9 2	aparecen	5	: 3	aparecen	4
?	aparece	3	¶	aparece	2
- ·	aparecen	1			

La letra más frecuente en inglés (según POE) es la *e*, apareciendo luego en sucesión de frecuencia descendente las siguientes: *a o i d h n r s t u y c f g l m w b k q x z*. LEGRAND, por experimentación, probabilidades, combinaciones de los símbolos e ingenio, llega a determinar la siguiente tabla de equivalencias, basada en parte por el desciframiento preciso de algunas palabras asociadas con la marinería:

5	↔	a	†	↔	d
8	↔	e	3	↔	g
4	↔	h	6	↔	i
*	↔	n	‡	↔	o
(↔	r	;	↔	t
?	↔	u			

La transcripción definitiva es la siguiente (donde la puntuación la obtiene LEGRAND observando el apiñamiento de los signos en determinados puntos del manuscrito):

A good glass in the bishop's hostel in the devil's seat— forty-one degrees and thirteen minutes— northeast and by north— main branch seventh limb east side— shoot from the left eye of the death's head— a bee-line from the tree through the shot fifty feet out.

Con un poco de información histórica y geográfica adicional LEGRAND es capaz de encontrar el sitio exacto donde se oculta el tesoro y desenterrarlo (encontrando, por supuesto, encima del arcón que lo contiene algunos esqueletos).

La mayoría de las historias noveladas de búsquedas de tesoros se basan en la existencia de un *mapa*. Quizás la formación matemática de POE y las posibles tareas de desciframiento propuestas en West Point con fines

de preparación militar lo inclinaron por la opción de un criptograma. Pero bien, éstas son sólo suposiciones. Lo importante de lo anterior es que nos conduce al tema tangencial de la teoría de códigos.

El ejemplo de la historia anterior es uno de los más sencillos métodos de criptación y consiste de una función biyectiva entre los elementos de un alfabeto dado en un conjunto de símbolos (el cual también puede llamarse un alfabeto). Esta función es a la vez el código y la clave. Esquemáticamente, un código transforma un mensaje (a_1, \dots, a_s) escrito en un alfabeto dado en otro mensaje (x_1, \dots, x_n) escrito en el nuevo alfabeto (el mensaje codificado). En general, existe una *transmisión del mensaje* por algún medio a otra persona, que puede ser el mismo remitente. En este proceso de transmisión puede haber lo que se llama *ruido de fondo*, causante de posibles errores, por lo que en general en el proceso de decodificación el mensaje resultante puede ser difícil de leer. Por esta razón en el alfabeto original el mensaje decodificado puede ser algo aparentemente diferente: (a'_1, \dots, a'_s) . En nuestro ejemplo, podemos considerar que el ruido de fondo que recibe LEGRAND consiste en no saber la puntuación del mensaje original, problema que, como hemos visto, resuelve ingeniosamente basándose en un involuntario proceder de KIDD al escribirlo sobre la vitela. Hoy en día es posible crear *códigos correctores de errores*.

Una manera de pasar de un alfabeto X a otro es permutar sus elementos, con lo cual se obtiene un código. Si tomamos, por ejemplo, el cuerpo \mathbb{F}_q finito de q elementos como nuestro alfabeto original, una permutación de los elementos de este conjunto produce, pues, un código. Si q es muy grande, el número de sus permutaciones es $q!$ que es mucho más grande, lo cual dificulta la escogencia de una permutación como código. Es conveniente, pues, tomar los códigos en un subconjunto más pequeño de permutaciones de \mathbb{F}_q . Los polinomios de permutación, los cuales definiremos más adelante, generan permutaciones que parecen ser menos numerosas. Como decidir si un polinomio $f(X) \in \mathbb{F}_q[X]$ es o no de permutación es muy difícil, su estudio es pertinente para la elaboración de códigos.

Pero hay otras razones de tipo criptográfico para estudiar los cuerpos finitos. Por ejemplo, en la *teoría algebraica de códigos* un q -código lineal C es un subespacio del \mathbb{F}_q -espacio \mathbb{F}_q^n de dimensión n (véase [33]).

2. Polinomios de permutación y algunos de sus problemas

Sea $K = \mathbb{F}_q$ un cuerpo finito con $q = p^r$ elementos. Con cada polinomio $f(X) \in K[X]$ está asociada una función polinomial $f : K \rightarrow K$, definida por $\alpha \mapsto f(\alpha)$, donde $f(\alpha)$ es el resultado de sustituir X por α . Esta función se suele llamar *inducida* por $f(X)$.

Como todo elemento $\alpha \in K$ satisface la ecuación $\alpha^q = \alpha$, vemos que las funciones polinomias asociadas con los polinomios X^q y X coinciden. Es, pues, natural *identificar* polinomios que producen la misma función polinomial mediante la siguiente relación de equivalencia: $f(X) \sim g(X)$, $f(X), g(X) \in K[X]$, si $f(\alpha) = g(\alpha)$, para todo $\alpha \in K$.

Un polinomio $f(X) \in K[X]$ se dice *reducido* si su grado es menor o igual a $q - 1$. Un resultado importante es el siguiente: *En cada clase de equivalencia módulo \sim existe un único polinomio reducido* (véase, por ejemplo, [1]).

Esto nos permite remitirnos siempre en la mayoría de nuestras discusiones sobre funciones polinomias a los polinomios reducidos.

Por otra parte, dada una función arbitraria $h : K \rightarrow K$ existe un polinomio $f(X) \in K[X]$ tal que $h(\alpha) = f(\alpha)$ para todo $\alpha \in K$. Es decir, *toda función de K en K puede reemplazarse por una función polinomial* (reducida si se considera conveniente [1]).

Ahora bien, las biyecciones de K en K conforman su *grupo simétrico* $\mathfrak{S}(K)$. Un polinomio $f(X)$ cuya función polinomial inducida sea un elemento de $\mathfrak{S}(K)$ se dice un *polinomio de permutación*.

Con \mathcal{P} designamos al conjunto de todos los polinomios de permutación reducidos.

Un problema inmediato es el siguiente: dado un elemento $\sigma \in \mathfrak{S}(K)$ hallar el único polinomio reducido $f(X)$ tal que $f(\alpha) = \sigma(\alpha)$ para todo $\alpha \in K$. Su solución teórica se encuentra en la siguiente proposición.

Proposición 2.1. Sea $K = \{\alpha_0, \alpha_1, \dots, \alpha_{q-1}\}$. Entonces existe una biyección entre \mathcal{P} y $\mathfrak{S}(K)$.

Demostración. Definiendo $\bar{\sigma} : f(X) \mapsto \bar{\sigma}(f) = \sigma_f$, donde $\sigma_f(\alpha) = f(\alpha)$, para todo $\alpha \in K$, obtenemos una aplicación de \mathcal{P} en $\mathfrak{S}(K)$. Recíprocamente, definiendo $\bar{f} : \sigma \mapsto \bar{f}(\sigma) = f_\sigma(X)$, donde

$$f_\sigma(X) := \sum_{i=0}^{q-1} \sigma(\alpha_i) \frac{(X - \alpha_0) \cdots \widehat{(X - \alpha_i)} \cdots (X - \alpha_{q-1})}{(\alpha_i - \alpha_0) \cdots \widehat{(\alpha_i - \alpha_i)} \cdots (\alpha_i - \alpha_{q-1})},$$

vemos que este polinomio es un polinomio reducido de grado inferior a $q - 1$ y tal que $f_\sigma(\alpha) = \sigma(\alpha)$, para todo $\alpha \in K$. Es fácil ver ahora que $\bar{f} \circ \bar{\sigma} = \text{id}_{\mathcal{P}}$ y $\bar{\sigma} \circ \bar{f} = \text{id}_{\mathfrak{S}(K)}$. \checkmark

Este criterio teórico no resulta muy útil en la práctica para decidir si un polinomio reducido es o no de permutación. En realidad, muy poco se sabe de cuándo un polinomio reducido es de permutación. Uno de los problemas actuales en la teoría de polinomios de permutación es, pues, el siguiente:

Problema 1. Aumentar el número de clases de polinomios de permutación proveyendo criterios adecuados. Ejemplos de estos criterios se encuentran en [9], [24], [25], [27], [37], [51], [55], [57], [59], [60], y en muchos más. En algunos de estos artículos se encuentran también tipos de polinomios que no pueden ser de permutación.

Desde el siglo XIX se conocen criterios para algunas clases de polinomios reducidos [15], algunos de los cuales presentamos a continuación. Otros son más recientes. Algunos de ellos los mencionaremos a lo largo de estos apuntes.

Proposición 2.2. Si $1 \leq m \leq q - 1$, el polinomio $p(X) = X^m \in K[X]$ es de permutación si, y sólo si, $(m, q - 1) = 1$.

Demostración. Demostremos primero que si se tiene $(m, q - 1) = 1$ entonces $p(\alpha) = \alpha^m$ es una biyección. Como K es un conjunto finito, basta ver que $p(\alpha) = \alpha^m$ es una aplicación inyectiva. Si $\alpha_1^m = \alpha_2^m$ y, por ejemplo, $\alpha_1 = 0$, es claro que $\alpha_1 = \alpha_2 = 0$. Supongamos, pues, que $\alpha_1, \alpha_2 \neq 0$, de modo que $\alpha_1^{q-1} = \alpha_2^{q-1} = 1$. Por hipótesis, existen enteros s

y t tales que $1 = sm + t(q - 1)$, de modo que

$$\alpha_1 = \alpha_1^{sm+t(q-1)} = \alpha_2^{sm+t(q-1)} = \alpha_2 .$$

Luego si $\alpha_1^m = \alpha_2^m$ forzosamente tendremos $\alpha_1 = \alpha_2$. Recíprocamente, si $p(\alpha) = \alpha^m$ es una biyección, tenemos necesariamente que $K = K^{(m)} = \{\alpha^m; \alpha \in K\}$. Ahora bien K^\times es un grupo cíclico de orden $q - 1$. Si ζ es un generador de K^\times , sabemos, por la teoría elemental de grupos, que ζ^m genera a K^\times , si, y sólo si, $(m, q - 1) = 1$. \checkmark

Un polinomio de la forma

$$g_k(X, \alpha) := \sum_{j=0}^{[k/2]} \frac{k}{k-j} \binom{k-j}{j} (-\alpha)^j X^{k-2j} , \tag{1}$$

donde $\alpha \in K$ y k es un entero, se dice un *polinomio de Dickson de segunda especie*. Esta denominación se debe a I. SCHUR. Los siguientes son los primeros polinomios de Dickson, para k impar:

$$\begin{aligned} g_1(X, \alpha) &= X \\ g_3(X, \alpha) &= X^3 - 3\alpha X \\ g_5(X, \alpha) &= X^5 - 5\alpha X^3 + 5\alpha^3 X . \end{aligned}$$

Se puede demostrar que podemos transformar $g_k(X, \alpha)$ en un polinomio de la forma $X^k - \alpha X^{-k} \in K[X, X^{-1}]$, lo cual resulta útil en muchos casos.

La siguiente proposición la demostró DICKSON [15, pág. 57] para k impar.

Proposición 2.3. *Un polinomio de Dickson $g_k(X, \alpha)$, con k impar, es un polinomio de permutación si, y sólo si, $(k, q^2 - 1) = 1$. \checkmark*

Problema 2. Es muy difícil decidir si un polinomio de Dickson de segunda especie es o no de permutación. Por lo tanto, es deseable obtener criterios para su clasificación.

En este sentido, por ejemplo, recientemente M. HENDERSON y R. MATTHEWS ([21], [22]) han logrado identificar ciertas familias de polinomios de Dickson que sí lo son. Para conocer el *status artis* de los polinomios de Dickson hasta 1995 recomendamos mirar [32] y [41].

Problema 3. Un polinomio $f(X) \in \mathbb{F}_q[X]$ se dice que define una *función polinomia completa* si $f(X), f(X) + X \in \mathcal{P}$. Este tipo de funciones tiene aplicaciones en cuadrados latinos ortogonales y en otros temas de la combinatoria, así como también en álgebra no asociativa.

En [39] G. L. MULLEN & H. NIEDERREITEN muestran que un polinomio de Dickson define un función polinomia completa sólo en ciertos casos especiales. La demostración de sus resultados se basa en un conocido teorema de S. LANG & A. WEIL sobre una cota para el número de soluciones de polinomios absolutamente irreducibles sobre \mathbb{F}_q (véanse [1] & [54]). De hecho, se han encontrado profundas relaciones entre polinomios de permutación, la teoría de funciones algebraicas y la geometría algebraica (véanse las secciones 3 y 4).

H. NIEDERREITER & K. H. ROBINSON conjeturaron que si $q = 2^n > 3$ toda función polinomia completa de \mathbb{F}_q tiene grado a lo sumo $q - 3$, conjetura que fue demostrada por WAN en 1986 ([58]). Una demostración muy sencilla la obtienen después Q. SUN & Q. F. ZHANG usando métodos locales [56].

Proposición 2.4. Si $f(X) \in \mathcal{P}$, entonces $f_1(X) = \alpha f(X + \beta) + \gamma \in \mathcal{P}$ si $\alpha, \beta, \gamma \in K$, $\alpha \neq 0$.

Demostración. Sean $\sigma_{1,\beta} : K \rightarrow K$, definida por $x \mapsto x + \beta$ y $\sigma_{\alpha,\gamma} : x \mapsto \alpha x + \gamma$. Es claro que estas dos funciones pertenecen a $\mathfrak{S}(K)$. Luego $\bar{f}_1 = \sigma_{\alpha,\gamma} \circ \bar{f} \circ \sigma_{1,\beta}$ es la permutación de K que corresponde al polinomio $f_1(X) = \alpha f(X + \beta) + \gamma \in \mathcal{P}$. \square

Si $f(X)$ es reducido es evidente que $f_1(X)$ es también reducido pues $f_1(X)$ y $f(X)$ tienen el mismo grado.

El polinomio que hemos designado con $f_1(X)$ se llama el *polinomio normalizado* de $f(X)$ si cumple las siguientes propiedades:

- (a) $f_1(X)$ es unitario;
- (b) $f_1(0) = 0$;
- (c) si $p \nmid n = \text{grado de } f_1(X)$, el coeficiente de X^{n-1} es cero.

Esta definición es de DICKSON [14], [15, pág. 62] quien los llama *polinomios reducidos*, apelativo que no usamos hoy para evitar confusión con la noción de polinomio reducido que hemos introducido antes. Allí

mismo DICKSON [15, pág. 63] hace un listado de todos los polinomios de permutación normalizados de grado a lo sumo 5:

Polinomio de permutación normalizado	q
X	para todo q
X^2	2^n
X^3	$3^n, 3m + 2$
$X^3 - \alpha X, \alpha \notin K^2$	3^n
$X^4 \pm 3X$	7
$X^4 + \alpha_2 X^2 + \alpha_3 X$ si su único cero es $x = 0$	2^n
X^5	$5^n, 5m \pm 2, 5m + 4$
$X^5 - \alpha X, \alpha \notin K^4$	5^n
$X^5 \pm 2^{1/2} X$	3^2
$X^5 \pm 2X^2$	7
$X^5 + \alpha X^3 \pm X^2 + 3\alpha^2 X, \alpha \notin K^2$	7
$X^5 + \alpha X^3 + \frac{\alpha^2}{5} X, \alpha$ arbitrario	$5m \pm 2$
$X^5 + \alpha X^3 + 3\alpha^2 X, \alpha \notin K^2$	13
$X^5 - 2\alpha X^3 + \alpha^2 X, \alpha \notin K^2$	5^n

Problema 4. Sorprendentemente, nadie ha extendido esta lista hasta hoy. Es pues atractivo proponer su extensión a polinomios de permutación normalizados de grado mayor.

Las siguientes proposiciones se encuentran demostradas en [15].

Proposición 2.5. Si \mathbb{F}_{q^m} es una extensión de \mathbb{F}_q , entonces el polinomio

$$f(X) = \sum_{j=0}^{m-1} \alpha_j X^{q^j} \in \mathbb{F}_{q^m}[X] \tag{2}$$

es una \mathbb{F}_q -aplicación lineal del \mathbb{F}_q -espacio vectorial \mathbb{F}_{q^m} y permuta a \mathbb{F}_{q^m} si, y sólo si, el único cero de $f(X)$ en \mathbb{F}_{q^m} es $\alpha = 0$. Si, además, cada $\alpha_j \in \mathbb{F}_q$ entonces $f(X)$ permuta a \mathbb{F}_{q^m} si, y sólo si,

$$\left(\sum_{j=0}^{m-1} \alpha_j X^j, X^m - 1 \right) = 1 .$$

Corolario. El polinomio (2) es de permutación si, y sólo si, $\det(\alpha_{i-j}^{q^j}) \neq 0$, $i, j = 0, \dots, m-1$.

Un polinomio como (2) se dice un *polinomio linealizado*. Sobre este tipo de polinomios también se trabaja intensamente (véase, por ejemplo, [18]). Están además relacionados con los llamados grupos de Mathieu [15].

Proposición 2.6. El polinomio $f(X) = X^{q^r} - \alpha X^{q^s} \in \mathbb{F}_{q^m}[X]$, donde $0 \leq s < r \leq m-1$, es de permutación si, y sólo si, $\alpha = 0$ o α no es una potencia $(q^r - q^s)$ -ésima de un elemento de \mathbb{F}_{q^m} .

Demostración. Si $\alpha = 0$, $f(X) = X^{q^r}$ es de permutación por la proposición 2.2, dado que $1 = (q^r, q-1)$. Si $\alpha \neq 0$, entonces $f(\beta) = \beta^{q^r} - \alpha\beta^{q^s} = 0$ ($\beta \in \mathbb{F}_{q^m}$) cuando, y sólo cuando, $\alpha\beta^{q^s} = \beta^{q^r}$. Si $\beta \neq 0$, vemos que $\alpha = \beta^{q^r - q^s} \in (\mathbb{F}_{q^m}^\times)^{q^r - q^s}$. \square

Problema 5. Dado $f(X) \in \mathcal{P}$, calcular el número $C(f)$ de elementos $\gamma \in \mathbb{F}_q$ para los cuales $f(X) + \gamma X \in \mathcal{P}$. Es claro que $C(f) \geq 1$, pues se tiene trivialmente el caso donde $\gamma = 0$.

En [18] se dan algunas condiciones para calcular $C(f)$ y se demuestra además que si $f(X) + \gamma X \in \mathcal{P}$ para por lo menos $\lfloor q/2 \rfloor$ valores de $\gamma \in \mathbb{F}_q$, entonces $f(X) - f(0)$ es un polinomio linealizado. Por otra parte, en [8] si $f(X) + \gamma X \in \mathcal{P}$ ($f(X) \in \mathcal{P}$), entonces el grado de $f(X)$ módulo $(X^q - X)$ es a lo sumo $q-1-C(f)$. En este mismo trabajo se clasifican los polinomios de grado a lo sumo 6 tales que $f(X)$, $f(X) - X$, $f(X) + X \in \mathcal{P}$.

Proposición 2.7. Si $q \equiv 1 \pmod{d}$ y $\alpha \notin \mathbb{F}_q^{\times d}$, entonces el polinomio $f(X) = X(X^d - \alpha)^{(q-1)/d}$ es un polinomio de permutación

Demostración. Sea $\beta \in \mathbb{F}_q$. Si $\beta = 0$, entonces $f(0) = f(\beta) = 0$. Supongamos, pues, que $\beta \neq 0$ y hagamos $Y = X^d - \alpha$, de modo que $f(X)^d = (Y + \alpha)Y^{q-1} = q(Y)$. Queremos entonces encontrar $y \in \mathbb{F}_q^\times$ tal que $(y + \alpha)y^{q-1} = \beta^d$. Si sustituimos y por $1/w$ en la anterior ecuación y multiplicamos por w^p , encontramos

$$1 + \alpha w = \beta^d w^q, \quad (3)$$

que tiene solución para todo $\beta \in \mathbb{F}_q^\times$. En efecto el polinomio $Z^q - (\alpha/\beta^d)Z$ es de permutación, en virtud de la proposición 2.6, pues (α/β^d) no es una potencia d -ésima en \mathbb{F}_q^\times y por fuerza tampoco es una potencia $(q-1)$ -ésima. Luego existe $w \in \mathbb{F}_q^\times$ que satisface (3). \square

Problema 6. En [15, pág. 59] DICKSON conjeturó que si $f(X) \in K[X]$ es un polinomio de permutación de grado q , entonces $p(X)$ es reducible al polinomio de permutación $f(X) = X(X^d - \alpha)^{(q-1)/d}$, donde $d \mid (q-1)$ y $\alpha \notin K^d$. La razón de esta conjetura es que en su tesis doctoral DICKSON [14] la demostró para $q = 3, 5, 7$ y parcialmente para $q = 11$.

Proposición 2.8. Si $(r, q-1) = 1$, $s \mid q-1$ y $g(X^s) \in K[X]$ tiene un cero distinto de 0, entonces $p(X) = X^r(g(X))^{(q-1)/s}$ es de permutación.

Otros resultados recientes relacionados con este tipo de polinomios los expresamos en la siguiente

Proposición 2.9. Los siguientes polinomios son de permutación:

- (a) $X^{(q+m-1)/m} + \alpha X$, donde $m \mid q-1$.
- (b) $X^r(X^d - \alpha)^{(q-1)/d}$, donde $d \mid q-1$.

El siguiente resultado debido a C. HERMITE [23] para $q = p$ y extendido luego por DICKSON a cualquier q [15], es en algunos sentidos el criterio más útil para decidir si un polinomio es o no de permutación.

Proposición 2.10. [Criterio de HERMITE] Un polinomio $p(X) \in \mathbb{F}_q[X]$ es de permutación si, y sólo si,

- (a) $p(X)$ tiene exactamente una raíz en \mathbb{F}_q ; y
- (b) para cada t con $1 \leq t \leq q-2$, $\not\equiv 0 \pmod{p}$, la reducción de $(p(X))^t$ módulo $(X^q - X)$ tiene grado $t \leq q-2$.

Corolario. Si $p(X) \in K[X]$ es de permutación, de grado $n > 1$, entonces $n \nmid (q-1)$.

Muy parecidos a los polinomios de Dickson son los llamados *polinomios de Chébichev de segunda especie* y grado k :

$$f_k(X) := \sum_{j=0}^{\lfloor k/2 \rfloor} \binom{k-j}{j} (-1)^j X^{k-2j}, \tag{4}$$

Se puede demostrar que $f_k(X) = Xf_{k-1}(X) - f_{k-2}(X)$ para $k \geq 2$.

En [34] se demuestra la siguiente proposición:

Proposición 2.11. *Sea $f_k(X) \in K[X]$ un polinomio de Chébishev de segunda especie. Si q es impar y $k + 1 \equiv \pm 2 \pmod{m}$, para $m = p$, $(q - 1)/2$ y $(q + 1)/2$ entonces $f_k(X)$ es de permutación, y $f_k(-\alpha) = -f_k(\alpha)$ y $f_k(\alpha) = \pm \alpha$ para todo $\alpha \in K$.*

Problema 7. Basados en evidencia computacional, LIDL & MULLEN conjeturaron que la condición de la anterior proposición es necesaria y suficiente para que $f_k(X) \in \mathcal{P}$, si $p > 5$. Si $p = 3, 5$ existen ejemplos de $q > p$ y de k para los cuales $f_k(X)$ permuta a \mathbb{F}_q pero no satisface las congruencias de la proposición. El problema consiste en verificar la verdad o falsedad de la conjetura propuesta.

Al respecto, S. D. COHEN en [10] demuestra que la conjetura es correcta si $q = p$. Para su demostración usa el siguiente resultado que se encuentra en [6]:

Proposición 2.12. *Si $p > 5$, $g_k : \mathbb{F}_q \rightarrow \mathbb{F}_q$ y $g_k(\alpha) = \pm f_k(\alpha)$, para todo $\alpha \in \mathbb{F}_q$, entonces*

$$\sum_{\alpha \in \mathbb{F}_q} (g_k(X))^{2r} = 0 \quad \text{si } r = 1, \dots, \frac{p-3}{2}.$$

✓

Para demostrarla, COHEN sólo necesita considerar los casos en que $r \leq 3$. Aunque su demostración es esencialmente teórica, en el caso $r = 3$ usó un paquete de álgebra simbólica para calcular las resultantes de varios polinomios. Poco tiempo después, el mismo COHEN [11] empleó un método similar para demostrar la conjetura cuando $q = p^2$, $p > 5$. Si $d > 2$ el método de COHEN podría conducir en teoría a una demostración completa de la conjetura, pero los cálculos previstos serían muy complicados, por lo que en 1995 este caso estaba aún sin resolver.

En [20] MARIE HENDERSON & R. MATTHEWS describen nuevas clases de polinomios de Chébishev para $p = 3, 5$ y obtienen algunos resultados en característica 2.

Queremos terminar esta sección estableciendo una de las numerosas conexiones entre los polinomios de permutación (que recordemos no son otra cosa que elementos de un grupo de permutaciones) y la teoría de los grupos. Si usamos como ley de composición la composición usual de funciones, tenemos el siguiente resultado:

Proposición 2.13 *El conjunto de los polinomios de la forma*

$$\alpha X^{(q+1)/2} + \beta X \in \mathbb{F}_q[X] \tag{5}$$

es cerrado para la composición módulo el polinomio $X^q - X$. En particular, los polinomios de permutación de la forma (5) que son de permutación conforman un grupo para esta ley de composición. El orden de este grupo está dado por $(q - 1)^2/2$.

Resultados relacionados con los de la anterior proposición se encuentran, por ejemplo, en [36].

3. Extensión de los polinomios de permutación a los anillos

$$\mathbb{Z}/p^n\mathbb{Z}$$

Una primera extensión de los anteriores problemas y resultados se hace para los anillos modulares $\mathbb{Z}/n\mathbb{Z}$. El teorema chino de los restos nos permite restringirnos al caso de los anillos $\mathbb{Z}/p^n\mathbb{Z}$, donde p es un número primo. Se puede demostrar lo siguiente:

Proposición 3.1. *Un polinomio $f(X) \in (\mathbb{Z}/p^n\mathbb{Z})[X]$ es de permutación si, y sólo si, $f(X)$ considerado como polinomio de coeficientes en $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ es de permutación y no tiene ceros singulares.*

Para los polinomios de Dickson escritos bajo la forma $g_k(X, \alpha) = X^k - \alpha^k X^{-k}$, W. NOBAUER demuestra lo siguiente:

Proposición 3.2. *Si $g_k(X, \alpha)$ se considera con coeficientes en $\mathbb{Z}/p^e\mathbb{Z}$, p primo, $e > 1$, entonces este polinomio es de permutación si, y sólo si, $(k, p(p^2 - 1)) = 1$.*

Nótese la similitud con la proposición 2.3. Existen muchos otros resultados en la literatura.

Estos resultados también se usan en criptografía. Por ejemplo, los puntos fijos de una permutación son de interés en la construcción de

criptosistemas RSA. Por ejemplo, uno puede usar las permutaciones $x \mapsto x^k$ en $\mathbb{Z}/n\mathbb{Z}$, donde m es primitivo (es decir, sin factores cuadráticos) para construir un criptosistema. Sin embargo, pueden surgir alteraciones debidas a los puntos fijos de las permutaciones inducidas. Por esta razón, vale la pena estudiar los puntos fijos, en particular, su número. Sobre estos asuntos se pueden consultar los siguientes trabajos: [5], [7], [12], [17], [24], [27], [30], [46], [48]. Por ejemplo, en [47] se demuestra la siguiente proposición:

Proposición 3.3. *Si $g_k(X, \alpha)$ se considera con coeficientes en $\mathbb{Z}/p^e\mathbb{Z}$, p primo, $e > 1$, el número N de puntos fijos de este polinomio esá dado por:*

$$N = \begin{cases} 2^e & \text{si } e < 3 \\ 2(k - \binom{k}{3}, 2^{e-2}) + 2(k^2 - 1, 2^{e-3}) + \frac{1}{2}(k^2 - 1, 2^{e-1}), & \text{donde} \\ & \binom{\cdot}{\cdot} \text{ es el s\u00edmbolo de Legendre} \end{cases}$$

si $p = 2$.

$$N = \left(\frac{k+1}{2}, 3^{e-1}2\right) + \left(\frac{k-1}{2}, 3^{e-1}2\right) + 3^\epsilon(k^2 - 1, 3^{e-1} - 1),$$

si $p = 3$, donde $\epsilon = 0$ si $3^{e-1} \mid (k^2 - 1)$ y $\epsilon = 1$ en caso contrario. Si $p > 3$, entonces

$$N = \left(\frac{k+1}{2}, p^{e-1}\frac{p-1}{2}\right) + \left(\frac{k+1}{2}, p^{e-1}\frac{p+1}{2}\right) \\ + \left(\frac{k-1}{2}, p^{e-1}\frac{p-1}{2}\right) + \left(\frac{k-1}{2}, p^{e-1}\frac{p+1}{2}\right)$$

4. Polinomios de permutaci\u00f3n en las \u00e1lgebras L_ν

Desde hace alg\u00fan tiempo hemos trabajado en la aritm\u00e9tica de los anillos de polinomios sobre cuerpos finitos, buscando resultados an\u00e1logos a los de la teor\u00eda cl\u00e1sica de los n\u00fameros (la llamada *aritm\u00e9tica superior*) o encontrando nuevas demostraciones siguiendo un \u00fanico hilo conductor, el cual pasamos a explicar de la misma manera que lo hacemos en [2].

Tomamos $\mathbb{F}_q[X]$ y en él un polinomio irreducible y unitario

$$p(X) = \pi_0 + \pi_1 X + \cdots + \pi_{d-1} X^{d-1} + X^d, \quad (6)$$

con el propósito de estudiar la estructura de los anillos

$$\mathbb{F}_q[X]/(p(X)^\nu), \quad \nu = 1, 2, \dots,$$

de la misma manera que se estudian los anillos $\mathbb{Z}/(p^\nu\mathbb{Z})$ en el caso clásico.

En primer lugar tenemos la siguiente proposición:

Proposición 4.1. *Sea $p(X)$ dado por la ecuación (6). Si x designa a la clase de equivalencia de X módulo $(p(X)^\nu)$, entonces:*

- (a) $\mathbb{F}_q[X][X]/(p(X)^\nu)$ es una \mathbb{F}_q -álgebra de dimensión νd y $q^{\nu d}$ elementos.
- (b) $1, x, \dots, x^{\nu d-1}$ es una \mathbb{F}_q -base de esta álgebra.
- (c) Si $\theta(a(X)) = \theta(\sum_{k=0}^m \alpha_k X^k) := \sum_{k=0}^m \alpha_k x^k$, entonces $\theta(p(X)) := z_\nu$ cumple las condiciones $z_\nu^\nu = 0, z_\nu^k \neq 0$ si $0 \leq k < \nu$.
- (d) Los polinomios unitarios de $\mathbb{F}_q[X]$ de grado estrictamente menor que νd forman un sistema completo de restos módulo $(p(X)^\nu)$.
- (e) El álgebra $\mathbb{F}_q[X]/(p(X)^\nu)$ contiene un cuerpo L isomorfo al cuerpo $\mathbb{F}_q[X]/(p(X))$ ($L \approx \mathbb{F}_{q^d}$).
- (f) La L -dimensión de

$$\mathbb{F}_q[X]/(p(X)^\nu) = L_\nu = \{\lambda_0 + \lambda_1 z_\nu + \cdots + \lambda_{\nu-1} z_\nu^{\nu-1}; \lambda_i \in L\}, \quad z_\nu^\nu = 0,$$

es ν , una de cuyas bases (llamada canónica) es precisamente $1, z_\nu, \dots, z_\nu^{\nu-1}$. \square

Observemos que L_ν , como L -álgebra, es la suma directa de ν cuerpos todos iguales a L . Por otra parte, es claro que $L_\nu \approx L[Z]/(Z^\nu)$.

Como vemos, hemos linealizado la estructura de $\mathbb{F}_q[X]/(p(X)^\nu)$, lo cual resulta muy útil. Por ejemplo, es fácil ahora demostrar la siguiente

Proposición 4.2. *El grupo de las unidades de L_ν está dado por*

$$L_\nu^\times = L^\times \times \{1 + \lambda_1 z_\nu + \cdots + \lambda_{\nu-1} z_\nu^{\nu-1}; \lambda_i \in L\}.$$

Este grupo tienen orden $(q^d - 1)q^{d(\nu-1)}$. \square

El subgrupo (que es un p -grupo)

$$U_\nu = \{1 + \lambda_1 z_\nu + \cdots + \lambda_{\nu-1} z_\nu^{\nu-1}; \lambda_i \in L\}$$

del grupo L_ν^\times se llama el grupo de las *unidades principales*. Su estructura está dada por

$$\prod_{\substack{j=1 \\ p \nmid j}}^{\nu-1} \left[\underbrace{C(p^{\theta_j}) \times \cdots \times C(p^{\theta_j})}_{m=td \text{ veces}} \right], \quad (7)$$

donde $t = [\mathbb{F}_q : \mathbb{F}_p]$, $m = [\mathbb{F}_q^d : \mathbb{F}_p]$ y $C(p^{\theta_j})$ designa al grupo cíclico con p^{θ_j} elementos y

$$\theta_j = \min\{\theta = 0, 1, 2, \dots; j p^\theta \geq \nu\}.$$

Con lo anterior es posible determinar cuándo L_ν^\times es cíclico [3]:

Proposición 4.3. *Para $p(X) \in K[X]$, unitario e irreducible, de grado d , tenemos*

- (a) Si $d > 1$, L_ν^\times es cíclico $\Leftrightarrow \nu = 1$.
- (b) Si $d = 1$ y $p \neq 2$, entonces L_ν^\times es cíclico $\Leftrightarrow K = \mathbb{F}_p$, $\nu = 1, 2$ ó $K = \mathbb{F}_q$, $q > p$, $\nu = 1$.
- (c) Si $d = 1$, $p = 2$, entonces L_ν^\times es cíclico \Leftrightarrow Si $q = 2$, $\nu = 1, 2, 3$ ó $q > 2$, $\nu = 1$.

Como vemos no hay muchos L_ν^\times que sean cíclicos, contrariamente a lo que sucede en el caso clásico: Si p es un número primo impar, entonces el grupo de las unidades de $\mathbb{Z}/p^\nu\mathbb{Z}$ es cíclico para todo $\nu \geq 1$.

El problema que nos proponemos es el siguiente: Investigar los polinomios de permutación $f(t_1, \dots, t_i) \in L_\nu[t_1, \dots, t_s]$, es decir, aquellos que inducen una biyección de $L_\nu \times \cdots \times L_\nu$ (s veces) en sí misma.

Empecemos por el caso más sencillo: $f(t) = t^k$ ($k \geq 1$). Es claro que $f(0) = 0$. Si $\nu = 1$ estamos en el caso de la proposición 2.2. Luego podemos suponer que $\nu \geq 2$. Escribimos

$$\lambda(z_\nu) := \lambda_0 + \lambda_1 z_\nu + \cdots + \lambda_{\nu-1} z_\nu^{\nu-1}.$$

El elemento de $\lambda(z_\nu) = z_\nu^{z-1}$, se convierte en $\lambda(z_\nu)^k = z_\nu^{k(\nu-1)}$ el cual es nulo si, y sólo si, $k(\nu-1) \geq \nu$, es decir, si $k \geq \frac{\nu}{\nu-1} > 1$. En este caso

$f(t) = t^k$ no puede ser de permutación. Por otra parte, $\lambda(z_\nu)^k \neq 0$ si, y sólo si, $k(\nu - 1) \leq \nu - 1$, es decir, si $k \leq 1$, o también si $k = 1$. Pero es claro que $f(t) = t$ es de permutación. Luego

Proposición 4.4. *Si $\nu \geq 2$, el único polinomio de la forma $f(t) = t^k$ que es de permutación es $f(t) = t$.*

La cosa no es, pues, muy prometedora. Pero lo anterior es un caso particular de los siguiente: *Un polinomio $f(t) \in L_\nu[t]$ es de permutación si, y sólo si, $f(t) \in L[t]$ es de permutación y no tiene raíces múltiples (Cfr. Proposición 3.1).*

La siguiente es otra posibilidad de generalización: en [6] BRISON da una generalización del concepto de polinomio de permutación que llama *polinomios grupo-permutantes*, la cual adaptamos así: Un polinomio $f(t) \in L_\nu[t]$ se dice grupo-permutante si induce en algún subgrupo de L_ν^\times una permutación de este subgrupo.

Por ejemplo, tenemos la siguiente proposición:

Proposición 4.5. *Si L_ν^\times es cíclico, entonces $f(t) = t^k$ permuta a L_ν^\times si, y sólo si, $\text{m.c.d.}(k, q^{d\nu}(q^d - 1)) = 1$.*

Demostración. Sea $\zeta(z_\nu)$ un generador de L_ν^\times . El elemento $\zeta(z_\nu)^k$ es un generador de este grupo de orden $(q^d - 1)q^{d(\nu-1)}$ si y sólo si, $\text{m.c.d.}(k, q^{d(\nu-1)}(q^d - 1)) = 1$. \square

Esta proposición abarca la 2.2 cuando $\nu = 1$, por lo cual la generalización propuesta parece adecuada.

El trabajo de BRISON utiliza como punto de partida los subgrupos cíclicos (en nuestro caso) de L_ν^\times . De acuerdo con la fórmula (7), estos son de dos formas:

- (a) $L^\times \times C(p^{\theta_j})$, de orden $(q^d - 1)p^{\theta_j}$,
- (b) $C(p^{\theta_j})$, de orden p^{θ_j} ,

donde $j = 1, \dots, \nu - 1$, $p \nmid j$. De aquí resulta que $f(t) = t^k$ permuta a los subgrupos del tipo (a) si, y sólo si, $\text{m.c.d.}(k, (q^d - 1)p^{\theta_j}) = 1$ y a los del tipo (b) si, y sólo si, $\text{m.c.d.}(k, p^{\theta_j}) = 1$ (la demostración de lo anterior sigue de la de la proposición 4.5).

Otras posibilidades de estudiar y clasificar los polinomios de permutación de L_ν son las sugeridas por SOPHIE FRISCH [19]) o por Q. F. ZHANG [61]. Pero de esto hablaremos en una ocasión próxima.

5. Nota final

Este artículo constituye el texto definitivo de la charla que dio el autor en el marco de la *Primera Conferencia Iberoamericana de Matemática Computacional*, Bogotá, julio de 2002, por invitación de los organizadores de este evento, invitación que se extendió a su publicación en esta revista. Por lo anterior, quiere agradecer a los organizadores del evento, en especial a la Sociedad Colombiana de Matemáticas.

REFERENCIAS

- [1] VÍCTOR S. ALBIS. *Varietades y ecuaciones sobre cuerpos finitos* (policopiado). Universidad Nacional de Colombia, Bogotá, 1985.
- [2] VÍCTOR S. ALBIS. *Lecciones sobre la aritmética de polinomios* (policopiado). Universidad Nacional de Colombia, Bogotá, 1999.
- [3] VÍCTOR S. ALBIS. *Raíces primitivas en cuerpos aritméticos de funciones algebraicas*. *Lecturas Mat.* **7** (1986), 15–23.
- [4] VÍCTOR S. ALBIS & R. CHAPARRO. *On a conjecture of Borevich and Shafarevich*. *Rev. Acad. Colomb. Cienc.* **21** (1997), 313–319 [MR 98g:11130].
- [5] G. R. BLACKLEY & DAVID CHAUM. *Advances in Cryptology. Theory and application of cryptographic techniques* (Santa Barbara CA 1984). *Lecture Notes in Computer Science* 196. Springer–Verlag, Berlin–New York, 1985 [MR 86j:94003].
- [6] OWEN J. BRISON. *On group-permutation polynomials*. *Portugal. Math.* **50** (1993), 365–383 [MR 95j:12001].
- [7] PASCALE CHARPIN. *Une description des codes de Reed–Solomon dans une algèbre modulaire*. *C. R. Acad. Sci. Paris Sér. I Math.* **299** (1984), 779–782 [MR 86m: 94036].
- [8] W. S. CHOU. *Set complete mappings of finite fields*. In *Finite fields, coding theory and advances in communications and computing* (Las Vegas 1991). *Lect. Notes in Pure and Appl. Math.* **141**, Dekker, NY, 1993 [MR 93m:11128].
- [9] W. S. CHOU. *Binomial permutations of finite fields*. *Bull. Austral. Math. Soc.* **38** (1988), 325–327 [MR 89m:11117].
- [10] STEPHEN D. COHEN. *Dickson polynomials of the second kind that are permutations*. *Canad. J. Math.* **46** (1994), 225–238 [MR 95c:11143].

- [11] STEPHEN D. COHEN. *Dickson permutations*. In *Number-theoretic and algebraic methods in computer sciences* (Moscow 1993), World Sci. Publishing, River Edge, NJ, 1995, 29–51 [MR 97a:11195].
- [12] STEPHEN D. COHEN & HARALD NIEDERREITER (Eds.) *Proceedings of the Third International Conference on Finite Fields and Applications* (Glasgow 1995). London Math. Soc. Lecture Notes Series, 233. Cambridge University Press, Cambridge, 1996 [MR h: 11002].
- [13] J. DEMEL, M. DEMLOVA & V. KPUBEK. *Fast algorithms constructing minimal subalgebras, congruences and ideals in a finite algebra*. Theoret. Comput. Sci. **36** (1985), 302–216 [MR 87c:68036].
- [14] L.E. DICKSON. *The analytic representation of substitutions on a power of a prime of letters with a discussion of the linear group*. Ann. of Math. **11** (1897), 65–120, 161–183.
- [15] L.E. DICKSON. *Linear Groups with an Exposition of the Galois Field Theory*. Dover Publ.: New York, 1958 [MR 21#3488].
- [16] D. DORNINGER, G. EIGENTHALER, H. K. KAISER & W. B. MULLER (Eds.) *Contributions to general algebra 8*. Holder–Pichler–Tempsky, Vienna, 1988 [MR 91g:00033].
- [17] E. ECKER. *Finite semigroups and the RSA-cryptosystem*. Lecture Notes in Comput. Sci. 149. Springer–Verlag, Berlin–New York, 1983 [MR 84k:94019].
- [18] R. J. EVANS, J. GREENE & H. NIEDERREITER. *Linearized polynomials and permutation polynomials of finite fields*, Michigan Math. J. **39** (1992), 405–413 [MR 93j:11080].
- [19] SOPHIE FRISCH. *When are weak permutation polynomials strong?*. Finite Fields Appl. **1** (1995), 437–439 [MR 96i:11133].
- [20] MARIE HENDERSON & REX MATHEWS. *The permutation properties of Chebyshev polynomials of the second kind over a finite field*. Finite Fields Appl. **1** (1995), 115–125 [MR 96b: 11155].
- [21] MARIE HENDERSON. *A note on the permutation behaviour of the Dickson polynomials of the second kind*. Bull. Austral. Math. Soc. **56** (1997), 499–505 [MR 99a: 11138].
- [22] MARIE HENDERSON & REX MATHEWS. *Dickson polynomials of the second kind which are permutation polynomials over a finite field*. New Zealand J. Math **27** (1998), 227–244 [MR 200e: 11148].
- [23] C. HERMITE. *Sur les fonctions de sept lettres*. C. R. Acad. Sci. Paris **57** (1863), 750–757. *Oeuvres*, vol. 2, Gauthier–Vilars, Paris, 1908, 280–288.
- [24] S. Y. KIM & J. B. LEE. *Permutation polynomials of the type $x^{1+((q-1)/m)}+ax$* . Commun. Koren Math. Soc. **10** (1995), 823–829 [MR 97k:11167].
- [25] J. B. LEE & Y. H. PARK. *Some permuting trinomials over finite fields*. Acta Math. Sci (Shuxue Wuli Xuebao) **17** (1997), 250–254 [MR 98i:11104].
- [26] J. LEVINE & J. V. BRAWLEY. *Some cryptographic applications of permutation polynomials*. Cryptologia **1** (1977), 76–92.

- [27] CHAO LI. *Elliptic curves of trace zero over finite fields*. Hunan Ann. Math. **18** (1998), 1–5 [MR 2000c: 11088].
- [28] R. LIDL & H. NIEDERREITER. *Finite Fields*. Encyclopedia of Mathematics and its Applications 20. Addison–Wesley, Reading MS, 1983 [MR 86c:11106].
- [29] R. LIDL & W. B. MULLER. *A note on polynomials and functions in algebraic cryptography*. Ars. Combin. **17A** (1984), 223–229.
- [30] R. LIDL & H. NIEDERREITER. *Introduction to Finite Fields and their Applications*. Cambridge University Press: Cambridge, 1986.
- [31] R. LIDL & G. L. MULLEN. *When does a polynomial over a finite field permute the elements of the field?* Amer. Math. Monthly **95** (1988), 243–246.
- [32] R. LIDL, G. L. MULLEN & G. TURNWALD. *Dickson polynomials*. Pitman Monographs and Surveys in Pure and Applied Mathematics 65. Logman Scientific & Technical, Harlow, 1993 [MR 94i:11097].
- [33] J. H. VAN LINT. *Introduction to Coding Theory* (2nd edition). Springer–Verla, Berlin, 1992.
- [34] R. W. MATHEWS. *Permutation polynomials in one and several variables*. Ph. D. Dissertation, University of Tasmania, 1982.
- [35] R. W. MATHEWS. *Permutation polynomials over algebraic number fields*. J. Number Theory **18** (1984), 249–260 [MR 85j:11136].
- [36] R. R. MATHEWS. *Some generalizations of Chebyshev polynomials and their induced group structure over a finite field*. Acta Arith. **41**, 323–335.
- [37] R. A. MOLLIN & C. SMALL. *On permutation polynomials over finite fields*. Internat. J. Math. Math. Sci. **10** (1987), 535–543 [MR 88i:11096].
- [38] GARY L. MULLEN & HARALD NIEDERREITER. *The structure of a group of permutation polynomials*. J. Austral. Math. Soc. Ser. A **38** (1985), 164–170 [MR 86f:11095].
- [39] GARY L. MULLEN & HARALD NIEDERREITER. *Dickson polynomials over finite fields and complete mappings*. (1987) [MR 88c:11074].
- [40] GARY L. MULLEN & THERESA P. VAUGHAN. *Cycles of linear permutations over a finite field*. Linear Algebra Appl. **108** (1988), 63–82 [MR 89m:11118].
- [41] GARY L. MULLEN. *Dickson polynomials over finite fields: a survey of recent results*. In *Number-theoretic and algebraic methods in computer science* (Moscow 1993). World Sci. Pub., River Edge NJ, 1995, 139–149 [MR 97b:11147].
- [42] WINFRIED B. MULLER & W. NOUBAUER. *Über die Fixpunkte der Potenzpermutationen*. Österreich. Akad. Wiss. Math. Natur. Kl. Sitzungsber. **192** (1983), 93–97 [MR 85:11008].
- [43] H. NIEDERREITER & K. H. ROBINSON. *Complete mappings of finite fields*. J. Austral. Math. Soc. Ser. A **33** (1982), 197–212 [MR 83j: 12015].
- [44] HARALD NIEDERREITER. *Finite fields and their applications*. In *Contributions to general algebra 7* (Vienna 1990), Holder–Pichler–Tempsky, Vienna 1991, 251–264 [MR 92j:11146].

- [45] RUPERT NOBAUER. *Redei-Permutationen auf Restklassenringen $\mathbb{Z}/(m)$* . Monats. Math. **106** (1988), 41–56 [MT 90c:11901].
- [46] WILFRIED NOBAUER. *Polynomfunktionen auf primen Restklassen*. Arch. Math **39** (1982), 431–435 [MR 84h:12028].
- [47] WILFRIED NOBAUER. *Über die Fixpunkte der Dickson-Permutationen*. Österreich. Akad. Wiss. Math. Natur. Kl. Sitzungsber. II **193** (1984), 115–133 [MR 87a: 11126].
- [48] WILFRIED NOBAUER. *On the length of cycles of polynomial permutations*. In *Contributions to general algebra 3* (Vienna 1984). Holder–Pichler–Tempsky, Vienna, 1985, 265–271 [MR 87f: 11101].
- [49] WILFRIED NOBAUER. *Über die Konjugierten der Dickson-Permutationen*. Österreich. Akad. Wiss. Math. Natur. Kl. Sitzungsber. II **196** (1987), 119–140.
- [50] WILFRIED NOBAUER. *Über die Fixpunkte von durch Dicksonpolynome dargestellten Permutationen*. Acta Arith. **45** (1985), 173–181 [MR 87a: 11125].
- [51] Y. H. PARK & J. B. LEE. *Permutation polynomials with exponents in an arithmetic progression*. Bull. Austral. Math. Soc **57** (1998), 243–252- [MR 99b: 11134].
- [52] REINHOLD PIEPER. *Cryptanalysis of Redei and Dickson permutations*. Appl. Algebra Engrg. Comm, Comput **4** (1993), 59–76.
- [53] E. A. POE, *The gold-bug*. In *18 Best Stories by Edgar Allan Poe*. Edited by Vincent Price & Chandler Brossard. Dell Pub., New York NY, 1965.
- [54] W. M. SCHMIDT. *Equations over finite fields*. Lect, Notes in Math. 536, Springer, Berlin, 1976 [MR 55# 2744].
- [55] CHARLES SMALL. *Permutation binomials*. Internat. J. Math. Math. Scie. **13** (1990), 337–342 [MR 91g:11148].
- [56] Q. SUN & Q. F. ZHANG. *A simple proof of a conjecture about complete mappings over finite fields*. Sichuan Daxue Xuebao **35** (1998), 840–842 [MR 99m:11143].
- [57] GERHARD TURNWALD. *Permutation polynomials of binomial type*. In *Contributions to general algebra 6*, Holder–Pichler–Tempsky, Vienna, 1988, 281–286.
- [58] D. Q. WAN. J. Austral. Math. Soc. Ser. A **41** (1986), 336–338 [MR 87k:11137].
- [59] D. Q. WAN & R. LIDL. *Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure*. Monatsh. Math. **112** (1991), 149–163.
- [60] T. L. XIE. *Permutation polynomials over finite fields \mathbb{F}_q* . Sichuan Daxue Xuebao **27** (1990), 414–417 [MR 91i:11173].
- [61] Q. F. ZHANG. *Permutation polynomials in several indeterminates over $\mathbb{Z}/m\mathbb{Z}$* . Chinese Ann. Math. Ser. A **16** (1995), 168–172 [MR 96g:11143].

(Recibido en agosto de 2001)

VICTOR SAMUEL ALBIS
DEPARTAMENTO DE MATEMÁTICAS
UNIVERSIDAD NACIONAL DE COLOMBIA, BOGOTÁ, COLOMBIA
e-mail: valbis@accefyn.org.co