Universidad de Valladolid

Facultad de Ciencias

Máster en Matemáticas

Polinomios sobre cuerpos finitos

Autor: Darío Sánchez Carpintero

Tutor: Jose Enrique Marcos Naveira

Curso: 2023-2024

Índice general

Capítulo 1

Introducción

La motivación de este trabajo reside en la creciente relevancia que han obtenido los sistemas de transmisión y cifrado de información en las últimas décadas. Para este fin, son de vital importancia los cuerpos finitos. Computacionalmente, son sencillos de construir: se comienza eligiendo una característica para el cuerpo, siendo esta un primo p, y se consideran los enteros módulo p, $\mathbb{Z}_p$. El resto de cuerpos finitos de característica p se construye a partir de este primero: se busca un polinomio $f(x)$ irreducible sobre $\mathbb{Z}_p$, y entonces $\mathbb{Z}_p[x]/(f(x))$ forma un dominio de integridad conmutativo. Por ser finito, también es un anillo de división, por lo que es un cuerpo finito.

Uno de los objetivos del capítulo de preliminares es demostrar que este proceso constructivo no solo permite obtener todos los cuerpos finitos, sino que también es la única manera de hacerlo. Además, este método viene dado por extensiones algebraicas, de forma que podemos considerar el cuerpo construido como un espacio vectorial cuya base viene dada por las raíces del polinomio irreducible. Veremos que estas raíces están todas relacionadas entre sí por una potencia del automorfismo de Frobenius. Esta potencia viene dada por el grado del polinomio irreducible.

El capítulo 3 hace más énfasis en el operador traza, y lo relaciona con el concepto de producto escalar en espacios vectoriales sobre el cuerpo de los números complejos. De forma análoga a estos, podemos conseguir dualidad sobre los vectores, y la utilizaremos para facilitar los cálculos de traza a través de bases duales. Trabajaremos también con bases normales, dadas por la órbita de un único elemento sobre el automorfismo de Frobenius, cuyo uso está justificado por su eficiencia computacial, aunque no llegaremos a demostrar dicha eficiencia.

El capítulo 4 se enfoca más en los elementos no nulos del cuerpo $\mathbb{F}_q$ (el cuerpo finito de q elementos) como grupo multicativo, $\mathbb{F}_q^*$. Este grupo tiene algún elemento primitivo, es decir, que lo genera totalmente. El objetivo del capítulo es caracterizar los elementos primitivos así como los polinomios de los que son raíces, denominados también primitivos. También es relevante considerar formas de construir nuevos polinomios primitivos a partir de otros.

El uso de elementos primitivos no es meramente teórico. Por ejemplo, estos tienen utilidad en el contexto de la criptografía: en el protocolo de intercambio de claves Diffie-Hellman, se realiza un intercambio de potencias de un elemento primitivo sobre un cuerpo finito, y este proceso resulta computacionalmente seguro (bajo los estándares de computación no cuántica) debido a la dificultad del problema del logaritmo discreto.

En los siguiente dos apartados, nos centramos específicamente en polinomios irreducibles. Tenemos dos objetivos que queremos cumplir con respecto a estos polinomios: el primero, es asegurarnos de que dado un polinomio $f(x) \in \mathbb{F}_q[x]$, entonces el $\mathbb{F}_q$-espacio vectorial $\mathbb{F}_q[x]/(f(x))$ se pueda considerar un cuerpo. El segundo es ser capaces de generar rápidamente y sin necesidad de cálculos complejos cuerpos finitos a partir de otros. En relación al primer objetivo, tenemos distintos criterios de irreducibilidad: o bien resultados que requieren cálculos numerosos y pesados, o bien otros más sencillos que apliquen a familias de polinomios limitadas, por ejemplo ciertas familias de trinomios. Con respecto al segundo objetivo, las propiedades que vamos a estudiar son aquellas que determinen la irreducibilidad de una cierta transformación de polinomios irreducibles, dada por una composición por un cociente de polinomios.
Ambos temas recibirán resultados auxiliares en el capítulo 6, donde nos enfocamos en polinomios irreducibles sobre $\mathbb{F}_2$, motivados por la gran relevancia en informática de los sistemas binarios.

El capítulo 7 está dedicado a la factorización de polinomios. La primera parte dscribe el algoritmo de Berlekam como proceso de factorización. Después de explicar su funcionamiento, nos enfocamos en justificar que es un método válido de factorización: en primer lugar, permite obtener como factores los polinomios irreducibles agrupados por su multiplicidad, es decir, si un polinomio irreducible $r(x)$ es parte de la factorización con multiplicidad m, entonces uno de los factores que se obtiene es $r(x)^m$. En segundo lugar, vemos que los factores irreducibles se pueden obtener casi directamente a partir de la derivada de la potencia obtenida.
El capítulo termina viendo la construcción de los polinomios ciclotómicos, obtenidos como factores del polinomio $x^n - 1$ para algún natural n, y finalmente la forma de determinar su irreducibilidad.

A modo de anexo, el capítulo final intenta determinar la construcción y estructura de las clausuras algebraicas de los cuerpos finitos, así como de las extensiones algebraicas en general. En concreto, se busca establecer una correspondencia entre estas extensiones y una familia de subconjuntos de los números naturales, denominada números de Steinitz.

Capítulo 2

Preliminares

Este capítulo está enfocado en cuerpos finitos y polinomios sobre ellos, sobre todo irreducibles, haciendo un pequeño repaso sobre propiedades básicas y desarrollando algunos resultados fundamentales que nos harán falta más adelante. Consideramos conocidas nociones básicas de cuerpos y extensiones algebraicas sobre cuerpos arbitrarios. Para esta parte seguimos los resultados de *Introduction to finite fields and their applications* [11].

2.1. Estructura de los cuerpos finitos

Parece intuitivo que los cuerpos finitos de un mismo orden sean isomorfos, o lo que es lo mismo, que un cuerpo finito quede completamente caracterizado por su orden, que es lo que buscaremos demostrar con los resultados de esta sección.

Usualmente, el cuerpo finito de q elementos se suele denotar por $\mathrm{GF}(q)$ o $\mathbb{F}_q$. De aquí en adelante, lo denotaremos por $\mathbb{F}_q$. Posteriormente, veremos que este cuerpo está bien definido.

Un primer resultado notable es que, sobre un conjunto finito, es equivalente considerar una estructura de cuerpo o una estructura de anillo de división. Este resultado está demostrado en [11, p. 67].

Teorema 2.1 (Teorema de Weddeburn)**.** *Todo anillo de división finito es un cuerpo.*

Si un cuerpo finito tiene característica p, podemos construir un subcuerpo sobre él de la siguiente manera: consideramos el conjunto de elementos generados aditivamente por el elemento 1, es decir, el conjunto $\{a \in \mathbb{F}_q,\ a = 1+\overset{i}{\cdots}+1 \quad | \quad 1 \leqslant i \leqslant p\}$. Esto es equivalente a considerar los enteros módulo p, que forman un cuerpo llamado subcuerpo primo.

Definición 2.2. *Sea K un cuerpo. Se define el* ***subcuerpo primo*** *de K como la intersección de todos los subcuerpos no vacíos de K. Además, este es isomorfo, o bien a $\mathbb{Q}$ si es de característica 0, o bien a $\mathbb{F}_p$ si es de característica p.*

Como tenemos un subcuerpo cuya construcción se puede realizar sobre cualquier cuerpo finito, podemos considerar los cuerpos finitos como espacios vectoriales sobre sus subcuerpos primos.

Teorema 2.3. *Sea F un cuerpo finito. Entonces F tiene p^n elementos, siendo p la característica de F y n el grado de F sobre su subcuerpo primo K.*

Demostración. La característica de F es evidentemente prima y como consecuencia K es un subcuerpo finito de F. Podemos considerar que F es un espacio vectorial sobre K, de dimensión (trivialmente finita) $n = [F : K]$. Por tanto, se puede tomar una K-base de F formada por n elementos $b_1, \ldots, b_n$, y todo elemento de F es de la forma $a_1b_1 + \cdots + a_nb_n$, siendo cada a_i un elemento de K. Como cada a_i puede tomar $p = |K|$ valores, tenemos que $|F| = p^n$. □

La presencia de un subcuerpo primo sugiere que este es fundamental a la hora de construir cualquier cuerpo finito. En particular, estos se obtienen como cuerpo extensión de un cierto polinomio de grado dado. Nos pondremos como objetivo la búsqueda de cuerpos finitos de cardinal cualquier potencia de la característica del subcuerpo primo.

Lema 2.4. *Dados F un cuerpo finito de q elementos y K un subcuerpo suyo, entonces el polinomio $x^q - x \in K[x]$ se descompone en F de la forma*

$$x^q - x = \prod_{a \in F} (x - a)$$

y F es el cuerpo de descomposición de dicho polinomio sobre K

Demostración. Veamos primero que todo elemento $a \in F$ anula ese polinomio, es decir, $a^q - a = 0$.

- Para $a = 0$ es trivial
- Sea $a \neq 0$. Los elementos no nulos de F forman un grupo multiplicativo de orden $q - 1$, de forma que $a^{q-1} = 1$ y $a^q = a$.

Hemos demostrado que todo elemento de F es raíz de $x^q - x$. Además, como un polinomio solo puede tener tantas raíces (sobre un cuerpo de descomposición) como su grado, tenemos que las q raíces de $x^q - x$ son los q elementos de F.

□

Teorema 2.5 (Existencia y unicidad de cuerpos finitos)**.** *Dados un primo p y un entero positivo n, existe un cuerpo finito de cardinal $q = p^n$, y todo cuerpo finito de ese cardinal es isomorfo al cuerpo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$*

Demostración. Vamos a demostrar por separado la existencia y la unicidad:

- (Existencia) Consideramos el polinomio $x^q - x$ y denotamos F su cuerpo de descomposición sobre $\mathbb{F}_p$. La derivada del polinomio es $qx^{q-1} - 1$. Como p divide a q, esto es igual a $-1 \neq 0$, ergo no hay raíces múltiples. Definimos $S = \{a \in F \quad | \quad a^q - a = 0\}$. Trivialmente, $x^q - x$ se descompone en S. Además, $0, 1 \in S$. Veremos que S es subcuerpo de F. Sean $a, b \in S$:

  - $(a - b)^q = a^q - b^q = a - b$. Por ende $a - b \in S$.
  - $(ab^{-1})^q = a(b^q)^{-1} = ab^{-1}$. Por ende $ab^{-1} \in S$.

  Entonces S es un subcuerpo de F. Por definición, F es el menor cuerpo en el que $x^q - x$ se descompone. Por tanto $S = F$. Además, S tiene q elementos (raíces de $x^q - x$). Deducimos que $|F| = q$.

- (Unicidad) Sea F cuerpo de q elementos. Sabemos que su característica es p y tiene subcuerpo primo $\mathbb{F}_p$. Por el lema anterior, F es un cuerpo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$. Como los cuerpos de descomposición son únicos salvo isomorfismo, el resultado queda demostrado. □

Hemos visto que tiene sentido considerar la notación $\mathbb{F}_q$ siendo q de la forma $q = p^n$ la potencia n-ésima de algún número primo p. Mantendremos esta notación a lo largo del capítulo.

Una vez caracterizados los cuerpos finitos, pasamos a estudiar su estructura viendo sus subcuerpos, estructuras cíclicas y extensiones algebraicas (finitas).

Teorema 2.6. *Sea $q = p^n$. Entonces para cada m divisor de n existe un único subcuerpo de $\mathbb{F}_q$ de orden p^m, y estos son todos los subcuerpos de $\mathbb{F}_q$.*

Demostración. Si $m|n$, entonces $(p^m - 1)|(q - 1)$. Por tanto, $(x^{p^m-1} - 1)|(x^{q-1} - 1)$ y como consecuencia inmediata $(x^{p^m} - x)|(x^q - x)$ (todo esto en $\mathbb{F}_p[x]$). Deducimos que el conjunto de raíces de $x^{p^m} - x$ (que constituye el cuerpo de descomposición de dicho polinomio) está contenido en $\mathbb{F}_q$, con lo que tenemos la existencia de un subcuerpo. La unicidad se deduce de que si hubiera otro, y existiera un elemento fuera de la intersección de ambos, el número de raíces de $x^{p^m} - x$ excedería p^m.

Para finalizar, basta ver que los subcuerpos de $\mathbb{F}_q$ tienen trivialmente orden p^m para algún m divisor de n por su comportamiento como espacios vectoriales. □

A continuación, vamos a ver un resultado de gran importancia y al que recurriremos en diferentes contextos a lo largo del trabajo:

Teorema 2.7. *Para todo cuerpo finito $\mathbb{F}_q$, el grupo multiplicativo $\mathbb{F}_q^*$ es cíclico.*

Demostración. Podemos suponer que $q \geqslant 3$.
Sea $p_1^{r_1} \dots p_m^{r_m}$ la factorización de $h = q - 1$. Para $1 \leqslant i \leqslant m$, el polinomio $x^{h/p_i} - 1$ tiene a lo sumo h/p_i raíces en $\mathbb{F}_q$. Como $h/p_i < h$, existe al menos un elemento no nulo de $\mathbb{F}_q$, denotado a_i, que no es raíz de $x^{h/p_i} - 1$. Si denotamos $b_i = a_i^{h/p_i^{r_i}}$, tenemos que $(b_i)^{p_i^{r_i}} = a_i^h = 1$. Por tanto, el orden de b_i es un divisor de $p_i^{r_i}$. Denotamos el orden de b_i por $p_i^{s_i}$, para un cierto $s_i \leqslant r_i$. Claramente $s_i = r_i$, pues $(b_i)^{p_i^{r_i-1}-} = a_i^{h/p_i}$ que es distinto de 1 por como se han elegido los a_i.

Definimos ahora el elemento $b = b_1 \dots b_m$. Veamos que tiene orden h.
Si el orden de b fuera algún divisor propio de h, este dividiría a h/p_i para algún i. Podemos suponer que divide al primero de ellos, h/p_1. Entonces, $1 = b^{h/p_1} = b_1^{h/p_1} \dots b_m^{h/p_1}$
Pero sabemos que $p_i^{r_i} | (h/p_1)$ para todo i tal que $2 \leqslant i \leqslant m$, por lo que $b_i^{h/p_1} = 1$ en dichos casos. Se deduce que $b_1^{h/p_1} = 1$ y el orden de b_1 divide a h/p_1, pero esto es imposible porque $p_1^{r_1} \nmid (h/p_1)$. En conclusión, el elemento b tiene orden $h = q - 1$ y por tanto b genera a $\mathbb{F}_q^*$. □

Definición 2.8. *Los generadores de $\mathbb{F}_q^*$ como grupo cíclico se denominan* ***elementos primitivos*** *de $\mathbb{F}_q$ (o de $\mathbb{F}_q^*$).*

Los elementos primitivos nos proporcionan una forma inmediata de ver que todo cuerpo finito se puede estudiar como extensión algebraica de cualquiera de sus subcuerpos, tomando como generador de la extensión cualquier elemento primitivo.

Teorema 2.9. *Sean $\mathbb{F}_q$ un cuerpo finito y $\mathbb{F}_r$ una extensión finita suya. Entonces $\mathbb{F}_r$ es una extensión simple algebraica de $\mathbb{F}_q$, donde cada elemento primitivo de $\mathbb{F}_r$ es un generador de la extensión.*

Demostración. La prueba es trivial. Si α es un elemento primitivo de $\mathbb{F}_r$, entonces $\mathbb{F}_q[\alpha] \subset \mathbb{F}_r$. Además $\mathbb{F}_q[\alpha]$ está trivialmente contenido en la unión del conjunto $\{0\}$ y el grupo multiplicativo generado por α, que equivale a $\{0\} \cup \mathbb{F}_r^*$, es decir, $\mathbb{F}_r$. □

Como las extensiones son simples y algebraicas, van acompañadas de un polinomio mínimo, lo que justifica la existencia de polinomios irreducibles de cualquier grado en cada cuerpo finito.

Corolario 2.10. *Para cada cuerpo finito $\mathbb{F}_q$ y cada entero positivo n, existe un polinomio irreducible de grado n en $\mathbb{F}_q[x]$*

Demostración. Tomamos $\mathbb{F}_r$ el cuerpo de orden q^n, extensión de grado n de $\mathbb{F}_q$, y $\alpha \in \mathbb{F}_r$ tal que $\mathbb{F}_q[\alpha] = \mathbb{F}_r$. Entonces el polinomio mínimo de α sobre $\mathbb{F}_q$ es un polinimio irreducible de grado n. □

2.2. Polinomios y extensiones de cuerpos finitos

Durante el resto del capítulo veremos resultados sobre polinomios irreducibles que nos permitirán estudiar el orden del grupo de Galois de las extensiones y algunas propiedades de los operadores norma y traza y de los polinomios primitivos.

Introducimos un par de lemas, que se encuentran en [11, p. 48] y [11, p. 49] respectivamente.

Lema 2.11. *Si α es una raíz del polinomio irreducible $f \in \mathbb{F}_q[x]$, entonces un polinomio $h \in \mathbb{F}_q[x]$ verifica $h(\alpha) = 0$ si y solo si f divide a h.* □

Lema 2.12. *Si $f \in \mathbb{F}_q[x]$ es un polinomio irreducible de grado m, entonces m divide a n si y solo si f divide a $x^{q^n} - x$.* □

Con estas propiedades podemos calcular todas las raíces de un polinomio irreducible a partir de cualquiera de ellas.

Teorema 2.13. *Si f es un polinomio irreducible en $\mathbb{F}_q[x]$ de grado m, entonces f tiene una raíz α en $\mathbb{F}_{q^m}$. Además, f tiene m raíces simples en $\mathbb{F}_{q^m}$, las cuales son α^{q^i}, para $0 \leqslant i < m$.*

Demostración. Si tomamos α en el correspondiente cuerpo de descomposición de f, tenemos que $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ y por ende $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Veamos ahora que α^q también es raíz de $f(x) = x^m + a_{n-1}x^{n-1} + \cdots + a_0$:

$$f(\alpha^q) = \alpha^{mq} + a_{n-1}\alpha^{(n-1)q} + \cdots + a_0 =$$

$$= (\alpha^m + a_{n-1}\alpha^{(n-1)} + \cdots + a_0)^q = 0$$

Entonces α^{q^i} es una raíz de f para $0 \leqslant i < m$. Falta ver que son distintas entre sí. Supongamos $\alpha^{q^j} = \alpha^{q^k}$ con $0 \leqslant j < k < m$. Entonces

$$\alpha^{q^{m+j-k}} = (\alpha^{q^j})^{q^{m-k}} = (\alpha^{q^k})^{q^{m-k}} = \alpha^m = \alpha$$

Por el Lema 2.11, $f|(x^{q^{m+j-k}} - x)$. Aplicando el Lema 2.12, tenemos que $m|(m + j - k)$. Hemos supuesto que $k > j$, ergo $m > m + j - k$, lo que nos lleva a una contradicción. □

Como corolario, podemos caracterizar los cuerpos de descomposición de los polinomios irreducibles sobre los cuerpos finitos según su grado.

Corolario 2.14. *Si f es un polinomio irreducible de grado m sobre $\mathbb{F}_q[x]$, entonces su cuerpo de descomposición es $\mathbb{F}_{q^m}$.*

Corolario 2.15. *Dos polinomios irreducibles del mismo grado en $\mathbb{F}_q[x]$ tienen cuerpos de descomposición isomorfos.*

En el Teorema 2.13 hemos visto que, dada α una raíz de un polinomio irreducible de grado m en $\mathbb{F}_q[x]$, las sucesivas potencias q-ésimas de α son todas las raíces simples de f, y se encuentran en el cuerpo $\mathbb{F}_{q^m}$. Decimos que las raíces están relacionadas por conjugación, o que son conjugadas unas de otras.

Definición 2.16. *Sea $\mathbb{F}_q$ un cuerpo finito y sean $\mathbb{F}_{q^m}$ una extensión suya y un elemento cualquiera $\alpha \in \mathbb{F}_{q^m}$. Para cada $0 \leqslant i < m$, decimos que α^{q^i} es un **conjugado** de α respecto de $\mathbb{F}_q$.*

La estructura cíclica de los grupos $\mathbb{F}_q^*$ nos facilita ver que los órdenes de los elementos de $\mathbb{F}_q^*$ se conservan por conjugación. Esto es debido a que $q^m - 1$ y q son coprimos cuando $q = p^n$ para algún primo p. Tenemos el siguiente resultado:

Teorema 2.17. *Los conjugados de cualquier elemento primitivo de $\mathbb{F}_q^*$ respecto de cualquier subcuerpo suyo son también primitivos.*

Para finalizar esta parte, veremos que la conjugación es precisamente lo que da lugar a los automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ y, de forma intuitiva, estos se diferencian exclusivamente por su acción sobre los elementos primitivos:

Teorema 2.18. *Los únicos automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ son las aplicaciones dadas por $\sigma_i(\alpha) = \alpha^{q^i}$, con $0 \leqslant i \leqslant m-1$, para cada $\alpha \in \mathbb{F}_{q^m}$.*

Demostración. Veamos que los σ_i son automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. La propiedad de homomorfismo es inmediata de comprobar, ergo tenemos que σ_i es un endomorfismo. Además es inyectivo, pues el único elemento con imagen nula es trivialmente el 0. Por estar definido en un conjunto finito y ser un endomorfismo inyectivo, tenemos que es biyectivo, y un automorfismo de $\mathbb{F}_{q^m}$. Por último, como $\alpha^q = \alpha, \forall \alpha \in \mathbb{F}_q$, entonces $\sigma_i(\alpha) = \alpha$ para cada $\alpha \in \mathbb{F}_q$, y tenemos un automorfismo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$.

Como consecuencia del Teorema 2.13, los σ_i son distintos entre sí, pues tienen imágenes distintas sobre los elementos primitivos de $\mathbb{F}_{q^m}$.

Terminemos viendo que son los únicos automorfismos posibles. Sean σ un automorfismo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ y β elemento primitivo de $\mathbb{F}_{q^m}$. Definimos el polinomio mínimo de β sobre $\mathbb{F}_q$, $f(x) = x^m + a_{n-1}x^{n-1} + \cdots + a_0$.
Por tanto

$$\begin{aligned} 0 &= \sigma(\beta^m + a_{n-1}\beta^{n-1} + \cdots + a_0) = \\ &= \sigma(\beta)^m + a_{n-1}\sigma(\beta)^{n-1} + \cdots + a_0 \end{aligned}$$

Tenemos que $\sigma(\beta)$ es una raíz de f. Por el Teorema 2.13, $\sigma(\beta) = \beta^{q^j}$ para algún j entre 0 y $m-1$. Por ser β primitivo, el automorfismo σ queda completamente determinado y es de la forma buscada. □

Tenemos definidos todos los automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ y por tanto su grupo de Galois.

2.3. Norma y traza

En esta parte consideraremos $K = \mathbb{F}_q$, una extensión cualquiera suya $F = \mathbb{F}_{q^m}$ y $\alpha \in F$. Tenemos que el polinomio mínimo de α es $f \in K[x]$ de grado d divisor de m.

Definición 2.19 (Polinomio característico)**.** *Definimos el* ***polinomio característico*** *de α sobre K como $g = f^{m/d} \in K[x]$.*

Si las raíces de f son $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$, podemos considerar también como expresión del polinomio característico

$$g(x) = x^m + a_{m-1}x^{n-1} + \cdots + a_0 = (x-\alpha)(x-\alpha^q)\ldots(x-\alpha^{q^{m-1}})$$

Definición 2.20. *Definimos la* ***traza*** *de α sobre K, $Tr_{F/K}(\alpha)$ como*

$$Tr_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}$$

La traza se puede caracterizar según el polinomio característico, de forma que

$$\mathrm{Tr}_{F/K}(\alpha) = -a_{m-1} \in K$$

Veamos algunas propiedades del operador traza:

Propiedades 2.21.

- *$Tr_{F/K}$ es una aplicación lineal de F hacia K.*
- *Para cada $a \in K$, se tiene que $Tr_{F/K}(a) = ma$.*
- *Para cada $\alpha \in F$, se tiene que $Tr_{F/K}(\alpha^q) = Tr_{F/K}(\alpha)$.*
- *Si E es una extensión finita de F, entonces $Tr_{E/K}(\alpha) = Tr_{F/K}(Tr_{E/F}(\alpha))$, para todo $\alpha \in E$.*

Definición 2.22. *Definimos la* ***norma*** *de α sobre K, $N_{F/K}(\alpha)$, como*

$$N_{F/K}(\alpha) = \alpha.\alpha^q \ldots \alpha^{q^{m-1}} = \alpha^{(q^m-1)/(q-1)}$$

Podemos caracterizar la norma a través de g el polinomio característico de α, de forma que

$$\mathrm{N}_{F/K}(\alpha) = (-1)^m a_0 \in K$$

Para finalizar, veamos algunas propiedes de la norma.

Propiedades 2.23.

- $N_{F/K}(\alpha\beta) = N_{F/K}(\alpha)N_{F/K}(\beta)$, *para todo* $\alpha, \beta \in F$.
- $N_{F/K}$ *lleva elementos no nulos de* F *a elementos no nulos de* K.
- $N_{F/K}(a) = a^m$, *para todo* $a \in K$.
- $N_{F/K}(\alpha^q) = N_{F/K}(\alpha)$, *para todo* $\alpha \in F$.
- *Si* E *es una extensión finita de* F, *entonces* $N_{E/K}(\alpha) = N_{F/K}(N_{E/F}(\alpha))$, *para todo* $\alpha \in E$.

Capítulo 3

Bases sobre cuerpos finitos

A la hora de trabajar sobre un cuerpo finito, es necesario tomar una base adecuada para las operaciones que se realicen sobre este. Si no se requieren operaciones complejas, es apropiado tomar la base más sencilla posible de calcular, la llamada base polinomial, dada por las potencias sucesivas $\{1, \alpha, \alpha^2 \ldots, \alpha^{n-1}\}$ de la raíz α de un polinomio irreducible de grado n. Pero esto no siempre es el caso. Un ejemplo claro es el operador traza, cuyo cálculo podemos simplificar escogiendo una base autodual, un concepto análogo al de base ortogonal para un producto escalar que se utiliza en los cuerpos reales y complejos.

En este capítulo consideramos siempre bases de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, y queremos utilizar resultados de [3], [11] y [18]. Comenzamos viendo algunas propiedades generales de bases sobre cuerpos finitos, entre las que se encuentran dos caracterizaciones de las bases.

Definición 3.1. *Sea $\{\alpha_1, \ldots, \alpha_n\}$ un subconjunto de $\mathbb{F}_{q^n}$:*

- *Definimos la **representación matricial regular** (sobre $\mathbb{F}_q$) del subconjunto $\{\alpha_1, \ldots, \alpha_n\}$ como la matriz*

$$A = (\alpha_i^{q^{j-1}}) = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_n^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \cdots & \alpha_n^{q^{n-1}} \end{pmatrix} \tag{3.1}$$

- *Definimos el **discriminante** de $\{\alpha_1, \ldots, \alpha_n\}$ (sobre $\mathbb{F}_q$) como*

$$\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_0, \ldots, \alpha_n) = det \begin{pmatrix} Tr(\alpha_1\alpha_1) & Tr(\alpha_1\alpha_2) & \cdots & Tr(\alpha_1\alpha_n) \\ Tr(\alpha_2\alpha_1) & Tr(\alpha_2\alpha_2) & \cdots & Tr(\alpha_2\alpha_n) \\ \cdots & \cdots & \ddots & \cdots \\ Tr(\alpha_n\alpha_1) & Tr(\alpha_n\alpha_2) & \cdots & Tr(\alpha_n\alpha_n) \end{pmatrix} \tag{3.2}$$

Si no se dice de forma explícita lo contrario, se considera que Tr denota $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$, y lo mismo para Δ. Notemos que A^tA tiene el mismo valor que la matriz de trazas

con la que se calcula el discriminante en (3.2). Por esto, es inmediato que $\det(A^tA) = \det(A)^2 = \Delta(\alpha_1, \ldots, \alpha_n)$. Vamos a comprobar que, cuando estos determinantes son no nulos, entonces el subconjuto elegido es una base.

Teorema 3.2. *Sea $(\alpha_1, \ldots, \alpha_n)$ un subconjunto de $\mathbb{F}_{q^n}$. Entonces $\{\alpha_1, \ldots, \alpha_n\}$ es una base sobre $\mathbb{F}_q$ si y solo si $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$ y la representación matricial regular de $\{\alpha_1, \ldots, \alpha_n\}$ es no singular.*

Demostración. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base de $\mathbb{F}_{q^n}$. Supongamos que $\Delta(\alpha_1, \ldots, \alpha_n) = 0$. Entonces podemos realizar una combinación lineal de las columnas de la matriz de trazas con resultado nulo, de forma que para todo $1 \leqslant j \leqslant n$, tenemos que

$$c_1\mathrm{Tr}(\alpha_1\alpha_j) + c_2\mathrm{Tr}(\alpha_2\alpha_j) + \cdots + c_n\mathrm{Tr}(\alpha_n\alpha_j) = 0$$

para $c_1, \ldots, c_n$ elementos fijos de $\mathbb{F}_q$. Si denotamos

$$\beta = c_1\alpha_1 + \cdots + c_n\alpha_n$$

entonces $\mathrm{Tr}(\beta\alpha_j) = 0$ para todo j, por lo que podemos deducir que $\mathrm{Tr}(\beta\alpha) = 0$ para todo α en $\mathbb{F}_{q^n}$. Si β es no nulo, tenemos que todo elemento de $\mathbb{F}_{q^n}$ posee traza nula, es decir, $x^{q^{n-1}} + x^{q^{n-2}} + \cdots + x^q + x$ tiene q^n raíces, lo cual es absurdo. Por tanto $\beta = 0$ y $c_1 = c_2 = \ldots = c_n = 0$.

Sea ahora $\{\alpha_1, \ldots, \alpha_n\}$ un conjunto de discriminante no nulo, y supongamos que no es una base. Podemos tomar una combinación lineal nula suya, esto es, $c_1\alpha_1 + \cdots + c_n\alpha_n = 0$, de forma que algún $c_i \neq 0$. Entonces para todo $1 \leqslant j \leqslant n$, podemos multiplicar la expresión previa por α_j para obtener que $c_1\alpha_1\alpha_j + \cdots + c_n\alpha_n\alpha_j = 0$, y aplicando la traza, $c_1\mathrm{Tr}(\alpha_1\alpha_j) + \cdots + c_n\mathrm{Tr}(\alpha_n\alpha_j) = 0$. Hemos supuesto que el discriminante es no nulo, de lo que sigue que la matriz de trazas de la forma de (3.2) es no singular, por lo que la última igualdad falla para algún $1 \leqslant j \leqslant n$ si los c_i son no nulos. Deducimos que $c_i = 0$ para $1 \leqslant i \leqslant n$, lo que contradice la hipótesis, por lo que $\{\alpha_1, \ldots, \alpha_n\}$ es una base. □

Como parte de la demostración anterior, hemos visto que siempre existe al menos un elemento de traza no nula. En particular, como la traza es un operador lineal, tenemos que para todo elemento $a \in \mathbb{F}_q$ existe algún elemento $\alpha \in \mathbb{F}_{q^n}$ tal que $\mathrm{Tr}(\alpha) = a$: si $\mathrm{Tr}(\beta) = b \neq 0$, denotando $\alpha = ab^{-1}\beta$, tenemos que $\mathrm{Tr}(\alpha) = ab^{-1}\mathrm{Tr}(\beta) = a$.

Como corolario del teorema, podemos ver que una base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ puede serlo también sobre otra extensión de grado n que la contenga:

Corolario 3.3 (Lema del alzamiento de bases)**.** *Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Entonces, para todo k tal que $mcd(n, k) = 1$, se tiene que $\{\alpha_1, \ldots, \alpha_n\}$ es una base de $\mathbb{F}_{q^{kn}}$ sobre $\mathbb{F}_{q^k}$.*

Demostración. Consideramos la representación matricial regular de $\{\alpha_1, \ldots, \alpha_n\}$ en $\mathbb{F}_{q^{kn}}$ sobre $\mathbb{F}_{q^k}$. Esta es de la forma

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^{q^k} & \alpha_2^{q^k} & \cdots & \alpha_n^{q^k} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{q^{k(n-1)}} & \alpha_2^{q^{k(n-1)}} & \cdots & \alpha_n^{q^{k(n-1)}} \end{pmatrix}$$

Por hipótesis, $\mathrm{mcd}(n,k) = 1$, por lo que k genera los enteros módulo n, con lo que concluimos que la representación matricial regular obtenida es una permutación de las filas de la representación matricial regular en $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Sabemos por el Teorema 3.2 que esta matriz es no singular, por lo cual sus permutaciones tampoco. Para finalizar, como la representación matricial inicial es no singular, aplicando de nuevo el Teorema 3.2 obtenemos que $\{\alpha_1, \ldots, \alpha_n\}$ es una base de $\mathbb{F}_{q^{kn}}$ sobre $\mathbb{F}_{q^k}$. □

3.1. Bases duales

En esta parte introducimos el concepto de dualidad, sustituyendo los resultados en el plano complejo con el producto escalar por un análogo en extensiones de cuerpo finitos con la traza del producto. Esto se puede simplificar si la calculamos a través de la representación matricial de los elementos del producto. Comenzamos con la definición principal de la sección:

Definición 3.4. *Sean $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_n\}$ dos bases de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Diremos que son **bases duales** entre sí, o que $\{\alpha_1, \ldots, \alpha_n\}$ es una **base primal** con **base dual** $\{\beta_1, \ldots, \beta_n\}$, si verifican que, para todo $1 \leqslant i, j \leqslant n$, $Tr(\alpha_i\beta_j) = \delta_{i,j}$, o, expresándolo en forma matricial,*

$$(Tr(\alpha_i\beta_j))_{1\leqslant i,j,\leqslant n} = I_n$$

siendo I_n la matriz identidad de rango n.

A partir de esta parte vamos a obviar los subíndices al definir las matrices.
Ya habíamos dado en la sección anterior una forma de calcular la matriz de trazas a partir de la representación matricial regular. En este caso en el que las bases no coinciden, se hace de forma análoga, y es sencillo calcular que, dadas A la representación de la base $\{\alpha_1, \ldots, \alpha_n\}$ y B la de $\{\beta_1, \ldots, \beta_n\}$, se tiene que

$$(\mathrm{Tr}(\alpha_i\beta_j)) = A^t B$$

Esto nos sirve como apoyo para justificar que en la definición de bases duales digamos que una es *la* base dual de la otra, y no *una* base dual.

Teorema 3.5 (Existencia y unicidad del dual de una base)**.** *Toda base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ tiene una única base dual.*

Demostración. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base de $\mathbb{F}_{q^n}$. Sea T su matriz de trazas, que por el Teorema 3.2 es invertible. Denotamos $a_{i,j}$ los elementos de T y $b_{i,j}$ los elementos de T^{-1}.

Vamos a construir un conjunto de elementos $\{\beta_1, \ldots, \beta_n\}$, dados por

$$\beta_j = \sum_{k=1}^{n} b_{j,k}\alpha_k$$

de forma que

$$(\beta_1, \ldots, \beta_n)^t = T^{-1}(\alpha_1, \ldots, \alpha_n)^t$$

Claramente $\{\beta_1, \ldots, \beta_n\}$ es una base, por ser T^{-1} no singular. Si calculamos las trazas de los productos, obtenemos que

$$\mathrm{Tr}(\alpha_i\beta_j) = \sum_{k=1}^{n} b_{j,k}\mathrm{Tr}(\alpha_i\alpha_k) = \sum_{k=1}^{n} b_{j,k}a_{i,k} = \sum_{k=1}^{n} b_{j,k}a_{k,i}$$

lo que se corresponde con la fila j y columna i de la matriz $T^{-1}T = I_n$ (claramente $a_{i,k} = a_{k,i}$ por ser T una matriz simétrica). Por tanto, $\mathrm{Tr}(\alpha_i\beta_j) = \delta_{i,j}$.

La unicidad es sencilla de demostrar. Si tomamos A y B las representaciones matriciales regulares de $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_n\}$ respectivamente, recordamos que $(\mathrm{Tr}(\alpha_i\beta_j)) = A^tB$. Entonces $A^tB = I_n$ y $B = (A^t)^{-1}$. Por ser la inversa única, también lo es la representación matricial de $\{\beta_1, \ldots, \beta_n\}$ (y por ende, también $\{\beta_1, \ldots, \beta_n\}$). □

Como caso particular, vamos a proponer un método para calcular una base dual dada una base polinomial.

Corolario 3.6. *Sea $\{1, \alpha, \ldots, \alpha^{n-1}\}$ una base polinomial de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ y sea $f(x)$ el polinomio irreducible de α sobre $\mathbb{F}_q$. Denotamos $f(x) = (x-\alpha)(\gamma_0+\gamma_1 x+\cdots+\gamma_{n-1}x^{n-1})$. Entonces la base dual de $\{1, \alpha, \ldots, \alpha^{n-1}\}$ viene dada por el conjunto $\{\beta_0, \ldots, \beta_{n-1}\}$, de forma que*

$$\beta_i = \frac{\gamma_i}{f'(\alpha)}$$

Demostración. Consideramos para $0 \leqslant i \leqslant n-1$ el polinomio en $\mathbb{F}_{q^n}[x]$

$$g_i(x) = x^i - \sum_{j=0}^{n-1} \frac{\alpha^{iq^j} f(x)}{f'(\alpha^{q^j})(x-\alpha^{q^j})}$$

Veamos que tiene las mismas raíces que $f(x)$. Sea α^{q^k} una de ellas. Si $j \neq k$, entonces el j-ésimo término del sumatorio se anula, pues $\frac{f(x)}{x-\alpha^{q^j}}$ sigue teniendo a α^{q^k} como raíz. Nos fijamos en el k-ésimo término. Recordamos que $f'(x) = \sum_{j=1}^{n}\prod_{s\neq j}(x-\alpha^{q^s})$. Entonces tenemos que los términos del sumatorio de $f'(x)$ se anulan en α^{q^k} cuando $j \neq k$. Entonces

$$g_i(\alpha^{q^k}) = \alpha^{iq^k} - \alpha^{iq^k}\left(\left[\frac{f(x)}{(x-\alpha^{q^k})}\right](\alpha^{q^k})\frac{1}{\prod_{s\neq k}(\alpha-\alpha^{q^s})}\right) =$$

$$= \alpha^{q^k} - \alpha^{q^k}\frac{\prod_{s\neq k}(\alpha-\alpha^{q^s})}{\prod_{s\neq k}(\alpha-\alpha^{q^s})} = 0$$

Este polinomio es de grado estrictamente menor que n, y además tiene al menos n raíces distintas, por lo que es idénticamente nulo para cada $0 \leqslant i \leqslant n-1$.

Podemos expresar esto en función de la traza, de forma que

$$\mathrm{Tr}\left(\frac{\alpha^i f(x)}{f'(\alpha^q)(x-\alpha^q)}\right) = \mathrm{Tr}\left(\frac{\alpha^i}{f'(\alpha^q)}(\gamma_0+\gamma_1 x+\cdots+\gamma_{n-1}x^{n-1})\right) = \\ = \sum_{j=1}^{n} \mathrm{Tr}\left(\frac{\alpha^i}{f'(\alpha^q)}\gamma_j x^j\right) = x^i$$

Esta última igualdad es donde se utiliza que $g_i(x) = 0$ para todo i. Si comprobamos la dualidad de la base de potencias con la base tomada en la hipótesis, tenemos que

$$\mathrm{Tr}(\alpha^i\beta_j) = \mathrm{Tr}\left(\frac{\alpha^i}{f'(\alpha)}\gamma_j\right) = \delta_{i,j} \qquad \square$$

Notemos que si $f(x)$ es mónico, entonces $\gamma_{n-1} = 1$. Vamos a ver como ejemplo un par de bases duales de $\mathbb{F}_{2^4}$ sobre $\mathbb{F}_2$. Consideramos el polinomio irreducible sobre $\mathbb{F}_2$ $f(x) = x^4 + x + 1$, y *alpha* una raíz suya. Tenemos que

$$f(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8) = \\ = (x+\alpha)(\alpha^{14}+(\alpha^6+\alpha^{10}+\alpha^{12})x+(\alpha^2+\alpha^4+\alpha^8)x^2+x^3) = \\ = (x+\alpha)(\alpha^{-1}+([\alpha^3+\alpha^2]+[\alpha^2+\alpha+1]+[\alpha^3+\alpha^2+\alpha+1])x+ \\ +(\alpha^2+[\alpha+1]+[\alpha^2+1])x^2+x^3) = \\ = (x+\alpha)(\alpha^3+1+\alpha^2 x+\alpha x^2+x^3)$$

Tenemos que $f'(\alpha) = \alpha$ y $\alpha^{-1} = \alpha^3 + 1$, con lo que podemos calcular los elementos de la base dual $\{\beta_1, \beta_2, \beta_3, \beta_4\}$:

$$\beta_1 = \alpha^6 + 1 = \alpha^3 + \alpha^2 + 1, \quad \beta_2 = \alpha, \quad \beta_3 = 1, \quad \beta_4 = \alpha^3 + 1$$

El uso de bases duales destaca a la hora de calcular la traza de un producto. Consideramos $x, y \in \mathbb{F}_{q^n}$, y queremos calcular $\mathrm{Tr}(xy)$. Si consideramos las bases duales $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_n\}$ de forma que $x = \sum_{i=1}^n a_i\alpha_i$ y $y = \sum_{i=1}^n b_i\beta_i$, entonces para calcular la traza del producto solo hay que considerar los productos de coeficientes cuyos índices coincidan, es decir:

$$\mathrm{Tr}(xy) = \sum_{i,j=1}^{n} a_i b_j \mathrm{Tr}(\alpha_i\beta_j) = \sum_{i,j=1}^{n} a_i b_j \delta_{i,j} = \sum_{i=1}^{n} a_i b_i$$

Con un proceso similar a este podemos realizar cambios de coordenadas entre bases duales. Consideremos el mismo par de bases duales, y consideramos un elemento arbitrario de $\mathbb{F}_{q^n}$ como coordenadas en la base $\{\alpha_1, \ldots, \alpha_n\}$

$$x = \sum_{i=1}^{n} a_i\alpha_i$$

Entonces la expresión de x en la base $\{\beta_1, \ldots, \beta_n\}$ sería

$$x = \sum_{i=1}^{n} \mathrm{Tr}(x\alpha_i)\beta_i$$

En otras palabras, la coordenada de un elemento con respecto a la i-ésima componente de una base primal queda completamente determinada por la traza del producto de dicho elemento con la i-ésima componente de la base dual.

Si fuéramos capaces de obtener una base autodual, estas operaciones se simplificarían significativamente. No obstante, hay restricciones que reducen el tipo de cuerpos finitos sobre los que se puede tomar una tal base. Esto lo podemos ver en unos resultados de [18, p. 175-178]:

Teorema 3.7. *Existe una base autodual de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ si y solo si q es una potencia de 2 o n es impar.*

También tenemos restricciones adicionales sobre la dualidad de las bases polinómicas

Teorema 3.8. *No existen bases polinómicas autoduales de $\mathbb{F}_{q^n}$ para $n \geqslant 2$.*

Demostración. Si una tal base polinomial fuera autodual, entonces $\mathrm{Tr}(\alpha \cdot \alpha) = 1$, y además $\mathrm{Tr}(1 \cdot \alpha^2) = 0$, lo que es absurdo. □

No obstante, sí que somos capaces de conseguir bases duales tales que ambas sean polinómicas. Estas solo se pueden calcular para binomios irreducibles, de manera sencilla. Para ver esto, introduciremos un concepto más general que la dualidad: diremos que dos bases $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_n\}$ son traza-ortogonales si $\mathrm{Tr}(\alpha_i\beta_j) = 0$ para $i \neq j$ y $\mathrm{Tr}(\alpha_i\beta_j) \neq 0$ para $i = j$. Estamos en condiciones de entender el siguiente resultado de [5]:

Teorema 3.9. *Sea $\{1, \alpha, \ldots, \alpha^n\}$ una base polinomial primal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, y sea $f(x)$ el polinomio irreducible de α. Entonces su base dual es polinómica si y solo si $f(x)$ es de la forma $x^n - c \in \mathbb{F}_q[x]$ con $n \equiv 1 \pmod{p}$, siendo p la característica de $\mathbb{F}_q$. Además, $\{1, \alpha^{-1}, \ldots, \alpha^{-(n-1)}\}$ es una base polinomial que es traza-ortogonal a la base primal.*

3.2. Bases normales

Vamos a ver otro tipo particular de bases formadas por elementos conjugados de la extensión, las bases normales. El estudio de estas bases está motivado por su eficiencia computacional en problemas de factorización y de logaritmo discreto. Comenzamos viendo su definición formal:

Definición 3.10. *Decimos que una base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ es **normal** si es de la forma $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ para algún $\alpha \in \mathbb{F}_q$.*

Para probar la existencia de bases normales en cuerpos finitos arbitrarios, necesitamos algunos resultados previos. El siguiente lema se puede encontrar en [11, p. 56]:

Lema 3.11. *[Lema de Artin] Sean G un grupo y F un cuerpo, y sean $\psi_1, \ldots, \psi_n$ n homomorfismos distintos de G en el grupo multiplicativo F^*. Si $a_1, \ldots, a_n$ son n elementos de F con alguno de ellos no nulo, entonces existe algún $g \in G$ tal que*

$$a_1\psi_1(g) + \cdots + a_n\psi_n(g) \neq 0$$

Recordamos además algunos conceptos de los operadores lineales sobre espacios vectoriales de dimensión finita. Decimos que un operador A sobre el F-espacio vectorial K de dimensión n tiene polinomio mínimo $f(x)$ si este es el polinomio mónico de menor grado tal que $f(A) \equiv 0$, esto es, $f(A)$ es idénticamente nulo como operador.
Definimos además el polinomio característico de A como el polinomio $g(x) = \det(xI_n - A)$. Nos será útil la siguiente propiedad de álgebra lineal:

Lema 3.12. *Sea V un espacio vectorial de dimensión finita n y sea A un operador lineal en V. Entonces el polinomio característico de A coincide con su polinomio mínimo si y solo si existe un elemento $\alpha \in V$ tal que $\{\alpha, A\alpha, A^2\alpha, \ldots, A^{n-1}\alpha\}$ genera a V.*

Un hecho a tener en cuenta es que el polinomio mínimo de un operador lineal divide a su polinomio característico. Con esto en mente, y considerando los lemas anteriores, ya podemos demostrar la existencia de bases normales:

Teorema 3.13 (Teorema de la base normal)**.** *Para todo cuerpo finito $\mathbb{F}_q$ y para todo natural n, existe una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

Demostración. Por el Teorema 2.18, tenemos que los automorfismos de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ vienen dados por $\sigma_i(\alpha) = \sigma^i(\alpha) = \alpha^{q^i}$ para algún $0 \leqslant i \leqslant n-1$. Es evidente que $\sigma^n = \mathrm{id}_{\mathbb{F}_{q^n}}$, por lo que el polinomio mínimo de la forma lineal σ divide a $x^n - 1$. Además, si consideramos el polinomio $a_1 + a_2x + \cdots + a_nx^{n-1}$ para n elementos $a_1, \ldots, a_n \in \mathbb{F}_q$ cualesquiera, tenemos por el Lema 3.11 que σ no anula a este polinomio (pues no se anula para algún $\sigma(g)$ con $g \in \mathbb{F}_q^n$), con lo que deducimos que el polinomio mínimo de σ es de grado estrictamente mayor que $n-1$, y en consecuencia este es $x^n - 1$. Es más, como el polinomio caracterísro de la forma lineal σ tiene grado n y además es divisible por el polinomio mínimo de σ, deducimos que este también es $x^n - 1$. Para finalizar, por el Lema 3.12 podemos tomar un elemento α de $\mathbb{F}_{q^n}$ cuya órbita por σ genere $\mathbb{F}_{q^n}$, es decir, α genera una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. □

Somos capaces de afinar todavía más el resultado anterior y tomar una base normal generada por un elemento primitivo de $\mathbb{F}_{q^n}$. Además, como $\mathrm{mcd}(q, q^n - 1) = 1$, todos los elementos de dicha base serían a su vez primitivos. Este resultado fue demostrado por H. W. Lenstra y R. J. Schoof en [10]:

Teorema 3.14. *Para todo cuerpo finito $\mathbb{F}_q$ y para todo natural n, existe una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ formada por elementos primitivos.*

Para comprobar que un elemento α genera una base normal, podemos utilizar el Teorema 3.2 y calcular el determinante de la representación matricial de la base $\{\alpha_1, \ldots, \alpha_n\}$ dada por $\alpha_i = \alpha^{q^{i-1}}$ para $1 \leqslant i \leqslant n$. Sin embargo, en el caso particular en el que n es una potencia de la característica del cuerpo, podemos utilizar el siguiente teorema de [18, p. 186] para evitar el cálculo del determinante:

Teorema 3.15. *Sea α un elemento de $\mathbb{F}_{q^n}$ y $n = p^e$ siendo p la característica de $\mathbb{F}_q$. Entonces α genera una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ si y solo si $Tr(\alpha) \neq 0$.*

Vamos a terminar el capítulo añadiendo algunos resultados sobre bases normales duales.

Teorema 3.16. *La base dual de una base normal es también normal.*

Demostración. Sean A y B las representaciones matriciales regulares de una base normal y de su base dual respectivamente. La matriz de trazas viene dada por A^tB, y esta es la identidad por ser duales entre sí. Claramente la representación matricial de una base es una matriz simétrica si y solo si dicha base es normal. Como $A = A^t$ y $B = (A^t)^{-1}$, es evidente que $B = B^t$, por lo que es una matriz simétrica y por tanto la representación matricial de una base normal. □

Por último, aunque sea relativamente compleja de calcular, en [5] tenemos una condición necesaria y suficiente bajo la cual una base normal resulta ser autodual:

Teorema 3.17. *Sean $\{\alpha_1, \ldots, \alpha_n\}$ una base primal normal generada por $\alpha \in \mathbb{F}_{q^n}$ y $\{\beta_1, \ldots, \beta_n\}$ su base normal dual, y sea la matriz $G = (Tr(\alpha_1\alpha_i\beta_j))$. Entonces la base primal es autodual si y solo si G es una matriz simétrica y $Tr(\alpha^2) = 1$.*

Capítulo 4

Polinomios primitivos

En esta parte, recordamos el concepto de primitividad ya visto para los elementos de un cuerpo finito $\mathbb{F}_{q^m}$ y lo extenderemos a los polinomios en $\mathbb{F}_q[x]$ de grado m para los que sean raíces. Nos será útil relacionar el orden de un elemento con el mínimo exponente e para el que su polinomio irreducible divida a $x^e - 1$.

4.1. Orden de polinomios

Sabemos que un polinomio irreducible f de grado m en $\mathbb{F}_q[x]$ divide a $x^{q^m} - x$ (Lema 2.12). Si suponemos que $f(0) \neq 0$, tenemos que f divide a $x^{q^m-1} - 1$. Necesariamente existe un exponente mínimo e para el que f divide a $x^e - 1$, lo que nos servirá de base para desarrollar el concepto de orden de un polinomio.

Definición 4.1. *Sea $f \in \mathbb{F}_q[x]$ un polinomio no nulo. Si $f(0) \neq 0$, llamaremos **orden** de f (ord(f)) al menor entero positivo e tal que $f|x^e - 1$. Si $f(0) = 0$, descomponemos f de forma que $f(x) = x^r g(x)$ y $g(0) \neq 0$, en cuyo caso ord(f) =ord(g).*

Vamos a justificar esta definición de forma más rigurosa mediante el siguiente resultado:

Lema 4.2. *Sea $f \in \mathbb{F}_q[x]$ de grado $m \geqslant 1$ y $f(0) \neq 0$. Entonces existe un entero positivo $e \leqslant q^m - 1$ de forma que $f(x)|(x^e - 1)$*

Demostración. El cociente $\mathbb{F}_q[x]/(f)$ contiene $q^m - 1$ clases no nulas. Por tanto, entre las q^m clases de elementos $x^i + (f), 0 \leqslant i \leqslant q^m - 1$, por el principio del palomar, tiene que existir al menos un par de clases x^r y x^s, $0 \leqslant r < s \leqslant q^m - 1$, de forma que $x^r \equiv x^s$ (mód f). Como $f(0) \neq 0$, entonces f y x son relativamente primos, por lo que $x^{s-r} \equiv 1$ (mód f), es decir, $f|(x^{s-r} - 1)$. □

Alternativamente, se puede caracterizar el orden de un polinomio irreducible a partir del orden de sus raíces:

Teorema 4.3. *Sea $f \in \mathbb{F}_q[x]$ polinomio irreducible de grado m y tal que $f(0) \neq 0$. Entonces ord(f) es el orden de cualquiera de sus raíces en $\mathbb{F}_{q^m}$.*

Demostración. Sea α una raíz de f. Por el Lema 2.11 sabemos que $\alpha^e = 1$ si y solo si $f|(x^e - 1)$. El resultado queda probado al recordar que todas las raíces de un polinomio irreducible tienen el mismo orden en $\mathbb{F}_{q^m}$. □

Como corolario inmediato, dado que el orden de todo subgrupo divide al orden del grupo en el que está contenido, tenemos:

Corolario 4.4. *Si $f \in \mathbb{F}_q[x]$ es un polinomio irreducible de grado m, entonces ord$(f)|(q^m - 1)$.*

El orden (e) de un polinomio f puede entenderse también como el menor polinomio ciclotómico Φ_e para el cual $f|\Phi_e$, pues todas las raíces de f son de orden e, y es precisamente el total de elementos de orden e lo que forma las raíces de Φ_e. Si utilizamos [11, Teorema 2.47], obtenemos que el número de factores irreducibles de orden m de Φ_e es $\phi(e)/m$ (siendo ϕ la función fi de Euler). Profundizaremos en este tema en el capítulo 7.

Estamos en condiciones de calcular el número de polinomios irreducibles de un cierto orden en un cuerpo finito, como se demuestra en [11, Teorema 3.5].

Teorema 4.5. *Si $e \geqslant 2$ y m es el orden multiplicativo de q (mód e), entonces existen $\phi(e)/m$ polinomios irreducibles mónicos de grado m y orden e en $\mathbb{F}_q[x]$.*
Si $e = m = 1$ existen 2. En cualquier otro caso, no existe ninguno.
En particular, el grado de un polinomio irreducible de orden e en $\mathbb{F}_q[x]$ es el orden multiplicativo de q (mód e).

Vamos a intentar obtener el orden de cualquier tipo de polinomio, empezando por el caso de potencias de polinomios irreducibles y después productos de irreducibles coprimos entre sí.

Lema 4.6. *Si d es un entero positivo, entonces un polinomio $f \in \mathbb{F}_q[x]$ con $f(0) \neq 0$ divide a $x^d - 1$ si y solo si ord(f) divide a d.*

Demostración. Si $e =$ord(f) divide a d, entonces $f|(x^e - 1)$ y $(x^e - 1)|(x^d - 1)$.
Recíprocamente, si $f|(x^d - 1)$, entonces $d \geqslant e$ y mediante división entera de d por e obtenemos $d = me + r$ para algún $r < e$, de forma que $(x^d - 1) = (x^{me} - 1)x^r + (x^r - 1)$, y dado que $f|(x^{me} - 1)$ concluimos que $f|(x^r - 1)$. Esto lleva a contradicción, ergo $r = 0$. □

Este lema es de vital importancia para dar restricciones sobre el orden de polinomios no irreducibles. En particular, lo usaremos para los casos de potencia de único polinomio

irreducible y de producto de polinomios irreducibles coprimos entre sí. Una vez vistos estos casos, veremos también que podemos considerar el caso de un polinomio cualquiera.

Teorema 4.7. *Sean $g \in \mathbb{F}_q[x]$ un polinomio irreducible con $g(0) \neq 0$, $ord(g) = e$ y $p = car(\mathbb{F}_q)$. Si $f = g^b$ para $b \in \mathbb{N}$ y t es el menor entero positivo que cumple $p^t \geqslant b$, entonces $ord(f) = ep^t$.*

Demostración. Denotamos $c = \text{ord}(f)$. Viendo que $g|f$ y $f|(x^c - 1)$, por el Lema 4.6 tenemos que $e|c$. Además, $f|(x^e - 1)^b$ y $(x^e - 1)^b|(x^e - 1)^{p^t} = x^{ep^t} - 1$. De nuevo por el Lema 4.6, $c|ep^t$. Tenemos que $c = ep^u$ para algún $u \leqslant t$, pues por el Corolario 4.4, sabemos que $p \nmid e$, y además $x^e - 1$ tiene solo raíces simples. Deducimos que $x^{ep^u} - 1$ tiene todas sus raíces de multiplicidad p^u. Como $g^b|(x^{ep^u} - 1)$, como las raíces de g^b son de multiplicidad b, deducimos que $b \leqslant p^u$ y por definición de t, tenemos que $u \geqslant t$. □

Teorema 4.8. *Sean $g_1, \ldots, g_k$ polinomios irreducibles (no nulos) en $\mathbb{F}_q[x]$ coprimos entre sí y de órdenes respectivos $e_i, 1 \leqslant i \leqslant k$. Si $f = g_1 \ldots g_k$, entonces $ord(f) = e_1 \ldots e_k$.*

Demostración. Sin perder generalidad suponemos que $g_i(0) \neq 0$ para todo i. Denotamos $e = \text{ord}(f)$ y $c = \text{mcm}(e_1, \ldots, e_k)$. Cada g_i divide a $x^{e_i} - 1$ y a $x^c - 1$. Por coprimalidad de los g_i, obtenemos que f divide a $x^c - 1$. Por el Lema 4.6, $e|c$ y tanto f como cada g_i divide a $x^e - 1$. Aplicando de nuevo 4.6, tenemos que cada $e_i|e$, por lo que $c|e$ □

Durante la demostración del teorema anterior, no es necesario utilizar que los g_i sean irreducibles, basta con que sean coprimos. Por tanto, podemos entonces obtener sin mucha dificultad el resultado buscado para el caso general:

Teorema 4.9 (Orden de un polinomio)**.** *Sean $\mathbb{F}_q$ cuerpo finito de característica p, y f un polinomio en $\mathbb{F}_q[x]$ con factorización en producto de polinomios irreducibles mónicos $f = ag_1^{b_1} \ldots g_k^{b_k}$, para algún $a \in \mathbb{F}_q$.*
Entonces $ord(f) = ep^t$, donde $e = mcm(ord(g_1), \ldots, ord(g_k))$ y t es el menor entero positivo tal que $p^t \geqslant max(b_1, \ldots, b_k)$

Procederemos a calcular los órdenes de algunas transformaciones algebraicas simples, siendo la primera de ellas el polinomio recíproco, que introduciremos a continuación.

Definición 4.10. *Sea*

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{F}_q[x]$$

Se define el ***polinomio recíproco*** *de f como*

$$f^*(x) = a_0 x^n + \cdots + a_n = x^n f(\tfrac{1}{x})$$

Básicamente, el polinomio recíproco (de uno dado) es aquel en el que se invierte el orden de sus coeficientes. Calculamos ahora su orden:

Teorema 4.11. *Sea $f \in \mathbb{F}_q[x]$ un polinomio no nulo. Entonces ord(f) = ord(f^*).*

Demostración.

- (Caso $f(0) \neq 0$). Por el Lema 2.11, tenemos que $f|(x^e - 1)$ (para algún e) si y solo si $f^*|(x^e - 1)$: si α es una raíz de f que verifica $\alpha^e = 1$, entonces $(\alpha^{-1})^e = (\alpha^e)^{-1} = 1$, siendo α^{-1} una raíz de f^*.
- (Caso $f(0) = 0$) Sea $f(x) = x^r g(x)$ con $g(0) \neq 0$. Entonces $\text{ord}(f) = \text{ord}(g) = \\ = \text{ord}(g^*)$. Como $g^* = f^*$, hemos terminado. □

La siguiente transformación está dada por el cambio de la variable x a la variable $-x$ [11, p. 81]. Nótese que esta transformación no es relevante en cuerpos de característica 2.

Teorema 4.12. *Sean q una potencia de primo impar y $f \in \mathbb{F}_q[x]$ tal que $f(0) \neq 0$. Sean e el orden de $f(x)$ y E el orden de $f(-x)$.*

- *Si $e \equiv 0 \pmod 4$, entonces $E = e$*
- *Si e es impar, entonces $E = 2e$*
- *Si $e \equiv 2 \pmod 4$ y todos los factores irreducibles de f tienen orden par, entonces $E = e/2$.*
  En otro caso, tenemos que $E = e$.

4.2. Primitividad

En esta sección, vamos a definir y caracterizar el concepto de primitividad aplicado a los polinomios, utilizando su orden.

Definición 4.13. *Diremos que un polinomio $f \in \mathbb{F}_q[x]$ de grado m es **primitivo** sobre $\mathbb{F}_q$ si es el polinomio mínimo (por tanto irreducible) de un elemento primitivo de $\mathbb{F}_{q^m}$.*

Los polinomios primitivos de grado n nos permiten clasificar los elementos primitivos, agrupándolos de n en n mediante la relación de conjugación. Que los elementos de esta agrupación son distintos es evidente por este lema:

Lema 4.14. *Si $f \in \mathbb{F}_q[x]$ es un polinomio primitivo de grado n, entonces f tiene n raíces distintas*

Demostración. Por el Teorema 2.13, las raíces de un polinomio primitivo de grado n son los n conjugados de alguna de sus raíces, α. A su vez, estas raíces son distintas. □

Dado un entero positivo m, sabemos que en el grupo cíclico de orden m hay exactamente $\phi(m)$ elementos de orden n. Si $q = p^n$, considerando el grupo multiplicativo de $\mathbb{F}_q$, existen $\phi(q-1)$ elementos de orden $q-1$, esto es, $\phi(q-1)$ elementos primitivos. Si los agrupamos según el polinomio primitivo del que sean raíz, seremos capaces de contar el número total de polinomios primitivos.

Teorema 4.15. *Existen exactamente* $\frac{\phi(q^n-1)}{n}$ *polinomios primitivos mónicos de grado* n *en* $\mathbb{F}_q[x]$

Demostración. En $\mathbb{F}_{q^n}$ existen $\phi(q^n-1)$ elementos primitivos sobre $\mathbb{F}_q$. Si agrupamos estos elementos por conjugación, cada clase proporciona las n raíces de un polinomio primitivo de grado n. Por el Teorema 2.13, estas son distintas entre sí. Entonces el número total de polinomios primitivos mónicos sobre un cierto cuerpo viene dado por el número de estas clases, $\frac{\phi(q^n-1)}{n}$. □

Vamos a dar dos caracterizaciones para polinomios primitivos. La primera es la más sencilla:

Teorema 4.16. *Sea* $f \in \mathbb{F}_q[x]$ *un polinomio de grado* m*. Entonces* f *es primitivo si y solo si* $f(0) \neq 0$ *y* $ord(f) = q^m - 1$.

Este resultado es sencillo de demostrar utilizando los Teoremas 4.7, 4.8 y 4.9, que caracterizan el orden de un polinomio. Además, la hipótesis $f(0) \neq 0$ sirve para descartar el caso $m = 1$, $q = 2$, $f(x) = x$.

El siguiente lema, derivado de la caracterización anterior, nos ayudará a probar otra condición equivalente a la de primitividad.

Lema 4.17. *Sea* $f \in \mathbb{F}_q[x]$ *un polinomio de grado positivo con* $f(0) \neq 0$ *y sea* r *el menor entero positivo tal que exista algún* $a \in \mathbb{F}_q^*$ *de forma que* $x^r \equiv a \pmod{f(x)}$*. Entonces* $ord(f) = hr$*, donde* h *es el orden multiplicativo de* a *en* $\mathbb{F}_q^*$.

Demostración. Definimos $e = \text{ord}(f)$. Como $x^e \equiv 1 \pmod{f}$, tenemos que $e \geqslant r$. Realizamos una división entera para obtener $e = sr + t$ con $0 \leqslant t < r$. Se tiene que $1 \equiv x^{sr+t} \equiv a^s x^t \pmod{f}$. De forma inmediata $x^t \equiv a^{-s} \pmod{f}$, esto es, $x^t \equiv b \pmod{f}$ para algún $b \in \mathbb{F}_q^*$. Como r es el mínimo entero positivo que cumple esa condición, deducimos que $t = 0$. Entonces $a^s \equiv 1 \pmod{f}$, por lo que $h|s$. Como $h \leqslant s$, tenemos que $sr = e \geqslant hr$. Por último, como $x^{hr} \equiv a^h \equiv 1 \pmod{f}$, deducimos que $e \leqslant hr$ y por tanto $e = hr$. □

Estamos en condiciones de enunciar y demostrar la segunda caracterización de primitividad:

Teorema 4.18. *Sea* $f \in \mathbb{F}_q[x]$ *un polinomio mónico de grado* $m \geqslant 1$.
Entonces el polinomio f *es primitivo si y solo si* $(-1)^m f(0)$ *es un elemento primitivo de*

$\mathbb{F}_q$, y además el menor entero positivo r para el que $x^r \equiv a \pmod{f(x)}$ para algún $a \in \mathbb{F}_q$ es $r = (q^m - 1)/(q - 1)$.
En el caso en el que f es primitivo, entonces $x^r \equiv (-1)^m f(0) \pmod{f(x)}$.

Demostración.
• Si f es primitivo, entonces alguna de sus raíces es un elemento primitivo $\alpha \in \mathbb{F}_{q^m}$. Viendo que f es el polinomio característico de α en $\mathbb{F}_q$ y calculando $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$, tenemos que

$$(-1)^m f(0) = \alpha^{(q^m-1)/(q-1)}$$

De manera inmediata, el orden en $\mathbb{F}_q$ de $(-1)^m f(0)$ es $q - 1$, por lo que este elemento es primitivo en $\mathbb{F}_q$.
Ahora, como f es el polinomio mínimo de α sobre $\mathbb{F}_q$, de la expresión anterior deducimos

$$x^{(q^m-1)/(q-1)} \equiv (-1)^m f(0) \pmod{f(x)}$$

de forma que $r \leqslant (q^m - 1)/(q - 1)$. Además $q^m - 1 = \mathrm{ord}(f)$ por el Teorema 4.16 y $\mathrm{ord}(f) \leqslant (q - 1)r$ por el lema anterior. Entonces $r = (q^m - 1)/(q - 1)$

• Para el recíproco, por el lema anterior y $r = (q^m - 1)/(q - 1)$, tenemos que $\mathrm{ord}(f)$ es coprimo con q. Por el Teorema 4.9, deducimos que f no tiene factores irreducibles con potencia mayor que 1, es decir, f es producto de factores irreducibles coprimos, $f = f_1 \dots f_k$, siendo cada f_i de grado m_i. Tenemos que $\mathrm{ord}(f_i) | (q^{m_i} - 1)$ y $q^{m_i} - 1$ divide a

$$d = (q^{m_1} - 1) \dots (q^{m_k} - 1)/(q - 1)^{k-1}$$

de modo que $\mathrm{ord}(f_i) | d$ para todo $1 \leqslant i \leqslant k$. Por el Lema 4.6, deducimos que $f_i | (x^d - 1)$ para todo i y por ser estos los factores irreducibles (coprimos) de f, su producto f también divide a $x^d - 1$.
Si suponemos que $k \geqslant 2$, entonces

$$d < (q^{m_1 + \dots + m_k} - 1)/(q - 1) = (q^m - 1)/(q - 1) = r$$

contradice que r sea el mínimo de los $x^r \equiv a \pmod{f(x)}$ para algún $a \in \mathbb{F}_q$, por lo que $k = 1$ y f es irreducible.

Para terminar, veamos que el orden de f es $q^m - 1$. Sea $\beta \in \mathbb{F}_{q^m}$ raíz del polinomio primitivo f. Sabíamos que

$$(-1)^m f(0) = \beta^{(q^m-1)/(q-1)} = \beta^r$$

con lo que $\beta^r = (-1)^m f(0)$ y $x^r \equiv (-1)^m f(0) \pmod{f(x)}$. El orden de $(-1)^m f(0)$ en $\mathbb{F}_q^*$ es $h = q - 1$, y tenemos que $\mathrm{ord}(f) = hr = q^m - 1$.
Como f es irreducible, concluimos que f es primitivo □

4.3. Construcciones de polinomios primitivos

Vamos a dirigir nuestro enfoque a casos particulares, construyendo polinomios primitivos a través de transformaciones algebraicas de otros o estudiando familias de polinomios primitivos dentro de cuerpos finitos concretos.

Algunos autores, como Z. X. Wan, utilizan el término periodo de un polinomio de manera alternativa al orden, utilizando una definición distinta pero equivalente:

Definición 4.19. *Consideramos $f(x) \in \mathbb{F}_q[x]$ un polinomo irreducible de grado n, tal que $f(x) \neq x$. Tenemos que $\mathbb{F}_q[x]/(f(x))$ define un cuerpo finito isomorfo a $\mathbb{F}_{q^n}$ por el Teorema 2.5. Llamamos* ***periodo*** *de f al orden de la clase de residuos sobre $\mathbb{F}_{q^n}^*$ que contiene al elemento x.*

Veamos que, en efecto, ambos conceptos son equivalentes.

Teorema 4.20. *Sea $f \in \mathbb{F}_q[x]$ un polinomio irreducible mónico de grado n, de tal forma que $f(x) \neq x$. Entonces el periodo de f es el orden de f.*

Demostración. Por el Teorema 2.13, las raíces del polinomio f son conjugadas, y por tanto tienen el mismo orden. Denotamos este orden por e y el periodo de f por l. Entonces $f|(x^e - 1)$. Tenemos que $x^e \equiv 1 \pmod{f(x)}$. Deducimos que $l|e$.
Si α una raíz de f, tenemos que $\alpha^l - 1 = 0$, por lo que l divide al orden de α, ergo al orden de f, e. Concluimos que $l = e$. □

Podemos obtener un resultado que nos servirá para recordar el Teorema 4.16.

Corolario 4.21. *Sea $f \in \mathbb{F}_q[x]$ un polinomio irreducible de grado m tal que $f(x) \neq x$. Entonces f es primitivo si y solo si el periodo de f es $q^m - 1$.*

Como resultado del teorema que veremos a continuación, podemos obtener fácilmente parejas de polinomios primitivos.

Teorema 4.22. *Sea $f \in \mathbb{F}_q[x]$ un polinomio de grado n tal que su término independiente es no nulo ($a_0 \neq 0$), y sea f^* su polinomio recíproco. Entonces f es irreducible si y solo si f^* es irreducible. Además, f es primitivo si y solo si f^* es primitivo.*

Demostración. Empecemos por demostrar que la irreducibilidad de f es equivalente a la de f^*.
Supongamos que $f = gh$ es reducible. Denotamos k el grado de g y $n - k$ el grado de h. Entonces

$$f^*(x) = x^n f(1/x) = (x^k g(1/x))(x^{n-k} h(1/x)) = g^*(x)h^*(x)$$

Por tanto, f^* es reducible. Como el término independiente de f es no nulo, tenemos que $(f^*)^* = f$. Por tanto f es reducible si y solo si f^* es reducible, que es lo que queríamos ver.

Por último, supongamos que f es primitivo. Sabemos que $f \neq x$ por ser $a_0 \neq 0$. Como f es primitivo, es un polinomio irreducible de orden $q^n - 1$. Por el Teorema 4.11 f^* es de orden $q^n - 1$, y por lo visto en esta demostración, también es irreducible. Usando el corolario anterior, concluimos que f^* es primitivo.
La otra implicación es análoga. □

Para finalizar el capítulo, vamos a estudiar un caso en el que todos los polinomios irreducibles sean primitivos. Particularmente, esto ocurre cuando se consideran polinomios de grado p un número primo sobre el cuerpo finito de 2 elementos, $\mathbb{F}_2$, y de forma que $2^p - 1$ sea a su vez un número primo, es decir, p es el exponente de un primo de Mersenne.

Teorema 4.23. *Sea p un entero positivo. Si $2^p - 1$ es un número primo, entonces p es primo y todo polinomio irreducible de grado p sobre $\mathbb{F}_2$ es primitivo.*

Demostración. Supongamos que existe un factor propio de p, denotado m, de forma que $1 < m < p$. Entonces $2^m - 1$ es un factor propio de $2^p - 1$, lo que es imposible por ser este primo.
Por otro lado, $p \neq 1$ pues en este caso $2^p - 1 = 1$ no sería primo. Concluimos que p es primo.

Consideramos $\mathbb{F}_{2^p}$ la extensión de $\mathbb{F}_2$ dada por un polinomio irreducible de grado p. Dentro del grupo multiplicativo $\mathbb{F}_{2^p}^*$, todo elemento distinto de 1 tiene como orden un divisor propio de $2^p - 1$. Como este número es primo por hipótesis, el orden es $2^p - 1$.
Sea f un polinomio irreducible de grado p. Trivialmente $f(x) \neq x$. Si α es una raíz de f, tenemos que $\alpha \neq 0, 1$. Por tanto, el orden de α, así como el orden de f, es igual a $2^p - 1$. Por el Corolario 4.21, obtenemos que f es primitivo. □

Parece intuitivo que se puedan encontrar otros casos similares considerando polinomios de grado $q^n - 1$, siendo q una potencia de primo. No obstante, si q es impar, necesariamente $q = 3$ y $n = 1$. Por otro lado, si q es una potencia de 2 (mayor que 2), entonces no podemos utilizar un análogo de la demostración anterior, puesto que en ella utilizamos que todo elemento distinto de 1 de $\mathbb{F}_{q^p}^*$ es primitivo, lo cual no ocurre cuando $q = 2^n$ para algún $n > 1$.

Capítulo 5

Polinomios irreducibles

Hemos visto que los polinomios irreducibles son fundamentales a la hora de generar extensiones de cuerpos finitos, así como caracterizar los polinomios primitivos. Como consecuencia, nos es útil saber caracterizar también los polinomios irreducibles, además de poder construirlos en casos particulares.

5.1. Criterios de irreducibilidad

Los resultados de esta sección están basados en el capítulo 10 de *Lectures on Finite Fields and Galois Rings* [18].
Comenzamos viendo una caracterización sencilla de la irreducibilidad

Teorema 5.1. *Sea $f \in \mathbb{F}_q[x]$ un polinomio de grado $n > 1$. Entonces f es irreducible si y solo si se verifican la condiciones siguientes:*

1. *$f|(x^{q^n} - x)$.*
2. *$mcd(f, x^{q^i} - x) = 1$ para todo i tal que $1 \leqslant i < n$.*

Demostración. Si f es irreducible, vimos en el Lema 2.12 que $f|(x^{q^n} - x)$. Además, es evidente que $n \nmid i$ para $1 \leqslant i < n$, por lo cual, aplicando de nuevo el Lema 2.12, $f \nmid (x^{q^i} - x)$ para $1 \leqslant i < n$. Por ser f irreducible, se cumple la condición *(2)*.

Si f es reducible, entonces tiene un factor irreducible de un grado menor que n. Denotamos a ese factor por g, de orden m. Entonces tenemos que $g|(x^{q^m} - x)$. Por tanto, la condición 2 no se cumple, pues $g|\text{mcd}(f, x^{q^m} - x)$ y $1 \leqslant m < n$. □

Podemos ver también algunos resultados sencillos que nos dan condiciones necesarias para que un polinomio sea irreducible.

Teorema 5.2. *Sea $f \in \mathbb{F}_q[x]$ un polinomio. Si f es irreducible, entonces:*

1. *El término constante de f es no nulo.*
2. *La suma de los coeficientes de f es no nula.*
3. *$mcd(f, f'(x)) = 1$*

Demostración. (1) es trivial.
(2) se demuestra viendo que si f es de grado mayor que 1 y la suma de sus coeficientes es nula, entonces $(x-1)|f$.

Veamos la condición *(3)*. Claramente f no tiene raíces múltiples, pues si tuviera alguna entonces no se cumpliría el Teorema 2.13. Además, $\text{mcd}(f, f'(x)) \neq 1$ si y solo si f tiene alguna raíz múltiple. □

De forma similar al capítulo anterior con la primitividad, podemos obtener más criterios de irreducibilidad, o bien restringiendo los tipos de polinomios con los que trabajamos, o bien la característica de los cuerpos finitos en los que se encuentran.
Vamos a comenzar viendo algunos criterios para binomios:

Teorema 5.3. *Sean t un entero positivo mayor que 1 y $a \in \mathbb{F}_q^*$ tal que $ord(a) = m$ con $m > 1$. Entonces el binomio $x^t - a \in \mathbb{F}_q[x]$ es irreducible sobre $\mathbb{F}_q$ si y solo si verifica las condiciones siguientes:*

1. *Todo divisor primo de t divide a m y no divide a $(q-1)/m$.*
2. *Si $4|t$, entonces $4|(q-1)$.*

Esta demostración tal y como está escrita en [18, Teorema 10.7] resulta bastante laboriosa. Por ello, nos enfocaremos en el caso en el que t es un número primo. En particular, esto vuelve redundante la segunda condición.

Demostración. En primer lugar, justificaremos que $m|(q-1)$. Sabemos que $a^{q-1} = 1$ por ser un elemento de $\mathbb{F}_q$, por lo que el orden de a tiene que dividir a $q-1$.

Supongamos que se cumple la condición *(1)*. Sea α una raíz de $x^t - a$ y sea $g \in \mathbb{F}_q[x]$ su polinomio mínimo sobre $\mathbb{F}_q$, con grado d. Podemos suponer que $d > 1$. Considerando las raíces conjugadas de α (todas distintas entre sí), tenemos que

$$g(x) = (x-\alpha)(x-\alpha^q)\dots(x-\alpha^{q^{d-1}})$$

Veamos primero que $\text{ord}(\alpha) = tm$. Por ser α raíz de $x^t - a$, $\alpha^t = a$. Como el orden de a es m, deducimos que el orden de α divide a tm. Si suponemos que $\text{ord}(\alpha) < tm$, entonces existe un número primo r tal que $r|tm$ y $\alpha^{tm/r} = 1$. Además, o bien $r|m$, o bien $r|t$ y, por la condición *(1)*, $r|m$. Concluimos que $a^{m/r} = 1$, lo que contradice la hipótesis de $\text{ord}(a) = m$. Por tanto $\text{ord}(\alpha) = tm$.
Como $\alpha \in \mathbb{F}_{q^d}$, tenemos que $\alpha^{q^d-1} = 1$. Entonces, como $\text{ord}(\alpha)|(q^d-1)$, deducimos que $tm|(q^d-1)$. En particular, $q^d \equiv 1 \pmod{tm}$. Sabemos que d es el menor entero positivo

para el cual $q^d \equiv 1 \pmod{tm}$, pues en caso contrario $g(x)$ no sería irreducible. Por tanto, el orden multiplicativo de $q \pmod{tm}$ es d.

Por otro lado, tenemos que

$$q^t - 1 = (q-1)(q^{t-1} + q^{t-2} + \cdots + q + 1)$$

Además, $q^i \equiv 1 \pmod{t}$ para todo $0 \leqslant i < t$. Por tanto, $t|(q^{t-1} + q^{t-2} + \cdots + q + 1)$. Como $m|(q-1)$, tenemos que $q^t - 1 \equiv 0 \pmod{mt}$. Hemos obtenido que $q^t \equiv 1 \pmod{mt}$, por lo cual el orden de q en $\mathbb{Z}^*_{mt}$ divide a t, esto es, $d|t$. Deducimos que $d = t$ por ser t primo y concluimos que el polinomio irreducible de α tiene grado t, por lo que es exactamente $x^t - a$.

Veamos ahora la implicación recíproca.
Supongamos que *(1)* no se cumple. Entonces, o bien $t \nmid m$, o bien t divide a $(q-1)/m$.
Si $t|(q-1)/m$, denotamos $(q-1)/m = ts$ para algún natural s. Denotamos por $\mathbb{F}_q^{*t}$ al conjunto de elementos de $\mathbb{F}_q^*$ que son potencia t-ésima de algún elemento de $\mathbb{F}_q^*$. Es fácil ver que $\mathbb{F}_q^{*t}$ tiene $(q-1)/t = ms$ elementos. Además, $\mathbb{F}_q^{*t}$ tiene un único subgrupo de orden m, que está generado por el elemento a de orden m. Tenemos que $a = b^t$ para algún $b \in \mathbb{F}_q^*$.
Entonces $x^t - a = x^t - b^t$ tiene a $x - b$ como divisor propio.

Supongamos ahora que t no divide a m ni a $(q-1)/m$. Evidentemente tampoco divide a $q-1$. Entonces t es coprimo con $q-1$ y podemos tomar un natural s de forma que $ts \equiv 1 \pmod{q-1}$. Entonces $a^{ts} = a^{e(q-1)+1} = a$, escogiendo un natural e tal que $ts + 1 = e(q-1)$. Para concluir, tenemos que $x^t - a = x^t - a^{ts}$ y obtenemos a $x - a^s$ como factor de $x^t - a$. □

Es evidente que ningún binomio es irreducible sobre $\mathbb{F}_2$. Veamos un binomio irreducible en $\mathbb{F}_{2^4}$: consideramos el polinomio $x^4 + x^3 + x^2 + x + 1$ irreducible sobre $\mathbb{F}_2$, y α una raíz de este polinomio. Podemos calcular el orden de α, que es 5. Deducimos que el polinomio $x^5 - \alpha$ es irreducible sobre $\mathbb{F}_{16}$.

Podemos obtener rápidamente familias de polinomios irreducibles considerando la caracterización anterior para $t = r^k$ para cualquier entero positivo k y ciertos primos r.

Corolario 5.4. *Sea $a \in \mathbb{F}_q^*$ tal que $ord(a) = m > 1$ y sean k un entero positivo cualquiera y r un número primo tal que $r|(q-1)$ y $r \nmid (q-1)/m$. Para el caso $r = 2$,$k \geqslant 2$, supongamos que $4|(q-1)$.*
Entonces, el polinomio $x^{r^k} - a \in \mathbb{F}_q[x]$ es irreducible.

Demostración. r^k tiene a r como único factor primo. La condición *(1)* del teorema anterior se cumple por hipótesis. Para r impar o $k \leqslant 1$, entonces $4 \nmid r^k$ y *(2)* se cumple de manera trivial. Si $r = 2$ y $k \geqslant 2$, entonces por hipótesis se cumple *(2)*. □

Por ejemplo, consideramos $f(x) = x^2 + x - 1 \in \mathbb{F}_3[x]$ y α una raíz de f. Es fácil

calcular que α tiene orden 8 en $\mathbb{F}_9$. Entonces el polinomio $x^{2^k} - \alpha$ es irreducible sobre $\mathbb{F}_9$ para todo entero positivo k, pues $2|8 = q - 1$ y $2 \nmid 1 = (q-1)/m$.

Después de trabajar sobre binomios, es natural continuar con el tipo de polinomio directamente más complejo. A continuación vamos a caracterizar mediante dos resultados la irreducibilidad de un tipo particular de trinomios, dado por $x^p - ax - b$ sobre $\mathbb{F}_q$ y siendo $q = p^n$.

Teorema 5.5. *Sean p un número primo y $q = p^n$ para algún entero positivo n. Entonces el trinomio $x^p - x - b \in \mathbb{F}_q[x]$ es irreducible si y solo si $Tr_{\mathbb{F}_q/\mathbb{F}_p}(b) \neq 0$.*

Demostración. Sea α una raíz de $x^p - x - b$. Es inmediato que $\alpha^p = \alpha - b$. Si elevamos ambos lados de la expresión anterior a la p-ésima potencia de forma iterativa, es sencillo ver que

$$\alpha^{p^i} = b^{p^{i-1}} + b^{p^{i-2}} + \cdots + b + \alpha \quad \text{, para } i = 1, 2, \ldots$$

Entonces

$$\alpha^q = b^{p^{n-1}} + \cdots + b + \alpha = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b) + \alpha$$

Si $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b) = 0$, entonces $\alpha^q - \alpha = 0$. En consecuencia, el polinomio irreducible de α se descompone en $\mathbb{F}_q$, y en particular $x - \alpha$ divide a $x^p - x - b$.

Por otro lado, si $t = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b) \neq 0$, entonces elevando a la q-ésima potencia la expresión anterior de forma iterativa, tenemos que

$$\alpha^{q^i} = \alpha + it \quad \text{, para } i = 1, 2, \ldots, p-1 \text{ y } \alpha^{q^p} = \alpha$$

Entonces α induce p elementos conjugados sobre $\mathbb{F}_q$, por lo cual son las raíces de un polinomio irreducible de grado p, el cual podemos considerar que es $x^p - x - b$. □

Como caso particular, consideremos $b \in \mathbb{F}_p$ tal que $b \neq 0$ y $q = p^n$ tal que $p \nmid n$. Entonces $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b) = nb \neq 0$.
Por ejemplo, $x^3 - x - 1$ es irreducible sobre $\mathbb{F}_{3^{3n+k}}$ para todo $n \in \mathbb{N}$ y para $k = 1$ o $k = 2$.

El resultado anterior nos será de ayuda para probar un caso concreto dentro de la demostración para el caso de trinomios más generales que queríamos ver:

Teorema 5.6. *Sean p un número primo y q una potencia positiva de p. Dados $a, b \in \mathbb{F}_q^*$ tenemos que $f(x) = x^p - ax - b$ es irreducible sobre $\mathbb{F}_q$ si y solo si existe algún $a_0 \in \mathbb{F}_q^*$ tal que $a = a_0^{p-1}$ y además $Tr_{\mathbb{F}_q/\mathbb{F}_p}(b/a_0^p) \neq 0$*

Demostración. Supongamos que $a = a_0^{p-1}$ y $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b/a_0^p) \neq 0$. Entonces,

$$f(x) = a_0^p \left(\left(\frac{x}{a_0} \right)^p - \left(\frac{x}{a_0} \right) - \left(\frac{b}{a_0^p} \right) \right)$$

Si hacemos el cambio de variable $y = \frac{x}{a_0}$, por el teorema anterior, $y^p - y - \left(\frac{b}{a_0^p} \right)$ es irreducible, por lo que f también lo es.

Supongamos ahora que $a \neq a_0^{p-1}$ para cualqier $a_0 \in \mathbb{F}_q$. Denotando $l(x) = x^p - ax$, tenemos que $l(x)$ tiene a 0 como única raíz en $\mathbb{F}_q$. Si consideramos a l como aplicación de $\mathbb{F}_q$ en $\mathbb{F}_q$, podemos razonar que es inyectiva: para $c, d \in \mathbb{F}_q$,

$$l(c) - l(d) = c^p - d^p - c + d = (c-d)^p - (c-d) = l(c-d)$$

entonces $l(c) = l(d)$ si y solo si $c = d$ porque l solo se anula en 0. Ahora, por ser $\mathbb{F}_q$ finito, l es biyectiva y suprayectiva. Entonces, para todo $b' \in \mathbb{F}_q$ existe un $\alpha \in \mathbb{F}_q$ tal que $\alpha^p - a\alpha - b' = 0$. Si consideramos el elemento b de la hipótesis, tomamos el α correspondiente y $(x-\alpha)|f$, ergo f es reducible.

Solo nos falta ver el caso $a = a_0^{p-1}$ para algún $a_0 \in \mathbb{F}_q^*$ y $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b/a_0^p) = 0$.
Si hacemos de nuevo el cambio de variable a $y^p - y - \left(\frac{y}{a_0^p}\right)$, podemos aplicar el teorema anterior y obtenemos que tanto este polinomio como f son reducibles por ser $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b/a_0^p) = 0$. □

Siguiendo la idea del ejemplo anterior, si $a \in \mathbb{F}_p$ y $a \neq 1$, entonces el polinomio $x^p - ax - b$ es reducible sobre $\mathbb{F}_p$ para todo $b \in \mathbb{F}_p$, puesto que para cualquier a_0 en este cuerpo, se verifica que $a_0^{p-1} = 1 \neq a$.

Como ejemplo de polinomio irreducible, tomamos $\alpha \in \mathbb{F}_{25}$ raíz de $x^2 - 2$ en $\mathbb{F}_5[x]$. Entonces el polinomio $x^5 + x - \alpha = x^5 - (-x) + \alpha$ es irreducible sobre $\mathbb{F}_{25}$, pues $\alpha^4 = 4 = -1$ y además $b/\alpha^5 = \alpha/(-\alpha) = -1$ y $\mathrm{Tr}_{\mathbb{F}_{25}/\mathbb{F}_5}(-1) = -2 \neq 0$.

5.2. Transformaciones de polinomios irreducibles

Una pregunta interesante es qué transformaciones de polinomios irreducibles van a ser a su vez irreducibles. Por ejemplo, sabemos que, dado f un polinomio irreducible de grado n, su recíproco, dado por $x^n f(x^{-1})$, va a ser también irreducible de grado n. Podemos ver algo similar al trabajar con otra transformación parecida: si tenemos que el par (a, b) no es proporcional a (c, d), esto es, $ad - cb \neq 0$, entonces $(cx+d)^n f\left(\frac{ax+b}{cx+d}\right)$ será también irreducible y de grado n.

La progresión natural es considerar situaciones que generalizan las transformaciones previas, polinomios de la forma $g(x)^n P\left(f(x)/g(x)\right)$. En este caso, f y g tienen que ser coprimos, pues de lo contrario el polinomio resultante sería $h(x)^n \left(g_0(x)^n P\left(f_0(x)/g_0(x)\right)\right)$, siendo h el máximo común divisor de f y g, (de grado mayor que 0) y denotando $f_0(x) = f(x)/h(x)$ y $g_0(x) = g(x)/h(x)$.

Teorema 5.7. *Sean $f(x)$, $g(x)$ y $P(x)$ polinomios sobre $\mathbb{F}_q$ tales que $P(x)$ es irreducible de grado n.*
Entonces el polinomio $g(x)^n P\left(f(x)/g(x)\right)$ es irreducible sobre $\mathbb{F}_q$ si y solo si existe una raíz $\lambda \in \mathbb{F}_{q^n}$ de $P(x)$ tal que $f(x) - \lambda g(x)$ es irreducible sobre $\mathbb{F}_{q^n}$.
Además, si $P(x) \neq cx$ para $c \in \mathbb{F}_q^*$, entonces el polinomio dado por dicha transformación es de grado hn, donde h es el máximo de los grados de f y g.

Demostración. Vamos a denotar $P_*(x) = g(x)^n P\left(f(x)/g(x)\right)$.

Veamos primero el caso $P(x) = cx$ para $c \in \mathbb{F}_q^*$. Tenemos que $P_*(x) = cf(x)$. Además, la única raíz de P es 0. Está claro que $cf(x)$ es irreducible si y solo si $f(x) = f(x) - 0g(x)$ también lo es.

Queda probar el resultado para $P(x) \neq cx$. Lo dividimos en los casos $n = 1$ y $n > 1$. Si $n = 1$, consideramos $P(x) = x - c$ para algún c no nulo, que es la única raíz de P. Entonces $P_*(x) = f(x) - cg(x)$, y el resultado es trivial.
Supongamos que $n > 1$. Sea $d(x) = \text{mcm}(f(x), g(x))$. Es evidente que $d(x)$ divide a $P_*(x)$ y a $f(x) - \lambda g(x)$ para cualquier raíz de $P(x)$, λ. Si tenemos que $d(x) \neq 1$, entonces $P_*(x)$ y $f(x) - \lambda g(x)$ son reducibles.

Para terminar, vamos a suponer que $d(x) = 1$ y que γ es una raíz de P_*. Entonces $f(\gamma)/g(\gamma)$ es una raíz de P, a la que llamaremos $\lambda \in \mathbb{F}_{q^n}$. Tenemos que $f(\gamma) = \lambda g(\gamma)$. Entonces γ es una raíz del polinomio $f(x) - \lambda g(x)$ de grado h sobre $\mathbb{F}_{q^n} = \mathbb{F}_q[\lambda]$.
Para finalizar, tenemos que $[\mathbb{F}_q[\lambda] : \mathbb{F}_q] = n$ (y además el grado de $P_*(x)$ sobre $\mathbb{F}_q$ es claramente hn), por lo que los siguientes enunciados son equivalentes:

- $P_*(x)$ es irreducible sobre $\mathbb{F}_q$.
- $[\mathbb{F}_q[\gamma] : \mathbb{F}_q] = hn$.
- $[\mathbb{F}_q[\gamma] : \mathbb{F}_q[\lambda]] = h$.
- $f(x) - \lambda g(x)$ es irreducible sobre $\mathbb{F}_{q^n}$. □

Durante el resto de la sección, utilizaremos λ al referirnos a una raíz cualquiera del polinomio irreducible $P(x)$ y $P_*(x)$ para el polinomio que resulta de la transformación vista en el resultado anterior para polinomios f y g dados.
Podemos aplicar el resultado anterior de manera inmediata cuando $f(x) - \lambda g(x)$ es uno de los binomios o trinomios que hemos visto en la sección previa. Por ejemplo, si $g(x) = 1$ la coprimalidad es inmediata, por lo que solo necesitamos ver que $f(x) - \lambda$ es irreducible sobre $\mathbb{F}_q[\lambda]$.
En el caso de $f(x) = x^t$, necesitamos ver que el binomio $x^t - \lambda$ es irreducible sobre $\mathbb{F}_{q^n}$.

Teorema 5.8. *Sean t un entero positivo y $P(x) \in \mathbb{F}_q[x]$ un polinomio irreducible de grado n y orden e, que no sea de la forma cx. Entonces $P(x^t)$ es irreducible sobre $\mathbb{F}_q$ si y solo si:*

1. *Todo divisor primo de t divide a e y no divide a $(q^n - 1)/e$.*
2. *Si $4|t$, entonces $4|(q^n - 1)$.*

Tomamos como ejemplo el polinomio $x^5 - \alpha$ sobre $\mathbb{F}_{16}$ (siendo α raíz de $x^4 + x^3 + x^2 + x + 1$) que vimos anteriormente. Tenemos que su orden es 25, por lo que el binomio $x^{5^n} - \alpha$ es irreducible sobre $\mathbb{F}_{16}$ para todo $n \geqslant 1$.

Podemos seguir un proceso análogo cuando $f(x)$ es un trinomio de la primera forma vista:

Teorema 5.9. *Sean p un número primo, q una potencia de p y $P(x)$ un polinomio irreducible de grado n sobre $\mathbb{F}_q$. Para $i \in \{0, 1, \ldots, n\}$ denotamos por c_i al coeficiente asociado a la potencia x^i de $P(x)$. Sea también $b \in \mathbb{F}_q$. Entonces $P(x^p - x - b)$ es irreducible sobre $\mathbb{F}_q$ si y solo si $Tr_{\mathbb{F}_q/\mathbb{F}_p}(nb + c_{n-1}) \neq 0$.*

Demostración. Es suficiente notar que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(b + \lambda) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b + \lambda))$ y que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b+\lambda) = nb + \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\lambda) = nb + c_{n-1}$. Al aplicar el Teorema 5.5, concluimos la demostración. □

Cuando $f(x) = x^2 + 1$ y $g(x) = x$, f y g son coprimos y tenemos que $f(x) - \lambda g(x)$ es de nuevo un trinomio. En particular, la transformación de cualquier polinomio $P(x)$ de grado n y con término constante no nulo será de la forma $P_*(x) = x^n P(x + x^{-1})$, lo que resulta claramente en un polinomio autorrecíproco de grado $2n$. Esto es porque

$$x^{2n} P_*(x^{-1}) = x^{2n} x^{-n} P(x^{-1} + (x^{-1})^{-1}) = x^n P(x + x^{-1}) = P_*(x)$$

Por el Teorema 5.7, la irreducibilidad de $P_*(x)$ en $\mathbb{F}_q$ depende de la de $x^2 - \lambda x + 1$. Al estudiar este polinomio, hay algunas particularidades que dependen de la paridad de q:

- Si q es par, entonces λ es un cuadrado sobre $\mathbb{F}_{q^n}$, pues $\lambda^{q^n} = \lambda$ y $\lambda = (\lambda^{q^n/2})^2$. En consecuencia, solo hace falta ver que la traza correspondiente es no nula.
- Si q es impar, podemos obtener las raíces de $x^2 - \lambda x + 1$ mediante el uso de la fórmula cuadrática. Para que este sea irreducible, necesitamos que $\sqrt{\lambda^2 - 4} \notin \mathbb{F}_{q^n}$. Denotaremos por $\mathbb{F}_{q^n}^2$ al conjunto de elementos que son cuadrados sobre $\mathbb{F}_{q^n}$. La condición que buscamos es $\lambda^2 - 4 \notin \mathbb{F}_{q^n}^{*2} = \mathbb{F}_{q^n}^2 - \{0\}$.
  Nos será útil ver que esto equivale a decir que $(\lambda^2 - 4)^{(q^n-1)/2} = -1$:

Lema 5.10. *Sean q una potencia de un primo impar y $\alpha \in \mathbb{F}_{q^n}$. Entonces $\alpha^{(q^n-1)/2} = -1$ si y solo si $\alpha \notin \mathbb{F}_{q^n}^{*2}$.*

Demostración. Si $\alpha \in \mathbb{F}_{q^n}^{*2}$, supongamos que $\alpha = e^2$. Entonces $\alpha^{(q^n-1)/2} = e^{(q^n-1)} = 1$.

Si $\alpha \notin \mathbb{F}_{q^n}^{*2}$, entonces $\alpha = \theta^r$ para algún elemento primitivo θ y algún r tal que $2 \nmid r$. Podemos escribir $\alpha^{(q^n-1)/2} = \theta^{r(q^n-1)/2}$. Por ser θ primitivo, su orden es $q^n - 1$. Además, como $2 \nmid r$, tenemos que $(q^n - 1) \nmid r(q^n - 1)/2$. Por tanto, $\theta^{r(q^n-1)/2} \neq 1$. Como las únicas raíces cuadradas de la unidad son 1 y -1, deducimos que $\alpha^{(q^n-1)/2} = -1$. □

Ya estamos en condiciones de estudiar la irreducibilidad de $P_*(x)$ en ambos casos:

Teorema 5.11. *Sea $q = 2^m$ y $P(x) = \sum_{i=0}^{n} c_i x^i$ un polinomio irreducible (de grado n) sobre $\mathbb{F}_q$. Supongamos que $c_0 \neq 0$. Entonces $P_*(x) = x^n P(x + x^{-1})$ es autorrecíproco de grado $2n$ y además es irreducible sobre $\mathbb{F}_q$ si y solo si $Tr_{\mathbb{F}_q/\mathbb{F}_2}(c_1/c_0) \neq 0$.*

Demostración. Por el Teorema 5.6, necesitamos ver que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_2}(\frac{-1}{\lambda^2}) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_2}(\lambda^{-2}) \neq 0$ (podemos ignorar el signo por ser característica 2). Tenemos que λ^{-1} es raíz del polinomio recíproco de $P(x)$. Por tanto, el coeficiente de x^{n-1} del polinomio irreducible y mónico de λ^{-1} es c_1/c_0, por lo que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\lambda^{-1}) = c_1/c_0$. Para terminar el resultado, podemos ver que

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_2}(\lambda^{-2}) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\lambda^{-2})) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\lambda^{-1}))$$

Esto es debido a que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\lambda^{-1})$ y $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\lambda^{-2})$ son elementos de $\mathbb{F}_q$ conjugados sobre $\mathbb{F}_2$, por lo que sus trazas sobre $\mathbb{F}_2$ coinciden. □

Veamos como ejemplo el polinomio $P(x) = x^3 + x + 1$ en $\mathbb{F}_2[x]$. Tenemos que

$$P_*(x) = x^3 P(x + x^{-1}) = x^6 + x^4 + x^3 + x^2 + 1$$

En este caso, $c_1/c_0 = 1$ y $P_*(x)$ es irreducible en $\mathbb{F}_q[x] = \mathbb{F}_{2^k}[x]$ si y solo si k es impar, pues $\mathrm{Tr}_{\mathbb{F}_{2^k}/\mathbb{F}_2}(1) = k$.

Veamos ahora el caso de característica impar:

Teorema 5.12. *Sea q una potencia de un primo impar y $P(x)$ un polinomio irreducible de grado n sobre $\mathbb{F}_q$. Entonces $P_*(x) = x^n P(x + x^{-1})$ es autorrecíproco de grado $2n$ y es irreducible sobre $\mathbb{F}_q$ si y solo si $P(2)P(-2) \notin \mathbb{F}_q^{*2}$.*

Demostración. Como vimos antes, $x^2 - \lambda x + 1$ es irreducible si y solo si $\lambda^2 - 4 \notin \mathbb{F}_{q^n}^{*2}$, y por el Lema 5.10, es equivalente a

$$\begin{aligned} -1 = (\lambda^2 - 4)^{(q^n-1)/2} = \\ = \{[(-\lambda + 2)(-\lambda - 2)]^{(q^n-1)/(q-1)}\}^{(q-1)/2} = \\ = \{\prod_{i=0}^{n-1}(2 - \lambda^{q^i})(-2 - \lambda^{q^i})\}^{(q-1)/2} = \\ = \{P(2)P(-2)\}^{(q-1)/2} \end{aligned}$$

De nuevo por el Lema 5.10, $P(2)P(-2)$ no es un cuadrado sobre $\mathbb{F}_{q^n}$. □

Veamos un ejemplo sobre $\mathbb{F}_7$. Por el Teorema 5.3, $f(x) = x^3 - 2$ es irreducible sobre $\mathbb{F}_7$. Como $f(2)f(-2) = (-1)(-3) = 3$ y esto no es un cuadrado en $\mathbb{F}_7$, entonces $x^3 f(x + x^{-1}) = x^3(x^3 + 3x + 3x^{-1} + x^{-3} - 2) = x^6 + 3x^4 - 2x^3 + 3x^2 + 1$ es irreducible en $\mathbb{F}_7[x]$.

Para terminar la sección, vamos a ver un par de casos particulares de transformaciones de polinomios irreducibles sobre $\mathbb{F}_2$. En [8] podemos encontrar resultados que hacen uso de transformaciones sencillas para construir sucesiones de polinomios irreducibles.

Teorema 5.13. *Sea n un natural par y sea $P(x) = \sum_{i=0}^{n} c_i x^i$ un polinomio irreducible sobre $\mathbb{F}_{2^s}$. Construimos la secuencia dada por*

$$F_0(x) = P(x)$$

$$F_{k+1} = (x^2 + x + 1)^{n2^k} F_k\left(\frac{1}{x^2 + x + 1}\right), \quad k \geqslant 0$$

Entonces todo polinomio de esta sucesión es irreducible si y solo si $c_1 = P'(1) = 1$*, siendo* $P'(x)$ *la derivada de* $P(x)$*.*

Este método nos proporciona polinomios F_k de grado $n2^k$ sobre cualquier extensión finita de $\mathbb{F}_2$. Si no obligamos a n a ser par, podemos tomar otra sucesión de polinomios irreducibles exigiendo una condición sobre la traza, a partir del siguiente resultado adicional de [8]:

Teorema 5.14. *Sea* $P(x) = \sum_{i=0}^{n} c_i x^i$ *un polinomio irreducible de grado* $n \geqslant 2$ *sobre* $\mathbb{F}_{2^s}$*. Construimos la secuencia dada por*

$$F_0(x) = P(x)$$
$$F_{k+1} = (x^2 + x + 1)^{n2^k} F_k\left(\frac{x^2 + x}{x^2 + x + 1}\right), \quad k \geqslant 0$$

Entonces todo polinomio de esta secuencia es irreducible sobre $\mathbb{F}_{2^s}$ *si y solo si*

$$Tr_{\mathbb{F}_{2^s}/\mathbb{F}_2}\left(\frac{P'(1)}{P(1)} + n\right) . Tr_{\mathbb{F}_{2^s}/\mathbb{F}_2}\left(\frac{c_1}{c_0} + n\right) = 1$$

Si aplicamos el resultado anterior para construir una sucesión de polinomios irreducibles sobre $\mathbb{F}_2$ la condición necesaria sería

$$\left(\frac{P'(1)}{P(1)} + n\right) . \left(\frac{c_1}{c_0} + n\right) = 1$$

5.3. Número total de polinomios irreducibles

El objetivo de esta sección es determinar completamente el número de polinomios irreducibles de grado fijo sobre un cuerpo finito cualquiera.
En primer lugar, vamos a ver algunos resultados de funciones aritméticas, tomando como referencia *Topics in Number Theory* [9].

Para llegar a nuestro objetivo, es fundamental conocer la función μ de Möbius:

Definición 5.15. *Para todo* $n \in \mathbb{N}$*, la función* μ ***de Möbius*** *viene dada por:*

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1. \\ 0 & \text{si } n \text{ contiene algún factor cuadrado distinto de } 1. \\ (-1)^r & \text{si } n \text{ contiene } r \text{ factores primos distintos.} \end{cases}$$

Recordamos el concepto de función multiplicativa:
Decimos que una función aritmética f (es decir, definida sobre los números naturales) es multiplicativa si para todo par de números naturales n, m coprimos entre sí, se tiene que

$f(nm) = f(n)f(m)$. Resulta sencillo ver que la función μ es una función multiplicativa. Por ende, a la hora de probar resultados sobre esta función, es suficiente probarlos para potencias de primos.

Por ejemplo, podemos redefinir la función μ para potencias de primos:

$$\mu(p^n) = \begin{cases} 1 & \text{si } n = 0. \\ -1 & \text{si } n = 1. \\ 0 & \text{si } n \geqslant 2. \end{cases}$$

También vamos a incluir un resultado que nos indicará que una cierta transformación de cualquier función multiplicativa (y que utilizaremos de forma frecuente) va a ser a su vez multiplicativa [9, Teorema 6.3].

Lema 5.16. *Sea f una función multiplicativa. Si la función F viene dada por*

$$F(n) = \sum_{d|n} f(d)$$

entonces F es una función multiplicativa

Este resultado nos será de utilidad para simplificar la transformación aplicada a la función μ.

Lema 5.17. *Sea M una función dada por $M(n) = \sum_{d|n} \mu(d)$. Entonces*

$$M(n) = \begin{cases} 1 & \textit{si } n = 1. \\ 0 & \textit{si } n \geqslant 2. \end{cases}$$

Demostración. Por el Lema anterior, sabemos que M es multiplicativa, así que nos podemos restringir a potencias de primos. Consideramos $M(p^m)$ para algún número primo p. Entonces $M(p^m) = \mu(1) + \mu(p) + \cdots + \mu(p^m) = 1 - 1 + 0 + 0 + \cdots + 0$. Es evidente que esta expresión vale, o bien 1 si $m = 0$, o bien 0 si $m \geqslant 1$. □

Con ayuda de estos dos lemas, vamos a conseguir ver que la transformación que hemos visto (dada por la suma de la evaluación en los divisores) va a tener un recíproco. Es decir, dada una función aritmética F, podemos obtener otra función aritmética de forma que $\sum_{d|n} f(d) = F(n)$ para todo $n \in \mathbb{N}$. En particular, si una es multiplicativa, entonces la otra también lo es [9, Teorema 6.8].

Teorema 5.18 (Fórmula de inversión de Möbius)**.** *Sean f una función aritmética y $F(n) = \sum_{d|n} f(d)$. Entonces*

$$f(n) = \sum_{d|n} F(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} F\left(\frac{n}{d}\right)\mu(d)$$

Demostración. Desarrollamos la expresión

$$\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right) = \sum_{d_1d_2=n}\mu(d_1)F\left(d_2\right) = \sum_{d_1d_2=n}\mu(d_1)\sum_{e|d_2}f(e) =$$
$$= \sum_{d_1e|n}\mu(d_1)f(e) = \sum_{e|n}f(e)\sum_{d_1|\frac{n}{e}}\mu(d_1) = \sum_{e|n}f(e)M\left(\frac{n}{e}\right)$$

Por el Lema anterior, $M\left(\frac{n}{e}\right) = 0$ cuando $e < n$ y vale 1 cuando $e = n$. Entonces la suma es $f(n)$. □

Falta preguntarse si el número de polinomios irreducibles de un cierto grado (n) sobre un cuerpo finito $\mathbb{F}_q$ tiene una transformación de este tipo con una expresión relativamente sencilla. Si recordamos el Lema 2.12, tenemos que el número de polinomios irreducibles que dividen a $x^{q^n} - x$ es el número de polinomios irreducibles de un grado divisor de n. Si demostramos que solo lo dividen una vez, podemos obtener una transformación que equivale al grado, q^n:

Teorema 5.19. *El producto de todos los polinomios irreducibles mónicos cuyo grado divide a n es $x^{q^n} - x$. Además, si denotamos $N_q(n)$ al número de polinomios irreducibles de grado n sobre $\mathbb{F}_q$, entonces para todo $n \in \mathbb{N}$*

$$q^n = \sum_{d|n} dN_q(d)$$

Demostración. El polinomio $x^{q^n} - x$ tiene como derivada $q^n x^{q^n-1} - 1 = -1$, por lo que no tiene raíces múltiples. Por el Lema 2.12, todo polinomio irreducible que divide a $x^{q^n} - x$ es de grado divisor de n, y además lo divide una sola vez.

Entonces el grado de $x^{q^n} - x$ es la suma de todos los grados de sus factores irreducibles, esto es:

$$q^n = \sum_{d|n} dN_q(d)$$ □

Como queríamos, hemos encontrado una función aritmética que se obtiene como suma en los divisores de n de una transformación simple de $N_q(n)$.
Lo único que queda hacer para obtener el resultado que estábamos buscando es aplicar la fórmula de inversión de Möbius a la función $f(n) = nN_q(n)$.

Teorema 5.20. *El número de polinomios irreducibles mónicos de grado n sobre $\mathbb{F}_q$ es*

$$N_q(n) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d$$

Veamos, por ejemplo, el número de polinomios irreducibles mónicos de grado 6 en $\mathbb{F}_5[x]$:

$$N_5(6) = \frac{1}{6}(5^6 - 5^3 - 5^2 + 5) = 2580$$

Capítulo 6

Polinomios sobre $\mathbb{F}_2$

Las propiedades con las que queremos trabajar están relacionadas con los criterios de primitividad e irreducibilidad vistos en capítulos anteriores. En este caso recurriremos a polinomios sencillos con una cantidad relativamente baja de coeficientes no nulos, a los que denominaremos polinomios de peso bajo.

Para este capítulo, se toma como referencia una variedad de artículos que estudian las propiedades de distintas familias de polinomios sobre el cuerpo $\mathbb{F}_2$. Este cuerpo es de gran interés, no solo por la simplicidad de los cálculos dentro de él, sino también por su extensiva utilización en el campo de la informática y la criptografía.

En particular, vamos a utilizar pentanomios además de trinomios, debido a que existen grados para los que no es posible encontrar trinomios irreducibles. Se cree que para todo grado $n > 4$, existe un pentanomio irreducible de grado n. Esta conjetura, y de manera más general la siguiente, motivan que el estudio de polinomios de peso bajo se enfoque en trinomios y pentanomios:

Conjetura. *Para cada $n \geqslant 3$, existe al menos un trinomio o un pentanomio irreducible de grado n sobre $\mathbb{F}_2$.*

Vamos a añadir también otros casos particulares, considerando trinomios y pentanomios que sean lo más sencillos posibles a la vez que mantengan cierta riqueza de resultados. Así mismo, buscamos reforzar los resultados con los que trabajemos mediante búsquedas por ordenador.

6.1. Trinomios sobre $\mathbb{F}_2$

Durante esta sección, vamos a centrarnos en familias de trinomios de la forma $x^n + x^k + 1$ sobre $\mathbb{F}_2$. Podemos suponer que $k \leqslant n/2$, puesto que tanto la irreducibilidad

como la primitividad se conservan al tomar polinomios recíprocos.

Una forma de estudiar la irreducibilidad de un polinomio es calcular el número de factores irreducibles que lo componen. No obstante, esto no es sencillo, pues suele ser tan difícil como calcular directamente esos factores. Alternativamente, podemos comprobar si el número de factores irreducibles es múltiplo de algún otro entero positivo. Esto es precisamente lo que se obtiene en un resultado de Swan [17], que permite comprobar la paridad del número de factores irreducibles:

Teorema 6.1. *Sean n, k enteros positivos tales que $n > k$ y solo uno de ellos es impar. El trinomio $x^n + x^k + 1$ tiene un número par de factores irreducibles sobre $\mathbb{F}_2$ en los siguientes casos:*

1. *n es par, k es impar, $n \neq 2k$ y $nk/2 \equiv 0, 1 \pmod 4$.*
2. *n es impar, k es par, $k \nmid 2n$ y $n \equiv \pm 3 \pmod 8$*
3. *n es impar, k es par, $k \mid 2n$ y $n \equiv \pm 1 \pmod 8$*

En cualquier otro caso, $x^n + x^k + 1$ tiene un número impar de factores irreducibles sobre $\mathbb{F}_2$.

En particular, este teorema nos indica que en los casos 1, 2 y 3, el polinomio x^n+x^k+1 es reducible. Además, podemos justificar la ausencia de casos en los que la paridad de n y k coincide. Si n y k son pares, es trivial que el polinomio es un cuadrado. Por otro lado, si ambos son impares, basta considerar el polinomio recíproco de exponentes n y $n - k$ que está dentro de las condiciones del teorema.

En el primer caso del teorema, podemos extraer un par de resultados más concretos. Si $n \equiv 0 \pmod 4$, entonces $nk/2 \equiv 2 \pmod 4$ para cualquier valor impar de k, por lo que siempre habrá un número impar de factores para estas condiciones.

El Teorema 6.1 nos proporciona también un corolario de gran relevancia. Si consideramos el caso en el que $n \equiv 0 \pmod 8$, entonces $nk/2 \equiv 0 \pmod 4$ y por tanto nos encontramos dentro del caso 1. Podemos deducir que:

Corolario 6.2. *Si $8|n$, entonces no existe ningún trinomio irreducible de grado n en $\mathbb{F}_2[x]$*

Como consecuencia, a la hora de realizar búsquedas de trinomios irreducibles por ordenador, no será necesario considerar ningún grado múltiplo de 8, lo cual reduce considerablemente los cálculos necesarios.

Vamos a ver una tabla, obtenida de [1], en la que se puede apreciar la distribución de los trinomios irreducibles en función de su grado módulo 8. Podemos observar que

cuando $n \equiv \pm 3$ (mód 8), hay muchos menos trinomios irreducibles de los que se podría esperar. No hay un resultado específico que lo explique, pero se puede tener en cuenta que la condición 2 del Teorema 6.1 requiere tomar k no divisores de $2n$ para obtener trinomios irreducibles, que son más comunes que los k que sí dividen a $2n$.

Cuadro 6.1: Número de trinomios irreducibles de grado $n < 5000$ módulo 8

n (mód 8)	0	1	2	3	4	5	6	7
Irreducibles	0	602	394	10	537	15	422	598

6.2. Construcciones de trinomios sobre $\mathbb{F}_2$

De forma similar a como se hizo en el capítulo anterior, vamos a buscar formas de construir trinomios irreducibles a partir de otros de menor grado. Tomamos especial enfoque en trinomios x^n+x^k+1 irreducibles con el menor k posible, debido a la simplicidad de cálculos. Como notación, escribimos los trinomios de la forma $T_{n,k}(x) = x^n + x^k + 1$.

Vamos a empezar viendo un resultado de Zierler [21]:

Teorema 6.3. *Sea* $f(x) = \sum a_i x^i$ *un polinomio irreducible de orden* e *sobre* $\mathbb{F}_2$*. Denotamos* $f^\alpha(x) = \sum a_i x^{2^i-1}$*. Entonces los factores irreducibles de* f^α *tienen grado* e*.*

A la hora de representar polinomios irreducibles de grado alto, resulta tedioso y poco esclarecedor escribir el orden. Para esto se utiliza el concepto de índice:
Si f es un polinomio irreducible de grado n y orden e sobre $\mathbb{F}_2$, denotamos índice de f a $(2^n - 1)/e$. Puede entenderse como la "distancia" a la que se encuentra f de ser un polinomio primitivo. Entonces, si el polinomio f tiene grado n e índice 1 (esto es, es primitivo), tenemos que f^α es de grado 2^n-1 y tiene factores irreducibles de orden 2^n-1, por lo que es irreducible.

Corolario 6.4. *Supongamos que* $f(x)$ *es un polinomio irreducible sobre* $\mathbb{F}_2$*. Entonces* $f(x)$ *es primitivo si y solo si* $f^\alpha(x)$ *es irreducible.*

Es fácil ver cómo este corolario le proporciona utilidad a la familia de trinomios $T_{n,1}$, debido a que $T^\alpha_{n,1}(x) = T_{2^n-1,1}(x)$

Por ejemplo, $T_{n,1}(x)$ es primitivo para $n = 2, 3, 4, 6, 7$. Por tanto, será además irreducible para $n = 3, 7, 15, 63, 127$. Veamos una tabla más completa, obtenida de [22]:

Cuadro 6.2: $n < 300$ para los que $T_{n,1}$ es irreducible

n	2	3	4	6	7	9	15	22	28	30	46	60	63	127	153	172
Índice	1	1	1	1	1	7	1	1	$3 \cdot 5$	$3^2 \cdot 11$	3	1	1	1	1	$3 \cdot 5$

El siguiente tipo de trinomios que vamos a estudiar es $T_{n,2} = x^n + x^2 + 1$. Como consecuencia del Teorema 6.1, tenemos que, para que $T_{n,2}$ sea irreducible, es necesario que n sea impar y $n \equiv \pm 3 \pmod 8$. En este caso, podemos recurrir a resultados de [4] para obtener familias finitas de trinomios irreducibles:

Teorema 6.5. *Sea $T_{n,2}$ un trinomio irreducible de orden e e índice d y sea p un primo impar. Si $p|e$ y $p \nmid d$, entonces $T_{np^k,2p^k}$ es irreducible para todo $k \in \mathbb{N}$. Además, el orden de $T_{np^k,2p^k}$ es ep^k*

Este resultado se puede generalizar a enteros positivos coprimos con el índice del trinomio:

Corolario 6.6. *Sea $T_{n,2}$ un trinomio irreducible de orden e e índice d, y sea c un entero positivo. Si $c|e$ y $(c, d) = 1$, entonces $T_{nc,2c}$ es irreducible de orden ec.*

Podemos relacionar este método de construcción de trinomios irreducibles con el caso propuesto anteriormente: todo trinomio irreducible $T_{m,k}$ y tal que $m \equiv \pm 3 \pmod 8$ va a ser una transformación dada por $f(x^p)$ para algún $f(x) = T_{n,2}(x)$.

Teorema 6.7. *Sea $T_{m,k}$ un trinomio irreducible sobre $\mathbb{F}_2$, tal que $m \equiv \pm 3 \pmod 8$. Entonces $T_{m,k}$ es de la forma $T_{np,2p}$ para un natural n tal que $n \equiv \pm 3 \pmod 8$ y un primo impar p tal que $p|e$ y $p \nmid d$, donde e y d denotan al orden y al índice de $T_{n,2}$, respectivamente.*

Tomemos como ejemplo el trinomio $T_{29,2}$, que forma parte de la tabla tomada de [4] que se encuentra a continuación. El índice de $T_{29,2}$ es 1 y su orden es $2^{29} - 1 = 233 \cdot 1103 \cdot 2089$. Entonces para $c \in \{223, 1103, 2089, 223 \cdot 1103, 223 \cdot 2089, 1103 \cdot 2089, 2^{29} - 1\}$, tenemos que $T_{29c,2c}$ es un trinomio irreducible de orden $(2^{29} - 1)c$. Además, se ve claramente que ninguno de estos es primitivo.

Cuadro 6.3: $n < 500$ tales que $T_{n,2}$ es primitivo sobre $\mathbb{F}_2$

n	3	5	11	21	29	35	93	123	333

Si realizamos una búsqueda por ordenador, podemos observar que el número de trinomios $T_{n,1}$ irreducibles es significativamente mayor que el de $T_{n,2}$. En [14] y [20] podemos ver que el número de polinomios irreducibles y de grado menor que 300000 para cada caso es 44 para $T_{n,1}$ y 22 para $T_{n,2}$. Además, los n más cercanos a 300000 (con $n < 300000$) para los que estos polinomios son irreducibles son respectivamente 248833 y 80141. Esto sugiere que además de haber un menor número de $T_{n,2}$ irreducibles, la tasa con la que este número aumenta es menor que la de $T_{n,1}$.

Una de las razones por la que esto ocurre puede ser porque se pueden construir polinomios del tipo $T_{n,1}$ a partir de otros, pero no hay un método análogo para $T_{n,2}$. Otra razón de más peso es la vista en la sección anterior: debido al Teorema 6.1 y a que hay más no divisores que divisores para los enteros positivos, tenemos que hay pocos trinomios de grado $n \equiv \pm 3 \pmod 8$, que son los únicos posibles para $T_{n,2}$ irreducible.

Entre los polinomios $T_{n,1}$ primitivos que generan otros irreducibles, se encuentra el caso ya discutido en el capítulo de polinomios primitivos en el que el grado del polinomio es un primo p exponente de un primo de Mersenne $2^p - 1$. En [23] podemos encontrar una tabla en la que se listan los trinomios $T_{p,k}$ irreducibles para todos los p que sean un exponente de Mersenne conocido y de forma que $k < p/2$ (debido a la propiedad sobre polinomios recíprocos vista en 4.22):

Cuadro 6.4: p primos tales que $2^p - 1$ es primo y k para los que $T_{p,k}$ es irreducible

p	2	3	5	7	13	17	19	31	61	89	107	127
k	1	1	2	1,3	X	3, 5, 6	X	3,6,7,13	X	38	X	1, 7, 15, 30, 63

521	607	1279	2203	2281	3217	4253
32, 48, 158, 168	105, 147, 273	216, 418	X	715, 915, 1029	67, 576	X

4423	9689	9941	11213
271, 369, 370, 649, 1393, 1419, 2098	84, 471, 1836, 2444, 4187	X	X

Por el Teorema 4.23, todos los $T_{p,k}$ que están listados en la tabla anterior son polinomios primitivos sobre $\mathbb{F}_2$. Por tanto, los polinomios $T^{\alpha}_{p,k}$ son irreducibles.

Para finalizar la sección, vamos a dar un algoritmo estándar para comprobar la primalidad de trinomios irreducibles. Este está basado en el Teorema 5.1 aplicado sobre $\mathbb{F}_2$. Sustituimos la condición $f|(x^{q^n} - x)$ por $x^{q^n} \equiv x \pmod{f}$.

Teorema 6.8. *Sea f un polinomio sobre $\mathbb{F}_2$ de grado $n > 1$. Entonces f es irreducible si y solo si se verifican la condiciones siguientes:*

1. $x^{2^n} \equiv x \pmod{f}$.
2. $mcd(f, x^{2^i} - x) = 1$ *para todo* i *tal que* $1 \leqslant i < n$.

Cuando n es un número primo, la condición 2 se vuelve trivial. Si f cumple 1 y tiene un factor irreducible de grado d, entonces por el Lema 2.12, tenemos que $d|n$. Si $d \neq n$, entonces $d = 1$. No obstante, comprobar la irreducibilidad de un polinomio con un factor de grado 1 es trivial, sin más dificultad que evaluar el valor de este en 0 y en 1. Entonces resulta muy sencillo calcular la irreducibilidad de trinomios de grado primo. En [2] se da como dato que el algoritmo que se obtine de manera natural a partir de este criterio obtiene la irreducibilidad de un trinomio en un tiempo lineal con su grado:

Teorema 6.9. *Sean n un número primo y k un natural tal que $n < k < 0$. Entonces el algoritmo que detetermina si $x^{2^n} \equiv x \pmod{T_{n,k}}$ elevando al cuadrado iterativamente al elemento $x \pmod{T_{n,k}}$, determina también si $T_{n,k}$ es irreducible sobre $\mathbb{F}_2$ en $O(n)$ operaciones y con un espacio requerido de $O(n)$.*

6.3. Pentanomios sobre $\mathbb{F}_2$

En el Corolario 6.2, así como en distintas búsquedas por ordenador, hemos encontrado numerosos grados para los que no existen trinomios irreducibles. La motivación

de esta sección se encuentra en buscar pentanomios irreducibles para los grados en los que no existen trinomios irreducibles. Recordamos la conjetura mencionada al principio del capítulo, que dice que sí podemos obtener pentanomios irreducibles para dichos grados. De esta forma, no sería necesario considerar otros polinomios a la hora de realizar operaciones algebraicas sobre $\mathbb{F}_2$.

Un resultado que podemos ver en [7] nos da un criterio de irreducibilidad para dos familias de pentanomios recíprocas:

Teorema 6.10. *Sean s y n enteros positivos tales que s es par y $n > 3s$. Tomamos dos polinomios $f(x) = x^n + x^{3s} + x^{2s} + x^s + 1$ y $g(x) = x^n + x^{n-3s} + x^{n-2s} + x^{n-s} + 1$. Si $n \not\equiv \pm 1 \pmod 8$, entonces f y g son reducibles en $\mathbb{F}_2[x]$.*

Con el objetivo de entender la distribución de los polinomios irreducibles en estas familias, G. Kapetanakis [7] utiliza SageMath para determinar la irreducibilidad de todos estos polinomios para $7 \leqslant n \leqslant 3000$ y todo s natural par válido. Denominaremos **pentanomios de clase 2** a las familias de polinomios en las condiciones del Teorema 6.10.

Se comprueban un total de 374250 polinomios, de los cuales 804 son irreducibles. Concluye que su distribución es mayormente equitativa para los posibles valores (congruencias módulo 8) de n y s considerados de forma independiente: hay 401 polinomios irreducibles para $n \equiv 1 \pmod 8$ y 403 para $n \equiv -1 \pmod 8$. Según el valor de s, tenemos 214 si $s \equiv 2 \pmod 8$, 188 si $s \equiv 4 \pmod 8$, 198 si $s \equiv 6 \pmod 8$ y 204 si $s \equiv 0 \pmod 8$.

También es interesante notar que la irreducibilidad de este tipo de polinomios es más frecuente que la de polinomios cualesquiera. Más concretamente, alrededor del 0,43 % de los pentanomios de clase 2 y de grado n tales que $7 \leqslant n \leqslant 3000$ son irreducibles sobre $\mathbb{F}_2$, mientras que un polinomio arbitrario del mismo grado resulta ser irreducible sobre este intervalo en un 0,13 % de las ocasiones, y esta proporción no aumenta significativamente al restringimos a polinomios sin raíces en $\mathbb{F}_2$.

El Teorema 6.10 nos dice que de los únicos pentanomios de clase 2 irreducibles son aquellos en los que s es impar o $n \equiv \pm 1 \pmod 8$. No obstante, al considerar s impar, la búsqueda por ordenador realizada por el autor no encontró ningún polinomio irreducible de clase 2 cuando $8|n$, y obtuvo muy pocos cuando $n \equiv \pm 3 \pmod 8$, de forma similar a como ocurría para trinomios.

Con el objetivo de comparar la relevancia de los trinomios y pentanomios irreducibles con la de un polinomio irreducible cualquiera, podemos intentar comparar su número total y su aumento para cada grado n. Recordamos que en el Teorema 5.20 damos una fórmula para calcular el número de polinomios irreducibles de grado n sobre cualquier cuerpo finito. No disponemos de una fórmula semejante para restringirnos al caso de trinomios y pentanomios, así que nos valemos de los datos obtenidos por ordenador en [19] para trinomios y [16] para pentanomios, además de tomar los datos de [15] sobre el total de polinomios irreducibles con el fin de evitar los cálculos. Consideramos los grados $1 < n < 30$.

Cuadro 6.5: Polinomios irreducibles de grado n sobre $\mathbb{F}_2$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Totales	2	1	2	3	6	9	18	30	56	99	186	335	630	1161	2182
Trinomios	0	1	2	2	2	3	4	0	4	2	2	4	0	2	6
Pentanomios	0	0	0	1	4	6	10	17	22	38	46	54	66	73	98

16	17	18	19	20	21	22	23	24	25
4080	7710	14532	27594	52377	99858	190557	364722	698870	1342176
0	6	5	0	4	4	2	4	0	4
94	152	124	158	199	184	226	296	202	406

26	27	28	29	30
2580795	4971008	9586395	18512790	35790267
0	0	8	2	4
328	334	418	380	486

Podemos observar que el número de pentanomios irreducibles aumenta considerablemente más despacio que el de polinomios arbitrarios. Por otro lado, el número de trinomios irreducibles es 0 para una gran cantidad de grados, mientras que en el resto no se puede encontrar una tendencia de crecimiento. Es más, en [19], donde se lista el número de trinomios irreducibles hasta el grado 100, la mayor cantidad se observa en el grado $n = 84$, con un total de 14.

Como nota adicional, es curioso notar que si para un natural n el número de trinomios irreducibles es impar, entonces n es par y además el polinomio $x^n + x^{n/2} + 1$ es irreducible. Esto ocurre como consecuencia del Teorema 4.22, y notando que solo puede haber trinomios autorecíprocos cuando n es par.

Capítulo 7

Factorización de polinomios

Ya hemos visto como se pueden identificar y construir polinomios irreducibles sobre $\mathbb{F}_q[x]$. Recordamos que los anillos de polinomios sobre cuerpos son dominios de factorización única, y nos proponemos buscar métodos para describir polinomios arbitrarios como un producto de polinomios irreducibles. Como caso particular, vamos a trabajar al final del capítulo con el n-ésimo polinomio ciclotómico, Φ_n, que es uno de los factores del polinomio $x^n - 1$. En esta parte vamos a tomar como referencia [11] y [18].

7.1. El algoritmo de Berlekamp

La idea en la que se basa el algoritmo que buscamos es sencilla. Partimos de un polinomio que queremos factorizar, $f(x)$, y tomamos otro polinomio $g(x)$. En el caso en el que $f(x)|(g(x)^p - g(x))$, a partir de una factorización de $g(x)^p - g(x)$ podemos obtener también otra de $f(x)$. Idealmente, queremos ser capaces de factorizar $g(x)^p - g(x)$ como producto de irreducibles, de forma que podamos extraer los factores irreducibles correspondientes a f (aunque sea sin contar su multiplicidad). En primer lugar, veamos una caracterización de esta condición:

Lema 7.1. *Sean $f(x) \in \mathbb{F}_q[x]$ un polinomio mónico y $q(x) \in \mathbb{F}_q[x]$ un polinomio cualquiera. Entonces las siguientes propiedades son equivalentes:*

$$g(x)^q \equiv g(x) \pmod{f(x)} \tag{7.1}$$

$$f(x) | \prod_{s \in \mathbb{F}_q} (g(x) - s) \tag{7.2}$$

$$f(x) | \prod_{s \in \mathbb{F}_q} mcd(f(x), g(x) - s) \tag{7.3}$$

Demostración. Recordemos que $x^q - x$ se descompone en $\mathbb{F}_q[x]$ como $\prod_{s \in \mathbb{F}_q}(x - s)$

(Lema 2.4). Si componemos ambas expresiones con $g(x)$, obtemos que

$$g(x)^q - g(x) = \prod_{s \in \mathbb{F}_q} (g(x) - s)$$

Es evidente que el que se cumpla la congruencia (7.1) equivale a que f divida a la expresión anterior, esto es, que se cumpla (7.2). La expresión de (7.3) se puede obtener al ver que la divisibilidad por $f(x)$ no cambia al eliminar factores irreducibles que no se encuentren en f. □

Una vez visto esto, podemos ver que $f(x)$ no es solo un factor del producto anterior, sino que se obtiene de manera exacta a partir de él:

Teorema 7.2. *Sea $f(x)$ un polinomio mónico sobre $\mathbb{F}_q$ y sea $g(x) \in \mathbb{F}_q[x]$ verificando*

$$g(x)^q \equiv g(x) \pmod{f(x)}$$

Entonces

$$f(x) = \prod_{s \in \mathbb{F}_q} mcd(f(x), g(x) - s) \tag{7.4}$$

Además, los factores $mcd(f(x), g(x) - s)$ con $s \in \mathbb{F}_q$ del producto descrito son coprimos dos a dos.

Demostración. Empecemos viendo la coprimalidad de estos factores.
Sean $s_1 \neq s_2 \in \mathbb{F}_q$.Tenemos que $(g(x) - s_1) - (g(x) - s_2) = s_2 - s_1 \neq 0$ y es una unidad en $\mathbb{F}_q$. Por tanto $g(x) - s_1$ y $g(x) - s_2$ son coprimos, e inmediatamente $\mathrm{mcd}(f(x), g(x) - s_1)$ y $\mathrm{mcd}(f(x), g(x) - s_2)$ también. Es trivial que $\mathrm{mcd}(f(x), g(x) - s) | f(x)$ para cualquier $s \in \mathbb{F}_q$ y estos son coprimos dos a dos. En consecuencia

$$\prod_{s \in \mathbb{F}_q} \mathrm{mcd}(f(x), g(x) - s) | f(x)$$

Utilizando la fórmula (7.3) del lema anterior, tenemos que

$$f(x) | \prod_{s \in \mathbb{F}_q} \mathrm{mcd}(f(x), g(x) - s)$$

con lo que concluimos la demostración. □

Es importante notar que la factorización dada por el teorema no tiene por qué ser de factores irreducibles, y además tampoco es necesariamente propia. Por ejemplo, cuando $g(x) \equiv s_0 \pmod{f(x)}$ para algún $s_0 \in \mathbb{F}_q$, trivialmente $s_0^q = s_0$ y además $\mathrm{mcd}(f(x), g(x) - s) = 1$ siempre que $s \neq s_0$:

$$f(x) = \prod_{s \in \mathbb{F}_q} \mathrm{mcd}(f(x), g(x) - s) =$$

$$= \mathrm{mcd}(f(x), g(x) - s_0) \prod_{s \neq s_0} \mathrm{mcd}(f(x), g(x) - s) =$$

$$= f(x) \prod_{s \neq s_0} 1$$

Definición 7.3. *Sean $f(x)$ y $g(x)$ un polinomios sobre $\mathbb{F}_q$ de forma que $f(x)$ es mónico y $g(x)^q \equiv g(x) \pmod{f(x)}$. Si la factorización dada por el Teorema 7.2 es propia, diremos que $g(x)$ es un **polinomio f-reductor**.*

Un caso evidente de polinomio f-reductor se puede obtener cuando $g(x)$ verifica (7.1) y $0 < \mathrm{gr}(g) < \mathrm{gr}(f)$. Por ejemplo, si tomamos $f(x) = x^7 + x^3 + x + 1$ y $g(x) = x^4 + x + 1$ sobre $\mathbb{F}_2$, se puede ver que $g(x)$ es f-reductor.

Una noción importante a la hora de considerar polinomios reductores como método de factorización, es que siempre puede tomarse al menos uno. Tenemos como resultado [11, Teorema 4.3], que nos asegura que este es el caso cuando f tiene una factorización propia.

Teorema 7.4. *Sea $f(x)$ un polinomio reducible sobre $\mathbb{F}_q$, y sea N el menor entero positivo tal que $x^N \equiv x \pmod{f(x)}$. Denotamos $T(x) = x + x^q + \cdots + x^{q^{N-1}}$ y sea $T_i(x) = T(x^i)$. Entonces $T_i(x)$ es un polinomio f-reductor para algún i entre 0 y $N-1$.* □

Podemos tomar el polinomio $f(x)$ de forma que no tenga factores repetidos: si $f(x)$ tiene factores repetidos, entonces $d(x) = \mathrm{mcd}(f(x), f'(x)) \neq 1$ y tenemos que $f(x)/d(x)$ sí que es libre de repeticiones. Además, podemos repetir el proceso sobre $d(x)$, de forma que se obtiene la factorización de $f(x)$ a partir de divisores suyos con todos los factores irreducibles distintos. Esto es de gran utilidad al considerar otra familia específica de polinomios reductores con la que podemos diseñar un algoritmo de factorización. Este está basado en el siguiente resultado, cuya demostración está en [11, Teorema 4.5].

Teorema 7.5. *Sea $f(x)$ un polinomio reducible y sin factores repetidos sobre $\mathbb{F}_q$, de forma que $f(0) \neq 0$ y $ord(f) = e$. Sea m_i el menor entero positivo tal que $x^{iq^{m_i}} \equiv x^i \pmod{f(x)}$ para cada $i \geqslant 0$. Denotamos $R_i(x) = x^i + x^{iq} + \cdots + x^{iq^{m_i-1}}$. Entonces aplicar la factorización de (7.4) con cada R_i, $1 \leqslant i < e$,* da como resultado la factorización en polinomios irreducibles de $f(x)$. □

Es importante notar que el método dado por el Teorema 7.2 requiere el cálculo de q máximos comunes divisores, por lo que su uso no resulta viable computacionalmente para cuerpo finitos grandes.

El cálculo de los polinomios f-reductores está justificado por su utilidad a la hora de obtener factorizaciones propias. Adicionalmente, calcular el número posible de estos simplifica la factorización en irreducibles de f, pues está directamente relacionado con el número de factores irreducibles distintos que lo dividen:

Teorema 7.6. *Sea $f(x)$ un polinomio mónico de grado $n \geqslant 1$ sobre $\mathbb{F}_q$. Si $f(x)$ es producto de potencias positivas de r polinomios irreducibles mónicos distintos, entonces el número de soluciones de $x^q - x = 0$ en $\mathbb{F}_q[x]/(f(x))$ es q^r.*

Demostración. Consideramos la factorización en irreducibles de f

$$f(x) = p_1(x)^{e_1} \dots p_r(x)^{e_r}$$

Por el Lema 7.1, $g(x)$ es solución de $x^q - x = 0$ si y solo si verifica (7.2), esto es

$$f(x) | \prod_{s \in \mathbb{F}_q} (g(x) - s)$$

Por ser los $g(x) - s$ coprimos dos a dos, cada $p_i(x)$ solo divide a uno de ellos, y lo hace e_i veces. Para cada $1 \leqslant i \leqslant r$ denotamos s_i de forma que

$$g(x) \equiv s_i \pmod{p_i(x)^{e_i}} \tag{7.5}$$

De esta forma, tenemos una correspondencia entre los elementos $g(x)$ que verifican (7.1) y las r-tuplas de $\mathbb{F}_q$ $(s_1, \dots, s_r)$, $s_i \in \mathbb{F}_q$ para todo i. Como el número total de estas r-tuplas es q^r, si demostramos que la correspondencia es biyectiva, habremos terminado el resultado.

Veamos la correspondencia recíproca. Sea $(s_1, \dots, s_r)$ una r-tupla de elementos de $\mathbb{F}_q$. Como los $p_i(x)^{e_i}$ son coprimos dos a dos en $\mathbb{F}_q[x]$, podemos aplicar el Teorema Chino de los Restos: existe un elemento $g(x) \in \mathbb{F}_q[x]$ tal que $g(x) \equiv s_i \pmod{p_i(x)^{e_i}}$ para todo i. Bajo estas condiciones, $g(x)$ cumple (7.2) y por tanto (7.1). De nuevo por el Teorema Chino de los Restos, todos los elementos que cumplan $g(x) \equiv s_i \pmod{p_i(x)^{e_i}}$ para todo i serán congruentes entre sí módulo $\operatorname{mcm}(p_1(x)^{e_1}, \dots, p_r(x)^{e_r})$, es decir, módulo $f(x)$. Concluimos que esta correspondencia en inyectiva módulo $f(x)$ y por tanto en $\mathbb{F}_q[x]/(f(x))$, y concluimos que es biyectiva por estar definida sobre un conjunto finito. □

Si $f(x)$ es un polinomio mónico de grado n, podemos considerar $\mathbb{F}_q[x]/(f(x))$ como un espacio vectorial de dimensión n sobre $\mathbb{F}_q$ y de base $\{1, x, \dots, x^{n-1}\}$. Tenemos que los elementos $g(x)$ tales que $g(x)^q \equiv g(x) \pmod{f(x)}$ forman un subespacio vectorial de $\mathbb{F}_q[x]/(f(x))$. Si tomamos las potencias q-ésimas de los elementos de la base, obtenemos elementos x^{qi}, $1 \leqslant i \leqslant n-1$, que se pueden expresar en función de coordenadas dadas por la misma base:

$$x^{qi} = \sum_{j=0}^{n-1} b_{i,j} x^i$$

Los elementos $b_{i,j}$ forman una matriz cuadrada de rango n a la que denotaremos B. Entonces un polinomio f-reductor sobre $\mathbb{F}_q[x]/(f(x))$ $g(x) = \sum_{i=0}^{n-1} a_i x^i$ cumple

$$g(x)^q = \sum_{i=0}^{n-1} a_i x^{qi} = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_{i,j} x^j = \sum_{i=0}^{n-1} a_i x^i = g(x)$$

Esto equivalente a resolver un sistema dado por

$$(a_0, \dots, a_{n-1}) B = (a_0, \dots, a_{n-1})$$

o, expresándolo como un sistema de ecuaciones lineales homogéneas,

$$(a_0, \ldots, a_{n-1})(B - I) = (0, \ldots, 0) \tag{7.6}$$

Las soluciones del sistema anterior forman el núcleo de la matriz $B - I$, que sabemos por el teorema previo que tiene dimensión r como espacio vectorial sobre $\mathbb{F}_q$. Por tanto, si k denota el rango de $B - I$, entonces $r = n - k$. Procedemos a construir una base del núcleo de $B - I$, denotada $\{h_1(x), \ldots, h_r(x)\}$. Podemos tomar $h_1(x) = 1$, pues está en el núcleo de forma trivial. Entonces el resto de los h_i tiene grado positivo y son polinomios f-reductores. Si realizamos iterativamente las factorizaciones dadas por $\mathrm{mcd}(f(x), h_i(x))$, se acabarán obteniendo una expresión con r potencias de irreducibles distintos, como veremos más adelante.

Definición 7.7. *El proceso de factorización dado por aplicar la factorización del Teorema 7.2 con los polinomios f-reductores obtenidos al resolver (7.6) es conocido como el* ***algoritmo de Berlekamp****.*

Como ejemplo, vamos a usar el algoritmo de Berlekamp para factorizar el trinomio $f(x) = x^5 + x^4 + 1$ en $\mathbb{F}_2[x]$. En primer lugar, tenemos que calcular $x^{2i} \pmod{f(x)}$ para $0 \leqslant i \leqslant 4 = \mathrm{gr}(f) - 1$. Tenemos que:

$$\begin{aligned}
x^0 &\equiv 1 \\
x^2 &\equiv x^2 \\
x^4 &\equiv x^4 \\
x^6 &\equiv 1 + x + x^4 \\
x^8 &\equiv 1 + x + x^2 + x^3 + x^4
\end{aligned}$$

Entonces

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad B - I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Podemos comprobar que $B - I$ tiene rango 3, por lo que podemos obtener 2 elementos linealmente independientes sobre $\mathbb{F}_2$ en el núcleo de $B - I$. Tomamos como base

$$h_1 = (1, 0, 0, 0, 0); \quad h_2 = (0, 0, 1, 1, 1)$$

Los polinomios correspondientes son $h_1(x) = 1$, $h_2(x) = x^2 + x^3 + x^4$. Como solo $h_2(x)$ es reductor, procedemos a calcular el máximo comun divisor de $f(x)$ y $h_2(x) - c$ para todo $c \in \mathbb{F}_2$, esto es, $h_2(x)$ y $h_2(x) - 1$:

$$\begin{aligned}
x^5 + x + 1 &= x(x^4 + x^3 + x^2) + (x^4 + x^3 + x + 1) \\
x^4 + x^3 + x^2 &= 1(x^4 + x^3 + x + 1) + (x^2 + x + 1) \\
x^4 + x^3 + x + 1 &= x^2(x^2 + x + 1) + (x^2 + x + 1)
\end{aligned}$$

Tenemos que $(f(x), h_2(x)) = x^2 + x + 1$. Entonces tenemos un factor irreducible de $f(x)$ y obtenemos una factorización de $f(x)$:

$$f(x) = x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$$

Como $x^3 + x + 1$ es evidentemente irreducible, no es necesario continuar con la factorización. Además, podemos confirmar que hemos conseguido la factorización buscada viendo que el número de factores coincide con el número de elementos de la base del núcleo.
En el caso en el que no pudiera verse de forma inmediata la irreducibilidad y no hubiera el número necesario de factores, entonces se continuaría calculando los máximos comunes divisores de los factores de f obtenidos y $h_2(x) - 1$.

El siguiente resultado, va a demostrar que, en efecto, el algoritmo de Berlekamp descompone el polinomio $f(x)$ en un producto de potencias de r irreducibles.

Teorema 7.8. *Sea $f(x)$ un polinomio reducible mónico sobre $\mathbb{F}_q$ y sean $h_1(x), \ldots, h_r(x)$ los elementos que forman la base del núcleo de la matriz $B - I$ en el algoritmo de Berlekamp. Entonces los factores propios de $f(x)$ dados por la factorización de* (7.4) *para cada $h_i(x)$ son r potencias distintas de factores irreducibles.*

Demostración. Consideramos dos factores irreducibles mónicos de $f(x)$, siendo estos $f_1(x)$ y $f_2(x)$. Entonces podemos considerar que para $1 \leqslant i \leqslant r$, $h_i(x) \equiv s_{i,j} \pmod{f_j(x)}$ para $j = 1, 2$ y para algún $s_{i,j} \in \mathbb{F}_q$.

Claramente $s_{i,1} \neq s_{i,2}$ para algún i. En caso contrario, tendríamos que, como cualquier polinomio $h(x)$ solución de $x^q - x$ en $\mathbb{F}_q[x]/(f(x))$ sería una combinación lineal de los $h_i(x)$ con coeficientes en $\mathbb{F}_q$, entonces $h(x) \equiv a_h \pmod{f_1(x)}$ y $h(x) \equiv a_h \pmod{f_2(x)}$ para algún $a_h \in \mathbb{F}_q$. Este elemento a_h vendría dado por la suma de los coeficientes de cada $h_i(x)$ multiplicado por el $s_{i,1}$ (o equivalentemente $s_{i,2}$) correspondiente.

No obstante, por el Teorema Chino de los Restos, podemos conseguir $h(x)$ una solución de $x^q - x \pmod{f(x)}$ de forma que esto no se cumpla, por ejemplo con $h(x) \equiv 0 \pmod{f_1(x)}$ y $h(x) \equiv 1 \pmod{f_2(x)}$.

Sea i un natural tal que $s_{i,1} \neq s_{i,2}$. Tenemos que

$$h_i(x)^q - h_i(x) = \prod_{s \in \mathbb{F}_q} (h_i(x) - s)$$

y cada factor irreducible de $f(x)$ divide a un único elemento $h_i(x) - s$, pues vimos en la demostración del Teorema 7.2 que estos son coprimos entre sí. Por tanto,
$h_i(x) \equiv s_{i,j} \pmod{f_j(x)}$, de forma que $s_{i,1} \neq s_{i,2}$ y deducimos que
$h_i(x) - s_{i,1} \equiv 0 \pmod{f_1(x)}$ y $h_i(x) - s_{i,1} \equiv s_{i,2} - s_{i,1} \not\equiv 0 \pmod{f_2(x)}$. Esto es, $f_1(x)$ divide a $h_i(x) - s_{i,1}$ y no divide a $h_i(x) - s_{i,2}$. En consecuencia, $h_i(x)$ separa a $f_1(x)$ y $f_2(x)$ en la factorización de (7.4). Como $f(x)$ tiene r factores irreducibles por el Teorema 7.6, hemos terminado el resultado. □

Lo único que nos falta para terminar el proceso de factorización es ser capaces de extraer un polinomio irreducible a partir de una potencia suya. Para esto recurrimos al siguiente teorema, cuya demostración resulta intuitiva:

Teorema 7.9. *Sea $f(x)$ una potencia de un polinomio irreducible mónico sobre $\mathbb{F}_q$. Supongamos que $f'(x) \neq 0$. Si $mcd(f(x), f'(x)) = 1$, entonces $f(x)$ es irreducible. En caso contrario, tenemos que $f(x)/mcd(f(x), f'(x))$ es irreducible.*

Demostración. El único caso en el que $f'(x) = 0$ es aquel en el que cada índice i con un coeficiente a_i no nulo de $f(x) = \sum_{i=0}^{n} a_i x^i$ es un múltiplo de la característica de $\mathbb{F}_q$, a la que denotamos p. Entonces $f(x) = h(x)^p$ para algún polinomio $h(x) \in \mathbb{F}_q[x]$. Podemos iterar este proceso hasta obtener un polinomio con derivada no nula.

Podemos suponer que $f'(x) \neq 0$. Sean $p(x)$ un polinomio irreducible y e un natural tales que $p(x)^e = f(x)$.

Si $\mathrm{mcd}(f(x), f'(x)) = 1$, entonces $p(x)^e$ no tiene raíces múltiples, por lo que $e = 1$ y $f(x) = p(x)$.

Si $\mathrm{mcd}(f(x), f'(x)) \neq 1$, entonces $f'(x) = ep(x)^{e-1}p'(x)$. Como $p(x) \nmid p'(x)$, tenemos que $\mathrm{mcd}(f(x), f'(x)) = p(x)^{e-1}$. Se puede calcular de manera inmediata que $p(x) = f(x)/p(x)^{e-1}$. □

7.2. Polinomios ciclotómicos

Vamos a utilizar esta sección para estudiar una factorización propia del polinomio $x^n - 1$ en $\mathbb{F}_q$. Sin perder generalidad, podemos suponer que $\mathrm{mcd}(n, q) = 1$, esto es, si denotamos por p a la característica de $\mathbb{F}_q$, tenemos que $p \nmid n$. En caso contrario, podemos considerar $x^n - 1 = (x^{n'} - 1)^{p^k}$, de forma que $\mathrm{mcd}(n', q) = 1$.

Es inmediato ver que todas las raíces de $f(x) = x^n - 1$ van a tener orden divisor de n. De manera recíproca, si un elemento de algún cuerpo de descomposición de $x^n - 1$ tiene orden divisor de n, entonces es raíz de este polinomio.
Por otro lado, tenemos que $f'(x) = nx^{n-1}$. Estamos suponiendo que $\mathrm{mcd}(n, p) = 1$, con lo que $f'(x) \neq 0$. Deducimos que $f(x)$ no tiene raíces múltiples, pues $\mathrm{mcd}(x^n - 1, x^{n-1}) = 1$.

Denotamos por $K^{(n)}$ al cuerpo de descomposición del polinomio $x^n - 1$ (sobre $\mathbb{F}_q$), llamado n-ésimo cuerpo ciclotómico. Podemos calcular este cuerpo, siendo de la forma $K^{(n)} = \mathbb{F}_{q^m}$, donde m es el menor entero positivo tal que $q^m \equiv 1 \pmod{n}$. Esto es debido a que podemos obtener un elemento de orden n sobre este cuerpo: si ξ es un elemento primitivo de $\mathbb{F}_{q^m}$, entonces $\xi^{(q^m-1)/n}$ es un elemento de orden n. De este modo, podemos obtener todas las raíces de $x^n - 1$, pues un elemento de orden n genera el único subgrupo multiplicativo de orden n, cuyos elementos son las n raíces buscadas de $x^n - 1$.

Bajo estas condiciones, podemos obtener la descomposición de $x^n - 1$ en $K^{(n)}$:

$$x^n - 1 = \prod_{\substack{\alpha \in K^{(n)} \\ \mathrm{ord}(\alpha) | n}} (x - \alpha)$$

Si notamos que las raíces n-ésimas de la unidad forman un grupo (multiplicativo) cíclico de orden n, entonces podemos denotar por ξ a una de esas raíces que sea generadora de dicho grupo, y por tanto de orden n. Diremos que ξ es una n-raíz primitiva de la unidad. En este caso, obtenemos la descomposición

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \xi^i) \tag{7.7}$$

El resultado que queremos demostrar es que los factores propios de $x^n - 1$ se pueden obtener separando sus raíces según su orden.

Definición 7.10. *Sean n un número natural y $\xi \in K^{(n)}$ una n-raíz primitiva de la unidad. Definimos el n-ésimo polinomio ciclotómico como*

$$\Phi_n(x) = \prod_{\substack{0 \leqslant i \leqslant n-1 \\ ord(\xi^i) = n}} (x - \xi^i) = \prod_{\substack{0 \leqslant i \leqslant n-1 \\ mcd(n,i) = 1}} (x - \xi^i)$$

Es evidente que el n-ésimo polinomio ciclotómico tiene orden n. También es inmediato que los polinomios ciclotómicos de órdenes divisores de n factorizan propiamente a $x^n - 1$:

$$x^n - 1 = \prod_{d | n} \Phi_d(x)$$

A continuación, vamos a ver que los polinomios ciclotómicos son polinomios sobre $\mathbb{F}_q$. En particular, tienen todos sus coeficientes sobre $\mathbb{F}_p$. Para ello, recordamos la fórmula de inversión de Möbius (Teorema 5.18):
Sea f una función aritmética y sea $F(n) = \sum_{d|n} f(d)$. Entonces

$$f(n) = \sum_{d | n} F(d) \mu\left(\frac{n}{d}\right)$$

Este resultado puede ser ampliado a productos de funciones aritméticas en lugar de sumas:

Teorema 7.11 (Fórmula multiplicativa de inversión de Möbius)**.** *Sea f una función aritmética y sea $F(n) = \prod_{d|n} f(d)$. Entonces*

$$f(n) = \prod_{d | n} F(d)^{\mu\left(\frac{n}{d}\right)}$$

Demostración. Basta considerar las funciones aritméticas $ln(f)$ y $ln(F)$, que se encuentran bajo las condiciones de la fórmula de inversión de Möbius. □

Con esta fórmula, somos capaces de calcular los polinomios ciclotómicos y obtener el resultado buscado.

Teorema 7.12. *Para todo n natural, el polinomio $\Phi_n(x)$ tiene coeficientes enteros. Por tanto, si se considera como polinomio sobre el cuerpo finito $\mathbb{F}_q$, entonces tiene todos sus coeficientes sobre el subcuerpo primo.*

Demostración. Sabemos que $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Podemos considerar que ambas son funciones aritméticas, por lo que podemos aplicar el Teorema 7.11 y calcular $\Phi_n(x)$:

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)}$$

Entonces $\Phi_n(x)$ es un cociente de polinomios mónicos con coeficientes enteros, y por tanto tiene coeficientes enteros.
La segunda parte del teorema se deduce de forma trivial al considerar las operaciones sobre $\mathbb{F}_p$. □

Para finalizar, vamos a facilitar la factorización completa de $x^n - 1$ añadiendo un par de resultados de [18] que sirven para calcular el número de factores irreducibles de los polinomios ciclotómicos.

Teorema 7.13. *Sea $q = p^e$ una potencia positiva de un primo y sean n y m naturales tal que $p \nmid n$ y m es el menor entero positivo tal que $q^m \equiv 1 \pmod{n}$. Entonces el n-ésimo polinomio ciclotómico $\Phi_n(x)$ es producto de $\phi(n)/m$ polinomios irreducibles mónicos de grado m.*

Con este resultado ya podemos calcular el número de factores irreducibles de $x^n - 1$. Si suponemos que p y n son coprimos, entonces el número de factores irreducibles distintos t viene dado por

$$t = \prod_{d|n} \phi(d)/m_d$$

donde m_d denota el menor entero positivo tal que $q^{m_d} \equiv 1 \pmod{d}$. Por otro lado, cuando $n = p^k n'$ para n' y p coprimos, entonces el producto en el que se sustituye n por n' denota el número de factores irreducibles con multiplicidad p^k de $x^n - 1$.

Como corolario, sabemos que los polinomios ciclotómicos son irreducibles en el caso en el que m_n y $\phi(n)$ coinciden.

Corolario 7.14. *Sea $q = p^e$ una potencia positiva de un primo y sea n un natural tal que $p \nmid n$. Entonces el n-ésimo polinomio ciclotómico $\Phi_n(x)$ es irreducible si y solo si $\phi(n)$ es el menor entero positivo de los m que cumplen que $q^m \equiv 1 \pmod{n}$.*

Capítulo 8

Clausura algebraica de los cuerpos finitos

Uno de los primeros resultados que hemos visto al principio de este trabajo es la existencia de extensiones algebraicas de grado cualquiera para un cuerpo finito arbitrario. Como consecuencia de esto, es evidente que la clausura algebraica de un cuerpo no puede ser nunca un cuerpo finito. Con el fin de describir la estructura básica de estas clausuras algebraicas, vamos a recurrir a resultados de *Topics in Galois Fields* [6]. Comenzamos recordando a modo de preliminares algunos conceptos de extensiones algebraicas.

Definición 8.1.

- *Sean K un cuerpo y E una extensión de K. Definimos la* ***clausura algebraica relativa*** *de K en E como*

$$cl(E/K) = \{\alpha \in E \ : \ \alpha \text{ es algebraico sobre } K\}$$

  Además, decimos que K es ***algebraicamente cerrado en*** *E si $cl(E/K) = E$.*

- *Sea K un cuerpo. Decimos que K es* ***algebraicamente cerrado*** *si todo polinomio sobre $K[x]$ tiene una raíz en K, o equivalentemente, si todo polinomio sobre $K[x]$ se descompone en K.*

- *Sean K un cuerpo y $\widehat{K}$ una extensión de K. Diremos que $\widehat{K}$ es la* ***clausura algebraica*** *de K si $\widehat{K}$ es algebraicamente cerrado y no existe ninguna extensión algebraicamente cerrada entre K y $\widehat{K}$.*

Como parte de la teoría de Galois, se ve que siempre es posible obtener una clausura algebraica, y esta es independiente de cómo se construya. Podemos obtener una demostración de esta propiedad en [6, p. 178-179]:

Teorema 8.2. *Para todo cuerpo K existe una clausura algebraica de K. Además, si $\widehat{K}$ y $\widehat{K}'$ son dos tales clausuras algebraicas, entonces $\widehat{K}$ y $\widehat{K}'$ son isomorfos.*

Después de esta parte introductoria, procemos a ver propiedades sobre los cuerpos finitos. Durante el resto del capítulo, vamos a trabajar con las extensiones del cuerpo finito $\mathbb{F}_q$, al que denotaramos F. Por otro lado, denotaremos por E_n a la extensión de F de grado n.
Introducimos un concepto que relaciona subconjuntos de números naturales con los grados de las extensiones finitas intermedias:

Definición 8.3. *Sea $S \subseteq \mathbb{N}$. Decimos que S es un **número de Steinitz** si para cualesquiera $n, m \in \mathbb{N}$ se verifica:*

- *Si $n \in S$ y $m|n$, entonces $m \in S$.*
- *Si $n, m \in S$, entonces $mcm(n, m) \in S$.*

En particular, el conjunto de extensiones finitas intermedias de una extensión cualquiera de F va a constituir un número de Steinitz. Para demostrar esto, haremos uso de un resultado apoyado por el Lema del alzamiento de bases, presente en el capítulo 3, y que explica como factorizan los polinomios primitivos de un cuerpo sobre sus extensiones. Una demostración alternativa se encuentra en [6, p. 123].

Lema 8.4. *Sea $f(x)$ un polinomio irreducible de grado n sobre $\mathbb{F}_q$. Sean m un natural y $d = mcd(n, m)$. Entonces $f(x)$ es producto de d polinomios irreducibles de grado n/d en $\mathbb{F}_{q^m}[x]$.*

Demostración. Vamos a dividir la demostración en tres casos. Sea α una raíz de $f(x)$.

Si m es un divisor de n, entonces el polinomio irreducible de α sobre $\mathbb{F}_{q^m}$ es de grado n/m, y es evidentemente un divisor irreducible de $f(x)$. Como esto ocurre para todas las raíces de $f(x)$, tenemos que este polinomio se factoriza como un producto de polinomios irreducibles de grado n/m, y su número es evidentemente $m = \text{mcd}(n, m)$.

Si m y n son coprimos, podemos aplicar el Corolario 3.3 a la base polinomial de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ generada por la raíz α, de forma que también es una base de $\mathbb{F}_{q^{nm}}$ sobre $\mathbb{F}_{q^m}$. En particular, el conjunto $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es linealmente independiente, por lo que el polinomio irreducible de α sobre $\mathbb{F}_{q^m}$ es de grado mayor o igual que n. Es evidente que este polinomio es $f(x)$.

Sean m un natural arbitrario, y sea $d = \text{mcd}(n, m)$. Entonces, como en el primer caso, $f(x)$ factoriza en d polinomios irreducibles de grado n/d sobre $\mathbb{F}_{q^d}$. Cada uno de estos polinomios se encuentra en el segundo caso para n/d y m/d naturales coprimos. Entonces los d polinomios obtenidos son irreducibles de grado n/d sobre $\mathbb{F}_{q^{d(m/d)}} = \mathbb{F}_{q^m}$. □

Este lema es de utilidad para calcular el grado de la extensión directamente superior a otras dos. Es decir, si E_n y E_m son dos extensiones de F y α es un elemento primitivo de E_n, entonces podemos calcular el grado de la extensión $E_m(\alpha)/E_m$ mediante el lema.

Esto nos permitirá ver que los grados de las extensiones intermedias cumplen la segunda condición que requieren los números de Steinitz.

Teorema 8.5. *Sea C una extensión de $F = \mathbb{F}_q$. Entonces $N(C/F)$ es un número de Steinitz, donde*

$$N(C/F) = \{n \in \mathbb{N} \ : \ \textit{existe una extensión intermedia de } C/F \textit{ de grado } n \textit{ sobre } F\}$$

Demostración. Sea $n \in N(C/F)$, y consideramos la extensión intermedias E_n. Si m es un divisor de n, entonces por el Teorema 2.5 existe una extensión de F de grado m, denotada E_m. De forma trivial, la extensión de grado $\frac{n}{m}$ de E_m es E_n, por lo que E_m es un cuerpo intermedio de C/F.

Ahora sean $n, m \in N(C/F)$, y sea α un elemento primitivo de E_n, y denotamos por $f(x)$ a su polinomio irreducible de grado n sobre F. Si tomamos $d = \text{mcd}(n, m)$, tenemos que $f(x)$ factoriza en un producto de d polinomios irreducibles de grado n/d sobre E_m por el lema anterior. Entonces

$$[E_m(\alpha) : F] = [E_m(\alpha) : E_m][E_m : F] = (n/d)m = \text{mcm}(n, m)$$

Entonces $E_m(\alpha) = E_{\text{mcm}(n,m)}$, y por tanto $\text{mcm}(n, m) \in N(C/F)$. □

Notemos que el cuerpo dado por $E_m(\alpha)$ siendo α un elemento primitivo de E_n puede ser representado también por $E_m E_n$, y se le llama la composición de los cuerpos E_m y E_n. Esta denota la menor extensión de F que contiene a las otras dos, y es de grado $\text{mcm}(n, m)$.
A continuación, vamos a demostrar que cada número de Steinitz puede dar una extensión algebraica de F. Si consiguiéramos ver que esta extensión es única salvo isomorfismo, entonces quedaría demostrado que hay una correspondencia biyectiva entre las extensiones algebraicas y los números de Steinitz. Veamos la primera parte:

Teorema 8.6. *Sean S un número de Steinitz y F un cuerpo finito. Entonces existe una extensión algebraica de F, A, tal que $N(A/F) = S$.*

Demostración. Si S es finito, basta tomar $A = E_n$ para $n = \text{máx}\{m \ : \ m \in S\}$.

Supongamos que S es infinito. Es sencillo ver que la intersección de dos números de Steinitz es también un número de Steinitz. Vamos a utilizar que S es unión de números de Steinitz finitos para realizar un proceso similar con la extensión algebraica buscada. Denotamos por D_n al número de Steinitz finito cuyos elementos son los divisores de n. En estas condiciones, $D_n \cap S$ es un número de Steinitz finito, y entonces tenemos que $D_n \cap S = D_l$, de forma que $l = \text{máx}\{m \ : \ m \in S \cap D_n\}$.
En este caso, denotamos $l = \text{mcd}(n, S)$. Se puede entender que l es el mayor divisor de n tal que $l \in S$. Consideramos la sucesión $(d_n)_{n \in \mathbb{N}^*}$ dada por

$$d_n = \text{mcd}(n!, S)$$

Claramente $d_n | d_{n+1}$, pues $n!|(n+1)!$. Entonces, para cada $n \in \mathbb{N}$ tomamos K_n una extensión de F de grado d_n. En particular, podemos considerar K_{n+1} es una extensión de K_n de grado d_{n+1}/d_n, y podemos ver a K_n como un subcuerpo de K_{n+1}. Tenemos una cadena creciente de cuerpos, dada por

$$F = K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n \subseteq \ldots$$

Entonces el conjunto

$$A = \bigcup_{n \in \mathbb{N}} K_n$$

es claramente una extensión algebraica de F, pues todos sus elementos son algebraicos sobre F, y además demostraremos que es la extensión buscada, esto es, $N(A/F) = S$.

Sea $m \in N(A/F)$. Existe E_m una extensión intermedia de A/F, de grado m sobre F. En particular, E_m es un subcuerpo de A, por lo que está contenido en K_k (cuyo grado sobre F es d_k) para algún k. Por tanto, $m|d_k$. Por elección de los d_n, estos son elementos de S, y por ser m divisor de d_k, tenemos que $m \in S$.

Sea ahora $m \in S$. Tenemos que $d_m = \text{mcd}(m!, S)$ es el mayor divisor de $m!$ contenido en S, por lo que $m|d_m$. Por tanto, hay un subcuerpo (y por tanto una extensión) de orden m sobre F contenido en $K_m \subseteq A$. Concluimos que $m \in N(A/F)$. □

Para terminar de ver la correspondencia entre números de Steinitz y extensiones intermedias algebraicas, falta ver que toda extensión algebraica de F es isomorfa a la construcción que hemos utilizado en la demostración anterior.

Corolario 8.7. *Sean A y A' dos extensiones algebraicas de un cuerpo finito F, tales que $N(A/F) = N(A'/F)$. Entonces existe un isomorfismo de A en A' que fija los elementos de F.*

Demostración. De forma análoga a como se hizo en el teorema anterior, tomamos $F = K_1 = K_1'$, y consideramos $d_n = \text{mcd}(n!, N(A/F)$ y K_n, K_n' extensiones intermedias de grado d_n de A/F y A'/F respectivamente, tales que

$$A = \bigcup_{n \in \mathbb{N}} K_n \qquad A' = \bigcup_{n \in \mathbb{N}} K_n'$$

Entonces K_n y K_n' son isomorfos y podemos tomar un isomorfismo α_n de K_n en K_n' que fije los elementos de F. Por un resultado de teoría de Galois, este isomorfismo se puede extender a un isomorfismo de K_{n+1} en K_{n+1}' que fija los elementos de F. El isomorfismo buscado es $\alpha = \bigcup_{n \in \mathbb{N}} \alpha_n$. □

Con este par de resultados, hemos probado lo siguiente:

Corolario 8.8. *Existe una correspondencia biyectiva entre los números de Steinitz y las extensiones algebraicas de un cuerpo finito.*

Una consecuencia inmediata es que las únicas extensiones algebraicas posibles para un cuerpo finito F son isomorfas a $\bigcup_{n\in S} E_n$, donde S es un número de Steinitz. En particular, si tenemos una extensión C/F (no necesariamente algebraica), entonces la clausura algebraica de F en C viene dada por

$$\mathrm{cl}(C/F) = \bigcup_{n\in N(C/F)} E_n$$

Para finalizar el capítulo, vamos a determinar la estructura de la clausura algebraica de los cuerpos finitos.

Teorema 8.9. *Sea $F = \mathbb{F}_q$ un cuerpo finito y sea A una extensión algebraica suya. Entonces A es la clausura algebraica de F si y solo si $N(A/F) = \mathbb{N}$, en cuyo caso*

$$A = \bigcup_{n\in\mathbb{N}} E_n$$

Demostración. Supongamos que $A = \widehat{F}$. Entonces para todo $n \in \mathbb{N}$ y para todo polinomio irreducible de grado n en $F[x]$, $f(x)$ se descompone en A. Es evidente que $E_n \subseteq A$, por lo que $n \in N(A/F)$, ergo $\mathbb{N} = N(A/F)$.

Supongamos que $N(A/F) = \mathbb{N}$, y sea $f(x)$ un polinomio en $A[x]$. Tomamos E una extensión algebraica de F que contenga a los coeficientes de $f(x)$, y α una raíz de $f(x)$. Entonces $E(\alpha)$ es una extensión finita y algebraica de F, a la que denotamos $E_m = \mathbb{F}_{q^m}$. Como $N(A/F) = \mathbb{N}$, entonces $m \in N(A/F)$, por lo que A/F tiene una extensión intermedia de grado m sobre F denotada $E_m^{'}$, que es isomorfa a E_m. En particular, como $\alpha \in E_m$, tenemos que existe un elemento $\beta \in E_m^{'}$ isomorfo a α, de forma que $\beta \in A$. Entonces $f(x)$ tiene como raíz a $\beta \in A$, como queríamos demostrar.

La segunda parte del resultado ocurre como consecuencia de calcular la extensión algebraica de F a partir del número de Steinitz $N(A/F)$, que es igual a A por el corolario anterior. En este caso, tenemos que

$$A = \bigcup_{n\in\mathbb{N}} K_n$$

Como $\mathrm{mcd}(n!, \mathbb{N}) = n!$, tenemos que $K_n = E_{n!}$. Por ser E_n subcuerpo de $E_{n!}$, la extensión A/F tiene como extensión intermedia de F a E_n para todo $n \in \mathbb{N}$. □

Bibliografía

[1] I. F. Blake, S. Gao, R. J. Lambert, *Construction and Distribution Problems for Irreducible Trinomials over Finite Fields*, Inst. Math. Appl. Conf. Ser., New Ser. **59**, 19-32 (1996)

[2] R. P. Brent, S. Larvala, P. Zimmermann, *A fast algorithm for testing reducibility of trinomials mod 2 and some new primitive trinomials of degree 3021377*, Mathematics of Computation, **Vol. 72**, Number 243, 1443–1452 (2002)

[3] N. A. Carella, *Topics in Normal Bases of Finite Fields*, arXiv:1304.0420, arxiv.org (2013)

[4] H. Fredricksen, R. Wisniewski, *On Trinomials* x^n+x^2+1 *and* $x^{8l\pm3}+x^k+1$ *Irreducible over GF(2)*, Information and Control, **50**, 58-63 (1981)

[5] W. Geiselmann, D. Gollmann, *Self-Dual Bases in* $\mathbb{F}_{q^n}$, Designs, Codes and Cryptography, **3**, 333-345 (1993)

[6] D. Hachenberger, D. Jungnickel, *Topics in Galois Fields*, Algorithms and Computation in Mathematics, **29**, Springer (2020)

[7] G. Kapetanakis, *A Swan-like note for a family of binary pentanomials*, Appl. Algebra Eng. Commun. Comput. **30**, 5, 361-372 (2019)

[8] M. K. Kyuregyan, S. Mehrabi, *Irreducible compositions of polynomials over finite fields of even characteristic*, Appl. Algebra Eng. Commun. Comput. **23**, No. 5-6, 207-220 (2012)

[9] W. J. Le Veque, *Topics in Number Theory*, Addison-Wesley Publishing Company Inc., tercera edición (1965)

[10] H. W. Lenstra, R. J. Schoof, *Primitive Normal Bases for Finite Fields*, Mathematics of Computation, **48**, 177, 217-231 (1987)

[11] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, edición revisada (1994)

[12] R. Lidl, G. Pilz, *Applied Abstract Algebra*, Springer, segunda edición (1998)

[13] S. Roman, *Field Theory*, Springer, segunda edición (2006)

[14] N. J. A. Sloane, *Numbers k such that $x^k + x + 1$ is irreducible over GF(2)*, The On-Line Encyclopedia of Integer sequences, A002475 (2002)

[15] N. J. A. Sloane, *Number of degree-n irreducible polynomials over GF(2);...*, The On-Line Encyclopedia of Integer sequences, A001037 (2012)

[16] J. Song, *$a(n)$ is the number of pentanomials $x^n + x^a + x^b + x^c + 1$ that are irreducible over GF(2) for $n > a > b > c > 0$*, The On-Line Encyclopedia of Integer sequences, A344146 (2021)

[17] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific Journal of Mathematics, **12**, 3, 1099-1106 (1962)

[18] Z. X. Wan, *Lectures on Finite Fields an Galois Rings*, World Scientific Publishing Co. Pte. Ltd (2003)

[19] R. G. Wilson, *$a(n)$ is the number of trinomials $x^n + x^k + 1$ that are irreducible over GF(2) for some k with $n > k > 0$* The On-Line Encyclopedia of Integer sequences, A057646 (2000)

[20] R. G. Wilson, *Numbers k such that $x^k + x^2 + 1$ is irreducible over GF(2)*, The On-Line Encyclopedia of Integer sequences, A057460 (2000)

[21] N. Zierler, *On the theorem of Gleason and Marsh*, Proc. Am. Math. Soc. **9**, 236-237 (1958)

[22] N. Zierler, *On $x^n + x + 1$ over GF(2)*, Information and Control **16**, 502-505 (1970)

[23] N. Zierler, *Primitive Trinomials Whose Degree is a Mersenne Exponent*, Information and Control **15**, 67-69 (1969)