Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Matemáticas

Polinomios irreducibles sobre cuerpos finitos

Autor: Javier Hernando Alonso

Tutor: José Enrique Marcos Naveira

2025

Índice general

Resumen

Este trabajo tiene como objetivo el estudio de los polinomios irreducibles sobre cuerpos finitos, desarrollando los fundamentos teóricos y destacando algunas de sus aplicaciones prácticas.

Se estudian propiedades de estos polinomios y de sus raíces, y se obtienen resultados que permiten construcciones de polinomios irreducibles. También dedicamos un apartado al teorema de Wedderburn, ya que, como veremos, es un teorema de gran importancia en el estudio de cuerpos finitos.

Finalmente centramos nuestra atención en los polinomios irreducibles sobre $\mathbb{F}_2[x]$, puesto que $\mathbb{F}_2$ es el cuerpo en el que se trabaja en las disciplinas actuales que requieren del manejo de polinomios irreducibles.

Palabras clave

Cuerpos finitos, polinomios irreducibles, polinomios primitivos, teorema de Wedderburn, binomios, trinomios, pentanomios.

Abstract

This work aims to study irreducible polynomials over finite fields, developing the theoretical foundations and highlighting some of their practical applications.

We study properties of these polynomials and their roots, and obtain results that allow the construction of irreducible polynomials. We also dedicate a section to Wedderburn's theorem, that, as we'll see, it is a theorem of great importance in the study of finite fields.

Finally, we focus our attention to the irreducible polynomials over $\mathbb{F}_2[x]$, since $\mathbb{F}_2$ is the field used in current disciplines that require handling irreducible polynomials.

Keywords

Finite fields, irreducible polynomials, primitive polynomials, Wedderburn's theorem, binomials, trinomials, pentanomials.

Introducción

El estudio de los cuerpos finitos constituye uno de los pilares fundamentales del álgebra moderna, tanto en su desarrollo más teórico como en sus aplicaciones en campos como la criptografía y la teoría de códigos. Los polinomios irreducibles son cruciales en el estudio de estos cuerpos, permitiéndonos construir y representar los cuerpos finitos, para así poder trabajar con estos.

Este trabajo se centra en el análisis de los polinomios irreducibles sobre cuerpos finitos, abordando los resultados clásicos que permiten el estudio de este tema, las propiedades principales de estos polinomios, algunos métodos de construcción de polinomios irreducibles, y estudiando ciertos polinomios concretos como los trinomios o los polinomios primitivos.

Los orígenes de la teoría de cuerpos finitos se remontan al matemático Évariste Galois (1811-1832), que fue el primero en trabajar con las estructuras algebraicas de grupos y cuerpos, y dio las ideas que más tarde se formalizarían en la teoría de grupos.

Aunque la representación de cuerpos finitos y el estudio de polinomios irreducibles tiene gran interés teórico, la motivación reciente tras el estudio de esta disciplina son principalmente sus aplicaciones en criptografía, siendo herramientas clave para el cifrado de claves públicas y privadas, y su uso en teoría de códigos, principalmente en códigos de corrección de errores, aunque también destacan otras aplicaciones como la generación de números pseudoaleatorios.

El primer tema es una breve recapitulación de los resultados básicos de cuerpos finitos más relevantes para este trabajo, principalmente el teorema de existencia y unicidad de cuerpos finitos, asumiendo conocimiento previo de la teoría de grupos y de resultados básicos de anillos y cuerpos.

En el segundo tema estudiamos el orden de los polinomios y algunas características de sus raíces, aplicadas particularmente a polinomios irreducibles en cuerpos finitos. También utilizamos las funciones de Euler y de Möbius para obtener resultados clásicos que nos permiten contar el número de polinomios irreducibles en un cuerpo finito, principalmente basándonos en el teorema de inversión de Möbius.

También nos centramos en un tipo particular de polinomios irreducibles, los polinomios primitivos, revisando teoremas de caracterización y abordando algunos resultados más actuales.

El enfoque principal del estudio está en obtener polinomios irreducibles concretos con los que poder trabajar para generar cuerpos finitos. Por tanto este tercer tema se dedica a obtener estos polinomios irreducibles, primero considerando criterios generales de irreducibilidad y luego centrándonos en polinomios específicos de mayor interés.

Estudiamos los binomios y trinomios que, debido a su bajo número de coeficientes distintos de cero, proveen ventajas computacionales al operar en un cuerpo representado por estos polinomios. Continuamos con los polinomios autorrecíprocos, que tienen uso en la teoría de códigos [12], y permiten generar secuencias de polinomios autorrecíprocos irreducibles que aumentan en grado.

Por último consideramos la irreducibilidad de los polinomios ciclotómicos, muy importantes en la teoría algebraica para generar extensiones de cuerpos.

Dedicamos un breve tema al teorema de Wedderburn, enunciado por Joseph Wedderburn en 1905, que establece que todo anillo de división finito es un cuerpo finito. Aunque no está directamente relacionado con los polinomios irreducibles sobre cuerpos finitos, consideramos que es un resultado suficientemente importante en el ámbito de los cuerpos finitos como para exponer su demostración, ya que muestra que para los anillos finitos no hay diferencias entre dominios, anillos de división y cuerpos.

Finalmente, el tema cinco se centra en estudiar los polinomios irreducibles sobre un cuerpo en particular, $\mathbb{F}_2[x]$. Este cuerpo tiene una conexión directa con la aritmética binaria y por su fácil implementación en hardware, es el utilizado principalmente para hacer los cálculos requeridos en cifrados y códigos correctores.

El manejo eficiente de las operaciones en cuerpos de la forma $\mathbb{F}_{2^n}$ es un tema de investigación actual, como se puede ver en los artículos [4] y [8], y encontrar buenos polinomios con los que representar este cuerpo es de gran importancia. Para la optimización de los tiempos de operaciones los polinomios con los que se trabaja en estos casos son los trinomios y los pentanomios.

Además en ciertas disciplinas como la generación de números pseudoaleatorios, que se estudia en un tema del libro *Introduction to finite fields and their applications* [10], es preferible utilizar polinomios primitivos para representar estos cuerpos, por lo que también dedicamos una breve sección a encontrar trinomios primitivos sobre $\mathbb{F}_2[x]$.

Durante el desarrollo de este trabajo consultaremos varios recursos online, de los que destacamos la enciclopedia online de sucesiones de enteros, que se abrevia como OEIS [14], creada por N. J. A. Sloane para almacenar sucesiones de interés matemático, y la gran búsqueda de primos de Mersenne por internet, o proyecto GIMPS [16], un proyecto de computación distribuida dedicado a encontrar números primos de la forma $2^p - 1$, con p un número primo.

También obtenemos algunas tablas y ejemplos con cálculos por ordenador, todos ellos usando MAPLE, un programa orientado al álgebra computacional.

Personalmente destaco la importancia de los trinomios, dedicando múltiples secciones a su estudio tanto en cuerpos finitos cualquiera como sobre el cuerpo $\mathbb{F}_2$. En particular, me ha llamado la atención la fuerte relación entre el teorema de Swan y la distribución de los trinomios irreducibles en $\mathbb{F}_2[x]$, que estudiaremos en el capítulo 5.

Capítulo 1

Preliminares de cuerpos finitos

Para el desarrollo de este trabajo, daremos por conocidos los resultados de las estructuras algebraicas de grupos, anillos y cuerpos, así como algunos resultados de extensiones finitas. El primer capítulo del libro *Introduction to finite fields and their applications* [10] cubre toda la información previa necesaria para el desarrollo de este trabajo.

También daremos por conocida la construcción del cuerpo de p elementos dada por las clases de $\mathbb{Z}$ módulo p, que se denotará por $\mathbb{F}_p$.

Esta sección de preliminares prepara los resultados principales de cuerpos finitos que necesitaremos a lo largo de este trabajo, siendo el más importante el teorema de existencia y unicidad de cuerpos finitos, que justifica la necesidad de encontrar polinomios irreducibles apropiados.

Seguiremos principalmente los resultados dados en el apartado 2.1 del libro *Introduction to finite fields and their applications* [10].

Lema 1.1. *Sea F un cuerpo finito y K un subcuerpo suyo de q elementos. Entonces F tiene q^m elementos, donde el grado de la extensión es $m = [F : K]$.*

Demostración. Consideramos F como un K-espacio vectorial, al ser F finito, su dimensión como espacio vectorial es finita. Si $[F : K] = m$, F tiene una base de m elementos, que denotamos $\mathcal{B} = \{b_1, \ldots, b_m\}$. Usando la base, todo elemento de F se puede representar como $a_1b_1 + \cdots + a_mb_m$, para cada $a_1, \ldots, a_m \in K$. Como cada a_i puede tomar q valores y hay m de ellos, deducimos que F debe tener q^m elementos. □

Con este resultado, establecemos el número de elementos que debe tener un cuerpo finito.

Teorema 1.2. *Sea F un cuerpo finito, p la característica de F y n el grado de F sobre su subcuerpo primo K. Entonces F tiene p^n elementos.*

Demostración. Como F es finito, su característica es un primo p, y por tanto, $K \cong \mathbb{F}_p$. Entonces K tiene p elementos y, aplicando el lema previo, deducimos que F tiene p^n elementos. □

Para estudiar como es el cardinal de todos los cuerpos finitos, preparamos los siguientes resultados.

Lema 1.3. *Sea F un cuerpo finito de q elementos. Entonces para cada $a \in F$ se cumple que $a^q = a$.*

Demostración. Si a=0 la igualdad es trivial. Si $a \neq 0$ consideramos el grupo multiplicativo F_q^*, donde ya sabemos que $a^{q-1} = 1$ para todos sus elementos, y por tanto, $a^q = a$. □

Lema 1.4. *Sea F un cuerpo finito de q elementos y K un subcuerpo de F. Entonces el polinomio $x^q - x \in K[x]$ factoriza en $F[x]$ como*

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

y por tanto F es un cuerpo de descomposición de $x^q - x$ sobre K.

Demostración. El polinomio $x^q - x$ tiene como mucho q raíces en F. Por el Lema 1.3, sabemos que todos los elementos en F son exactamente las q raíces de este polinomio, y por tanto F es su menor cuerpo de descomposición. □

Con estos resultados previos tenemos la base necesaria para construir todos los cuerpos finitos posibles. Ya sabemos que todo cuerpo finito debe tener p^n elementos, pero ahora probaremos que existe un cuerpo finito con p^n elementos para cualquier p primo y n natural.

Para esto demostramos el teorema de existencia y unicidad de cuerpos finitos.

Teorema 1.5. *Para cada p primo y n natural existe un cuerpo finito de $q = p^n$ elementos. Todo cuerpo de q elementos es isomorfo al cuerpo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$.*

Demostración. Empezaremos probando su existencia. Consideramos $x^q - x$ en $\mathbb{F}_p[x]$ y F su cuerpo de descomposición sobre $\mathbb{F}_p$. Las q raíces que tiene en F son distintas, ya que su derivada es $qx^{q-1} - 1 = -1$ en $\mathbb{F}_p[x]$.

Definimos el siguiente subespacio de F con q elementos, $S = \{a \in F : a^q - a = 0\}$.

Podemos comprobar fácilmente que cumple las propiedades para ser subcuerpo demostrando que cumple unas equivalentes.

- Primero vemos que $0, 1 \in S$. Claramente ambos cumplen la ecuación de S.
- Veamos que si $a, b \in S$ entonces $a + b \in S$. Sabemos que en un cuerpo de característica p, $(a - b)^q = a^q - b^q$. Además, al estar en S, $a^q = a, b^q = b$. Luego $a - b$ cumple $(a - b)^q = a - b$, por lo que $a - b \in S$.
- Por último, si $a, b \in S$ y $b \neq 0$, entonces $(ab^{-1})^q = a^q (b^q)^{-1} = ab^{-1}$. Por tanto $ab^{-1} \in S$.

Por la construcción de S, este contiene todas las raíces de $x^q - x$, luego el polinomio debe descomponer en S y por tanto, $F{=}S$. Como S tiene exactamente q elementos, F es un cuerpo finito de q elementos.

Ahora probaremos la unicidad. Sea F un cuerpo finito cualquiera de q elementos. F tiene característica p, como vimos en un lema previo, y entonces $\mathbb{F}_p$ será un subcuerpo de F.

Por el Lema 1.4, F es cuerpo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$ y su unicidad salvo isomorfismo se deduce de la unicidad de cuerpos de descomposición. □

Como ahora tenemos unicidad, nos referiremos al cuerpo de q elementos como $\mathbb{F}_q$ a partir de este punto. También consideraremos que $q = p^n$ para algún p primo y n natural.

Ahora veremos un resultado que permite determinar todos los subcuerpos de $\mathbb{F}_q$.

Teorema 1.6. *Sea $\mathbb{F}_q$ el cuerpo finito de $q = p^n$ elementos, con p primo y n natural. Entonces, todo subcuerpo de $\mathbb{F}_q$ tiene orden p^m donde m es un divisor de n. Además, para todo m con $m|n$, hay un subcuerpo de orden p^m y es el único con p^m elementos.*

Demostración. Como $\mathbb{F}_q$ es de característica p, todo subcuerpo K de $\mathbb{F}_q$ tiene característica p y por tanto, p^m elementos, con $m \in \mathbb{N}$. Por el Lema 1.1, sabemos que $\mathbb{F}_q$ tiene p^{ms} elementos, para algún $s \in \mathbb{N}$, luego $m \cdot s = n$ y $m|n$.

Si m es un divisor cualquiera de n, existe $k \in \mathbb{N}$ tal que $m \cdot k = n$. Usando esto vemos que $p^m - 1$ divide a $p^n - 1$

$$p^{mk} - 1 = (p^m - 1) \cdot (p^{m(k-1)} + p^{m(k-2)} + \cdots + 1).$$

De la misma forma, como $p^m - 1$ es divisor de $p^n - 1$, vemos que $x^{p^m-1} - 1$ divide a $x^{p^n-1} - 1$ en $\mathbb{F}_p[x]$. De aquí deducimos que el cuerpo de descomposición de $x^{p^m-1} - 1$ en $\mathbb{F}_p[x]$ debe estar contenido en el cuerpo de descomposición de $x^{p^n-1} - 1$, que es $\mathbb{F}_q$.

Por el Teorema 1.5 sabemos que este cuerpo de descomposición tiene p^m elementos. Como tiene todas las raíces de $x^{p^m-1} - 1$, no puede haber otro subcuerpo distinto de p^m elementos, pues tendría otra raíz del polinomio. □

Lo siguiente que estudiaremos serán dos maneras de representar cuerpos finitos que permiten su uso en la práctica con mayor facilidad.

Teorema 1.7. *El grupo multiplicativo de $\mathbb{F}_q$, representado por $\mathbb{F}_q^*$, es cíclico.*

Demostración. Dado que el caso q=2 es obvio, asumimos $q \geq 3$. Sea $h = q - 1 = p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$ su descomposición en factores primos.

Para cualquier i con $1 \leq i \leq m$, el polinomio $x^{h/p_i} - 1$ tiene como mucho h/p_i raíces en $\mathbb{F}_q$. Por tanto, como $h/p_i < h$, debe haber algún elemento distinto de cero que no sea raíz de este polinomio en $\mathbb{F}_q$ y que denotaremos a_i.

Consideremos el elemento $b_i = a_i^{h/(p_i^{r_i})}$, que cumple $b_i^{p_i^{r_i}} = a_i^{q-1} = 1$ y por tanto, el orden de b_i divide a $p_i^{r_i}$, que al ser p_i primo, debe ser de la forma $p_i^{s_i}$ con $0 \leq s_i \leq r_i$. Además

$$b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1$$

luego el orden de b_i es $p_i^{r_i}$. Finalmente construimos el elemento $b = b_1 b_2 \cdots b_m$, en $\mathbb{F}_q$, que tiene orden h. Para ver esto utilizamos reducción al absurdo.

Supongamos que el orden de b es un divisor propio de h y por tanto divide a h/p_i para algún $1 \leq i \leq m$, digamos h/p_1. Entonces

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} \dots b_m^{h/p_1}.$$

Además, considerando $2 \leq i \leq m$, se cumple que $p_i^{r_i}$ divide a h/p_1 y como $b_i^{p_i^{r_i}} = 1$, entonces $b_i^{h/p_1} = 1$. Por tanto $1 = b^{h/p_1} = b_1^{h/p_1}$ y el orden de b_1 divide a h/p_1, pero el orden de b_1 es $p_1^{r_1}$, que es primo con h/p_1.

De esta forma llegamos a un absurdo y deducimos que el orden de b es h=$q - 1$, luego b es un generador de $\mathbb{F}_q^*$ y este es un grupo cíclico. □

Este resultado nos permite escribir el cuerpo $\mathbb{F}_q^*$ como las potencias de cierto elemento. Como estos elementos serán de gran interés, los incluiremos en la siguiente definición.

Definición 1.8. Un generador del grupo cíclico $\mathbb{F}_q^*$ se denomina elemento primitivo de $\mathbb{F}_q$.

Definimos ahora dos cuerpos que necesitamos para el siguiente teorema.

Definición 1.9. Sea E un cuerpo y F uno de sus subcuerpos.

Consideramos $\alpha \in E$ y $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ y definimos

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n.$$

También definimos los cuerpos

$$F[\alpha] = \{f(\alpha) : f(x) \in F[x]\} \text{ y } F(\alpha) = \{f(\alpha)/g(\alpha) : f(x), g(x) \in F[x], g(x) \neq 0\}.$$

Verificar que los conjuntos definidos son cuerpos es sencillo y por tanto se omite la comprobación.

El siguiente teorema nos permite representar un cuerpo de q^n elementos como el cuerpo de q elementos cociente con un polinomio irreducible de grado n.

Teorema 1.10. *Sea E un cuerpo, F un subcuerpo, $\alpha \in E$ y sea $p(x) \in F[x]$ un polinomio irreducible de grado n con $p(\alpha) = 0$. Entonces todo elemento en $F[\alpha]$ se puede representar de forma única como $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, con $a_0, \ldots, a_{n-1} \in F$, y por tanto, si F es un cuerpo finito de q elementos, $|F[\alpha]| = q^n$. Además $F[\alpha] \cong F[x]/(p(x))$.*

Demostración. Sea $p(x) = p_0 + p_1x + \cdots + p_nx^n$ con $p_0, \ldots, p_n \in F, p_n \neq 0$. Entonces

$$p(\alpha) = p_0 + p_1\alpha + \ldots + p_n\alpha^n = 0$$

y como p_n tiene inverso, podemos escribir α^n como combinación lineal de $1, \alpha, \ldots, \alpha^{n-1}$.

Multiplicando $p(\alpha)$ por α, tenemos

$$p_0\alpha + p_1\alpha^2 + \ldots + p_n\alpha^{n+1} = 0$$

y de la misma forma, podemos escribir α^{n+1} como combinación lineal de $1, \alpha, \ldots, \alpha^n$, y desarrollando α^n, lo podemos escribir como combinación lineal de $1, \alpha, \ldots, \alpha^{n-1}$.

Continuando de esta forma podemos escribir todas las potencias de α como combinación lineal de $1, \alpha, \ldots, \alpha^{n-1}$, y por tanto, se puede escribir así para todos los elementos en $F[\alpha]$.

Ahora veremos la unicidad de la expresión. Si un elemento de $F[\alpha]$ se puede representar como

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \text{ y } b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}, \text{ con } a_i, b_i \in F$$

entonces tenemos

$$a_0 - b_0 + (a_1 - b_1)\alpha + \cdots + (a_{n-1} - b_{n-1})\alpha^{n-1} = 0.$$

Sea $h(x) = a_0 - b_0 + (a_1 - b_1)x + \cdots + (a_{n-1} - b_{n-1})x^{n-1}$, entonces $h(\alpha) = 0$. Por tanto α es una raíz y $(x - \alpha)|h(x), (x - \alpha)|p(x)$.

Como $h(x)$ y $p(x)$ comparten un divisor, $mcd(h(x), p(x)) \neq 1$, además $h(x)$ es de grado menor que $p(x)$ y por tanto $h(x)$=0. Es decir $a_0 = b_0, ..., a_{n-1} = b_{n-1}$ y tenemos la unicidad.

Con la unicidad es claro que la aplicación que manda un polinomio $a_0+a_1x+\cdots+a_{n-1}x^n+(p(x))$ de $F[x]/(p(x))$ a $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ en $F[\alpha]$ es un isomorfismo. □

Veamos como aplicar este teorema para operar en un cuerpo finito.

Ejemplo 1.11. Sea $x^7 + x + 1 \in \mathbb{F}_2[x]$ y α una de sus raíces. Es fácil comprobar que es irreducible, y entonces por el Teorema 1.10

$$\mathbb{F}_{2^7} = \mathbb{F}_2[\alpha] = \{a_0 + a_1\alpha + \cdots + a_6\alpha^6 : a_0, \ldots, a_6 \in \mathbb{F}_2\}$$

Entonces dos elementos α^i y α^j con $0 \leq i, j \leq 6$ se pueden multiplicar de la siguiente forma. Sea $i + j = 7 + k$ con $0 \leq k \leq 5$, al ser α raíz de $x^7 + x + 1$ tenemos que $\alpha^7 = \alpha + 1$ luego

$$\alpha^i \cdot \alpha^j = \alpha^{i+j} = \alpha^7 \cdot \alpha^k = (\alpha + 1)\alpha^k = \alpha^k + \alpha^{k+1}.$$

Si queremos multiplicar dos elementos cualesquiera de $\mathbb{F}_{2^7}$, siendo $a_0, \ldots, a_6, b_0, \ldots, b_6 \in \mathbb{F}_2$,

$$(a_0 + a_1\alpha + \cdots + a_6\alpha^6) \cdot (b_0 + b_1\alpha + \cdots + b_6\alpha^6) = \sum_{i+j \leq 6} a_i b_j \alpha^{i+j} + \sum_{\substack{i+j=7+k \\ 0 \leq k \leq 5}} a_i b_j (\alpha^k + \alpha^{k+1}),$$

y obtenemos fácilmente de esta expresión un elemento de $\mathbb{F}_{2^7}$ expresado como $c_0 + c_1\alpha + \cdots + c_6\alpha^6$ con $c_0, \ldots, c_6 \in \mathbb{F}_2$.

Ahora demostramos unos resultados que nos permitirán encontrar siempre un polinomio irreducible de grado n en un cuerpo finito.

Teorema 1.12. *Sea $\mathbb{F}_q$ el cuerpo finito de q elementos y $\mathbb{F}_r$ una extensión finita del cuerpo. Entonces $\mathbb{F}_r$ es una extensión simple de $\mathbb{F}_q$ y cualquier elemento primitivo de $\mathbb{F}_r$ genera $\mathbb{F}_r$ sobre $\mathbb{F}_q$.*

Demostración. Sea α un elemento primitivo de $\mathbb{F}_r$. Como $\mathbb{F}_r$ es una extensión de $\mathbb{F}_q$, claramente $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_r$. Por otro lado, el 0 y todas las potencias de α pertenecen a $\mathbb{F}_q(\alpha)$ y, al ser α generador de $\mathbb{F}_r$, esto implica que $\mathbb{F}_q(\alpha) \supseteq \mathbb{F}_r$.

Con esto tenemos la igualdad $\mathbb{F}_q(\alpha) = \mathbb{F}_r$ y, al ser α un elemento primitivo genérico, el teorema queda probado. □

Recordamos la definición de polinomio mínimo, que nos será muy útil al ser un polinomio irreducible que podemos encontrar en cualquier cuerpo finito.

Definición 1.13. Si $\alpha \in F$ es algebraico sobre K, entonces el polinomio mónico $m_\alpha \in K[x]$ que genera el ideal $J = \{f \in K[x] : f(\alpha) = 0\}$ está únicamente determinado y se llama el polinomio mínimo de α sobre K. El grado de α sobre F se define como el grado de su polinomio mínimo m_α, o equivalentemente como $[F(\alpha) : F]$.

Corolario 1.14. *Para cada cuerpo finito $\mathbb{F}_q$ y $n \in \mathbb{N}$ existe un polinomio irreducible en $\mathbb{F}_q[x]$ de grado n.*

Demostración. Sea $\mathbb{F}_r$ la extensión de $\mathbb{F}_q$ de orden q^n, luego $[\mathbb{F}_r : \mathbb{F}_q] = n$. Por el teorema previo, $\mathbb{F}_q(\alpha) = \mathbb{F}_r$ para algún $\alpha \in \mathbb{F}_r$. Entonces el polinomio mínimo de α sobre $\mathbb{F}_q$ cumple las propiedades necesarias, ya que es un polinomio irreducible en $\mathbb{F}_q[x]$ que es de grado n. □

Capítulo 2

Propiedades de los polinomios irreducibles sobre cuerpos finitos

Como hemos visto en la sección previa, los polinomios irreducibles son una herramienta clave para construir y operar con cuerpos finitos. En este capítulo estudiaremos algunas propiedades de los polinomios irreducibles en cuerpos finitos que nos permitirán posteriormente construirlos y estudiarlos en más detalle.

Veremos el comportamiento de las raíces de un polinomio en su cuerpo de descomposición y algunas propiedades básicas del orden de un polinomio. También estudiaremos cuántos polinomios irreducibles de grado fijo hay en un cuerpo finito aprovechando las funciones ϕ de Euler y μ de Möbius.

En la última sección definiremos los polinomios primitivos, un tipo especial de polinomios irreducibles, veremos como caracterizarlos y estudiaremos cuando ciertos polinomios pueden ser primitivos.

2.1. Raíces y orden de polinomios

Empezamos esta sección con resultados sobre las raíces de un polinomio irreducible. Vamos a ver que siempre podemos construir el resto de raíces del polinomio si tenemos una de ellas, y su relación con el cuerpo en el que están. Seguimos el capítulo 2.2 del libro *Introduction to finite fields and their applications* [10].

Primero introducimos un par de lemas que nos permiten estudiar cuál es el cuerpo de descomposición de las raíces.

Lema 2.1. *Sea $f \in \mathbb{F}_q[x]$ un polinomio irreducible sobre un cuerpo finito $\mathbb{F}_q$ y sea α una raíz de f en una extensión de $\mathbb{F}_q$. Entonces, para un polinomio $h \in \mathbb{F}_q[x]$, se tiene que $h(\alpha) = 0$ si y solo si f divide a h.*

Demostración. Sea a el coeficiente que acompaña al término de mayor grado de f y definimos $g(x) = a^{-1}f(x)$. Entonces, g es un polinomio irreducible mónico en $\mathbb{F}_q[x]$ con $g(\alpha) = 0$, y por lo tanto es el polinomio mínimo de α sobre $\mathbb{F}_q$.

De la definición de polinomio mínimo se obtiene directamente que $f(\alpha) = 0$ si y solo si el polinomio mínimo de α sobre $\mathbb{F}_q$ divide a f, y por esta propiedad el resultado es inmediato. □

Lema 2.2. *Sea $f \in \mathbb{F}_q[x]$ un polinomio irreducible sobre $\mathbb{F}_q$ de grado m. Entonces $f(x)$ divide a $x^{q^n} - x$ si y solo si m divide a n.*

Demostración. Supongamos que $f(x)$ divide a $x^{q^n}-x$. Sea α una raíz de f en su cuerpo de descomposición sobre $\mathbb{F}_q$. Entonces α es raíz de $x^{q^n}-x$ y por tanto pertenece a su cuerpo de descomposición, que es $\mathbb{F}_{q^n}$.

De esto se deduce que $\mathbb{F}_q(\alpha)$ es un subcuerpo de $\mathbb{F}_{q^n}$. Como $[\mathbb{F}_q(\alpha):\mathbb{F}_q]=m$, $[\mathbb{F}_{q^n}:\mathbb{F}_q]=n$ y $[\mathbb{F}_{q^n}:\mathbb{F}_q]=[\mathbb{F}_{q^n}:\mathbb{F}_q(\alpha)]\cdot[\mathbb{F}_q(\alpha):\mathbb{F}_q]$ claramente m divide a n.

Recíprocamente, si m divide a n, entonces el Teorema 1.6 implica que $\mathbb{F}_{q^m}$ es subcuerpo de $\mathbb{F}_{q^n}$. Si α es una raíz de f en su cuerpo de descomposición sobre $\mathbb{F}_q$, por el Teorema 1.10, $[\mathbb{F}_q(\alpha):\mathbb{F}_q]=m$ y $\mathbb{F}_q(\alpha)\cong\mathbb{F}_{q^m}$.

Por la contención vista previamente, $\alpha\in\mathbb{F}_{q^n}$, luego $\alpha^{q^n}=\alpha$, y se ve que α es una raíz de $x^{q^n}-x\in\mathbb{F}_q[x]$. Se deduce del lema previo que $f(x)$ divide a $x^{q^n}-x$. □

Utilizando estos lemas, conseguimos todas las raíces de un polinomio irreducible a partir de una dada.

Teorema 2.3. *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, todas las raíces de f son simples y están dadas por los m elementos distintos $\alpha,\alpha^q,\alpha^{q^2},\ldots,\alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$.*

Demostración. Sea α una raíz de f en su cuerpo de descomposición sobre $\mathbb{F}_q$.

Entonces $\mathbb{F}_q(\alpha)=\mathbb{F}_{q^m}$ por el Teorema 1.10, y $\alpha\in\mathbb{F}_{q^m}$. Ahora mostramos que si $\beta\in\mathbb{F}_{q^m}$ es una raíz de f, entonces β^q también lo es.

Escribimos $f(x)=a_mx^m+\cdots+a_1x+a_0$ con $a_i\in\mathbb{F}_q$ para $0\le i\le m$. Entonces, usando el Lema 1.3 y que $(a+b)^q=a^q+b^q$, tenemos

$$f(\beta^q)=a_m\beta^{qm}+\cdots+a_1\beta^q+a_0=a_m^q\beta^{qm}+\cdots+a_1^q\beta^q+a_0^q=(a_m\beta^{qm}+\cdots+a_1\beta^q+a_0)^q=f(\beta)^q=0$$

Así, los elementos $\alpha,\alpha^q,\alpha^{q^2},\ldots,\alpha^{q^{m-1}}$ son raíces de f. Probaremos que son distintos por reducción al absurdo.

Supongamos,que $\alpha^{q^j}=\alpha^{q^k}$ para algunos enteros j y k con $0\le j<k\le m-1$. Elevando esta igualdad a la potencia q^{m-k}, obtenemos

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

Se obtiene del Lema 2.1 que $f(x)$ divide a $x^{q^{m-k+j}}-x$. Por el Lema 2.2, esto solo es posible si m divide a $m-k+j$. Pero $0<m-k+j<m$, lo cual lleva a una contradicción. □

Como todas las raíces pertenecen a $\mathbb{F}_{q^m}$, es fácil comprobar que este cuerpo es el de descomposición de f.

Corolario 2.4. *Sea f un polinomio irreducible en $\mathbb{F}_q[x]$ de grado m. Entonces el cuerpo de descomposición de f sobre $\mathbb{F}_q$ es $\mathbb{F}_{q^m}$.*

Demostración. El Teorema 2.3 muestra que f descompone completamente en $\mathbb{F}_{q^m}$. Si α es una raíz de f en $\mathbb{F}_{q^m}$

$$\mathbb{F}_q(\alpha,\alpha^q,\alpha^{q^2},\ldots,\alpha^{q^{m-1}})=\mathbb{F}_q(\alpha)=\mathbb{F}_{q^m}.$$

La segunda igualdad se ve en el Teorema 1.10. □

Introducimos una definición para los elementos que aparecen en el teorema previo, independientemente de si son raíces de un polinomio irreducible en $\mathbb{F}_q[x]$ o no, para estudiar su relación con el cuerpo al que pertenecen, o su relación con otros polinomios.

Definición 2.5. Sea $\mathbb{F}_{q^m}$ una extensión de $\mathbb{F}_q$ y sea $\alpha \in \mathbb{F}_{q^m}$. Entonces se definen los conjugados de α con respecto a $\mathbb{F}_q$ como los elementos, no necesariamente distintos, $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$.

Empezamos estudiando la relación de los conjugados con su orden en un cuerpo.

Teorema 2.6. *Los conjugados de $\alpha \in \mathbb{F}_q^*$ con respecto a cualquier subcuerpo de $\mathbb{F}_q$ tienen el mismo orden en el grupo $\mathbb{F}_q^*$.*

Demostración. Si p es la característica de $\mathbb{F}_q$, tenemos que $\mathbb{F}_q = \mathbb{F}_{p^m}$ para algún $m \in \mathbb{N}$, y por tanto, los conjugados de α respecto a cualquier subcuerpo de $\mathbb{F}_q$ son de la forma α^{p^k} para algún $k \in \mathbb{N}$.

Para ver el orden de estos elementos, podemos considerar el siguiente isomorfismo.

$$\begin{aligned} \lambda : \mathbb{F}_q &\to \mathbb{F}_q \\ x &\mapsto x^{p^r}. \end{aligned}$$

Al ser un isomorfismo de grupos, el orden de un elemento y su imagen son el mismo, y como esto es válido para cualquier $r \in \mathbb{N}$, todos los posibles conjugados de la forma α^{p^k} tienen el mismo orden que α. □

Si el orden de α es $q-1$, y por tanto α es primitivo en $\mathbb{F}_q$, el siguiente corolario es directo.

Corolario 2.7. *Si α es un elemento primitivo de $\mathbb{F}_q$, entonces también lo son todos sus conjugados con respecto a cualquier subcuerpo de $\mathbb{F}_q$.*

Veamos un ejemplo concreto donde obtenemos los conjugados de un polinomio de grado 4 en $\mathbb{F}_2[x]$ y en $\mathbb{F}_4[x]$.

Ejemplo 2.8. Sea $\alpha \in \mathbb{F}_{16}$ una raíz de $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Entonces los conjugados de α con respecto a $\mathbb{F}_2$ son $\alpha, \alpha^2, \alpha^4 = \alpha + 1$, y $\alpha^8 = \alpha^2 + 1$, siendo cada uno de ellos un elemento primitivo de $\mathbb{F}_{16}$. Los conjugados de α con respecto a $\mathbb{F}_4$ son α y $\alpha^4 = \alpha + 1$.

Podemos determinar ciertos automorfismos de un cuerpo finito usando los elementos conjugados.

Sea $\mathbb{F}_{q^m}$ una extensión de $\mathbb{F}_q$. Por un automorfismo α de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ entendemos un automorfismo de $\mathbb{F}_{q^m}$ que fija los elementos de $\mathbb{F}_q$. Es decir, requerimos que α sea una función biyectiva de $\mathbb{F}_{q^m}$ en sí mismo, con $\alpha(a+b) = \alpha(a) + \alpha(b)$ y $\alpha(ab) = \alpha(a)\alpha(b)$ para todos $a, b \in \mathbb{F}_{q^m}$, y que $\alpha(a) = a$ para todo $a \in \mathbb{F}_q$.

Teorema 2.9. *Los automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ son exactamente $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$, las aplicaciones definidas por $\sigma_j(a) = a^{q^j}$ para $a \in \mathbb{F}_{q^m}$ y $0 \leq j \leq m-1$.*

Demostración. Para cada σ_j y todos $a, b \in \mathbb{F}_{q^m}$ se tiene claramente que $\sigma_j(ab) = \sigma_j(a)\sigma_j(b)$, y también $\sigma_j(a+b) = \sigma_j(a) + \sigma_j(b)$, ya que la característica del cuerpo es p y $q = p^n$. Por lo tanto σ_j es un endomorfismo de $\mathbb{F}_{q^m}$. Además, $\sigma_j(a) = 0$ si y solo si $a = 0$, por lo que σ_j es inyectiva.

Como $\mathbb{F}_{q^m}$ es un conjunto finito con más elementos que $\mathbb{F}_q$, σ_j es sobreyectiva y, por tanto, un automorfismo de $\mathbb{F}_{q^m}$. Además, se tiene que $\sigma_j(a) = a$ para todo $a \in \mathbb{F}_q$ por el Lema 1.3, por lo que cada σ_j es un automorfismo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$.

Las aplicaciones $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ son distintas ya que toman valores distintos en un elemento primitivo de $\mathbb{F}_{q^m}$.

Supongamos ahora que α es un automorfismo arbitrario de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Sea β un elemento primitivo de $\mathbb{F}_{q^m}$ y sea $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathbb{F}_q[x]$ su polinomio mínimo sobre $\mathbb{F}_q$. Entonces

$$0 = \sigma\left(\beta^m + a_{m-1}\beta^{m-1} + \cdots + a_0\right) = \sigma(\beta)^m + a_{m-1}\sigma(\beta)^{m-1} + \cdots + a_0,$$

y por tanto $\alpha(\beta)$ es raíz de f en $\mathbb{F}_{q^m}$. Como β también es raíz de f se sigue del Teorema 2.3 que $\alpha(\beta) = \beta^{q^j}$ para algún j, $0 \leq j \leq m-1$.

Como β un elemento primitivo, para cada $a \in \mathbb{F}_{q^m}$ existe un $k \in \mathbb{N}$ tal que $a = \beta^k$, y como α es un homomorfismo tenemos

$$\sigma(a) = \sigma(\beta^k) = \sigma(\beta)^k = (\beta^{q^j})^k = (\beta^k)^{q^j} = a^{q^j}$$

y obtenemos que $\alpha(a) = a^{q^j}$. □

Finalizamos esta parte con un resultado que relaciona el polinomio mínimo de una raíz con sus conjugados, junto a otras propiedades de los polinomios mínimos que nos servirán para posteriores resultados. Hemos obtenido este teorema de la sección 3.2 del libro *Introduction to finite fields and their applications* [10].

Teorema 2.10. *Sea $\alpha \in \mathbb{F}_{q^n}$. Supongamos que el grado de α sobre $\mathbb{F}_q$ es d y sea m_α el polinomio mínimo de α sobre $\mathbb{F}_q$. Entonces:*

(i) *m_α es irreducible sobre $\mathbb{F}_q$ y $\deg(m_\alpha) = d$ divide a n.*

(ii) *$f \in \mathbb{F}_q[x]$ satisface $f(\alpha) = 0$ si y solo si $m_\alpha \mid f$.*

(iii) *Si α es un elemento primitivo de $\mathbb{F}_{q^n}$, entonces $\deg(m_\alpha) = n$.*

(iv) *Si f es un polinomio mónico irreducible de $\mathbb{F}_q[x]$ tal que $f(\alpha) = 0$, entonces $f = m_\alpha$.*

(v) *m_α divide a $x^{q^d} - x$ y a $x^{q^n} - x$.*

(vi) *Las raíces de m_α son $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ y son todas distintas. Además m_α es el polinomio mínimo sobre $\mathbb{F}_q$ de todos estos elementos y $\alpha^{q^d} = \alpha$.*

Demostración.

(i) Sabemos que m_α debe ser irreducible por la definición de polinomio mínimo, ya que si otro polinomio lo dividiese entonces m_α no generaría el ideal. La segunda parte se obtiene de que $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)] \cdot [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ y de que $[\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ es el grado de α por definición.

(ii) Se obtiene directamente de que el polinomio mínimo genera el ideal que vimos en su definición.

(iii) Si α es un elemento primitivo de $\mathbb{F}_{q^n}$, al ser $\mathbb{F}_{q^n}$ extensión de $\mathbb{F}_q$ tenemos que $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ y por tanto, $[\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)] = 1$. De la igualdad en (i) obtenemos que $\deg(m_\alpha) = n$.

(iv) Por (ii) tenemos que $m_\alpha \mid f$ y, al ser f irreducible, $f = m_\alpha$.

(v) Por el Lema 2.2, el polinomio mínimo m_α divide a $x^{q^n} - x$ si $d \mid n$ y por (i) d divide a n. De la misma forma, $m_\alpha \mid x^{q^d} - x$.

(vi) Por el Teorema 2.3, $\alpha \in \mathbb{F}_{q^d}$, luego $\alpha^{q^d} = \alpha$, y $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ son todas las raíces de m_α. Para la segunda parte, si llamamos β a una de esas raíces, aplicando (iv) sobre m_β, como $m_\alpha(\beta) = 0$ y m_α es mónico e irreducible, tenemos $m_\alpha = m_\beta$ para todas las raíces. □

Ahora que hemos estudiado los conjugados de una raíz, podemos emplearlo para definir y estudiar el orden de un polinomio, que cuando es irreducible, podremos relacionar con el orden de sus raíces. Para esta breve parte, seguiremos el principio del capítulo 3.1 del libro *Introduction to finite fields and their applications* [10].

El siguiente lema justifica su definición.

Lema 2.11. *Sea $f \in \mathbb{F}_q[x]$ un polinomio de grado $m \geq 1$ con $f(0) \neq 0$. Entonces existe un natural $e \leq q^m - 1$ tal que f divide a $x^e - 1$.*

Demostración. El grupo $\mathbb{F}_q[x]/(f)$ tiene $q^m - 1$ clases no nulas. Dado que $f(0) \neq 0$, las clases $x^j + (f)$, $0 \leq j \leq q^m - 1$ son todas no nulas, y existen enteros s y t con $0 \leq s < t \leq q^m - 1$ tales que $x^t \equiv x^s \bmod(f)$. Entonces se tiene que $x^{t-s} \equiv 1 \bmod(f)$, luego $f \mid (x^{t-s}-1)$ con $0 < t-s \leq q^m-1$. □

Un método para determinar e es simplemente probar si $f \mid x^e - 1$ para $e = m, m+1, \ldots$ hasta que se cumpla. Este no es un muy buen método, pero si el polinomio f es irreducible, obtendremos resultados que reducen el número de posibles candidatos.

Definición 2.12. Sea $f \in \mathbb{F}_q[x]$ con $f(0) \neq 0$. Entonces, el menor número natural e tal que $f \mid (x^e-1)$ se llama el orden de f. Si $f(0) = 0$, entonces f es de la forma $x^h g$ con $h \in \mathbb{N}$ y $g \in \mathbb{F}_q[x]$, $g(0) \neq 0$, para un polinomio g único. El orden de f se define entonces como el orden de g.

El orden de un polinomio irreducible puede caracterizarse mediante el orden de sus raíces.

Teorema 2.13. *Sea $f \in \mathbb{F}_q[x]$ un polinomio irreducible sobre $\mathbb{F}_q$ de grado $m \geq 2$. Entonces* $\operatorname{ord}(f)$ *es igual al orden de cualquier raíz de f en $\mathbb{F}_{q^m}^*$.*

Demostración. Vemos que $f(0) \neq 0$, ya que de otro modo sería divisible por x. $\mathbb{F}_{q^m}$ es el cuerpo de descomposición de f sobre $\mathbb{F}_q$. Usando el Teorema 2.3 y el Teorema 2.6 vemos que las raíces de f tienen el mismo orden en $\mathbb{F}_{q^m}^*$.

Sea $\alpha \in \mathbb{F}_{q^m}$ una raíz de f, entonces, como f es el polinomio mínimo de α por una constante, por el Lema 2.1, también cumple que $\alpha^e = 1$ si y solo si $f \mid x^e - 1$. El resultado se deduce de la definición de $\operatorname{ord}(f)$ y del orden de α en el grupo $\mathbb{F}_{q^m}^*$. □

Con esto podemos obtener una condición necesaria que debe cumplir el orden de un polinomio irreducible.

Corolario 2.14. *Si $f \in \mathbb{F}_q[x]$ es un polinomio irreducible sobre $\mathbb{F}_q$ de grado k, entonces* $\operatorname{ord}(f)$ *divide a $q^k - 1$.*

Demostración. Si $f = cx$ con $c \in \mathbb{F}_q^*$, entonces $\operatorname{ord}(f) = 1$. En caso contrario, el resultado se deduce del teorema previo y de que el orden de cualquier elemento en $\mathbb{F}_{q^k}^*$ divide al orden del grupo multiplicativo. □

Veamos tres casos donde usamos estos teoremas para obtener el orden de un polinomio irreducible más fácilmente.

Ejemplo 2.15. 1. $f = x^3 + x + 1 \in \mathbb{F}_2[x]$ es irreducible. Entonces $\text{ord}(f)$ debe ser un divisor de $2^3 - 1 = 7$. Así que $\text{ord}(f) = 7$.

2. Si $f \in \mathbb{F}_2[x]$ es irreducible de grado 4, entonces $4 \leq \text{ord}(f)$ y $\text{ord}(f) \mid 2^4 - 1 = 15$. Por tanto, $\text{ord}(f)$ es igual a 5 o a 15, lo cual puede estudiarse mucho más rápido que todos los candidatos de 4 a 15. Tenemos tres opciones de f:

   $f_1 = x^4 + x^3 + x^2 + x + 1$,
   $f_2 = x^4 + x + 1$,
   $f_3 = x^4 + x^3 + 1$.

   Fácilmente, podemos obtener $\text{ord}(f_1) = 5$ ya que $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$.

   Como estamos en $\mathbb{F}_2[x]$, el único polinomio de grado 1 que queda es x. Entonces, se ve que ni f_2 ni f_3 dividen a $x^5 - 1$ y por tanto $\text{ord}(f_2) = \text{ord}(f_3) = 15$

3. De manera similar al primer ejemplo, todo polinomio irreducible en $\mathbb{F}_2[x]$ de grado 5 debe tener orden 31.

Los siguientes resultados nos muestran que podemos calcular el orden de un polinomio a partir de los órdenes de los polinomios en los que descompone en su descomposición canónica. Primero vemos un lema que relaciona la divisibilidad de un polinomio con la divisibilidad de su orden.

Lema 2.16. *Sea $c \in \mathbb{N}$ y $f \in \mathbb{F}_q[x]$ un polinomio tal que $f(0) \neq 0$ y $\text{ord}(f) = e$. Entonces $f(x)$ divide $x^c - 1$ si y sólo si e divide c.*

Demostración. Supongamos que e divide c. Por la definición de orden $f(x)$ divide $x^e - 1$, y como e divide c tenemos que $x^e - 1$ divide $x^c - 1$, luego $f(x) \mid x^c - 1$.

Ahora supongamos que $f(x)$ divide $x^c - 1$. Por definición de orden, $c \geq e$, así que podemos escribir $c = me + r$ con $m \in \mathbb{N}$ y $0 \leq r < e$. Entonces $x^c - 1 = (x^{me} - 1)x^r + (x^r - 1)$ y como $f(x)$ divide $x^e - 1$, también divide $x^{me} - 1$, luego $f(x)$ divide $x^r - 1$, que por definición de orden solo es posible para $r = 0$.

Por lo tanto, $c = me$, es decir, $e \mid c$. □

Ahora, apoyándonos en este lema, conociendo el orden de un polinomio $f(x)$ calculamos el orden de sus potencias $f(x)^n$, con $n \in \mathbb{N}$.

Teorema 2.17. *Sea $g \in \mathbb{F}_q[x]$ un polinomio irreducible sobre $\mathbb{F}_q$ con $g(0) \neq 0$ y $\text{ord}(g) = e$, y sea $f = g^b$ con $b \in \mathbb{N}$. Sea t el menor natural tal que $p^t \geq b$, donde p es la característica de $\mathbb{F}_q$. Entonces $\text{ord}(f) = ep^t$.*

Demostración. Sea $c = \text{ord}(f)$. Claramente $f(x) \mid x^c - 1$ y por tanto $g(x) \mid x^c - 1$. Por el Lema 2.16, deducimos que $e \mid c$.

Además, $g(x)$ divide $x^e - 1$ y por tanto, $f(x)$ divide $(x^e - 1)^b$. Como $b \leq p^t$, $f(x)$ también divide $(x^e - 1)^{p^t} = x^{ep^t} - 1$ y por el Lema 2.16, c divide ep^t.

Combinando que e divide c, c divide ep^t y p es primo, tenemos que $c = ep^u$ con $0 \leq u \leq t$. Ahora observamos que, por el Corolario 2.14, $e \mid q^k - 1$ con k el grado de $g(x)$, por lo que e no es un múltiplo de p y entonces $x^e - 1$ sólo tiene raíces simples.

Por lo tanto, todas las raíces de $x^{ep^u} - 1 = (x^e - 1)^{p^u}$ tienen multiplicidad p^u. Como $c = ep^u$ y $f(x) = g(x)^b$ tenemos que $g(x)^b$ divide $x^{ep^u} - 1$, y por el Teorema[tal], todas las raíces de $g(x)$ son simples. Luego todas las raíces de $g(x)^b$ tienen multiplicidad b, y comparando las multiplicidades de las raíces con $x^{ep^u} - 1$, tenemos que $b \leq p^u$.

Como t era el menor natural tal que $b \leq p^t$ entonces $u \geq t$, de esto concluimos que $u = t$ y, por lo tanto, $c = ep^t$. □

Vemos ahora que también podemos calcular el orden de un polinomio a partir de los órdenes de su descomposición en polinomios coprimos dos a dos.

Teorema 2.18. *Sean $g_1, \ldots, g_k$ polinomios no nulos coprimos dos a dos en $\mathbb{F}_q$, y sea $f = g_1 \cdots g_k$. Entonces* $\operatorname{ord}(f)$ *es igual al mínimo común múltiplo de* $\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_k)$.

Demostración. Si $g_i(0) = 0$ para algún $1 \leq i \leq k$, podemos escribir $f(x) = x^r h_1(x) \cdots h_k(x)$ con $r \in \mathbb{N}$ tal que $h_i(0) \neq 0$ para todo $1 \leq i \leq k$, y por la definición de orden, el orden de f y de $h_1 \cdots h_k$ es el mismo. Por tanto basta considerar el caso en que $g_i(0) \neq 0$ para todo $1 \leq i \leq k$.

Sea $e = \operatorname{ord}(f)$, $e_i = \operatorname{ord}(g_i)$ para todo $1 \leq i \leq k$, y $c = \operatorname{mcm}(e_1, \ldots, e_k)$. Entonces, $g_i(x) \mid x^{e_i} - 1$ para todo $1 \leq i \leq k$ y $x^{e_i} - 1 \mid x^c - 1$. Por lo tanto $g_i(x)$ divide $x^c - 1$ para todo $1 \leq i \leq k$ y como son coprimos dos a dos, obtenemos que $f(x)$ divide $x^c - 1$ y por el Lema 2.16 e divide a c.

Por otro lado, $f(x)$ divide $x^e - 1$, luego $g_i(x)$ divide $x^e - 1$ para todo $1 \leq i \leq k$. De nuevo por el Lema 2.16, deducimos que $e_i \mid e$ para todo $1 \leq i \leq k$, y por lo tanto c divide a e.

Concluimos así que $e = c$. □

Finalmente, combinando los dos teoremas previos, podemos obtener el orden de un polinomio a partir de los órdenes de su descomposición canónica.

Teorema 2.19. *Sea $\mathbb{F}_q$ un cuerpo finito de característica p, y sea $f \in \mathbb{F}_q[x]$ un polinomio de grado mayor o igual que 1 tal que $f(0) \neq 0$. Sea $f = a f_1^{b_1} \cdots f_k^{b_k}$, con $a \in \mathbb{F}_q$, $b_1 \ldots b_k \in \mathbb{N}$ y $f_1, \ldots f_k \in \mathbb{F}_q[x]$ polinomios mónicos e irreducibles distintos, la descomposición canónica de f en $\mathbb{F}_q[x]$. Entonces* $\operatorname{ord}(f) = ep^t$ *donde e es el mínimo común múltiplo de* $\operatorname{ord}(f_1), \ldots, \operatorname{ord}(f_k)$ *y t el menor natural tal que $p^t \geq \max\{b_1, \ldots, b_k\}$.*

Demostración. Como $f_1, \ldots f_k$ son polinomios irreducibles distintos, claramente son coprimos dos a dos y por tanto $f_1^{b_1} \ldots f_k^{b_k}$ también son coprimos dos a dos. Por tanto podemos aplicar el Teorema 2.18 a estos polinomios, y deducimos que $\operatorname{ord}(f)$ es igual al mínimo común múltiplo de $\operatorname{ord}(f_1^{b_1}), \ldots, \operatorname{ord}(f_k^{b_k})$.

Aplicando el Teorema 2.17 a $f_i^{b_i}$ tenemos que $\operatorname{ord}(f_i^{b_i}) = \operatorname{ord}(f) p^{t_i}$, con t_i el menor natural tal que $p^{t_i} \geq b_i$, para todo $1 \leq i \leq k$. Por lo tanto,

$$\operatorname{mcm}\{\operatorname{ord}(f_1^{b_1}), \ldots, \operatorname{ord}(f_k^{b_k})\} = \operatorname{mcm}\{\operatorname{ord}(f_1), \ldots, \operatorname{ord}(f_k)\} \cdot p^{\max\{t_1, \ldots, t_k\}} = ep^t$$

ya que claramente el máximo de $t_1, \ldots, t_k$ es el menor natural tal que $p^{\max\{t_1, \ldots, t_k\}} \geq \max\{b_1, \ldots, b_k\}$. □

2.2. Número de polinomios irreducibles

Ya hemos visto al final del primer capítulo que siempre tenemos un polinomio irreducible de cualquier grado en un cuerpo $\mathbb{F}_q$. El objetivo de esta sección es determinar cuántos polinomios hay para un grado fijo utilizando las funciones φ de Euler y μ de Möbius.

También obtendremos fórmulas explícitas para el producto de polinomios irreducibles, que podríamos factorizar para extraer todos los polinomios irreducibles de cierto grado. Para esta sección nos apoyaremos tanto en el capítulo 13 del libro *Applied Abstract Algebra* [11] como en el 3.2 del libro *Introduction to finite fields and their applications* [10].

Empezamos definiendo las funciones φ de Euler y μ de Möbius.

Definición 2.20. Sea φ la función phi de Euler, donde $\varphi(n)$ indica el número de enteros positivos menores o iguales que n que son coprimos con n.

Si $n = p_1^{t_1} \cdots p_k^{t_k}$, donde los p_i son primos distintos, entonces

$$\varphi(n) = (p_1 - 1)p_1^{t_1-1} \cdots (p_k - 1)p_k^{t_k-1} = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Definición 2.21. La aplicación $\mu : \mathbb{N} \to \{0, 1, -1\}$ definida por

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^k & \text{si } n \text{ es el producto de } k \text{ primos distintos}, \\ 0 & \text{si } n \text{ es divisible por el cuadrado de un primo.} \end{cases}$$

se llama la función μ de Möbius.

Vemos una propiedad simple y que nos será muy útil de la función μ de Möbius.

Lema 2.22.

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \textit{si } n = 1, \\ 0 & \textit{si } n > 1. \end{cases}$$

Demostración. Para verificar esto, si $n > 1$, sólo debemos considerar aquellos divisores positivos d de n tales que $\mu(d) \neq 0$, es decir, para los cuales $d = 1$ o d es un producto de primos distintos.

Si $p_1, p_2, \ldots, p_k$ son los primos distintos que dividen a n, entonces obtenemos:

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{1 \leq i_1 < i_2 \leq k} \mu(p_{i_1}p_{i_2}) + \sum_{1 \leq i_1 < i_2 < i_3 \leq k} \mu(p_{i_1}p_{i_2}p_{i_3}) + \cdots + \mu(p_1p_2 \cdots p_k)$$

$$= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k = (1 + (-1))^k = 0.$$

El caso $n = 1$ es trivial. □

El siguiente teorema nos permitirá usar la función μ de Möbius para poder contar el número de polinomios irreducibles de grado fijo.

Teorema 2.23. Fórmula de Inversión de Möbius.

(i) ***(Forma aditiva)*** *Sean $f, g : \mathbb{N} \to (A, +)$ aplicaciones de $\mathbb{N}$ en un grupo abeliano aditivo A. Entonces:*

$$g(n) = \sum_{d|n} f(d) \quad \Longleftrightarrow \quad f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d).$$

(ii) ***(Forma multiplicativa)*** *Sean $f, g : \mathbb{N} \to (A, \cdot)$ aplicaciones de $\mathbb{N}$ en un grupo abeliano multiplicativo A. Entonces:*

$$g(n) = \prod_{d|n} f(d) \quad \Longleftrightarrow \quad f(n) = \prod_{d|n} g(d)^{\mu(n/d)}.$$

Demostración. Empezamos por la implicación a la derecha de la forma aditiva.

Suponemos $g(n) = \sum_{d|n} f(d)$ y, considerando el lema previo en la última igualdad, obtenemos

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

Las últimas igualdades se obtienen considerando que, para cada c fijo con $c \mid \frac{n}{d}$, tenemos que d cumple $d \mid \frac{n}{c}$, y como c recorre todos los divisores de n, podemos reordenar la suma cambiando los papeles de c y d.

Para el recíproco, suponiendo $g(n) = \sum_{d|n} f(d)$ y considerando una idea similar para reordenar las sumas, tenemos

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \sum_{c|d} \mu\left(\frac{d}{c}\right) g(c) = \sum_{c|n} g(c) \sum_{\substack{d:c|d \\ d|n}} \mu\left(\frac{d}{c}\right).$$

Consideramos el cambio de variable $d = c \cdot m$, donde $m \mid \frac{n}{c}$, y aplicando el lema previo, podemos continuar la igualdad con

$$\sum_{c|n} g(c) \sum_{m|\frac{n}{c}} \mu(m) = g(n).$$

La forma multiplicativa es la misma que la aditiva pero reemplazando sumas por productos y productos por potencias. □

Ahora tenemos todas las herramientas necesarias para empezar a contar polinomios irreducibles. Primero contamos los polinomios irreducibles mónicos con el grado y orden fijo.

Teorema 2.24. *Sea $e \in \mathbb{N}$ un divisor de $q^m - 1$. Entonces hay exactamente $\frac{\varphi(e)}{m}$ polinomios irreducibles mónicos de grado m y orden $e \geq 2$ sobre $\mathbb{F}_q$.*

Demostración. Si e es el orden asociado a un polinomio irreducible de grado m, por el Corolario 2.14, tenemos que $e \mid q^m - 1$. Entonces $x^e - 1 \mid x^{q^m-1} - 1$, y m es el menor natural que cumple esto, ya que por el Corolario 2.4, sabemos que $\mathbb{F}_{q^m}$ es el menor cuerpo de descomposición de estos polinomios.

Primero veremos que los polinomios irreducibles mónicos de grado m y orden e son exactamente los polinomios mínimos de las raíces primitivas e-ésimas de la unidad.

Sea f es un polinomio irreducible mónico de grado m y orden e, y α una de sus raíces. Si $m \geq 2$, por el Teorema 2.13, todas las raíces de f son raíces primitivas e-ésimas de la unidad. Si $m = 1$, usando que f tiene orden e, es fácil ver que su raíz es una raíz primitiva e-ésima de la unidad. Finalmente, por el Teorema 2.10(iv), tenemos que $f = m_\alpha$, el polinomio mínimo de una raíz primitiva e-ésima de la unidad.

Ahora consideremos m_α el polinomio mínimo asociado a una raíz primitiva e-ésima de la unidad, α tiene orden e, y por el Teorema 2.10(vi) sabemos que todas sus raíces son los conjugados de α. Usando esto, por el Teorema 2.6, todas las raíces de m_α tienen orden e. Como m es el menor natural que cumple $x^e - 1 \mid x^{q^m-1} - 1$, el cuerpo de descomposición de todas las raíces de m_α es $\mathbb{F}_{q^m}$ y por tanto el grado del polinomio mínimo es $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = [\mathbb{F}_{q^m} : \mathbb{F}_q] = m$.

Además, como todas sus raíces tienen orden e, tenemos que e es el menor natural tal que $m_\alpha \mid x^e - 1$, y por tanto, e es el orden de m_α. Así tenemos que este polinomio mínimo es un polinomio irreducible mónico de grado m y orden e.

Finalmente, como tenemos $\varphi(e)$ raíces primitivas e-ésimas de la unidad, tenemos $\varphi(e)$ polinomios mínimos asociados. Como ya hemos visto antes, todas las raíces de estos polinomios son raíces primitivas e-ésimas de la unidad, y por el Teorema 2.10(vi), las m raíces de uno de estos polinomios generan el mismo polinomio mínimo. Por tanto, tenemos $\frac{\varphi(e)}{m}$ polinomios mínimos distintos, es decir, tenemos $\frac{\varphi(e)}{m}$ polinomios irreducibles mónicos de grado m y orden e. □

Gracias a los resultados de las raíces de polinomios irreducibles, sabemos cuáles son los polinomios que dividen a $x^{q^n} - x$, y podemos emplear este hecho para dar su factorización en polinomios irreducibles. Además, esto nos permitirá enumerar todos los polinomios irreducibles mónicos de grado fijo.

Teorema 2.25. *Se verifica la igualdad $x^{q^n} - x = \prod_i f_i$, con el producto extendido sobre todos los polinomios irreducibles mónicos distintos sobre $\mathbb{F}_q$ cuyos grados dividen a n.*

Demostración. Por el Lema 2.2, todos los polinomios que dividen a $x^{q^n} - x$ son los polinomios mónicos irreducibles cuyos grados dividen a n sobre $\mathbb{F}_q$, a excepción de productos por una constante.

Además, como la derivada de $x^{q^n} - x$ es -1, el polinomio no tiene raíces repetidas. Esto implica que en su descomposición en polinomios irreducibles no hay ninguno repetido. Por último, como no comparten raíces, los polinomios son coprimos.

Entonces tenemos que estos polinomios son todos los que dividen a $x^{q^n} - x$, ninguno se repite y todos son coprimos entre ellos. Luego el producto de todos ellos debe ser igual a $x^{q^n} - x$. □

Corolario 2.26. *Sea $N_q(d)$ el número de polinomios irreducibles mónicos en $\mathbb{F}_q[x]$ de grado d. Entonces, para todo $n \in \mathbb{N}$ se tiene*

$$q^n = \sum_{d|n} d \cdot N_q(d),$$

donde la suma se extiende sobre todos los divisores positivos d de n.

Demostración. El resultado se deduce del teorema previo comparando el grado de $x^{q^n} - x$ con el grado total de la factorización de $x^{q^n} - x$. □

Aplicando las propiedades de la función μ de Möbius, del corolario anterior obtenemos una fórmula explícita para el número de polinomios irreducibles mónicos con grado fijo.

Teorema 2.27. *El número de polinomios irreducibles mónicos de grado n sobre $\mathbb{F}_q$ está dado por*

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

Demostración. El Corolario 2.26 nos dice que $\sum_{d|n} d \cdot N_q(d) = q^n$. La forma aditiva de la fórmula de inversión de Möbius, Teorema 2.23(i), nos da el resultado deseado considerando $f(n) = n \cdot N_q(n)$ y $g(n) = q^n$ para todo $n \in \mathbb{N}$,

$$\sum_{d|n} d \cdot N_q(d) = q^n \Leftrightarrow n \cdot N_q(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot q^d = \sum_{d|n} \mu(d) \cdot q^{n/d}.$$

La última igualdad se obtiene cambiando d por $\frac{n}{d}$, ya que si d recorre todos los divisores de n, también los recorre $\frac{n}{d}$. □

Con esto podemos calcular la cantidad de polinomios irreducibles en un cuerpo. Las cuentas son sencillas para grados bajos y cuerpos pequeños, como por ejemplo, para polinomios de grado 10 en $\mathbb{F}_4$.

Ejemplo 2.28. El número de polinomios irreducibles mónicos en $\mathbb{F}_q[x]$ de grado 10 está dado por:

$$N_q(10) = \frac{1}{10}\left(\mu(1)q^{10} + \mu(2)q^5 + \mu(5)q^2 + \mu(10)q\right) = \frac{1}{10}\left(q^{10} - q^5 - q^2 + q\right).$$

En el caso $q = 4$ tenemos que $N_4(10)$ =104.754. Luego hay 104.754 polinomios irreducibles mónicos en $\mathbb{F}_4[x]$ de grado 10.

Usando la fórmula obtenida en el teorema, calculamos con MAPLE la Tabla 2.1 con el número de polinomios irreducibles mónicos en $\mathbb{F}_2[x]$ para todos los grados menores o iguales que 18.

Grado n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$N_2(n)$	2	1	2	3	6	9	18	30	56	99	186	335	630	1161	2182	4080	7710	14532

Cuadro 2.1: Número de polinomios irreducibles mónicos en $\mathbb{F}_2[x]$ de grado n.

Para verificar los cálculos podemos consultar la enciclopedia online de sucesiones de enteros OEIS [14], una página creada y mantenida por N. J. A. Sloane donde se almacenan miles de sucesiones de interés matemático.

Concretamente consultamos la sucesión A001037 en OEIS [14] y, considerando que su sucesión comienza en $n = 0$, vemos que hemos obtenido los mismos resultados.

Y finalmente, podemos obtener una fórmula explícita para el producto de estos polinomios.

Teorema 2.29. *El producto $I(q, n)$ de todos los polinomios irreducibles mónicos en $\mathbb{F}_q[x]$ de grado n está dado por*

$$I(q,n) = \prod_{d|n}\left(x^{q^d} - x\right)^{\mu(n/d)} = \prod_{d|n}\left(x^{q^{n/d}} - x\right)^{\mu(d)}$$

Demostración. Agrupando los productos de polinomios de grado fijo d en $I(q, d)$, el Teorema 2.25 implica que $x^{q^n} - x = \prod_{d|n} I(q, d)$.

Ahora consideraremos $f(n) = I(q, n)$ y $g(n) = x^{q^n} - x$ para todo $n \in \mathbb{N}$ y aplicando la fórmula de inversión de Möbius multiplicativa del Teorema 2.5 obtenemos

$$x^{q^n} - x = \prod_{d|n} I(q,d) \Leftrightarrow I(q,n) = \prod_{d|n}\left(x^{q^d} - x\right)^{\mu(n/d)} = \prod_{d|n}\left(x^{q^{n/d}} - x\right)^{\mu(d)}$$

donde la última igualdad se obtiene cambiando d por $\frac{n}{d}$ por un razonamiento similar al usado en el teorema previo. □

Ejemplo 2.30. Para $q = 2$, $n = 4$ obtenemos:

$$I(2,4) = (x^{16} - x)^{\mu(1)}(x^4 - x)^{\mu(2)}(x^2 - x)^{\mu(4)} = \frac{x^{16} - x}{x^4 - x} = \frac{x^{15} - 1}{x^3 - 1} = x^{12} + x^9 + x^6 + x^3 + 1.$$

Todos los polinomios irreducibles mónicos en $\mathbb{F}_2[x]$ de grado 4 pueden determinarse factorizando este polinomio, y más generalmente, todos los polinomios irreducibles mónicos de grado n sobre $\mathbb{F}_q[x]$ se pueden obtener factorizando $I(q, n)$.

2.3. Polinomios primitivos

Si tenemos un cuerpo finito $\mathbb{F}_{q^n}$, siendo q la potencia de un primo y $n \in \mathbb{N}$, representar el cuerpo como $\mathbb{F}_q[x]/(f(x))$, donde $f(x)$ es un polinomio irreducible, tiene ventajas para operar eficientemente.

Si además una de las raíces de $f(x)$ es primitiva en $\mathbb{F}_{q^n}$ nos permite representar el cuerpo como potencias de la raíz, y un polinomio con esta propiedad es de utilidad en ciertos campos, por ejemplo la generación de números pseudoaleatorios, como se puede ver en el capítulo 7.4 del libro *Introduction to finite fields and their applications* [10]. Por lo tanto esta sección se dedica a estudiar este tipo de polinomios.

Los siguientes resultados se han obtenido de la sección 7.3 del libro *Finite fields and Galois rings* [17] y de la sección 3.1 del libro *Introduction to finite fields and their applications* [10].

Definición 2.31 ([17])**.** Sea $f(x)$ un polinomio mónico de grado $n \geq 1$ sobre $\mathbb{F}_q$. Si alguna raíz de $f(x)$ es un elemento primitivo de $\mathbb{F}_{q^n}$ entonces diremos que $f(x)$ es un polinomio primitivo de grado n sobre $\mathbb{F}_q$.

Otra definición posible para los polinomios primitivos es la siguiente, encontrada por ejemplo en el libro *Introduction to finite fields and their applications* [10]. Demostramos que son definiciones equivalentes.

Lema 2.32. *Un polinomio $f(x) \in \mathbb{F}_q[x]$ de grado $n \geq 1$ es primitivo sobre $\mathbb{F}_q$ si y solo si es el polinomio mínimo en $\mathbb{F}_q$ de un elemento primitivo de $\mathbb{F}_{q^n}$.*

Demostración. Si $f(x)$ es primitivo, supongamos que ξ es una raíz de $f(x)$ y un elemento primitivo de $\mathbb{F}_{q^n}$. Consideremos m_ξ el polinomio mínimo de ξ, y aplicando el Teorema 2.10 tenemos que el grado de m_ξ es n y $m_\xi \mid f$. Como $f(x)$ también es un polinomio mónico de grado n, $m_\xi = f$.

La otra implicación es inmediata. □

El siguiente teorema recopila las propiedades más relevantes de los polinomios primitivos. El resultado más importante es el que nos dice que todos los polinomios primitivos son irreducibles.

Teorema 2.33 ([17])**.** *Para cada cuerpo finito $\mathbb{F}_q$ y $n \in \mathbb{N}$ existe un polinomio primitivo de grado n en $\mathbb{F}_q$. Además, todas las raíces de un polinomio primitivo de grado n en $\mathbb{F}_q$ son elementos primitivos de $\mathbb{F}_{q^n}$ y todos los polinomios primitivos en $\mathbb{F}_q$ son irreducibles sobre $\mathbb{F}_q$. Finalmente, el número de polinomios primitivos de grado n en $\mathbb{F}_q$ es $\varphi(q^n - 1)/n$.*

Demostración. Sea $\mathbb{F}_q$ un cuerpo finito cualquiera y $n \in \mathbb{N}$. Consideramos ξ un elemento primitivo de $\mathbb{F}_{q^n}$ y su polinomio mínimo m_ξ, que aplicando el Teorema 2.10(iii) vemos que es de grado n, luego por el lema previo es un polinomio primitivo de grado n en $\mathbb{F}_q$.

Ahora sea $f(x)$ un polinomio primitivo de grado n en $\mathbb{F}_q$. Por el lema previo es un polinomio mínimo, luego es irreducible, y aplicando el Teorema 2.10(vi) y el Teorema 2.6 todas sus raíces tienen el mismo orden y por tanto son primitivas en $\mathbb{F}_{q^n}$.

Finalmente, como $\varphi(q^n - 1)$ es el número de elementos primitivos de $\mathbb{F}_{q^n}$, si consideramos el polinomio mínimo en $\mathbb{F}_q$ asociado a un elemento primitivo ξ, por el Teorema 2.10 el polinomio mínimo es el mismo para los n elementos primitivos $\xi, \xi^q, \ldots \xi^{q^{n-1}}$ y es distinto del polinomio mínimo asociado a otro elemento primitivo. Entonces, por el lema previo, el número de polinomios primitivos de grado n sobre $\mathbb{F}_q$ es $\varphi(q^n - 1)/n$. □

Ahora podemos obtener la primera caracterización de los polinomios primitivos, que nos dice que un polinomio es primitivo si y solo si es de orden máximo. La condición $f(0) \neq 0$ solo se necesita para descartar el polinomio $f(x) = x \in \mathbb{F}_2$, que claramente no es primitivo.

Teorema 2.34 ([10])**.** *Un polinomio $f \in \mathbb{F}_q[x]$ de grado m es primitivo sobre $\mathbb{F}_q$ si y solo si f es mónico, $f(0) \neq 0$, y $\operatorname{ord}(f) = q^m - 1$.*

Demostración. Si f es primitivo sobre $\mathbb{F}_q$, por Teorema 2.33 f es mónico e irreducible, luego $f(0) \neq 0$. Como f es irreducible y al ser primitivo tiene raíces de orden $q^m - 1$, por el Teorema 2.13 obtenemos que $\operatorname{ord}(f) = q^m - 1$.

Para probar el recíproco suponemos que f es mónico, $f(0) \neq 0$, y $\text{ord}(f) = q^m - 1$, claramente $\text{ord}(f) = q^m - 1$ implica que $m > 1$. Primero probamos la irreducibilidad de f por reducción al absurdo, suponiendo que f es reducible sobre $\mathbb{F}_q$. Si f es reducible o es una potencia de un polinomio irreducible, o descompone como producto de dos polinomios coprimos de grado positivo.

Si $f = g^b$ con $g \in \mathbb{F}_q[x]$ irreducible sobre $\mathbb{F}_q$, $g(0) \neq 0$ y $b \geq 2$, de acuerdo con el Teorema 2.17, la característica de $\mathbb{F}_q$ divide $\text{ord}(f)$ y por tanto divide $q^m - 1$, lo cual es una contradicción.

En el segundo caso, tenemos $f = g_1 g_2$ con $g_1, g_2 \in \mathbb{F}_q[x]$ mónicos, coprimos y de grados positivos m_1 y m_2, respectivamente. Si $e_i = \text{ord}(g_i)$ para $i = 1, 2$, entonces por el Teorema 2.18 se cumple $\text{ord}(f) \leq e_1 e_2$. Además, por el Lema 2.11 se tiene $e_i \leq q^{m_i} - 1$ para $i = 1, 2$, y por lo tanto $\text{ord}(f) \leq (q^{m_1} - 1)(q^{m_2} - 1) < q^{m_1+m_2} - 1 = q^m - 1$, lo cual es una contradicción.

Por lo tanto, f es irreducible sobre $\mathbb{F}_q$, y se sigue del Teorema 2.13 que f tiene una raíz de orden $q^m - 1$ en $\mathbb{F}_{q^m}^*$ y entonces es un polinomio primitivo sobre $\mathbb{F}_q$. □

Para la segunda caracterización de polinomios primitivos necesitamos el siguiente lema.

Lema 2.35 ([10]). *Sea $f \in \mathbb{F}_q[x]$ un polinomio no constante con $f(0) \neq 0$ y sea r el menor natural tal que x^r es congruente módulo $f(x)$ a algún elemento de $\mathbb{F}_q$. Si ese elemento es $a \in \mathbb{F}_q^*$ entonces $\text{ord}(f) = hr$, donde h es el orden de a en $\mathbb{F}_q^*$.*

Demostración. Si $\text{ord}(f) = e$, por la Definición 2.12, $f \mid x^e - 1$ luego $x^e \equiv 1 \bmod f(x)$ y entonces tenemos que $e \geq r$. Podemos escribir $e = sr + t$ con $s \in \mathbb{N}$ y $0 \leq t < r$.

Entonces,

$$1 \equiv x^e \equiv x^{sr+t} \equiv a^s x^t \bmod f(x) \ , \ x^t \equiv a^{-s} \bmod f(x)$$

y por la definición de r, esto solo es posible si $t = 0$.

La equivalencia queda $a^s \equiv 1 \bmod f(x)$, y al no depender de x, esto indica que $a^s - 1 = 0$, y entonces $s \geq h$ y $e = sr \geq hr$. Por otro lado, $x^{hr} \equiv a^h \equiv 1 \bmod f(x)$, y por lo tanto $hr \geq e$, y $hr = e$. □

Teorema 2.36 ([10]). *El polinomio mónico $f \in \mathbb{F}_q[x]$ de grado $m \geq 1$ es un polinomio primitivo sobre $\mathbb{F}_q$ si y solo si $(-1)^m f(0)$ es un elemento primitivo de $\mathbb{F}_q$ y el menor $r \in \mathbb{N}$ tal que x^r es congruente módulo $f(x)$ a algún elemento de $\mathbb{F}_q$ es $r = (q^m - 1)/(q - 1)$.*

En el caso en que f sea primitivo sobre $\mathbb{F}_q$, se cumple que $x^r \equiv (-1)^m f(0) \bmod f(x)$.

Demostración. Si f es primitivo de grado m sobre $\mathbb{F}_q$, entonces f tiene una raíz $\alpha \in \mathbb{F}_{q^m}$, la cual es un elemento primitivo de $\mathbb{F}_{q^m}$. Por el Teorema 2.10 f es el polinomio mínimo de α y podemos descomponerlo como $f(x) = (x - \alpha)(x - \alpha^q) \cdots (x - \alpha^{q^{m-1}})$, lo que nos proporciona la siguiente igualdad,

$$f(0) = (-1)^m \alpha \cdot \alpha^q \cdots \alpha^{q^{m-1}} = (-1)^m \alpha^{\frac{q^m-1}{q-1}}.$$

Entonces tenemos que $\alpha^{\frac{q^m-1}{q-1}} = (-1)^m f(0) \in \mathbb{F}_q$, y como α tiene orden $q^m - 1$, se deduce que el orden de $(-1)^m f(0)$ en $\mathbb{F}_q^*$ es $q - 1$; es decir, $(-1)^m f(0)$ es un elemento primitivo de $\mathbb{F}_q$.

Si consideramos el polinomio $g(x) = x^{\frac{q^m-1}{q-1}} - \alpha^{\frac{q^m-1}{q-1}}$, tenemos que $g(\alpha) = 0$ y por el Teorema 2.10 $f \mid g$. Luego $x^{\frac{q^m-1}{q-1}} \equiv \alpha^{\frac{q^m-1}{q-1}} \bmod f(x)$, que por definición de r implica que $r \leq \frac{q^m-1}{q-1}$.

Por el Lema 2.35, como el orden máximo en $\mathbb{F}_q^*$ es $q - 1$, $\text{ord}(f) \leq (q - 1)r$ y por el Teorema 2.34 $\text{ord}(f) = q^m - 1$, luego $r \geq \frac{q^m-1}{q-1}$ y entonces tenemos que $r = \frac{q^m-1}{q-1}$ y el elemento que cumple las condiciones del teorema es $(-1)^m f(0)$.

Recíprocamente, supongamos que se satisfacen las condiciones del teorema. De la igualdad $r = \frac{q^m-1}{q-1} = q(q^{m-2} + \cdots + 1) + 1$ se deduce que r y q son coprimos, y por el Lema 2.35 tenemos que

$\text{ord}(f) = hr$ donde h es el orden de un elemento en $\mathbb{F}_q^*$, es decir que $h \mid q-1$, y por tanto h y q son relativamente coprimos. De esto deducimos que $\text{ord}(f)$ y q son coprimos.

Por el Teorema 2.19, si la descomposición canónica de f es $f(x) = f_1^{b_1}(x) \cdots f_k^{b_k}(x)$, tenemos que $\text{ord}(f) = ep^t$ con e, p, t definidos de la forma indicada en el teorema. Al ser p la característica de $\mathbb{F}_q$, para que $\text{ord}(f)$ y q sean coprimos, t debe ser 0. Entonces, por la definición de t, $b_1 = \cdots = b_k = 1$ y por tanto $f(x) = f_1(x) \cdots f_k(x)$ donde f_i, $1 \leq i \leq k$, son polinomios mónicos e irreducibles en $\mathbb{F}_q$.

Si $m_i = \deg(f_i)$, entonces $\text{ord}(f_i) \mid q^{m_i} - 1$ para $1 \leq i \leq k$, según el Corolario 2.14. Ahora bien, para cualquier $i \in \{1, \ldots, k\}$ claramente $q^{m_i} - 1$ divide a

$$d = \frac{(q^{m_1} - 1) \cdots (q^{m_k} - 1)}{q^k - 1} = (q^{m_i} - 1)(\frac{q^{m_1} - 1}{q-1} \cdots \frac{q^{m_{i-1}} - 1}{q-1} \frac{q^{m_{i+1}} - 1}{q-1} \cdots \frac{q^{m_k} - 1}{q-1}).$$

Por lo tanto $\text{ord}(f_i)$ divide d para $1 \leq i \leq k$.

Del Lema 2.16 se deduce que $f_i(x)$ divide $x^d - 1$ para todo i, y por consiguiente $f(x)$ divide $x^d - 1$ y $x^d \equiv 1 \bmod f(x)$. Si suponemos $k > 1$, entonces $d < \frac{q^{m_1 + \cdots m_k} - 1}{q-1} = r$, lo cual contradice la definición de r. Por lo tanto, $k = 1$ y f es irreducible sobre $\mathbb{F}_q$.

Si $\beta \in \mathbb{F}_{q^m}$ es una raíz de f, por un razonamiento similar al del principio de la demostración, f es el polinomio mínimo de β y deducimos que $\beta^r = (-1)^m f(0)$, y por tanto, $x^r \equiv (-1)^m f(0) \bmod f(x)$.

Dado que el orden de $(-1)^m f(0)$ en $\mathbb{F}_q^*$ es $q-1$, se deduce del Lema 2.35 que $\text{ord}(f) = q^m - 1$, y por lo tanto, f es primitivo sobre $\mathbb{F}_q$ según el Teorema 2.34. □

Para la segunda parte de la sección obtenemos resultados que garantizan que ciertos tipos de polinomios nunca pueden ser primitivos. Estos se han obtenido del artículo de Li Yujuan, Wang Huaifu y Zhao Jinhua [9], donde se muestra que hay interés reciente por este tipo de polinomios debido a sus aplicaciones.

Teorema 2.37. *Sean $m, n \geq 2$ números naturales y p primo. Los trinomios de la forma $x^n + ax + b$ sobre $\mathbb{F}_{p^m}$ no son primitivos si $b^{1-n}a^n \in \mathbb{F}_{p^u}^*$, donde $\mathbb{F}_{p^u}$ denota un subcuerpo propio de $\mathbb{F}_{p^m}$.*

Como el artículo requiere algo de estudio previo de Linear Feedback Shift Registers (LFSR), no veremos la demostración del teorema, pero queda demostrado por los autores en el artículo. Además, nos permite demostrar el siguiente corolario solo utilizando resultados que ya conocemos.

Corolario 2.38. *Sean $m, n \geq 2$ números naturales y p primo. No existen trinomios primitivos de la forma $x^n + jx + \lambda \in \mathbb{F}_{p^m}[x]$ si $j \in \mathbb{F}_{p^u}^*$, con $\mathbb{F}_{p^u}$ un subcuerpo propio de $\mathbb{F}_{p^m}$ y $n \equiv 1 \bmod p^m - 1$.*

Demostración. Sea $x^n + jx + \lambda$ un trinomio que cumple las condiciones del corolario, luego tenemos que $\lambda \in \mathbb{F}_{p^m}^*$ así que se tiene $\lambda^{p^m - 1} = 1$, y $n \equiv 1 \bmod p^m - 1$.

Entonces $\lambda^{n-1} = 1 \in \mathbb{F}_{p^u}^*$ y, como $j \in \mathbb{F}_{p^u}^*$, tenemos que $j^n \in \mathbb{F}_{p^u}^*$. Por lo tanto, $\lambda^{1-n} j^n \in \mathbb{F}_{p^u}^*$ y aplicando el Teorema 2.37 obtenemos que $x^n + jx + \lambda$ no es primitivo. □

Si nos restringimos al caso en $\mathbb{F}_4$, obtenemos un resultado muy interesante. El teorema presentado en el artículo también se demostraba para los $n \equiv 4 \bmod 5$, pero este caso requiere un desarrollo previo de Linear Feedback Shift Registers (LFSR), luego para este trabajo nos limitamos a los casos $n \equiv 0, 1 \bmod 3$, que sí podemos demostrar con los resultados ya vistos.

Teorema 2.39. *Si $n \equiv 0, 1 \bmod 3$ entonces no existen trinomios primitivos de la forma $x^n + x + \alpha$ sobre $\mathbb{F}_4$.*

Demostración. Sea $x^n + x + \alpha$ un trinomio en $\mathbb{F}_4$. Por el Teorema 2.36, si α no es un elemento primitivo de $\mathbb{F}_4$ entonces $x^n + x + \alpha$ no es primitivo en $\mathbb{F}_4$, ya que en este cuerpo $-1 = 1$.

Ahora consideramos el caso en el que α es un elemento primitivo de $\mathbb{F}_4$, es decir, α es generador de $\mathbb{F}_4^* = \{1, \alpha, \alpha+1\}$ y por tanto $\alpha^2 = \alpha + 1$.

Si $n \equiv 1 \bmod 3$, es un caso particular del Corolario 2.38 con $m = 2$, $p = 2$, $j = 1$ y $\lambda = \alpha$.

Si $n \equiv 0 \bmod 3$, entonces $n = 3z$ y el trinomio queda $x^{3z} + x + \alpha$. Como

$$(\alpha + 1)^3 = \alpha^3 + 3\alpha^2 + 3\alpha + 1 = 1 + (\alpha + 1) + \alpha + 1 = 1$$

claramente α+1 es raíz del trinomio. Luego el trinomio no es irreducible sobre $\mathbb{F}_4$ y por el Teorema 2.33 no puede ser primitivo sobre $\mathbb{F}_4$. □

Capítulo 3

Construcción de polinomios irreducibles sobre cuerpos finitos

Una vez vistas las propiedades de los polinomios irreducibles, nos centramos en construirlos de forma explícita viendo condiciones de irreducibilidad y exponemos algunos ejemplos en cuerpos finitos concretos, como $\mathbb{F}_2$.

Empezaremos viendo criterios de irreducibilidad para cualquier polinomio sobre un cuerpo finito, y luego desarrollaremos criterios para ciertos tipos de polinomios. Primero cubriremos los binomios y trinomios que, al tener pocos coeficientes distintos de cero, son fáciles de manejar y permiten construcciones explícitas que siempre son irreducibles.

También estudiaremos los polinomios autorrecíprocos, estos se pueden conseguir a partir de cualquier polinomio aplicando un operador que, bajo ciertas condiciones, mantiene la irreducibilidad.

Finalmente, dada su gran importancia en varias áreas del álgebra, dedicamos una sección a estudiar las propiedades de los polinomios ciclotómicos y su irreducibilidad.

3.1. Criterios de irreducibilidad

Si queremos estudiar apropiadamente los polinomios irreducibles, es necesario tener criterios para saber si un polinomio dado es irreducible. En esta sección probaremos algunos criterios expuestos en el capítulo 10.1 del libro *Finite fields and Galois rings* [17].

Empezamos viendo tres condiciones necesarias para la irreducibilidad de polinomios.

Teorema 3.1. *Sea $f(x)$ un polinomio sobre $\mathbb{F}_q$. Si $f(x)$ es irreducible sobre $\mathbb{F}_q$, entonces se cumplen las siguientes condiciones.*

(i) El término constante de $f(x)$ es distinto de cero.

(ii) La suma de los coeficientes de $f(x)$ es distinta de cero.

(iii) $\mathrm{mcd}(f(x), f'(x)) = 1$.

Demostración. Para los tres casos, probamos el contrarrecíproco.

(i) Claramente, si el término constante es cero entonces x divide a $f(x)$.

(ii) Si los coeficientes de $f(x)$ suman cero, entonces $f(1) = 0$ y por tanto $x - 1$ divide a $f(x)$.

(iii) Si el $\mathrm{mcd}(f(x), f'(x)) \neq 1$, como el grado de $f'(x)$ es menor que el de $f(x)$, tenemos que $\mathrm{mcd}(f(x), f'(x))$ divide a $f(x)$. □

Para el caso $q = 2$, podemos obtener algunas condiciones más.

Corolario 3.2. *Sea $f(x) \in \mathbb{F}_2[x]$. Si $f(x)$ es irreducible sobre $\mathbb{F}_2$, entonces se verifica lo siguiente.*

(i) El número de términos de $f(x)$ con coeficiente igual a 1 es impar.

(ii) Existe un término x^m en $f(x)$ con coeficiente igual a 1 tal que $2 \nmid m$.

Demostración.

(i) Es un caso particular del Teorema 3.1(ii) cuando el cuerpo es $\mathbb{F}_2$.

(ii) Lo vemos por reducción al absurdo. Si el polinomio es de la forma $f(x) = 1 + x^{m_1} + \cdots + x^{m_k}$ para algunos $k, m_1, \ldots, m_k \in \mathbb{N}$ tal que $2 \mid m_i$ con $i = 1, \ldots, k$, como estamos en un cuerpo de característica 2,
$$f(x) = (1 + x^{m_1/2} + \cdots + x^{m_k/2})^2$$
con lo que $f(x)$ es reducible y tenemos un absurdo. □

Para los siguientes resultados, necesitamos definir el polinomio recíproco.

Definición 3.3. Sea
$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x],$$
donde $a_n \neq 0$. Entonces, el polinomio recíproco $\tilde{f}$ de f se define como
$$\tilde{f}(x) = x^n f\left(\frac{1}{x}\right) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n.$$

Podemos estudiar la irreducibilidad del recíproco o la del polinomio original indistintamente, como muestra este teorema.

Teorema 3.4. *Sea $f(x)$ un polinomio de grado $n > 1$ con constante distinta de cero sobre $\mathbb{F}_q$. Entonces $f(x)$ es irreducible si y solo si su polinomio recíproco $\tilde{f}(x)$ es irreducible.*

Demostración. Vamos a demostrar que $f(x)$ es reducible si y solo si $\tilde{f}(x)$ es reducible.

Si $f(x)$ es reducible, $f(x) = g(x)h(x)$ para algunos $g, h \in \mathbb{F}_q[x]$ de grado mayor que 1. Entonces
$$x^n \cdot f\left(\frac{1}{x}\right) = x^{\deg g} \cdot g\left(\frac{1}{x}\right) \cdot x^{\deg h} \cdot h\left(\frac{1}{x}\right), \ \tilde{f}(x) = \tilde{g}(x)\tilde{h}(x)$$
y, como la constante de $f(x)$ es distinta de cero, también lo son las de $g(x)$ y $h(x)$. Por tanto los grados de sus polinomios recíprocos siguen siendo mayor que 1 y $\tilde{f}(x)$ es reducible.

Si $\tilde{f}(x)$ es reducible, como la constante de $f(x)$ es no nula, se ve claramente de la definición que $\tilde{\tilde{f}}(x) = f(x)$. Entonces, aplicando el razonamiento previo a $\tilde{f}(x)$, $f(x)$ es reducible. □

De momento solo tenemos condiciones necesarias para saber si un polinomio es irreducible. El siguiente resultado nos dará una condición necesaria y suficiente que nos reduce el problema de irreducibilidad a calcular un mínimo común divisor para una lista de polinomios.

Teorema 3.5. *Sea $f(x) \in \mathbb{F}_q[x]$ un polinomio de grado n. Entonces $f(x)$ es irreducible sobre $\mathbb{F}_q$ si y solo si se cumplen las siguientes condiciones.*

(i) El polinomio $f(x)$ divide a $x^{q^n} - x$.

(ii) Para todo número natural $i < n$ tal que $i \mid n$ se tiene que $\mathrm{mcd}(f(x), x^{q^i} - x) = 1$.

Demostración. Si $f(x)$ es irreducible sobre $\mathbb{F}_q$, por el Lema 2.2 se cumplen (i) y (ii).

Si $f(x)$ no es irreducible sobre $\mathbb{F}_q$, entonces tiene un factor irreducible $g(x)$ sobre $\mathbb{F}_q$. Supongamos que (i) se cumple y que $\deg(g(x)) = m$, veamos que entonces (ii) no se cumple.

Sea α una raíz de $g(x)$, entonces es raíz de $f(x)$ y de $x^{q^n} - x$. Como $\alpha^{q^n} - \alpha = 0$ tenemos que $\alpha \in \mathbb{F}_{q^n}$ y como $g(x)$ es un polinomio irreducible de grado m en $\mathbb{F}_q[x]$, aplicando el Teorema 1.10 podemos escribir $\mathbb{F}_{q^m} = \mathbb{F}_q[\alpha]$. Entonces $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$, lo que implica por el Teorema 1.6 que $m \mid n$.

Por tanto aplicando otra vez el Lema 2.2 se tiene que $g(x)$ divide a $(x^{q^m} - x)$, y por tanto $\mathrm{mcd}(f(x), x^{q^m} - x) \neq 1$ para algún $m < n$ tal que $m \mid n$. □

3.2. Binomios

En esta sección caracterizaremos todos los binomios irreducibles siguiendo el apartado 10.2 del libro *Finite fields and Galois rings* [17]. Empezamos viendo unos lemas que nos lo permitirán.

Recordamos que, para cualquier m natural, $\mathbb{Z}_m^*$ denota el grupo multiplicativo de todas las clases módulo m cuyos representantes son coprimos con m, y $\mathrm{ord}_m(a)$ denota el orden de la clase $\bar{a}$ en el grupo $\mathbb{Z}_m^*$.

Lema 3.6. *Sean $q \geq 2$ y $m \geq 2$ enteros coprimos, y sea* $\mathrm{ord}_m(q) = l$. *Sea $t \geq 2$ un entero tal que se cumplen las siguientes condiciones.*

(i) Todo divisor primo de t divide a m, pero no a $(q^l - 1)/m$.

(ii) Si $4 \mid t$, entonces $4 \mid (q^l - 1)$.

Entonces $\mathrm{ord}_{mt}(q) = lt$.

Demostración. Podemos considerar el $\mathrm{ord}_{mt}(q)$ ya que t divide a m y por tanto es coprimo con q, luego mt es coprimo con q.

Razonaremos por inducción sobre el número de divisores primos de t, contándolos el número de veces que indique su multiplicidad.

Supongamos que el número de divisores es 1, entonces t es primo. Como $\mathrm{ord}_m(g) = l$, $ql \equiv \mathrm{mod}\, m$ y entonces $d = \frac{ql-1}{m} \in \mathbb{Z}$. Considerando $q^l = 1 + dm$ tenemos que

$$q^{lt} = (1 + dm)^t = 1 + \binom{t}{1} dm + \binom{t}{2} (dm)^2 + \cdots + \binom{t}{t-1} (dm)^{t-1} + (dm)^t.$$

Claramente $mt \mid tmd$ y $mt \mid \binom{t}{i}(md)^i$ cuando $i = 2, \ldots, t$ ya que $t \mid m$.

Por tanto $q^{lt} \equiv 1 \,\mathrm{mod}(mt)$. Consideramos $\mathrm{ord}_m\, t(q) = k$,entonces $q^k \equiv 1 \,\mathrm{mod}(mt)$ y $k \mid lt$. De aquí obtenemos que $q^k \equiv 1 \,\mathrm{mod}\, m$, y como $\mathrm{ord}_m(q) = l$, tenemos que $l \mid k$. Como t es primo y $l \mid k, k \mid lt$, entonces $k = l$ o $k = lt$.

Suponemos que $k = l$, entonces $q^l \equiv 1 \bmod(mt), mt \mid q^l - 1$, y como $q^l - 1 = md$ tenemos $t \mid \frac{q^l-1}{m}$. Esto contradice (i), y por tanto, $k = lt$.

Ahora suponemos que el lema es cierto para enteros con $n-1$ divisores primos, y sea t con n divisores primos que cumple (i) y (ii). Veamos que $\mathrm{ord}_{mt}(gt) = lt$.

Tenemos que t tiene al menos 2 divisores primos. Consideramos $t = rt_0$ con r divisor primo de t. Podemos aplicar a r el razonamiento previo ya que lo único que pedimos es que sea primo y divida a m, y r lo cumple. Entonces $\mathrm{ord}_{mr}(q) = lr$.

Si probamos que se cumple (i) y (ii) para $\mathrm{ord}_{mr}(q) = lr$ entonces por la hipótesis de inducción tenemos que $\mathrm{ord}_{mrt_0}(q) = lrt_0$, es decir, $\mathrm{ord}_{mt}(q) = lt$.

(ii) Si $4 \mid t_0$, entonces $4|t$ y por (ii) $4 \mid q^l - 1$, además $q^l - 1 \mid q^{lr} - 1$ y tenemos que $4 \mid t_0 \Rightarrow 4 \mid q^{lr} - 1$.

(i) Sea r_0 factor primo de t_0, entonces lo es de t y por (i) tenemos que $r_0 \mid m$ y deducimos que $r_0 \mid mr$. Falta ver que $r_0 \nmid \frac{q^{lr}-1}{mr}$.

Vemos que $q^{lr} - 1 = c(q^l - 1)$ con $c = q^{l(r-1)} + \cdots + q^l + 1$. Sea $d_0 = c \cdot \frac{q^l-1}{mr} = \frac{cd}{r}$. Como r es divisor primo de t, $r \mid m$, además $q^l \equiv 1 \bmod(m)$, y de esto obtenemos que $q^l \equiv 1 \bmod(r)$. Por tanto

$$c \equiv q^{l(r-1)} + \cdots + q^l + 1 \equiv 1 + \cdots + 1 \equiv r \equiv 0 \bmod(r),\ c/r \in \mathbb{Z}.$$

Reescribimos lo que queremos conseguir,

$$\frac{q^{lr} - 1}{mr} = \frac{c(q^l - 1)}{mr} = \frac{q^l - 1}{m} \cdot \frac{c}{r},$$

como r_0 es primo, si $r_0 \nmid \frac{c}{m}$ y $r_0 \nmid \frac{q^l-1}{m}$ entonces $r_0 \nmid \frac{c}{m} \cdot \frac{q^l-1}{m}$. Ya que r_0 es divisor primo de t, tenemos por (i) que $r_0 \nmid \frac{q^l-1}{m}$, veamos que $r_0 \nmid \frac{c}{m}$. Dado que $r_0 \mid m$ y $q^l - 1 = md$, entonces

$$q^l \equiv 1 \bmod(r_0) \text{ y } c \equiv q^{l(r-1)} + \cdots + q^l + 1 \equiv 1 + \cdots + 1 \equiv r \bmod(r_0).$$

Si $r_0 \neq r$, como ambos son primos, de la igualdad anterior obtenemos $\frac{c}{r} \equiv 1 \bmod(r_0)$, luego $r_0 \nmid \frac{c}{r}$.

Si $r_0 = r$, como $q^l \equiv 1 \bmod(r)$, para cierto $b \in \mathbb{Z}$ tenemos $q^l - 1 = br$ y $q^l - 1 \equiv br \bmod(r^2)$. Entonces

$$q^{lj} \equiv (1 + br)^j \equiv 1 + \binom{j}{1} br + \binom{j}{2} (br)^2 + \cdots + \binom{j}{j} (br)^j \equiv 1 + jbr \bmod(r^2) \text{ para todo } j \in \mathbb{N},$$

$$c \equiv q^{(r-1)l} + q^{(r-2)l} + \cdots + q^l + 1 \equiv r + br \left(\sum_{j=1}^{r-1} j \right) \equiv r + br \cdot \frac{r(r-1)}{2} \bmod(r^2).$$

Se sigue que

$$\frac{c}{r} \equiv 1 + b\frac{r(r-1)}{2} \bmod(r).$$

Si $r \neq 2$, como es primo entonces es impar, y $\frac{c}{r} \equiv 1 + br\frac{r-1}{2} \equiv 1 \bmod(r)$, lo que implica que, como $r = r_0$, $r_0 \nmid \frac{c}{r}$.

Si $r = 2$ entonces $4 = rr_0$, $rr_0 \mid rt_0$ y $rt_0 = t$, así que $4 \mid t$. Por (ii) $4 \mid (q^l - 1)$. Pero en este caso $c = q^l + 1 = q^l - 1 + 2$, $c \equiv 2 \bmod(4)$, $\frac{c}{2} \equiv 1 \bmod(4)$ y finalmente $\frac{c}{2} \equiv 1 \bmod(2)$ implica que, como $r_0 = 2$, $r_0 \nmid \frac{c}{2}$. □

Corolario 3.7. *Sea q la potencia de un primo y $m \geq 2$ un entero tal que $m \mid (q-1)$. Sea $t \geq 2$ un entero que satisface las siguientes dos condiciones.*

(i) Todo divisor primo de t divide a m, pero no a $(q-1)/m$.

(ii) Si $4 \mid t$ entonces $4 \mid (q-1)$.

Entonces $\mathrm{ord}_{mt}(q) = t$.

Demostración. Claramente, $\mathrm{mcd}(q, q-1) = 1$. Como $m \mid (q-1)$, tenemos $\mathrm{mcd}(q, m) = 1$ y $q - 1 = km$ para algún $k \in \mathbb{Z}$. Luego $q \equiv 1 \bmod m$ y $\mathrm{ord}_m(q) = 1$. Por lo tanto, el corolario se obtiene inmediatamente aplicando el Lema 3.6. □

Con esta demostración podremos saber cuándo un binomio es irreducible en cualquier cuerpo.

Teorema 3.8. *Sea $t > 2$ un entero y $a \in \mathbb{F}_q^*$ con $\mathrm{ord}(a) = m > 1$. Entonces, el binomio $x^t - a$ es irreducible en $\mathbb{F}_q[x]$ si y solo si se cumplen las siguientes condiciones.*

(i) Cada factor primo de t divide a m, pero no a $(q-1)/m$.

(ii) Si $4 \mid t$ entonces $4 \mid (q-1)$.

Demostración. Observamos que $a^{q-1} = 1$ y $\mathrm{ord}(a) = m$ implica que $m \mid q-1$ y por tanto $\frac{q-1}{m}$ es un número natural. Además, como $m > 1$, tenemos que $q > 2$.

Primero suponemos que se verifican (i) y (ii), y probamos que $x^t - a$ es irreducible. Sea θ raíz de $x^t - a$ en su cuerpo de descomposición, m_θ su polinomio mínimo sobre $\mathbb{F}_q$ y d el grado del polinomio mínimo.

Por el Teorema 2.10(ii) tenemos que $m_\theta \mid x^t - a$ y por el Teorema 2.10(vi), $m_\theta(x) = (x-\theta)(x-\theta^q)\cdots(x-\theta^{q^{d-1}})$ y $\theta^{q^d} = \theta$.

Ahora veamos que θ tiene orden mt. Sabemos que $\theta^{mt} = a^m = 1$, y si $\mathrm{ord}(\theta) < mt$, debe haber un divisor primo de mt tal que $\theta^{mt/r} = 1$. Como r es primo y $r \mid mt$, entonces $r \mid t$ o $r \mid m$, y por (i), si $r \mid t$, tenemos que $r \mid m$ y podemos escribir

$$a^{m/r} = (\theta^t)^{m/r} = \theta^{mt/r} = 1.$$

Esto implica que el orden de a no es m, lo que nos lleva a un absurdo y por tanto, $\mathrm{ord}(\theta) = mt$.

Sabiendo que su orden es mt, tenemos que $\theta^{q^d-1} = 1 \Leftrightarrow mt \mid q^d - 1 \Leftrightarrow q^d \equiv 1 \bmod(mt)$, y como d es el menor natural tal que $\theta^{q^d} = \theta$ también es el menor natural tal que $q^d \equiv 1 \bmod(mt)$ y entonces $d = \mathrm{ord}_{mt}(q)$.

Como $m \mid q-1$ y t cumple (i) y (ii), podemos aplicar el Corolario 3.7 y tenemos que $t = \mathrm{ord}_{mt}(q)$. Entonces $\deg(m_\theta) = t$, y como $m_\theta \mid x^t - a$, tenemos que $x^t - a$ es irreducible.

Ahora probaremos el contrarrecíproco.

Primero supongamos que (i) no se cumple. Entonces, existe un factor primo r de t que divide a $(q-1)/m$ o que no divide a m. Consideramos $t = rt_1$ para algún $t_1 \in \mathbb{N}$.

Si r divide a $\frac{q-1}{m}$, tenemos $rs = (q-1)/m$ para algún $s \in \mathbb{N}$. Tenemos que el subgrupo de $\mathbb{F}_q^*$ formado por las r-ésimas potencias, $\mathbb{F}_q^{*r} = \{x^r : x \in \mathbb{F}_q^*\}$, claramente tiene orden $(q-1)/r = ms$. Por lo tanto este contiene al subgrupo de orden m generado por a. Por pertenecer a al subgrupo de r-ésimas potencias, $a = b^r$ para algún $b \in \mathbb{F}_q^*$, y así $x^t - a = x^{rt_1} - b^r$ tiene el factor $x^{t_1} - b$ y por tanto es reducible.

Si r no divide ni a $(q-1)/m$ ni a m, r no divide a $q-1$. Además, como r es primo y $q-1>1$, $r \neq q-1$, tenemos $q-1 \neq r$ y por tanto son coprimos. Entonces podemos considerar un $r_1 \in \mathbb{N}$ tal que $r_1 r \equiv 1 \bmod (q-1)$, y así $x^t - a = (x^{rt_1} - a^{r_1 r}$, que tiene el factor $x^{t_1} - a^{r_1}$.

Finalmente, supongamos que se verifica (i) pero no (ii). Entonces $t = 4t_2$ para algún $t_2 > 0$ y $4 \nmid (q-1)$. Por lo tanto, 2 es un divisor primo de t. Por la condición (i), $2 \mid m$, así que m debe ser par. Como $m \mid (q-1)$, q debe ser impar. Pero $4 \nmid (q-1)$, entonces $4 \nmid m$ y $m/2$ es impar. Por lo tanto $\mathrm{ord}(a) = m$ implica $a^{m/2} = -1$, y así $x^t - a = x^t + a^{(m/2)+1} = x^t + a^d$, donde $d = (m/2)+1$ es par. Entonces $a^{d/2}/2 \in \mathbb{F}_q^*$, y por tanto $(a^{d/2}/2)^{q-1} = 1$ y $(a^{d/2}/2)^{q+1} = (a^{d/2}/2)^2$. Como q es impar y $4 \nmid (q-1)$, $4 \mid (q+1)$. Entonces, tenemos

$$a^d = 4(a^{d/2}/2)^2 = 4(a^{d/2}/2)^{q+1} = 4c^4 \quad \text{con } c = (a^{d/2}/2)^{(q+1)/4},$$

lo cual conduce a la factorización

$$x^t - a = x^t + a^d = x^{4t_2} + 4c^4 = (x^{2t_2} + 2cx^{t_2} + 2c^2)(x^{2t_2} - 2cx^{t_2} + 2c^2).$$

□

De este criterio obtenemos un corolario que nos permite construir un binomio irreducible.

Corolario 3.9. *Sea r un divisor primo de $q-1$ y k un número natural. Sea $a \in \mathbb{F}_q^*$ y $\mathrm{ord}(a) = m > 1$ en $\mathbb{F}_q^*$. Suponemos que r no divide a $(q-1)/m$ y además si $r = 2$ y $k \geq 2$, suponemos que $4 \mid (q-1)$. Entonces $x^{r^k} - a$ es irreducible sobre $\mathbb{F}_q$.*

Demostración. Sea $\mathrm{ord}(a) = m$ en $\mathbb{F}_q^*$, esto implica que $m \mid (q-1)$. Sea $t = r^k$, entonces el único divisor primo de t es r. Como $r \mid (q-1)$ y $r \nmid (q-1)/m$, deducimos que $r \mid m$. Por lo tanto, la condición (i) del Teorema 3.8 se cumple.

Si $4 \mid t$ entonces $r = 2$ y $k \geq 2$, y por hipótesis, $4 \mid (q-1)$, así que la condición (ii) también se cumple. Aplicando el Teorema 3.8 tenemos que $x^{r^k} - a$ es irreducible sobre $\mathbb{F}_q$. □

Ahora veremos como usar este corolario para construir binomios irreducibles.

Ejemplo 3.10. Empleando el corolario previo, podemos deducir que, para cualquier k natural,

(a) $x^{2^k} + 2$ y $x^{2^k} - 2$ son irreducibles sobre $\mathbb{F}_5$.

(b) $x^{3^k} + 3$, $x^{3^k} - 3$, $x^{3^k} + 2$ y $x^{2^k} - 2$ son irreducibles sobre $\mathbb{F}_7$.

(c) $x^{3^k} + \alpha$ es irreducible sobre $\mathbb{F}_4$, donde $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ y α es una raíz de $x^2 + x + 1$.

A partir de (c) deducimos que

(d) $x^{2 \cdot 3^k} + x^k + 1 = (x^{3^k} + \alpha)(x^{3^k} + \alpha^2)$ es irreducible sobre $\mathbb{F}_2$.

3.3. Trinomios

Continuamos estudiando la irreducibilidad de trinomios, siguiendo el capítulo 10.3 del libro *Finite fields and Galois rings* [17]. De forma similar a la sección de binomios, obtendremos una caracterización para ciertos trinomios irreducibles y una construcción explícita de éstos.

Empezamos definiendo la función traza, necesaria para caracterizar los trinomios.

Definición 3.11. Sea q la potencia de un primo y n un entero positivo. Si α es un elemento de $\mathbb{F}_{q^n}$, su traza relativa a $\mathbb{F}_q$ se define como

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i},$$

Si $\mathbb{F}_{q^n}$ y $\mathbb{F}_q$ están claros por el contexto, escribimos $\mathrm{Tr}(\alpha)$.

Ahora vemos sus propiedades básicas.

Lema 3.12. *Sea $\alpha \in \mathbb{F}_{q^m}$, f el polinomio mínimo de α sobre $\mathbb{F}_q[x]$, de grado d, y $g(x) = f(x)^{m/d} = x^m + a_{m-1}x^{m-1} + \cdots + a_0$. Entonces $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = -a_{m-1}$, y en particular, $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$.*

Demostración. Como solo usaremos estos cuerpos para la traza, la denotaremos $\mathrm{Tr}(\alpha)$. Primero, por el Teorema 2.10(i), vemos que $d \mid m$, y por tanto $g(x) = f(x)^{m/d} \in \mathbb{F}_q[x]$. Además, por el Teorema 2.10(vi), las raíces de f son $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ y $\alpha^{q^d} = \alpha$. Por tanto, los conjugados de α respecto $\mathbb{F}_q$ son las raíces de f repetidas m/d veces.

Por lo tanto,

$$g(x) = f(x)^{m/d} = (x-\alpha)^{m/d}(x-\alpha^q)^{m/d}\cdots(x-\alpha^{q^{d-1}})^{m/d} = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{m-1}}),$$

y una comparación de los coeficientes con $g(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ muestra que $\mathrm{Tr}(\alpha) = -a_{m-1}$. En particular, $\mathrm{Tr}(\alpha)$ es siempre un elemento de $\mathbb{F}_q$. □

Teorema 3.13. *La función traza $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$, que escribiremos Tr, satisface las siguientes propiedades:*

(i) $\mathrm{Tr}(a+b) = \mathrm{Tr}(a) + \mathrm{Tr}(b)$ *para todo $a, b \in \mathbb{F}_{q^m}$;*

(ii) $\mathrm{Tr}(ca) = c\,\mathrm{Tr}(a)$ *para todo $c \in \mathbb{F}_q, a \in \mathbb{F}_{q^m}$;*

(iii) $\mathrm{Tr}(a) = ma$ *para todo $a \in \mathbb{F}_q$;*

(iv) $\mathrm{Tr}(a^q) = \mathrm{Tr}(a)$ *para todo $a \in \mathbb{F}_{q^m}$;*

(v) Si la característica de $\mathbb{F}_q$ es p, $\mathrm{Tr}(a^p) = (\mathrm{Tr}(a))^p$ *para todo $a \in \mathbb{F}_{q^m}$.*

Demostración.

(i) Para $a, b \in \mathbb{F}_{q^m}$, si la característica del cuerpo es p, usamos que $(a+b)^{p^k} = a^{p^k} + b^{p^k}$ para todo $k \in \mathbb{N}$, y que $q = p^n$ para algún $n \in \mathbb{N}$, y obtenemos

$$\mathrm{Tr}(a+b) = (a+b)+(a+b)^q+\cdots+(a+b)^{q^{m-1}} = a+a^q+\cdots+a^{q^{m-1}}+b+b^q+\cdots+b^{q^{m-1}} = Tr(a)+Tr(b).$$

(ii) Para $c \in \mathbb{F}_q$, tenemos $c^{q^j} = c$ para todo $j \in \mathbb{N}$ por el Lema 1.3. Por lo tanto,

$$\mathrm{Tr}(ca) = (ca) + (ca)^q + \cdots + (ca)^{q^{m-1}} = c(a + a^q + \cdots + a^{q^{m-1}}) = c\,\mathrm{Tr}(a).$$

(iii) Similarmente a (ii), si $a \in \mathbb{F}_q$, $a^{q^j} = a$ para todo $j \in \mathbb{N}$ y por tanto,

$$\mathrm{Tr}(a) = a + a^q + \cdots + a^{q^{m-1}} = a + a + \cdots + a = ma.$$

(iv) Para $a \in \mathbb{F}_{q^m}$, tenemos $a^{q^m} = a$ por el Lema 1.3. Por lo tanto,

$$\mathrm{Tr}(a^q) = a^q + (a^q)^q + \cdots + (a^q)^{q^{m-1}} = a^q + a^{q^2} + \cdots + a^{q^{m-1}} + a^{q^m} = a^q + a^{q^2} + \cdots + a^{q^{m-1}} + a = \mathrm{Tr}(a).$$

(v) Como a pertenece a un cuerpo de característica p podemos escribir

$$\mathrm{Tr}(a^p) = \sum_{i=0}^{n-1} (\alpha^p)^{q^i} = \sum_{i=0}^{n-1} (\alpha^{q^i})^p = (\sum_{i=0}^{n-1} \alpha^{q^i})^p = (\mathrm{Tr}(a))^p.$$

□

Finalmente, vemos la propiedad de transitividad de la traza.

Teorema 3.14. *Sea K un cuerpo finito, F una extensión finita de K y E una extensión finita de F. Entonces, para todo $a \in E$ se cumple*

$$\mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(a)) = \mathrm{Tr}_{E/K}(a).$$

Demostración. Si $a \in E$, por Lema 3.12, sabemos que $\mathrm{Tr}_{E/F}(a) \in F$, y entonces aplicarle $\mathrm{Tr}_{F/K}$ a ese elemento tiene sentido.

Sea $K = \mathbb{F}_q$, $[F : K] = m$ y $[E : F] = n$, de modo que $F = \mathbb{F}_{q^m}$, $[E : K] = [E : F][F : K] = mn$. Entonces, para $a \in E$, tenemos

$$\mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(a)) = \sum_{i=0}^{m-1} (\mathrm{Tr}_{E/F}(a))^{q^i} = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n-1} a^{q^{mj}} \right)^{q^i} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a^{q^{mj+i}} = \sum_{k=0}^{mn-1} a^{q^k} = \mathrm{Tr}_{E/K}(a). \quad \square$$

Ahora que hemos definido la traza, podemos presentar un primer criterio de irreducibilidad.

Teorema 3.15. *Sea $q = p^n$, donde p es un número primo y n un número natural. Entonces el trinomio*

$$x^p - x - b, \quad b \in \mathbb{F}_q,$$

es irreducible sobre $\mathbb{F}_q$ si y solo si $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b) \neq 0$.

Demostración. Sea θ una raíz de $x^p - x - b$. Entonces $\theta^p = \theta + b$.

Por inducción probamos que

$$\theta^{p^i} = \theta + b + b^p + \cdots + b^{p^{i-1}}, \quad i = 1, 2, \ldots.$$

El caso $i = 1$ lo hemos visto antes.

Si la ecuación se verifica para $i - 1$, tenemos que

$$\theta^{p^{i-1}} = \theta + b + b^p + \cdots + b^{p^{i-2}}$$

y, elevando la ecuación a p,

$$\theta^{p^i} = (\theta + b + b^p + \cdots + b^{p^{i-2}})^p = \theta^p + b^p + \cdots + b^{p^{i-1}} = \theta + b + b^p + \cdots + b^{p^{i-1}}.$$

Las últimas igualdades se obtienen usando que el cuerpo es de característica p.

En particular,

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

Con esto podemos ver una implicación por el contrarrecíproco. Supongamos que $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b) = 0$, entonces $\theta^q = \theta$, es decir, todas las raíces de $x^p - x - b$ están en $\mathbb{F}_q$. En consecuencia, $x^p - x - b$ es un producto de factores lineales en $\mathbb{F}_q[x]$, y por tanto es reducible.

Ahora vemos la otra implicación, suponiendo que $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b) \neq 0$. Sea $\tau = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b)$, entonces $\tau \in \mathbb{F}_p^*$ por resultado de traza (citar) y, como $b^q = b$,

$$\theta^{q^i} = \theta^{p^{ni}} = \theta + i\tau, \quad i = 1, 2, \ldots, p-1; \quad \theta^{q^p} = \theta + p\tau = \theta.$$

Así, θ tiene exactamente p conjugados distintos sobre $\mathbb{F}_q$ y por el Teorema 2.10(vi), el polinomio mínimo de θ sobre $\mathbb{F}_q$ tiene grado p. Finalmente, por el Teorema 2.10(ii), $m_\theta \mid x^p - x - b$, y al tener ambos el mismo grado, $x^p - x - b$ debe ser irreducible. □

De este teorema es inmediato que $x^p - x - b$ es irreducible en $\mathbb{F}_p$ para cualquier $b \in \mathbb{F}_p^*$.

Ahora introducimos los polinomios linealizados, que se usarán para simplificar posteriores demostraciones.

Definición 3.16. Sea q una potencia de un número primo p. Un polinomio de la forma

$$l(x) = l_v x^{p^v} + l_{v-1} x^{p^{v-1}} + \cdots + l_1 x^p + l_0 x,$$

donde $v \in \mathbb{N}$, $l_i \in \mathbb{F}_q$ para $i = 0, 1, 2, \ldots, v$, se llama polinomio linealizado sobre $\mathbb{F}_q$.

Si $l(x)$ es un polinomio linealizado sobre $\mathbb{F}_q$ y $b \in \mathbb{F}_q$, entonces a $l(x) - b$ se le denomina polinomio afín sobre $\mathbb{F}_q$.

Vemos también algunas de sus propiedades básicas, que nos servirán más adelante.

Lema 3.17. *Sea $l(x)$ un polinomio linealizado sobre $\mathbb{F}_q$ cuerpo de característica p. Entonces*

$$l(x+y) = l(x) + l(y), \quad \forall x, y \in \mathbb{F}_q,$$

$$l(cx) = c \cdot l(x), \quad \forall x \in \mathbb{F}_q,\ c \in \mathbb{F}_p.$$

Recíprocamente, si un polinomio $l(x) \in \mathbb{F}_q[x]$ cumple ambas condiciones, entonces $l(x)$ es un polinomio linealizado sobre $\mathbb{F}_q$.

Demostración. La primera propiedad es evidente si vemos que $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ para todo $n \in \mathbb{N}$. Es sencillo verlo por inducción.

Si $n = 1$, como estamos en un cuerpo de característica p, $(x+y)^p = x^p + y^p$.

Si es cierto para $n-1$, tenemos

$$(x+y)^{p^n} = ((x+y)^{p^{n-1}})^p = (x^{p^{n-1}} + y^{p^{n-1}})^p = x^{p^n} + y^{p^n}$$

Para ver la segunda propiedad, basta tener en cuenta que $c^{p^n} = c$ para todo $n \in \mathbb{N}$, ya que $c \in \mathbb{F}_p$.

Ahora supongamos que $l(x) \in \mathbb{F}_q[x]$ es un polinomio que cumple ambas propiedades. Lo evaluamos en $x + y$,

$$l(x+y) = l_0 + l_1(x+y) + l_2(x+y)^2 + \cdots + l_v(x+y)^v$$
$$= l_0 + l_1 x + l_2 x^2 + \cdots + l_v x^v + l_0 + l_1 y + l_2 y^2 + \cdots + l_v y^v + p(x,y) = l(x) + l(y) + p(x,y),$$

donde $p(x,y) \in \mathbb{F}_q[x,y]$ es un polinomio de términos $C_{i,k} \cdot l_k \cdot x^i \cdot y^{k-i}$ con $i = 1, \ldots, k-1$, $k = 2, \ldots, v$, $C_{i,k}$ constantes que dependen de i y k, y término independiente $-l_0$.

De la ecuación previa deducimos que si $l(x+y) = l(x) + l(y)$, $p(x,y)$ debe ser 0, y entonces tanto el término constante como $C_{i,k} \cdot l_k \cdot x^i \cdot y^{k-i}$ serán igual a 0. Si $C_{i,k} \neq 0$ para algún i, necesariamente $l_k = 0$. Como el polinomio está formado por los términos que sobran al desarrollar la ecuación anterior, sabemos que $C_{i,k} = 0$ para todo i solo si $(x+y)^k = x^k + y^k$, es decir, solo cuando k sea una potencia de p.

Por tanto tenemos que $l_k = 0$ cuando $k \neq 1, p, p^2, \ldots$ y obtenemos un polinomio de la forma $l(x) = l_1 x + l_p x^p + \cdots + l_{p^t} x^{p^t}$, que es linealizado. □

Lema 3.18. *Supongamos que el polinomio linealizado $l(x)$ sobre $\mathbb{F}_q$ no tiene raíces distintas de cero en $\mathbb{F}_q$. Entonces para cada $b \in \mathbb{F}_q$, hay un $a \in \mathbb{F}_q$ tal que $x - a$ divide al polinomio afín $l(x) - b$.*

Demostración. Definimos la siguiente función

$$\begin{aligned} l : \mathbb{F}_q &\to \mathbb{F}_q \\ x &\mapsto l(x). \end{aligned}$$

Veamos que esta función es inyectiva. Para $\alpha, \beta \in \mathbb{F}_q$, si $l(\alpha) = l(\beta)$, entonces $l(\alpha - \beta) = l(\alpha) - l(\beta) = 0$. Por hipótesis, $l(x)$ no tiene raíces distintas de cero en $\mathbb{F}_q$. Así que $\alpha - \beta = 0$ y por tanto, l es inyectiva. Dado que es una función inyectiva entre dos cuerpos finitos con el mismo cardinal, l también es suprayectiva. Entonces, para cualquier $b \in \mathbb{F}_q$, existe un elemento $a \in \mathbb{F}_q$ tal que $l(a) = b$. Por lo tanto, a es una raíz de $l(x) - b$ y entonces $x - a$ divide a $l(x) - b$. □

A partir del criterio de irreducibilidad anterior, podemos deducir un criterio más general.

Teorema 3.19. *Sea q una potencia de p primo. Para $a, b \in \mathbb{F}_q^*$, el trinomio $x^p - ax - b$ es irreducible sobre $\mathbb{F}_q$ si y solo si $a = a_0^{p-1}$ para algún $a_0 \in \mathbb{F}_q^*$ y $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b/a_0^p) \neq 0$.*

Demostración. Primero suponemos que $a = a_0^{p-1}$ para algún $a_0 \in \mathbb{F}_q^*$ y $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b/a_0^p) \neq 0$. Entonces

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

y podemos hacer el cambio de variable $y = x/a_0$. Por el Teorema 3.15, $y^p - y - b/a_0^p$ es irreducible sobre $\mathbb{F}_q$, y eso implica que $x^p - ax - b$ también lo es.

Para la otra implicación, probamos el contrarrecíproco. Sea $a \neq a_0^{p-1}$ para cualquier $a_0 \in \mathbb{F}_q^*$. Entonces, el polinomio linealizado $x^p - ax = x(x^{p-1} - a)$ no tiene raíces distintas de cero en $\mathbb{F}_q$. Por el Lema 3.18, el trinomio $x^p - ax - b$ es reducible.

Finalmente, supongamos que $a = a_0^{p-1}$ para algún $a_0 \in \mathbb{F}_q^*$, pero $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b/a_0^p) = 0$. Usando el mismo cambio de variable que antes, por el Teorema 3.15, $y^p - y - b/a_0^p$ es reducible sobre $\mathbb{F}_q$, y entonces $x^p - ax - b$ también lo es. □

Tenemos también la siguiente manera de construir trinomios irreducibles directamente, para la que necesitamos definir $p^r \parallel n$.

Definición 3.20. Decimos que p^r divide exactamente a n, y lo denotamos $p^r \parallel n$, si $p^r \mid n$ y $p^{r+1} \nmid n$.

Teorema 3.21. *Sea p un primo tal que $p \equiv 3 \bmod 4$ y sea $r \geq 2$ tal que $2^r \parallel (p+1)$. Definimos elementos $a_1, a_2, \ldots, a_r$ de $\mathbb{F}_p$ recursivamente de la siguiente forma,*

$$\begin{aligned} a_1 &= 0, \\ a_i &= ((a_{i-1}+1)/2)^{(p+1)/4} \quad \text{para } i = 2, 3, \ldots, r-1, \\ a_r &= ((a_{r-1}-1)/2)^{(p+1)/4}. \end{aligned}$$

Entonces, para cualquier k natural, el trinomio

$$x^{2^k} - 2a_r x^{2^{k-1}} - 1$$

es irreducible sobre $\mathbb{F}_p$, y sobre $\mathbb{F}_{p^m}$ para cualquier entero impar m. Además, el trinomio divide a $x^{2^{r+k-1}} + 1$.

No veremos la demostración del teorema en este trabajo. Está expuesta de las páginas 228 a 230 en el libro *Finite fields and Galois rings* [17].

Los resultados conseguidos en esta sección nos permiten también construir nuevos polinomios irreducibles a partir de otros usando trinomios.

Teorema 3.22. *Sea $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ un polinomio irreducible sobre el cuerpo finito $\mathbb{F}_q$ de característica p, y sea $b \in \mathbb{F}_q^*$. Entonces, el polinomio $f(x^p - x - b)$ es irreducible sobre $\mathbb{F}_q$ si y solo si $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(mb - a_{m-1}) \neq 0$.*

Demostración. Supongamos que $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(mb - a_{m-1}) \neq 0$. Sea $K = \mathbb{F}_q$ y sea F el cuerpo de descomposición de f sobre K, que por el Corolario 2.4 es $\mathbb{F}_{q^m}$. Si $\alpha \in F$ es una raíz de f, entonces, según el Teorema 2.3, todas las raíces de f son $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$, y $F = K(\alpha)$. Además, $\mathrm{Tr}_{F/K(\alpha)} = -a_{m-1}$, por el Lema 3.12, y usando el Teorema 3.13 y el Teorema 3.14 obtenemos

$$\mathrm{Tr}_{F/\mathbb{F}_p}(\alpha + b) = \mathrm{Tr}_{K/\mathbb{F}_p}(\mathrm{Tr}_{F/K}(\alpha + b)) = \mathrm{Tr}_{K/\mathbb{F}_p}(-a_{m-1} + mb) \neq 0.$$

Por el Corolario 3.15, el trinomio $x^p - x - (\alpha + b)$ es irreducible sobre F. Así, $[F(\beta) : F] = p$, donde β es una raíz de $x^p - x - (\alpha + b)$. Además tenemos que $[F : K] = [\mathbb{F}_{q^m} : \mathbb{F}_q] = m$, y usando esto deducimos que

$$[F(\beta) : K] = [F(\beta) : F][F : K] = pm.$$

Ahora, como β es raíz de $x^p - x - (\alpha + b)$, $\alpha = \beta^p + \beta - b$, por lo que $\alpha \in K(\beta)$ y entonces $K(\beta) = K(\alpha, \beta) = F(\beta)$. Así, $[K(\beta) : K] = [F(\beta) : K] = pm$ y el polinomio mínimo de β sobre K tiene grado pm.

Pero $f(\beta^p - \beta - b) = f(\alpha) = 0$, por lo que β es una raíz del polinomio $f(x^p - x - b) \in K[x]$ de grado pm. Entonces tenemos que β es raíz de su polinomio mínimo y de $f(x^p - x - b)$, ambos polinomios mónicos del mismo grado sobre K, y usando el Teorema 2.10(iv), claramente $f(x^p - x - b)$ es el polinomio mínimo de β y por tanto, es irreducible sobre K.

Finalmente, probamos la otra implicación por el contrarrecíproco. Suponemos que $\mathrm{Tr}_F(mb - a_{m-1}) = 0$, entonces considerando $\alpha \in F$ una raíz de f, por la cadena de igualdades vista en la otra implicación,

$$\mathrm{Tr}_{F/\mathbb{F}_p}(\alpha + b) = \mathrm{Tr}_{K/\mathbb{F}_p}(-a_{m-1} + mb) = 0.$$

Y de la misma forma, por el Corolario 3.15, el trinomio $x^p - x - (\alpha + b)$ es reducible sobre F.

Así $[F(\beta) : F] < p$ para cualquier raíz β de $x^p - x - (a + b)$. Los mismos argumentos que antes muestran que β es una raíz de $f(x^p - x - b)$ y que $[K(\beta) : K] < pm$, por lo que aplicando el Teorema 2.10(ii), como β es raíz de $f(x^p - x - b)$ y m_β, tenemos que $f(x^p - x - b)$ es reducible sobre K. $\square$

3.4. Polinomios autorrecíprocos

Los polinomios autorrecíprocos tienen cierto uso en teoría de códigos, en esta sección veremos como emplear estos polinomios para construir sucesiones de polinomios irreducibles autorrecíprocos sobre cuerpos de característica 2. Seguiremos los artículos [12] y [5], donde se obtienen y detallan los resultados de esta sección.

Recordamos que vimos los polinomios recíprocos en la Definición 3.3, empezamos definiendo los polinomios autorrecíprocos.

Definición 3.23. Un polinomio $f(x) = \sum_{i=0}^{n} a_i x^i$ de grado n es autorrecíproco si coincide con su recíproco, es decir, sus coeficientes de la forma a_j coinciden con a_{n-j} con $0 \leq j \leq n$.

Ahora definimos el operador de funciones que será clave para construir la sucesión de polinomios irreducibles.

Definición 3.24. Dado un polinomio $f(x) = \sum_{i=0}^{n} a_i x^i$ de grado n en $\mathbb{F}_q[x]$, el operador Q asocia $f(x)$ a $f^Q(x) = x^n f(x + \frac{1}{x})$, polinomio de grado $2n$ en $\mathbb{F}_q$. Si $f(x) = \sum_{i=0}^{n} a_i x^i$, tal que $a_0 \neq 0 \neq a_n$, la transformada queda $f^Q(x) = \sum_{i=0}^{n} a_i (1 + x^2)^i x^{n-i}$.

Es fácil ver que f^Q siempre es un polinomio autorrecíproco considerando la simetría del binomial, $\binom{n}{j} = \binom{n}{n-j}$, y desarrollando las potencias de $x + \frac{1}{x}$.

Vamos a estudiar si el operador Q mantiene la irreducibilidad. Para un cuerpo finito general tenemos la siguiente condición de irreducibilidad.

Lema 3.25. *Sea f un polinomio irreducible de grado n sobre $\mathbb{F}_q$. Entonces, f^Q es irreducible si y solo si el polinomio*

$$g(x) = x^2 - \beta x + 1 \in \mathbb{F}_{q^n}[x]$$

es irreducible, donde β es cualquier raíz de f.

Demostración. Si $f(x) = \sum_{i=0}^{n} a_i x^i$, como es irreducible y de grado n, $a_0 \neq 0 \neq a_n$, y por lo visto en la definición, $f^Q(x) = \sum_{i=0}^{n} a_i (1 + x^2)^i x^{n-i}$, obtenemos que 0 no es una raíz de f^Q, ya que $f^Q(0) = a_n$, por tanto si α es una raíz de f^Q, entonces $\alpha + 1/\alpha$ es raíz de f.

Por otro lado, si θ es una raíz de f, podemos encontrar un α tal que $\theta = \alpha + 1/\alpha$, y α sería raíz de f^Q. Entonces si tomamos $\beta = \alpha + 1/\alpha$, donde α es una raíz de f^Q, entonces β es una raíz de f.

Por el Teorema 2.10, f^Q es irreducible si y solo si el grado de α es $2n$ sobre $\mathbb{F}_q$. Como $g \in \mathbb{F}_{q^n}[x]$ es de grado 2 y por definición de β, tenemos que $g(\alpha) = 0$, podemos escribir $[\mathbb{F}_q(\alpha):\mathbb{F}_q]=[\mathbb{F}_q(\alpha):\mathbb{F}_{q^n}]\cdot n$, y entonces el grado de α es $2n$ si y solo si g es irreducible. □

Si nos restringimos a los cuerpos de la forma $\mathbb{F}_{2^k}$, obtenemos mejores criterios de irreducibilidad.

Teorema 3.26 ([12])**.** *Sea $f(x) = x^n + \cdots + a_1 x + a_0 \in \mathbb{F}_{2^k}[x]$, con $k \in \mathbb{N}$, un polinomio irreducible. Entonces $f^Q(x)$ es irreducible si y solo si* $\mathrm{Tr}_{\mathbb{F}_{2^k}/\mathbb{F}_2}(a_1/a_0) = 1$.

Demostración. Para simplificar la notación definimos $F = \mathbb{F}_2$, $K = \mathbb{F}_{2^k}$ y $L = \mathbb{F}_{2^{nk}}$. Por el Lema 3.25 sabemos que $f^Q(x)$ es irreducible si y solo si $x^2 + \beta x + 1 \in L[x]$ es irreducible, siendo β una raíz de f.

Claramente $\beta \neq 0$ ya que f es irreducible, luego podemos aplicar el Teorema 3.19 a este trinomio y tenemos que $x^2 + \beta x + 1$ es irreducible si y solo si $\mathrm{Tr}_{L/F}(1/\beta^2) \neq 0$. Por el Lema 3.12 esta traza pertenece a $\mathbb{F}_2$, y entonces si es distinta de 0, es igual a 1. Además, aplicando el Teorema 3.13(v), $\mathrm{Tr}_{L/F}(1/\beta^2) = (\mathrm{Tr}_{L/F}(1/\beta))^2$.

Entonces nos queda que $x^2+\beta x+1$ es irreducible si y solo si $\mathrm{Tr}_{L/F}(1/\beta)=1$. Por la transitividad de la traza 3.14, tenemos que $\mathrm{Tr}_{L/F}(1/\beta)=\mathrm{Tr}_{K/F}(\mathrm{Tr}_{L/K}(1/\beta))$. Si vemos que $\mathrm{Tr}_{L/K}(1/\beta)=a_1/a_0$ habremos probado el teorema.

Por el Lema 3.12 si vemos que el polinomio $g(x)=x^n+\frac{a_1}{a_0}x^{n-1}+\cdots+\frac{a_{n-1}}{a_0}x+1\in\mathbb{F}_{2^k}[x]$ es el polinomio mínimo de $1/\beta$ tendremos que $\mathrm{Tr}_{L/K}(1/\beta)=a_1/a_0$. Claramente $a_0\cdot g(x)$ es el polinomio recíproco de $f(x)$ y por el Teorema 3.4, al ser $f(x)$ irreducible, $g(x)$ también lo es. Sustituyendo $g(x)$ en $1/\beta$, al ser β raíz de $f(x)=x^n+\cdots+a_1x+a_0$, tenemos que

$$g(1/\beta)=\frac{a_0+a_1\beta+\cdots+a_{n-1}\beta^{n-1}+\beta^n}{a_0\beta^n}=0$$

luego, por el Teorema 2.10(iv), $g(x)$ es el polinomio mínimo de $1/\beta$ y con esto obtenemos que $f^Q(x)$ es irreducible si y solo si $\mathrm{Tr}_{K/F}(a_1/a_0)=1$. □

En el caso $k=1$, la traza de a_1/a_0 es a_1/a_0, y con esa observación, el corolario siguiente es inmediato.

Corolario 3.27. *Si $f(x)=x^n+\cdots+a_1x+1\in\mathbb{F}_2[x]$ es irreducible, entonces $f^Q(x)$ es irreducible si y solo si $a_1=1$.*

Con estos resultados podemos probar un teorema que nos permite conseguir una sucesión de polinomios autorrecíprocos irreducibles sobre $\mathbb{F}_{2^k}[x]$, para cualquier $k\in\mathbb{N}$.

Para abreviar, de ahora en adelante nos referiremos a los polinomios mónicos irreducibles autorrecíprocos como polinomios SRIM, que son sus siglas en inglés.

Teorema 3.28. *Sea $f(x)=x^n+a_1x^{n-1}+\cdots+a_1x+1\in\mathbb{F}_{2^k}[x]$ un polinomio SRIM tal que $\mathrm{Tr}(a_1)=1$. Entonces $f^Q(x)=x^{2n}+b_1x^{2n-1}+\cdots+b_1x+1$ es también un polinomio SRIM y satisface $\mathrm{Tr}(b_1)=1$.*

Demostración. Para simplificar la notación, definimos

$$F:=\mathbb{F}_2,\quad K:=\mathbb{F}_{2^k},\quad L:=\mathbb{F}_{2^{nk}},\quad G:=\mathbb{F}_{2^{2nk}}.$$

Si α es una raíz de f, entonces $\beta=\alpha+1/\alpha$ es una raíz de f^Q. Por el teorema previo, f^Q es irreducible, y por el lema previo, $g(x)=x^2+\beta x+1\in L[x]$ es irreducible, y α es raíz de g. Por el Teorema 2.10, como todos estos polinomios son mónicos e irreducibles, coinciden con el polinomio mínimo asociado a sus raíces. Aplicando el Lema 3.12, tenemos las siguientes identidades.

$$\mathrm{Tr}_{G/L}(\alpha)=\beta,\quad \mathrm{Tr}_{L/K}(\beta)=a_1,\quad \mathrm{Tr}_{G/K}(\alpha)=b_1.$$

Aplicando la propiedad de transitividad de la traza, tenemos

$$\mathrm{Tr}_{K/F}(b_1)=\mathrm{Tr}_{K/F}(\mathrm{Tr}_{G/K}(\alpha))=\mathrm{Tr}_{K/F}(\mathrm{Tr}_{L/K}(\beta))=\mathrm{Tr}_{K/F}(a_1)=1.$$

□

Ahora juntando estos dos teoremas, partiendo de un polinomio irreducible f en $\mathbb{F}_2$ de grado n con coeficiente $a_1=1$ y aplicando el operador Q, si el coeficiente b_1 de f^Q es 1 podremos generar una sucesión de polinomios autorrecíprocos irreducibles de grados $n2^i$ donde i es el número de veces que hemos aplicado el operador Q.

Ejemplo 3.29. Los polinomios con coeficiente $a_1 = 1$ más sencillos posibles son $x^n + x + 1$. El artículo [19] nos proporciona una tabla con los polinomios irreducibles de la forma $x^n + x + 1$ con $n \leq 30000$. Podemos empezar viendo si alguno de estos polinomios proporciona un polinomio SRIM con coeficiente asociado a x igual a 1 al aplicarle el operador Q. Para esto se ha calculado en MAPLE la transformada por Q de estos polinomios.

Polinomio	Transformada por Q
$x^2 + x + 1$	$x^4 + x^3 + x^2 + x + 1$
$x^3 + x + 1$	$x^6 + x^3 + 1$
$x^4 + x + 1$	$x^8 + x^5 + x^4 + x^3 + 1$
$x^6 + x + 1$	$x^{12} + x^8 + x^7 + x^6 + x^5 + x^4 + 1$
$x^7 + x + 1$	$x^{14} + x^{12} + x^{10} + x^7 + x^4 + x^2 + 1$
$x^9 + x + 1$	$x^{18} + x^{16} + x^{10} + x^9 + x^8 + x^2 + 1$
$x^{15} + x + 1$	$x^{30} + x^{28} + x^{26} + x^{24} + x^{22} + x^{20} + x^{18} + x^{15} + x^{12} + x^{10} + x^8 + x^6 + x^4 + x^2 + 1$
$x^{22} + x + 1$	$x^{44} + x^{40} + x^{36} + x^{32} + x^{23} + x^{22} + x^{21} + x^{12} + x^8 + x^4 + 1$
$x^{28} + x + 1$	$x^{56} + x^{48} + x^{40} + x^{32} + x^{29} + x^{28} + x^{27} + x^{24} + x^{16} + x^8 + 1$

Parece que aplicar el operador Q a cualquier polinomio irreducible es una manera poco efectiva de obtener los polinomios que estamos buscando. Podemos intentar buscar polinomios autorrecíprocos irreducibles directamente.

Ejemplo 3.30. Buscar polinomios irreducibles tal que al aplicarles el operador Q tengan los coeficientes adecuados para aplicar estos resultados parece ser bastante más ineficiente que buscar directamente polinomios SRIM con coeficiente lineal 1. Los polinomios autorrecíprocos más sencillos de esta forma en $\mathbb{F}_2[x]$ son $x^n + x^{n-1} + x^{n/2} + x + 1$ con n par.

Hacemos una búsqueda con MAPLE por los polinomios de esta forma para $n \leq 3000$, y obtenemos que los siguientes polinomios cumplen que son irreducibles, y por tanto son SRIM, en $\mathbb{F}_2[x]$.

$$
\begin{aligned}
x^2 + x + 1 \\
x^4 + x^3 + x^2 + x + 1 \\
x^{10} + x^9 + x^5 + x + 1 \\
x^{16} + x^{15} + x^8 + x + 1 \\
x^{100} + x^{99} + x^{50} + x + 1 \\
x^{196} + x^{195} + x^{98} + x + 1 \\
x^{730} + x^{729} + x^{365} + x + 1 \\
x^{1600} + x^{1599} + x^{800} + x + 1 \\
x^{2206} + x^{2205} + x^{1103} + x + 1 \\
x^{2800} + x^{2799} + x^{1400} + x + 1
\end{aligned}
$$

Por tanto, si queremos un polinomio autorrecíproco irreducible de grado 64 en $\mathbb{F}_2$, aplicamos el operador Q a $x^{16} + x^{15} + x^8 + x + 1$ y obtenemos la siguiente secuencia

$$f(x) = x^{16} + x^{15} + x^8 + x + 1$$

$$f^Q(x) = x^{32} + x^{31} + x^{29} + x^{27} + x^{25} + x^{24} + x^{23} + x^{21} + x^{19} + x^{16} + x^{13} + x^{11} + x^9 + x^8 + x^7 + x^5 + x^3 + x + 1$$

$$f^{Q^2}(x) = x^{64} + x^{63} + x^{59} + x^{57} + x^{56} + x^{53} + x^{51} + x^{49} + x^{48} + x^{47} + x^{43} + x^{37} + x^{32} + x^{27} + x^{21} + x^{17} + x^{16} + x^{15} + x^{13} + x^{11} + x^8 + x^7 + x^5 + x + 1$$

De esta forma podemos obtener polinomios SRIM de grado $2^i \cdot 16$ para todo i natural, y de la misma forma, podemos obtener polinomios SRIM de grado $2^i \cdot n$ siempre que encontremos un polinomio SRIM de grado n con su coeficiente asociado a x igual a 1.

Esta búsqueda se puede generalizar a cualquier cuerpo finito gracias al siguiente teorema, y para demostrarlo necesitamos este lema previo.

Lema 3.31. *Para un cuerpo finito $\mathbb{F}_q$ con q impar, un elemento $b \in \mathbb{F}_q$ no es el cuadrado de un elemento, es decir, no existe un $a \in \mathbb{F}_q$ tal que $a^2 = b$ si y solo si $b^{\frac{q-1}{2}} = -1$.*

Demostración. Para ambas implicaciones probaremos el contrarrecíproco. Primero supongamos que existe un $a \in \mathbb{F}_q$ tal que $a^2 = b$, entonces $b^{\frac{q-1}{2}} = a^{q-1} = 1$.

Ahora supongamos que $b^{\frac{q-1}{2}} = 1$. Sea g un generador del grupo multiplicativo $\mathbb{F}_q^*$ y $k \in \mathbb{N}$ tal que $b = g^k$, entonces $1 = b^{\frac{q-1}{2}} = g^{\frac{q-1}{2}k}$. Luego el orden de g divide a $\frac{q-1}{2}k$, y como el orden de g es $q-1$, k debe ser par. Por lo tanto, si elegimos $a = g^{k/2}$, tenemos que $a^2 = b$. □

Teorema 3.32 ([12])**.** *Sea q una potencia impar de un primo. Si f es un polinomio mónico irreducible de grado n sobre $\mathbb{F}_q$, entonces f^Q es irreducible si y solo si $f(2) \cdot f(-2)$ no es un cuadrado en $\mathbb{F}_q$.*

Demostración. Por el Lema 3.25 sabemos que f^Q es irreducible en $\mathbb{F}_q$ si y solo si $x^2 - \beta x + 1$ es irreducible en $\mathbb{F}_{q^n}$, siendo β cualquier raíz de f. Y este polinomio, al ser de grado 2, es irreducible si y solo si no tiene raíces en $\mathbb{F}_{q^n}$.

Como estamos en un cuerpo que no es de característica 2, podemos calcular las posibles raíces de $x^2 - \beta x + 1$ con la fórmula $x = \frac{-\beta \pm \sqrt{\beta^2 - 4}}{2}$. Luego este polinomio es irreducible si y solo si $\beta^2 - 4$ no es el cuadrado de otro elemento en $\mathbb{F}_{q^n}$.

Además, por el Teorema 2.10, f es el polinomio mínimo de β y todas sus raíces son de la forma β^{q^i} con $0 \leq i \leq n-1$. Por tanto, el polinomio f se puede escribir como $f(x) = \prod_{i=0}^{n-1}(x - \beta^{q^i})$. Usando esto obtenemos la siguiente cadena de igualdades.

$$(\beta^2 - 4)^{\frac{q^n-1}{2}} = ([(2-\beta)(-2-\beta)]^{\frac{q^n-1}{q-1}})^{\frac{q-1}{2}} = [\prod_{i=0}^{n-1}(2-\beta)^{q^i}(-2-\beta)^{q^i}]^{\frac{q-1}{2}} = [\prod_{i=0}^{n-1}(2-\beta^{q^i})(-2-\beta^{q^i})]^{\frac{q-1}{2}} = (f(2)f(-2))^{\frac{q-1}{2}}.$$

Y finalmente por el Lema 3.31 tenemos la siguiente cadena de implicaciones.

$$\beta^2 - 4 \text{ no es el cuadrado de un elemento en } \mathbb{F}_{q^n} \iff (\beta^2-4)^{\frac{q^n-1}{2}} = -1 \iff (f(2)f(-2))^{\frac{q-1}{2}} = -1 \iff f(2)f(-2) \text{ no es el cuadrado de un elemento en } \mathbb{F}_q.$$

□

Sin embargo, buscar condiciones para que $f(2) \cdot f(-2)$ no sea un cuadrado no lleva a ningún resultado satisfactorio. El artículo [5] introduce otro operador, que sí permite construir una secuencia de polinomios SRIM sobre $\mathbb{F}_q$. Dedicaremos el final de esta sección a ilustrar el resultado principal de este artículo.

Definición 3.33. Dado un polinomio $f(x) = \sum_{i=0}^{n} a_i x^i$ de grado n en $\mathbb{F}_q[x]$, con q impar, el operador R asocia $f(x)$ a $f^R(x) = (2x)^n f(\frac{1}{2}(x + \frac{1}{x})) = 2^n f^Q(\frac{x}{2})$, polinomio de grado $2n$ en $\mathbb{F}_q$.

Por un razonamiento similar al hecho para el operador Q, para cualquier polinomio mónico f, tenemos que f^R es un polinomio autorrecíproco y mónico.

Lema 3.34. *En un cuerpo finito $\mathbb{F}_q$ con q impar, -1 es el cuadrado de otro elemento en $\mathbb{F}_q$ si y solo si $q \equiv 1 \bmod 4$.*

Demostración. Sea g un elemento primitivo de $\mathbb{F}_q$, entonces todos los elementos que son cuadrados de otro elemento en $\mathbb{F}_q$ deben ser de la forma g^{2k} para $1 \leq k \leq \frac{q-1}{2}$. Como g es primitivo tenemos que $g^{\frac{q-1}{2}} = -1$, y por tanto -1 es un cuadrado si y solo si $\frac{q-1}{2}$ es par, es decir, $q \equiv 1 \bmod 4$. □

Teorema 3.35 ([5])**.** *Sea $f_0(x)$ un polinomio mónico irreducible de grado $n \geq 1$ en $\mathbb{F}_q$, con q impar. Suponemos que el grado n es par si $q \equiv 3 \bmod 4$ y que $f_0(1)f_0(-1)$ no es un cuadrado en $\mathbb{F}_q$. Para todo $m \geq 1$ definimos $f_m = f_{m-1}^R$, entonces f_m es un polinomio irreducible sobre $\mathbb{F}_q$ de grado $n2^m$ para cada $m \geq 1$.*

Demostración. Durante esta demostración, denotaremos el producto $f(1)f(-1)$ como $\lambda(f)$. Como claramente el operador R asocia un polinomio f de grado n a f^R de grado $2n$, entonces f_m debe tener grado $2^m n$.

Primero vamos a probar por inducción que $\lambda(f_m) = (-1)^n c_m^2 \lambda(f_0)$ con $c_m \in \mathbb{F}_q$. Para el caso $m = 1$ tenemos la cadena de igualdades

$$\lambda(f_1) = f_0^R(1) f_0^R(-1) = 2^n(-2)^n f_0(1) f_0(-1) = (-1)^n c_1^2 \lambda(f_0)$$

siendo $c_1 = 2^n$.

Suponiendo que la igualdad se cumple para $m-1$, como f_{m-1} es de grado $n2^{m-1}$ tenemos

$$\begin{aligned}\lambda(f_m) = f_{m-1}^R(1) f_{m-1}^R(-1) = 2^{n2^{m-1}}(-2)^{n2^{m-1}} \lambda(f_{m-1}) = 2^{n2^{m-1}}(-2)^{n2^{m-1}}(-1)^n c_{m-1}^2 \lambda(f_0) \\ = (-1)^n c_m^2 \lambda(f_0)\end{aligned}$$

siendo $c_m = 2^{n2^{m-1}} c_{m-1}$.

Por el Lema 3.34, como q es impar o bien (-1) es un cuadrado o bien n es par por hipótesis. Por tanto podemos escribir $\lambda(f_m) = (-1)^n c_m^2 \lambda(f_0) = d_m^2 \lambda(f_0)$, y como $\lambda(f_0)$ no es un cuadrado entonces $\lambda(f_m)$ no es un cuadrado para ningún m.

Finalmente, para cada m podemos definir $g_m(x) = 2^{n2^m} f_m(\frac{x}{2})$. Este polinomio es de grado $n2^m$, luego cumple que $g_m^Q = x^{n2^m} g_m(x + \frac{1}{x}) = (2x)^{n2^m} f_m(\frac{1}{2}(x + \frac{1}{x})) = f_m^R$. Por tanto $f_{m+1} = f_m^R = g_m^Q$ y podemos aplicar el Lema 3.32, entonces f_{m+1} es irreducible si y solo si $g_m(2)g_m(-2)$ no es un cuadrado.

Como $g_m(2)g_m(-2) = 2^{n2^{m+1}} f_m(1) f_m(-1) = 2^{n2^{m+1}} \lambda(f_m)$ y $\lambda(f_m)$ no es un cuadrado para ningún m, entonces f_{m+1} es irreducible para todo m. □

3.5. Polinomios ciclotómicos

En esta última sección del capítulo desarrollamos los polinomios ciclotómicos sobre cuerpos finitos, cómo construirlos y cuándo son irreducibles, siguiendo el apartado 9.3 del libro *Finite fields and Galois rings* [17]. Empezamos exponiendo como definir un polinomio ciclotómico en $\mathbb{C}$.

Sea $\mathbb{C}$ el cuerpo de los números complejos, n un entero positivo, y ξ una raíz primitiva n-ésima de la unidad. Tenemos la factorización completa de $x^n - 1$ en factores lineales sobre $\mathbb{C}$:

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

Como las potencias de ξ forman un grupo cíclico, sabemos que $\text{ord}(\xi^i) = \frac{n}{\text{mcd}(n,i)}$, por lo tanto, el orden de cada ξ^i es un divisor de n. Sea $d > 0$ un divisor de n. Definimos

$$\Phi_d(x) = \prod_{\substack{\text{ord}(\xi^i)=d \\ 0 \le i \le n-1}} (x - \xi^i).$$

Este polinomio no depende de la elección de n o ξ, siempre que $d \mid n$ y ξ sea raíz primitiva n-ésima de $x^n - 1$, ya que los ξ^i con orden d son todas las raíces primitivas d-ésima de $x^d - 1$.

Considerando ξ_d una raíz primitiva d-ésima de $x^d - 1$, es claro que ξ_d^i es una raíz primitiva d-ésima solo si $\text{mcd}(d, i) = 1$ y entonces, el grado de $\Phi_d(x)$ debe ser $\varphi(d)$. Llamamos d-ésimo polinomio ciclotómico a $\Phi_d(x)$.

Si al factorizar $x^n - 1$ agrupamos los productos según el orden de las raíces, obtenemos

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

Y aplicando la versión multiplicativa de la fórmula de inversión de Möbius, Teorema 2.23, deducimos

$$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)},$$

lo que implica el siguiente teorema.

Teorema 3.36. *Para todo entero positivo n, $\Phi_n(x)$ es un polinomio con coeficientes enteros.*

Demostración. La ecuación previa nos permite expresar $\Phi_n(x)$ como el cociente de dos polinomios mónicos con coeficientes enteros. El numerador es el producto de todos los términos $x^d - 1$ para los que $\mu(n/d) = 1$, y el denominador es el producto de todos los términos para los cuales $\mu(n/d) = -1$.

Si llamamos $p(x)$ al numerador y $q(x)$ al denominador tenemos $p(x), q(x) \in \mathbb{Z}[x]$ mónicos tal que $p(x) = \Phi_n(x) \cdot q(x)$. Entonces, necesariamente $\Phi_n(x) \in \mathbb{Z}[x]$. □

Este teorema justifica definir $\Phi_n(x)$ como el polinomio ciclotómico n-ésimo sobre cualquier cuerpo finito $\mathbb{F}_q$, donde los coeficientes enteros de $\Phi_n(x)$ deben interpretarse como elementos en el cuerpo primo $\mathbb{F}_p$ de $\mathbb{F}_q$.

Ejemplo 3.37. Usando la expresión que tiene $\Phi_n(x)$ como cociente de polinomios obtenemos

$$\Phi_{15}(x) = \frac{(x^{15} - 1)(x - 1)}{(x^5 - 1)(x^3 - 1)} = \frac{x^{10} + x^5 + 1}{x^2 + x + 1} = x^9 - x^7 + x^5 - x^4 + x^3 - x - 1.$$

También tenemos

$$\Phi_{20}(x) = \frac{(x^{20} - 1)(x^2 - 1)}{(x^{10} - 1)(x^4 - 1)} = \frac{x^{10} + 1}{x^2 + 1} = x^8 - x^6 + x^4 - x^2 + 1.$$

Ahora estudiamos la factorización de $\Phi_n(x)$ sobre un cuerpo finito dado. Para empezar, tenemos este resultado.

Teorema 3.38. *Sea p un número primo y n tal que* $\mathrm{mcd}(p,n)=1$. *Entonces*

$$\Phi_{np^k}(x)=\Phi_n(x)^{p^k-p^{k-1}}$$

en cualquier cuerpo de característica p.

Demostración. Primero consideramos que

$$\Phi_{np^k}(x)=\prod_{d\mid np^k}\left(x^d-1\right)^{\mu(np^k/d)}=\prod_{d\mid np^k}\left(x^{np^k/d}-1\right)^{\mu(d)}$$

ya que si d recorre todos los divisores de np^k, entonces np^k/d también los recorre, luego con una reordenación del producto tenemos la última igualdad.

Ahora, como sabemos que $\mathrm{mcd}(p,n)=1$, si $d\mid np^k$ tenemos dos posibilidades; o bien $d\mid n$, o bien $p\mid d$ y $d\mid np^k$. Si $p^2\mid d$, d es divisible por el cuadrado de un primo y eso implica que $\mu(d)=0$.

Entonces podemos reducir el producto al caso $d\mid n$, o al caso $d=d_1p$ para cierto d_1 tal que $d_1\mid n$, que es lo mismo que decir que $d_1p\mid np$. Con esto podemos continuar la igualdad de la siguiente forma.

$$\begin{aligned}\prod_{d\mid np^k}\left(x^{p^kn/d}-1\right)^{\mu(d)}&=\prod_{d\mid n}\left(x^{p^kn/d}-1\right)^{\mu(d)}\prod_{dp\mid np}\left(x^{p^kn/dp}-1\right)^{\mu(dp)}\\&=\left(\prod_{d\mid n}(x^{n/d}-1)^{\mu(d)}\right)^{p^k}\left(\prod_{d\mid n}(x^{n/d}-1)^{-\mu(d)}\right)^{p^{k-1}}.\end{aligned}$$

La última igualdad se obtiene teniendo en cuenta que $(a-b)^{p^k}=a^{p^k}-b^{p^k}$ en un cuerpo de característica p, y que $\mu(dp)=-\mu(d)$ por definición, al ser p primo.

Finalmente, podemos reescribir la última expresión que hemos obtenido,

$$\left(\prod_{d\mid n}(x^{n/d}-1)^{\mu(d)}\right)^{p^k}\left(\prod_{d\mid n}(x^{n/d}-1)^{-\mu(d)}\right)^{p^{k-1}}=\Phi_n(x)^{p^k}\Phi_n(x)^{-p^{k-1}}=\Phi_n(x)^{p^k-p^{k-1}},$$

lo que nos da el resultado que buscamos. □

En el siguiente ejemplo recurriremos a este teorema para simplificar el cálculo de polinomios ciclotómicos.

Ejemplo 3.39. Consideremos $\Phi_{36}(x)$. Tenemos $36=9\cdot 2^2=4\cdot 3^2$. Por el teorema previo, sobre cualquier cuerpo de característica 2,

$$\Phi_{36}(x)=\Phi_9(x)^2=\Phi_3(x)^2=(x^6+x^3+x+1)^2.$$

Y sobre cualquier cuerpo de característica 3,

$$\Phi_{36}(x)=\Phi_4(x)^3=\Phi_4(x)=(x^2+1)^3=(x^6+1)^2.$$

Si factorizamos $\Phi_n(x)$ sobre un cuerpo de característica p, podemos calcular el polinomio ciclotómico sobre un factor de n al que no divida p y aplicar el teorema previo para obtener $\Phi_n(x)$. Por tanto, la suposición de que $p\nmid n$ no nos restringe a la hora de manejar polinomios ciclotómicos.

Teorema 3.40. *Sea q la potencia de un p número primo y asumimos que $p \nmid n$. Sea m el menor natural tal que $q^m \equiv 1 \bmod n$. Entonces $\Phi_n(x)$ factoriza sobre $\mathbb{F}_q$ como el producto de $\varphi(n)/m$ polinomios irreducibles mónicos de grado m.*

Demostración. Sea ξ un elemento primitivo del cuerpo finito $\mathbb{F}_{q^m}$. Entonces, el orden de ξ es $q^m - 1$. Como $q^m \equiv 1 \pmod{n}$, podemos considerar $\frac{q^m-1}{n} \in \mathbb{N}$. Sea $\alpha = \xi^{(q^m-1)/n}$, entonces α es de orden n y todas las potencias α^i, donde $1 \leq i \leq n-1$ y $\mathrm{mcd}(i,n) = 1$, también son de orden n. Hay $\varphi(n)$ de estos elementos.

Como $\xi \in \mathbb{F}_{q^m}$ y es primitivo, ξ es raíz de $x^{q^m-1} - 1$ y por tanto es raíz primitiva $q^m - 1$-ésima de la unidad. Entonces podemos considerar

$$\Phi_n(x) = \prod_{\substack{1 \leq i \leq q^m-1 \\ \mathrm{ord}(\xi)=n}} (x - \xi^i) = \prod_{\substack{1 \leq i \leq n-1 \\ \mathrm{mcd}(i,n)=1}} (x - \alpha^i).$$

ya que los α^i tenían orden n solo cuando $\mathrm{mcd}(i,n) = 1$, y como el grado de $\Phi_n(x)$ es $\varphi(n)$, no puede haber más elementos de orden n en $\mathbb{F}_{q^m}$ que los α^i.

Ahora consideramos el polinomio mínimo de α^i y lo denotamos por m_α. Por el Teorema 2.10(vi), $m_\alpha = (x - \alpha^i)(x - \alpha^{iq}) \cdots (x - \alpha^{iq^{d-1}})$ y, como todas las raíces son distintas, d es el menor natural tal que $\alpha^{iq^d} = \alpha^i$.

Entonces tenemos que $\alpha^{i(q^d-1)} = 1$, usando que el orden de α^i es n, deducimos que $n \mid q^d - 1$ y $q^d \equiv 1 \bmod n$. Como m es el menor natural que cumple esta propiedad, $m \leq d$. Siguiendo este razonamiento en la otra dirección, tenemos que $q^m \equiv 1 \bmod n$ implica $\alpha^{i(q^d-1)} = 1$, y como d es el menor natural que cumple esto, $d \leq m$.

Luego $m_\alpha = (x - \alpha^i)(x - \alpha^{iq}) \cdots (x - \alpha^{iq^{m-1}})$ es el polinomio irreducible de m elementos, y si consideramos que $p \nmid n$, es claro que $\mathrm{mcd}(iq^j, n) = 1$. Entonces todas las raíces del polinomio mínimo están en el polinomio ciclotómico que hemos construido.

Agrupando el polinomio ciclotómico en los polinomios mínimos de cada raíz, como estos tienen grado m y hay $\varphi(n)$ raíces, obtenemos una descomposición en $\mathbb{F}_q$ de $\varphi(n)/m$ polinomios irreducibles. □

Con este teorema tenemos una factorización de $\Phi_n(x)$, y de esto es fácil deducir un corolario para ver cuándo $\Phi_n(x)$ es irreducible.

Corolario 3.41. *Sea q una potencia de p número primo tal que $p \nmid n$. Entonces, $\Phi_n(x)$ es irreducible sobre $\mathbb{F}_q$ si y solo si $\varphi(n)$ es el menor entero positivo tal que $q^{\varphi(n)} \equiv 1 \bmod n$.*

Demostración. Si suponemos que $\Phi_n(x)$ es irreducible, factoriza en un polinomio irreducible. Entonces, por el teorema previo, $\varphi(n) = m$ y por tanto $\varphi(n)$ es el menor natural tal que $q^m \equiv 1 \bmod n$.

Razonando en la otra dirección, si $\phi(n)$ es el menor natural tal que $q^{\phi(n)} \equiv 1 \bmod n$, aplicando el teorema previo, $\varphi(n) = m$. Esto implica que $\Phi_n(x)$ factoriza en un polinomio irreducible, es decir, es irreducible. □

Ejemplo 3.42. En el caso de $\mathbb{F}_2$, podemos ver cuándo $\varphi(n)$ coincide con el orden multiplicativo de 2 en $\mathbb{Z}_n$ para los n impares. Usando esto calculamos en MAPLE todos los polinomios ciclotómicos irreducibles $\Phi_n(x)$ con n impar menor o igual que 125.

n	3	5	9	11	13	19	25	27	29	37	53	59	61	67	81	83	101	107	121	125
$\varphi(n)$	2	4	6	10	12	18	20	18	28	36	52	58	60	66	54	82	100	106	110	100

Cuadro 3.1: Valores de todo n impar menor o igual que 100 asociado a un $\Phi_n(x)$ irreducible en $\mathbb{F}_2[x]$, y su respectivo $\varphi(n)$.

n	$\varphi(n)$	Polinomio ciclotómico de grado $\varphi(n)$
3	2	x^2+x+1
5	4	$x^4+x^3+x^2+x+1$
9	6	x^6+x^3+1
11	10	$x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$
13	12	$x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$
25	20	$x^{20}+x^{15}+x^{10}+x^5+1$
27	18	$x^{18}+x^9+1$
81	54	$x^{54}+x^{27}+1$
121	110	$x^{110}+x^{99}+x^{88}+x^{77}+x^{66}+x^{55}+x^{44}+x^{33}+x^{22}+x^{11}+1$
125	100	$x^{100}+x^{75}+x^{50}+x^{25}+1$

Cuadro 3.2: Algunos de los $\Phi_n(x)$ irreducibles en $\mathbb{F}_2[x]$.

Capítulo 4

Teorema de Wedderburn

Un teorema de interés en cuerpos finitos es el Teorema de Wedderburn, que nos permite extender todos los resultados vistos hasta ahora en cuerpos finitos a anillos de división finitos.

Aunque el teorema no está directamente relacionado con los polinomios irreducibles, debido a su gran relevancia en la teoría de cuerpos finitos merece una breve mención en este trabajo. El teorema simplifica la clasificación de estructuras algebraicas, eliminando las distinciones entre dominios, anillos de división y cuerpos en el caso finito.

La demostración que veremos está ilustrada en el libro *Introduction to finite fields and their applications* [10] y requiere de ciertos resultados previos sobre polinomios ciclotómicos. Ahora que hemos estudiado estos polinomios tenemos las herramientas necesarias para la demostración.

Recordamos que un grupo es anillo de división si cumple las condiciones de cuerpo excepto la conmutatividad del producto.

Teorema 4.1 (Wedderburn [18])**.** *Todo anillo de división finito es un cuerpo finito.*

Demostración. Sea E un anillo de división finito y F un subconjunto de E definido de la siguiente forma, $F = \{\lambda \in E : \lambda x = x\lambda \text{ para todo } x \in E\}$. Claramente $0, 1 \in F$ y si λ, $\mu \in F$ tenemos que $\lambda\mu$, $\lambda - \mu \in F$.

Además, si $\lambda \neq 0 \in F$, podemos considerar $(y^{-1}\lambda^{-1}y)^{-1} = y^{-1}\lambda y = y$ para todo $y \in E^*$, y entonces $\lambda^{-1} = y^{-1}\lambda^{-1}y$ para todo $y \in E^*$, es decir, $\lambda^{-1} \in F$. Por lo tanto F es un cuerpo conmutativo.

Como E es finito, F es un cuerpo finito, $|F| = q$ para algún $q \in \mathbb{N}$, y considerando E como un espacio vectorial sobre F de dimensión finita n tenemos que $|E| = q^n$. Si probamos que $n = 1$, tendremos que E es un cuerpo finito. Razonamos por reducción al absurdo, suponiendo que $n > 1$.

Definimos la siguiente relación de equivalencia, $x \sim y \Leftrightarrow \exists z \in E^*$ tal que $z^{-1}xz = y$, y denotamos la clase de equivalencia de y por C_y. También definimos para cada $y \in E^*$ el normalizador de y, $N_y = \{x \in E : xy = yx\}$, que con cálculos similares a los hechos para F se ve que es un anillo de división.

Veamos ahora que para cualquier $y \in E$, considerando $A_y = \{aya^{-1} : a \in E^*\}$, tenemos que $C_y = A_y$. Si $b \in A_y$, entonces $b = aya^{-1}$ para algún $a \in A_y$ y por tanto tomando z como a se cumple que $z^{-1}bz = y$, es decir, $b \in C_y$. Si $b \in C_y$, existe un $z \in E^*$ tal que $z^{-1}bz = y$, luego $b \in A_y$.

Usando esto, podemos ver que C_y tiene solo un elemento si y solo si $y \in F$. Si C_y tiene solo un elemento, debe ser y, luego para todo $a \in E^*$ tenemos que $aya^{-1} = y$, y por tanto $y \in F$. Si $y \in F$, para todo $a \in E^*$ tenemos que $aya^{-1} = y$, luego solo y está en C_y.

Podemos escribir E^* como la unión disjunta de todas sus clases de equivalencia. Como $F = \mathbb{F}_q$, el cardinal de F^* es $q-1$ y por tanto en E^* hay exactamente $q-1$ clases de equivalencia de un solo elemento.

Para contar el número de elementos del resto de clases vamos a establecer una biyección entre los elementos de A_y y las clases laterales por la izquierda de N_y^*, es decir, los conjuntos de la forma aN_y^* con $a \in E^*$.

Para un $y \in E^*$ fijo, si consideramos $a, b \in E^*$ tal que $aya^{-1}, byb^{-1} \in A_y$, tenemos la siguiente cadena de implicaciones.

$$aya^{-1} = byb^{-1} \iff y = a^{-1}byb^{-1}a = (a^{-1}b)y(a^{-1}b)^{-1} \iff a^{-1}b \in N_y^* \iff b \in aN_y^*.$$

Como cada clase lateral por la izquierda de N_y^* son los elementos de E^* módulo N_y^* tenemos que $|C_y| = |A_y| = |E^*|/|N_y^*|$.

También podemos considerar cada N_y como un espacio vectorial de F, y por tanto $|N_y| = q^{n(y)}$ siendo $n(y)$ la dimensión del espacio vectorial.

Supongamos que $y_1, \ldots, y_s$ son representantes de cada clase de equivalencia de más de un elemento y $\lambda_1, \ldots, \lambda_{q-1}$ son representantes de cada clase de equivalencia de un solo elemento no nulo. Entonces la partición de E^* en sus clases de equivalencia queda

$$q^n - 1 = |E^*| = \sum_{i=1}^{q-1} |C_{\lambda_i}| + \sum_{j=1}^{s} |C_{y_j}| = q - 1 + \sum_{j=1}^{s} \frac{q^n - 1}{q^{n(y_j)} - 1}.$$

Ahora, como N_y^* es subgrupo de E^*, tenemos que $q^{n(y)} - 1 \mid q^n - 1$. Si $n = n(y)m + t$ con $0 \leq t < n(y)$, entonces $q^n - 1 = q^{n(y)m}q^t - 1 = q^t(q^{n(y)m} - 1) + q^t - 1$.

Como $q^{n(y)} - 1$ divide a $q^n - 1$ y a $q^{n(y)m} - 1$ tenemos que también divide a $q^t - 1$. Pero $q^t - 1 < q^{n(y)} - 1$, luego t debe ser cero y entonces $n(y)$ divide a n para cualquier $y \in E^*$.

Para la siguiente parte de la demostración necesitamos ver que $\Phi_n(x)$ divide a $x^n - 1$ y a $\frac{x^n-1}{x^{n(y)}-1}$. Como hemos visto en la sección de polinomios ciclotómicos, $x^n - 1 = \prod_{d|n} \Phi_d(x)$, luego $\Phi_n(x)$ divide a $x^n - 1$.

Considerando que $x^n - 1 = (x^{n(y)} - 1)\frac{x^n-1}{x^{n(y)}-1}$ y que las raíces de $\Phi_n(x)$ son de orden n mientras que las raíces de $x^{n(y)} - 1$ son de orden menor o igual que $n(y)$, tenemos que $\Phi_n(x)$ no comparte raíces con $x^{n(y)} - 1$ y entonces debe dividir a $\frac{x^n-1}{x^{n(y)}-1}$.

Por tanto, sustituyendo la ecuación de clases de equivalencia en q tenemos que $\Phi_n(q)$ debe dividir a

$$q^n - 1 - \sum_{i=1}^{s} \frac{q^n - 1}{q^{n(y_i)} - 1} = q - 1.$$

Finalmente, consideramos $\Phi_n(x) = \prod_{\xi \in C_n}(x - \xi)$ sobre $\mathbb{C}$, donde C_n es el conjunto de raíces primitivas n-ésimas de la unidad.

Por un razonamiento geométrico, podemos considerar que $|q - \xi| > q - 1$, ya que las raíces están en la circunferencia unidad centrada en el 0 y q está a la derecha del 1 en la recta real, por lo que está más próximo a 1 que al resto de raíces.

Evaluando $\Phi_n(x)$ otra vez en q,

$$|\Phi_n(q)| = \prod_{\xi \in C_n} |q - \xi| > (q-1)^{\varphi(n)} \geq q - 1.$$

Por tanto $|\Phi_n(q)|$ no puede dividir a $q - 1$, con lo que llegamos a contradicción. □

Capítulo 5

Polinomios irreducibles sobre $\mathbb{F}_2[x]$

Hasta ahora hemos estado trabajando sobre cuerpos finitos cualquiera, pero si echamos un vistazo al uso actual de los cuerpos finitos en la criptografía o la teoría de códigos, tanto por motivos de hardware como de eficiencia de las operaciones, los cuerpos que se utilizan son $\mathbb{F}_{2^n}$. Por tanto necesitaremos polinomios irreducibles sobre $\mathbb{F}_2$ para representar estos cuerpos y operar sobre ellos.

Los resultados de irreducibilidad que hemos visto en el capítulo previo no son muy útiles al aplicarlos en $\mathbb{F}_2$, así que obtendremos nuevos resultados de irreducibilidad centrados exclusivamente en polinomios sobre $\mathbb{F}_2[x]$.

En artículos como [4] y [8] se representa el cuerpo $\mathbb{F}_{2^n}$ con trinomios o pentanomios irreducibles, que serán los polinomios en los que centraremos nuestro estudio en esta sección.

También exploraremos una técnica para obtener polinomios primitivos que solo funciona en $\mathbb{F}_2$, y la aplicaremos en particular a trinomios, obteniendo así trinomios primitivos de grados muy altos.

5.1. Trinomios irreducibles

Si buscamos construir cuerpos de característica 2, necesitaremos polinomios irreducibles sobre $\mathbb{F}_2$. Por su bajo número de coeficientes distintos de cero, los binomios y trinomios generan cuerpos donde las operaciones son más eficientes, y en cuerpos de característica 2 claramente los binomios nunca pueden ser irreducibles. Por esta razón primero estudiaremos cómo encontrar trinomios irreducibles sobre $\mathbb{F}_2$ y veremos si podemos caracterizarlos.

Blake, Gao y Lambert estudian la distribución de trinomios irreducibles y conjeturan posibles caracterizaciones en el artículo [1]. Durante esta sección nos apoyaremos en dicho artículo para estudiar con más detalle los casos en los que ciertos trinomios son irreducibles.

Para estudiar la irreducibilidad de trinomios sobre $\mathbb{F}_2$, el resultado más fuerte que tenemos nos lo proporciona Swan [15].

Teorema 5.1 (Swan [15])**.** *Sean $0 < k < n$ números naturales. El trinomio $x^n + x^k + 1$ tiene un número par de factores sobre $\mathbb{F}_2$ en cada uno de los siguientes casos:*

(a) n es par, k es impar, $n \neq 2k$ y $nk/2 \equiv 0$ o $1 \bmod 4$,

(b) n es impar, k es par, $k \nmid 2n$ y $n \equiv \pm 3 \bmod 8$,

(c) n es impar, k es par, $k \mid 2n$ y $n \equiv \pm 1 \bmod 8$.

No veremos la demostración de este resultado ya que es bastante complicada y se sale del alcance de este trabajo. Sin embargo, usaremos este resultado para ver un corolario que garantiza la reducibilidad de ciertos trinomios.

Corolario 5.2. *No existe ningún trinomio irreducible de grado n en $\mathbb{F}_2[x]$ si $n \equiv 0 \bmod 8$.*

Demostración. Sean $0 < k < n$ números naturales, consideramos el trinomio $x^n + x^k + 1$ en $\mathbb{F}_2[x]$. Veamos que si $n \equiv 0 \bmod 8$, el trinomio no puede ser irreducible. Como $n \equiv 0 \bmod 8$, entonces n debe ser par y por tanto, si k es par, podemos escribir el trinomio como $(x^{n/2} + x^{k/2} + 1)^2$, es decir, es reducible.

Para los casos con k impar, aplicando la parte (a) del teorema de Swan, el trinomio debe tener un número par de factores, y por tanto no puede ser irreducible.

Veamos que se cumplen las condiciones para aplicar el teorema de Swan en este caso. Como $n \equiv 0 \bmod 8$, tenemos que 8 debe ser un factor de n, y como k es impar, necesariamente $n \neq 2k$. De la misma forma, 4 debe ser un factor de $n/2$, y por tanto, $nk/2 \equiv 0$.

Con esto hemos probado que $x^n + x^k + 1$ debe ser reducible para los casos de k par y k impar. □

A partir de este punto denotaremos al trinomio $x^n + x^k + 1$ como $T_{n,k}$. Para los posibles n, k que no se cubren en el Teorema de Swan basta considerar que si ambos son pares, como $T_{n,k} \in \mathbb{F}_2[x]$, tenemos que $T^2_{n/2,k/2} = T_{n,k}$, luego siempre es reducible, y si ambos son impares, por el Teorema 3.4, la reducibilidad de $T_{n,k}$ es equivalente a la de $T_{n,n-k}$, al que podemos aplicar el Teorema de Swan.

Apoyándose en las consideraciones previas y en el Teorema de Swan, los autores del artículo se preguntan si los trinomios irreducibles también tienen una correlación con el grado módulo 8, y calculan la Tabla 5.1 mostrando el número de trinomios irreducibles en $\mathbb{F}_2[x]$ según su grado módulo 8.

En el artículo se destaca la abundancia relativa de trinomios irreducibles cuando $n \equiv \pm 1 \bmod 8$ y la escasez relativa cuando $n \equiv \pm 3 \bmod 8$, lo que puede indicar una relación de los trinomios irreducibles con su grado módulo 8.

También destacan ciertas relaciones que se mantienen tanto en la tabla como en las condiciones del teorema de Swan, como la simetría entre $n \equiv 3 \bmod 8$ y $n \equiv -3 \bmod 8$, o entre $n \equiv 1 \bmod 8$ y $n \equiv -1 \bmod 8$.

Para ver esto con más detalle podemos desglosar los casos de n par en los que el teorema de Swan no garantiza que un trinomio sea reducible, y ver si se alinea con la Tabla 5.1. No consideraremos los casos donde n, k son pares, ya que en estos casos los trinomios son siempre reducibles, como hemos visto antes.

- Si $n \equiv 2 \bmod 8$, k impar.

  No se cumplen las condiciones del teorema de Swan si $n = 2k$ o $nk/2 \equiv 2$ o $3 \bmod 4$.Como $n \equiv 2 \bmod 8$, tenemos que $n/2 \equiv 1 \bmod 4$, luego la condición $nk/2 \equiv 2$ o $3 \bmod 4$ queda $k \equiv 2$ o $3 \bmod 4$. Como k es impar, solo se puede dar $k \equiv 3 \bmod 4$.

- Si $n \equiv -2 \bmod 8$, k impar.

  Razonando de la misma forma que antes, obtenemos que los trinomios que no cumplen las condiciones son de la forma $n = 2k$ o $k \equiv -3 \equiv 1 \bmod 4$.

- Si $n \equiv 4 \bmod 8$, k impar.

  En este caso tenemos que $n/2 \equiv 2 \bmod 4$, luego $nk/2 \equiv 2k \bmod 4$. Entonces no cumplen las condiciones los trinomios con $n = 2k$ o $2k \equiv 2$ o $3 \bmod 4$. Claramente el caso $2k \equiv 3 \bmod 4$ no se puede dar y como k es impar, $2k \equiv 2 \bmod 4$ se da para todo k.

Rango/Grado mod 8	1	2	3	4	5	6	7	**Total**
1–200	73	27	7	73	5	30	82	297
201–400	92	36	0	74	2	25	76	305
401–600	85	26	0	71	0	35	71	288
601–800	87	30	1	73	0	34	94	319
801–1.000	81	31	1	77	2	29	83	304
1.001–1.200	87	28	0	67	3	36	84	305
1.201–1.400	79	29	0	74	0	29	86	297
1.401–1.600	92	29	0	75	0	41	98	335
1.601–1.800	93	22	0	66	0	26	71	278
1.801–2.000	82	21	0	58	0	33	97	291
2.001–2.200	86	28	0	75	0	27	108	324
2.201–2.400	96	29	1	77	0	23	83	309
2.401–2.600	79	26	0	84	1	31	73	294
2.601–2.800	87	27	1	85	0	23	104	327
2.801–3.000	69	29	0	59	0	16	83	256
3.001–3.200	99	23	0	74	0	29	85	310
3.201–3.400	79	29	0	77	0	37	88	310
3.401–3.600	83	28	0	74	0	32	84	301
3.601–3.800	92	23	0	86	0	28	91	320
3.801–4.000	88	25	0	75	0	29	90	307
4.001–4.200	82	32	0	57	1	37	73	282
4.201–4.400	75	34	0	72	0	35	96	312
4.401–4.600	89	36	0	66	2	34	85	312
4.601–4.800	101	32	0	84	0	20	71	308
4.801–5.000	75	25	0	67	1	30	84	282
9.801–10.000	71	31	0	76	0	33	102	313

Cuadro 5.1: Número total de trinomios irreducibles $T_{n,k}(x)$ en el rango indicado, con $k \leq n/2$.

Podemos ver que, al igual que en la Tabla 5.1, hay una simetría entre los casos $n \equiv 2 \bmod 8$ y $n \equiv 6 \bmod 8$, mientras que para $n \equiv 4 \bmod 8$ se mantiene alrededor del doble de casos.

Ver en qué casos estas similitudes se mantienen podría indicarnos posibles condiciones para caracterizar los trinomios irreducibles, y también ilustraría si estas condiciones podrían ser similares a las que da el teorema de Swan.

Para hacer esta comparación construimos la Tabla 5.2 donde para cada n fijo, calculamos con MAPLE el número de posibles k que no cumplen las condiciones del teorema de Swan, es decir, los trinomios $x^n + x^k + 1$ en $\mathbb{F}_2[x]$ que el teorema de Swan no garantiza que sean reducibles, y comparar ambas tablas parece indicar que el teorema de Swan tiene una fuerte relación con la irreducibilidad de los trinomios.

Continuando con el estudio de los trinomios en $\mathbb{F}_2[x]$, en el artículo [6] los autores aplican el teorema de Butler [3] a trinomios en $\mathbb{F}_2[x]$ para caracterizar los trinomios irreducibles de la forma $x^{8n\pm3} + x^k + 1$. Durante el resto de esta sección demostraremos algunos de los resultados siguiendo este artículo y obtendremos varios criterios de irreducibilidad para trinomios.

Definición 5.3. Definimos el índice de un polinomio irreducible $f(x)$ de grado n sobre $\mathbb{F}_q$ como $\frac{q^n-1}{e}$ donde e es el orden de f.

Aplicando el Corolario 2.14 es inmediato ver que el índice es un número natural.

Teorema 5.4 (Butler [3])**.** *Sea $f(x)$ un polinomio irreducible de grado n sobre $\mathbb{F}_q$ de orden e, índice*

Rango/Grado mod 8	1	2	3	4	5	6	7	**Total**
1–200	1.142	325	63	625	61	350	1.216	3.782
201–400	3.618	950	75	1.875	73	975	3.692	11.258
401–600	6.117	1.575	83	3.125	87	1.600	6.192	18.779
601–800	8.615	2.200	89	4.375	89	2.225	8.684	26.277
801–1.000	11.107	2.825	93	5.625	91	2.850	11.186	33.777
1.001–1.200	13.606	3.450	95	6.875	101	3.475	13.684	41.286
1.201–1.400	16.103	4.075	97	8.125	93	4.100	16.178	48.771
1.401–1.600	18.602	4.700	97	9.375	97	4.725	18.670	56.266
1.601–1.800	21.098	5.325	101	10.625	97	5.350	21.182	63.778
1.801–2.000	23.606	5.950	105	11.875	105	5.975	23.674	71.290
2.001–2.200	26.090	6.575	99	13.125	97	6.600	26.172	78.758
2.201–2.400	28.600	7.200	101	14.375	109	7.225	28.674	86.284
2.401–2.600	31.098	7.825	105	15.625	107	7.850	31.168	93.778
2.601–2.800	33.586	8.450	105	16.875	95	8.475	33.664	101.250
2.801–3.000	36.096	9.075	103	18.125	113	9.100	36.174	108.786
3.001–3.200	38.594	9.700	111	19.375	103	9.725	38.664	116.272
3.201–3.400	41.094	10.325	111	20.625	113	10.350	41.166	123.784
3.401–3.600	43.592	10.950	101	21.875	109	10.975	43.660	131.262
3.601–3.800	46.094	11.575	117	23.125	109	11.600	46.176	138.796
3.801–4.000	48.582	12.200	111	24.375	107	12.225	48.664	146.264
4.001–4.200	51.091	12.825	107	25.625	115	12.850	51.162	153.775
4.201–4.400	53.592	13.450	117	26.875	111	13.475	53.670	161.290
4.401–4.600	56.090	14.075	107	28.125	111	14.100	56.156	168.764
4.601–4.800	58.580	14.700	111	29.375	117	14.725	58.670	176.278
4.801–5.000	61.089	15.325	119	30.625	101	15.350	61.158	183.767
9.801–10.000	123.576	30.950	115	61.875	111	30.975	123.634	371.236

Cuadro 5.2: Número total de trinomios $T_{n,k}(x)$ que el teorema de Swan no garantiza que sean reducibles en el rango indicado, con $k \leq n/2$.

d. Sean M, m_1, m_2 números naturales tal que $\mathrm{mcd}(M, q) = 1$ *y* $M = m_1 m_2$ *donde* $\mathrm{mcd}(m_1, e) = 1$ *y cada divisor primo de m_2 es un divisor primo de e. Entonces*

(i) El orden de las raíces de $f(x^M)$ es de la forma gm_2e, donde $g \mid m_1$;

(ii) Si $g \mid m_1$, entonces $f(x^M)$ tiene exactamente

$$\frac{Nm_2\varphi(g)}{S(gm_2e; q)}$$

factores irreducibles de grado $S(gm_2e; q)$ con raíces de orden gm_2e, donde $S(a; q)$ denota el orden de q módulo a.

La demostración de este resultado es muy complicada para el alcance de este trabajo, por lo que no la expondremos. Veamos que aplicando este teorema a un trinomio bajo ciertas condiciones nos permite construir trinomios irreducibles.

Teorema 5.5. *Supongamos que $T_{n,2}$ es un trinomio irreducible en $\mathbb{F}_2$, de orden e e índice $d = \frac{2^n-1}{e}$, y sea P un número primo. Si $P \mid e$ y $P \nmid d$, entonces $T_{NP,2P}$ es irreducible con orden Pe.*

Demostración. Primero veamos que podemos aplicar el teorema de Butler. Por el Corolario 2.14 tenemos que $e \mid 2^n - 1$, y por esto e es impar, además como $P \mid e$, entonces $P \neq 2$. Ahora consideramos

$M = P$, $m_1 = 1$, $m_2 = P$, que al ser P un primo distinto de 2, claramente cumplen que $\mathrm{mcd}(M, 2) = 1$, $M = m_1 m_2$, $\mathrm{mcd}(m_1, e) = 1$ y cada divisor primo de m_2 es un divisor primo de e, ya que $P \mid e$ por hipótesis. También suponemos que $P \nmid d$ y que $T_{n,2}$ es irreducible, así que podemos aplicar el teorema y ver en cuántos factores descompone $T_{nP,2P}$.

Por el segundo apartado del teorema de Butler, si $g \mid 1$, es decir $g = 1$, tenemos que $T_{nP,2P}$ tiene exactamente $\frac{nP}{S(Pe;2)}$ factores. Veamos ahora que $S(Pe; 2) = nP$.

Como $e \mid 2^n - 1$, tenemos que $2^n \equiv 1 \bmod e$. Con esto podemos escribir, para cierto $k \in \mathbb{N}$,

$$2^n = 1 + ek,\ 2^{nP} = (1 + ek)^P = 1 + \sum_{j=1}^{P} \binom{P}{j} (ek)^j,\ 2^{nP} \equiv 1 \bmod Pe.$$

Para ver que el orden de 2 es nP, supongamos que $2^t \equiv 1 \bmod Pe$ para un $t < nP$ y llegaremos a un absurdo. Como $2^t \equiv 1 \bmod Pe$, tenemos que $2^t \equiv 1 \bmod e$, y ya hemos visto que n también lo cumple. Por tanto, $t \mid n$ o $n \mid t$. Además, como $2^{nP} \equiv 1 \bmod Pe$, vemos que $t \mid nP$.

Si $n \mid t$, como $t \mid nP$, P es primo y $t < nP$, debe ocurrir que $t = n$. También, como $2^n - 1 = ed$ y $p \nmid d$, se ve que $2^n \not\equiv 1 \bmod Pe$. Entonces, tanto si $t \mid n$ como si $t = n$, llegamos a un absurdo, ya que $2^t \equiv 1 \bmod Pe$.

Por tanto, $\mathrm{ord}_{Pe}(2) = nP$ y entonces $T_{nP,2P}$ es irreducible, y por el Teorema 2.13, su orden es el mismo que el de sus raíces, es decir, Pe. □

Ahora planteamos un par de lemas que nos permitirán demostrar el teorema que caracteriza todos los trinomios de la forma $T_{nP^k,2P^k}$ a partir de $T_{n,2}$.

Recordamos que la notación $P^a \parallel n$, P^a divide exactamente a n, significa que $P^a \mid n$ y $P^{a+1} \nmid n$.

Lema 5.6. *Para un primo P distinto de 2, si $P^a \parallel 2^n - 1$ entonces $P^{a+1} \parallel 2^{nP} - 1$.*

Demostración. Tenemos que probar que $P^{a+1} \mid 2^{nP-1}$ y $P^{a+2} \nmid 2^{nP} - 1$. Empezamos viendo que

$$2^{nP} - 1 = (2^n - 1)(2^{n(P-1)} + 2^{n(P-2)} + \cdots + 2^n + 1),$$

como $P^a \parallel (2^n - 1)$, podemos escribir $2^n = 1 + P^a M$ con $M \in \mathbb{N}$, $P \nmid M$.

Entonces, para $j \in \mathbb{N}$,

$$2^{jn} = (1 + P^a M)^j = 1 + jP^a M + K,$$

siendo K una suma de términos donde $P^{2a} \mid K$. Por tanto

$$\sum_{j=0}^{P-1} 2^{jn} = P + \frac{(P-1)P}{2} P^a M + C \text{ donde } P^{2a} \mid C.$$

Como P es un primo distinto de 2, es impar, y por tanto el sumatorio se puede escribir como $P + P^{a+1}q$, para algún $q \in \mathbb{N}$. De esto se deduce que P divide exactamente a $\sum_{j=0}^{P-1} 2^{jn}$, y como también tenemos que P^a divide exactamente a $2^n - 1$, tenemos que P^{a+1} divide exactamente a $2^{nP} - 1$. □

Lema 5.7. *Si un trinomio de la forma $T_{U,2}$ es reducible, todo trinomio de la forma $T_{UV,2V}$ es reducible.*

Demostración. Si $f(x)$ es un factor de $T_{U,2}(x) = x^U + x^2 + 1$, al poder escribir $T_{UV,2V}$ como $T_{U,2}(x^V) = x^{UV} + x^{2V} + 1$, tenemos que $f(x^V)$ es factor de $T_{UV,2V}$.

Teorema 5.8. *Sea $T_{n,2}$ trinomio de orden e, índice d, y sea P primo tal que $P \mid e$ y $P \nmid d$. Si $T_{n,2}$ es irreducible entonces $T_{nP^t,2P^t}$ es irreducible para todo $t \in \mathbb{N}$. Si $T_{nP^t,2P^t}$ es irreducible para algún $t \in \mathbb{N}$ entonces $T_{n,2}$ es irreducible. Además, cuando es irreducible, el orden de $T_{nP^t,2P^t}$ es $P^t e$.*

Demostración. Si suponemos $T_{n,2}$ irreducible, P primo tal que $P \mid e$ y $P \nmid d$, podemos probar la implicación, y que el orden de $T_{nP^t,2P^t}$ es $P^t e$, usando inducción sobre t.

Para $t = 1$, aplicamos directamente el Teorema 5.5, y tenemos que $T_{nP,2P}$ es irreducible de orden Pe.

Suponemos que $T_{nP^{t-1},2P^{t-1}}$ es irreducible, de orden $P^{t-1}e$, índice $\frac{2^{nP^{t-1}}-1}{P^{t-1}e}$, veamos que se cumple para t. Si aplicamos el Teorema 5.5, deducimos que $T_{nP^t,2P^t}$ es irreducible de orden $P^t e$. Notamos ahora que se cumplen las condiciones para aplicar el teorema, es decir, $P \mid P^{t-1}e$, que claramente es cierto, y $P \nmid \frac{2^{nP^{t-1}}-1}{P^{t-1}e}$.

Tenemos por hipótesis que $P \mid e$, sea $a \in \mathbb{N}$ tal que $P^a \parallel e$. Entonces $P^a \mid 2^n - 1$ y como $P \nmid d = \frac{2^n-1}{e}$, $P^a \parallel 2^n - 1$. Usando el lema previo 5.6 tenemos que $P^{a+1} \parallel 2^{nP} - 1$, repitiendo esto llegamos a $P^{a+t-1} \parallel 2^{nP^{t-1}} - 1$. Aplicando esto y que $P^a \parallel e$, es claro que $P \nmid \frac{2^{nP^{t-1}}-1}{P^{t-1}e}$.

El contrarrecíproco es directo al aplicar el lema previo 5.7 con $U = n$ y $V = P^t$. □

Este teorema nos proporciona una motivación para estudiar los trinomios $T_{n,2}$, ver si son irreducibles y calcular sus órdenes e índices. En el artículo [6], los autores hacen estos cálculos y obtienen la tabla 5.3.

N	Índice	Factorización de $2^N - 1$
3	1	7
5	1	31
11	1	$23 \cdot 89$
21	1	$7 \cdot 7 \cdot 127 \cdot 337$
29	1	$233 \cdot 1.103 \cdot 2.089$
35	1	$31 \cdot 71 \cdot 127 \cdot 122.921$

Cuadro 5.3: Tabla de N tal que $x^N + x^2 + 1$ es irreducible

Ejemplo 5.9. Con la tabla 5.3, podemos obtener los posibles P primos tal que se les puede aplicar el Teorema 5.8. Por ejemplo, el trinomio $x^{11} + x^2 + 1$ es irreducible, su índice es 1, y por tanto su orden es $23 \cdot 89$, es decir, todos los polinomios $T_{11 \cdot 23^t, 2 \cdot 23^t}$ son irreducibles.

De esta forma, si buscamos un polinomio irreducible de grado 147, como $147 = 3 \cdot 7^2$ y $T_{3,2}$ es irreducible de orden 7, tenemos que $T_{147,98}$ es un trinomio irreducible de grado 147.

Finalmente, en el artículo [6] se extiende el resultado y se prueba el siguiente teorema, que caracteriza todos los trinomios irreducibles $T_{n,k}$ donde $n \equiv \pm 3 \bmod 8$ a partir de $T_{n,2}$.

Teorema 5.10. *Los únicos trinomios irreducibles $T_{M,K}$ con $M \equiv \pm 3 \bmod 8$ son de la forma $T_{nP,2P}$, donde $P \mid e$, siendo e el orden de $T_{n,2}$ y $P \nmid d$, con d el índice de $T_{n,2}$, y con $n \equiv \pm 3 \bmod 8$.*

5.2. Trinomios primitivos

En esta sección nos centraremos en estudiar los trinomios primitivos, y como razonaremos posteriormente, nos interesará estudiarlos en $\mathbb{F}_2[x]$.

Como los polinomios primitivos de grado n sobre $\mathbb{F}_q[x]$ son aquellos cuyas raíces son elementos primitivos de $\mathbb{F}_{q^n}$, una manera de buscar polinomios primitivos de grado n es considerar los casos donde $q^n - 1$ es un número primo, ya que el orden de las raíces en $\mathbb{F}_{q^n}$ debe dividir a $q^n - 1$, luego todos los polinomios irreducibles de grado n en $\mathbb{F}_q[x]$ serán primitivos.

Veamos ahora en que casos $q^n - 1$ es un número primo.

Teorema 5.11. *Sea q potencia de un primo, $n \in \mathbb{N}$ y supongamos que $q^n - 1$ es primo. Si q es impar entonces $q = 3$ y $n = 1$, si $q = 2$ entonces n es primo, y si $q \neq 2$ es una potencia de 2 entonces $n = 1$. En particular, si $2^n - 1$ es primo, todos los polinomios mónicos irreducibles de grado n en $\mathbb{F}_2[x]$ son primitivos.*

Demostración. Si q es impar, $q - 1$ es par. Como $q - 1 \mid q^n - 1$ tenemos que 2 es un factor de $q^n - 1$ y como $q^n - 1$ es primo, $q^n - 1 = 2$. Si $q > 3$ o $q = 3$, $n > 1$ entonces $q^n - 1 > 2$, luego solo es posible el caso $q = 3$ y $n = 1$.

Si $q = 2$, supongamos que n no es un primo y veamos que llegamos a un absurdo. Sean $m, k \in \mathbb{N}$ tal que $1 < m, k < n$ y $mk = n$, claramente $(2^m - 1)(2^{(k-1)m} + 2^{(k-2)m} + \cdots + 2^m + 1) = 2^n - 1$ luego $2^m - 1 \mid 2^n - 1$ y como $1 < m < n$, tenemos que $2^n - 1$ no es primo. Esto contradice las hipótesis y por tanto llegamos a un absurdo.

Si q es una potencia de 2, $q = 2^r$ con $r > 1$. Entonces tenemos que $q^n - 1 = 2^{nk} - 1$, y usando el caso previo, nk es primo luego $n = 1$. Por tanto el único caso en el que $q^n - 1$ es primo y $n > 1$ es $q = 2$.

Finalmente, si $2^n - 1$ es primo, como los órdenes de elementos en $\mathbb{F}_{2^n}^*$ dividen a $2^n - 1$, los elementos distintos de 0 y 1 son primitivos en $\mathbb{F}_{2^n}$. Entonces si consideramos un polinomio mónico e irreducible de grado n en $\mathbb{F}_2[x]$, por el Corolario 2.4 sus raíces están en $\mathbb{F}_{2^n}$ y entonces son elementos primitivos de $\mathbb{F}_{2^n}$, luego el polinomio es primitivo por definición. □

Como nos muestra este teorema, los polinomios a considerar son los pertenecientes a $\mathbb{F}_2[x]$ y nos interesa el caso $2^p - 1$ donde p es un número primo, lo que motiva la siguiente definición.

Definición 5.12. Si $2^p - 1$ es un número primo, lo llamaremos primo de Mersenne y lo denotaremos por M_p. Al exponente p lo llamaremos exponente de Mersenne.

El proyecto GIMPS [16] se dedica a buscar primos de Mersenne, y es la página que hemos consultado para obtener los exponentes de Mersenne que listamos en la Tabla 5.4. Si vamos a buscar trinomios irreducibles sobre $\mathbb{F}_2[x]$ cuyo grado es un exponente de Mersenne, podemos aplicar primero el Teorema de Swan para simplificar la búsqueda.

Sea $T_{p,s}$ un trinomio tal que p es un exponente de Mersenne, y por tanto primo, y $p \equiv \pm 3 \bmod 8$. Entonces, aplicando el Teorema de Swan 5.1, $T_{p,s}$ solo puede ser irreducible si $s \mid 2p$, y como p es primo solo hay que comprobar el caso $T_{p,2}$, excepto en el caso $p = 3$ que es el único que cumple $p - 1 \mid 2p$, por lo que se puede considerar el trinomio $T_{3,1}$.

En el caso contrario, si p es un exponente de Mersenne tal que $p \equiv \pm 1 \bmod 8$, aplicando el Teorema de Swan 5.1 solo descartamos el caso $T_{p,2}$.

En [2], Richard P. Brent lista todos los exponentes de Mersenne p hasta 74.207.281 junto a los $T_{p,s}$ irreducibles con $s \leq p$, ya que para $s > p$ solo hace falta considerar el recíproco $T_{p,p-s}$ por el Teorema 3.4. Recopilamos estos trinomios irreducibles en la Tabla 5.4, destacando el hecho de que ningún $p \equiv \pm 3 \bmod 8$ mayor que 5 cumple que $T_{p,2}$ es irreducible y 57.885.161 es el único exponente de Mersenne que cumple $57.885.161 \equiv \pm 1 \bmod 8$ y no existe ningún trinomio irreducible de tal grado.

El proyecto GIMPS [16] ha encontrado tres exponentes de Mersenne mayores que 74.207.281, que no aparecen en la lista [2]. De estos tres exponentes, $p_1 =$77.232.917 y $p_2 =$82.589.933 son equivalentes a 5 módulo 8, luego solo hay que estudiar la irreducibilidad de $T_{p_1,2}$ y $T_{p_2,2}$. Una comprobación en MAPLE nos muestra que ambos trinomios son reducibles en $\mathbb{F}_2$.

Otra manera de encontrar trinomios primitivos en $\mathbb{F}_2$ es aplicando el Teorema 2.36. Por ejemplo, si aplicamos el teorema a los trinomios de la forma $T_{k,1} = x^k + x + 1$, $k \geq 2$, tenemos que $T_{k,1}$ es primitivo si y solo si 1 es primitivo en $\mathbb{F}_2$, que se cumple siempre, y el menor $r \in \mathbb{N}$ tal que x^r es congruente a algún elemento de $\mathbb{F}_2$ módulo $x^k + x + 1$ es $r = 2^k - 1$. Claramente, x^r no puede ser

p	s
2	1
3	1
5	2
7	1, 3
17	3, 5, 6
31	3, 6, 7, 13
89	38
127	1, 7, 15, 30, 63
521	32, 48, 158, 168
607	105, 147, 273
1.279	216, 418
2.281	715, 915, 1.029
3.217	67, 576
4.423	271, 369, 370, 649, 1.393, 1.419, 2.098
9.689	84, 471, 1.836, 2.444, 4.187
19.937	881, 7.083, 9.842
23.209	1.530, 6.619, 9.739
44.497	8.575, 21.034
110.503	25.230, 53.719
132.049	7.000, 33.912, 41.469, 52.549, 54.454
756.839	215.747, 267.428, 279.695
859.433	170.340, 288.477
3.021.377	361.604, 1.010.202
6.972.593	3.037.958
24.036.583	8.412.642, 8.785.528
25.964.951	880.890, 4.627.670, 4.830.131, 6.383.880
30.402.457	2.162.059
32.582.657	5.110.722, 5.552.421, 7.545.455
42.643.801	55.981, 3.706.066, 3.896.488, 12.899.278, 20.150.445
43.112.609	3.569.337, 4.463.337, 17.212.521, 21.078.848
74.207.281	9.156.813, 9.999.621, 30.684.570

Cuadro 5.4: Números p, $s \leq p/2$ tal que $T_{p,s}$ es irreducible y p es exponente de Mersenne

congruente a 0 módulo $x^k + x + 1$, luego solo tenemos que calcular el menor r tal que $x^r \equiv 1$ módulo $x^k + x + 1$.

Podemos encontrar trinomios primitivos calculados de esta forma en la enciclopedia online de sucesiones de enteros OEIS [14]. Recordamos que OEIS es una página creada y mantenida por N. J. A. Sloane donde se almacenan miles de sucesiones de interés matemático.

Consultando las sucesiones A002475, A073639 en OEIS [14] vemos los valores de k tal que $T_{k,1}$ es irreducible y primitivo sobre $\mathbb{F}_2$ respectivamente. Listamos únicamente los irreducibles cuya primitividad se ha comprobado, según lo indicado en A073639 y obtenemos lo siguiente.

Grados k tal que $x^k + x + 1$ es irreducible sobre $\mathbb{F}_2$: 2, 3, 4, 6, 7, 9, 15, 22, 28, 30, 46, 60, 63, 127, 153, 172, 303, 471, 532, 865, 900, 1366, 2380, 3310.

Grados k tal que $x^k + x + 1$ es primitivo sobre $\mathbb{F}_2$: 2, 3, 4, 6, 7, 15, 22, 60, 63, 127, 153, 471, 532, 865, 900, 1366.

Hemos verificado la primitividad de los trinomios en MAPLE con la técnica detallada previamente para $2 \leq k \leq 20$ ya que a partir de estos grados empieza a ser computacionalmente pesado.

Podemos hacer lo mismo con los trinomios de la forma $x^k + x^2 + 1$, consultando las sucesiones A057460, A074710 en OEIS [14] para tener los valores de k tal que $T_{k,2}$ es irreducible y primitivo sobre $\mathbb{F}_2$ respectivamente, y listando solo los irreducibles cuya primitividad se ha comprobado, según lo indicado en A074710.

Grados k tal que $x^k + x^2 + 1$ es irreducible sobre $\mathbb{F}_2$: 3, 5, 11, 21, 29, 35, 93, 123, 333, 845.

Grados k tal que $x^k + x^2 + 1$ es primitivo sobre $\mathbb{F}_2$: 3, 5, 11, 21, 29, 35, 93, 123, 333, 845.

Como se puede ver ambas sucesiones coinciden, aunque no parece ser indicativo de una propiedad general. El siguiente término a comprobar sería el 4125.

También hemos verificado la primitividad de estos trinomios en MAPLE para $3 \leq k \leq 20$.

5.3. Pentanomios irreducibles

Como ya hemos visto, usar trinomios para representar cuerpos finitos tiene muchas ventajas, principalmente por solo tener tres coeficientes distintos de cero.

Pero como hemos visto en el Corolario 5.2, para todos los grados que son múltiplos de 8 no tenemos ningún polinomio irreducible, y si no encontramos un trinomio irreducible en $\mathbb{F}_2[x]$ la siguiente opción sería un pentanomio. Es razonable preguntarse si solo usar trinomios o pentanomios es suficiente para encontrar siempre algún polinomio irreducible de cualquier grado o necesitamos expandir la búsqueda a otros polinomios.

En el artículo [13], Gadiel Seroussi lista trinomios o pentanomios irreducibles de la siguiente forma. Para el grado n, si existe algún trinomio irreducible $T_{n,k}$ se escribe en la tabla el trinomio irreducible de menor k, y si no existe, se busca algún pentanomio irreducible de la forma $x^n + x^{j_1} + x^{j_2} + x^{j_3} + 1$ y se escribe en la tabla el de menor orden lexicográfico, es decir, el de menor j_1 y si varios pentanomios irreducibles tienen el mismo j_1 se escribe el de menor j_2 y si coincide j_2 el de menor j_3.

En la Tabla 5.5 mostramos una versión reducida de lo obtenido en el artículo [13], y se puede ver que siempre podemos encontrar algún trinomio o pentanomio irreducible para todos los grados que hemos considerado. Los datos del artículo coinciden con esto, para todo grado $2 \leq n \leq$10.000 siempre se puede encontrar un trinomio o un pentanomio irreducible en $\mathbb{F}_2[x]$, lo que lleva a la siguiente conjetura.

Conjetura 5.13. Para cada $n \in \mathbb{N}$, si no existe ningún trinomio irreducible de grado n en $\mathbb{F}_2[x]$ siempre existe un pentanomio irreducible de grado n en $\mathbb{F}_2[x]$.

También destaca en la Tabla 5.5 que los pentanomios $x^n + x^{j_1} + x^{j_2} + x^{j_3} + 1$ siempre tienen un valor de j_1 bastante bajo, incluso en los grados más altos. De hecho, como se muestra en el artículo [13], el mayor valor de j_1 en la tabla es $j_1 = 56$ para $n =$9.760.

Conclusión

Con esto concluimos este trabajo, en el que hemos cubierto lo que hemos considerado los aspectos principales de los polinomios irreducibles sobre cuerpos finitos, así como sus aplicaciones más actuales.

Esperamos haber ilustrado por qué el estudio de polinomios irreducibles sobre cuerpos finitos es relevante, destacando particularmente la importancia del cuerpo $\mathbb{F}_2$ en la actualidad, y esperamos también haber transmitido al lector el mismo interés en el tema que me ha generado a mí durante estos meses de trabajo.

Grado módulo 8

1	2	3	4	5	6	7	8
	2,1	3,1	4,1	5,2	6,1	7,1	8,4,3,1
9,1	10,3	11,2	12,3	13,4,3,1	14,5	15,1	16,5,3,1
17,3	18,3	19,5,2,1	20,3	21,2	22,1	23,5	24,4,3,1
25,3	26,4,3,1	27,5,2,1	28,1	29,2	30,1	31,3	32,7,3,2
33,10	34,7	35,2	36,9	37,6,4,1	38,6,5,1	39,4	40,5,4,3
41,3	42,7	43,6,4,3	44,5	45,4,3,1	46,1	47,5	48,5,3,2
49,9	50,4,3,2	51,6,3,1	52,3	53,6,2,1	54,9	55,7	56,7,4,2
57,4	58,19	59,7,4,2	60,1	61,5,2,1	62,29	63,1	64,4,3,1
65,18	66,3	67,5,2,1	68,9	69,6,5,2	70,5,3,1	71,6	72,10,9,3
73,25	74,35	75,6,3,1	76,21	77,6,5,2	78,6,5,3	79,9	80,9,4,2
81,4	82,8,3,1	83,7,4,2	84,5	85,8,2,1	86,21	87,13	88,7,6,2
89,38	90,27	91,8,5,1	92,21	93,2	94,21	95,11	96,10,9,6
97,6	98,11	99,6,3,1	100,15	101,7,6,1	102,29	103,9	104,4,3,1
9.905,219	9.906,2.027	9.907,10,7,1	9.908,2.699	9.909,11,10,7	9.910,27,16,15	9.911,483	9.912,42,35,15
9.913,1.899	9.914,95	9.915,29,17,8	9.916,4.483	9.917,32,9,6	9.918,381	9.919,1.185	9.920,49,18,14
9.921,901	9.922,2.691	9.923,37,33,26	9.924,30,29,26	9.925,12,9,7	9.926,1.445	9.927,1.987	9.928,39,38,31
9.929,1382	9.930,331	9.931,34,10,3	9.932,2.397	9.933,23,6,2	9.934,34,7,3	9.935,2.216	9.936,22,21,1
9.937,451	9.938,25,19,9	9.939,32,26,17	9.940,2.059	9.941,29,12,10	9.942,133	9.943,3.069	9.944,15,14,6
9.945,1.882	9.946,2.355	9.947,23,17,8	9.948,1.535	9.949,32,24,10	9.950,2.453	9.951,1.334	9.952,31,30,11
9.953,539	9.954,343	9.955,9,8,5	9.956,851	9.957,25,11,4	9.958,17,14,4	9.959,381	9.960,30,15,10
9.961,2.707	9.962,20,14,3	9.963,34,29,20	9.964,2.691	9.965,34,24,23	9.966,1.701	9.967,4.399	9.968,36,3,2
9.969,295	9.970,2.587	9.971,11,8,5	9.972,519	9.973,27,24,12	9.974,2.045	9.975,124	9.976,21,19,5
9.977,2.954	9.978,1.483	9.979,26,10,2	9.980,707	9.981,30,27,22	9.982,993	9.983,785	9.984,27,10,7
9.985,1.974	9.986,1.143	9.987,14,11,10	9.988,3.129	9.989,21,20,6	9.990,573	9.991,495	9.992,7,4,2
9.993,121	9.994,29,22,3	9.995,41,40,31	9.996,1.447	9.997,26,10,6	9.998,4.013	9.999,2.951	10.000,19,13,9

Cuadro 5.5: Pares n, k asociados al trinomio irreducible $x^n + x^k + 1$ o 4-uplas n, j_1, j_2, j_3 asociadas al pentanomio irreducible $x^n + x^{j_1} + x^{j_2} + x^{j_3} + 1$ seleccionando para cada grado el menor trinomio y, si no existe, el menor pentanomio según el orden lexicográfico.

Bibliografía

[1] I.F. Blake, S. Gao and R.J. Lambert. *Construction and distribution problems for irreducible trinomials over finite fields*, Applications of finite fields, 19-32, Inst. Math. Appl. Conf. Ser. New Ser., 59, Oxford Univ. Press, New York, 1996.

[2] R. P. Brent. *Search for primitive trinomials (mod 2)*, `https://maths-people.anu.edu.au/~brent/ftp/trinom/table.txt`, 2008.

[3] M. C. R. Butler. *The irreducible factors of $f(x^m)$ over a finite field*, Journal of the London Mathematical Society 30, 480-482, 1955.

[4] A. Cilardo. *Efficient Bit-Parallel $GF(2^m)$ Multiplier for a Large Class of Irreducible Pentanomials*, IEEE Transactions on computers 58 No. 7, 1001-1008, 2009.

[5] S. D. Cohen. *The explicit construction of irreducible polynomials over finite fields*, Designs, Codes and Cryptography 2, 169-174, 1992.

[6] H. Fredricksen and 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.

[7] D.W. Hardy, F. Richman and C.L. Walker. *Applied algebra. Codes, ciphers and discrete algorithms*, CRC Press Taylor & Francis Group (2nd ed.), 2009.

[8] J. L. Imaña. *LFSR-Based Bit-Serial $GF(2^m)$ Multipliers Using Irreducible Trinomials*, IEEE Transactions on computers 70 No. 1, 156-162, 2021.

[9] Y. Li, H. Wang and J. Zhao. *On the Primitivity of some Trinomials over Finite Fields*, Cryptology ePrint Archive, Paper 2013/252, `https://eprint.iacr.org/2013/252`, 2013.

[10] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications*, Cambridge University Press (Revised ed.), 2000.

[11] R. Lidl and G. Pilz. *Applied Abstract Algebra*, Springer-Verlag, 1998.

[12] H. Meyn. *On the construction of irreducible self-reciprocal polynomials over finite fields*, Applicable Algebra in Engineering, Communication and Computing 1, 43-53, 1990.

[13] G. Seroussi. *Table of low-weight binary irreducible polynomials*, `https://api.semanticscholar.org/CorpusID:18027797`, 1962.

[14] N. J. A. Sloane. *The on-line encyclopedia of integer sequences*, `https://oeis.org`, 1964.

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

[16] *The Great Internet Mersenne Prime Search*, `https://www.mersenne.org/`.

[17] Z-X. Wan. *Finite fields and Galois rings*, World Scientific, 2012.

[18] J. H. M. Wedderburn. *A theorem on finite algebras*, Transactions of the American Mathematical Society 6, 349-352, 1905.

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