FACULTAD
DE
CIENCIAS

POLINOMIOS IRREDUCIBLES SOBRE CUERPOS FINITOS

(IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS)

Trabajo de fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autora: María Sanz Ruiz

Director: Daniel Sadornil Renedo

Junio-2021

Resumen

Es bien sabido que cualquier cuerpo finito tiene p^n elementos con p un número primo y n un entero positivo. Recíprocamente, para cada primo p y cada entero positivo n existe un único cuerpo finito (salvo isomorfismo) con p^n elementos, $\mathbb{F}_{p^n}$.

La construcción de $\mathbb{F}_{p^n}$ se realiza como extensión del cuerpo primo $\mathbb{F}_p$ a partir de un polinomio irreducible de grado n; esto es: $\mathbb{F}_{p^n}$ es isomorfo al cuerpo $\mathbb{F}_p[x]/(f(x))$ con f un polinomio irreducible sobre $\mathbb{F}_p$ de grado n. Por la unicidad del cuerpo finito, éste también puede construirse a partir de $\mathbb{F}_{p^r}$ con r un divisor de n, utilizando un polinomio irreducible sobre $\mathbb{F}_{p^r}$ de grado $\frac{n}{r}$.

En este trabajo de fin de grado se pretende estudiar para un cuerpo finito $\mathbb{F}_q$, $q = p^r$, cómo construir un polinomio irreducible de grado dado que permita dar una construcción efectiva de cualquier cuerpo finito. Asimismo, se determinará el número de polinomios irreducibles existentes sobre un cuerpo finito de grado dado, así como la cantidad de polinomios irreducibles con ciertas características.

Palabras clave: cuerpos finitos, polinomios irreducibles, polinomios invariantes

Abstract

It is well known that any finite field has p^n elements, where p is a prime number and n a positive integer. Reciprocally, for every prime number p and every positive integer n there exists a unique up to isomorphism finite field with p^n elements: $\mathbb{F}_{p^n}$.

The field $\mathbb{F}_{p^n}$ is defined as an extension of the prime field $\mathbb{F}_p$ from an irreducible polynomial of degree n: this is, $\mathbb{F}_{p^n}$ is isomorphic to the field $\mathbb{F}_p[x]/(f(x))$ where $f \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree n. Since every finite field is unique, it can also be constructed from $\mathbb{F}_{p^r}$ where r divides n using an irreducible polynomial of degree $\frac{n}{r}$ over $\mathbb{F}_{p^r}$.

This work aims to study, for a finite field $\mathbb{F}_q$ with $q = p^n$, how to build an irreducible polynomial of a fixed degree that enables the effective construction of any finite field. In addition, this work will determine the number of irreducible polynomials of a fixed degree over a finite field, and the number of irreducible polynomials with determined characteristics.

Keywords: finite fields, irreducible polynomials, invariant polynomials

Agradecimientos

Hace tiempo, cuando yo era demasiado tímida para mi propio bien, mi abuela me dijo que consultase todas las dudas a los profesores, por muy triviales que parecieran. Tal y como me lo explicó ella, más vale preguntar y quedar como una tonta una vez, que callarse y seguir siendo tonta siempre. La primera parte de estos agradecimientos va dedicada al director de este trabajo: Dani. No sólo has respondido a todas y cada una de mis dudas tontas, sino que siempre lo has hecho con una sonrisa. Asimismo, gracias por tu preocupación constante y por tu exhaustiva minuciosidad: este Trabajo de Fin de Grado no sería una realidad sin ellas.

La segunda parte de estos agradecimientos es para mis padres. Gracias por vuestra paciencia infinita y por vuestra fe inquebrantable en mí. Son los mejores regalos que podíais hacerme y estoy segura de que me acompañarán siempre.

Por último, la sección final de estos agradecimientos está dedicada a todos los demás amigos y familiares que me habéis acompañado durante todo este tiempo y que siempre seguiréis a mi lado. No habría podido llegar aquí sin vosotros, que comprendéis la vida y os burláis de los números.

Gracias.

Índice general

Introducción

La teoría de los cuerpos finitos es una rama del álgebra que comienza a surgir en torno al siglo XVII gracias a las contribuciones de importantes precursores como Pierre de Fermat (1601-1665), Leonhard Euler (1707-1783), Joseph-Louis Lagrange (1736-1813) y Adrien-Marie Legendre (1752-1833).

Es a partir del siglo XIX cuando se empiezan a formalizar muchos de los conceptos propios de este ámbito. En 1801, Carl Friedrich Gauss (1777-1855) publicó su obra *Disquisitiones arithmeticae*, en la que se habla de congruencias, ecuaciones polinómicas sobre cuerpos finitos o la función de Euler; contenidos esenciales a la hora de trabajar con cuerpos finitos. Más tarde, en 1830, Évariste Galois (1811-1832) publicó su texto *Sur la théorie des nombres*, que constutuye la base de lo que hoy se conoce como Teoría de Galois. Este texto supuso una revolución en el estudio de los cuerpos finitos.

A lo largo del siglo XIX varios autores trabajaron en el tema: entre ellos son destacables Joseph Alfred Serret (1819-1885), Theodor Schönemann (1812-1868) y Richard Dedekind (1831-1916), que continuaron desarrollando las ideas de Gauss y Galois y estudiando polinomios sobre cuerpos finitos. Más tarde autores como Camille Jordan (1838-1922), Eliakim Hastings Moore (1862-1932) o Leonard Eugene Dickson (1874-1954) contribuyeron a formalizar estas ideas y presentarlas de manera más abstracta.

El estudio de los cuerpos finitos tiene una gran cantidad de aplicaciones. Es especialmente destacable su uso en códigos: los cuerpos finitos son la base de los códigos lineales detectores-correctores de errores que, como su propio nombre indica, permiten detectar y corregir errores que se producen durante la transmisión de información. Un ejemplo de esto es el código de Reed-Solomon.

La criptografía es un ámbito en el que los cuerpos finitos juegan un papel muy importante. Los sistemas de cifrado de datos se dividen en varios tipos: de llave privada, o de llave pública. Actualmente varios sistemas de cifrado de llave privada se basan en estructuras algebraicas relacionadas con cuerpos finitos: en concreto algunos de ellos son el Advanced Encryption Standard (AES), el Twofish o el Secure And Fast Encryption Routine (SAFER). Asimismo, hay varios sistemas de cifrado de llave pública basados en curvas elípticas; los polinomios que definen a dichas curvas son elementos de $\mathbb{F}_q[x, y]$ para algún q potencia de primo. Las principales aplicaciones de la criptografía incuyen la banca electrónica, firma digital, o tarjetas inteligentes.

De hecho, los cuerpos finitos son de gran utilidad en el área de la geometría algebraica, a través de la cual se pueden definir códigos y curvas algebraicas, cuyo uso se acaba de exponer. Otro campo de estudio relevante es el de las sucesiones sobre cuerpos finitos, por ejemplo para su

uso en cifrados de clave privada, es es un aspecto que ha cobrado gran relevancia debido al desarrollo de las comunicaciones digitales, y que tiene aplicaciones en sistemas GPS o de transmisión de televisión.

Es así evidente que el estudio de los cuerpos finitos es de gran importancia y que, a su vez, el estudio de la teoría de Galois es fundamental para comprenderlos. Por este motivo, parte del primer capítulo de este trabajo se dedica a dar una pequeña introducción sobre este tema. En el apartado de Preliminares también se habla de conceptos como la traza de un elemento, el orden de un polinomio y ciertas funciones destacadas. Las nociones que se introducen son esenciales para la comprensión del documento, así como para su autocontención.

Se han mencionado anteriormente las diversas aplicaciones de los cuerpos finitos: se hace evidente entonces la necesidad de construirlos. Como se expondrá a lo largo del presente documento, el problema de la construcción de cuerpos finitos está intrínsecamente ligado al de la obtención de polinomios irreducibles sobre los mismos: en el segundo capítulo de este trabajo se presenta un método para la construcción de polinomios irreducibles de cierto grado sobre un cuerpo finito. Esto permitirá obtener una extensión de dicho cuerpo.

Para concluir, una vez que se ha comprobado de manera constructiva la existencia de polinomios irreducibles de cualquier grado sobre un cuerpo finito, en el último capítulo de este documento se presentan varios resultados enfocados a contar cuántos hay. Además de tratar el caso generalizado, se estudiará el número de polinomios irreducibles con varias características predeterminadas.

Capítulo 1

Preliminares

1.1. Teoría de Galois

Se comienza haciendo un repaso de conceptos vistos en la asignatura "Teoría de Galois". En esta sección se estudiarán definiciones básicas que se manejarán a lo largo del resto del documento, como las de polinomio irreducible, extensión de cuerpos, o cuerpo de escisión. Estos conceptos y resultados han sido tomados de la referencia [6].

Definición 1.1 *Sea f un polinomio con coeficientes en un dominio de factorización única. Se dice que f es* ***mónico*** *si el coeficiente asociado a su término de mayor grado es 1. Es* ***primitivo*** *si el máximo común divisor de sus coeficientes es 1. Dos polinomios f y g son* ***asociados*** *si existe una unidad u tal que $f(x) = ug(x)$. Finalmente, f es* ***irreducible*** *si sólo se puede descomponer en productos de unidades y un polinomio asociado a él.*

Los polinomios irreducibles, como se verá más tarde, están estrechamente relacionados con las extensiones de cuerpos, cuya definición se da a continuación.

Definición 1.2 *Un cuerpo F es una* ***extensión*** *de otro cuerpo K si K es un subcuerpo de F. Se representa: $K \hookrightarrow F$. En ese caso, F es un K-espacio vectorial. El* ***grado de la extensión*** *es la dimensión de F como K-espacio vectorial, y se representa por $[F : K]$. Si es finito, se dice que la extensión es finita.*

Definición 1.3 *Sea $Y \subseteq F, K \subseteq F$. El* ***subcuerpo de F generado por Y sobre K*** *se representa por $K[Y]$. Si $Y = \{u_1, ...u_r\}$, entonces $K(u_1, ...u_r)$ es una extensión de K* ***finitamente generada.***

El hecho de que una extensión sea finitamente generada no implica que sea finita, pero toda extensión finita sí es finitamente generada.

Definición 1.4 *Sea $K \hookrightarrow F$ una extensión, u un elemento de F; u es* ***algebraico*** *si es raíz de algún polinomio no nulo en K.*

Un polinomio que cobra especial relevancia en este ámbito es el polinomio mínimo de un elemento. La siguiente definición ofrece una explicación acerca de la importancia de los polinomios irreducibles como herramienta para generar extensiones de cuerpos.

Definición 1.5 *Sea $K \hookrightarrow F$ una extensión, $u \in F$ un elemento algebraico sobre K.*

i) *$K(u)$ es isomorfo a $K[x]/(f(x))$, con $f(x)$ irreducible, mónico y $f(u) = 0$.*

ii) *$\{1, u...u^{n-1}\}$ es base de $K(u)$ como K-espacio vectorial, y el grado de la extensión $[K(u) : K] = n$.*

El polinomio f que cumple estas características es el ***polinomio mínimo*** *de u sobre K.*

Si f es un polinomio cualquiera sobre un cuerpo K, sus raíces no serán necesariamente elementos del mismo cuerpo, pero sí de otro que lo contiene. Ese cuerpo es justamente el cuerpo de escisión:

Definición 1.6 *Un polinomio* ***escinde*** *en F si todas sus raíces son elementos de F. Un cuerpo F es* ***cuerpo de escisión*** *de $f \in K[x]$ si:*

i) *f escinde en F.*

ii) *$F = K(u_1...u_r)$, siendo $u_1...u_r$ las raíces de f.*

Se deduce de esta definición que el cuerpo de escisión de un polinomio es único.

Definición 1.7 *Un polinomio irreducible $f \in K[x]$ es un* ***polinomio separable*** *si en algún cuerpo de escisión F de f sobre K todas sus raíces son simples. Un elemento u algebraico sobre K es un* ***elemento separable*** *si lo es el polinomio mínimo de u sobre K. Una extensión algebraica $K \hookrightarrow F$ es una* ***extensión separable*** *si todo elemento de F es separable sobre K.*

Definición 1.8 *Se dice que $K \hookrightarrow F$ es una* ***extensión normal*** *si todo polinomio irreducible en $K[x]$ que tiene una raíz en F, escinde en F.*

1.2. Cuerpos finitos

Como en particular se van a estudiar los cuerpos finitos se presentan los contenidos básicos relativos a este ámbito, y se añaden demostraciones para que el trabajo sea autocontenido. Aun así, se puede encontrar más información relacionada con el contenido de esta sección en las referencias de las que ha sido tomada, [6], [10] y [13].

Claramente, un cuerpo finito debe constar de un número finito de elementos. Sin embargo dicho número no puede ser cualquiera: el resultado siguiente muestra exactamente cuál es el número de elementos de un cuerpo finito.

Teorema 1.9 (Cardinal de un cuerpo finito) *Si F es un cuerpo finito, su cardinal es p^m para algún $m \geq 1$ entero.*

Demostración: Es bien sabido que, si F es un cuerpo, su característica será 0 ó p con p primo. En este caso, como F además es finito, $char(F) = p$. Sea $\pi(F)$ el cuerpo primo de F (es decir,

la intersección de todos los subcuerpos de F). El grado de la extensión $[F : \pi(F)] = m$ es necesariamente finito, y por tanto el cardinal de F es p^m. □

Recíprocamente, dados un primo p y un entero m cualesquiera siempre es posible construir un cuerpo de p^m elementos:

Teorema 1.10 (Unicidad de cuerpos finitos) *Dados un primo p y un entero positivo m, existe un único cuerpo (salvo isomorfismo) con p^m elementos.*

Demostración: Se considera el polinomio $p(X) = X^{p^m} - X \in \mathbb{F}_p$. Sea F su cuerpo de escisión sobre $\mathbb{F}_p$. Dado que $p'(X) = p^m X^{p^m-1} = -1$ en el cuerpo F_p, el polinomio $p(X)$ no tiene raíces múltiples; su grado es p^n y tendrá por tanto ese número de raíces distintas.
A continuación se comprueba que el conjunto A de raíces de ese polinomio es un cuerpo:

i) $0, 1 \in A$ trivial.

ii) Sean $a, b \in A$: $(a-b)^{p^n} - (a-b) = a^{p^m} - b^{p^m} - a + b = (a^{p^m} - a) - (b^{p^m} - b) = 0$ y por tanto, al ser $a - b$ raíz del polinomio, $a - b \in A$.

iii) Del mismo modo, $(ab^{-1})^{p^m} - (ab^{-1}) = a^{p^m} b^{-p^m} - ab^{-1} = ab^{-1} - ab^{-1} = 0$ y entonces $ab^{-1} \in A$.

Es decir: A cumple por tanto lo necesario para ser un cuerpo, y tiene p^m elementos: queda probada la existencia. Además, A es cuerpo de escisión del polinomio, y como el cuerpo de escisión es único, queda probada la unicidad. □

Durante el resto del documento, se denotará al único cuerpo con p^n elementos como $\mathbb{F}_{p^n}$, y siempre que se escriba $\mathbb{F}_q$ se asumirá que $q = p^n$ es una potencia de primo.

El resultado que se presenta a continuación también está relacionado con la cardinal de los cuerpos: en concreto, describe lo que ocurre cuando un cuerpo contiene a otro.

Teorema 1.11 *Sean F y K dos cuerpos finitos. Si $F \subset K$, entonces $|F|$ divide a $|K|$.*

Demostración: Como F es un cuerpo finito, tiene p^n elementos (p es primo, n entero). Entonces $\mathbb{F}_p \subseteq \mathbb{F}_{p^n} \subseteq K$, y el cuerpo primo de K es también $\mathbb{F}_p$. Por tanto K será una extensión de grado m de $\mathbb{F}_p$: $K = \mathbb{F}_{p^m}$.
Entonces, $m = [\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}][\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}]n$, y por tanto, como n divide a m, p^n divide a p^m. □

Por tanto, cualquier cuerpo finito de cardinal p^n es una extensión de grado n de $\mathbb{F}_p$, y puede generarse a partir de un polinomio irreducible de grado n sobre $\mathbb{F}_p$.

Lema 1.12 *Sean $q = p^r$ para algún primo p, $n \in \mathbb{N}$.*

i) Para todo $a \in \mathbb{F}_{q^n}$ existe un único polinomio mónico irreducible $f \in \mathbb{F}_q[x]$ tal que a es raíz de f y el grado de f, $\delta(f)$ divide a n: el polinomio mínimo de a. Recíprocamente, para todo $f \in \mathbb{F}_q[x]$ mónico, irreducible, de forma que $\delta(f)$ divide a n, f es separable, y tiene todos sus ceros en $\mathbb{F}_{q^n}$.

ii) Si $m(x)$ es el polinomio mínimo de a sobre $\mathbb{F}_q$, $m(x)$ divide a todo $f(x) \in \mathbb{F}_q[x]$ con $f(a) = 0$.

iii) Si d es el menor entero positivo tal que $a^{q^d} = a \in \mathbb{F}_{q^n}$, d divide a n y es el grado del polinomio mínimo de a, $m(x)$. De hecho,

$$m(x) = (x-a)(x-a^q)(x-a^{q^2})...(x-a^{q^{d-1}})$$

Demostración:

i) Sea $a \in \mathbb{F}_{q^n}$. La extensión $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^n}$ es finita: por tanto, a es un elemento algebraico de $\mathbb{F}_q$. Tomamos $f \in \mathbb{F}_q[X]$ el polinomio mínimo de a; f es entonces mónico, irreducible, y a es raíz suya. Además, $\mathbb{F}_q \hookrightarrow \mathbb{F}_q(a) \hookrightarrow \mathbb{F}_{q^n}$, y por tanto $deg(f) = [\mathbb{F}_q(a) : \mathbb{F}_q]$ divide a $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. Sea ahora $f \in \mathbb{F}_q[X]$ mónico, irreducible, tal que $\delta(f)$ divide a n. El cardinal de $\mathbb{F}_q[X]/(f)$ es $q^{\delta(f)}$, y por tanto $\mathbb{F}_q[X]/(f)$ es isomorfo a $\mathbb{F}_{q^{\delta(f)}}$. Dado que $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^{\delta(f)}}$ es una extensión finita de un cuerpo finito, es de Galois; entonces el polinomio f tiene todas sus raíces distintas y factoriza completamente en $\mathbb{F}_{q^{\delta(f)}}$. Pero, como $\delta(f)$ divide a n, $\mathbb{F}_{q^{\delta(f)}} \subset \mathbb{F}_{q^n}$ y las raíces de f están en $\mathbb{F}_{q^n}$.

ii) Si $f(a) = q(a)m(a) + r(a)$ con $\delta(r) < \delta(m)$, necesariamente $r \equiv 0$ para que se cumpla que $r(a) = 0$ y m sea el poliomio mínimo.

iii) Claramente, $a^{q^n} = a$. Si se divide entre el d definido anteriormente, $n = ld + r$ con $l, r \in \mathbb{Z}$, $0 \leq l$ y $0 \leq r < d$. Entonces $a = a^{q^n} = a^{q^{ld+r}} = (a^{q^{ld}})^{q^r} = a^{q^r}$; para que esto se cumpla con $r < d$, r tiene que ser 0 y por lo tanto d divide a n.
Está claro que $a^{q^i} \neq a^{q^j}$ para $1 \leq i, j < d$; si hubiera dos iguales, con $i > j$, entonces $a^{q^{i-j}} = (a^{q^i})^{q^{-j}} = (a^{q^j})^{q^{-j}} = a^{q^0} = a$; como d es el menor entero para el que $a^{q^d} = a$, entonces necesariamente $i = j$. Sea ahora el polinomio $m_1(x) = (x-a)(x-a^q)(x-a^{a^2})...(x-a^{q^{d-1}})$; claramente, a es una raíz suya, y el apartado anterior permite asegurar que el polinomio mínimo m divide a m_1. Además, los elementos $a^q, a^{q^2}...a^{q^{d-1}}$ también son raíces de m, y por lo tanto $\delta(m) \geq d$; pero, como divide a m_1 cuyo grado es d, necesariamente han de ser iguales. □

Estos resultados muestran que cualquier cuerpo finito de cardinal p^n será una extensión de grado n de $\mathbb{F}_p$, y podrá generarse a partir de un polinomio irreducible de grado n sobre $\mathbb{F}_p$.
Además, si n no es primo (por ejemplo, $n = n_1 n_2...$), también será posible generar $\mathbb{F}_{p^n}$ a partir de un polinomio de grado n_1 sobre $\mathbb{F}_{p^{n_2}}$, o viceversa...

1.3. Traza

Se introduce ahora el concepto de traza de un elemento de $\mathbb{F}_q$, y se se relaciona con el de la traza de un polinomio. El objetivo de esta sección es ofrecer una colección de resultados y observaciones que permitan al lector entender de forma más clara resultados posteriores en los que se mencionan estos temas. Se puede encontrar más información sobre trazas en la sección 2.3 de la referencia [10].

Dados n y q naturales, q potencia de primo, se considera la extensión de cuerpos $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^n}$. Entonces $\mathbb{F}_{q^n}$ se puede ver como un espacio vectorial de dimensión n sobre el cuerpo $\mathbb{F}_q$. Se presenta la traza como una aplicación de $\mathbb{F}_{q^n}$ en $\mathbb{F}_q$.

Definición 1.13 *Sea α un elemento de $\mathbb{F}_{q^n}$. La **traza** de α se define como:*

$$Tr(\alpha) = \alpha + \alpha^q + ... + \alpha^{q^{n-1}}$$

*Si además $q = p$ primo, se dice que $Tr(\alpha)$ es la **traza absoluta** de α.*

Aunque la notación generalmente será la de $Tr(\alpha)$, se denotará $Tr_{F,K}(\alpha) = Tr(\alpha)$ donde $F = \mathbb{F}_{q^n}$ y $K = \mathbb{F}_q$ cuando pueda existir confusión acerca de los cuerpos en los que se está trabajando.

Observación 1.14 *Se considera $f \in \mathbb{F}_q[x]$ el polinomio mínimo de α, de grado d sobre $\mathbb{F}_q$, y la extensión $\mathbb{F}_q \hookrightarrow \mathbb{F}_q(\alpha) \hookrightarrow \mathbb{F}_{q^n}$: al estudiar el grado de las extensiones se hace evidente que el grado de f, $\delta(f) = d$ divide a n. El polinomio característico de α es justamente $g = f^{\frac{n}{d}}$, que es un elemento de $\mathbb{F}_q[x]$, y cuyas raíces son $\{\alpha, \alpha^q ... \alpha^{q^{n-1}}\}$. Si se expresa $g(x) = x^n + a_{m-1}x^{n-1} + ... + a_0$, al utilizar las fórmulas de Cardano-Vieta se obtiene que la traza de α es justamente $Tr(\alpha) = -a_{n-1}$, y es un elemento de $\mathbb{F}_q$. Por tanto, si el polinomio mínimo de α, f, es exactamente de grado n, entonces la traza de α es precisamente la suma de todas las raíces de f; o, equivalentemente, la suma de todos los conjugados de α.*

A continuación se estudian algunas propiedades de la traza, cuya utilidad se pondrá de manifiesto en demostraciones de resultados acerca del número de polinomios mónicos e irreducibles con una traza determinada del capítulo 3 de este trabajo.

Proposición 1.15 *Se consideran los cuerpos $\mathbb{F}_q$ y $\mathbb{F}_{q^n}$. Se satisfacen las siguientes propiedades:*

i) $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$ *para todos los elementos α y $\beta \in \mathbb{F}_{q^n}$.*

ii) $Tr(c\alpha) = cTr(\alpha)$ *para todo $c \in \mathbb{F}_q$.*

iii) $Tr(\alpha) = n\alpha$ *si $\alpha \in \mathbb{F}_q$*

iv) $Tr(\alpha^q) = Tr(\alpha)$ *para todo $\alpha \in \mathbb{F}_{q^n}$*

Demostración:

i) Como la traza de $\alpha+\beta$ es un elemento de $\mathbb{F}_q$, $Tr(\alpha+\beta) = \alpha+\beta+(\alpha+\beta)^q+...+(\alpha+\beta)^{q^{n-1}} = \alpha + \beta + \alpha^q + \beta^q + ... + \alpha^{q^{n-1}} + \beta^{q^{n-1}}$ de lo que se obtiene el resultado deseado.

ii) Dado que c es un elemento de $\mathbb{F}_q$, $c^q = c$ (basta con considerar el orden de c en el grupo cíclico $\mathbb{F}_q^*$), y entonces: $Tr(c\alpha) = c\alpha + c^q\alpha^q + ... + c^{q^{n-1}}\alpha^{q^{n-1}} = c\alpha + c\alpha^q + ... + c\alpha^{q^{n-1}}$ como se quería ver.

iii) Para probar este resultado se considera una vez más el hecho de que, como α es un elemento de $\mathbb{F}_q$, entonces $\alpha^q = \alpha$. Al sustituir en la fórmula de la traza dada por la definición, se obtiene la suma de α n veces, que es lo que se quiere probar.

iv) Siguiendo un razonamiento parecido a los anteriores, en esta ocasión se tiene que $\alpha^{q^n} = \alpha$. Entonces: $Tr(\alpha^q) = \alpha^q + \alpha^{q^2} + ... + \alpha^{q^n} = Tr(\alpha)$ □

Es necesario tener en cuenta que la traza está definida teniendo en cuenta los cuerpos $\mathbb{F}_q$ y $\mathbb{F}_{q^n}$, y que su significado varía en base a considerar α como elemento de un cuerpo distinto. Con el objetivo de estudiar cómo se produce dicho cambio se tiene el siguiente resultado:

Teorema 1.16 (Transitividad de la traza) *Sea la extensión de cuerpos $K \hookrightarrow F \hookrightarrow E$, con $K = \mathbb{F}_q$.*

$$Tr_{E,K}(\alpha) = Tr_{F,K}(Tr_{E,F}(\alpha))$$

para todo α elemento de E.

Demostración: Se supone que las extensiones $K \hookrightarrow F$ y $F \hookrightarrow E$ tienen grados m y n, respectivamente.
Basta con desarrollar la fórmula dada por la deficinión:

$$\begin{aligned} Tr_{F,K}(Tr_{E,F}(\alpha)) &= \sum_{i=0}^{m-1} Tr_{E,F}(\alpha)^{q^i} = \sum_{i=0}^{m-1}(\sum_{j=0}^{n-1}\alpha^{q^{jm}})^{q^i} = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\alpha^{q^{jm+i}} = \sum_{k=0}^{mn-1}\alpha^{q^k} \\ &= Tr_{E,K}(\alpha) \end{aligned}$$

□

1.4. Orden de polinomios

Por último, se estudia el orden de un polinomio. Los resultados y definiciones que se presentan a continuación pueden ser encontrados en [6] y en el capítulo 2 de [10].

Para introducir esta sección se estudian los siguientes polinomios: $f(x) = x^3 + x + 1$ sobre $\mathbb{F}_2$ y $g(x) = x^2 + 2x + 1$ sobre $\mathbb{F}_3$. Es de inmediata comprobación que f divide a $x^7 - 1$. En el caso de g, se comprueba que g divide a $x^6 - 1$. Cabe entonces preguntarse si para todo polinomio sobre un cuerpo finito existe un entero e tal que dicho polinomio divide a $x^e - 1$. A continuación se comprueba que así es:

Proposición 1.17 *Sea $f \in \mathbb{F}_q[x]$ un polinomio no constante de grado n tal que $f(0) \neq 0$. Existe un entero positivo e tal que $e \leq q^n - 1$ y f divide a $x^e - 1$.*

Demostración: Como f tiene grado n, el anillo $\mathbb{F}_q[x]/(f)$ tiene q^n clases (contando el cero, que sería la clase de los múltiplos de f).

Las clases $x^j + (f)$ donde $j = 0...q^m - 1$ son todas distintas de $0 + (f)$, y hay q^m; utilizando el principio del Palomar (o del sentido común, porque en este caso se ve trivial) se sigue que debe haber dos iguales: es decir, existen $0 \leq r < s \leq q^m - 1$ con $x^s \equiv x^r$ mód (f).

Además, como $f(0)$ no es 0, $mcd(x, f) = 1$, y $x^{s-r} \equiv 1$ mód (f) y por lo tanto f divide a $x^{s-r} - 1$: entonces $e = s - r$ es justamente el entero que se busca. □

Por tanto, es posible dar la definición del orden de un polinomio:

Definición 1.18 *Sea $f \in \mathbb{F}_q[x]$ un polinomio no constante de grado n tal que $f(0) \neq 0$. El menor entero positivo e tal que f divide a $x^e - 1$ es el* ***orden*** *de f.*
Si $f(0) = 0$, entonces $f(x) = x^k g(x)$ con $g(0) \neq 0$, y se considera $ord(f) := ord(g)$.

Se utilizará a veces la notación $ord_m(a)$ para hablar del orden de la clase del elemento a en el grupo $(\mathbb{Z}/m\mathbb{Z})^*$.

A continuación se presenta una relación entre el orden de un polinomio y el de sus raíces. Dicha relación funciona a su vez a modo de caracterización del concepto:

Teorema 1.19 *Sea $f \in \mathbb{F}_q[x]$ un polinomio no constante de grado n tal que $f(0) \neq 0$. El orden de f es igual al de cualquiera de sus raíces en $\mathbb{F}_{q^n}^*$*

Demostración: Como el grado de f es n, su cuerpo de escisión es $\mathbb{F}_{q^n}$. Las raíces de f tienen todas el mismo orden: si α es una raíz de f, entonces el conjnto de raíces de f es $\{\alpha, \alpha^q, \alpha^{q^2}...\alpha^{q^{n-1}}\}$: supóngase que el orden de α es e: es decir, e es el menor entero con $\alpha^e = 1$. Sea ahora $i = 2...n-1$: $(\alpha^{q^i})^e = (\alpha^e)^{q^i} = 1$. Además esto no se cumple para ningún entero menor que e.

Para cualquier raíz α de f, $\alpha^e = 1$ si y sólo si es también raíz de $x^e - 1$; esto a su vez se cumple para toda raíz α si y sólo si el polinomio f divide a $x^e - 1$, y e es el mínimo entero que cumple estas dos cosas. □

Para concluir esta sección se estudian brevemente los polinomios ciclotómicos y su relación con el orden.

Definición 1.20 *El* ***polinomio ciclotómico de orden n*** *es aquel cuyas raíces son las raíces n-ésimas de la unidad (es decir, los ξ que verifican $\xi^n = 1$). Tiene la siguiente expresión:*

$$\phi_n(x) = \prod_{0 \leq d < n, mcd(d,n)=1} (x - \xi^d)$$

Y su grado es $\varphi(n)$

El siguiente resultado proporciona una factorización del polinomio ciclotómico de orden r como producto de polinomios del mismo orden. Su gran relevancia se pondrá de manifiesto en varias demostraciones distintas a lo largo del documento, y por ese motivo aparece incluido en esta sección.

Teorema 1.21 *Sea $K := \mathbb{F}_q$ y $F := K(\zeta_r)$, donde ζ_r es una raíz del polinomio ciclotómico de orden r, ϕ_r. Entonces,*

i) El grado de la extensión $[F : K] = d$ coincide con el orden de q en el grupo de las unidades de $\mathbb{Z}/r\mathbb{Z}$

ii) ϕ_r factoriza en $\mathbb{F}_q[x]$ como el producto de $\frac{\varphi(r)}{d}$ polinomios mónicos e irreducibles de grado d.

Demostración:

i) Si ζ es una raíz primitiva r-ésima de la unidad, $\zeta^{q^d} = \zeta$, de lo que se deduce que r divide a $q^d - 1$, y por tanto que $q^d \equiv 1$ mód r.
Si existiera $d' < d$ con $q^{d'} \equiv 1$ mód r, se tendría que $\zeta^{q^{d'}} = \zeta$ y ζ estaría en cualquier extensión de $\mathbb{F}_q$ de grado d' (sería raíz de $x^{q^{d'}} - x$). Pero como $\mathbb{F}_{q^d}$ es el cuerpo de escisión de ϕ_r, $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^d} \hookrightarrow \mathbb{F}_{q^{d'}}$ y $d > d'$, lo que contradice la hipótesis. Por tanto, como d es el menor entero que lo cumple, es el orden de q en $(\mathbb{Z}/r\mathbb{Z})^*$.

ii) Se considera ahora el polinomio mínimo de cualquier raíz de la unidad: por lo visto en el apartado anterior, su grado es d, pues F es su cuerpo de escisión.
Entonces todos los factores irreducibles del polinomio ciclotómico de orden r tienen grado d, y ϕ_r tiene grado $\varphi(r)$: entonces ϕ_r tiene $\frac{\varphi(r)}{d}$ factores irreducibles de grado d. □

Además, las raíces de dichos factores deben de ser las raíces de la unidad de orden r. Por tanto los factores de ϕ_r serán los polinomios mónicos e irreducibles de grado d y orden r sobre $\mathbb{F}_q$:

$$\phi_n(x) = \prod_{f \in P(d,q,r)} f$$

donde $P(d, q, r)$ es el conjunto de dichos polinomios.

1.5. Funciones de Möbius y de Euler

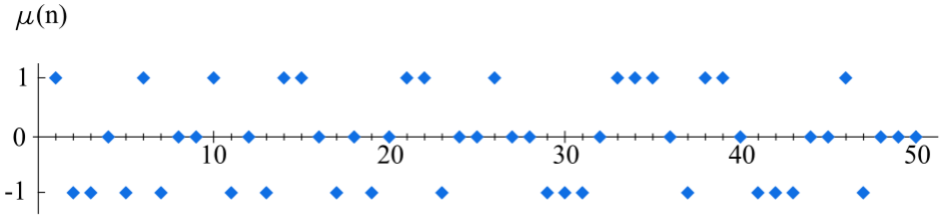
Para concluir el capítulo de preliminares, se presentan las funciones de Möbius y de Euler, cuya relevancia se pondrá especialmente de manifiesto a la hora de contar polinomios irreducibles. Las principales referencias de esta sección son [10] y [13].

Definición 1.22 *Se llama* ***función de Möbius*** *a la función $\mu : \mathbb{N} \to \mathbb{C}$ definida de la siguiente manera:*

$$\mu(n) = \begin{cases} 1 & \textit{si } n \textit{ es libre de cuadrados, producto de un número par de primos} \\ -1 & \textit{si } n \textit{ es libre de cuadrados, producto de un número impar de primos} \\ 0 & \textit{si } n \textit{ no es libre de cuadrados} \end{cases}$$

A continuación se muestran ejemplos de esta función aplicada a los números del 1 al 10 (tabla) y del 1 al 50 (gráfica):

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1



Algunas propiedades interesantes de la función de Möbius son las siguientes:

Proposición 1.23

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & si\ n = 1 \\ 0 & si\ n \geq 2 \end{cases}$$

Demostración: Dado $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$, sea $P_n = \{p_1, p_2, \ldots, p_r\}$. Para comprobar que la propiedad es cierta, basta con definir la siguiente aplicación:

$$\begin{array}{ccc} f : \{d : d \mid n, ; \mu(d) \neq 0\} & \to & \mathcal{P}(P_n) \\ d & \mapsto & \{p_i, ; p_i \mid d\} \end{array}$$

Se comprueba que la aplicación es biyectiva:

i) Es inyectiva: sean d_1, d_2 divisores de n libres de cuadrados, de tal forma que su imagen por f sea la misma: como d_1 y d_2 son libres de cuadrados, $f(d_1)$ es el conjunto de sus divisores (quitando el 1), y lo mismo para $f(d_2)$. Entonces, dado que tienen los mismos divisores, se deduce que $d_1 = d_2$, y por tanto la aplicación es inyectiva.

ii) Es sobreyectiva: un elemento de $\mathcal{P}(P_n)$ es un conjunto de divisores primos de n. Al hacer el producto de todos ellos, siempre vamos a obtener un d que divide a n, libre de cuadrados; es decir, un elemento d tal que $f(d)$ es justamente el conjunto dado.

Se tiene que $\mathcal{P}(P_n)$ es un conjunto potencia, y por lo tanto tiene el mismo número de elementos de cardinal par que impar. Como f es biyectiva, esto significa que en el conjunto de partida hay la misma cantidad de elementos con número de divisores par que impar: es decir, hay la misma cantidad de d tal que $\mu(d) = 1$ o $\mu(d) = -1$.
Por lo tanto, al hacer el sumatorio $\sum_{d|n} \mu(d)$, el resultado es 0 (se suma $1 - 1$ el mismo número de veces). □

El siguiente resultado sirve para estudiar la relación entre polinomios de una cierta forma por medio de la función de Möbius, y es especialmente útil a la hora de contar polinomios.

Teorema 1.24 (Inversión de la función de Möbius) *Sean $f, g : \mathbb{N} \to \mathbb{C}$, cumpliendo $f(n) = \sum_{d|n} g(d)$. Entonces, $g(n) = \sum_{d|n} f(\frac{n}{d})\mu(d)$. Del mismo modo, si $f(n) = \prod_{d|n} g(d)$, entonces $g(n) = \prod_{d|n} f(\frac{n}{d})^{\mu(d)}$*

Demostración: Se tiene:

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

El último paso de esa cadena de igualdades viene del hecho de que d divide a n y c divide a $\frac{n}{d}$ si y sólo si c divide a n y d divide a $\frac{n}{c}$. Entonces:

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

Lo que hay dentro del segundo sumatorio es 0 excepto cuando $\frac{n}{c} = 1$; por tanto se obtiene:

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

La demostración es análoga en el caso multiplicativo. □

El siguiente lema es parecido al Teorema de Inversión de la función de Möbius, y por ello se incluye a continuación. Será útil para demostrar algunos resultados que se verán más adelante. Se puede encontrar en la referencia [12]

Lema 1.25 *Sean R un conjunto, $\{X(d,t)\}_{d\in\mathbb{N},t\in R}$ una familia de subconjuntos de R tal que:*

i) $X(1,t) = \{t\}$ *para todo t en R*

ii) Los conjuntos $\{e' \in X(d',e) : e \in X(d,t)\}$ *y* $\{e \in X(dd',t)\}$ *sean iguales*

Sean $A, B : \mathbb{N} \times R \to C$ dos funciones con valores en C un anillo conmutativo con unidad. Entonces son equivalentes:

$$A(n,t) = \sum_{d|n} \sum_{e\in X(d,t)} B(\frac{n}{d}, e)$$

y

$$B(n,t) = \sum_{d|n} \mu(d) \sum_{e\in X(d,t)} A(\frac{n}{d}, e)$$

Demostración: Es parecida a la de la fórmula de inversión de Möbius: sólo hay que sustituir los valores de A y B en cada caso y reorganizar los subíndices de los sumatorios.

Para finalizar el capítulo de preliminares, se procede a explicar algunos aspectos de la función de Euler, cuya relevancia es innegable en el el ámbito de los cuerpos finitos.

Definición 1.26 *Se llama **función φ de Euler** a aquella que actúa sobre los números naturales de la siguiente forma:*

$$\varphi(n) = |\{m \in \mathbb{N} : m < n, mcd(m,n) = 1\}|$$

Algunas de sus más conocidas propiedades son las siguientes:

Lema 1.27 (Propiedades de la función φ de Euler) *Sea φ la función dada por la definición anterior. Se cumple lo siguiente:*

i) $\varphi(p) = p - 1$ *para todo p primo*

ii) $\varphi(p^k) = (p-1)p^k$ *para todo p primo, k número natural*

iii) $\varphi(mn) = \varphi(m)\varphi(n)$ *si m y n son primos entre sí*

La demostración de estas propiedades es trivial.

Capítulo 2

Construcción de polinomios irreducibles

Este capítulo se apoya especialmente en las referencias [14] y [2].

Como se ha explicado anteriormente, un cuerpo finito de cardinal p^n puede generarse a partir de un polinomio irreducible de grado n sobre $\mathbb{F}_p$. Si $n = r_1^{e_1} r_2^{e_2} ... r_l^{e_l}$ y se dispone de un polinomio de grado $r_i^{e_i}$ para cada $i = 1...l$, utilizando los resultados de la sección final de este capítulo se podrá generar un polinomio de grado n irreducible sobre $\mathbb{F}_p$.

Por lo tanto, es necesario asegurar que, para cada r, e con r primo y e un entero positivo, existe un polinomio irreducible de grado r^e sobre $\mathbb{F}_p$. En vez de hacerlo directamente, se va a dividir este problema en varios casos:

(a) Grado impar, r igual a la característica del cuerpo: $r = p \neq 2$

(b) Grado par, r igual a la característica del cuerpo: $r = p = 2$

(c) Grado par ($r = 2$) y característica $p \equiv 1$ mód 4

(d) Grado par ($r = 2$) y característica $p \equiv 3$ mód 4

(e) Grado impar y $r \neq p$

En cada una de las secciones siguientes se dan una serie de resultados cuyo objetivo es construir un polinomio irreducible de grado r^e sobre $\mathbb{F}_p$ en cada uno de los casos descritos.

Los polinomios que se intentarán construir en cada caso habrán de ser lo más sencillos posible; en concreto, muchos de ellos serán binomios y trinomios. Se define a continuación este tipo de polinomios:

Definición 2.1 *Se dice que un polinomio de $\mathbb{F}_q[x]$ es un **binomio** (o **trinomio**) si sólo tiene dos (o tres) coeficientes distintos de 0.*

Se procede entonces a estudiar cada uno de los casos descritos anteriormente por separado.

2.1. Caso (a)

En este caso los polinomios que se proporcionan son trinomios. Con el fin de asegurar su irreducibilidad más adelante, se estudian varios resultados por separado, cuya utilidad se pondrá de manifiesto en el teorema final de la sección.

Proposición 2.2 *Si $q = p^m$ con p primo, el trinomio*

$$x^p - x - b$$

con b un elemento de $\mathbb{F}_q$ es irreducible si y sólo si $Tr_{\mathbb{F}_q,\mathbb{F}_p}(b) \neq 0$.

Demostración: Se comienza demostrando por inducción que, para todo i natural y θ raíz del polinomio, $\theta^{p^i} = \theta + b + b^p + ... + b^{p^{i-1}}$.
Para $i = 1$: si θ es una raíz de $x^p - x - b$, entonces cumple $\theta^p = \theta + b$.
Ahora, se supone cierta la igualdad para $i - 1$; entonces, sobre $\mathbb{F}_q$ cuya característica es p, $\theta^{p^i} = (\theta^{p^{i-1}})^p = (\theta + b + b^p + ... + b^{p^{i-2}})^p = \theta + b + (b + b^p + ... + b^{p^{i-2}})^p = \theta + b + b^p + ... + b^{p^{i-1}}$, como se quería probar.
En concreto, si se toma $i = m$,

$$\theta^{p^m} = \theta + b + b^p + ... + b^{p^{m-1}} = \theta + Tr(b)$$

Esto significa que $Tr(b) = 0$ si y sólo si $\theta^q = \theta$: dicho de otra forma, si y sólo si todas las raíces de $x^p - x - b$ pertenecen a $\mathbb{F}_q$.
Hasta ahora se ha visto que $x^p - x - b$ es producto de factores lineales de $\mathbb{F}_q$ si y sólo si la traza de b es 0. Pero lo que se quiere estudiar es la irreducibilidad del trinomio, y podría darse el caso de que se descomponga en factores no lineales.
Lógicamente, esto sólo ocurre si $Tr_{\mathbb{F}_q,\mathbb{F}_p}(b) \neq 0$. Si se siguen tomando potencias, se llega a que $\theta^{q^i} = \theta + iTr(b)$ para todo $i = 1...p - 1$, y, en concreto, $\theta^{q^p} = \theta$ (y todos los elementos θ^{q^i} son distintos). Esto quiere decir que el polinomio mínimo de θ sobre $\mathbb{F}_q$ tiene grado p, y por tanto tiene que ser $x^p - x - b$. Se concluye entonces que este trinomio es irreducible. □

Se presenta ahora un lema acerca de la irreducibilidad de una particular composición de polinomios, cuya demostración se puede ver en [14].

Lema 2.3 *Sean f y g dos polinomios en $\mathbb{F}_q[x]$ distintos de 0, y P un polinomio irreducible en $\mathbb{F}_q[x]$ de grado $n \geq 1$. Entonces $g(x)^n P(\frac{f(x)}{g(x)})$ es irreducible sobre $\mathbb{F}_q$ si y sólo si $f(x) - \lambda g(x)$ es irreducible sobre $\mathbb{F}_{q^n}$, donde λ es una raíz de P.*
Además, si P no es de la forma $P(x) = cx$ con $c \in \mathbb{F}_q$, entonces $g(x)^n P(\frac{f(x)}{g(x)})$ tiene grado hn, donde $h = max\{\delta(f), \delta(g)\}$.

La siguiente proposición relaciona los dos resultados anteriores y se utiliza en la demostración del teorema central de esta sección.

Proposición 2.4 *Sea $q = p^m$ con p primo, $f(x) = x^n + c_{n-1}x^{n-1} + ... + c_1x + c_0$ un polinomio mónico e irreducible sobre $\mathbb{F}_q$, y $b \in \mathbb{F}_q$. Entonces $f(x^p - x - b)$ es irreducible sobre $\mathbb{F}_q$ si y sólo si $Tr_{\mathbb{F}_q,\mathbb{F}_p}(nb - c_{n-1}) \neq 0$*

Demostración: Sea $\alpha \in \mathbb{F}_{q^n}$ una raíz de f. Por el lema 2.3, tomando $g(x) = 1$, $P = f$ y la que sería la f en el lema como $x^p - x - b$, $f(x^p - x - b)$ es irreducible sobre $\mathbb{F}_q$ si y sólo si $x^p - x - b - \alpha$ lo es sobre $\mathbb{F}_{q^n}$. Aplicando la proposición 2.2 esto es equivalente a que $Tr_{\mathbb{F}_{q^n},\mathbb{F}_p}(b + \alpha) \neq 0$; pero $Tr_{\mathbb{F}_{q^n},\mathbb{F}_p}(b + \alpha) = Tr_{\mathbb{F}_q,\mathbb{F}_p}(Tr_{\mathbb{F}_{q^n},\mathbb{F}_q}(b + \alpha)) = Tr_{\mathbb{F}_q,\mathbb{F}_p}(nb - c_{n-1}) \neq 0$. □

El teorema que permite construir polinomios irreducibles en las condiciones del caso (a) hace uso de los polinomios recíprocos; por eso se incluye ahora una breve explicación sobre los mismos.

Definición 2.5 *Sea f un elemento de $\mathbb{F}_q[x]$. su **polinomio recíproco** f^* como $f^*(x) = x^n f(\frac{1}{x})$, siendo $n = \delta(f)$. Se dice que f es **autorrecíproco** si $f = f^*$.*

Por ejemplo, dado $f(x) = x^3 + 2x^2 + 3x + 4$, su polinomio recíproco es:

$$f^*(x) = x^3 f(\frac{1}{x}) = x^3(\frac{1}{x^3} + \frac{2}{x^2} + \frac{3}{x} + 4) = 4x^3 + 3x^2 + 2x + 1$$

Por otra parte, el polinomio $g(x) = x^2 + 4x + 1$ es un polinomio autorrecíproco: $g^*(x) = x^2(\frac{1}{x^2} + \frac{4}{x} + 1) = x^2 + 4x + 1$.

Observación 2.6 *Es claro que f^* y f tienen el mismo grado si 0 no es raíz de f. Al sustituir en la fórmula dada por la definición, si $f(x) = a_0 + a_1 x + ... + a_n x^n$, entonces $f^*(x) = a_0 x^n + a_1 x^{n-1} + ... + a_n$. En f^*, el coeficiente que acompaña al término de grado n es a_0, que sólo se anula si el 0 es raíz de f.*

Se presenta ahora el teorema que permite construir polinomios irreducibles en las condiciones del caso (a).

Teorema 2.7 *Sea p un número primo, y $f(x) = x^n + c_{n-1}n^{n-1} + ... + c_1 x + c_0$ un polinomio mónico e irreducible de grado n sobre $\mathbb{F}_p$, tal que existe un elemento $a \in \mathbb{F}_p^*$ con $(na + c_{n-1})f'(a) \neq 0$. Sea $g(x) = x^p - x + a$. Se definen los siguientes polinomios:*

$$f_0(x) = f(g(x))$$

$$f_k(x) = f_{k-1}^*(g(x)) \text{ para todo } k \geq 1$$

donde f^* es el polinomio recíproco de f. Entonces los polinomios f_k son irreducibles sobre $\mathbb{F}_p$ y tienen grado np^{k+1}.

Demostración: Se va a probar que, para cada k natural, existe $c \in \mathbb{F}_p^*$ tal que tanto $f_k(x) = f_k'(x) = c$ para todo x (por lo que $f_k'(a) \neq 0$), f_k es irreducible en $\mathbb{F}_p$ y su grado es $n_k := np^{k+1}$. Se va a demostrar por inducción sobre k. Cada f_k se expresará de la siguiente manera:

$$f_k(x) = \sum_{i=0}^{n_k} f_{ki} x^i$$

Si $k = 0$, se aplica la regla de la cadena para deducir que $f_0'(x) = f'(g(x))g'(x)$. El coeficiente de f_0 que acompaña al término de grado 1 es justamente la derivada $f_0'(0) = f'(g(0))g'(0) = -f'(a)$, teniendo en cuenta que $g(0) = a$ y $g'(0) = -1$ (esto se comprueba de manera inmediata,

pues $a \in \mathbb{F}_p^*$). Como además g es un polinomio constante sobre $\mathbb{F}_p$, también lo es f_0, y $g'(x) = -1$ para todo x. Entonces, $f_0'(a) = f'(g(a))g'(a) = -f(a)$. Este elemento es distinto de 0 por hipótesis.

Además, el grado de f_0 es np. Usando la proposición 2.4, $f_0(x) = f(g(x))$ es un polinomio irreducible sobre $\mathbb{F}_p$ si y sólo si $Tr_{\mathbb{F}_p,\mathbb{F}_p}(na + c_{n-1}) = na + c_{n-1} \neq 0$; esto también se cumple por hipótesis, y por lo tanto f_0 es irreducible.

Se suponen ahora ciertas las propiedades para k, y se procede a demostrarlas para $k+1$. Como el grado de f_k es np^{k+1}, el polinomio $f_k^*(g(x))$ tiene grado $np^{k+1}p = np^{k+2}$. Dado que el polinomio f_k es irreducible, su término independiente f_{k0} es distinto de 0, y $(f_{k0})^{-1}f_k^*(x)$ es un polinomio mónico, de tal forma de que el coeficiente del término x^{n_k-1} es $(f_{k0})^{-1}f_{k1} \neq 0$. Además, este número es justamente $Tr_{\mathbb{F}_p,\mathbb{F}_p}(n_k a + (f_{k0})^{-1}f_{k1}) = (f_{k0})^{-1}f_{k1}$. Utilizando otra vez la proposición 2.4 se obtiene que f_{k+1} es irreducible sobre $\mathbb{F}_p$.

Falta demostrar que f_{k+1} y f_{k+1}' toman siempre el mismo valor sobre $\mathbb{F}_p$ y que $f_{k+1,1} = f_{k+1}'(a)$. Sustituyendo en la definición, $f_{k+1}(x) = f_k^*(g(x)) = \sum_{i=0}^{n_k} f_{ki}g(x)^{n_k-i}$. Entonces, teniendo en cuenta que $g'(x) = -1$, se tiene que $f_{k+1}'(x) = \sum_{i=0}^{n_k} f_{ki}ig(x)^{n_k-i-1}$ (basta con derivar la fórmula anterior). Además, como $g(x)$ es constante en $\mathbb{F}_p$, también lo son f_{k+1} y su derivada, y el coeficiente $f_{k+1,1} = f_{k+1}'(0) = f_k^*(g(0))g'(0) = -(f_k^*)'(a) = -f_k'(a^{-1})a^{n_k-1}$, que es distinto de 0 por la hipótesis de inducción; luego $f_{k+1}'(a) = -f_k^{*\prime}(a) \neq 0$. □

En particular, del teorema anterior se deduce el siguiente corolario:

Corolario 2.8 *Si $f_0(x) = x^p - x - 1$ y $f_k(x) = f_{k-1}^*(x^p - x - 1)$, los polinomios f_k son irreducibles sobre $\mathbb{F}_p$ de grado p^{k+1} para todo $k = 0, 1....$*

Demostración: Basta con aplicar el teorema anterior, tomando $f(x) = x$, $a = -1$; con la notación precendente, $(na + c_{n-1})f'(a) = a = -1 \neq 0$. □

Por ejemplo, si se quiere generar un polinomio irreducible en $\mathbb{F}_3$ de grado 9, en este caso se tendría $r = p = 3$, y $k = 1$. Entonces $f_0(x) = x^3 - x - 1$ es irreducible de grado 3. El siguiente polinomio de la sucesión sería $f_1(x) = 2x^9 + 2x^6 + 2x^4 + 2x^2 + x + 1$, que es, como se quería, irreducible de grado 9 sobre $\mathbb{F}_3$. Si además se quisiera que el polinomio obtenido fuera mónico, bastaría con multiplicar por 2 para obtener $x^9 + x^6 + x^4 + x^2 + 2x + 2$, mónico e irreducible.

Del mismo modo, el trinomio $x^5 - x - 1$ es irreducible sobre $\mathbb{F}_5$.

2.2. Caso (b)

En este caso, al igual que en el anterior, los polinomios que se van a construir son trinomios.

Anteriormente, se han estudiado los trinomios de la forma $x^p - x - b$, y se ha visto que son irreducibles si y sólo si $Tr_{\mathbb{F}_q,\mathbb{F}_p}(b) \neq 0$. De forma similar, es posible comprobar la irreducibilidad

de cualquier trinomio $x^p - ax - b$ mediante el siguiente resultado, cuya demostración se puede encontrar en la referencia [14]

Lema 2.9 *Sea $q = p^m$ con p primo. Si $a, b \in \mathbb{F}_q^*$, el trinomio $x^p - ax - b$ es irreducible en $\mathbb{F}_q[x]$ si y sólo si $a = a_0^{p-1}$ para algún $a_0 \in \mathbb{F}_q^*$ y $Tr_{\mathbb{F}_q,\mathbb{F}_p}(\frac{b}{a_0^p}) \neq 0$*

De manera similar a la sección anterior, se relaciona en la siguiente proposición la irreducibilidad de ciertos polinomios con la traza de algunos de sus coeficientes cuando se trabaja en un cuerpo de característica 2.

Proposición 2.10 *Sean $q = 2^m$ y $f(x) = c_n x^n + c_{n-1}x^{n-1} + ... + c_1 x + c_0$ irreducible en $\mathbb{F}_q[x]$, de grado n. El polinomio $x^n f(x + x^{-1})$ es autorrecíproco de grado $2n$ sobre $\mathbb{F}_q$, y además es irreducible si y sólo si $Tr_{\mathbb{F}_q,\mathbb{F}_2}(\frac{c_1}{c_0}) \neq 0$.*

Demostración: Sea $g(x) = x^n f(x + x^{-1})$. Es evidente que g es de grado $2n$. Su polinomio recíproco es $g^*(x) = x^{2n}g(x^{-1}) = x^{2n}x^{-n}f(x^{-1} + x) = g(x)$, y por lo tanto es autorrecíproco. Utilizando el lema 2.3 el problema de la irreducibilidad de g se reduce a comprobar si $x^2 - x\alpha + 1$ es irreducible en $\mathbb{F}_{q^n}$, donde α es una raíz de f. A su vez, utilizando el lema anterior, esto es equivalente a que se cumpla $Tr_{\mathbb{F}_{q^n},\mathbb{F}_2}(\alpha^{-2}) \neq 0$. Pero $Tr_{\mathbb{F}_{q^n},\mathbb{F}_2}(\alpha^{-2}) = (Tr_{\mathbb{F}_{q^n},\mathbb{F}_2}(\alpha^{-1}))^2 = (Tr_{\mathbb{F}_q,\mathbb{F}_2}(Tr_{\mathbb{F}_{q^n},\mathbb{F}_q}(\alpha^{-1})))^2 = (Tr_{\mathbb{F}_q,\mathbb{F}_2}(\frac{-c_1}{c_0}))^2) = (Tr_{\mathbb{F}_q,\mathbb{F}_2}(\frac{c_1}{c_0}))^2)$. Por lo tanto, basta con que se cumpla $Tr_{\mathbb{F}_q,\mathbb{F}_2}(\frac{c_1}{c_0}) \neq 0$. □

Por último, se presenta el teorema principal de esta sección, que permite construir poliomios irreducibles de grado par en un cuerpo de característica 2, seguido de un corolario que explica cómo se hace esta construcción en las condiciones del caso (b).

Teorema 2.11 *Sean $q = 2^m$ y $f(x) = c_n x^n + c_{n-1}x_{n-1} + ... + c_1 x + c_0 \in \mathbb{F}_q[x]$ irreducible, con $c_0 c_n \neq 0$. Se definen los siguientes polinomios:*

$$f_0(x) = f(x)$$

$$f_k(x) = x^{n2^{k-1}} f_{k-1}(x + x^{-1})$$

Para todo $k \geq 0$ el polinomio f_k es autorrecíproco de grado $n2^k$. Además,

i) f_1 es irreducible si $Tr_{\mathbb{F}_q,\mathbb{F}_2}(\frac{c_1}{c_0}) \neq 0$.

ii) Para $k > 1$, f_k es irreducible si $Tr_{\mathbb{F}_q,\mathbb{F}_2}(\frac{c_1}{c_0}) \neq 0$ y $Tr_{\mathbb{F}_q,\mathbb{F}_2}(\frac{c_{n-1}}{c_n}) \neq 0$.

Demostración: Se comprueba que cada f_k es de grado $n2^k$ y que es autorrecíproco gracias a la proposición 2.10. El primer punto también se deduce de este mismo resultado.

A continuación se va a aplicar inducción sobre k para probar la segunda parte. Si $k = 1$ y $Tr_{\mathbb{F}_q,\mathbb{F}_2}(\frac{c_1}{c_0}) \neq 0$, ya se ha visto que f_1 es irreducible. Se supone el resultado cierto para k, junto con la condición $Tr_{\mathbb{F}_q,\mathbb{F}_2}(\frac{c_{n-1}}{c_n}) \neq 0$. A fin de simplificar la notación, se definen: $n_k = n2^k$ y $f_k(x) = \sum_{i=0}^{n_k} c_{ki}x^i$. Por definición, $f_k(x) = x^{n_{k-1}} f_{k-1}(\frac{1+x^2}{x})$, que justamente coincide con

$= x^{n_{k-1}} \sum_{i=0}^{n_{k-1}} c_{k-1,i}(\frac{1+x^2}{x})^i = \sum_{i=0}^{n_{k-1}} c_{k-1,i}(1+x^2)^i(x)^{n_{k-1}-i} = \sum_{i=0}^{n_k} c_{ki}x^i.$
Igualando coeficientes, $c_{k0} = c_{k-1,n_{k-1}}$ y $c_{k1} = c_{k-1,n_{k-1}}$. Usando otra vez la proposición 2.10 se deduce que f_{k+1} es irreducible si y sólo si $Tr_{\mathbb{F}_q,\mathbb{F}_2}(\frac{c_{k1}}{c_{k0}}) \neq 0$. Dado que todos los f_k son autorrecíprocos, se tienen las siguientes relaciones entre los coeficientes:

$$c_{k0} = c_{k-1,n_{k-1}} = c_{k-1,0} = ... = c_{1,0} = c_{0,n_0} = c_n$$

$$c_{k1} = c_{k-1,n_{k-1}-1} = c_{k-1,1} = ... = c_{1,1} = c_{0,n_0-1} = c_{n-1}$$

Por tanto la condición anterior sobre la traza es equivalente a que $Tr_{\mathbb{F}_q,\mathbb{F}_2}(\frac{c_{n-1}}{c_n}) \neq 0$; y si esto se cumple, f_{k+1} es irreducible. □

Corolario 2.12 *Si $f_0(x) = x + 1 \in \mathbb{F}_2[x]$ y $f_k(x) = x^{2^{k-1}} f_{k-1}(x + x^{-1})$, los polinomios f_k son mónicos e irreducibles sobre $\mathbb{F}_p$ de grados 2^k para todo $k = 0, 1....$*

Demostración: Basta con aplicar el teorema anterior: $n = 1$, $c_0c_1 = 1 \neq 0$. Además, se comprueba trivialmente la condición sobre las trazas, puesto que los únicos coeficientes de f son $c_0 = c_1 = 1$. □

En este caso, un posible ejemplo sería hallar polinomios de grado 2^k en $\mathbb{F}_2$, con $k = 0, 1, 2$. En el caso $k = 0$, se tiene $f_0(x) = x + 1$.
Si $k = 1$, $f_1(x) = xf_0(x + x^{-1}) = x^2 + x + 1$ es un polinomio irreducible de grado 2 sobre $\mathbb{F}_2$. Si $k = 2$, se obtiene que $x^4 + x^3 + x^2 + x + 1$ es irreducible de grado 4 en $\mathbb{F}_2[x]$.

2.3. Caso (c)

Los polinomios que se van a generar en esta ocasión son binomios. Para estudiar su irreducibilidad se van a dar antes varios resultados. El concepto de radical es muy útil para simplificar la notación en este caso, y por ello viene incluido a continuación.

Definición 2.13 *El **radical** de un número $rad(n)$ es su mayor divisor libre de cuadrados.*

El siguiente lema será útil a la hora de estudiar la irreducibilidad de binomios. Su demostración se puede encontrar, como en otras ocasiones, en la referencia [14].

Lema 2.14 *Sean q una potencia de primo, $m \geq 2$ un entero que divide a $q - 1$, $n \geq 2$ un entero tal que se cumplen:*

i) $rad(n)$ divide a m en $\mathbb{F}_q^*$

ii) $mcd(n, \frac{q-1}{m}) = 1$

iii) Si 4 divide a n, entonces $q \equiv 1$ mód 4

Entonces $ord_{mn}(q) = n$.

Se presenta ahora un teorema que proporciona una caracterización de los binomios irreducibles. Este resultado no sólo será útil para construir binomios irreducibles, sino que también servirá para contarlos en el próximo capítulo. Más detalles sobre este teorema se pueden encontrar en las referencias [10] y [14].

Teorema 2.15 *Un binomio $x^n - a$ de $F_q[x]$ es irreducible si y sólo si se cumplen:*

i) $rad(n)$ divide al orden de a ($ord(a)$) en $\mathbb{F}_q^*$

ii) $mcd(n, \frac{q-1}{ord(a)}) = 1$

iii) Si 4 divide a n, entonces $q \equiv 1$ mód 4

Demostración: Sea el binomio $f(x) = x^n - a$. Se distinguen varios casos:

Se supone primero que se cumplen todas las condiciones. Sea θ una raíz de $x^n - a$, y $m(x)$ el polinomio mínimo de θ sobre $\mathbb{F}_q$, de grado d. Usando el lema 1.12, m divide a $x^n - a$ y $m(x) = (x - \theta)(x - \theta^q)(x - \theta^{q^2})...(x - \theta^{q^{d-1}})$, donde $\theta, \theta^q, \theta^{q^2}...\theta^{q^{d-1}}$ son distintas entre sí y $\theta^{q^d} = \theta$. Además se sabe que $\theta^{ord(a)n} = a^{ord(a)} = 1$; por tanto el orden de θ es un divisor de $ord(a)n$. Se comprueba que es es justamente $ord(a)n$.

Si fuese menor, existiría un divisor primo r de $ord(a)n$ para el que se cumple $\theta^{\frac{ord(a)n}{r}} = 1$. Además, por ser primo, r divide a n o al orden de a; y, de hecho, si divide a n también divide a $ord(a)$, usando la primera condición. Pero entonces $a^{\frac{ord(a)}{r}} = (\theta^n)^{\frac{ord(a)}{r}} = 1$, y entonces a no tendría orden $ord(a)$. Por lo tanto el orden de θ es $ord(a)n$.
Entonces $\theta^{q^d-1} = 1$ si y sólo si $q \equiv 1$ mód $ord(a)n$, y d es el menor entero para el que $\theta^{q^d} = \theta$; pues el polinomio mínimo de θ tiene grado d y sus raíces son las sucesivas potencias de grado q^i para $i = 0...d-1$; por lo tanto d es el menor entero para el que $q^d \equiv 1$ mód $ord(a)n$. Entonces $d = ord_{ord(a)n}(q)$. Además, teniendo en cuenta el lema 2.14 y las condiciones del enunciado, $ord_{ord(a)n}(q) = n$. Luego el grado del polinomio mínimo de θ es justamente n, $x^n - a = m(x)$ y el binomio $x^n - a$ es irreducible.

Si no se cumplen las dos primeras condiciones, se descompone $n = rt_1$ donde r es primo que no divide a $ord(a)$ o que sí divide a $\frac{q-1}{ord(a)}$.
Si r divide a $\frac{q-1}{ord(a)}$, entonces existe s tal que $rs = \frac{q-1}{ord(a)}$, y por lo tanto $\frac{q-1}{r} = ord(a)s$. Dado que a es un elemento de $\mathbb{F}_q^*$, que tiene $q-1$ elementos, y su orden divide a $\frac{q-1}{r}$, entonces existe un elemento b de $\mathbb{F}_q^*$ tal que $a = b^r$; como se ha visto en preliminares, el subgrupo de potencias de $\mathbb{F}_q$ de orden r tiene orden $\frac{q-1}{r} = ord(a)s$, y es cíclico; por tanto tiene un subgrupo de orden $ord(a)$ que debe ser $< a >$. Entonces $x^n - a = x^{rt_1} - b^r$ tiene como factor a $x^{t_1} - b$, y no sería irreducible.

Si r no divide ni a $ord(a)$ ni a $\frac{q-1}{ord(a)}$, entonces r no divide a $q-1$. Como r es primo, esto significa que existe un número entero y tal que $ry \equiv 1$ mód $q-1$. Dado que $\mathbb{F}_q^*$ es un grupo cíclico de orden $q-1$, $a^{ry} = a$ y se obtiene que $x^{rt_1} - a^{ry}$ tiene como factor a $x^{t_1} - a^y$ y por tanto no es irreducible.

Se supone ahora que las dos primeras condiciones se cumplen, pero la tercera no. Es decir, se estudia el caso en el que 4 divide a n, pero no divide a $q-1$.

Dado que 4 divide a n, entonces 2 también; de hecho, como 2 es primo, 2 también divide a $rad(n)$. Este, a su vez, divide a $ord(a)$, que divide a $q-1$: de lo que se deduce que $q-1$ es par; y por tanto q es impar. Por hipótesis, $q \not\equiv 1$ mód 4, así que tiene que ser $q \equiv 3$ mód 4.
Como 4 no divide a $q-1$, tampoco puede dividir a $ord(a)$; entonces $\frac{ord(a)}{2}$ es impar, y $a^{\frac{ord(a)}{2}} = -1$.
Se puede reescribir el polinomio $x^n - a = x^n + a^{\frac{ord(a)}{2}+1} = x^n - a^d$ tomando $d = \frac{ord(a)}{2} + 1$, que es un número par.
Se deduce que $\frac{a^{\frac{d}{2}}}{2}$ es un elemento de $\mathbb{F}_q^*$, y que $(\frac{a^{\frac{d}{2}}}{2})^{q-1} = 1$. Multiplicando en esta igualdad por $(\frac{a^{\frac{d}{2}}}{2})^2$, se obtiene que $(\frac{a^{\frac{d}{2}}}{2})^{q+1} = (\frac{a^{\frac{d}{2}}}{2})^2$.
Por otro lado, como $q \equiv 3$ mód 4; entonces, 4 necesariamente divide a $q+1$. Se verifica entonces la siguiente cadena de igualdades:

$$a = a^d = 4(\frac{a^{\frac{d}{2}}}{2})^2 = 4(\frac{a^{\frac{d}{2}}}{2})^{q+1} = 4c^4$$

donde $c = (\frac{a^{\frac{d}{2}}}{2})^{\frac{q+1}{4}}$.
Como, por hipótesis, 4 divide a n, sea $n = 4n_1$. Llegados a este punto se tiene la siguiente factorización:

$$x^n - a = x^n + a^d = x^{4n_1} + 4c^4 = (x^{2n_1} + 2cx^{n_1} + 2c^2)(x^{2n_1} - 2cx^{n_1} + 2c^2)$$

y por lo tanto $x^n - a$ no es irreducible. □

El resultado que se presenta a continuación se deduce fácilmente del teorema que se acaba de ver, y ofrece una condición suficiente para comprobar si un binomio es irreducible:

Corolario 2.16 *Sean r un divisor primo de $q-1$, $k \geq 0$ un entero, $a \in \mathbb{F}_q^*$ con $ord(a) > 1$. Si*

i) r no divide a $\frac{q-1}{ord(a)}$.

ii) 4 divide a $q-1$ cuando $r = 2$ y $k \geq 2$

Entonces $x^{r^k} - a$ es irreducible en $\mathbb{F}_q[x]$

Demostración: Dado que a pertenece a $\mathbb{F}_q^*$, su orden $ord(a)$ divide a $q-1$. Sea $t = r^k$; t tiene un único divisor primo, que es r. Como r divide a $q-1$ pero no a $\frac{q-1}{ord(a)}$, entonces necesariamente r divide a $ord(a)$. Se cumplen así las dos primeras condiciones del teorema anterior. Además, si 4 divide a t entonces r tiene que ser 2. Como k es mayor o igual que 2, entonces 4 divide a $q-1$, y se cumple la tercera condición del teorema anterior; por tanto $x^{r^k} - a$ es irreducible. □

Por ejemplo, si se quiere obtener un binomio irreducible de grado 2 en $\mathbb{F}_5$, aplicando el corolario habría que encontrar un elemento $a \in \mathbb{F}_5$ con $ord(a) > 1$. Si se toma $a = 2$, se cumplen las dos condiciones especificadas en el corolario:

i) En este caso $r = 2$ no divide a $\frac{q-1}{ord(a)} = \frac{5-1}{ord(2)} = 1$

ii) Como $q - 1 = 4$, 4 siempre lo divide y no hace falta comprobar más

Entonces el binomio $x^2 - 2$ es irreducible en $\mathbb{F}_5$ de grado 2. Además, se pueden hallar más binomios irreducibles sobre $\mathbb{F}_5$ haciendo variar el valor de la k: por ejemplo, $x^{32} - 2$ y $x^{256} - 2$ también son irreducibles.

2.4. Caso (d)

En esta sección se ofrece un único teorema, que permite generar trinomios irreducibles en las condiciones del caso (d).

Teorema 2.17 *Sea p un número primo que cumpla $p \equiv 3 \bmod 4$ (es decir, $4 = 2^2$ divide a $p+1$). Sea $r \geq 2$ el entero que cumple que 2^r divide exactamente a $p+1$; entonces, 2^{r+1} divide exactamente a p^2-1. Se definen los siguientes elementos de $\mathbb{F}_p$:*

$$a_1 = 0$$

$$a_i = \left(\frac{a_{i-1}+1}{2}\right)^{\frac{p+1}{4}} \text{ para } i = 2...r-1$$

$$a_r = \left(\frac{a_{r-1}-1}{2}\right)^{\frac{p+1}{4}}$$

Para cualquier entero $k \geq 1$, el trinomio $x^{2^k} - 2a_r x^{2^{k-1}} - 1$ es irreducible sobre $\mathbb{F}_q$, y es divisor de $x^{2^{r+k-1}} + 1$.

Demostración: La demostración de este teorema se divide en varios apartados:

i) Se comprueba que, para todo $l = 1...r-1$, el trinomio $x^2 - 2a_l x + 1$ es irreducible y divide a $x^{2^l} + 1$. Esto se hace distinguiendo entre los casos $l < r-1$ y $l = r+1$.

ii) Se utiliza este último caso para demostrar que el trinomio $x^2 - 2a_r x - 1$ es también irreducible (este es el trinomio del teorema tomando $k = 0$).

iii) Se estudia lo que ocurre cuando $k > 0$.

Para demostrar que para todo $l = 1...r-1$ el polinomio $x^2 - 2a_l x + 1$ es irreducible, se va a utilizar la inducción. Si $l = 1$, quedaría $x^2 + 1$, que es irreducible porque -1 no es un residuo cuadrático módulo p ($p \equiv 3 \bmod 4$). Supóngase ahora que la propiedad se cumple para todo $1 \leq l < r$.

Como $x^2 - 2a_l x + 1$ divide a $x^{2^l} + 1$, $x^4 - 2a_l x^2 + 1$ divide a $x^{2^{l+1}} + 1$. Sea entonces β una raíz de $x^4 - 2a_l x^2 + 1$ en la correspondiente extensión de $\mathbb{F}_p$. Como β es también raíz de $x^{2^{l+1}}$, $ord(\beta) = 2^{l+2}$. En general, como 2^{r+1} divide exactamente a p^2-1, $\mathbb{F}_{p^2}$ contiene todas las raíces de la unidad de orden 2^{k+1} para $0 \leq k \leq r$. Pero, además, 2^2 no divide a $p-1$, así que si $1 \leq k \leq r$ toda raíz primitiva de la unidad no es un elemento de $\mathbb{F}_p$, y por tanto tiene grado 2 sobre $\mathbb{F}_p$. Más concretamente, dado que $ord(\beta) = 2^{l+2}$ y $l+1 \leq r$, β es un elemento de $\mathbb{F}_{p^2}$ de grado 2 sobre $\mathbb{F}_p$.

Como β es una raíz de $x^4 - 2a_l x^2 + 1$, esto significa que $x^4 - 2a_l x^2 + 1$ es el producto de dos factores (mónicos) irreducibles de grado 2 sobre $\mathbb{F}_p$; sea uno de ellos $x^2 - 2sx + t$ el polinomio mínimo de β: sustituyendo, $\beta^2 + t = 2s\beta$, y $\beta^4 = (4s^2 - 2t)\beta^2 - t^2 = 2a_l\beta^2 - 1$. Como se ha visto antes, dado que $\beta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, se puede considerar $\{1, \beta\}$ una base de $\mathbb{F}_{p^2}$ sobre $\mathbb{F}_p$, y de la igualdad se deduce:

$$t^2 = 1 \text{ y } 4s^2 - 2t = 2a_l$$

Es ahora cuando se hace la distinción entre cuando $l < r-1$ y $l = r-1$.

En el primer caso, si $l < r-1$, claramente $l+2 \leq r$. Dado que $t^2 = 1$, t sólo puede ser 1 ó -1. Se comprueba que $t = 1$. Si fuera $t = -1$, entonces el polinomio mínimo de β sería $x^2 - 2sx - 1$, irreducible en $\mathbb{F}_p$, cuyas raíces son raíces primiticas de la unidad de orden 2^{l+2}. Pero, como $l+2 \leq r$, todas estas raíces están contenidas en $\mathbb{F}_{p^2}$ y son de grado 2 sobre $\mathbb{F}_p$. De modo similar a lo hecho anteriormente, el polinomio $x^4 - 2sx - 1$ es el producto de dos polinomios irreducibles de grado 2 sobre $\mathbb{F}_p$; uno de ellos $x^2 - 2s'x + t'$. Como en el caso anterior, se tendría $(t')^2 = -1$ con $t' \in \mathbb{F}_p$, pero -1 no es residuo cuadrático módulo p; esto es una contradicción. Así que tiene que ser $t = 1$. Ahora que se ha hallado este valor, es posible sustituir en la ecuación $4s^2 - 2t = 2a_l$ para deducir que $2s^2 = a_l + 1$, y que por lo tanto $\frac{a_l+1}{2} \in (\mathbb{F}_p^*)^2$; y se tiene $(\frac{a_l+1}{2})^{\frac{p-1}{2}} = 1$. Si $a_{l+1} = (\frac{a_l+1}{2})^{\frac{p+1}{4}}$, entonces $a_{l+1}^2 = (\frac{a_l+1}{2})^{\frac{p+1}{2}} = (\frac{a_l+1}{2})^{\frac{p-1}{2}}(\frac{a_l+1}{2}) = (\frac{a_l+1}{2})$. Entonces los factores de $x^4 - 2a_l x^2 + 1$ son $(x^2 - 2a_{l+1}x + 1)$ y $(x^2 + 2a_{l+1}x + 1)$; queda así visto que $(x^2 - 2a_{l+1}x + 1)$ es irreducible y claramente divide a $x^{2^{l+1}} + 1$.

Si $l = r - 1$, $l + 3 = r + 2 > r + 1$. En este caso se tiene $t = -1$, demostrando de la misma forma que no puede ser $t = 1$. Si lo fuera, $2s^2 = a_{r-1} + 1$ y se tendría la descomposición en irreducibles $x^4 - 2a_{r-1}x^2 + 1 = (x^2 - 2sx + 1)(x^2 + 2sx + 1)$, cuyas raíces son raíces primiticas de la unidad de orden 2^{r+1}; entonces, las raíces de $x^4 + 2sx^2 + 1$ y $x^4 - 2sx^2 + 1$ serían raíces de la unidad de orden 2^{r+2}, que a su vez divide exactamente a $p^4 - 1$. Es decir, el grado de dichas raíces sobre $\mathbb{F}_p$ es 4, y los polinomios $x^4 - 2sx^2 + 1$ y $x^4 + 2sx^2 + 1$ serían irreducibles sobre $\mathbb{F}_p$.

Ahora, si $\frac{s+1}{2} = (s')^2$ para algún $s' \in \mathbb{F}_p$, entonces $x^2 - 2s'x + 1$ divide a $x^4 - 2sx^2 + 1$, que es irreducible. Entonces $\frac{s+1}{2} \notin \mathbb{F}_p^2$. Del mismo modo se puede deducir que $\frac{-s-1}{2}$ tampoco es un elemento de $\mathbb{F}_p^2$. Se ha visto que, dado que $p \equiv 3$ mód 4, -1 no es un elemento de $\mathbb{F}_p^2$. Entonces, para cualquier elemento m, se tiene que m ó $-m$ han de ser elementos de $\mathbb{F}_p^2$; pero ni $\frac{s+1}{2}$ ni $\frac{-s-1}{2}$ lo son, lo cual es una contradicción. Así que en el caso $l = r + 1$, $t = -1$, y $2s^2 = a_{r-1} - 1$; entonces, $\frac{a_{r-1}-1}{2} \in \mathbb{F}_p^2$ y $(\frac{a_{r-1}-1}{2})^{\frac{p-1}{2}}$. Como $a_r = (\frac{a_{r-1}-1}{2})^{\frac{p-1}{4}}$, entonces $a_r^2 = (\frac{a_{r-1}-1}{2})^{\frac{p-1}{2}}$ y se tiene la descomposición $x^4 - 2a_{r-1}x^2 + 1 = (x^2 - a_r x - 1)(x^2 + 2a_r x - 1)$. Por lo tanto $x^2 - a_r x - 1$ es irreducible y divide a $x^{2^r} + 1$. Se concluye así la segunda parte de la demostración.

Se pretende ahora demostrar el teorema sobre el trinomio $x^{2^k} - 2a_r x^{2^{k-1}} - 1$ usando inducción sobre k; todo lo anterior ha servido para probar que lo es en el caso $k = 0$. Se supone cierto en el caso k: es decir, $x^{2^k} - 2a_r x^{2^{k-1}} - 1$ divide a $x^{2^{r+k-1}} + 1$, de lo que inmediatamente se deduce que $x^{2^{k+1}} - 2a_r x^{2^k} - 1$ divide a $x^{2^{r+k}} + 1$. Quedaría probar que es irreducible.

Sean α_1 y α_2 las raíces de $x^2 - 2a_r x - 1$: son elementos de $\mathbb{F}_p^2$ y tienen orden 2^{r+1}. Usando el corolario 2.16 se obtiene que los binomios $x^{2^k} - \alpha_1$ y $x^{2^k} - \alpha_2$ son irreducibles sobre $\mathbb{F}_{p^2}$ para cualquier $k \geq 1$, y por lo tanto su producto es irreducible sobre $\mathbb{F}_p$. Pero dicho producto es justamente $x^{2^{k+1}} - 2a_r x^{2^k} - 1$ el polinomio que se quería estudiar. □

Se aplica este teorema para generar un ejemplo: se van a intentar encontrar trinomios irreducibles de grados 2 y $4 = 2^2$ en $\mathbb{F}_3$. Entonces $p = 3 \equiv 3$ mód 4, como se pide en el enunciado. Además, si se toma $r = 2$, $2^r = 4$ divide exactamente a $p + 1 = 4$.
En este caso, $a_1 = 0$ y $a_2 = a_r = (\frac{a_1-1}{2})^{\frac{p+1}{4}} = -\frac{1}{2}$. El teorema anterior afirma que para cualquier entero $k \geq 1$ el trinomio $x^{2^k} - 2(-\frac{1}{2})x^{2^{k-1}} - 1$ es irreducible. En concreto, si $k = 1$, se obtiene el trinomio irreducible $x^2 + x - 1$. Por otra parte, si $k = 2$, $x^4 + x^2 - 1$ es irreducible en $\mathbb{F}_3$.

2.5. Caso (e)

La siguiente proposición fue demostrada por Meyn en 1990. Se incluye por su utilidad en el teorema de construcción de esta sección.

Proposición 2.18 *Sea q una potencia de primo impar, $P(x)$ un polinomio irreducible de grado $n > 0$ en $\mathbb{F}_q[x]$. El polinomio $x^n P(x + x^{-1}) \in \mathbb{F}_q$ es irreducible si y sólo si $P(2)P(-2) \notin \mathbb{F}_q^{*2}$.*

Demostración: Se considera $x^n P(x + x^{-1}) = g(x)^n P(\frac{f(x)}{g(x)})$, donde $g(x) = x$ y $f(x) = x^2 + 1$. Aplicando el lema 2.3, $x^n P(x + x^{-1})$ es irreducible sobre $\mathbb{F}_q$ si y sólo si $x^2 - \lambda x + 1$ es irreducible sobre $\mathbb{F}_{q^n}$, donde λ es una raíz de P. Para que este polinomio de segundo grado sea irreducible, tiene que ocurrir que su discriminante $\lambda^2 - 4 \notin \mathbb{F}_{q^n}^2$. Pero se tiene que $\lambda^2 - 4$ no es un cuadrado en $\mathbb{F}_{q^n}^2$ si y sólo si $-1 = (\lambda^2 - 4)^{\frac{q^n-1}{2}}$. Además, $(\lambda^2 - 4)^{\frac{q^n-1}{2}} = (((2 - \lambda)(-2 - \lambda))^{\frac{q^n-1}{q-1}})^{\frac{q-1}{2}} = (\prod_{i=0}^{n-1}((2-\lambda)(-2-\lambda))^{q^i})^{\frac{q-1}{2}} = (\prod_{i=0}^{n-1}(2-\lambda^{q^i})(-2-\lambda^{q^i}))^{\frac{q-1}{2}} = (P(2)P(-2))^{\frac{q-1}{2}}$. En consecuencia, $x^2 - \lambda x + 1$ es irreducible si y sólo si $P(2)P(-2)$ no es un cuadrado. □

El siguiente teorema explica cómo construir un binomio de grado r^e irreducible sobre $\mathbb{F}_{p^n}$ para un cierto n. A continuación se utilizan los conceptos de traza y polinomio mínimo para construir otro polinomio de grado r^e irreducible sobre $\mathbb{F}_p$, que al fin y al cabo es lo que se pretendía en un principio.

Teorema 2.19 *Sea p primo, $r \neq p$ primo impar, $n = ord_r(p)$. Sea $f \in \mathbb{F}_p[x]$ un polinomio irreducible de grado n y α una raíz suya en $\mathbb{F}_{p^n}$. Sea $a \in \mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$ que no sea un elemento de $\mathbb{F}_{p^n}^{*r}$. Entonces para todo entero positivo e, el binomio $x^{r^e} - a$ es irreducible en $\mathbb{F}_{p^n}$.*

Además, si β es una raíz de este binomio, entonces $\beta \in \mathbb{F}_{p^{nr^e}}$ y $\gamma = Tr_{\mathbb{F}_{p^{nr^e}},\mathbb{F}_{p^{r^e}}}(\beta) = \sum_{i=0}^{m-1} \beta^{p^{ir^e}}$ tiene grado r^e en $\mathbb{F}_p$. Entonces el polinomio mínimo de γ es irreducible sobre $\mathbb{F}_p$ de grado r^e.

Demostración: Sea m el orden de a en $\mathbb{F}_{p^n}^*$. Como $a \notin \mathbb{F}_{p^n}^r$, r no divide a $\frac{p^n-1}{m}$, así que el binomio $g(x) = x^{r^e} - a$ es irreducible para cualquier entero positivo e, como se ha visto en el corolario 2.16. Así que, si β es una raíz de este binomio, la extensión $\mathbb{F}_{p^n}(\beta)$ es $\mathbb{F}_{p^{nr^e}}$, y por lo tanto $\gamma = Tr_{\mathbb{F}_{p^{nr^e}},\mathbb{F}_{p^{r^e}}}(\beta)$ es un elemento de $\mathbb{F}_{p^{r^e}}$.

Se comprueba ahora que $mcd(n, r) = 1$; en caso contrario, si r divide a n (es decir, $n = rn_0$), se tendría:

$$p^r \equiv p^{rn_0} \equiv p^n \equiv 1 \text{ mód } r$$

y n no sería $ord_r(p)$. Así que $mcd(n, r) = 1$ y, como r es primo, $mcd(n, r^t) = 1$ para cualquier $t > 0$.

Se pretende comprobar que el grado de γ sobre $\mathbb{F}_p$ es r^e; supóngase entonces que el grado de γ sobre $\mathbb{F}_p$ es r^t con $t < e$. Como se ha visto antes que $mcd(n, r^t) = 1$, entonces el grado de γ sobre $\mathbb{F}_{p^n}$ también es r^t. Por otra parte, $[\mathbb{F}_{p^n}(\beta) : \mathbb{F}_{p^n}(\beta^r)] = r$, y $\gamma \in \mathbb{F}_{p^n}(\beta^r)$. Ahora, para cada $0 \leq i \leq n - 1$, sea $p^{ir^e} = x_i r + y_i$ donde $0 < y_i < r$. Como el $ord_r(p) = n$, $ord_r(p^{r^e})$ también es n mód r, y los y_i son todos distintos para cada i. Ahora, utilizando la expresión de γ, $(\beta^r)^{x_0}\beta^{y_0} + ... + (\beta^r)^{x_{m-1}}\beta^{y_{m-1}} - \gamma = 0$, donde, como se ha visto antes, m es el orden de a en

$\mathbb{F}_{p^n}^*$. Por lo tanto β es una raíz de un polinomio (distinto de 0) en $\mathbb{F}_{p^n}(\beta^r)[x]$, y por lo tanto β no tendría grado r sobre $\mathbb{F}_{p^n}(\beta^r)$, lo cual no puede ser. Queda así probado que el grado de γ sobre $\mathbb{F}_p$ es r^e, y con ello el teorema. □

Se utiliza ahora este resultado para construir varios ejemplos:

i) Sobre $\mathbb{F}_2$ ($p = 2$) se construye un polinomio irreducible de grado $r = 3$. Para eso se toma un polinomio de irreducible de grado $n = ord_3(2) = 2$ sobre $\mathbb{F}_2$: $f(x) = x^2 + x + 1$ y α una raíz suya, que permite generar $\mathbb{F}_2[\alpha] = \mathbb{F}_{2^2}$. Además, este mismo elemento $\alpha = a$ no es potencia cúbica en $\mathbb{F}_4$, y por tanto el binomio $x^3 - \alpha$ es irreducible sobre $\mathbb{F}_4$, y se puede generar $\mathbb{F}_{2^6}$ a partir de β una raíz suya. A continuación se calcula $\gamma = Tr_{\mathbb{F}_{2^6},\mathbb{F}_{2^3}}(\beta) = \beta + \beta^{2^3} = (\alpha + 1)\beta^2 + \beta$, y el polinomio mínimo de γ es $x^3 + x + 1$, irreducible sobre $\mathbb{F}_2$ de grado 3, como se pretendía.

ii) Si se aplica el mismo método para calcular un polinomio de grado 5 sobre $\mathbb{F}_2$, se utiliza $f(x) = x^4 + x^3 + x^2 + x + 1$, se obtiene el binomio irreducible $x^5 - \alpha$ sobre $\mathbb{F}_{2^4}$, donde α es una raíz de f. A partir de este binomio se calcula $\gamma = Tr_{\mathbb{F}_{2^6},\mathbb{F}_{2^3}}(\beta)$, cuyo polinomio mínimo es $x^5 + x^2 + 1$ irreducible sobre $\mathbb{F}_2$.

iii) Por último, para generar un polinomio irreducible sobre $\mathbb{F}_3$ de grado 5, siguiendo el mismo método se utilizan $f(x) = x^4 - x - 1$, el binomio $x^5 - \alpha$ con α raíz de f que resulta no ser potencia quinta, y $\gamma = Tr_{\mathbb{F}_{3^{20}},\mathbb{F}_{3^5}}(\beta)$ con β raíz del binomio. El polinomio mínimo de γ es $x^5 + x^3 + x + 2$ irreducible sobre $\mathbb{F}_3$.

2.6. Juntando los polinomios

Ya se ha visto que es posible generar polinomios irreducibles sobre $\mathbb{F}_p$ de grado r^e para r primo y e entero. El objetivo principal de este capítulo, sin embargo, era generar polinomios irreducibles de grado $n = r_1^{e_1} r_2^{e_2} ... r_l^{e^l}$; para ello, en esta sección se ofrecen formas de operar con los polinomios de grados $r_i^{e^i}$ obtenidos anteriormente para obtener polinomios irreducibles de grado n sobre $\mathbb{F}_p$.

Teorema 2.20 *Sean f y g dos polinomios irreducibles de grados m y n sobre $\mathbb{F}_q$, cumpliendo $mcd(m, n) = 1$. Sean $\alpha_1 ... \alpha_m$ y $\beta_1 ... \beta_n$ las raíces de estos polinomios en $\mathbb{F}_{q^m}$ y $\mathbb{F}_{q^n}$. Entonces:*

$$(f \odot g)(x) = \prod_{i=1}^{m} \prod_{j=1}^{n} (x - \alpha_i \beta_j)$$

y

$$(f \oplus g)(x) = \prod_{i=1}^{m} \prod_{j=1}^{n} (x - (\alpha_i + \beta_j))$$

son ambos polinomios irreducibles de grado mn sobre $\mathbb{F}_q$.

Demostración: Como $\alpha_1 ... \alpha_m$ y $\beta_1 ... \beta_n$ son las raíces de f y g, se puede asumir que están ordenadas de la siguiente manera: $\alpha_1^q = \alpha_2$, $\alpha_2^q = \alpha_3$... y, del mismo modo, $\beta_1^q = \beta_2$, $\beta_2^q = \beta_3$... Como $mcd(m, n) = 1$, esto se puede aplicar a $\alpha_i \beta_j$ y a $\alpha_i + \beta_j$ para ir obteniendo todas las combinaciones posibles para cada i y j. Aplicando el lema 1.12, $f \odot g$ es el polinomio mínimo de $\alpha_1 \beta_1$ y $f \oplus g$ es el de $\alpha_1 + \beta_1$; se deduce trivialmente que por lo tanto su grado es mn y son

irreducibles sobre $\mathbb{F}_q$. $\square$

Definición 2.21 *Los polinomios anteriores $f \odot g$ y $f \oplus g$ son, respectivamente, el* ***producto compuesto*** *y la* ***suma compuesta*** *de f y g.*

Si $f(x) = x^m + a_{m-1}m^{m-1} + ... + a_1x + a_0$ y $g(x) = x^n + b_{n-1}x^{n-1} + ... + b_1x + b_0$ son polinomios mónicos, entonces se pueden definir las matrices compañeras:

$$A = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & \vdots \\ & & & 1 & -a_{m-1} \end{pmatrix} \qquad B = \begin{pmatrix} 0 & & & & -b_0 \\ 1 & 0 & & & -b_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & \vdots \\ & & & 1 & -b_{n-1} \end{pmatrix}$$

cuyos polinomios característicos $det(A - xI_m)$, $det(B - xI_n)$ son precisamente f y g. A continuación se proporcionará una manera alternativa de calcular $f \odot g$ y $f \oplus g$ sin necesidad de conocer sus raíces. Para ello, es necesario definir el producto de Kronecker:

Definición 2.22 *Sean*

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix} \; y \; B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$$

dos matrices cuadradas, no necesariamente de la misma dimensión. El ***producto de Kronecker*** *de A y B es la siguiente matriz:*

$$A \otimes B = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & \cdots & a_{11}b_{1n} & \cdots & \cdots & a_{1m}b_{11} & a_{1m}b_{12} & \cdots & a_{1m}b_{1n} \\ a_{11}b_{21} & a_{11}b_{22} & \cdots & a_{11}b_{2n} & \cdots & \cdots & a_{1m}b_{21} & a_{1m}b_{22} & \cdots & a_{1m}b_{2n} \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \cdots & \vdots \\ a_{11}b_{n1} & a_{11}b_{n2} & \cdots & a_{11}b_{nn} & \cdots & \cdots & a_{1m}b_{n1} & a_{1m}b_{n2} & \cdots & a_{1m}b_{nn} \\ \vdots & \vdots & & \vdots & \ddots & & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots & & \ddots & \vdots & \vdots & & \vdots \\ a_{m1}b_{11} & a_{m1}b_{12} & \cdots & a_{m1}b_{1n} & \cdots & \cdots & a_{mm}b_{11} & a_{mm}b_{12} & \cdots & a_{mm}b_{1n} \\ a_{m1}b_{21} & a_{m1}b_{22} & \cdots & a_{m1}b_{2n} & \cdots & \cdots & a_{mm}b_{21} & a_{mm}b_{22} & \cdots & a_{mm}b_{2n} \end{pmatrix}$$

En concreto, si A y B son las matrices compañeras de f y g, entonces es de inmediata comprobación que:

$$f \odot g = det(xI_{mn} - A \otimes B) \text{ y } f \oplus g = det(xI_{mn} - A \otimes I_n - I_m \otimes B)$$

Esto permite aplicar el teorema 2.20 para calcular polinomios irreducibles de grado mn sobre $\mathbb{F}_q$ sin necesidad de conocer las raíces de f y g.

Por ejemplo, se van a usar estos resultados junto con los ejemplos vistos en las anteriores secciones para generar polinomios de grado $60 = 2^2 \cdot 3 \cdot 5$ irreducibles sobre $\mathbb{F}_2$ y $\mathbb{F}_3$.

Para el caso de $\mathbb{F}_2$ se utilizarán los polinomios $f(x) = x^4 + x^3 + x^2 + x + 1$, $g(x) = x^3 + x + 1$ y $h(x) = x^5 + x^2 + 1$; el producto de sus grados es 60, y se ha visto antes que son irreducibles sobre $\mathbb{F}_2$. Al usar el método que se ha explicado en esta sección, se obtiene:

$$(f \odot g)(x) = x^{12} + x^{10} + x^9 + x^8 + x^7 + x^4 + x^2 + x + 1$$

irreducible de grado 12. Ahora se puede repetir este procedimiento usando el polinomio de grado 5 para hallar un polinomio irreducible de grado 60 sobre $\mathbb{F}_2$:

$$((f \odot g) \odot h)(x) = x^{60} + x^{57} + x^{54} + x^{48} + x^{47} + x^{46} + x^{40} + x^{39} + x^{36} + x^{33} + x^{30}$$

$$+x^{27} + x^{26} + x^{25} + x^{24} + x^{22} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{11} + x^8 + x^7 + x^4 + x^2 + 1$$

En el caso de $\mathbb{F}_3$, los polinomios irreducibles que se van a utilizar van a ser $f(x) = x^4 + x^2 - 1$, $g(x) = x^3 - x - 1$ y $h(x) = x^5 + x^3 + x - 1$. Entonces:

$$(f \odot g)(x) = x^{12} + 2x^{10} + 2x^8 + 2x^6 + x^4 + x^2 + 2$$

es un polinomio irreducible de grado 12 sobre $\mathbb{F}_3$, y

$$((f \odot g) \odot h)(x) = x^{60} + 2x^{58} + 2x^{56} + x^{54} + 2x^{52} + x^{48} + 2x^{46} + x^{44} + x^{42} + 2x^{38} + 2x^{36}$$

$$+2x^{34} + x^{28} + x^{26} + x^{24} + x^{22} + 2x^{20} + x^{16} + 2x^{14} + x^{12} + x^6 + x^4 + x^2 + 2$$

es un polinomio irreducible de grado 60 sobre $\mathbb{F}_3$, como se quería.

Capítulo 3

Número de polinomios irreducibles

En el capítulo de Preliminares se ha visto que un cuerpo finito de p^n elementos puede construirse a partir de un polinomio irreducible de grado n sobre $\mathbb{F}_p$. Los resultados expuestos en el capítulo 2 han permitido dar un algoritmo para construir dichos polinomios irreducibles. Estas construcciones no son generales; es decir, no construyen cualquier polinomio de grado fijo, sino uno en particular. En este capítulo se determinará, dados q una potencia de primo y n un entero, cuántos polinomios irreucibles de grado n existen sobre $\mathbb{F}_q$. Primero se tratará el caso general, para posteriormente determinar el número de polinomios irreducibles con algunas características particulares.

El teorema siguiente, demostrado inicialmente por Gauss, responde a la primera cuestión sobre el número de polinomios irreducibles, y se puede encontrar en la referencia [10].

Teorema 3.1 (Fórmula de Gauss) *El número $N_q(n)$ de polinomios mónicos, irreducibles sobre $\mathbb{F}_q[x]$ de grado n viene dado por:*

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

Demostración: Como $\mathbb{F}_q$ es un cuerpo, $q = p^k$ es una potencia de un primo.

Se define $M(q,n) = \{f \in \mathbb{F}_q[X]$ tal que f es mónico e irreducible, y $\delta(f)|n\}$.

Claramente, del lema 1.12 se deduce que:

$$\prod_{f \in M(q,n)} f = \prod_{a \in \mathbb{F}_{q^n}} (X - a) = X^{q^n} - X$$

Tomando el grado en ambos lados,

$$\delta(\prod_{f \in M(q,n)} f) = \delta(\prod_{a \in \mathbb{F}_{q^n}} (X - a))$$

$$\sum_{f \in M(q,n)} \delta(f) = q^n$$

Pero,

$$\sum_{d|n} dN_q(d) = \sum_{f \in M(q,n)} \delta(f) = q^n$$

Usando el teorema de inversión de la función de Möbius, tomando $f(n) = q^n$ y $g(d) = dN_q(n)$ se obtiene:

$$nN_q(n) = \sum_{d|n} q^d \mu(\frac{n}{d})$$

□

Un ejemplo de aplicación del teorema es el siguiente: el número de polinomios irreducibles de grado 30 en $\mathbb{F}_2$ es $35790267 = \frac{1}{30}(2^{30} - 2^{15} - 2^{10} - 2^6 + 2^5 + 2^3 + 2^2 - 2)$.

La demostración que se acaba de dar hace uso de la función de Möbius, de su fórmula de inversión (ver 1.24) y del lema 1.12. A continuación se ofrece una prueba del mismo resultado haciendo uso del principio de inclusión-exclusión. Más detalles sobre esta prueba se pueden encontrar en la referencia [5]. Se incluye la siguiente demostración por su simplicidad y porque ayuda fácilmente a entender el significado de los términos que aparecen en la fórmula $\frac{1}{n}\sum_{d|n} \mu(d) q^{\frac{n}{d}}$: tanto los $q^{\frac{n}{d}}$, como el signo que los acompaña, dado por $\mu(d)$.

En primer lugar se va a tratar el caso $n = 1$: el número de polinomios irreducibles de grado 1 en $\mathbb{F}_q$ es q. En efecto, son todos de la forma $(X - a)$ para todo $a \in \mathbb{F}_q$. Este es el mismo valor que se obtiene sustituyendo en la fórmula que se quiere demostrar.

Ahora, suponiendo $n > 1$, se definen los conjuntos

$$P_n = \{f \text{ mónicos, irreducibles de grado } n \text{ sobre } \mathbb{F}_q\}$$

$$R_n = \{a \in \mathbb{F}_{q^n} : f(a) = 0 \text{ para algún } f \in P_n\}$$

Claramente, cada polinomio de P_n tiene exactamente n raíces. Entonces el cardinal de R_n es

$$|R_n| = n|P_n|$$

Por eso basta con calcular $|R_n|$ para demostrar el resultado.

Además, $R_n = \{a \in \mathbb{F}_{q^n}, a \notin \mathbb{F}_{q^r}, r < n\}$
$= \{a \in \mathbb{F}_{q^n} | a \text{ no está en ningún subcuerpo propio de } \mathbb{F}_{q^n}\}$
$= \{a \in \mathbb{F}_{q^n} | a \text{ no está en ningún subcuerpo propio, maximal de } \mathbb{F}_{q^n}\}$

En efecto: como los subcuerpos propios y maximales contienen a todos los demás subcuerpos propios, la contención del primero en el segundo es trivial. En el otro sentido, si a no está en ningún subcuerpo propio maximal, tampoco puede estar en otro subcuerpo contenido en él.

Después de haber eliminado el caso $n = 1$, se procede a descomponer $n = p_1^{r_1} ... p_k^{r_k}$ como producto de potencias de primos. Se obtiene entonces que los subcuerpos propios maximales de $\mathbb{F}_{q^n}$ son de la forma $F_1 = \mathbb{F}_{q^{\frac{n}{p_1}}}, ... F_k = \mathbb{F}_{q^{\frac{n}{p_k}}}$. Además, las intersecciones de estos cuerpos son precisamente: $F_a \bigcap F_b = \mathbb{F}_{q^{\frac{n}{p_a p_b}}}$, $F_a \bigcap F_b \bigcap F_c = \mathbb{F}_{q^{\frac{n}{p_a p_b p_c}}}$ ... etc. (Se deduce del teorema 1.11)

Entonces $|R_n| = |(F_1 \bigcup ... \bigcup F_k)^C|$. Para calcular este cardinal se usa el principio de inclusión-exclusión:

$$|R_n| = |\mathbb{F}_{q^n}| - \sum_{i=1}^{k} |\mathbb{F}_{q^{\frac{n}{p_i}}}| + \sum_{1 \leq i < j \leq k} |\mathbb{F}_{q^{\frac{n}{p_i p_j}}}| - ... + (-1)^k |\mathbb{F}_{q^{\frac{n}{p_1 \cdots p_k}}}|$$

Se puede expresar esta fórmula utilizando la función de Möbius así:

$$|R_n| = \sum_{d|n} \mu(d) |\mathbb{F}_{q^{\frac{n}{d}}}| = \sum_{d|n} \mu(d) q^{\frac{n}{d}}$$

Sustituyendo de lo obtenido antes, se llega al resultado que se busca. □

Esta demostración puede interpretarse de forma más visual a partir del lema 1.12, teniendo en cuenta las contenciones entre los diversos cuerpos finitos (ver figura 3.1).

Para comprobarlo, se estudia el ejempo $q = 2, n = 30$: se pretende hallar el número de polinomios de grado 30 que hay en $\mathbb{F}_2$. Se comienza entonces por el cuerpo $\mathbb{F}_{2^{30}}$:

$$30N_2(30) = 2^{30} + ...$$

Los subcuerpos maximales de $\mathbb{F}_{2^{30}}$ son $\mathbb{F}_{2^{15}}$, $\mathbb{F}_{2^{10}}$ y $\mathbb{F}_{2^6}$: se restan sus cardinales de la fórmula:

$$30N_2(30) = 2^{30} - 2^{15} - 2^{10} - 2^6 + ...$$

A continuación se suman los cardinales de las intersecciones: $\mathbb{F}_{2^5}$ es intersección de $\mathbb{F}_{2^{10}}$ y $\mathbb{F}_{2^{15}}$, etc... Como están indicadas en la figura:

$$30N_2(30) = 2^{30} - 2^{15} - 2^{10} - 2^6 + 2^5 + 2^3 + 2^2 + ...$$

En este ejemplo concreto, sólo quedaría restar el cardinal de $\mathbb{F}_2$, que es la única intersección triple:

$$30N_2(30) = 2^{30} - 2^{15} - 2^{10} - 2^6 + 2^5 + 2^3 + 2^2 - 2$$

Multiplicando toda la ecuación por $\frac{1}{30}$ se obtiene el resultado deseado.

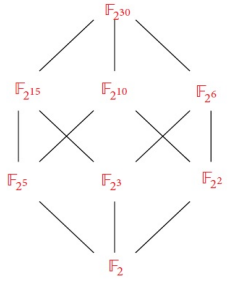


Figura 3.1: Estructura de subcuerpos

Se estudian ahora varios resultados acerca del producto de los polinomios mónicos irreducibles de cierto grado, enfocados a dar otra fórmula que permita calcular $N_q(n)$ utilizando la función de Euler. El siguiente lema es ampliamente conocido en el ámbito de cuerpos finitos, y puede encontrarse en [6], [10] y [13].

Lema 3.2 *Sean $\mathbb{F}_q$ un cuerpo finito, n un número natural. El producto de todos los polinomios mónicos, irreducibles cuyo grado divide a n es $I_q(n) = x^{q^n} - x$.*

Demostración: Se comienza probando que todo polinomio en $\mathbb{F}_q$ irreducible, mónico y cuyo grado divide a n es un factor de $x^{q^n} - x$: sea $f(x)$ un polinomio en las condiciones anteriores, de tal forma que $n = dr$, siendo d el grado de f. Si $\mathbb{F}_q(\alpha)$ es un cuerpo raíz de f sobre $\mathbb{F}_q$, se tiene que $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = d$ y por tanto $|\mathbb{F}_q(\alpha)| = q^d$, de lo que se deduce que $\alpha^{q^d} = \alpha$. Resulta entonces que $\alpha^{q^n} = \alpha^{q^{dr}} = \alpha^{(q^d)^r}$; es decir, α^{q^d} r veces, que resulta ser α. Por tanto, $\alpha^{q^n} = \alpha$. Se obtiene entonces que α es raíz de $x^{q^n} - x$, y que f es divisor del polinomio.

Se considera ahora f un factor irreducible, mónico de grado d de $x^{q^n} - x$, y K un cuerpo de escisión de $x^{q^n} - x$ sobre $\mathbb{F}_q$. Hay que comprobar que d divide a n (es decir, que los factores de $x^{q^n} - x$ son sólo los que se especifica y ninguno más). Si α es una raíz de f, $\mathbb{F}_q(\alpha) \subseteq K$. La siguiente ecuación:

$$[K : \mathbb{F}_q] = [K : \mathbb{F}_q(\alpha)][\mathbb{F}_q(\alpha) : \mathbb{F}_q]$$

Permite alcanzar el resultado deseado, dado que $[K : \mathbb{F}_q] = n$ y, como antes, $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = d$. □

De este lema se deduce fácilmente el siguiente resultado:

Teorema 3.3 *El producto $I_q(n)$ de todos los polinomios mónicos, irreducibles de grado n en $\mathbb{F}_q[x]$ es:*

$$I_q(n) = \prod_{d|n} (x^{q^d} - x)^{\mu(\frac{n}{d})} = \prod_{d|n} (x^{q^{\frac{n}{d}}} - x)^{\mu(d)}$$

Demostración: Como se ha visto en el lema anterior, $x^{q^n} - x = \prod_{d|n} I_q(d)$. Se aplica el teorema de inversión de la función de Möbius (1.24) en el caso multiplicativo, con la notación precedente: $f(n) = x^{q^n} - x$ y $g(d) = N_q(d)$; entonces $g(n) = I_q(n) = \prod_{d|n} f(d)^{\mu(\frac{n}{d})} = \prod_{d|n} (x^{q^d} - x)^{\mu(\frac{n}{d})}$ □

El siguiente resultado, al igual que los anteriores, estudia el producto de todos los polinomios mónicos e irreducibles de grado n sobre $\mathbb{F}_q$. Se puede encontrar en la referencia [10].

Teorema 3.4 *El producto $I_q(n)$ de todos los polinomios mónicos, irreducibles de grado n en $\mathbb{F}_q[x]$ también se puede expresar de la siguiente manera:*

$$I_q(n) = \prod_{m|(q^n-1)} \phi_m(x)$$

siendo ϕ_m el polinomio ciclotómico de orden m.

Demostración: Sea $S = \{\alpha \in \mathbb{F}_{q^n} |$ el grado de α sobre $\mathbb{F}_q$ es $n\}$. Se tiene que α es un elemento de S si y sólo si es raíz de $I_q(n)$. Esto es fácil de ver: si α es un elemento de S, entonces su polinomio mínimo será mónico, irreducible y de grado n. Por tanto α es raíz de $I_q(n)$. Por el contrario, si α es raíz de $I_q(n)$, entonces es raíz de un polinomio mónico, irreducible de grado n sobre $\mathbb{F}_q$; es decir, α es un elemento de S. Entonces $I_q(n) = \prod_{\alpha \in S} (x - \alpha)$.

Sea ahora m el orden de α, (es decir, el menor número que cumple $\alpha^m = 1$). Como α es un elemento de $\mathbb{F}^*_{q^n}$, m es divisor de $q^n - 1$. Se considera la partición de S en los conjuntos

$S_m = \{\alpha \in S |$ su orden es $m\}$. Retomando la fórmula anterior, $I_q(n) = \prod_{m|q^n-1} \prod_{\alpha \in S_m} (x - \alpha)$.

Por último, sólo queda considerar que en realidad S_m es el conjunto de raíces m-ésimas de la unidad sobre $\mathbb{F}_q$, y se obtiene $I_q(n) = \prod_{m|(q^n-1)} \phi_m(x)$, como se quería. □

Estos resultados permiten dar otra forma de calcular $N_q(n)$ utilizando la función de Euler. La siguiente fórmula también se puede encontrar en la referencia [13].

Teorema 3.5 *Sean un cuerpo $\mathbb{F}_q$, n un número natural. Se define $D_n = \{r : r|(q^n - 1)$ pero r no divide a $q^m - 1\ \forall m < n\}$. El número $N_q(n)$ de polinomios mónicos, irreducibles sobre $\mathbb{F}_q[x]$ de grado n es:*

$$N_q(n) = \frac{1}{n} \sum_{r \in D_n} \varphi(r)$$

Demostración: Se sabe que el polinomio ciclotómico de orden n factoriza de la siguiente manera: $\phi_n(x) = \prod_{f \in P(n,q,r)} f$ donde $P(n, q, r)$ es el conjunto de polinomios mónicos, irreducibles, de grado n y orden r sobre $\mathbb{F}_q$. Igualando los grados de ambos lados de la descomposición, $n|P(n, q, r)| = \varphi(r)$. Es decir, se obtiene $|P(n, q, r)| = \frac{\varphi(r)}{n}$.

Como lo que se quiere hallar es el número de polinomios mónicos, irreducibles de grado n en $\mathbb{F}_q[x]$ independientemente de su orden, se considerarán los conjuntos $P(n, q, r)$ para todos los r posibles: es decir, todo r en D_n. Sumando los cardinales de todos estos conjuntos se obtiene la fórmula deseada: $N_q(n) = \frac{1}{n} \sum_{r \in D_n} \varphi(r)$. □

Hasta este momento se ha calculado el número de polinomios mónicos e irreducibles en $\mathbb{F}_q$ de varias maneras, pero las fórmulas obtenidas no proporcionan información demasiado útil acerca de su tamaño a simple vista. Por ello se presenta a continuación un resultado acerca de las cotas inferior y superior de $N_q(n)$, así como un breve estudio acerca del comportamiento asintótico de este número y de su densidad sobre la cantidad de polinomios total en un cuerpo finito. Se puede encontrar más información sobre el comportamiento de $N_q(n)$ en la referencia [3].

Teorema 3.6 *El número $N_q(n)$ de polinomios mónicos, irreducibles sobre $\mathbb{F}_q[x]$ de grado n (siendo $q = p^n$ potencia de primo) está acotado de la siguiente forma:*

$$\frac{q^n}{n} - 2\frac{q^{\frac{n}{2}}}{n} < N_q(n) \leq \frac{q^n}{n}$$

Demostración: En el caso $n = 1$, sustituyendo se obtiene $q - 2\sqrt{q} < q \leq q$, que es correcto. Se estudia ahora lo que ocurre cuando $n > 1$. Para la desigualdad de la derecha, basta con ver que $\frac{q^n}{n} - N_q(n)$ es mayor que 0.

$$\frac{q^n}{n} - N_q(n) = \frac{1}{n}(q^n - \sum_{d|n} q^d \mu(\frac{n}{d})) = -\frac{1}{n} \sum_{d|n, d \neq n} q^d \mu(\frac{n}{d})$$

Sea p' el factor primo más pequeño de n. Entonces lo anterior:

$$-\frac{1}{n} \sum_{d|n, d \neq n} q^d \mu(\frac{n}{d}) = \frac{1}{n}(q^{\frac{n}{p'}} - \sum_{d|n, d < \frac{n}{p'}} q^d \mu(\frac{n}{d}))$$

Evidentemente,

$$q^{\frac{n}{p'}} - \sum_{d|n, d\leq \frac{n}{p'}} q^d \mu(\frac{n}{d}) \geq q^{\frac{n}{p'}} - \sum_{1\leq d\leq \frac{n}{p'}} q^d \geq q^{\frac{n}{p'}} - \frac{q^{\frac{n}{p'}} - q}{q-1}$$

La primera desigualdad se cumple porque, al quitar la función μ, todos los términos del sumatorio pasan a tener signo negativo, mientras que antes algunos tenían signo positivo y otros eran 0. La segunda desigualdad se deduce fácilmente de la fórmula de una progresión geométrica.

Como q es potencia de primo, $q \geq 2$ y $q^{\frac{n}{p'}} - \frac{q^{\frac{n}{p'}}-q}{q-1} \geq q^{\frac{n}{p'}} - q^{\frac{n}{p'}} + q = q > 0$, como se buscaba.

Para la cota inferior, basta con fijarse en que $q^{\frac{n}{p'}} + \frac{q^{\frac{n}{p'}}-q}{q-1} < 2q^{\frac{n}{2}}$, y sustituyendo como antes se obtiene $N_q(n) > \frac{q^n}{n} - 2\frac{q^{\frac{n}{2}}}{n}$ □

Es interesante además estudiar el comportamiento asintótico de $N_q(n)$. Se ha visto en el teorema 3.6 que $\frac{q^n}{n} - 2\frac{q^{\frac{n}{2}}}{n} < N_q(n) \leq \frac{q^n}{n}$; de esta expresión se deduce inmediatamente que $N_q(n) = \frac{q^n}{n} + \mathcal{O}(\frac{q^{\frac{n}{2}}}{n})$. Dividiendo toda la fórmula entre $\frac{q^n}{n}$ y teniendo en cuenta que $\frac{q^{\frac{n}{2}}}{q^n} = q^{-\frac{n}{2}}$ tiende a 0 cuando n tiende a infinito, se obtiene que $lim_{n\to\infty} \frac{N_q(n)}{\frac{q^n}{n}} = 1$, y, por lo tanto, que $N_q(n)$ se aproxima a $\frac{q^n}{n}$ cuando n tiende a infinito.

Se observa, por tanto, que la densidad de los polinomios irreducibles de grado n es aproximadamente $\frac{1}{n}$.

3.1. Autorrecíprocos

Se recuerda que un polinomio autorrecíproco es aquel f que cumple $f(x) = x^n f(\frac{1}{x})$, donde n es el grado de f. A continuación se presenta una serie de resultados que facilitarán la tarea de contar cuántos polinomios irreducibles, mónicos y autorrecíprocos hay en un cuerpo finito. Estos resultados pueden encontrarse en la referencia [11].

A fin de simplificar el texto, a partir de ahora se dirá que un polinomio f es *"srim"* (self-reciprocal irreducible monic polynomials) si cumple justamente estas características: autorrecíproco, mónico e irreducible.

Lema 3.7 *Sea f un polinomio en $\mathbb{F}_q[x]$.*

i) Si f es autorrecíproco entonces para todo α raíz de f, α^{-1} también es raíz de f.

ii) Por el contrario, dado f irreducible que cumple que si α es raíz de f, α^{-1} raíz de f, entonces f^* es:

  i) $-f(x)$ si $f(x) = x - 1$ y $q \neq 2$
  ii) $f(x)$ en todos los demás casos.

iii) Si f es autorrecíproco y 1 o -1 no son una de sus raíces, entonces $\delta(f)$ es par.

Demostración:

i) La primera propiedad se comprueba de manera obvia aplicando la definición.

ii) Se esstudian los dos casos:

   i) Si $f(x) = x - 1$, se comprueba imnediatamente a partir de la definición que se cumple el enunciado.

   ii) Sea $f(x) = a_0 + ... + a_n x^n$ un polinomio irreducible para el que, si α es raíz suya, α^{-1} también lo es. Su polinomio recíproco es $f^*(x) = a_n + ... + a_0 x^n$, aplicando la fórmula dada en la definición. Susutituyendo se obtiene que, para todo α raíz de f, α^{-1} es raíz de f^*. Pero, además, α^{-1} es raíz de f, y aplicando este mismo razonamiento, $(\alpha^{-1})^{-1} = \alpha$ es raíz de f^*. Por lo tanto las raíces de f y f^* coinciden, su descomposición es la misma en el cuerpo de escisión que corresponda y son, necesariamente, el mismo polinomio o el opuesto uno del otro: pero este último caso no puede ocurrir pues al hacer la transformación de f a f^* el signo de los coeficientes no varía.

iii) La tercera parte del lema se deduce trivialmente de la segunda. □

Una consecuencia que se puede extraer del lema anterior es que todos los polinomios srim excepto $x+1$ y $x-1$ tienen grado par: por tanto será interesante estudiar el número de polinomios srim de grado $2n$ que hay en $\mathbb{F}_q[x]$. Se presenta a continuación una expresión para el producto de todos estos polinomios; aunque Carlitz dio la primera prueba del resultado en [4], la que se expone en este trabajo es de Meyn ([11]).

Teorema 3.8 *Sea $H_{q,n}(x) := x^{q^n+1} - 1$. Se tiene:*

i) Cada polinomio srim de grado $2n$ en $\mathbb{F}_q[x]$ es un factor de $H_{q,n}(x)$.

ii) Cada factor de $H_{q,n}(x)$ con grado mayor o igual que 2 es un polinomio srim de grado $2d$ cumpliendo que d divide a n y $\frac{n}{d}$ es impar.

Demostración:

i) Sea f un polinomio en las condiciones del enunciado anterior. Si α es una raíz suya en el cuerpo de escisión $\mathbb{F}_{q^{2n}}$, entonces $R := \{\alpha, \alpha^q, \alpha^{q^2} ... \alpha^{q^{2n}-1}\}$ son todas sus raíces en $\mathbb{F}_{q^{2n}}$. Como es autorrecíproco, se sigue de la primera parte del lema anterior que existe un j en $\{0, 1, .., 2n-1\}$ tal que $\alpha^{q^j} = \alpha^{-1}$ (es una de sus raíces), y por lo tanto α es raíz de $H_{q,j}(x) = x^{q^j+1} - 1$.
Dado que $q^{2j} - 1 = (q^j + 1)(q^j - 1)$, se tiene que $H_{q,j}$ a su vez divide a $x^{q^{2j}-1} - 1$. Además, f divide a $x^{q^{2n}-1} - 1$: $\alpha^{q^{2n}-1}$ es, por un lado, raíz de f, y por otro unidad del grupo R, cuyo orden es $2n$. Esto significa que cumple la ecuación $\alpha^{2n} = 1$ y también es raíz de $x^{q^{2n}-1} - 1$. Se tiene entonces que $2n$ divide a $2j$, y por tanto $j = n$; es decir, f es un factor de $H_{q,n}(x)$.

ii) Sea ahora g un factor irreducible (de grado d mayor o igual que 2) de $H_{q,n}$: se pretende probar que es un polinomio autorrecíproco, de forma que d divide a n y $\frac{n}{d}$ es impar.
Sea α una raíz de g: como g es factor de $H_{q,n}$, entonces se cumple que $\alpha^{q^n+1} - 1 = 0$ (pues es raíz suya), y, despejando, se obtiene $\alpha^{q^n} = \alpha^{-1}$. De aquí se deduce que si α es raíz de g, también lo es α^{-1}. De hecho, como en el anterior caso, el conjunto de raíces es $\{\alpha, \alpha^q, \alpha^{q^2} ... \alpha^{q^d-1}\}$, y si se siguen tomando potencias de α de la misma forma, se siguien obteniendo raíces de las que ya se tienen. Usando la segunda parte del lema anterior se concluye que g es por tanto un polinomio autorrecíproco de grado $d = 2t$ divisor de $2n$

(usando un argumento similar al del apartado anterior), y por tanto factor de $H_{q,d}$. Como $H_{q,d}$ es a su vez factor de $H_{q,n}$, q^d+1 divide a q^n-1 y $\frac{n}{d}$ es impar. □

Es posible ahora enunciar el resultado que se buscaba sobre el número de polinomios srim de grado $2n$ sobre $\mathbb{F}_q$:

Teorema 3.9 *El número de polinomios srim sobre $\mathbb{F}_q$ de grado $2n$ es:*

i) $\frac{1}{2n}\sum_{d|n,dimpar}\mu(d)(q^{\frac{n}{d}}-1)$ *si q es impar.*

ii) $\frac{1}{2n}\sum_{d|n,dimpar}\mu(d)q^{\frac{n}{d}}$ *si q es potencia de 2.*

Demostración: Se considera $R_{q,n}(x)$ el producto de todos los polinomios srim de grado $2n$ sobre $\mathbb{F}_q$. Con la notación precedente, se tiene que:

$$H_{q,n}(x)=(x^{1+e_q}-1)\prod_{d|n,\frac{n}{d}impar}R_{q,d}(x)$$

donde $e_q\equiv q$ mód 2. Es decir: si q es par, se multiplica por $x+1$, y si es impar, por $x^2-1=(x+1)(x-1)$, que son el producto de polinomios srim de grado 1 en cada caso.

Se define entonces $H^0_{q,n}:=\frac{H_{q,n}}{(x^{1+e_q}-1)}$, que será por tanto $H^0_{q,n}=\prod_{d|n,\frac{n}{d}impar}R_{q,d}(x)$. Ahora es posible aplicar a esta igualdad la fórmula de inversión de Möebius; con la notación del Teorema 1.24, se tiene $f(n)=H^0_{q,n}(x)$ y $g(d)=R_{q,d}(x)$. Se obtiene por tanto:

$$R_{q,n}(x)=\prod_{d|n,\frac{n}{d}impar}H^0_{q,\frac{n}{d}}(x)^{\mu(d)}$$

Para deducir el número de polinomios srim de grado $2n$ basta con calcular el grado de $R_{q,n}(x)$; como el grado de cada srim es $2n$, el grado de $R_{q,n}(x)$ será $2n$ multiplicado por el número de srims. Además, dicho grado será igual al de $\prod_{d|n,\frac{n}{d}impar}H^0_{q,\frac{n}{d}}(x)$.

Teniendo presente que, si q es par, $H^0_{q,\frac{n}{d}}(x)=\dfrac{x^{q^{\frac{n}{d}+1}}-1}{x+1}$, el grado del producto anterior será $\sum_{d|n,\frac{n}{d}impar}\mu(d)(q^{\frac{n}{d}}+1-1)=\sum_{d|n,\frac{n}{d}impar}\mu(d)q^{\frac{n}{d}}$. Por tanto, en el caso de q par el número de polinomios srim es $\frac{1}{2n}\sum_{d|n,dimpar}\mu(d)q^{\frac{n}{d}}$.

En el caso en el que q es impar, el razonamiento es análogo pero hay que tener en cuenta que $H^0_{q,\frac{n}{d}}(x)=\frac{x^{q^{\frac{n}{d}+1}}-1}{x^2-1}$; por tanto el grado del producto será $\sum_{d|n,\frac{n}{d}impar}\mu(d)(q^{\frac{n}{d}}-1)$, y el número de

polinomios srim es $\frac{1}{2n}\sum_{d|n,dimpar}\mu(d)(q^{\frac{n}{d}}-1)$. □

A modo de ejemplo se estudia el caso en el que $q=2$ y $n=15$: es decir, se va a calcular el número de polinomios srim de grado 30 que hay en $\mathbb{F}_2$.
Como en este caso q es una potencia de 2, se utiliza la segunda parte de la fórmula, y el número que se obtiene es:

$$\frac{1}{30}\sum_{d|15,dimpar}\mu(d)2^{\frac{15}{d}}$$

que, desarrollando, es: $\frac{1}{30}(\mu(1)2^{15}+\mu(3)2^5+\mu(5)2^3+\mu(15)2)=\frac{1}{30}(2^{15}-2^5-2^3+2)=1091$.
Ahora que se dispone de esta cifra es posible compararla con la del número total de polinomios irreducibles de grado 30 en $\mathbb{F}_2$, que, como se ha visto antes, es 35790267. Se observa así que los polinomios srim son sólo un pequeño porcentaje de los irreducibles.

3.2. Invariantes por traslación

Definición 3.10 *Un elemento f de $\mathbb{F}_q[x]$ es **invariante por traslación** si $f(x+b)=f(x)$ para todo $b\in\mathbb{F}_q$*

Se pretende a continuación calcular el número de polinomios mónicos e irreducibles de este tipo que existen en un cuerpo finito. Para ello es necesario conocer algunos resultados previos. Esta sección se apoya en la referencia [7].

Se comienza determinando para cada polinomio invariante por traslación un entero que depende de la estructura del conjunto formado por sus raíces, y que será de importancia en el estudio de este tipo de polinomios.

Proposición 3.11 *Sea $\mathbb{F}_q$ un cuerpo de característica p, f un polinomio mónico, irreducible e invariante por traslación de grado $n\geq 2$ y θ una raíz suya. Se tiene que p divide a n ($n=pm$), el conjunto $\{s\in\mathbb{N}:\theta^{q^s}=\theta-b\}$ es no vacío y su elemento mínimo r cumple $0<r<pm$ y m divide a r.*

Demostración: Como f es invariante por traslación y θ es una raíz suya, también lo es $\theta-b$. Por lo tanto existe un número natural s, con $0<s<n$, tal que $\theta^{q^s}=\theta-b$ (s es distinto de 0, porque si no b tendría que ser siempre 0). Es decir, el conjunto es no vacío, y tiene un elemento mínimo, r.

Este número r cumple $\theta^{q^r}=\theta-b$, y $0<r<n$ (está tomado de la misma forma que s en el conjunto anterior). Además, dado que $\theta^{q^{jr}}=\theta-jb$, $\theta^{pr}=\theta$ (tener en cuenta la característica del cuerpo). Esto indica que n (el grado de f) divide a pr; existe x entero tal que $pr=nx$. Se puede decir entonces que p divide a nx. Además, como p es primo, tiene que dividir a n o a x.

Si p no divide a n, entonces obligatoriamente divide a x, y $r=n\frac{x}{p}$: por lo tanto n divide a r; esto es absurdo, pues r es estrictamente menor que n.
Por lo tanto $n=pm$. Juntando esta ecuación con la de $pr=nx$ se obtiene que m divide a r. □

A continuación se caracterizan los polinomios irreducibles de grado fijo invariantes por traslación como los factores irreducibles de un polinoimo determinado. Esto es análogo al resultado en el que se ha visto que el polinomio ciclotómico de orden r factoriza en polinomios irreducibles de orden r.

Teorema 3.12 *Sea f un polinomio mónico, irreducible, de grado n con coeficientes en $\mathbb{F}_q$ un cuerpo de característica p. Se considera el polinomio $F_{k,b} = x^{q^k} - x + b$. El polinomio f divide a $F_{k,b}$ si y sólo si se cumplen:*

i) $f(x+b) = f(x)$

ii) *p divide a n. Es decir, $n = pm$.*

iii) *Además, el m anterior divide a k.*

iv) $\frac{k}{m} \not\equiv 0 \text{ mód } p$

Demostración: Hay que demostrar una doble implicación; se comienza suponiendo que f divide a $F_{k,b}$.

i) Sea θ una raíz de f; es también, por tanto, raíz de $F_{k,b}$, y cumple $\theta^{q^k} = \theta - b$. Además, como θ es raíz de f, también lo es θ^{q^k}, y por tanto se tiene que $\theta - b$ es raíz de f. Queda así probado que f es invariante por traslación.

ii) Se ha probado en el punto anterior que f es invariante por traslación. Haciendo uso de la Proposición 3.11, es inmediato que p divide a n.

iii) Como $n = pm$ divide a pk, es inmediato que m divide a k.

iv) Para ver este último punto se va a usar la proposición anterior. Sea $r = mín\{s \in \mathbb{N} : \theta^{q^s} = \theta - b\}$: r satisface $0 < r < pm$ y m divide a r: $r = mt$. Entonces, dividiendo las desigualdades anteriores entre m, $0 < t < p$. Como $\theta^{q^k} = \theta - b = \theta^{q^r}$, $k \equiv r$ mód n, y (otra vez dividiendo entre m), $\frac{k}{m} \equiv t$ mód p, que es distinto de 0.

Queda así probada la primera implicación. Para el recíproco, hay que ver que f divide a $F_{k,b}$ si se cumplen los cuatro puntos anteriores.
Sea, otra vez, θ una raíz de f. Usando la proposición anterior, $\theta^{q^{tm}} = \theta - b$, y como $k \equiv tm$ mód n, $\theta^{q^k} = \theta - b$. Es decir, θ cumple la ecuación de $F_{k,b}$ y es por tanto raíz suya, y por tanto f divide a $F_{k,b}$. □

Dado que todas las raíces de $F_{m,b}$ son simples, es posible expresarlo como el producto de los polinomios que lo dividen:

$$x^{q^m} - x + b = \prod_{d|k} \prod f$$

donde para el segundo producto se toman los polinomios mónicos, irreducibles, invariantes por traslación de grado d.

Después de haber visto el teorema anterior, el siguiente resultado es prácticamente inmediato:

Corolario 3.13 *El número de polinomios sobre $\mathbb{F}_q$ (de característica p) mónicos, irreducibles e invariantes por traslación de grado n es:*

$$|T_n| = \frac{p-1}{pm} \sum_{d|m, mcd(q,d)=1} \mu(d) q^{\frac{m}{d}}$$

si $n = pm$(es decir, p divide al grado), y 0 en otro caso.

Demostración: Tomando grados a ambos lados de $x^{q^k} - x + b = \prod_{d|k} \prod f$, se obtiene que $q^k = \sum_{d|k} \sum pd|T_{pm}^j|$, donde T_{pm} es el conjunto de polinomios mónicos, irreducibles e invariantes por traslación de grado pm, y se considera su partición en los conjuntos T_{pm}^j, de igual cardinal, donde los elementos de cada T_{pm}^j son aquellos en los que $t = j$ (el mismo t de la demostración anterior, con $r = mt$...).

i) Se demuestra a continuación que el cardinal de T_{pm}^j es independiente de j: para ello, se comprueba que para todo j con $0 < j < n$ existe una biyección entre T_{pm}^j y T_{pm}^1.
Dicha biyección viene dada por la aplicación:

$$\Psi : T_{pm}^1 \to T_{pm}^j$$

$$f(x) \to j^{-n} f(jx)$$

La aplicación inversa de Ψ es:

$$\Psi^{-1} : T_{pm}^1 \to T_{pm}^j$$

$$g(x) \to j^n f(\frac{1}{j}x)$$

Es trivial comprobar que ambas son inyectivas y, por tanto, biyectivas.

Como la partición de T_{pm} se hace en $p-1$ conjuntos (j varía entre 0 y p), el cardinal de cada T_{pm}^j es $\frac{1}{p-1}|T_{pm}|$. Sustituyendo en la ecuación,

$$q^k = \sum_{d|k, \frac{k}{d} \not\equiv 0 \text{ mód } p} \frac{p}{p-1} d|T_{pd}|$$

Para alcanzar el resultado, lo único que queda por hacer es utilizar la fórmula de Inversión de Möbius, como se viene haciendo en todas las demostraciones de este tipo. □

Como ejemplo del resultado se estudia una vez más el caso en el que $n = 30$ y $q = 2$. ¿Cuántos polinomios mónicos, irreducibles, invariantes por traslación de grado 30 hay en $\mathbb{F}_2$?

En este caso, como $q = 2$ primo, $p = 2$. Como p divide al grado ($30 = 2 \cdot 15$), el número de polinomios no es 0, y se puede usar la fórmula para calcularlo:

$$|T_{30}| = \frac{2-1}{2 \cdot 15} \sum_{d|15, mcd(2,d)=1} \mu(d) 2^{\frac{15}{d}}$$

En el subíndice del sumatorio aparece la condición de que el máximo común divisor de d y 2 sea 1: esto es equivalente a que d sea impar, y por tanto el resultado que se obtiene, en esta ocasión, es casualmente el mismo que con los polinomios autorrecíprocos. Se comprueba:

$$\begin{aligned}|T_{30}| &= \frac{2-1}{2\cdot 15}\sum_{d|15, mcd(2,d)=1}\mu(d)2^{\frac{15}{d}} \\ &= \frac{1}{30}(\mu(1)\cdot 2^{15}+\mu(3)\cdot 2^5+\mu(5)\cdot 2^3+\mu(15)\cdot 2) \\ &= \tfrac{1}{30}(2^{15}-2^5-2^3+2) \\ &= 1091\end{aligned}$$

Una vez más, el número de polinomios mónicos irreducibles invariantes por traslación es muy pequeño comparado con el de mónicos irreducibles.

3.3. Invariantes por homotecia

Definición 3.14 *Sea a un elemento de $\mathbb{F}_q$ distinto de 0 y de 1. Un elemento f de $\mathbb{F}_q[x]$ es **invariante por la homotecia** $x \longmapsto ax$ si $f(ax) = f(x)$.*

Por ejemplo, el polinomio $f(x) = x^4 + x^2 + 1$ perteneciente a $\mathbb{F}_3[x]$ es invariante por la homotecia $x \longmapsto 2x$, pues $2^4x^4 + 2^2x^2 + 1 = 16x^4 + 4x^2 + 1 = x^4 + x^2 + 1$; es decir, se recupera el polinomio original.

Durante esta sección se va a estudiar el número de polinomios mónicos, irreducibles e invariantes por homotecia que hay en un cuerpo finito. Para ello se necesitan algunos resultados de ellos, muchos de ellos análogos a los que se han usado para contar los polinomios invariantes por traslación. La referencia usada en esta sección también es [7].

Se comienza caracterizando las raíces de los polinomios invariantes por homotecia: el siguiente lema se utilizará implícitamente en muchas de las demostraciones de este apartado.

Lema 3.15 *Sea f un polinomio invariante por la homotecia $x \to ax$. Se tiene que θ es raíz de f si y sólo si $\frac{\theta}{a}$ es raíz de f.*

Demostración: Dado que f es invariante por la homotecia $x \to ax$, se puede escribir $f(x) = f(ax)$. Si θ es raíz de f, $f(\frac{\theta}{a}) = f(a\frac{\theta}{a}) = f(\theta) = 0$ y por tanto $\frac{\theta}{a}$ también es raíz de f. La implicación contraria se deduce utilizando la misma cadena de igualdades. □

Proposición 3.16 *Sea f un polinomio mónico, irreducible, invariante por la homotecia $x \to ax$ de grado $n \geq 2$, y θ una raíz suya. Entonces el orden de a en $\mathbb{F}_q$, $ord(a)$, divide a n ($n = ord(a)m$), el conjunto $R_a(\theta) := \{s \in \mathbb{N} : \theta^{q^s} = \frac{\theta}{a}\}$ es no vacío, y su elemento mínimo $r := mínR_a(\theta)$ satisface $0 < r < n$, m divide a r y $mcd(\frac{r}{m}, ord(a)) = 1$.*

Demostración: Se considera el polinomio $f(ax)$: su coeficiente principal es a^n. Como f es mónico e invariante por esta homotecia, $a^n = 1$ y por tanto el orden de a divide a n.
Como θ es una raíz de $f(x)$, $\frac{\theta}{a}$ es también raíz de $f(x) = f(ax)$. Entonces existe un único valor

r distinto de 0 (si no, a sería 1) tal que $\frac{\theta}{a} = \theta^{q^r}$.
Se sabe que las raíces son de la forma θ^{q^i} donde $0 \leq i < n$, todas distintas, dado que sobre un cuerpo finito f siempre es separable. Entonces el valor r tendrá que ser estrictamente menor que n, y ya se tiene $0 < r < n$.
Sólo queda comprobar que existe un elemento mínimo r al que m divide y de tal forma que $\frac{r}{m}$ y $ord(a)$ son coprimos. Es fácil ver que para todo j natural, $\theta^{q^{jr}} = \frac{\theta}{a^j}$. Se demuestra aplicando inducción:

i) En el caso en el que $j = 1$, se obtiene $\theta^q = \frac{\theta}{a}$. Las otras raíces son $\theta_i = \theta^{q^i}$; entonces $\theta_i = \frac{\theta^{q^i}}{a} = \frac{\theta^{q^i}}{a^{q^i}} = (\frac{\theta}{a})^{q^i}$, recuperando lo anterior.

ii) Para ver que es cierto para todo j natural, se supone cierto para j y se estudia el caso $j+1$: $\theta^{q^{(j+1)r}} = \theta^{q^{jr+r}} = \theta^{q^{jr}q^r} = (\theta^{q^{jr}})^{q^r} = (\frac{\theta}{a^j})^{q^r}$, aplicando la hipótesis de inducción. Además, $(\frac{\theta}{a^j})^{q^r} = \frac{\theta^{q^r}}{(a)^j} = \frac{\theta}{a^{j+1}}$, teniendo en cuenta una vez más que a es un elemento de $\mathbb{F}_q$ y el caso en el que $j = 1$.

Tomando $j = ord(a)$, $\theta^{q^{ord(a)r}} = \theta$. Por lo tanto, dado que f (cuyo grado es n) es el polinomio mínimo de θ, es inmediato que $\theta^{q^n} = \theta$, y $n = ord(a)m$ divide a $ord(a)r$, de lo que se deduce que m divide a r.
El valor r asociado al conjunto $R_a(\theta)$ no depende de θ:

i) Sea $\theta_i = \theta^{q^i}$ (donde $0 \leq i < n$) una raíz cualquiera: $(\theta^{q^i})^{q^r} = (\theta^{q^r})^{q^i} = \frac{\theta q^i}{a q^i} = \frac{\theta_i}{a}$, teniendo en cuenta que, como a es un elemento de $\mathbb{F}_q$, $a^{q^i} = a$.

Se escribe $r = tm$. Dado que r es un elemento del conjunto anterior, $\theta^{q^r} = \theta^{q^{tm}} = \frac{\theta}{a}$. Sea $mcd(t, ord(a)) = u$:

i) Si $ord(a) = ul_1$, $\theta^{q^{tml_1}} = \theta^{q^{rl_1}} = \frac{\theta}{a^{l_1}}$

ii) Del mismo modo, si $t = ut_1$, entonces $\theta^{q^{t_1 ord(a)m}} = \theta^{q^{\frac{t}{u} ul_1 m}} = \theta^{q^{tml_1}} = \frac{\theta}{a^{l_1}}$

De esto se deduce que $ord(a) = l_1$, pues $\theta^{q^{t_1 ord(a)m}} = \theta^{q^{t_1 n}} = \theta^{q^{nt_1}} = (\theta^{q^n})^{t_1} = \theta$.Por lo tanto tiene que ocurrir $u = 1$; es decir, $t = \frac{r}{m}$ y $ord(a)$ han de ser coprimos. □

A partir de esta proposición que se acaba de ver es posible dar la siguiente definición, que permite simplificar la notación durante el resto de la sección.

Definición 3.17 *El **tipo** de un polinomio f en las condiciones de la proposición anterior es $t_f = \frac{r}{m}$.*

A continuación, como en el caso de los polinomios invariantes por traslación, se caracterizan los polinomios irreducibles de grado fijo e invariantes por homotecia como los factores irreducibles de un polinomio determinado.

Teorema 3.18 *Sea f un polinomio mónico, irreducible, de grado n con coeficientes en $\mathbb{F}_q$ un cuerpo de característica p. Se considera el polinomio $G_{k,a} = x^{q^k-1} - \frac{1}{a}$. El polinomio f divide a $G_{k,a}$ si y sólo si se cumplen:*

i) $f(ax) = f(x)$

ii) El orden de a, $ord(a)$*, divide a* n*. Es decir,* $n = ord(a)m$*.*

iii) Además, el m *anterior divide a* k*.*

iv) $\frac{k}{m} \equiv t_f$ mód $ord(a)$*.*

Demostración: Se comienza suponiendo que f divide a $G_{k,a}$. Sea θ una raíz de f. Entonces:

i) Como θ también es raíz de $G_{k,a}$, $\theta^{q^k-1} = \frac{1}{a}$. Multiplicando todo por θ, se obtiene que $\theta^{q^k} = \frac{\theta}{a}$: es decir, las raíces de $f(x)$ también son raíces de $f(ax)$ (y al revés).

ii) Se deduce de manera inmediata a partir de I) y de la proposición anterior.

iii) De I) se deduce como en la demostración de la proposición anterior que ($\theta^{q^{jr}} = \frac{\theta}{a^j}$) tomando $j = ord(a)$, $\theta^{q^{ord(a)k}} = \frac{\theta}{a^{ord(a)}} = \theta$. De aquí se deduce que n divide a $ord(a)k$. Como $n = ord(a)m$, entonces m divide a k.

iv) Como f es invariante por homotecia de grado $n = ord(a)m$, entonces se concluye que $\theta^{q^{t_f m}} = \theta^{q^r} = \frac{\theta}{a}$. Por lo tanto, $t_f m \equiv k$ mód $ord(a)m$, lo cual significa que $\frac{k}{m} \equiv t_f$ mód $ord(a)$, como se quería ver.

Recíprocamente, se supone que se cumplen las cuatro condiciones y se va a ver que θ es también raíz de $G_{k,a}$.
Como θ es raíz de f, $\theta^{q^{tm}} = \frac{\theta}{a}$. De IV) se deduce que $k \equiv tm$ mód $ord(a)m$, ya que $\frac{k}{m} \equiv t_f$ mód $ord(a)$, $\frac{k}{m} = t_f + ord(a)h$ y se puede despejar $k = t_f m + ord(a)mh$; entonces, $k \equiv t_f m$ mód $ord(a)m$.
Por lo tanto, $\theta^{q^{tm}} = \theta^{q^k} = \frac{\theta}{a}$. Dividiendo todo entre θ, se obtiene $\theta^{q^k-1} = \frac{1}{a}$: por lo tanto θ también es raíz de $G_{k,a}$. □

Una vez visto este resultado, como en los casos anteriores, se trabaja con factorizaciones de $G_{a,k}$ y se estudia su grado para contar cuántos polinomios mónicos, irreducibles invariantes por homotecia hay en $\mathbb{F}_q[x]$.

Corolario 3.19 *El número de polinomios mónicos, irreducibles e invariantes por la homotecia* $x \to ax$ *que hay en* $\mathbb{F}_q[x]$ *es:*

$$|H(a,q,n)| = \frac{\varphi(ord(a))}{ord(a)n} \sum_{d|m,(\frac{m}{d},ord(a))=1} \mu(d)(q^{\frac{m}{d}} - 1)$$

si $n = ord(a)m$*, y* 0 *en caso contrario.*

Demostración: Del teorema anterior se sigue que se puede descomponer $G_{k,a} = \prod_{d|k,(\frac{k}{d},ord(a))=1} \prod_{f \in H_{\frac{k}{d}}(q,n)} f$,
donde $H_t(q,n)$ es el conjunto de polinomios mónicos, irreducibles, invariantes por homotecia de tipo t.

A continuación, dado $j > 0$, se utiliza la relación entre el conjunto de polinomios de tipo jt^{-1} invariantes por la homotecia $x \to ax$, y el de polinomios de tipo j invariantes por la homotecia $x \to a^t x$: es fácil comprobar que estos dos conjuntos son iguales si $mcd(j, ord(a)) = mcd(t, ord(a)) = 1$. En primer lugar, se deduce que $ord(a^t) = ord(a)$: sea ahora θ una raíz de f. Teniendo en cuenta la proposición 3.16 y la definición del tipo, se deduce que f es invariante por la homotecia $x \to a^t x$ si y sólo si $\theta^{q^{jm}} = \frac{\theta}{a^t}$; esto a su vez se cumple si y sólo si $\theta^{q^{jt^{-1}m}} = \frac{\theta}{a}$, que es condición necesaria y suficiente para que f sea de tipo jt^{-1} e invariante por la homotecia $a \to ax$.

Se consideran ahora los polinomios $G_{k,a^t} = x^{q^k-1} - \frac{1}{a^t} = \prod_{d|k(\frac{k}{d})=1} \prod_{f \in H_{\frac{k}{dt}}(q,n)} f$ para cada t entre 0 y $ord(a)$ con $mcd(t, ord(a)) = 1$, y su producto:

$$\begin{aligned}
\prod_{\substack{0<t<ord(a)\\(t,ord(a))=1}} G_{k,a^t} &= \prod_{\substack{0<t<ord(a)\\(t,ord(a))=1}} \prod_{\substack{d|k\\(\frac{k}{d},ord(a))=1}} \prod_{f \in H_{\frac{k}{dt}}(q,n)} f \\
&= \prod_{\substack{d|k\\(\frac{k}{d},ord(a))=1}} \prod_{\substack{0<t<ord(a)\\(t,ord(a))=1}} \prod_{f \in H_{\frac{k}{dt}}(q,n)} f \\
&= \prod_{\substack{d|k\\(\frac{k}{d},ord(a))=1}} \prod_{\substack{0<t<ord(a)\\(t,ord(a))=1}} \prod_{f \in H_t(q,n)} f \\
&= \prod_{\substack{d|k\\(\frac{k}{d},ord(a))=1}} \prod_{f \in H(q,n)} f.
\end{aligned}$$

Tomando grados a ambos lados de la ecuación, se obtiene:

$$\varphi(ord(a))(q^k - 1) = \sum_{d|k,(\frac{k}{d},ord(a))=1} ord(a)d|H(q, ord(a)d)|$$

Lo único que queda para demostrar el resultado es aplicar el teorema de Inversión de Möbius (teorema 1.24), como se ha hecho en ocasiones anteriores. Para ello se necesitan las condiciones adecuadas: se divide la ecuación entre $\varphi(ord(a))$, se escribe m en vez de k y se utiliza el carácter de Dirichlet, definido de la siguiente manera: $\chi_1(\frac{m}{d}) = 1$ si $mcd(\frac{m}{d}, ord(a)) = 1$ y 0 en caso contrario.
La fórmula queda: $q^n - 1 = \sum_{d|m} \frac{ord(a)d}{\varphi(a)} |H(ord(a)d)| \chi_1(\frac{m}{d})$. Se obtiene:

$$\frac{ord(a)m}{\varphi(ord(a))} |H(q, ord(a)m)| = \sum_{d|m,(\frac{m}{d},ord(a))=1} \mu(d)(q^{\frac{m}{d}} - 1)$$

Llegados a este punto sólo queda despejar. □

En esta ocasión se va a estudiar un ejemplo del teorema un poco diferente a los demás: los elementos de F_2 son 0 y 1, y no tiene sentido considerar las homotecias asociadas a ellos. Se estudia entonces el número de polinomios mónicos, irreducibles e invariantes por homotecias, de grado $n = 30$ en $F_5[x]$:

i) Invariantes por $x \to 2x$ y $x \to 3x$; en $\mathbb{F}_5^*$, es fácil comprobar que $ord(2) = ord(3) = 4$. Como 30 no es múltiplo de 4, no hay ningún polinomio con estas características.

ii) Invariantes por $x \to 4x$: en este caso $ord(4) = 2$, que sí divide a 30. Se aplica entonces la fórmula: $|H(4, 5, 30)| = \frac{\varphi(2)}{2 \times 15} \sum_{d|15,(\frac{15}{d},2))=1} \mu(d)(5^{\frac{15}{d}} - 1) = \frac{1}{30}((5^{15} - 1) - (5^5) - 1) - (5^3 - 1) + (5 - 1)) = 1017252504$.

Es difícil comparar este número con la cantidad de polinomios mónicos e irreducibles de grado 30 que hay en el cuerpo porque este último es demasiado grande como para calcularlo con exactitud, aunque se estima que es del orden de 10^{20}. En cualquier caso, la proporción es de un orden muy pequeño.

3.4. Traza prescrita

A la hora de contar polinomios irreducibles con ciertas características, cobra especial importancia el número de polinomios irreducibles con algún coeficiente predeterminado. Durante esta sección se intentará determinar el número de polinomios mónicos e irreducibles con traza determinada. Para ello se utilizará principalmente la referencia [12], y algunas observaciones de la referencia [10] que se también se pueden encontrar en el capítulo de Preliminares de este texto.

Aunque en la tercera sección del capítulo de preliminares se ha hablado de la traza de un elemento, se presenta a continuación una definición de la traza de un polinomio. Esta definición será más cómoda de usar durante esta sección.

Definición 3.20 *Sea $f(x) = x^n + ... + a_1x + a_0$ un polinomio mónico con coeficientes en $\mathbb{F}_q$. Su **traza** es $-a_{n-1}$.*

Observación 3.21 *Esta definición se relaciona con la dada en el capítulo de Preliminares en el sentido de que la traza de un polinomio es la traza de cualquiera de sus raíces.*

Se procede ahora a calcular el número de polinomios mónicos, irreducibles con traza determinada en $\mathbb{F}_[x]$. Para ello se estudian dos casos aparte:

- Cuando la traza es distinta de 0: en este caso se va a ver que no importa su valor.
- Cuando la traza es 0.

Teorema 3.22 *El número de polinomios de grado n mónicos, irreducibles con traza t en $\mathbb{F}_q$ es:*

$$N_q(n,t) = \frac{1}{qn} \sum_{d|n,(d,q)=1} \mu(d) q^{\frac{n}{d}}$$

si $t \neq 0$

Una vez obtenido este número, para calcular cuántos polinomios de este tipo hay con traza $t = 0$ sólo hay que restar todos los mónicos irreducibles menos los que tienen otras trazas:

$$N_q(n,0) = N_q(n) - (q-1)N_q(n,t)$$

Para cualquier $t \neq 0$

Demostración: Sea β un elemento de $\mathbb{F}_{q^n}$. Su traza es: $Tr(\beta) := \beta + \beta^q + \beta^{q^2} + ... + \beta^{q^{n-1}}$
Si $C(q,n)$ es el conjunto de polinomios mónicos irreducibles en $\mathbb{F}_q$ de grado n y f_β el polinomio mínimo de β, entonces se tiene lo siguiente:

$$\bigcup_{\beta \in \mathbb{F}_{q^n}} \{f_\beta\} = \bigcup_{d|n} dC(q,d)$$

Además, si se restringe la unión a los elementos β con traza t:

$$\bigcup_{\beta\in\mathbb{F}_{q^n},Tr(\beta)=t} = \{f_\beta\} = \bigcup_{d|n} \frac{n}{d}\{f \in C(q,\frac{n}{d}) : Tr(f^d) = t\}$$

En este caso la notación $\frac{n}{d}\{f \in C(q,\frac{n}{d}) : Tr(f^d) = t\}$ significa que se toman $\frac{n}{d}$ copias del conjunto. A su vez, este conjunto es:

$$\bigcup_{d|n} \frac{n}{d}\{f \in C(q,\frac{n}{d}) : dTr(f) = t\}$$

$$\bigcup_{d|n}\bigcup_{de=t} \frac{n}{d}\{f \in C(q,\frac{n}{d}) : Tr(f) = e\}$$

$$\bigcup_{d|n}\bigcup_{de=t} \frac{n}{d}\{f \in C(q,\frac{n}{d},e)\}$$

donde $C(q,\frac{n}{d},e)$ es el conjunto de polinomios mónicos irreducibles sobre $\mathbb{F}_q$ de grado $\frac{n}{d}$ y traza e.

Para continuar haciendo la demostración se pretende contar el número de elementos de los conjuntos $\bigcup_{\beta\in\mathbb{F}_{q^n},Tr(\beta)=t} \{f_\beta\}$ y $\bigcup_{d|n}\bigcup_{de=t} \frac{n}{d}\{f \in C(q,\frac{n}{d},e)\}$ e igualarlos. Para obtener el cardinal del primer conjunto basta con saber que el número de elementos de $\mathbb{F}_{q^n}$ con traza t no depende de t:

i) Si se define la aplicación ρ que a cada elemento α de $\mathbb{F}_{q^n}$ lo envía a $\alpha+\gamma$, con γ un elemento fijo de traza 1, entonces, dado que la traza es aditiva, ρ envía el conjunto de x elementos de traza t al conjunto de x elementos de traza $t+1$, y x no varía.

Este es, además, el motivo por el que en la fórmula del teorema no se utiliza en ningún momento el valor t. Por lo tanto, el número de elementos β de traza t será el número de soluciones de la ecuación:

$$Tr(\beta) := \beta + \beta^q + \beta^{q^2} + ... + \beta^{q^{n-1}} = t$$

Es decir, el primer conjunto tiene q^{n-1} elementos.

Por otro lado, el segundo tiene $\sum_{d|n}\sum_{de=t} \frac{n}{d}N(q,\frac{n}{d},e)$ elementos, donde $N(q,\frac{n}{d},e)$ indica el número de polinomios mónicos irreducibles sobre $\mathbb{F}_q$ de grado $\frac{n}{d}$ y traza e (es decir, el número de elementos del conjunto $N_q(\frac{n}{d},e)$). Por lo tanto, $q^{n-1} = \sum_{d|n}\sum_{de=t}\frac{n}{d}N(q,\frac{n}{d},e)$ Haciendo uso del lema 1.25, se puede invertir esta fórmula de la siguiente manera: $N_q(n,t) = \frac{1}{nq}\sum_{d|n}\sum_{de=t}\mu(d)q^{\frac{n}{d}}$.

Se considera ahora el caso en el que t es distinto de 0, suponiendo (como siempre) que q es potencia de un primo p. Si p no divide a d, entonces la ecuación $de = t$ tiene una única solución para e. Por tanto, si $t \neq 0$, $N_q(n,t) = \frac{1}{qn}\sum_{d|n,(d,q)=1}\mu(d)q^{\frac{n}{d}}$ □

Una vez más se va a estudiar a modo de ejemplo el caso en el que $q = 2$ y $n = 30$. ¿Cuál es el número de polinomios de grado 30 mónicos, irreducibles con traza 1 en $\mathbb{F}_2$? ¿Y con traza 0?

i) Con traza 1: $I_2(30,1) = \frac{1}{60}\sum_{d|30,(d,2)=1}\mu(d)2^{\frac{30}{d}}$. Los divisores impares de 30 son $\{1,3,5,15\}$: es decir, sustituyendo en la fórmula, $I_2(30,1) = \frac{1}{60}(\mu(1)2^{30} + \mu(3)2^{10} + \mu(5)2^6 + \mu(15)2^2) = 17895679$

ii) Con traza 0: $I(2,30,0) = N_2(30) - I(2,30,1) = 35790267 - 17895679 = 17894588$

3.5. Binomios

Al principio del capítulo 2 de este documento se han definido los binomios. A lo largo de esta sección se pretenden dar resultados encaminados a hallar el número de binomios mónicos e irreducibles que hay en un cuerpo finito.

Se comienza con una observación de carácter trivial acerca de cuándo un binomio es irreducible.

Observación 3.23 *Sea f un binomio de grado n: $f(x) = ax^n + bx^{n-i}$, con $i > 0$ un número natural. Para que f sea mónico e irreducible, tiene que ocurrir:*

i) $a = 1$ *(mónico)*

ii) $i = n$ *y* $b \neq 0$*: si no, x sería un factor de f, que ya no sería irreducible.*

Esto quiere decir que, a la hora de estudiar la irreducibilidad de los binomios sobre $\mathbb{F}_q$, sólo se tendrán en cuenta los de tipo $x^n - a$ para algún $a \in \mathbb{F}_q$.

En el capítulo anterior se dio la definición de radical de un número. A continuación se amplía este concepto:

Recuérdese que el **radical** de un número $rad(n)$ es su mayor divisor libre de cuadrados. Se define también:

$$rad_4(n) = \begin{cases} rad(n) & \text{si } n \text{ 4 no divide a n} \\ 2rad(n) & \text{si } n \text{ 4 divide a n} \end{cases}$$

Este número será útil en el siguiente resultado, cuyo propósito es calcular el número de binomios irreducibles de $\mathbb{F}_q[x]$. También será importante para esto el teorema 2.15, que caracteriza los binomios irreducibles y que se ha visto en el capítulo anterior. Más información acerca del número de binomios irreducibles se puede encontrar en la referencia [8].

Teorema 3.24 *El número de binomios mónicos e irreducibles de grado n en $\mathbb{F}_q[x]$ es:*

$$B_q(n) = \frac{\varphi(n)}{n}(q-1)$$

si $rad_4(n)$ divide a $q-1$ y 0 en otro caso.

Demostración: Partiendo del teorema 2.15, se utilizan la primera y la tercera condición para ver que $rad_4(n)$ divide a $q-1$: es fácil ver que $rad(n)$ divide siempre a $q-1$, con lo que el caso en el que 4 no divide a n queda resuelto. Por otra parte, $rad_4(n)$ es $2rad(n)$ si 4 divide a n: como $q \equiv 1$ mód 4, 4 sí divide a $q-1$; aunque no a $rad(n)$, que es libre de cuadrados y múltiplo de 2. En este caso, por tanto, $2rad(n) = rad_4(n)$ también divide a $q-1$. (Si esto no se cumple, se contradice el lema anterior y por lo tanto el número $B_q(n)$ de binomios mónicos e irreducibles de grado n es 0).
Entonces, el número de binomios con estas características sería:

$$B_q(n) = \sum_{a \in T} 1$$

donde $T = \{a \in \mathbb{F}_q^* : rad(n)|ord(a), mcd(n, \frac{q-1}{ord(a)}) = 1\}$.
Como $\mathbb{F}_q^*$ es un grupo cíclico de orden $q-1$, para todo j divisor de $q-1$ existe un elemento de $\mathbb{F}_q^*$ de orden j. De hecho, hay $\varphi(j)$ elementos de orden j en $\mathbb{F}_q^*$. Entonces el sumatorio queda como:

$$B_q(n) = \sum_{j \in T'} \varphi(j)$$

donde $T' = \{j : j|(q-1), rad(n)|j, mcd(n, \frac{q-1}{j}) = 1\}$.
Se descompone ahora $q-1 = RS$ con R el mayor divisor de $q-1$ que cumpla $mcd(R, rad(n)) = 1$. Es decir, todos los divisores de s son divisores de n. Entonces, para todo j divisor de $q-1$, las condiciones:

i) $rad(n)$ divide a j

ii) $mcd(n, \frac{q-1}{j}) = 1$

se pueden reescribir como: $j = Sd$ para algún d divisor de R. Entonces,
$B_q(n) = \sum_{d|R} \varphi(Sd) = \sum_{d|R} \varphi(S)\varphi(d) = \varphi(S) \sum_{d|R} \varphi(d) = \varphi(S)R = \frac{\varphi(n)}{n} SR$
$= \frac{\varphi(n)}{n}(q-1)$, como se quería probar. □

Por ejemplo, este teorema se puede usar para calcular el número de binomios irreducibles de grado $n = 2$ sobre $\mathbb{F}_7$: en primer lugar, se comprueba que $rad_4(n) = 2$ divide a $q - 1 = 6$, y a continuación se sustituye en la fórmula, obteniendo $B_7(2) = \frac{\varphi(2)}{2}(7-1) = 3$ binomios irreducibles sobre $\mathbb{F}_7$, que son $x^2 + 1$, $x^2 + 2$ y $x^2 + 4$. El resultado también sirve para deducir que no hay ningún binomio irreducible de grado 4 sobre $\mathbb{F}_7$, pues $rad_4(4) = 4$ que no divide a 6.

3.6. Otros resultados

De manera similar al caso de la traza, es posible definir la norma de un polinomio de la siguiente manera:

Definición 3.25 *Sea $f(x) = x^n + ... + a_1x + a_0$ un polinomio mónico con coeficientes en $\mathbb{F}_q$. Su **norma** es $(-1)^n a_0$.*

A continuación se ofrecen dos resultados sobre el número de polinomios mónicos, irreducibles sobre $\mathbb{F}_q$ de grado y norma fijos. En el primero se tiene en cuenta el orden, mientras que el segundo es más general. La demostración de estos resultados se puede encontrar en [15].

Se recuerda la siguiente notación, que se ha utilizado anteriormente en este mismo capítulo: $D_n = \{r : r|(q^n - 1)$ pero r no divide a $q^m - 1\ \forall m < n\}$.

Lema 3.26 *Sean q una potencia de primo, n un entero. Sea $r \in D_n$ con $r = d_r m_r$, donde $d_r = mcd(r, \frac{q^n-1}{q-1})$. Si $a \in \mathbb{F}_q^*$ y $ord(a) = m_r$, entonces el número $N_q(n, a, r)$ de polinomios mónicos, irreducibles sobre $\mathbb{F}_q$ de grado n, orden r y norma $(-1)^n a$ es:*

$$N_q(n, a, r) = \frac{\varphi(r)}{n\varphi(ord(a))}$$

Teorema 3.27 *En las condiciones del lema anterior, el número $N_q(n,a)$ de polinomios mónicos, irreducibles sobre $\mathbb{F}_q$ de grado 30 y norma $(-1)^n a$ es:*

$$N_q(n,a)\frac{1}{n\varphi(ord(a))}\sum_{\substack{r\in D_n\\ ord(a)=m_r}}\varphi(r)$$

En el caso de $\mathbb{F}_2$, para que un polinomio sea irreducible es evidente que su norma tiene que ser $a=1$, y que por tanto $ord(a)=1$. Si se buscan polinomios de grado $n=4$, se tiene que $D_n=\{r : r|15 \text{ pero } r \text{ no divide a } 1,3,7\ \forall m<n\}=\{5,15\}$. Por tanto sólo hay polinomios irreducibles con estas características de orden 5 ó 15. En el primer caso, $N_2(4,1,5)=\frac{\varphi(5)}{4}=1$. Si se quiere hallar el número total, sólo habría que sumar ambos casos (es decir, aplicar el segundo resultado) para obtener que hay $N_2(4,1)=\frac{1}{4}\sum_{\substack{r\in\{5,15\}\\ ord(a)=m_r}}\varphi(r)=\frac{1}{4}(4+8)=3$ polinomios de grado 4 y norma 1 irreducibles sobre $\mathbb{F}_2$.

Es posible además estudiar el comportamiento asintótico del número de polinomios irreducibles de cierto grado en los que han sido fijadas tanto la traza como la norma. En la referencia [9] se pueden encontrar más detalles y resultados sobre este número. En particular, las dos proposiciones que se presentan a continuación:

Proposición 3.28 *El número $N_q(n,t,a)$ de polinomios irreducibles sobre $\mathbb{F}_q$ de grado n, traza t y norma a cuando $n\to\infty$ cumple:*

$$N_q(n,t,a)=\frac{q^n-1}{nq(q-1)}+\mathcal{O}(q^{\frac{n}{2}})$$

Para acotar el error de esta fórmula hay un resultado general; sin embargo, tratando por separado los casos en los que la traza se anula o no, la cota puede ser más refinada:

Proposición 3.29 *El número $N_q(n,t,a)$ de polinomios irreducibles sobre $\mathbb{F}_q$ de grado n, traza t y norma a cuando $n\to\infty$ cumple:*

i) $\left|N_q(n,t,a)-\frac{q^n-1}{nq(q-1)}\right|<\frac{2}{q-1}q^{\frac{n}{2}}$ *si* $t\neq 0$

ii) $\left|N_q(n,0,a)-\frac{q^{n-1}-1}{n(q-1)}\right|<\frac{2}{q-1}q^{\frac{n}{2}}$

Es de fácil comprobación que si p es un polinomio autorrecíproco de grado $2n$, entonces existe un polinomio f de grado n tal que $p(x)=x^n f(x+x^{-1})$. Esto se puede generalizar de la siguiente manera: si se toman dos polinomios $g(x)=a_2x^2+a_1x+a_0$ y $h(x)=b_2x^2+b_1x+b_0$, se considera la transformación de f, $p(x)=h(x)^n f(\frac{g(x)}{h(x)})$. La siguiente proposición es una generalización del teorema sobre el número de polinomios srim irreducibles que Carlitz dio en su momento, y se puede encontrar en la referencia [1]

Proposición 3.30 *El número de polinomios irreducibles f de grado n sobre $\mathbb{F}_q$ cuya transformación $p(x) = h(x)^n f(\frac{g(x)}{h(x)})$ también es irreducible viene dado por:*

$$\begin{cases} 0 & \text{si } a_1 = b_1 = 0 \text{ y } q \text{ es potencia de } 2 \\ \dfrac{q^n - 1}{2n} & \text{si } q \text{ es impar y } n \text{ es potencia de } 2 \\ \dfrac{1}{2n} \displaystyle\sum_{\substack{d|n \\ d \text{ impar}}} \mu(d) q^{\frac{n}{d}} & \text{en otro caso} \end{cases}$$

Bibliografía

[1] O. Ahmadi Generalization of a theorem of Carlitz Finite Fields and their Applications 17, 473-480, 2011

[2] I.F. Blake, X. Gao, R.C. Mullin, S.A. Vanstone, T. Yaghoobian; Applications of Finite Fields, 1993 Springer Science+Business Media New York

[3] A. Braat, Counting irreducible polynomials over finite fields, 2018 Utrecht University

[4] L. Carlitz, Some theorems on irreducible reciprocal polynomials over a finite field, Journal für die reine und angewandte Mathematik 227, 212-220, 1967

[5] S.K. Chebolu, J.Mináč; Counting Irreducible Polynomials over Finite Fields Using the Inclusion-Exclusion Principle, Mathematics Magazine 84 (5), 369-371, 2011

[6] P. Fernández-Ferreirós, Teoría de Galois, Universidad de Cantabria

[7] T. Garefalakis, On the action of $GL_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$, Journal of Pure and Applied Algebra 215 (8), 1835-1843, 2011

[8] R. Heyman, I.E. Shparlinski; Counting irreducible binomials over finite fields, Finite Fields and Their Applications, 38, 1-12, 2016

[9] B.O. Koma The Number of Irreducible Polynomials Over a Finite Field With Prescribed Coefficients Sharif University, 1995

[10] R. Lidl, H. Niederreiter; Introduction to finite fields and their applications, 1986 Cambridge University Press

[11] H. Meyn, On the Construction of Irreducible Self-Reciprocal Polynomials Over Finite Fields, Applicable Algebra in Engineering, Communication and Computing, 43-53, 1990

[12] C.R. Miers, F. Ruskey, J. Sawada; The number of irreduciblie polynomials and Lyndon word with given trace, SIAM Journal on Discrete Mathematics 14 (2), 240-245, 2001

[13] G.L. Mullen, D. Panario; Handbook of finite fields, 2013 CRC Press

[14] Z-X. Wan, Lectures on Finite Fields and Galois Rings, 2003 World Scientific Publishing Co Pte Ltd

[15] J.L. Yucas, Irreducible polynomials over finite fields with prescribed trace/prescribed constant term Finite Fields and Their Applications, 12, 211-221, 2006